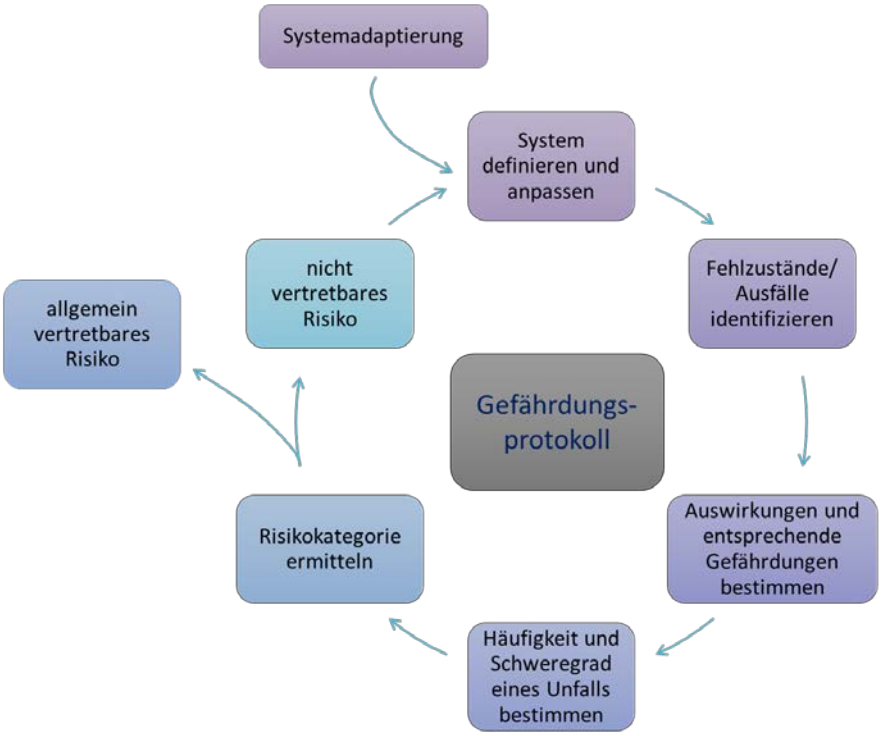
Deutsches Zentrum für
Schienenverkehrsforschung beim
Eisenbahn-Bundesamt

Berichte
des Deutschen Zentrums
für Schienenverkehrsforschung

Bericht 21 (2022)

Anwendung der CSM-Verordnung 402/2013/EU für das Teilsystem "Verkehrsbetrieb und Verkehrssteuerung"



Berichte des Deutschen Zentrums
für Schienenverkehrsforschung, Nr. 21 (2022)
Projektnummer 2018-S-3-1217

Anwendung der CSM-Verordnung 402/2013/EU für das Teilsystem "Verkehrsbetrieb und Verkehrssteuerung"

von

Jenny Oelsner, Dr. Jens Buder, Dr. Michael Dieter Kunze

CERSS Kompetenzzentrum Bahnsicherungstechnik GmbH, Dresden

Im Auftrag des Deutschen Zentrums für Schienenverkehrsforschung beim Eisenbahn-Bundesamt

Impressum

HERAUSGEBER
Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt

August-Bebel-Straße 10
01219 Dresden

www.dzsf.bund.de

DURCHFÜHRUNG DER STUDIE
CERSS Kompetenzzentrum Bahnsicherungstechnik GmbH
Bernhardstraße 77
01187 Dresden

ABSCHLUSS DER STUDIE
September, 2021

REDAKTION
DZSF
Zaki Kebdani, Dr. Thomas Buder, Prof. Dr.-Ing. Martin Lehnert, Forschungsbereich Sicherheit

BILDNACHWEIS
CERSS Kompetenzzentrum Bahnsicherungstechnik GmbH

PUBLIKATION ALS PDF
https://www.dzsf.bund.de/Forschungsergebnisse/Forschungsberichte

ISSN 2629-7973

doi: 10.48755/dzsf.220005.01

Dresden, Februar 2022

Inhaltsverzeichnis

Kurzbeschreibung / Abstract **7**

1 Einleitung **9**
1.1 Motivation 9
1.2 Herangehensweise 9
1.3 Abgrenzung 11

2 Klassifizierung von grundlegenden Prozessen **13**
2.1 Sicherheitsbescheinigung 13
2.2 Sicherheitsmanagementsystem im fiktiven EVU 13

3 Vorläufige Systemdefinition und Signifikanzprüfung **15**
3.1 Vorläufige Systemdefinition des fiktiven EVU 15
3.2 Sicherheitsrelevanz- und Signifikanzprüfung 16

4 Systemdefinition **17**
4.1 Methodisches Vorgehen 17
4.1.1 Produktorientierte Systemdefinition 17
4.1.2 Prozessorientierte Systemdefinition 18
4.2 Produktorientierte Systemdefinition im fiktiven EVU 20
4.3 Prozessorientierte Systemdefinition im fiktiven EVU 22
4.3.1 Fahrt durchführen 22
4.3.2 Fahrzeug abrüsten 23
4.4 Zusammenfassung der Systemdefinition im fiktiven EVU 24

5 Gefährdungsermittlung und -einstufung **26**
5.1 Methodisches Vorgehen 26
5.2 Beschreibung einzelner Methoden 29
5.2.1 Fehlzustandsart- und -auswirkungsanalyse 29
5.2.2 Ereignisbaumanalyse 30
5.2.3 Risikomatrix 32
5.3 Ausgewählte Gefährdungen im fiktiven EVU 34
5.3.1 Gefährdung bei fehlendem Personal im Notfallmanagement 34
5.3.2 Gefährdungen bei Dispositionstätigkeiten durch Fehler im computergestützten System 35
5.3.3 Gefährdungen bei Abstellung eines Güterzugs mit Gefahrgut 37
5.3.4 Gefährdungen bei technischen Fehlern des Zugintegritätssystems 39

6 Risikoevaluierung 41
6.1 Methodisches Vorgehen 41
6.1.1 Zugrundelegung von Regelwerken 41
6.1.2 Heranziehung eines Referenzsystems 44
6.1.3 Explizite Risikoabschätzung 44
6.2 Risikoevaluierung im fiktiven EVU 47
6.2.1 Zugrundelegung von Regelwerken und Risikoevaluierung 47
6.2.2 Heranziehung eines Referenzsystems und Risikoevaluierung 52
6.2.3 Explizite Risikoabschätzung und -evaluierung 55
7 Bestimmung der Sicherheitsanforderungen 58
7.1 Methodisches Vorgehen 58
7.1.1 Kategorien der Sicherheitsanforderungen 58
7.1.2 Sicherheitsanforderungen im Risikomanagementverfahren 59
7.2 Sicherheitsanforderungen und -maßnahmen im fiktiven EVU 60
7.2.1 Nachweis bei Zugrundelegung von Regelwerken 61
7.2.2 Nachweis bei Heranziehung eines Referenzsystems 61
7.2.3 Nachweis bei expliziter Risikoanalyse 61
8 Zusammenfassung und Ausblick 63
Abkürzungsverzeichnis 65
Abbildungsverzeichnis 67
Tabellenverzeichnis 69
Quellenverzeichnis 70
Anhänge 72

Kurzbeschreibung

Der vorliegende Forschungsbericht zum Thema „Anwendung der CSM-Verordnung 402/2013/EU für das Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“ durchläuft am Beispiel eines neu in den deutschen Schienenverkehr eintretenden, fiktiven Eisenbahnverkehrsunternehmens (EVU) beispielhaft das Risikomanagementverfahren gemäß [CSM15]. Der Fokus liegt dabei auf der Darstellung des methodischen Vorgehens. Insbesondere soll somit eine Hilfestellung für die Durchführung des CSM-konformen Risikomanagementverfahrens im Bereich betrieblicher und organisatorischer Änderungen konzipiert werden, um so vor allem Branchenneueinsteigern eine Hilfestellung zu geben.

Strebt ein EVU die erstmalige Teilnahme am Eisenbahnbetrieb in Deutschland an, so wird dies im Rahmen dieses Forschungsprojekts als betriebliche und organisatorische Änderung am Eisenbahnsystem definiert. Folglich ist ein Risikomanagementverfahren zur Bewertung der Auswirkungen auf das Sicherheitsniveau und die Erfüllung der Sicherheitsanforderungen nach [CSM15] anzuwenden. Hierfür werden verschiedene Methoden zur Durchführung des Risikomanagementverfahrens eingeführt und diese anhand des fiktiven EVU beispielhaft vorgestellt.

Es sei an dieser Stelle betont, dass die für das fiktive EVU dargelegten Erkenntnisse für real existierende EVU unterschiedlich und daher nicht unmittelbar übertragbar sind. Durch differente Anwendungsbedingungen oder abweichende Prozesse und Sicherheitsmanagementmaßnahmen lassen sich andere Gefährdungen, Schäden oder Eintrittswahrscheinlichkeiten identifizieren. Auch variierende Fehler und Ausfälle können sich ergeben.

Abstract

This study deals with the topic “Implementation of the CSM regulation (EU) 402/2013 for the operation and traffic management subsystem”. This research report provides the risk management process for an operational and organisational change of a new railway operator in Germany according to [CSM15]. Thereby, the methodological approach is applied in order to provide assistance for new entrants to the German railway market.

Within the bounds of this study, a railway operator aspiring to take part in the railway system in Germany for the first time is recognised as a change in the railway system. Consequently, a risk management process is required to assess the impact on safety levels and compliance with safety requirements. For this purpose, various methods are described. Based on a fictive railway operator, the application of this process is presented.

Please note that the described examples are different to real railway operators. The findings are not directly applicable. Due to different service conditions, processes and safety management policies, varying hazards, injuries or probabilities of occurrence might be identified. Diversifying failures and faults could also be the consequence.

1 Einleitung

1.1 Motivation

Strebt ein Eisenbahnverkehrsunternehmen (EVU) die erstmalige Teilnahme am Eisenbahnbetrieb in Deutschland an, so wird dies im Rahmen dieses Forschungsprojekts als Änderung am Eisenbahnsystem definiert. Folglich ist ein Risikomanagementverfahren zur Bewertung der Auswirkungen auf das Sicherheitsniveau und die Erfüllung der Sicherheitsanforderungen nach der Durchführungsverordnung über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken [CSM15] anzuwenden. Nachfolgend wird die konsolidierte Durchführungsverordnung als CSM-Verordnung bezeichnet.

Ziel der CSM-Verordnung ist es, mithilfe von gemeinsamen Sicherheitsmethoden (Common Safety Methods – CSM) das Vorgehen zur Beurteilung von Risiken im Bahnsystem allgemeingültig festzulegen und u. a. bei der Ermittlung von Auswirkungen auf das Sicherheitsniveau des Eisenbahnsystems verbindlich anzuwenden. Somit kann durch eine Harmonisierung von Risikomanagementverfahren im gesamten Gebiet der Europäischen Union der „Zugang zum Markt für Schienenverkehrsdienste“ [CSM15] erleichtert werden.

Das Risikomanagementverfahren wird für betriebliche und organisatorische Änderungen bisher noch nicht in einem vergleichbaren Umfang angewandt, wie es bei technischen Änderungen im Eisenbahnsystem der Fall ist. Im Rahmen dieses Forschungsprojekts soll daher eine exemplarische Durchführung des in [CSM15] definierten Verfahrens für ein beispielhaftes EVU vorgestellt werden. Insbesondere soll eine Hilfestellung für die Durchführung des CSM-konformen Risikomanagementverfahrens im Bereich betrieblicher und organisatorischer Änderungen konzipiert werden, um so vor allem Branchenneueinsteigern eine Hilfestellung zu geben.

1.2 Herangehensweise

Um eine Hilfestellung für die Anwendung der CSM-Verordnung herauszuarbeiten, wird im Forschungsprojekt ein exemplarisches Vorgehen betrachtet.

Anhand des Beispiels eines neu in den deutschen Schienenverkehrsmarkt eintretenden, fiktiven EVU soll die Anwendung des Risikomanagementverfahrens gemäß CSM-Verordnung dargelegt werden. Dieses fiktive EVU strebt die Teilnahme am Eisenbahnbetrieb mit Personenbeförderung inklusive der Durchführung von Hochgeschwindigkeitsverkehren sowie Gütertransporten, einschließlich des Transports von gefährlichen Gütern, an. Konkrete Strecken, welche durch die Fahrzeuge des fiktiven EVU befahren werden, sind nicht Gegenstand dieses Berichts.

Der Ablauf des Risikomanagementverfahrens ist in der Anlage zu Anhang I [CSM15] dargestellt. Abbildung 1 veranschaulicht die darin definierten Vorgehensweisen abstrahiert.

Ein Risikomanagementverfahren nach [CSM15] beginnt mit folgenden Verfahrensschritten:

- vorläufige Systemdefinition,
- Sicherheitsrelevanz- und Signifikanzprüfung sowie
- Systemdefinition.

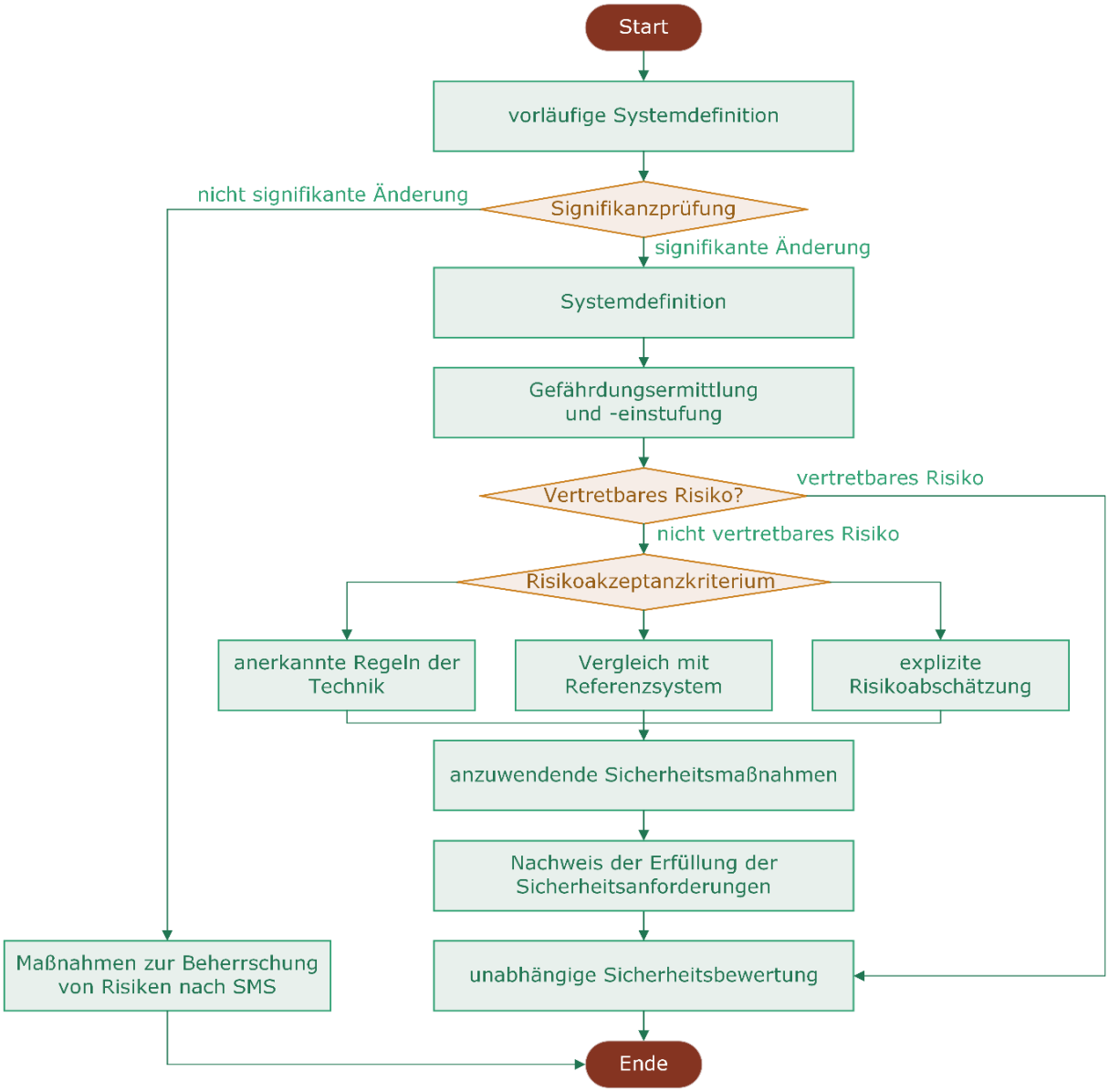


Abbildung 1: Ablauf des Risikomanagementverfahrens nach [CSM15]

Bei Feststellung einer sicherheitsrelevanten und signifikanten Änderung wird eine CSM-konforme Systemdefinition erstellt. Die technischen Spezifikationen für die Interoperabilität des Teilsystems „Verkehrsbetrieb und Verkehrssteuerung“ [TSI19] (TSI OPE – technical specifications for interoperability relating to the operation and traffic management subsystem) dient für die vorliegenden Betrachtung als Grundlage. Dabei wird die Systemdefinition sowohl produkt- als auch prozessorientiert dargestellt. Sie richtet sich nach den in Anhang I Punkt 2.1.2 [CSM15] angegebenen Aspekten.

Ausgehend von der herausgearbeiteten Systemdefinition werden potenzielle Gefährdungen identifiziert und bewertet. Die Gefährdungsermittlung soll alle Gefährdungen identifizieren, die aus dem System selbst und seinen Wechselwirkungen mit den interagierenden Systemen innerhalb definierter Systemgrenzen erwachsen können. Grundsätzlich werden sicherheitsrelevante Abläufe und Tätigkeiten im System betrachtet und potenzielle Versagensarten inklusive deren Auswirkungen auf das Gesamtsystem (Eisenbahnbetrieb in Deutschland) in einem Gefährdungsprotokoll erfasst. Simultan zur Gefährdungsermittlung erfolgt eine Identifizierung und Bewertung von potenziellen Konsequenzen. Dabei werden mögliche

Schadensquellen und die bei Eintreten der Gefährdung daraus resultierenden Folgen bestimmt. Die so durchgeführte Risikoabschätzung dient der Selektion von allgemein vertretbaren und nicht tolerierbaren Gefährdungen. Hierbei kommt die Methode der Risikomatrix zur Anwendung.

Alle nicht vertretbaren Gefährdungen werden später in der Risikoevaluation weiter untersucht. Dies erfolgt unter Anwendung der drei Risikoakzeptanzgrundsätze:

- Zugrundelegung von Regelwerken,
- Heranziehung eines Referenzsystems sowie
- explizite Risikoabschätzung.

Abschließend werden auf Basis der Ergebnisse der Anwendung der Risikoakzeptanzgrundsätze Sicherheitsanforderungen bestimmt und Sicherheitsmaßnahmen festgelegt. Das wesentliche Ziel hierbei besteht darin, entsprechende Festlegungen zu treffen, damit der erstmalige Betrieb von Eisenbahnverkehr in Deutschland durch das fiktive EVU mit vertretbaren Risiken aufgenommen werden kann.

1.3 Abgrenzung

Die in diesem Forschungsprojekt dargelegte Beschreibung eines fiktiven EVU weist zum Teil stark abweichende Systembestandteile oder Abläufe im Vergleich zu realen Eisenbahnverkehrsunternehmen auf. Hintergrund dessen ist, dass alle Schritte des Risikomanagements nach [CSM15] in vollem Umfang durchlaufen werden sollen. So werden z. B. unterschiedliche Abläufe und vollkommen neue Systemkomponenten des fiktiven EVU einschließlich definierter Prozesse beschrieben. Das Ziel des Forschungsprojekts besteht nicht in der Vorgabe der Organisation eines EVU, sondern in der beispielhaften Durchführung des Risikomanagements gemäß CSM-Verordnung. Dementsprechend liegt der Fokus auf den angewandten Methoden und nicht auf der beispielhaften Darstellung des fiktiven EVU. Aus dem gleichen Grund können identifizierte Gefährdungen ggf. konstruiert oder gar abwegig erscheinen.

Die in Kapitel 5 beschriebene Systemdefinition stellt zunächst ein vorläufiges Abbild des Systems dar. Das liegt darin begründet, dass in den nachfolgenden Kapiteln der gesamte Prozess des Risikomanagementverfahrens durchlaufen werden soll. Ein System, welches bereits von Beginn an alle potenziellen Gefährdungen durch eingesetzte Komponenten und Verfahren (Barrieren) eliminiert, ist hierfür nicht zweckdienlich. Gleichfalls soll mit Hilfe der hier dargelegten Prozessschritte der Sicherheitsgewinn durch Beachtung des Risikomanagementverfahrens aufgezeigt werden.

Die Systemdefinition behandelt lediglich sicherheitsrelevante Prozesse und Bestandteile des betrachteten fiktiven EVU. Sie soll nicht das gesamte fiktive EVU repräsentieren, sondern vornehmlich das EVU in der Durchführung von Eisenbahnverkehrsbetrieb und -steuerung beschreiben. Dies ist darin begründet, dass die Systemdefinition nur der vorbereitende Schritt für die nachfolgende Gefährdungsermittlung und Risikobewertung ist.

Eine detaillierte Beschreibung der vollumfänglichen Organisationsstruktur des fiktiven EVU beinhaltet der Nachweis der Anforderungen an das Sicherheitsmanagementsystem (SMS). Das zugrunde gelegte SMS gehört jedoch explizit nicht zu den hier beschriebenen Dokumentationen des Risikomanagementverfahrens. Es wird vorausgesetzt, dass das betrachtete fiktive EVU das eingeführte SMS hinreichend protokolliert. Auf die dafür vorzuhaltenden Dokumente wird an den betreffenden Stellen innerhalb des Forschungsprojekts verwiesen. Das liegt darin begründet, dass eine umfangreiche Beschreibung aller Prozesse, Beteiligter, Nachweise und sonstiger Belege des SMS den Rahmen des Forschungsprojekts überschreiten würde.

Auf eine konkrete Betrachtung spezieller Risiken, welche z. B. streckenspezifisch bei Tunnelfahrten bestehen können, sei an dieser Stelle aufgrund von Vereinfachung verzichtet.

Die berücksichtigten Ausfallursachen und Fehler sind ausschließlich zufälliger Natur. Es wird nicht davon ausgegangen, dass absichtliche Fehlhandlungen der Beschäftigten des fiktiven EVU auftreten. Das bedeutet, dass Missbrauch und bewusste Fehlbedienungen nicht in die Überlegungen einbezogen werden. Dies ist ein bei Risiko- und Sicherheitsbetrachtungen gängiges Vorgehen.

Gefährdungen in interagierenden Systemen gehören nicht zum Betrachtungsgegenstand, da ausschließlich „für das gesamte zu bewertende System und gegebenenfalls für dessen relevante Funktionen sowie dessen Schnittstellen“ [CSM15] die vorhersehbaren Gefährdungen ermittelt werden müssen. Entsprechend sind organisatorische Prozesse und technische Komponenten der interagierenden Systeme nicht zu berücksichtigen. Bei Letzterem wird vorausgesetzt, dass durch den Zulassungsprozess und inkludierter Beachtung der relevanten Normen bei der Entwicklung dieser sicherheitsrelevanten Bahnprodukte das sichere Funktionieren gewährleistet ist.

Das in Abschnitt 7.2.2 vorgestellte Referenzsystem ist ein rein fiktives computergestütztes Dispositionssystem. Jegliche Berührungspunkte mit real existierenden Systemen sind nicht beabsichtigt, da das methodische Vorgehen im Vordergrund steht.

Weiterhin sind jegliche Abschätzungen der Eintrittswahrscheinlichkeiten der expliziten Risikoabschätzung frei gewählt. Sie sollen ausdrücklich keine realistischen Angaben darstellen, da der Leser dieses Berichts die eigenen Randbedingungen detailliert untersuchen und nicht dazu verleitet werden soll, die Daten unmittelbar zu verarbeiten. Der Fokus liegt daher auch hier in der systematischen Anwendung der Vorgaben der CSM-Verordnung.

Die Implementierung der Sicherheitsanforderungen sowie der Nachweis der Erfüllung der daraus abgeleiteten Sicherheitsmaßnahmen kann nur erfolgen, wenn durch die Anwendung der Risikoakzeptanzgrundsätze die ermittelten Gefährdungen mit einem vertretbaren Niveau bewertet werden. Eine umfassende Protokollierung ist hierbei notwendig. Im Zuge der in Abschnitt 8.2 vorgestellten Bestimmung der Sicherheitsanforderungen und Festlegung von Sicherheitsmaßnahmen wird davon ausgegangen, dass für das betrachtete System dieser Nachweis vollständig vorliegt.

Es sei explizit darauf hingewiesen, dass das Forschungsprojekt keine Vorgaben für die Organisation und Konfiguration eines EVU definiert. Die hier beschriebene Ausgestaltung der Bestandteile, Abläufe und Tätigkeiten des für die betriebliche und organisatorische Änderung zugrunde gelegten Systems dient lediglich als zweckmäßige Systemdefinition für die in der CSM-Verordnung definierten Schritte zum Risikomanagement eines EVU. Der Fokus des Forschungsprojekts liegt auf dem methodischen Vorgehen der notwendigen Schritte zur Anwendung sowie des Nachweises des in Anhang I [CSM15] definierten Risikomanagementverfahrens. Entsprechend unterstützt die exemplarische Gestaltung eines EVU anhand des hypothetischen Beispiels das hier vorgestellte Verfahren zur Anwendung und zum Nachweis des Risikomanagementverfahrens und weist dementsprechend keinen normativen Charakter auf. Ein hiervon abweichendes Verfahren kann in der Praxis von den Vorschlagenden jederzeit angewandt werden.

In diesem Forschungsbericht wird für Berufs- und Funktionsbezeichnungen aus Gründen der Lesbarkeit die männliche oder weibliche Form gewählt, es sind jedoch immer alle Geschlechter angesprochen. Alle Ansprachen sind diskriminierungsfrei zu verstehen.

2 Klassifizierung von grundlegenden Prozessen

Die Prozesse der Sicherheitsbescheinigung und des SMS sowie die Anwendung der TSI OPE stehen in engem Zusammenspiel mit den Anforderungen an das Risikomanagementverfahren nach CSM-Verordnung. Sie sind jedoch nicht explizit Bestandteil des Risikomanagements nach [CSM15]. Nichtsdestotrotz können diese Prozesse nicht voneinander entkoppelt werden. Aus diesem Grund sollen grundlegende Prozesse auf Basis der Sicherheitsbescheinigung oder des Sicherheitsmanagementsystems, die im fiktiven EVU implementiert sein müssen, in reduziertem Umfang betrachtet werden.

2.1 Sicherheitsbescheinigung

Das fiktive EVU beabsichtigt den Betrieb von Eisenbahnverkehr in Deutschland aufzunehmen. Hierzu wird eine Sicherheitsbescheinigung (SiBe) gemäß § 7a Allgemeines Eisenbahngesetz [AEG20] unter Nachweis des Sicherheitsmanagementsystems gemäß Verordnung (EU) 2018/762 [SMS18] beantragt.

Im Rahmen des hier betrachteten Risikomanagementverfahrens „zur Bewertung der Auswirkungen von Änderungen auf das Sicherheitsniveau und die Erfüllung der Sicherheitsanforderungen“ [CSM15] werden nicht alle erforderlichen Tätigkeiten und Nachweise im Rahmen der Beantragung der Sicherheitsbescheinigung betrachtet.

2.2 Sicherheitsmanagementsystem im fiktiven EVU

Das fiktive EVU implementiert zur Wahrung der funktionalen Sicherheit im Eisenbahnsystem ein fundiertes und weitreichendes Sicherheitsmanagementsystem. Die Basis des SMS bildet die ausführliche Dokumentation von Prozessen, Beteiligten, Anforderungen und Rahmenbedingungen, dessen grundlegendes Dokument die Beschreibung der Sicherheitsordnung des Unternehmens ist.

Eine ausführliche Wiedergabe der Nachweise würde den Rahmen dieses Forschungsprojekts überschreiten. Daher sei nur der jeweilige Bereich, in welchem das SMS wirksam wird, benannt (siehe Abbildung 2). Eine Übersicht über ausgewählte Bereiche des SMS ist im Anhang A1 enthalten.

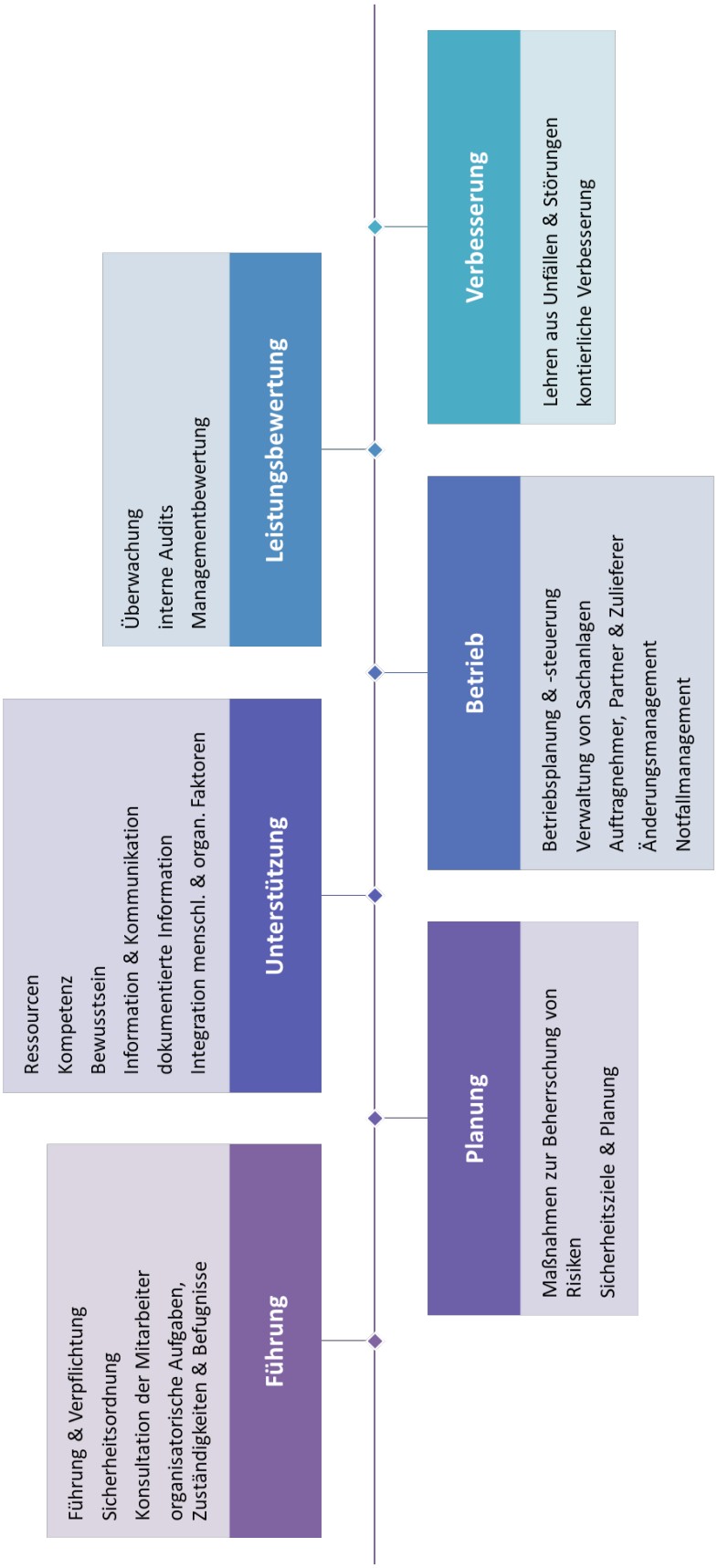


Abbildung 2: Bereiche des Sicherheitsmanagementsystem (SMS) nach

3 Vorläufige Systemdefinition und Signifikanzprüfung

3.1 Vorläufige Systemdefinition des fiktiven EVU

Im Rahmen des Risikomanagementverfahrens nach [CSM15] steht der eigentlichen Risikobewertung die Erstellung einer vorläufigen Systemdefinition voran. Diese soll dazu dienen, die Auswirkungen einer konkreten Änderung zu bestimmen. Solche Änderungen, die mit Bezug auf das bestehende Eisenbahnsystem eine Sicherheitsrelevanz und Signifikanz vorweisen, müssen das Risikomanagementverfahren vollumfänglich durchlaufen. Bei anderen Änderungen von geringerer Bedeutung kommen entsprechend [SMS18] die unternehmenseigenen Verfahren zum Umgang mit Risiken im EVU zur Anwendung.

Das fiktive EVU soll, gemäß den Vorgaben aus Abschnitt 1.2, das gesamte Spektrum des Eisenbahnbetriebs in Deutschland abdecken. Hierzu wird seitens des fiktiven EVU der Betrieb von

- Schienenpersonenverkehr (SPV) im:
  - Fernverkehr mit Hochgeschwindigkeitsverkehr und
  - Nahverkehr sowie
- Schienengüterverkehr (SGV) einschließlich der Beförderung von gefährlichen Gütern

beabsichtigt. Zugfahrten werden ausschließlich im Auftrag von Kunden (Auftraggeber und Besteller) durchgeführt. Dies bedeutet, dass die Grundlage für die Tätigkeiten des fiktiven EVU stets die Anforderung einer Schienenverkehrsbeförderungsleistung durch eine externe Partei ist.

Darüber hinaus wird das fiktive EVU Beschäftigte in den Berufsgruppen Triebfahrzeugführer/in und Zugbegleiter/in sowohl selbst beschäftigen als auch über eine Arbeitnehmerüberlassung verpflichten. Für die Disposition sowie den gesamten Managementbereich wird ausschließlich eigenes Personal eingesetzt.

Die für den Betrieb erforderlichen Fahrzeuge werden größtenteils neu angeschafft (gekauft). Es erfolgt jedoch auch der Einsatz von Fahrzeugen, die über ein Leasingunternehmen angemietet werden. Für alle genutzten Fahrzeuge gilt, dass sie über eine Inbetriebnahmegenehmigung für den Einsatz im gesamten deutschen Eisenbahnnetz verfügen.

Das fiktive EVU ist die registrierte ECM (für die Instandhaltung zuständige Stelle – Entity in Charge of Maintenance) für die eingesetzten Fahrzeuge. Dabei werden die folgenden Instandhaltungsfunktionen untervergeben und somit ausschließlich durch externe Instandhaltungseinrichtungen durchgeführt:

- Instandhaltungsentwicklung,
- Fuhrpark-Instandhaltungsmanagement und
- Instandhaltungserbringung.

Das fiktive EVU übernimmt im SGV lediglich den Transport zwischen Güterverkehrszentren (GVZ). Für die Zusammenstellung der Güterzüge sowie die Be- und Entladung der Güterwagen ist jeweils ein externes Unternehmen verantwortlich.

3.2 Sicherheitsrelevanz- und Signifikanzprüfung

Vor der Durchführung des Risikomanagementverfahrens muss die Sicherheitsrelevanz und Signifikanz der betrachteten Änderung überprüft werden. Das Risikomanagementverfahren muss bei einer bestehenden sicherheitsrelevanten und signifikanten Änderung zwingend zur Anwendung kommen. Bei sicherheitsrelevanten aber nicht signifikanten Änderungen muss die Änderung durch eigene, implementierte Sicherheitsmethoden untersucht werden. Hierzu gehören geplante Instrumente und Abläufe, welche im Zuge des SMS-Prozesses *Maßnahmen zur Beherrschung von Risiken* definiert werden.

Der Fokus des Forschungsprojekts liegt in der exemplarischen Beschreibung des Risikomanagementverfahrens gemäß CSM-Verordnung. Daher ist die im Anhang 2 vorgestellte Sicherheitsrelevanz- und Signifikanzprüfung lediglich als dem Verfahren vorangestellte Zugabe zum Risikomanagementverfahren zu verstehen. Das Ergebnis ist für das fiktive EVU eine sicherheitsrelevante und signifikante Änderung. Für real existierende EVU und deren Änderungen ist zwingend eine individuelle Überprüfung vorzusehen.

4 Systemdefinition

4.1 Methodisches Vorgehen

Nachstehend werden verschiedene Verfahrensweisen, welche für die Erstellung einer Systemdefinition Anwendung finden können, beschrieben. Diese Methoden können jeweils grafisch oder textbasiert erfolgen. Eine Kombination ist ebenfalls möglich. Änderungen am Eisenbahnsystem werden durch einen Vorschlagenden definiert und eingebracht, dessen Rolle in [CSM15] festgelegt ist. Es ist eigenständig durch den Vorschlagenden zu entscheiden, welches Vorgehen für die jeweils vorliegende Änderung zielführend ist. Dabei muss ein Kompromiss im Spannungsfeld zwischen Detailgenauigkeit und zu stark verallgemeinerter Herangehensweise gefunden werden. Zwar bietet eine detaillierte Definition bessere Möglichkeiten der anschließenden Gefährdungsermittlung, es kann jedoch auch dazu führen, dass Einzelheiten, die für das Risikomanagementverfahren gar nicht von Bedeutung sind, zeitaufwändig betrachtet werden.

Damit insbesondere Branchenneueinsteigern eine Hilfestellung gegeben werden kann, welches Vorgehen sich für die jeweilige konkrete Änderung eignet, werden im Rahmen dieses Forschungsprojekts die produkt- und prozessorientierte Systemdefinition detailliert vorgestellt und in den Abschnitten 5.2 und 5.3 beispielhaft sowohl grafisch als auch textbasiert exemplarisch für das fiktive EVU realisiert.

4.1.1 Produktorientierte Systemdefinition

Die produktorientierte Systemdefinition dient dazu, die Struktur eines Systems anhand von Baugruppen und Komponenten zu beschreiben. Es entsteht eine strukturelle Unterteilung. Bei technischen Systemen können recht einfach die vorhandenen Baugruppen und Schnittstellen ermittelt werden; Baupläne stellen bereits eine produktorientierte Systemdefinition dar. Betrachtet man das betriebliche und organisatorische System des Verkehrsbetriebs und der Verkehrssteuerung, so bestehen keine Baupläne, welche herangezogen werden können. Ziel der produktorientierten Systemdefinition ist daher, den Bauplan des Unternehmens zu skizzieren. Ein Organigramm, das organisatorische Abteilungen, Ressorts und den Informationsaustausch eines Unternehmens darlegt, kann als erste Eingangsgröße dienen. Darüber hinaus benötigt es weiterer Überlegungen bezüglich der beteiligten Mitarbeitergruppen, Abteilungen und Objekte.

Eine wesentliche Anforderung an die produktorientierte Systemdefinition besteht darin, dass für die Betrachtung von beteiligten Akteuren an sicherheitsrelevanten Prozessen eine ausreichend große Detaillierung erreicht wird. Diese sollte jedoch nicht dazu führen, dass alle Einzelelemente im Unternehmen aufgeführt werden. Managementbereiche und Beschäftigtengruppen, die keinen Einfluss auf den allgemeinen (sicherheitsrelevanten) Eisenbahnbetrieb haben, müssen nicht zum Bestandteil der produktorientierten Systemdefinition im Sinne des Risikomanagementverfahrens gehören. Sie wirken sich nicht auf die Sicherheit im Bahnsystem aus und spielen daher für die Betrachtung von den zu ermittelnden spezifischen Risiken keine Rolle. Als Beispiel hierfür lässt sich die Buchhaltung eines EVU benennen. Potenzielle Fehler dieser Beschäftigtengruppe haben keine unmittelbare Auswirkung auf die Durchführung des sicheren Eisenbahnbetriebs.

Die produktorientierte Systemdefinition kann rein textbasiert erfolgen. Hierbei wird die strukturelle Unterteilung niedergeschrieben, was mit Schwierigkeiten hinsichtlich der Vollständigkeit, Verständlichkeit und Übersichtlichkeit für Außenstehende verbunden sein kann. Eine weitere Herangehensweise ist die graphische Darstellung des Systems, seiner Komponenten und deren Beziehungen untereinander (siehe Abbildung 3). Während diese Form der Darbietung eine grundsätzliche Übersichtlichkeit gewährt, kann es insbesondere für Unbeteiligte zu Interpretationsspielräumen kommen. Im vorliegenden Fall des

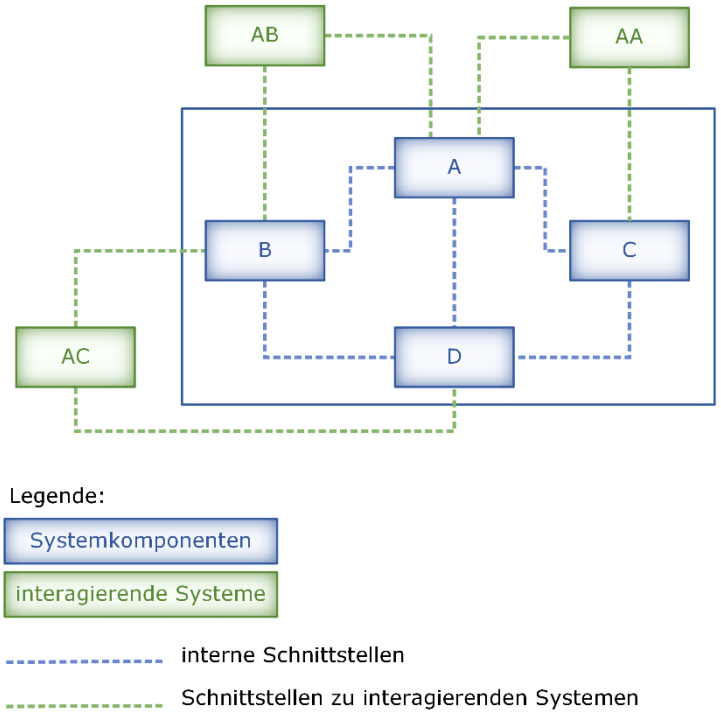


Abbildung 3: Beispielhafte Darstellung einer produktorientierten Systemdefinition

fiktiven EVU kommt deshalb eine Kombination der graphischen und verbalisierten Charakterisierung zur Anwendung. Sie soll lediglich als Beispiel dienen. Eine abweichende Darstellung der am Eisenbahnbetrieb beteiligten Personen und Gegenstände kann selbstverständlich gewählt werden.

Anhand der produktorientierten Systemdefinition können folgende Aspekte entsprechend dem Anhang I Punkt 2.1.2 [CSM15] Rechnung getragen werden:

- Bestandteile des Systems inklusive menschlicher, technischer und betrieblicher Komponenten (Aspekt b),
- Systemgrenzen inklusive interagierender Systeme (Aspekt c),
- physische Schnittstellen zu interagierenden Systemen (Aspekt d),
- Systemumgebung (im Sinne von Umfeld der betrieblichen Bewegungen der Schienenfahrzeuge und organisatorischen Entscheidungen) (Aspekt e),
- bestehende Sicherheitsmaßnahmen (Aspekt f),
- Annahmen, welche die Risikobewertung begrenzen (Aspekt g).

4.1.2 Prozessorientierte Systemdefinition

Eine weitere Möglichkeit der Systemdefinition stellt die Charakterisierung der Abläufe im Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“ mittels einer prozessorientierten Systemdefinition dar. Dabei werden einzelne Prozessschritte mit ihren Aufgaben und Tätigkeiten beschrieben.

Die prozessorientierte Systemdefinition dient dazu, die Vernetzung der Strukturelemente (Komponenten, interagierende Systeme) aufzuzeigen. Somit können Funktionen der Systemkomponenten beschrieben werden. Unter Berücksichtigung der Gefährdungsermittlung und -einstufung (siehe Kapitel 6) können infolgedessen einzelne Tätigkeiten, die potenzielle Risiken beinhalten bzw. zur Folge haben, definiert werden. Die Einbindung der menschlichen Einflussgrößen lässt sich insbesondere durch die Betrachtung der separaten Prozesse berücksichtigen.

Anhand der prozessorientierten Systemdefinition können folgende Aspekte entsprechend dem Anhang I Punkt 2.1.2 [CSM15] Rechnung getragen werden:

- Funktionen des Systems inklusive menschlicher, technischer und betrieblicher Komponenten (Aspekt b),
- interagierende Systeme (Aspekt c),
- funktionale Schnittstellen (Aspekt d),
- Systemumgebung (im Sinne von Umfeld der betrieblichen Bewegungen der Schienenfahrzeuge und organisatorischen Entscheidungen) (Aspekt e),
- bestehende Sicherheitsmaßnahmen (Aspekt f),
- Annahmen, welche die Risikobewertung begrenzen (Aspekt g).

Die prozessorientierte Systemdefinition lässt sich ebenfalls rein textbasiert dokumentieren. Hierbei werden die einzelnen Arbeitsabläufe niedergeschrieben. Dies kann auch mit Schwierigkeiten hinsichtlich der Vollständigkeit, Verständlichkeit und Übersichtlichkeit für Außenstehende verbunden sein.

Eine weitere Möglichkeit der Herangehensweise bietet die graphische Darstellung der Prozesse mittels Prozessablaufdiagrammen, wie sie Abbildung 4 exemplarisch wiedergibt. Auch hier lassen sich Fehlinterpretationen nicht ausschließen. Im Rahmen des Forschungsprojekts wird analog zur produktorientierten Systemdefinition eine Kombination der graphischen und verbalisierten Beschreibung vorgestellt.

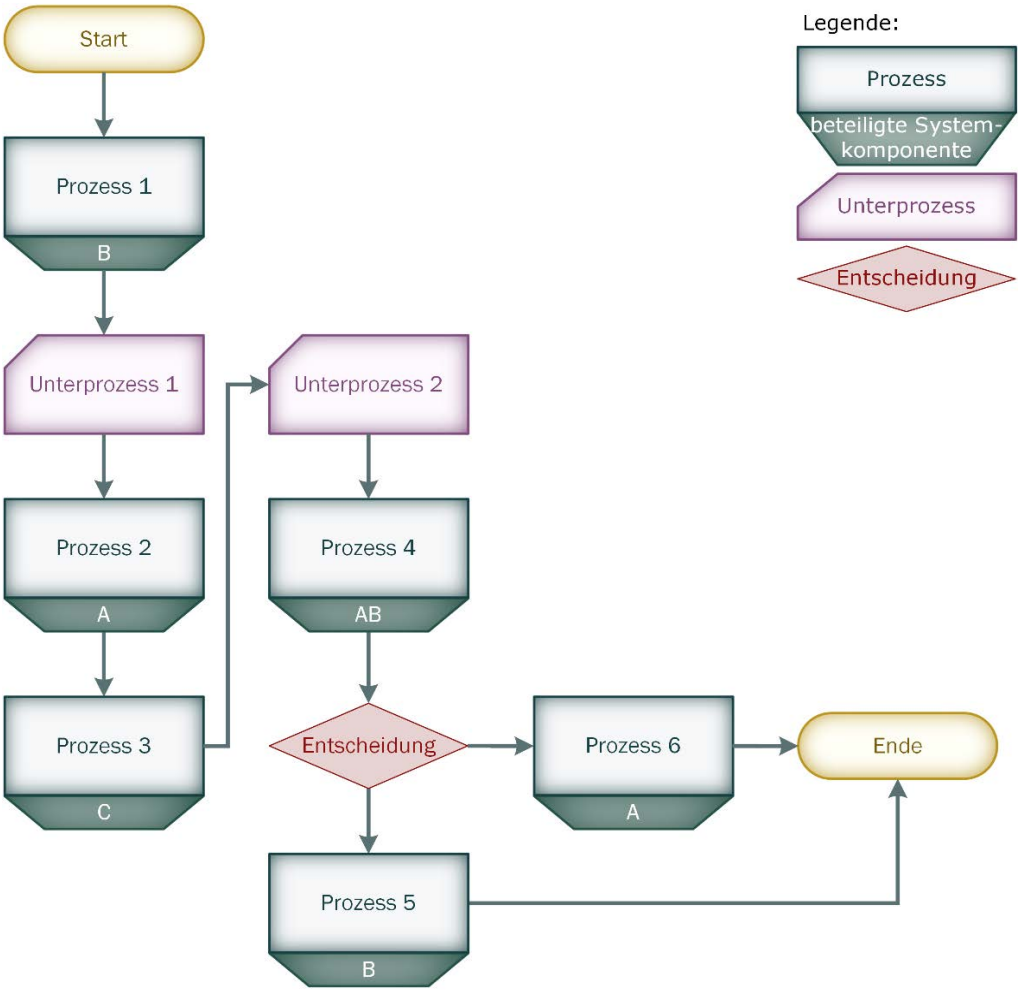


Abbildung 4: Beispielhafte Darstellung einer prozessorientierten Systemdefinition

Die überwiegende Mehrheit der in einem EVU zur Anwendung kommenden Prozesse lässt sich bereits im Zuge der Implementierung des SMS beschreiben. Da die Veranschaulichung des zugrunde gelegten SMS nicht zum Bestandteil der hier demonstrierten Arbeiten zur Dokumentation des Risikomanagementverfahrens gehört, werden bei der beispielhaften Vorstellung der prozessorientierten Systemdefinitionen für das fiktive EVU an geeigneten Stellen ebendiese Prozesse des SMS dargestellt. Dies erfolgt jedoch in unterschiedlichen Detaillierungsgraden entsprechend der für die nachfolgenden Schritte des Forschungsprojekts erforderlichen Informationen.

4.2 Produktorientierte Systemdefinition im fiktiven EVU

Dieser Abschnitt umfasst die funktionale Klassifikation des betrachteten Systems sowie die Abgrenzung zu anderen, interagierenden Systemen einschließlich ihrer Schnittstellen.

Abbildung 5 zeigt die schematische Darstellung der produktorientierten Systemdefinition für das Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“ für das fiktive EVU. Im Anhange 3 befindet sich eine großformatige Ausfertigung dieser Abbildung (siehe Abbildung A.25) sowie eine ausführliche Beschreibung der Komponenten und interagierenden Systeme.

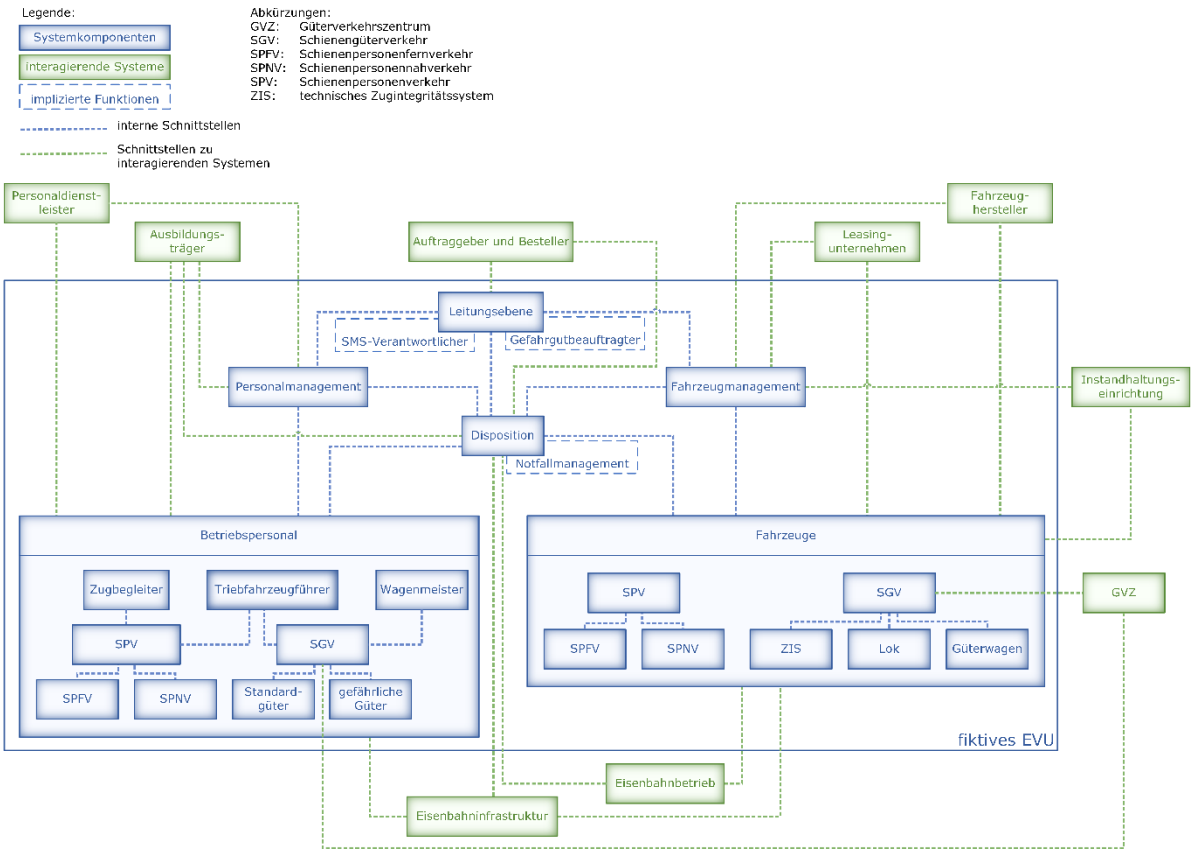


Abbildung 5: Produktorientierte Systemdefinition, Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“

Das im Fokus stehende System besteht aus Systemkomponenten (blau gekennzeichnet) und interagierenden Systemen (grün gekennzeichnet), die über Schnittstellen miteinander verbunden sind. Zu den Bestandteilen gehören:

- die Bereiche:
  - Leitungsebene mit dem SMS-Verantwortlichen und dem Gefahrgutbeauftragten,
  - Fahrzeugmanagement,
  - Personalmanagement,
  - Disposition mit Disponenten und dem Notfallmanagement,

- das Betriebspersonal:
  - Triebfahrzeugführer:
    im SPV und
    im SGV,
  - Zugbegleiter im SPV sowie
  - Wagenmeister im SGV,

- die Komponenten:
  - Fahrzeuge:
    für SPV und
    für SGV,
  - technisches Zugintegritätssystem für Güterzüge,

- sowie die Schnittstellen zu den interagierenden Systemen:
  - Auftraggeber und Besteller,
  - (externe) Instandhaltungseinrichtung,
  - Eisenbahnbetrieb,
  - Eisenbahninfrastruktur,
  - Güterverkehrszentrum,
  - Ausbildungsträger,
  - Personaldienstleister,
  - Fahrzeughersteller sowie
  - Leasingunternehmen.

Das innovative technische Zugintegritätssystem (ZIS) ist ein rein hypothetisches System, welches allein aus dem Grund der Anwendung der expliziten Risikoabschätzung und -evaluierung nach [CSM15] im fiktiven EVU Anwendung findet. Intention des Einsatzes dieses neuartigen, in der Realität noch nicht eingesetzten Systems liegt ausschließlich in der Veranschaulichung des methodischen Vorgehens der Anwendung dieses Risikoakzeptanzgrundsatzes. Aus diesem Grund wird die Beschreibung der Komponenten und Funktionsweise des elektronischen Systems nur insoweit detailliert dargestellt, dass die explizite Risikoabschätzung und -evaluierung ermöglicht wird. Im Risikomanagementverfahren eines realen EVU müsste die Systemdefinition hingegen wesentlich umfangreicher gestaltet sein.

Es sei hierbei angemerkt, dass die Einführung eines solchen neuartigen Systems selbst schon eine eigenständige Änderung darstellt, welche ein autarkes Risikomanagementverfahren erfordert.

Das ZIS basiert auf der fortdauernden Identifikation des Gesamtgewichtes des Zuges (vgl. [WIN18]). Neben der originären Aufgabe der Feststellung der Zugintegrität eines Güterzugs soll das System auch Ladungsverlust während der Zugfahrt detektieren und dem Triebfahrzeugführer melden. Dazu besteht das System aus den in Abbildung 6 grün dargestellten Komponenten.

Abbildung 6: Schematische Darstellung des Zugintegritätssystem (ZIS)

Jeder Güterwagen des fiktiven EVU verfügt über einen Beladungssensor, der die Zuladung des Güterwagens kontinuierlich misst. Über die von allen Beladungssensoren übertragenen Daten von Eigengewicht und Zuladung ermittelt die Auswerteeinheit permanent das Gesamtgewicht des Güterzugs. Das ZIS gibt eine Warnmeldung an den Triebfahrzeugführer über eine Anzeige aus, sofern während der Fahrt eine Reduktion des Gewichts über einen definierten Schwellwert identifiziert wird. Dies kann beispielsweise durch Zugtrennung oder Ladungsverlust verursacht sein.

4.3 Prozessorientierte Systemdefinition im fiktiven EVU

Dieser Abschnitt umfasst die Charakterisierung der sicherheitsrelevanten Abläufe des betrachteten Systems sowie zwischen interagierenden Systemen. Anhang 4 charakterisiert die sicherheitsrelevanten Prozesse ausführlich. Es sei an dieser Stelle angemerkt, dass sich operative Prozesse nicht aus den Anforderungen der CSM-Verordnung ableiten lassen. Vielmehr stellen sie die Grundlage für die nachfolgenden Schritte des Risikomanagementverfahrens dar.

Abbildung 7 zeigt einen Ausschnitt eines sicherheitsrelevanten Prozesses. Einzelne Prozessschritte dieses Teilprozesses sollen für die Durchführung des Risikomanagementverfahrens als Beispiel herangezogen werden. Konkret werden bei den Prozessschritten *Halteplatz am Ausfahrgleis einnehmen*, *Zugtrennung detektieren*, *Meldung Zugtrennung an Triebfahrzeugführer*, *Abbremsen und an Zielgleis der Zugfahrt anhalten* sowie *Fahrzeug abstellen* in der Gefährdungsermittlung und -einstufung Ausfälle bzw. Fehlzustände identifiziert. Ziel dieser Darstellung ist es, ein Verständnis für die in Abschnitt 5.2.4 betrachteten Ausfälle bzw. Fehlzustände zu generieren. Zweifelsfrei können in allen anderen dargestellten Prozessschritten ebenfalls Ausfälle bzw. Fehlzustände zu Gefährdungen führen. Der gesamthafte Prozess der Fahrtvorbereitung, -durchführung und Fahrzeugabrüstung wird im Anhang 4, Unterkapitel 4.5 wiedergegeben.

Die Teilprozesse *Fahrt durchführen* sowie *Fahrzeug abrüsten* (siehe Abbildung 7) sind Bestandteil des Prozesses *Fahrt vorbereiten, durchführen und Fahrzeug abrüsten*. Die Prozessschritte sollen nachfolgend näher beschrieben werden. Dabei liegt der Fokus insbesondere auf den für das Risikomanagementverfahren relevanten bzw. zu realen EVU potenziell abweichenden Prozessschritten.

4.3.1 Fahrt durchführen

In der Ausgangslage für den Prozess *Fahrt durchführen* befindet sich der Güterzug beladen und für die anstehende Fahrt abfahrtbereit am Halteplatz des Ausfahrgleises des GVZ. Die Prozesse der *Be- und Entladung* sowie *Vorbereitungsarbeiten* werden im Anhang A4, Unterkapitel 4.5 wiedergegeben. Sobald das Ausfahrsignal am Ausfahrgleis den Fahrtbegriff zeigt, fährt der Zug ab. Der Unterprozess *Fahrt* beginnt und dauert so lange an, bis sich der Zug dem nächsten Verkehrshalt nähert.

Besonderheit an diesem Unterprozess im SGV ist der Einsatz des ZIS. Dieses System detektiert kontinuierlich während der Zugfahrt eine potenzielle Reduktion des Gesamtgewichts und gibt eine entsprechende Warnmeldung an den Triebfahrzeugführer aus. Dieser tätigt daraufhin situationsgerecht entsprechende Handlungen, um den sicheren Zustand einzunehmen und informiert die Beteiligten.

Nähert sich das Fahrzeug dem nächsten Verkehrshalt, wird die Geschwindigkeit entsprechend verringert und der Güterzug hält im vorgesehenen Zielgleis. Es schließt sich der Prozess der *Be- und Entladung* an (siehe Anhang A4 Unterkapitel 4.5.2). Der Prozessablauf wird erst beendet, wenn der letzte planmäßige Halt der Fahrt stattgefunden hat. Anschließend kann der Güterzug zum Abstellplatz gefahren werden und der Vorgang zum Abrüsten wird analog zum SPV eingeleitet.

4.3.2 Fahrzeug abrüsten

Die Fahrt zum Abstellplatz erfolgt für das Fallbeispiel des fiktiven EVU grundsätzlich als Rangierfahrt. Anschließend werden durch den Triebfahrzeugführer Tätigkeiten entsprechend des Betriebsregelwerks durchgeführt. Dazu gehören auch Eintragungen im Betriebsbuch, insbesondere durchgeführte Prüftätigkeiten und identifizierte technische Störungen. Handelt es sich bei zuletzt genannten um solche, die einer Instandsetzung bedürfen, wird der Prozess der *Instandhaltung* gestartet, anderenfalls schließt der Prozess ohne weitere Aktivität.

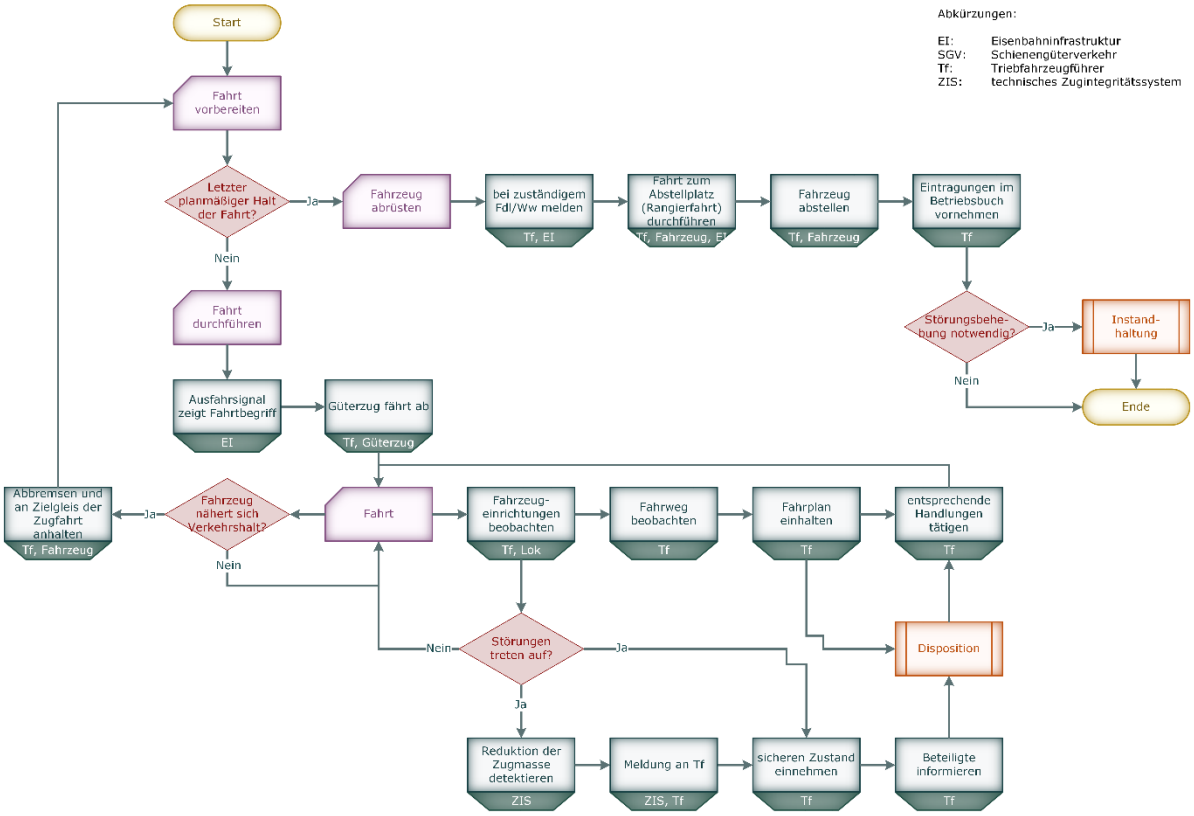


Abbildung 7: Teilprozess Fahrt durchführen und Fahrzeug abrüsten im SGV

4.4 Zusammenfassung der Systemdefinition im fiktiven EVU

Wie bereits in Abschnitt 1.2 ausgeführt, soll die Systemdefinition den Aspekten gemäß Anhang I Punkt 2.1.1 [CSM15] genügen. Hierzu gehören die nachfolgend betrachteten Bestandteile.

Zweckbestimmung des Systems

Als Zweckbestimmung kann die vorgesehene Verwendung der Änderung gesehen werden. Im vorliegenden Fall des fiktiven EVU stellt dies der erstmalige Betrieb von Schienenpersonennahverkehr (SPNV), Schienenpersonenfernverkehr (SPFV) sowie der Gütertransport von Standard- und Gefahrgut im deutschen Schienennetz entsprechend den Anwendungsgebieten der TSI OPE [TSI19] dar.

Funktionen und Bestandteile des Systems

Erforderliche Systemkomponenten sind in Abschnitt 5.2 definiert bzw. in Abbildung 5 in blau hinterlegt. Eine ausführliche Beschreibung der Komponenten findet sich im Anhang A3 (siehe Abbildung A.25). Die zu den Komponenten zugehörigen Abläufe und Tätigkeiten im Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“ veranschaulicht Anhang A4.

Systemgrenzen

Als Systemkomponenten werden lediglich am Eisenbahnbetrieb beteiligte Bestandteile des fiktiven EVU betrachtet. Infolgedessen gelten alle anderen Akteure mit Interaktionspunkten am Eisenbahnbetrieb als interagierende Systeme. Diese sind im Rahmen der Systemgrenzen zu berücksichtigen und müssen vom EVU selbst definiert werden.

Für das fiktive EVU sind die Systemgrenzen im Anhang A3, Abschnitt 3.8 beschrieben. Zudem lassen sie sich in Abbildung 5 bzw. Abbildung A.25 als grün hinterlegte, interagierende Systeme identifizieren. Diese interagierenden Systeme werden an den entsprechenden Stellen in den Prozessablaufdiagrammen berücksichtigt.

Physische und funktionale Schnittstellen

Physische und funktionale Schnittstellen bestehen zwischen dem betrachteten System und interagierenden Systemen. Sofern vorhanden, werden funktionale Schnittstellen zu den interagierenden Systemen in den Prozessbeschreibungen (siehe Anhang A4) dahingehend charakterisiert, dass die vorgesehenen Interaktionen von Komponenten bzw. Beteiligten des fiktiven EVU mit anderen Systemen und deren Komponenten bzw. Beteiligten erläutert sind. Zudem lassen sich die funktionalen Schnittstellen den Prozessablaufdiagrammen (siehe Anhang A4) entnehmen.

Systemumgebung

Die CSM-Verordnung definiert verschiedene Arten der Systemumgebung, wie „Energie- und Wärmefluss, Erschütterungen, Vibrationen, elektromagnetische Beeinflussung“ [CSM15]. Diese Arten sind v. a. bei technischen Änderungen relevant. Für betriebliche oder organisatorische Änderungen können solche Systemumgebungen kaum definiert werden.

Bei dieser betrieblichen und organisatorischen Änderung können daher Systemumgebungen lediglich im Sinne des Umfelds der betrieblichen Bewegungen der Schienenfahrzeuge und organisatorischen Entscheidungen berücksichtigt und beschrieben werden. Dies erfolgte im Rahmen der produkt- und prozessorientierten Systemdefinition.

Bestehende Sicherheitsmaßnahmen

Bereits bestehende Sicherheitsmaßnahmen sind im vorhandenen SMS definiert. Hierzu sei auf Abschnitt 2.2 bzw. Anhang A1 und den jeweiligen Anmerkungen zum Prozess (siehe Anhang A4) verwiesen. Bereits vorhandene Sicherheitsanforderungen an Komponenten des EVU bestehen zum gegenwärtigen Betrachtungszeitpunkt nicht. Diese ergeben sich angesichts der Ergebnisse des Risikomanagementverfahrens.

Annahmen, die die Grenzen der Risikobewertung bestimmen

Zu den Annahmen der Systemdefinition gehört, dass davon ausgegangen wird, dass das fiktive EVU ein fundiertes und weitreichendes SMS implementiert hat (siehe Abschnitt 2.2), sowie den Nachweis zur Sicherheitsbescheinigung gemäß § 7a [AEG20] unter Nachweis des SMS [SMS18] ordnungsgemäß und ausführlich durchläuft (siehe Abschnitt 2.1).

Darüber hinaus gelten alle Abgrenzungen, welche in den Anhängen A3und A4 definiert werden, als Randbedingungen zum System.

5 Gefährdungsermittlung und -einstufung

5.1 Methodisches Vorgehen

Für die Identifizierung und Bewertung potenzieller Gefährdungen der in Kapitel 5 definierten Änderung werden systematische Verfahren angewandt. Das Ziel besteht dabei darin, alle durch das System verursachten Gefährdungen auf den Menschen, den Betrieb und die Umwelt gezielt zu ermitteln und deren Akzeptanz bzw. Vertretbarkeit zu bestimmen. Zur Anwendung kommen hierbei diverse anerkannte Methoden, um eine möglichst strukturierte, hierarchische Herangehensweise zu erzielen. Daher gilt das in Abbildung 8 dargestellte Wirkungsmodell.

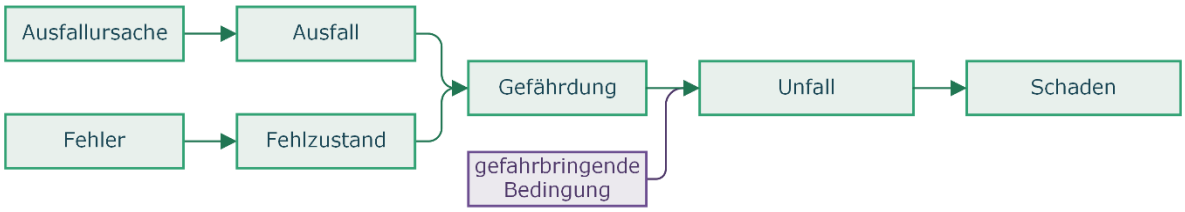


Abbildung 8: Darstellung des Wirkungsmodells

Ein Ausfall beschreibt den „Verlust der Fähigkeit [einer Komponente], wie gefordert zu funktionieren“ [EN126]. Ein Fehler wird dagegen als Status der „Nichtübereinstimmung zwischen einem [...] beobachteten oder gemessenen Wert [und] theoretisch richtige[m] Wert“ [EN126] angesehen. Im Rahmen dieses Risikomanagementverfahrens wird jedoch nicht weiter zwischen Ausfall oder Fehler unterschieden. Ebenfalls erfolgt keine Differenzierung zwischen systematischen und zufälligen Fehlern. Allerdings werden, wie bereits in Abschnitt 1.3 definiert, keine absichtlichen Fehlhandlungen im Rahmen der Gefährdungsidentifikation betrachtet.

Ein Fehler oder Ausfall führt jedoch nicht zwangsläufig zu einem katastrophalen Ereignis. Erst unter bestimmten Gegebenheiten kann aus einer Gefährdung, welche aus einem Ausfall oder Fehlzustand erwächst, ein Unfall mit resultierendem Schaden hervorgehen. Die dafür notwendige Einflussgröße wird gefahrbringende Bedingung genannt.

Im Rahmen der hier vorliegenden Analyse werden folgende typische Fehler bzw. Ausfallursachen betrachtet:

- menschliches Fehlverhalten,
- organisatorische Fehler oder
- technische Fehler.

Bei Vorhandensein führen diese zu einem Fehlzustand/Ausfall, aus dem wiederum Gefährdungen resultieren. Relevante Unfälle, die bei Risikoanalysen im Eisenbahnsystem betrachtet werden, sind beispielsweise Zugkollisionen und Zugentgleisungen. Weiterhin gehören Umweltkontaminationen, die z. B. durch ausgetretene Gefahrgüter entstehen, dazu. Die jeweiligen Unfallfolgen werden entsprechend ihres Schadensausmaßes definiert.

Mithilfe dieses Wirkungsmodells lässt sich ein Gefährdungsprotokoll erstellen. Dabei kommt der in Abbildung 9 dargestellte Ablauf zur Anwendung. Sofern nicht vertretbare Risiken identifiziert werden, erfolgt eine erneute Überprüfung und ggf. Anpassung des betrachteten Systems, was eine abermalige

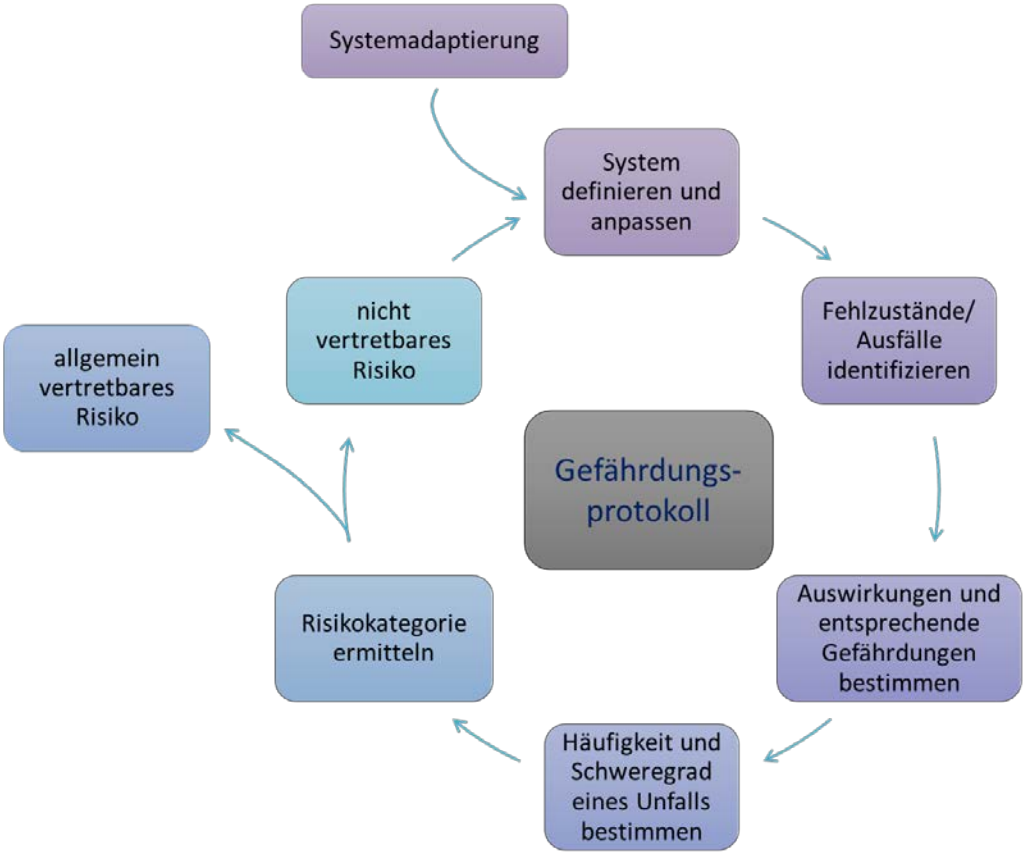


Abbildung 9: Ablauf zur Erstellung des Gefährdungsprotokolls

Durchführung der Prozessschritte zur Folge hat. Selbstverständlich können auch abweichende Verfahren zur Identifizierung und Bewertung von Gefährdungen zur Anwendung kommen. Nachfolgend soll jedoch ausschließlich das hier gewählte Verfahren näher beschrieben werden.

Entsprechend der CSM-Verordnung wird das Gefährdungsprotokoll als „die Unterlage, in der erkannte Gefährdungen, die damit zusammenhängenden Maßnahmen und die Ursachen der Gefährdungen dokumentiert [...] werden“ [CSM15], definiert.

Das Gefährdungsprotokoll wird unter Berücksichtigung der vorliegenden Änderung für alle identifizierten Tätigkeiten (Funktionen) sowie deren Schnittstellen erstellt. Dies bietet ein strukturiertes Vorgehen, um „sämtliche nach vernünftigem Ermessen vorhersehbaren Gefährdungen für das gesamte zu bewertende System“ [CSM15] betrachten zu können. Somit wird auch deutlich, warum eine ausführliche Auseinandersetzung mit den eigenen Prozessen und interagierenden Systemen einen entscheidenden Vorteil bei der Gefährdungsermittlung spielen kann.

Zunächst werden die einzelnen Prozessschritte, ihre Beteiligten und daraus resultierende Ausfallursachen und Fehler analysiert. Daraus lassen sich jeweils potenzielle Konsequenzen ableiten.

Es ist sinnvoll, Expertinnen verschiedener Bereiche bei den Überlegungen der Gefährdungsanalyse einzubeziehen. Da sie über Kenntnisse des Systems und der Prozesse verfügen, können sie potenzielle Fehlerquellen aus ihrer Erfahrung heraus identifizieren. Dagegen ermöglicht eine Einbeziehung von Außenstehenden eher, andere Gefahrenquellen im System zu bestimmen. Durch diese beidseitige Herangehensweise lässt sich ein weitreichendes, ausgewogenes Gefährdungsprotokoll erstellen. Gleichfalls empfiehlt

es sich auch solche Fehlerquellen in das Gefährdungsprotokoll aufzunehmen, die nicht zu einer Gefährdung führen. Somit wird die spätere Bearbeitung und Vertiefung bei etwaigen betrieblichen und organisatorischen Änderungen im EVU vereinfacht, da bereits potenzielle Fehlerquellen identifiziert und dokumentiert sind. Diese können bei Änderungen einfacher angepasst und hinsichtlich ihrer Risikoauswirkungen neu bewertet werden.

Bei der Gefährdungseinstufung wird die allgemeine Risikodefinition impliziert. Als Risiko wird die Kombination aus Eintrittswahrscheinlichkeit eines unerwünschten Ereignisses und dem damit verbundenen Schadensausmaß angesehen. Demzufolge kann die Wertung einer Gefährdung unter Zugrundelegung der Häufigkeit des Gefahrenfalls sowie des potenziellen Schadensausmaßes erfolgen. Im Sinne der CSM-Verordnung wird als Gefährdung der „Umstand, der zu einem Unfall führen könnte“ [CSM15] verstanden. Ein Unfall im Eisenbahnverkehr hat aufgrund der Systemeigenschaften meist ein hohes Schadensausmaß, wie z. B. (zahlreiche) Tote oder beachtliche Umweltschäden.

Die Folgen und die Häufigkeit des Gefahrenfalls werden im nächsten Schritt kategorisiert. Es gilt dabei jedoch zu beachten, dass eingesetzte Schätzungen stets einer Ungewissheit unterliegen. Durch den Einsatz formeller Methoden (siehe Abschnitte 6.1.1 und 6.1.2) kann diese Ungewissheit reduziert werden.

Darüber hinaus ist es sinnvoll, jeweils eine Begründung der Einstufung des Schadensausmaßes und der Häufigkeit des Gefahrenfalls zu dokumentieren. Somit kann auf zusätzliche Erklärungen für die unabhängige Bewertung zur Begründung der Einteilung vertretbarer Risiken weitgehend verzichtet werden. Aus der herausgearbeiteten Kombination von Schadensausmaß und Häufigkeit des Gefahrenfalls ergibt sich nun das zugeordnete Risiko.

Nach der erfolgten Gefährdungseinstufung lässt sich feststellen, welche Gefährdungen im Rahmen des weiteren Vorgehens des Risikomanagementverfahrens detailliert zu betrachten sind und welche dagegen als allgemein vertretbares Risiko eingestuft werden können. Letztere müssen dementsprechend „nicht weiter analysiert, sondern lediglich im Gefährdungsprotokoll erfasst werden“ [CSM15]. Als allgemein vertretbar gelten Gefährdungen, deren Risiko vernachlässigbar ist. Werden zusätzliche Elemente des SMS infolge eines nicht vertretbaren Risikos definiert, so sind diese entsprechend Anhang I Punkt 2.2.4 [CSM15] im Gefährdungsprotokoll zu dokumentieren.

Es sei an dieser Stelle angemerkt, dass sich die für das fiktive Beispiel vorgenommenen Einstufungen der durch die Änderung hervorgerufenen Gefährdungen keinesfalls direkt auf andere EVU übertragen lassen. Stets muss das betrachtete System sowie seine Systemgrenzen, Schnittstellen und Systemumgebungen in einer Einzelfallentscheidung analysiert werden.

[CSM15] definiert in Anhang I Punkt 2.2.6, dass die Gefährdungsermittlung in ihrem Umfang reduziert werden kann. Dies gilt unter der Bedingung, dass zur Risikobeherrschung alleinig die Zugrundelegung von Regelwerken oder die Heranziehung eines Referenzsystems angewandt wird. In diesem Fall ist es ausreichend, sich auf die Punkte

- Prüfung der Relevanz des Regelwerks/Referenzsystems und
- Identifikation von Abweichungen des Regelwerks/Referenzsystems

zu konzentrieren. Im vorliegenden Forschungsprojekt sollen hingegen alle drei Risikoakzeptanzgrundsätze exemplarisch angewandt werden, weswegen die verkürzte Gefährdungsermittlung und -einstufung nicht angewandt wird.

5.2 Beschreibung einzelner Methoden

5.2.1 Fehlzustandsart- und -auswirkungsanalyse

Das Gefährdungsprotokoll soll dazu dienen, alle Gefährdungen sowie alle entsprechenden Sicherheitsmaßnahmen und Systemannahmen, die im Zuge des Risikobewertungsverfahrens ermittelt werden, strukturiert darzustellen. Um ein organisiertes Vorgehen bei der Erstellung des Gefährdungsprotokolls zu gewährleisten, ist die Anwendung der Fehlzustandsart- und -auswirkungsanalyse – kurz FMEA – geeignet. Die FMEA (Failure Mode and Effects Analysis) stellt eine induktive Methode zur Identifizierung von Gefährdungen und ihren Auswirkungen dar. Sie wird in der Norm DIN EN 60812 [DIN812] beschrieben und besteht aus den in Abbildung 10 dargestellten Schritten. Die FMEA kann durch eine Kritikalitätsanalyse zur FMECA (Failure Mode, Effects and Criticality Analysis) erweitert werden. Dabei erfolgt eine Bewertung der relativen Bedeutung des Fehlzustands. Werden in [DIN812] FMEA und FMECA synonym verwendet, kommt in diesem Bericht FME(C)A als Bezeichnung zum Einsatz.

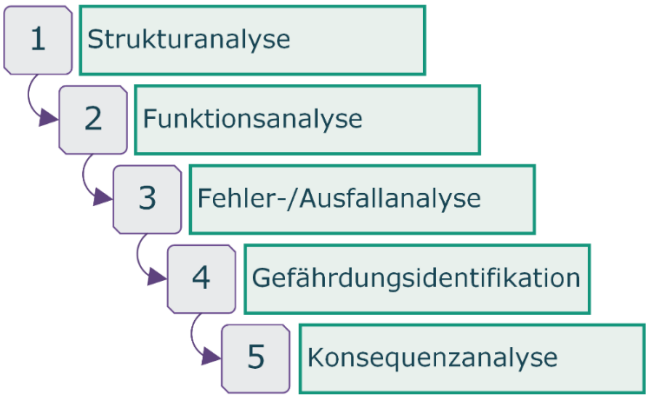


Abbildung 10: Ablauf einer FMEA nach [DIN812]

Zu Beginn der FME(C)A sind Informationen zum Aufbau des Systems und dessen Schnittstellen zusammenzutragen. Anschließend erfolgt eine Bestimmung einzelner Funktionen für jedes Strukturelement. Im Rahmen einer betrieblichen und organisatorischen Änderung sind die Funktionen als auszuführende Tätigkeiten definiert. Die ersten beiden Schritte der FME(C)A werden bereits im Rahmen der Systemdefinition durchgeführt (siehe Kapitel 5).

Im nächsten Schritt werden nun potenzielle Fehler und Ausfälle im System und seiner Komponenten sowie deren Auswirkungen analysiert. Hierfür können als Basis einfache, strukturierte Überlegungen in Form von Ursache-Wirkungs-Analysen dienen. Jede Systemkomponente oder Funktion kann dabei auf unterschiedliche Art und Weise ausfallen.

Anschließend werden potenziell gefährliche Auswirkungen für jeden einzelnen Fehler bzw. Ausfall determiniert. Die sogenannte Gefährdungsidentifikation erfolgt dabei systematisch. Ziel ist es, alle relevanten Gefährdungen durch das System auf den Menschen, den Betrieb und die Umwelt zu ermitteln. Um die vielfältigen Gefährdungen möglichst umfassend identifizieren zu können, ist es sinnvoll, die Systemdefinition mit einem hohen Detaillierungsgrad und in einem sehr ausführlichen Umfang herauszuarbeiten. Zur Gefährdungsermittlung können ebenso strukturierte Ursache-Wirkungs-Ketten angewandt werden.

Der letzte Schritt der FME(C)A ist die Konsequenzanalyse, bei der die Folgen der resultierenden Gefährdungen sowie deren Schadensausmaß einschließlich der Häufigkeit des Eintretens abgeschätzt werden. Hierzu bietet die Anwendung einer Ereignisbaumanalyse (siehe Abschnitt 5.2.2) ein geeignetes Mittel zur

Abschätzung der Folgen und Häufigkeit. Daraus lässt sich die Kritikalität des Ausfalls bzw. Fehlers bestimmen. Gemäß [DIN812] existieren zwei Methoden zur Abschätzung der Kritikalität. Zum einen kann eine Kombination aus Schwere- und Wahrscheinlichkeitskategorisierung (siehe Kapitel 5.2.3) gewählt werden.

Zum anderen ermöglicht die Methode der Risikopriorität szahl (RPZ) die Abschätzung der Kritikalität. Hierbei werden die Parameter Schweregrad, Auftretenswahrscheinlichkeit und Aufdeckungsmöglichkeit verknüpft und jeweils mittels einer Bewertungsskala von eins bis zehn abgeschätzt. Diese werden gemäß Formel 1 miteinander multipliziert.

$$RPZ = Schweregrad \cdot Auftretenswahrscheinlichkeit \cdot Aufdeckungsmöglichkeit \qquad (1)$$

Es sei jedoch angemerkt, dass es keine normative Abstufung der Bewertungsskalen und der Kritikalitätsabschätzung gibt. Aus diesem Grund wird im hier vorliegenden Beispiel die Kritikalitätsabschätzung mittels Risikomatrix (siehe Abschnitt 6.1.3) durchgeführt.

5.2.2 Ereignisbaumanalyse

Um ein streng strukturierteres Vorgehen zu ermöglichen, lassen sich an geeigneten Stellen Ereignisbäume zur Identifizierung potenzieller Auswirkungen von Fehlern, Ausfällen oder Gefahren benutzen. Prinzipiell können Ereignisbäume für jedweden Fehler und Ausfall bzw. alle Gefährdungen aufgestellt werden. Bei für die Expertenrunde eindeutigen Sachverhalten ist es jedoch bedenkenlos möglich, auf separate Ereignisbäume zu verzichten und stattdessen Entscheidungen direkt im Gefährdungsprotokoll zu dokumentieren.

Die Ereignisbaumanalyse dient zur schrittweisen Bestimmung von Folgeereignissen mit Hilfe der Erstellung eines sogenannten Ereignisbaums. Hierbei wird ein Anfangsereignis, wie z. B. ein Ausfall/Fehlzustand oder eine Gefährdung, links dargestellt. Davon ausgehend öffnen sich Äste, ähnlich eines Baums, nach rechts. Jeder Ast stellt ein potenzielles Folgeereignis des vorherigen Ereignisses dar. Daraus können wiederum vielzählige Folgeereignisse resultieren. Diese Verzweigungen lassen sich solange fortführen, bis ein anvisiertes Endergebnis erreicht wird. Ein solches Endergebnis stellt im Rahmen einer Risikobetrachtung üblicherweise ein Schadensausmaß dar, z. B. Tote oder ein Umweltschaden. Abbildung 11 zeigt einen Ereignisbaum schematisch.

Stehen statistische Größen zur Abschätzung der Auftretenswahrscheinlichkeiten der Folgeereignisse zur Verfügung, lässt sich mittels Multiplikation der Einzelwahrscheinlichkeiten die Wahrscheinlichkeit des Eintretens des anvisierten Ergebnisses ermitteln. Allerdings fehlt in der Regel bei organisatorischen oder menschlichen Fehlern eine statistisch belastbare Datengrundlage, sodass es qualitativer Aussagen von Experten zur Wahrscheinlichkeitsabschätzung bedarf. Gleichzeitig müssen die Ereignisse unabhängig voneinander sein.

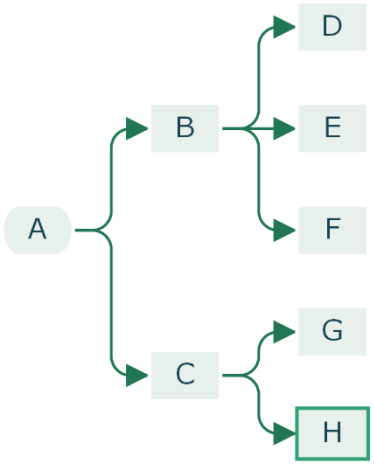


Abbildung 11: Schematische Darstellung eines Ereignisbaums

Ereignis **A** entspricht in Abbildung 11 dem Anfangsereignis. Hieraus resultieren die Folgeereignisse **B** und **C**. Ereignis **B** weist beispielhaft wiederum drei, Ereignis **C** zwei Folgeereignisse auf. Ereignis **H** stellt ein anvisiertes Endergebnis dar und ist aus diesem Grund besonders hervorgehoben. Die Quelle-Ziel-Relation **A–C–H** bildet die in einer Risikobetrachtung entscheidende Kausalkette für das anvisierte Endergebnis.

Neben der Art des in Abbildung 11 vorgestellten Ereignisbaums gibt es auch weitere Darstellungsmöglichkeiten, wie Abbildung 12 zeigt. In diesem Ereignisbaum werden Entscheidungen mit Ja und Nein beantwortet. Entsprechend ergeben sich jeweils zwei Verzweigungen. Im vorliegenden Beispiel sind Auftretenswahrscheinlichkeiten für die einzelnen Entscheidungen bekannt und am jeweiligen Ast vermerkt.

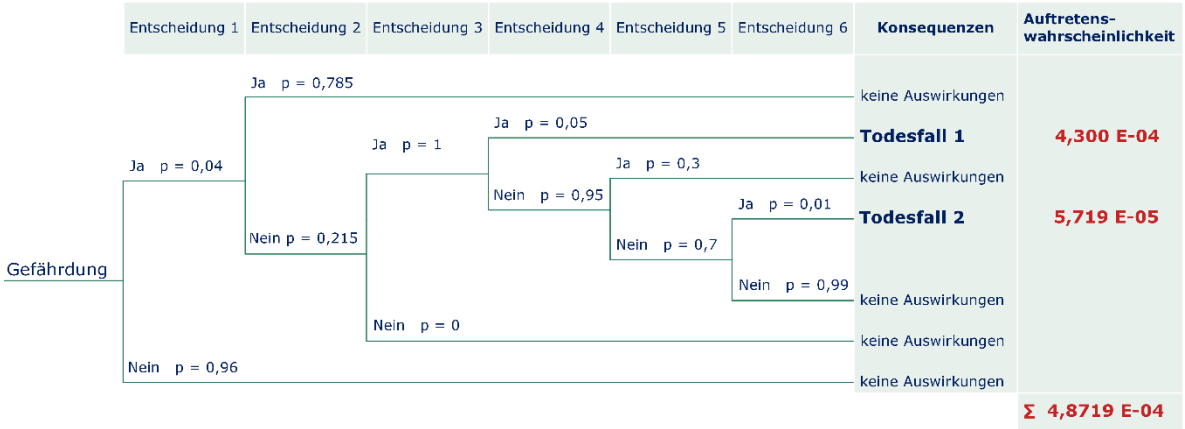


Abbildung 12: Differente Darstellung eines Ereignisbaums

Die Wahrscheinlichkeit des Eintretens eines Todesfalls bei der vorliegenden Gefährdung in Abbildung 12 kann entsprechend der Pfadregeln bei Zufallsversuchen nach Formel 2 berechnet werden.

$$P(Todesfälle) = (0{,}04 \cdot 0{,}215 \cdot 1 \cdot 0{,}05) + (0{,}04 \cdot 0{,}215 \cdot 1 \cdot 0{,}95 \cdot 0{,}7 \cdot 0{,}01) = (4{,}300 \cdot 10^{-4}) + (5{,}719 \cdot 10^{-5}) = 4{,}8719 \cdot 10^{-4} = 0{,}048719\,\% \quad (2)$$

Mittels der in Abbildung 12 definierten Wahrscheinlichkeiten der Entscheidungen wird die Auftretenswahrscheinlichkeit für einzelne Todesfälle bei der betrachteten Gefährdung aufsummiert. Für das in Abbildung 12 gezeigte Beispiel ergibt sich eine Auftretenswahrscheinlichkeit für einen Todesfall von $4{,}8719 \cdot 10^{-4}$.

Bei der Erstellung des Gefährdungsprotokolls kommt vorwiegend die erste Darstellungsart (siehe Abbildung 11) zur Anwendung, da diese Variante einen größeren Freiheitsgrad gewährleistet. So können einzelne Verzweigungen abstrahiert oder reduziert dargestellt werden. Außerdem sind im vorliegenden Beispiel der Betriebsaufnahme des fiktiven EVU keine statistischen Größen für die Berechnung von Auftretenswahrscheinlichkeiten bekannt. In diesem Fall bietet die Darstellung der Bäume gemäß Abbildung 11 eine Grundlage für fundierte Experteneinschätzungen. Damit lässt sich entsprechend der Untersuchungsziele beurteilen, welche Ereignisse häufiger oder weniger häufig eintreten werden. Für andere Fragestellungen kann selbstverständlich die Darstellungsart gemäß Abbildung 12 oder eine abweichende Form zielführender sein.

5.2.3 Risikomatrix

Das in Abschnitt 6.1 benannte Prozedere stellt abstrakt gesehen bereits eine erste Anwendung des Risikoakzeptanzgrundsatzes der expliziten Risikoabschätzung dar. Dies ist darauf zurückzuführen, dass es eines definierten Vorgehens zur Abschätzung allgemein vertretbarer Risiken bedarf. Gemäß CSM-Verordnung dürfen „[a]us Gefährdungen resultierende Risiken [...] dann als allgemein vertretbar eingestuft werden, wenn das Risiko so gering ist, dass die Einführung zusätzlicher Sicherheitsmaßnahmen nicht angemessen wäre“ [CSM15]. Eine genauere Definition stellt die CSM-Verordnung nicht bereit. Aus diesem Grund wird im Forschungsprojekt das definierte Verfahren der Risikomatrix herangezogen. Andere Verfahren sind potenziell gleichwohl geeignet, das allgemein vertretbare Risiko auf der Grundlage einer Expertenbewertung zu bestimmen.

Die Anwendung einer Risikomatrix dient der Einstufung der Kritikalität einzelner Ausfälle bzw. Fehler und ihrer potenziellen Gefährdungen. Basis dafür bildet die allgemein gültige Definition des Risikos als Kombination von Häufigkeit eines Schadens und dem dabei auftretenden Schadensausmaß. Entsprechend werden beide Faktoren in ein tabellarisches Verhältnis gesetzt.

Die Risikomatrixeinstufung erfolgt in drei Schritten (siehe Abbildung 13). Zunächst wird auf Basis der Konsequenzanalyse die Häufigkeit des Auftretens eines gefährlichen Ereignisses kategorisiert. Hierzu erfolgt eine Einteilung nach Tabelle 1.

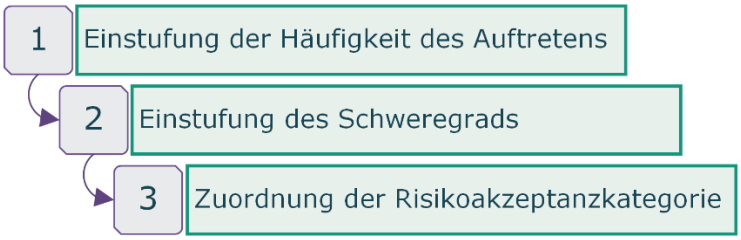


Abbildung 13: Ablauf zur Aufstellung einer Risikomatrix nach [EN126]

Eine Vorgabe zur Kalibrierung und Risikoakzeptanz wird u. a. im informativen Anhang C in der für die Entwicklung von Bahnanwendungen relevanten Norm DIN EN 50126-1 [EN126] definiert. Zwar bilden hier technische Systeme die Grundlage für die Kategorisierungen, dennoch soll aufgrund der vagen Beschreibung allgemein vertretbarer Risiken der CSM-Verordnung auf diese Methode im Rahmen dieses Forschungsprojekts zurückgegriffen werden. Die Anwendung der Risikomatrix nach [EN126] ist eine gängige und anerkannte Methode, um Risiken qualitativ zu bewerten. Darüber hinaus steht sie im Einklang mit Anhang I Punkt 2.2.3 [CSM15].

TABELLE 1: KATEGORISIERUNG DER HÄUFIGKEIT DES GEFAHRENFALLS NACH [EN126]

Häufigkeit des Gefahrenfalls	**Definition**
häufig	Es wird angenommen, dass das Ereignis ständig auftreten wird.
wahrscheinlich	Es wird angenommen, dass das Ereignis oft auftreten wird.
gelegentlich	Es wird angenommen, dass das Ereignis mehrere Male auftreten wird.
selten	Es wird angenommen, dass das Ereignis irgendwann einmal auftreten wird.
unwahrscheinlich	Es wird angenommen, dass das Ereignis ausnahmsweise auftreten kann.
sehr unwahrscheinlich	Es wird angenommen, dass das Ereignis nicht auftreten kann.

Im zweiten Schritt erfolgt die Kategorisierung des abgeschätzten Schadensausmaßes anhand der in Tabelle 2 dargestellten Prinzipien. Dabei ist nach gängigen und standardisierten Methoden das größte Schadensausmaß maßgeblich für die Kategorisierung. Wenn beispielsweise bei einem Unfall austretende Gefahrgüter einen extremen Umweltschaden (katastrophal) und gleichzeitig leichte Verletzungen (geringfügig) verursachen, dann ist der extreme Umweltschaden ausschlaggebend für die Schadensausmaßkategorie *katastrophal*.

TABELLE 2: KATEGORISIERUNG DES SCHADENSAUSMAßES NACH [EN126]

Schadensausmaß	**Definition**
katastrophal	zahlreiche Tote und/oder extremer Umweltschaden
kritisch	mindestens ein Toter und/oder schwerer Umweltschaden
geringfügig	schwere/leichte Verletzungen und/oder geringer Umweltschaden
unbedeutend	möglicherweise leichte Verletzungen

Die anschließende Risikoabschätzung kann durch Verknüpfung der Häufigkeit mit dem Ausmaß eines Gefahrenfalls vorgenommen werden. Hierbei erfolgt eine Kategorisierung unterschiedlicher Gefährdungen. Nach DIN EN 50126-1 kommt die in Tabelle 3 definierte Klassifizierung zur Anwendung. Das Ergebnis bildet eine Matrix, in der die einzelne Gefährdung einer Risikokategorie zugeordnet ist.

TABELLE 3: RISIKOKATEGORIEN NACH [EN126]

Risikokategorie	**Anzuwendende Maßnahmen**
untragbar	Risiko muss eliminiert werden.
unerwünscht	Risiko darf nur dann akzeptiert werden, wenn eine Minderung nicht durchführbar ist.
tolerabel	Risiko kann unter der Voraussetzung angemessener Kontrollen akzeptiert werden.
vernachlässigbar	Risiko ist akzeptabel.

Tabelle 4 zeigt die im Rahmen dieser Risikoabschätzung angewandte Risikomatrix.

TABELLE 4: RISIKOMATRIX NACH [EN126]

Häufigkeit	**Schadensausmaß**			
	unbedeutend	**geringfügig**	**kritisch**	**katastrophal**
häufig	unerwünscht	untragbar	untragbar	untragbar
wahrscheinlich	tolerabel	unerwünscht	untragbar	untragbar
gelegentlich	tolerabel	unerwünscht	unerwünscht	untragbar
selten	vernachlässig-bar	tolerabel	unerwünscht	unerwünscht
unwahrscheinlich	vernachlässig-bar	vernachlässig-bar	tolerabel	unerwünscht
sehr unwahrschein-lich	vernachlässig-bar	vernachlässig-bar	vernachlässig-bar	tolerabel

Werden untragbare und unerwünschte Risiken ermittelt, bedarf es Schutzmaßnahmen im Rahmen des weiteren Vorgehens. Bei tolerablen Risiken kann von weiteren Maßnahmen abgesehen werden, sofern geeignete Kontrollmaßnahmen eingeführt sind. Zu diesen geeigneten Kontrollmaßnahmen zählen die kontrollierten und wirksamen Prozesse des SMS. Es bedarf jedoch stets einer Einzelfallentscheidung.

5.3 Ausgewählte Gefährdungen im fiktiven EVU

Nachfolgend steht die Analyse der im fiktiven EVU entstehenden Gefährdungen entsprechend ihrer Kritikalität im Mittelpunkt. Dabei wird im Einklang mit dem Forschungsschwerpunkt nicht der gesamte Inhalt des Gefährdungsprotokolls des fiktiven EVU vorgestellt. Vielmehr liegt der Fokus auf den für die Anwendung der drei Risikoakzeptanzgrundsätze zugrundeliegenden nicht vertretbaren Gefährdungen.

Ein Auszug des beispielhaften Gefährdungsprotokolls für die nicht vertretbaren Gefährdungen ist im Anhang 5, Tabelle A.22 dargestellt. Es sei an dieser Stelle angemerkt, dass sich die für das fiktive Beispiel vorgenommenen Einstufungen der durch die Änderung hervorgerufenen Gefährdungen keinesfalls direkt auf andere EVU übertragen lassen. Bei real existierenden EVU können durch verschiedene Umgebungsbedingungen und Systemkomponenten stets andere, zusätzliche oder weniger Fehler, Ausfälle und Gefährdungen vorkommen. Darüber hinaus werden im Rahmen der Systemdefinition explizit Vereinfachungen wie auch Erweiterungen in den Prozessen und Komponenten des fiktiven EVU vorgenommen, um in den nachfolgenden Schritten des Risikomanagements den Fokus auf das methodische Vorgehen legen zu können.

5.3.1 Gefährdung bei fehlendem Personal im Notfallmanagement

Da nicht alle Disponenten im Notfallmanagement geschult werden, fehlen Disponenten für die Tätigkeiten bei Notfällen, wenn der Bedarf an Personal im Notfallmanagement durch Missmanagement der Personalleitung (als organisatorischer Fehler klassifiziert) nicht erkannt wird. Das beinhaltet ebenfalls die Be-

rücksichtigung und Prognose der Verfügbarkeit von Fachkräften am Arbeitsmarkt. Zu dieser Gefährdung kann es allerdings auch kommen, wenn durch menschliches Fehlverhalten der Bedarf zu spät erkannt wird. Das Gefährdungsprotokoll im Anhang 5, Tabelle A.22 gibt diese Gefährdungen in Nr. 1 und 2 wieder.

Dadurch können notwendige Maßnahmen bei Störungen und Unfällen nicht getroffen werden. Schlimmstenfalls resultieren weitere Folgeunfälle mit einem katastrophalen Schadensausmaß. Die Häufigkeit des Gefahrenfalls kann mit *selten* bestimmt werden. Hintergrund dessen ist, dass ein SMS-Prozess *Kompetenzmanagement* implementiert ist. Jedoch können trotz des strukturierten Ablaufs der *Einstellung von Mitarbeitern* unvorhergesehene längere Ausfälle von Disponenten im Notfallmanagement auftreten. Das trifft z. B. bei Schwangerschaft/Mutterschutz oder längerer Erkrankung von Beschäftigten zu. Es ergibt sich ein unerwünschtes Risiko. Außergewöhnlich hohe Krankenstände bei EVU haben auch in der Corona-Pandemie zur zeitweisen Unterbrechung des Betriebs geführt, wenn die organisatorisch vorgesehenen Reserven nicht ausreichten.

Dieses Risiko gilt entsprechend Tabelle 3 nur dann als allgemein vertretbar, „wenn eine Minderung nicht durchführbar ist“ [EN126]. Diese Definition steht im Einklang mit der Darlegung in Anhang I Punkt 2.2.3 [CSM15]. Eine geeignete zusätzliche Schutzmaßnahme ist jedoch in der Anpassung des SMS zu finden und folglich zu implementieren. Ein Vorteil der Erstellung des Gefährdungsprotokolls besteht darin, dass damit ebenfalls die eingeführten Maßnahmen im SMS überprüft und ggf. angepasst werden können. Wie Anhang I Punk 2.2.4 [CSM15] darlegt, werden die Modifikationen der Sicherheitsmaßnahmen im Gefährdungsprotokoll erfasst und es wird eine erneute Bewertung des sich ergebenden Risikos vorgenommen.

Im vorliegenden Fall erfolgt eine Anpassung des *Kompetenzmanagements* in dem Sinne, dass nun alle Disponenten im Notfallmanagement zu schulen sind. Somit lässt sich die Wahrscheinlichkeit des Gefahrenfalls reduzieren. Daraufhin kann ein sehr unwahrscheinliches Auftreten dieser Gefährdung bestimmt werden, was zu der angepassten Risikokategorie „tolerabel“ führt. Tabelle 5 gibt die Änderungen im Gefährdungsprotokoll wieder.

5.3.2 Gefährdungen bei Dispositionstätigkeiten durch Fehler im computergestützten System

Infolge von Fehlern im computergestützten Dispositionssystem (technischer Fehler) ist es möglich, dass Dispositionsentscheidungen falsch verarbeitet werden (siehe Nr. 3 des Gefährdungsprotokolls im Anhang A5, Tabelle A.22 bzw. Tabelle 6).

Falsch oder fehlerhaft verarbeitete Dispositionsentscheidungen können bei fehlenden bzw. nicht eintretenden Barrieren in der fehlerhaften Disposition von Fahrzeugen oder von Triebfahrzeugführern resultieren. Diese können zu einer Zugentgleisung, einer Kontamination der Umwelt sowie zu einer Kollision von Fahrzeug und Ladung führen. Der Ereignisbaum des Anhangs A6, Abbildung A.36 veranschaulicht diesen Sachverhalt. bzw. der verkürzt dargestellte Ereignisbaum In Abbildung 14 wird der Sachverhalt verkürzt wiedergegeben.

Dabei sei herausgestellt, dass der reduzierte Ereignisbaum Pfade mit Sicherheitsbarrieren nicht wiedergibt. Am Beispiel der *falschen Disposition von Fahrzeugen* sei dies kurz erläutert. Wie im Anhang A6, Abbildung A.36 dargestellt ist, führt dieser Fehlzustand nicht unweigerlich zu einem extremen Umweltschaden. Sofern z. B. durch diesen Fehlzustand Triebwagen des SPNV fälschlicherweise für den SPFV eingesetzt werden, kann dies entweder dazu führen, dass der Triebwagen nicht über die für die zu befahrende Strecke notwendige Zugbeeinflussungseinrichtung verfügt oder die Kapazität zu gering ist. Im ersten Fall kann die Betriebsleistung nicht erbracht werden, da die Sicherheitsmechanismen der streckenseitigen

TABELLE 5: AUSZUG AUS DEM GEFÄHRDUNGSPROTOKOLL FÜR GEFÄHRDUNGEN BEI FEHLENDEM PERSONAL IM NOTFALLMANAGEMENT UND BEWERTUNG DER SCHUTZMAßNAHMEN

Nr.	1	2
Funktion (Tätigkeit)	Bedarf an Personal erkennen	
Ausfallursache Fehler	Bedarf wird nicht erkannt, Missmanagement	Bedarf wird zu spät erkannt
	organisatorischer Fehler	menschlicher Fehler
Ausfall Fehlzustand	fehlendes Personal im Notfallmanagement	Personal im Notfallmanagement kann nicht rechtzeitig eingestellt werden
Gefährdung	notwendige Maßnahmen bei Störungen werden nicht getroffen	
Unfall	Folgeunfall	
Schadens-ausmaß	katastrophal	
	zahlreiche Tote, extremer Umweltschaden	
Häufigkeit	selten	
	kann durch unvorhergesehene längere Ausfälle, z. B. Schwangerschaft/Mutterschutz, Krankheit, irgendwann einmal eintreten	
Kritikalität	unerwünscht	unerwünscht
Schutzmaßnahme	Anpassung des SMS (Kompetenzmanagement): alle Disponenten werden für Tätigkeiten im Notfallmanagement geschult	
Auswirkung auf	Reduzierung der Häufigkeit	
Schadens-ausmaß	katastrophal	
	zahlreiche Tote	
Häufigkeit	sehr unwahrscheinlich	
	alle Disponenten sind im Notfallmanagement geschult und jeder kann den ausgefallenen Disponenten ersetzen	
Kritikalität	tolerabel	tolerabel

Zugbeeinflussungseinrichtung ein Befahren verhindern. Sofern die Kapazität des Triebwagens zu gering ist, kann dies dazu führen, dass Passagiere im Gang stehen und es dadurch bei Bremsungen zu leichten Verletzungen kommen kann.

Lediglich wenn ein nicht dafür geeigneter Güterwagen für den Transport von Gefahrgut eingeplant wird, kann es unter der Voraussetzung, dass implementierte Sicherheitsbarrieren nicht greifen, zu einer Kontamination der Umwelt durch Gefahrgutaustritt kommen.

Die in Abbildung 14 verkürzt dargestellt resultierenden Unfälle gehen jeweils mit einem katastrophalen Schadensausmaß einher. Dadurch, dass zum aktuellen Zeitpunkt keine Anforderungen an das computergestützte Dispositionssystem definiert sind, wird im Gefährdungsprotokoll eine seltene Häufigkeit gewählt, was zu einer unerwünschten Risikokategorie führt. Im Rahmen des weiteren Ablaufs des Risikomanagements (siehe Abschnitt 7.2.2) soll für diese Gefährdungen ein Referenzsystem zur Risikoevaluierung herangezogen werden.

TABELLE 6: AUSZUG AUS DEM GEFÄHRDUNGSPROTOKOLL FÜR GEFÄHRDUNGEN BEI DISPOSITIONSTÄTIGKEITEN DURCH FEHLER IM COMPUTERGESTÜTZTEN SYSTEM

Nr.	3
Funktion (Tätigkeit)	Dienst- und Umlaufpläne erstellen
Ausfallursache Fehler	Fehler im computergestützten Dispositionssystem
	technischer Fehler
Ausfall Fehlzustand	Disposition wird falsch/fehlerhaft verarbeitet
Gefährdung	diverse
Unfall	Zugentgleisung, Kontamination der Umwelt (Gefahrgutaustritt), Kollision Fahrzeug mit Ladung
Schadens-ausmaß	katastrophal
	zahlreiche Tote, extremer Umweltschaden
Häufigkeit	selten
	Anforderungen an computergestütztes Dispositionssystem nicht definiert
Kritikalität	unerwünscht

5.3.3 Gefährdungen bei Abstellung eines Güterzugs mit Gefahrgut

Insgesamt drei Gefährdungen lassen sich durch den organisatorischen Fehler *fehlende Definition zu Abstellorten bzgl. Sicherung des Gefahrguts* identifizieren (siehe Nr. 4, 9 und 10 des Gefährdungsprotokolls im Anhang 5, Tabelle A.22 bzw. Tabelle 7). Das fiktive EVU transportiert gefährliche Güter, welche ein hohes Gefahrenpotenzial in Bezug auf terroristischen Missbrauch aufweisen.

Der organisatorische Fehler liegt konkret in der Randbedingung begründet, dass in der zugrunde gelegten Ordnung für die internationale Eisenbahnbeförderung gefährlicher Güter (RID – Règlement concernant le transport international ferroviaire de marchandises Dangereuses) in Kapitel 1.10 keine detaillierten Anforderungen betreffend der ordnungsgemäßen Sicherung, guten Beleuchtung und angemessenen Unzugänglichkeit von „Plätze[n] für das zeitweilige Abstellen [und] Fahrzeugdepots“ [RID21] definiert werden. Dies kann dazu führen, dass der Halteplatz nicht geeignet ist. Am falschen Halteplatz sind gefährliche Güter ggf. dem Missbrauch durch Dritte ausgeliefert. Werden gefährliche Güter unsachgemäß behandelt bzw. für terroristische Zwecke eingesetzt, können katastrophale Schäden hervorgehen.

Da es im fiktiven EVU keine Bestimmungen für die Ausgestaltung von (zeitweiligen) Abstellplätzen gibt, wird davon ausgegangen, dass solch ein Ereignis mehrere Male auftreten wird. Es ergibt sich dadurch eine untragbare Risikokategorie. Risikominderungsmaßnahmen sollen im weiteren Risikomanagementverfahren mit Hilfe der Zugrundelegung von Regelwerken identifiziert und das Risiko folglich weiter evaluiert werden.

An diesem Beispiel wird deutlich, welchen praktischen Vorteil die ausführliche Gefährdungsermittlung für den Anwender darstellen kann. Durch detaillierte Überprüfungen der implementierten Prozesse und der daraus oder dabei entstehenden Gefährdungen lassen sich eventuell bestehende Lücken in den Prozessen identifizieren und beseitigen.

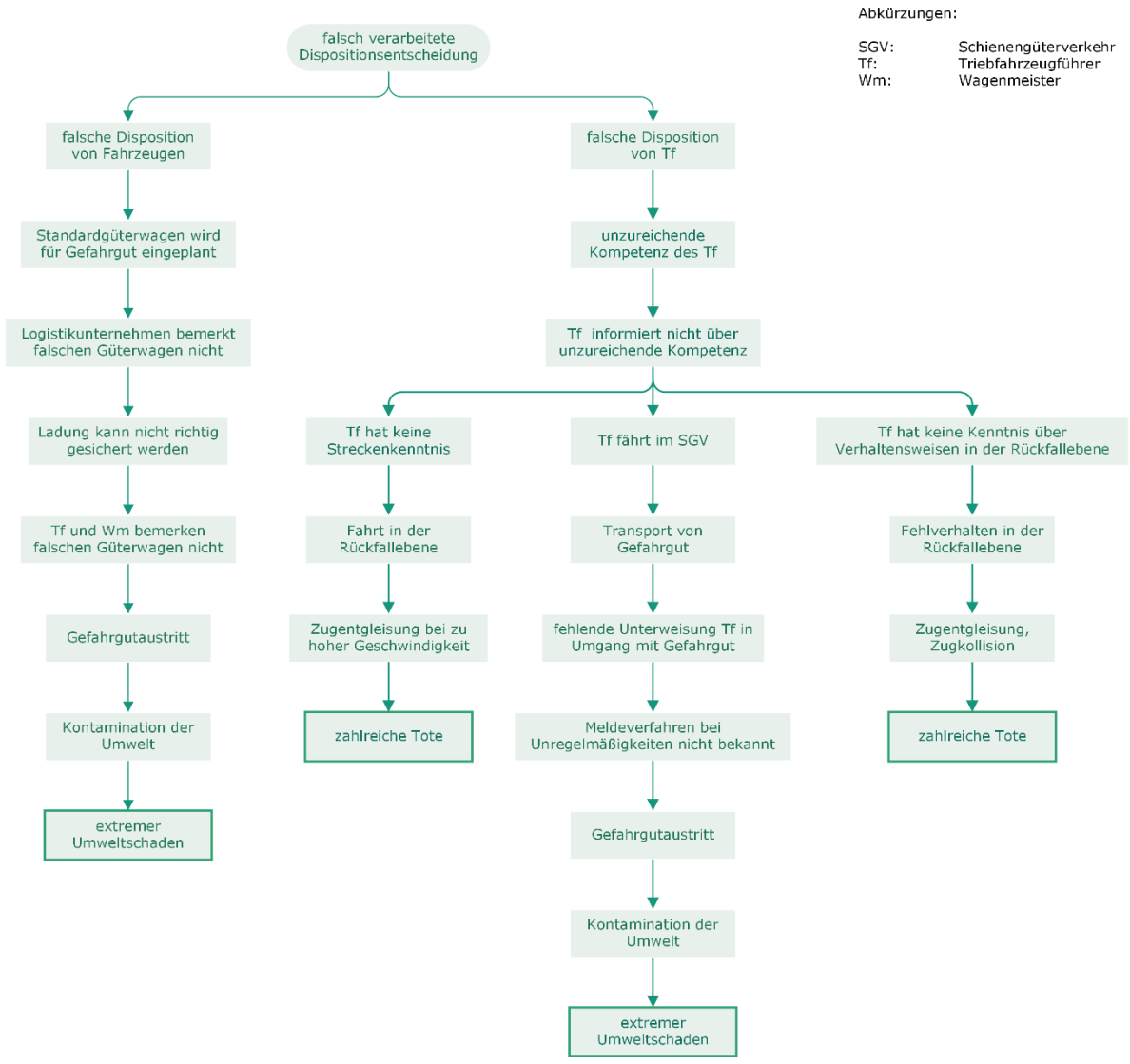


Abbildung 14: Reduzierter Ereignisbaum: falsch/fehlerhaft verarbeitete Dispositionsentscheidung

5.3.4 Gefährdungen bei technischen Fehlern des Zugintegritätssystems

Zwei unerwünschte Risiken gehen aus technischen Fehlern des ZIS hervor. Diese lassen sich im SGV im Unterprozess *Fahrt durchführen* ermitteln (siehe Nr. 6 und 8 des Gefährdungsprotokolls im Anhang 5, Tabelle A.22 bzw. Tabelle 8).

Durch technische Fehler oder Ausfälle besteht die Möglichkeit, dass ein Ladungsverlust oder eine Zugtrennung nicht detektiert wird. Zu derartigen Fehlern gehören beispielsweise:

- der Ausfall einer Komponente (technischer Ausfall),
- ein systematischer Fehler während der Systementwicklung (implementierter Technikfehler),
- fehlerhafte Spezifizierung der Anwendungsbedingungen des ZIS (Fehler im Lastenheft).

TABELLE 7: AUSZUG AUS DEM GEFÄHRDUNGSPROTOKOLL FÜR GEFÄHRDUNGEN BEI ABSTELLUNG EINES GÜTERZUGS MIT GEFAHRGUT

Nr.	4	9	10
Unterprozess	Fahrt vorbereiten	Fahrt durchführen	Fahrzeug abrüsten
Funktion (Tätigkeit)	Halteplatz am Ausfahrgleis einnehmen	Abbremsen und an Zielgleis der Zugfahrt anhalten	Fahrzeug abstellen
Ausfallursache Fehler	fehlende Definition zu Abstellorten bzgl. Sicherung des Gefahrguts		
	organisatorischer Fehler		
Ausfall Fehlzustand	Halteplatz ist nicht ausreichend gesichert, unbeleuchtet und/oder für Öffentlichkeit zugänglich		
Gefährdung	Einwirkung von Dritten		
Unfall	Kontamination der Umwelt (Gefahrgutaustritt) bei unsachgemäßer Verwendung durch Dritte		
Schadensausmaß	katastrophal		
	extremer Umweltschaden		
Häufigkeit	gelegentlich		
	Anforderungen für Plätze für das zeitweilige Abstellen von Fahrzeugen nicht definiert.		
Kritikalität	untragbar	untragbar	untragbar

Lediglich bei einem unbemerkten Ladungsverlust kann es infolge einer Entgleisung des betrachteten oder eines nachfolgenden Zugs zu einem Unfall mit einem katastrophalen Schadensausmaß kommen. Bei einer unbemerkten Zugtrennung greifen die im Zug und in der Eisenbahninfrastruktur implementierten Sicherheitsmechanismen. Der Zug wird bei Abriss der Bremsleitung gestoppt und der betreffende Gleisabschnitt nicht freigemeldet (siehe Nr. 5 und 7 des Gefährdungsprotokolls im Anhang 5, Tabelle A.22 bzw. Tabelle 8).

Aufgrund dessen, dass Sicherheitsanforderungen an das innovative ZIS noch nicht definiert sind, kann angenommen werden, dass diese Gefährdungen ausnahmsweise auftreten können. Wie das hier vorgestellte Beispiel der Einführung eines neuen technischen Systems verdeutlicht, bietet die Gefährdungsidentifikation die Möglichkeit fehlende Sicherheitsanforderungen zu identifizieren.

Im Rahmen des weiterführenden Risikomanagementverfahrens (siehe Abschnitt 6.2.3) werden die Gefährdungen, welche das ZIS hervorruft, mittels der expliziten Risikoabschätzung betrachtet. Das Ergebnis bildet ein harmonisiertes Entwurfsziel für technische Funktionen, welches im Entwicklungsprozess im System implementiert und durch verschiedene Sicherheitsmechanismen gewährleistet wird.

TABELLE 8: AUSZUG AUS DEM GEFÄHRDUNGSPROTOKOLL FÜR GEFÄHRDUNGEN BEI TECHNISCHEM FEHLER DES ZIS

Nr.	5	6	7	8
Unterprozess	Fahrt durchführen			
Funktion (Tätigkeit)	Zugtrennung detektieren		Meldung Zugtrennung an Triebfahrzeugführer	
Ausfallursache Fehler	diverse		diverse	
	technischer Fehler		technischer Fehler	
Ausfall Fehlzustand	Reduktion des Zuggewichts wird nicht detektiert		Reduktion des Zuggewichts wird nicht gemeldet	
Gefährdung	unbemerkte Zugtrennung	unbemerkter Ladungsverlust	unbemerkte Zugtrennung	unbemerkter Ladungsverlust
Unfall	kein Unfall durch Sicherheitsmechanismen (Gleisfreimeldung)	Zugentgleisung durch Ladung auf Strecke	kein Unfall durch Sicherheitsmechanismen (Gleisfreimeldung)	Zugentgleisung durch Ladung auf Strecke
Schadensausmaß	–	katastrophal	–	katastrophal
	–	zahlreiche Tote, extremer Umweltschaden	–	zahlreiche Tote, extremer Umweltschaden
Häufigkeit	–	unwahrscheinlich	–	unwahrscheinlich
	–	kann ausnahmsweise auftreten	–	kann ausnahmsweise auftreten
Kritikalität	keine Gefährdung	unerwünscht	keine Gefährdung	unerwünscht

6 Risikoevaluierung

6.1 Methodisches Vorgehen

Die Risikoevaluierung bildet den eigentlichen Fokus des Risikomanagementverfahrens nach der CSM-Verordnung. Hierzu werden die in [CSM15] definierten Risikoakzeptanzgrundsätze

- Zugrundelegung von Regelwerken,
- Heranziehung eines Referenzsystems und
- Explizite Risikoabschätzung

für alle in den vorherigen Schritten identifizierten Gefährdungen angewandt, die sich nicht der Kategorie *allgemein vertretbare Gefährdungen* zuordnen lassen (siehe Abschnitt 6.2).

Mit der Anwendung der Risikoakzeptanzgrundsätze wird die Zielstellung verfolgt, zusätzliche Sicherheitsmaßnahmen für nicht vertretbare Risiken zu identifizieren und somit eine Systemadaptierung hervorzurufen.

Den gesamthaften schematischen Ablauf des methodischen Vorgehens der Anwendung der definierten Risikoakzeptanzgrundsätze enthält Abbildung 15. Nachfolgend erfolgt eine detaillierte Beschreibung des notwendigen Vorgehens der Risikoevaluierung gemäß CSM-Verordnung.

6.1.1 Zugrundelegung von Regelwerken

Beim Risikoakzeptanzgrundsatz *Zugrundelegung von Regelwerken* ist zu überprüfen, ob sich nicht vertretbare Risiken durch die Einhaltung von Rechtsnormen und Richtlinien (kurz Regelwerke) adäquat kontrollieren lassen. Dabei gelten folgende Anforderungen an Regelwerke gemäß Anhang I Punkt 2.3.2 der CSM-Verordnung [CSM15]:

- im Bahnsektor generell anerkannt,
- für die betrachtete Gefährdung relevant und
- für die Bewertungsstelle zugänglich.

Als Regelwerk versteht die CSM-Verordnung „die schriftlich festgelegten Regeln, anhand deren festgestellt wird, ob das mit einer oder mehreren spezifischen Gefährdungen verbundene Risiko vertretbar ist.“ [CSM15]

Für die Nutzung dieses Risikoakzeptanzgrundsatzes wird zunächst ein für die konkret betrachtete Gefährdung relevantes, anerkanntes und zugängliches Regelwerk recherchiert. Dazu gehören europäische Normen, Verordnungen und Technische Spezifikationen für die Interoperabilität sowie nationale Gesetze, Sicherheitsvorschriften, Normen und Leitfäden.

Bei erfolgreichen Rechercheergebnissen wird anschließend überprüft, ob die zugehörigen Regelwerksvorgaben für die konkret zu bewertende Gefährdung zutreffend sind oder sich in Prozessen implementieren lassen. Werden diese Vorgaben eingehalten, kann das ursprünglich als nicht vertretbar eingeschätzte Risiko fortan als allgemein vertretbar eingestuft werden. Diese Bewertungsänderung ist im Gefährdungsprotokoll entsprechend zu hinterlegen. Abbildung 16 stellt den Ablauf der Anwendung dieses Risikoakzeptanzgrundsatzes komprimiert dar.

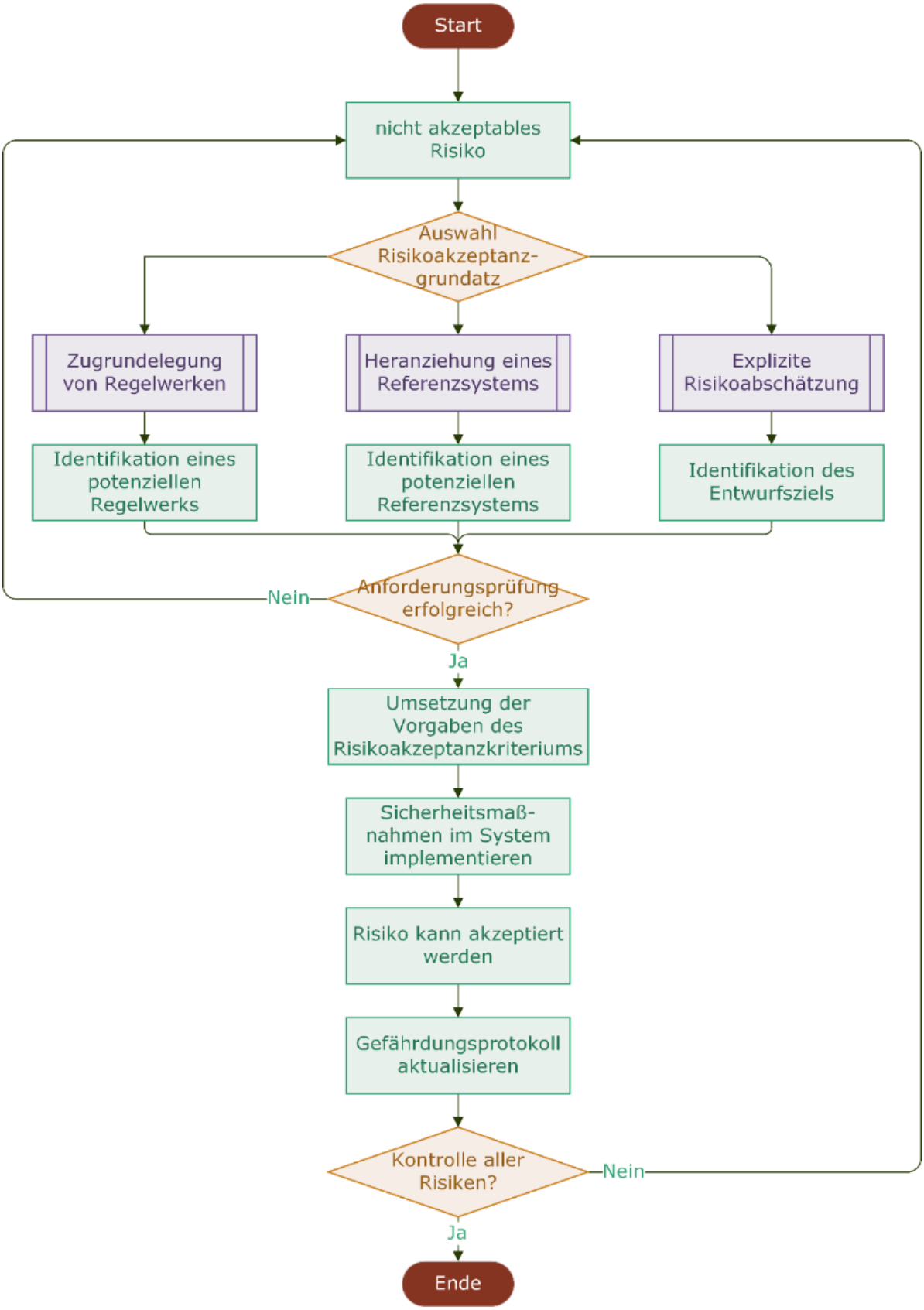


Abbildung 15: Ablauf der Anwendung der Risikoakzeptanzgrundsätze (vereinfachte Darstellung) nach [CSM15]

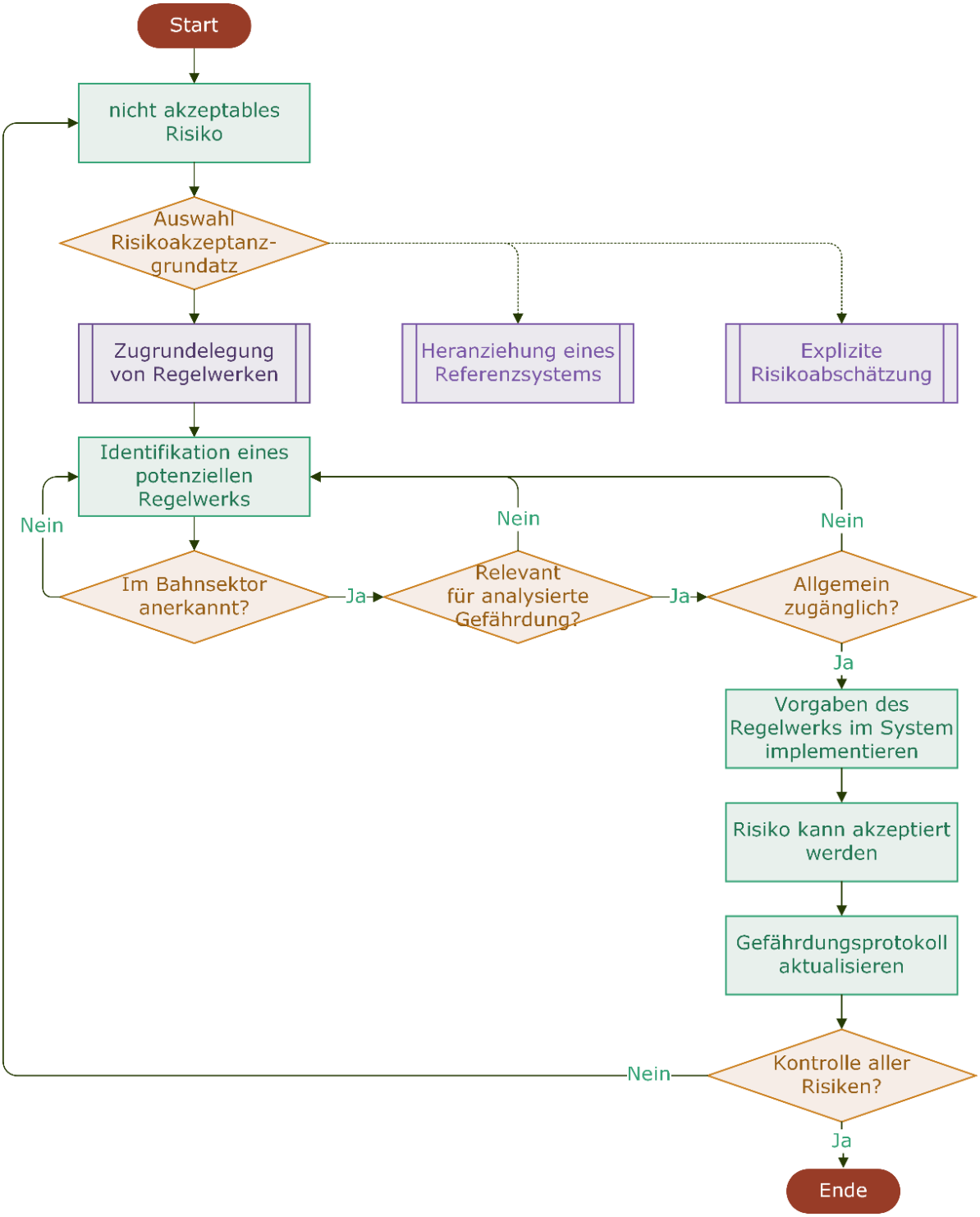


Abbildung 16: Ablauf *Zugrundelegung von Regelwerken* und Risikoevaluierung nach [CSM15]

Sofern das herangezogene Regelwerk die Gefährdung nicht vollumfänglich beherrscht, sind zusätzliche Sicherheitsmaßnahmen zu treffen. Zum einen kann mittels Nachweises mindestens gleicher Sicherheit dokumentiert werden, dass der verfolgte Ansatz, welcher im betrachteten Regelwerk nicht lückenlos abgedeckt wird, ein identisches oder höheres Sicherheitsniveau bewirkt. Zum anderen kann die weiterführende Anwendung anderer Risikoakzeptanzgrundsätze zur Risikoreduktion notwendig sein.

6.1.2 Heranziehung eines Referenzsystems

Eine weitere Möglichkeit des Umgangs mit nicht vertretbaren Risiken stellt ein Vergleich mit einem Referenzsystem dar. Die dahinterstehenden methodischen Grundsätze gehen davon aus, dass gleichwertige Gefährdungen akzeptiert werden können, sofern dies bereits in anderen bewährten Systemen der Fall ist. Dazu muss das Vergleichssystem ebenfalls bestimmte Anforderungen gemäß Anhang I Punkt 2.4.2 [CSM15] erfüllen. Ein solches Referenzsystem muss

- betriebsbewährt sein,
- ein akzeptables Sicherheitsniveau aufweisen (und dieses in einem Genehmigungsprozess nachweisen/nachgewiesen haben),
- über ähnliche Funktionen und Schnittstellen verfügen sowie
- unter ähnlichen Betriebs- und Umgebungsbedingungen arbeiten.

Es ist somit notwendig, das eigene und das zu vergleichende System bezüglich der genannten Vorgaben zu untersuchen. Über einen Vergleich der identifizierten Anforderungen und Schnittstellen sowie System- und Umgebungsbedingungen kann anschließend eine fundierte Entscheidung zur Eignung des Referenzsystems für das zu bewertende (bisher nicht vertretbare) Risiko getroffen werden. Wichtig ist dabei, dass die Vorgaben nicht identisch im Referenzsystem umgesetzt sein müssen, sondern lediglich ähnliche Rahmenbedingungen zu identifizieren sind.

Als potenzielle Referenzsysteme bieten sich für ein neu in den deutschen Schienenverkehr eintretendes EVU andere, bereits in Deutschland verkehrende EVU mit deren Systembestandteilen an. Im nächsten Schritt ist zu überprüfen, ob die betrachtete Gefährdung im Referenzsystem abgedeckt und beherrscht wird. Nur wenn diese Voraussetzung erfüllt ist, lässt sich durch Übernahme der im Referenzsystem implementierten Sicherheitsanforderungen das betrachtete Risiko fortan als allgemein vertretbar einstufen. Im Gefährdungsprotokoll sind die Sicherheitsmaßnahmen zu dokumentieren. Abbildung 17 stellt den Ablauf der Anwendung dieses Risikoakzeptanzgrundsatzes komprimiert dar. Sofern die Gefährdung nicht vollumfänglich im herangezogenen Referenzsystem abgedeckt wird, sind geeignete Maßnahmen zu treffen. Dies kann die weiterführende Anwendung anderer Risikoakzeptanzgrundsätze sein.

6.1.3 Explizite Risikoabschätzung

Die explizite Risikoabschätzung kann quantitativ oder qualitativ für Risiken, welche weder „durch Zugrundelegung von Regelwerken oder Referenzsystemen bereits als vertretbar angesehen werden“ [CSM15], erfolgen. Eine Möglichkeit der expliziten Risikoabschätzung ist die Anwendung der harmonisierten Entwurfsziele.

Die CSM-Verordnung wurde hierzu im Jahr 2015 für elektrische, elektronische und programmierbare elektronische technische Eisenbahnsysteme präzisiert. Dabei werden harmonisierte Entwurfsziele (DT – Design Targets) hinsichtlich des Schadensausmaßes, welcher bei Ausfall der technischen Systemfunktionen zu erwarten ist, unterschieden. So muss das Risiko eines zu einem katastrophalen Unfall führenden technischen Systemausfalls „nicht weiter reduziert werden, wenn es nachweislich höchst unwahrscheinlich ist, dass es zu einem Ausfall kommt“ [CSM15]. Bei Funktionsausfällen mit „einem kritischen Unfall [...] muss das damit verbundene Risiko nicht weiter reduziert werden, wenn es nachweislich unwahrscheinlich ist, dass es zu einem Ausfall kommt“ [CSM15].

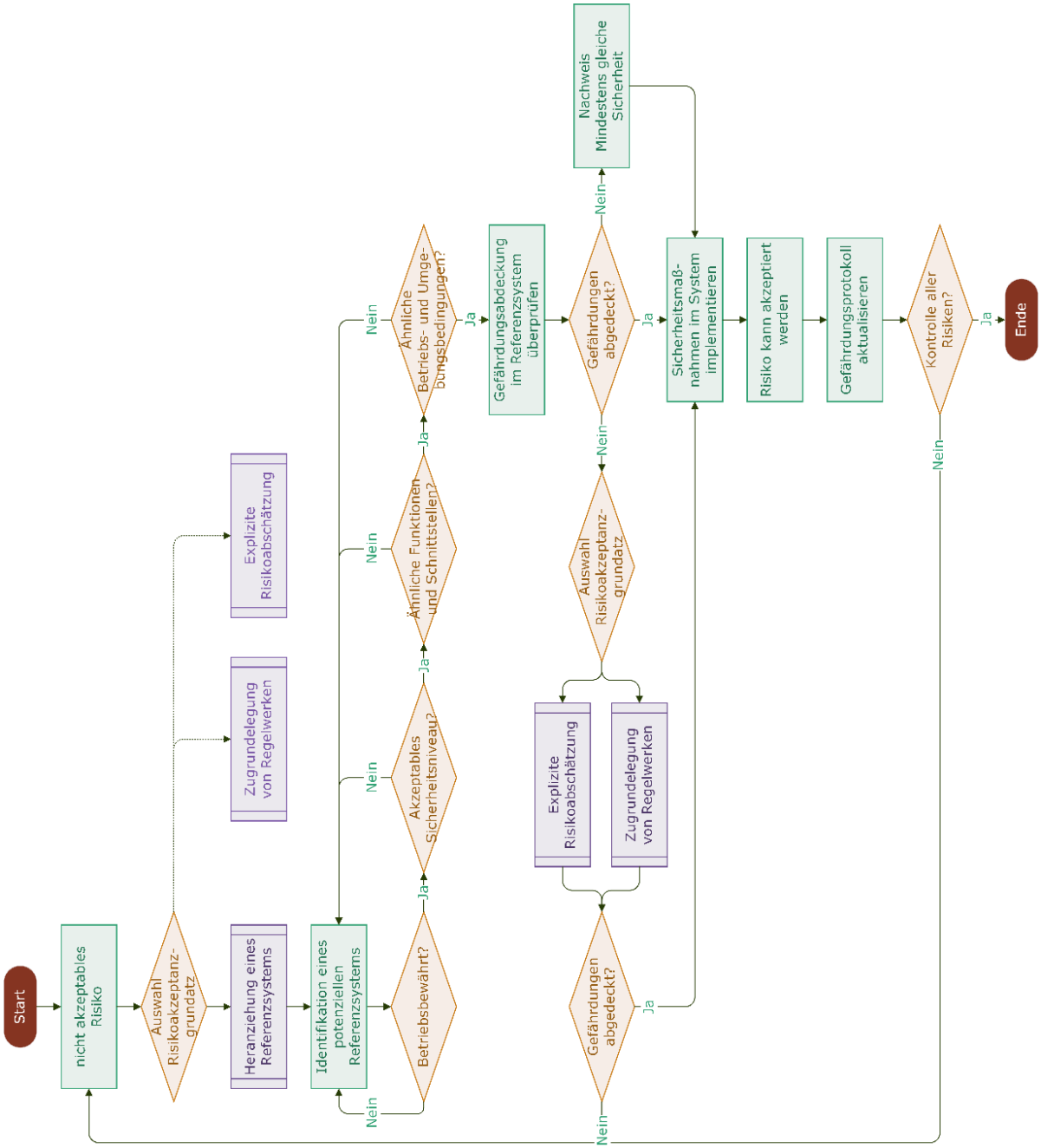


Abbildung 17: Ablauf *Heranziehung eines Referenzsystems* und Risikoevaluierung nach [CSM15]

Ebenfalls definiert [CSM15] die Begriffe höchst unwahrscheinlich und unwahrscheinlich:

- höchst unwahrscheinlich: „das Auftreten eines Ausfalls mit einer Ausfallrate von höchstens 10^{-9} je Betriebsstunde“ [CSM15] und
- unwahrscheinlich: „das Auftreten eines Ausfalls mit einer Ausfallrate von höchstens 10^{-7} je Betriebsstunde“[CSM15].

Somit lassen sich bei Anwendung der expliziten Risikoabschätzung direkt technische Sicherheitsanforderungen an „elektrische, elektronische und programmierbare elektronische technische“ [CSM15] Eisen-

bahnsysteme stellen. Diese müssen im Entwicklungsprozess ebendieser Systeme erfolgreich implementiert und nachgewiesen werden. Für mechanische Systeme ist die Anwendung der harmonisierten Entwurfsziele nicht qualifiziert.

Selbstverständlich können zusätzliche, nicht im System implementierte Barrieren das Risiko senken. In diesem Fall wird das Entwurfsziel der Systemfunktion entsprechend der Auswirkungen der Sicherheitsbarrieren reduziert. Diese Sicherheitsbarrieren lassen sich in technische, betriebliche und organisatorische Maßnahmen unterscheiden (vgl. [HOL15]). Mithilfe einer Ereignisbaumanalyse (siehe Abschnitt 6.1.2) kann

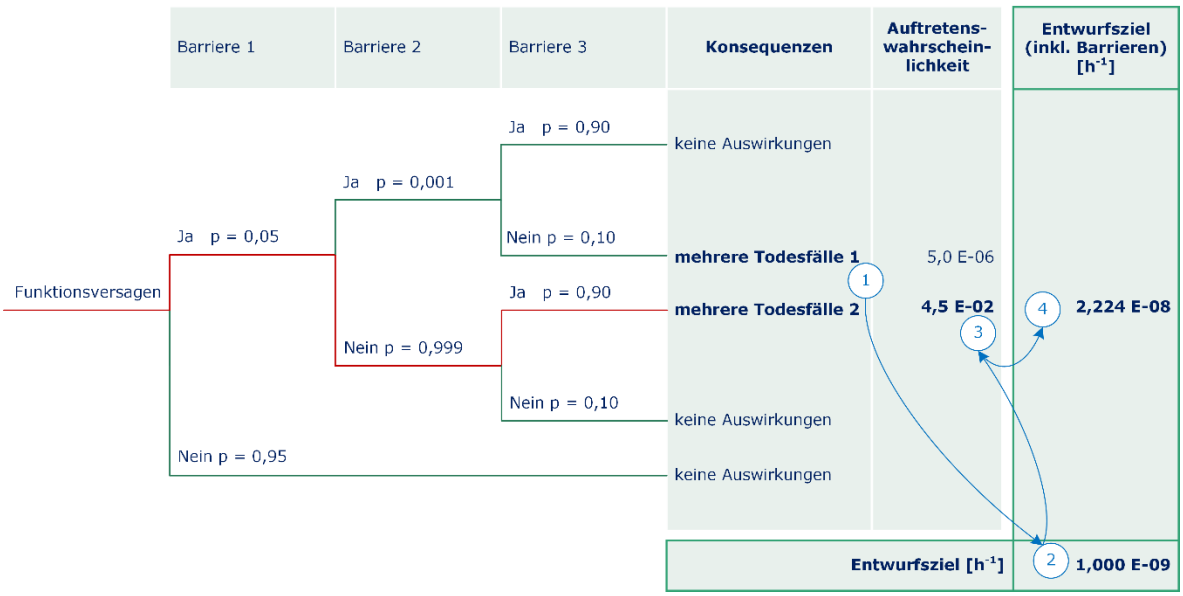


Abbildung 18: Ermittlung des Entwurfsziels bei implementierten Barrieren nach [ERA17]

der Sicherheitsbeitrag der Barrieren bestimmt und die notwendige Ausfallrate des technischen Systems ermittelt werden. Abbildung 18 zeigt einen beispielhaften Ereignisbaum zur Ermittlung der Auswirkungen von Sicherheitsbarrieren. Die Berechnungsgrundlage stellt der Leitfaden der ERA (European Union Agency for Railways) zur Anwendung der harmonisierten Entwurfsziele [ERA17] dar.

Das Entwurfsziel unter der Berücksichtigung von Sicherheitsbarrieren kann beispielhaft in vier Schritten ermittelt werden.

Die Ausgangssituation der Betrachtungen ist ein Funktionsversagen des elektrischen, elektronischen oder programmierbaren elektronischen technischen Eisenbahnsystems und dabei wirkende Sicherheitsbarrieren (in Abbildung 18 drei Barrieren).

- Schritt 1
  Die Sicherheitsbarrieren werden im Ereignisbaum dargestellt und mit zugehörigen Eintrittswahrscheinlichkeiten hinterlegt. Im vorliegenden Beispiel können sich in zwei Fällen Unfälle mit mehreren Toten ereignen.

- Schritt 2
  Entsprechend des katastrophalen Schadensausmaßes bei einem Unfall ist ein höchst unwahrscheinliches Entwurfsziel ($1 \cdot 10^{-9}\ h^{-1}$) zu definieren.

- Schritt 3
  Der nächste Schritt besteht darin, den kritischen Pfad im Ereignisbaum auszuwählen. Dieser weist die höchste Auftretenswahrscheinlichkeit auf. Im Beispiel aus Abbildung 18 betrifft dies den unteren Pfad (rot hinterlegt), da seine Auftretenswahrscheinlichkeit $4{,}5\ \%$ und die des oberen Pfads lediglich $0{,}0005\ \%$ beträgt.

- Schritt 4
  Das Entwurfsziel für die betrachtete Funktion $DT(Funktion)$ ergibt sich durch die Berechnungsvorschrift gemäß Formel 3.

$$DT\ (Funktion) = \frac{DT(Ausgangslage)}{P(kritischer\ Pfad)} \qquad (3)$$

Das Risiko kann nach Anhang Punkt 2.5.7 der CSM-Verordnung [CSM15] als allgemein vertretbar angesehen werden, wenn folgende Nachweise erbracht werden:

- Nachweis der Erfüllung der harmonisierten Entwurfsziele,
- Nachweis der Beherrschung von systematischen Fehlern und
- Nachweis der sicheren Integration des technischen Systems in das betrachtete Eisenbahnsystem.

Die Voraussetzungen der erfolgreichen Nachweisführung gelten u. a. dann als erfüllt, wenn ein DIN EN 5012x-konformer Entwicklungsprozess erfolgreich durchlaufen wird.

Abbildung 19 visualisiert den beschriebenen Prozess der expliziten Risikoabschätzung. Dabei werden auch sicherheitsbezogene Anwendungsbedingungen (SRAC – Safety Related Application Conditions) betrachtet.

6.2 Risikoevaluierung im fiktiven EVU

6.2.1 Zugrundelegung von Regelwerken und Risikoevaluierung

Aus den bisherigen Betrachtungen in Abschnitt 6.2 ergeben sich drei nicht vertretbare Risiken, für welche die Zugrundelegung von Regelwerken vorgesehen ist. Dies betrifft die Prozesse, aus denen die Gefährdung eines extremen Umweltschadens infolge des Fehlers *fehlende Definition zu Abstellorten bzgl. der Sicherung des Gefahrguts* resultiert. Diese Fehler sind im Gefährdungsprotokoll (siehe Anhang A5, Tabelle A.22 und Tabelle 7) dokumentiert und unter den Nummern 5, 10 und 11 zu finden.

Maßgebliche Vorgaben für den Gefahrguttransport enthält [RID21]. Allerdings wurde bereits in Abschnitt 5.3.3festgestellt, dass keine detaillierten Anforderungen hinsichtlich der ordnungsgemäßen Sicherung, guten Beleuchtung und angemessenen Unzugänglichkeit von Abstellorten definiert werden. Der Leitfaden Umsetzung der gesetzlichen Sicherungsbestimmungen für die Beförderung gefährlicher Güter (Kapitel 1.10 ADR/RID/ADN 2017) [VCI17] des Verbands der Chemischen Industrie e. V. (VCI) stellt eine umfassende Detaillierung der in [RID21] definierten Vorgaben dar. Das genannte Regelwerk ist entsprechend des in Abbildung 16 dargestellten Ablaufs auf Eignung für die Risikobewertung zu überprüfen und für die Risikokontrolle anzuwenden.

Dafür muss zunächst herausgefunden werden, ob der Leitfaden den Anforderungen gemäß [CSM15] genügt. Es bleibt festzuhalten, dass der Leitfaden erweiterte Vorgaben für den Umgang mit gefährlichen Gütern beim (Eisenbahn-)Transport in Bezug auf Maßnahmen zur Sicherung im Sinne von Security ent-

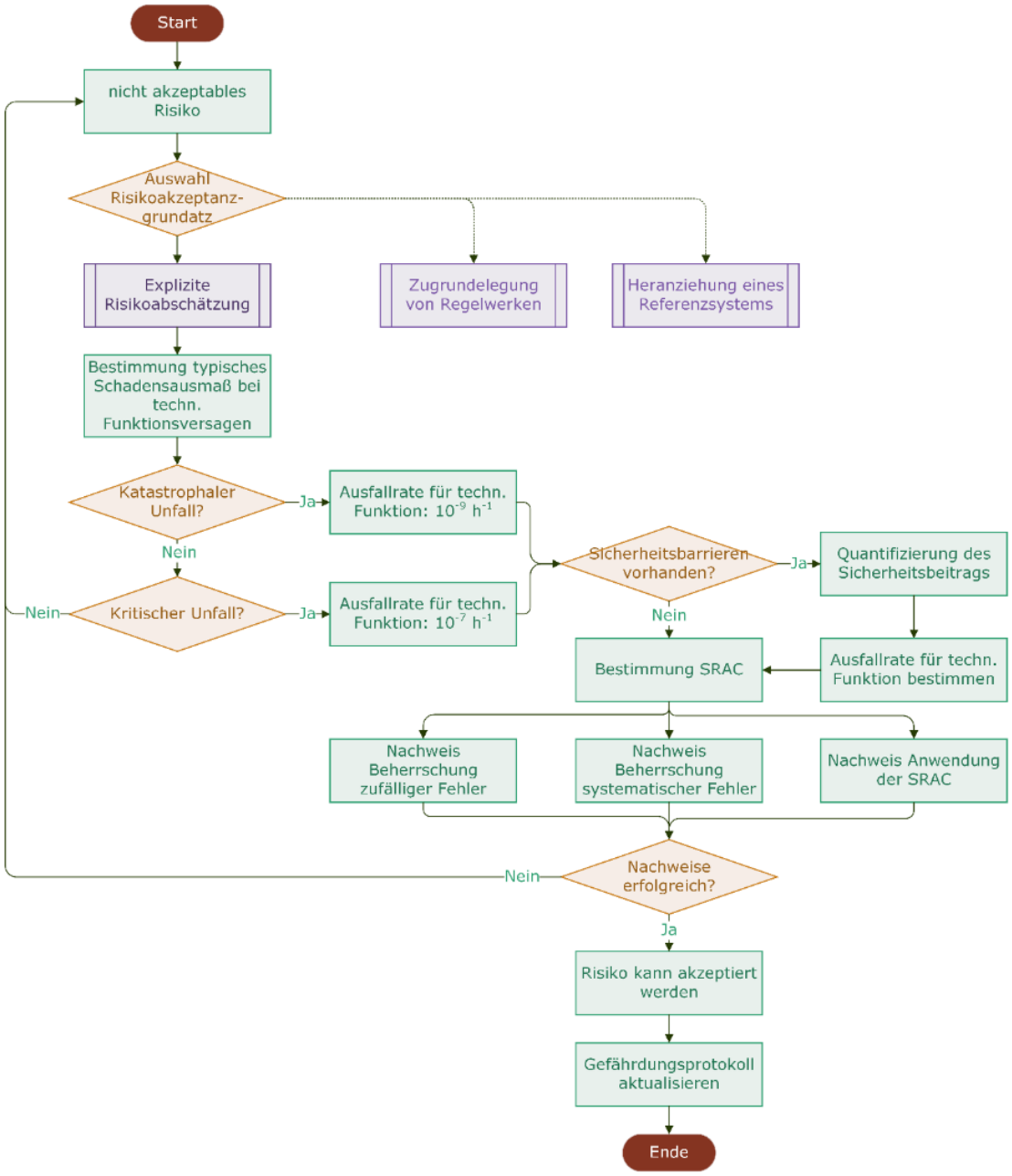


Abbildung 19: Ablauf Explizite Risikoabschätzung und -evaluierung nach [CSM15]

hält. Für den Eisenbahnverkehr relevante Verbände, wie der Verband Deutscher Verkehrsunternehmen e. V. (VDV) und der Bundesverband Güterkraftverkehr Logistik und Entsorgung e. V. (BGL) haben den Leitfaden als Umsetzungsempfehlung erarbeitet. Dieser ist auf der Internetpräsenz des VCI abrufbar.

Demzufolge kann der Leitfaden als

- im Eisenbahnsektor allgemein anerkannt,
- öffentlich zugänglich und
- für die Beherrschung der betreffenden Gefährdungen relevant

angesehen werden.

Die identifizierten und im ersten Abschnitt reflektierten Gefährdungen entstehen durch im fiktiven EVU fehlende Vorgaben für Abstellorte beim Transport von Gefahrgut. Folglich müssen Gegenmaßnahmen bei ebendiesen Vorgaben ansetzen. Tabelle 9 gibt auszugsweise Anforderungen des zugrunde gelegten Leitfadens [VCI17] und deren Umsetzungsweise im fiktiven EVU wieder.

TABELLE 9: VORGABEN DES ZUGRUNDE GELEGTEN LEITFADENS (AUSZUG)

Vorgabe aus [VCI17]	**Umsetzung im fiktiven EVU**
„Unter ‚Bereichen für das zeitweilige Abstellen während der Beförderung' sind solche zu verstehen, auf denen es regelmäßig und beabsichtigt zu einer Unterbrechung im Verlauf der Beförderung kommt (z. B. wegen des Wechsels der Beförderungsart). Unterbrechung in diesem Sinne sind nicht das Halten oder Parken z. B. an einer Raststätte oder die Zugbildung in einem Rangierbahnhof."	Halteplätze am Ausfahrgleis des GVZ, Zielgleise am GVZ und Abstellplätze müssen den nachfolgenden Anforderungen genügen. Für die Umsetzung, Kontrolle und Aufrechterhaltung ist der Gefahrgutbeauftragte des fiktiven EVU zuständig.
„‚Ordnungsgemäß gesichert' sind diese Bereiche, wenn durch angemessene technische oder organisatorische Maßnahmen der Zugang geregelt ist (z. B. bestehen eindeutige Zugangsregelungen, mit denen der Zugang/der Aufenthalt von Unbefugten untersagt wird)."	Für die genannten Orte muss eine eindeutige Zugangsregelung ausgewiesen sein. Der Aufenthalt von Unbefugten ist untersagt.
„Als ‚gut beleuchtet' gelten diese Bereiche insbesondere dann, wenn bereits die Verpflichtung zur Beleuchtung aufgrund von arbeitsschutzrechtlichen Vorgaben erfüllt wird. Unbenommen bleibt der Einsatz gleichwertiger technischer Überwachungssysteme (z. B. Infrarot - Überwachung)."	Die genannten Orte müssen beleuchtet sein. Davon kann abgewichen werden, wenn ein technisches Überwachungssystem eingesetzt wird.
„‚Soweit möglich und angemessen, für die Öffentlichkeit unzugänglich' bedeutet, dass ein solcher Zugang vor allem durch organisatorische Maßnahmen verhindert wird (z. B. Zugangsregelungen für Personen und Fahrzeuge – auch über die Schiene -, keine öffentlichen Zugangswege). Bauliche Maßnahmen (z. B. Zaun) und Bestreifung sind nicht grundsätzlich erforderlich, wenn aufgrund anderer Maßnahmen unberechtigte Dritte eindeutig erkennbar und ausgrenzbar sind."	Für die genannten Orte muss eine eindeutige Zugangsregelung ausgewiesen sein. Der Aufenthalt von Unbefugten ist untersagt.

Vorgabe aus [VCI17]	**Umsetzung im fiktiven EVU**
„Für den Schienenverkehr sollte im Einzelnen bei der Nutzung von Bereichen für das zeitweilige Abstellen berücksichtigt werden: - Abstand zu besonderen Gefahrenpunkten und schutzbedürftigen Objekten - gut beleuchtet und frei von Aufwuchs - im Sichtbereich örtlich besetzter Stellen - Gefahr der Einwirkung durch Dritte aufgrund der örtlichen Gegebenheiten möglichst gering“	Die genannten Orte müssen so ausgestaltet sein, dass - ein Abstand zu Gefahrpunkten und schutzbedürftigen Objekten gewährleistet ist, - sie beleuchtet oder technisch überwacht sind, - sie frei von Bewuchs sind, - sie beaufsichtigt oder technisch überwacht sind, - eine Einwirkung durch Dritte eliminiert werden kann.
„In örtlichen Regeln ist festzulegen - in welchen Gleisen Gefahrgutzüge- oder -wagen abgestellt werden können, - wer das Vorhandensein von Gefahrgutwagen feststellt und wem meldet, - welche Stelle für das Einleiten der Überwachungsmaßnahmen verantwortlich ist und wer ggf. wie zu verständigen ist, - wie die Überwachung nachgewiesen werden soll, - wer bei unbefugten Eingriffen oder Verdacht auf solche Eingriffe zu verständigen ist.“	Für die genannten Orte werden örtliche Regeln aufgestellt, sofern sie im Verantwortungsbereich des fiktiven EVU liegen. Für Orte, die nicht im Verantwortungsbereich des fiktiven EVU liegen, ist das jeweilige Eisenbahninfrastrukturunternehmen (EIU) zuständig. Diese örtlichen Regeln müssen vom fiktiven EVU überprüft werden. Es gelten folgende Anforderungen: - Definition von Gleisen, in denen Güterwagen mit Gefahrgut abgestellt werden dürfen, - Definition einer Meldekette, - Definition der zuständigen Stelle der Überwachungsmaßnahmen, - Definition des Nachweises der Überwachung.

Vorgabe aus [VCI17]	Umsetzung im fiktiven EVU
„Folgende Überwachungsmaßnahmen kommen insbesondere in Betracht: Beaufsichtigung Örtlich besetzte Stellen beaufsichtigen Gefahrgutwagen im Sichtbereich. Dabei ist insbesondere auf Eingriffe Betriebsfremder sowie auf andere Unregelmäßigkeiten zu achten. Alternativ ist eine technische Überwachung, z. B. durch Kamera oder Bewegungsmelder, zulässig. Besichtigung Ist eine Beaufsichtigung nicht möglich, sind regelmäßige Besichtigungen durchzuführen. Bei der Besichtigung muss insbesondere geprüft werden: - Sind die Türen und Luken geschlossen? - Tritt Ladegut aus? - Liegen Hinweise auf Eingriffe Unbefugter sowie auf andere Unregelmäßigkeiten vor?“	Die genannten Orte werden durch örtlich besetzte Stellen oder technische Überwachungseinrichtungen beaufsichtigt. Ist eine manuelle oder technische Beaufsichtigung nicht realisierbar, sind regelmäßige Besichtigungen durchzuführen.

Die in der Umsetzung beschriebenen Anforderungen, Realisierungen und Überprüfungen verringern als Schutzmaßnahme die Häufigkeit des Gefahrenfalls für die genannten Fehler. Dies ist im überarbeiteten Gefährdungsprotokoll (siehe Anhang A7, Tabelle A.23) zu dokumentieren. Damit ergibt sich ein allgemein vertretbares Risiko. Abbildung 20 stellt den beispielhaften Ablauf der Anwendung dieses Risikoakzeptanzgrundsatzes dar.

Für das hier beschriebene Beispiel sei festgehalten, dass der Leitfaden [VCI17] bei real existierenden EVU nicht unbedingt deren Gefährdungen vollumfänglich auf ein vertretbares Maß eindämmt. In diesem Fall sind weitere Sicherheitsmaßnahmen festzulegen bzw. andere Risikoakzeptanzgrundsätze anzuwenden (vgl. [CSM15] Anhang I Punkt 2.3.7 f.).

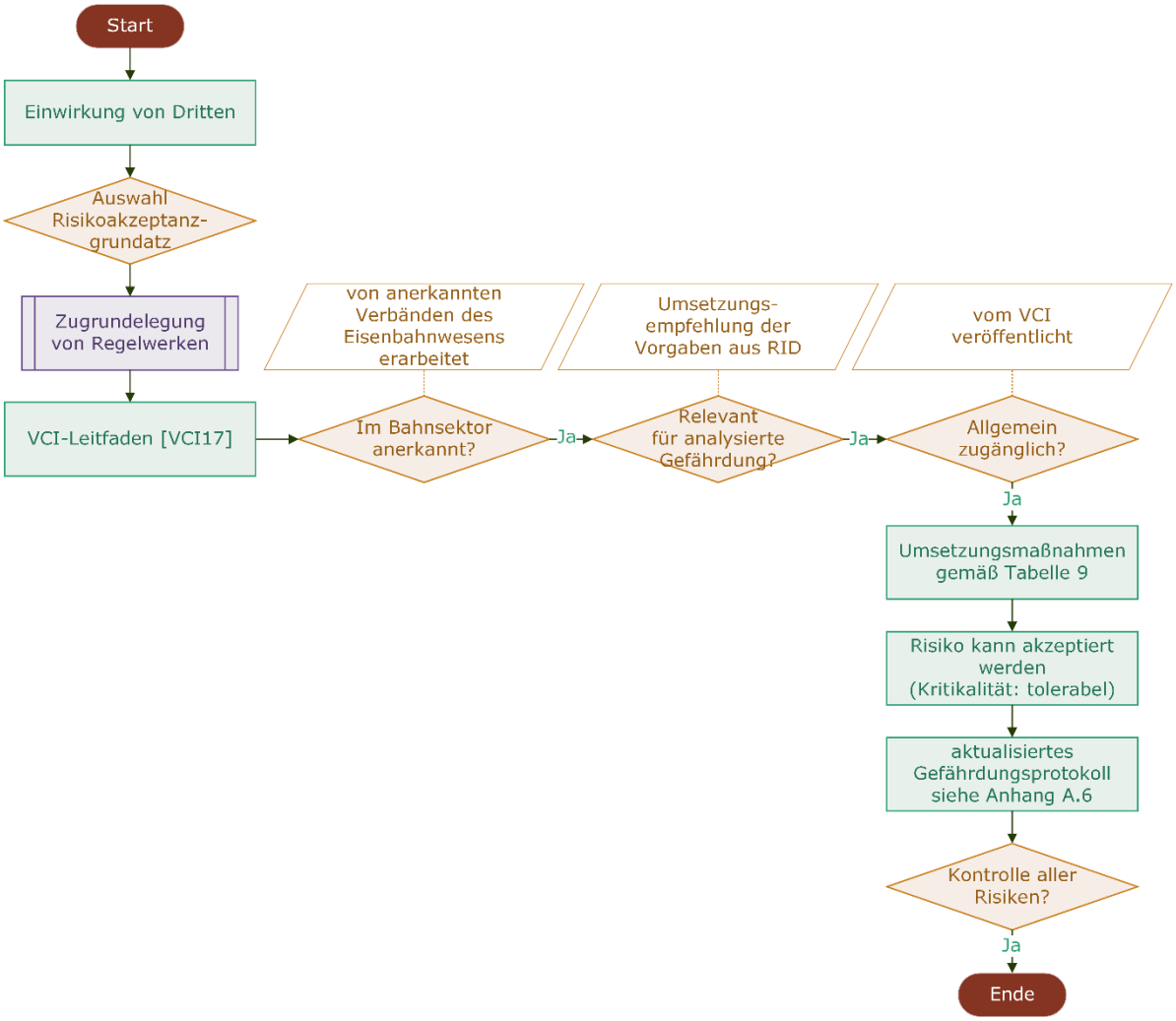


Abbildung 20: Ablauf der Anwendung der Zugrundelegung von Regelwerken und Risikoevaluierung im fiktiven EVU

6.2.2 Heranziehung eines Referenzsystems und Risikoevaluierung

Für die beispielhafte Heranziehung eines Referenzsystems und dessen Risikoevaluierung ist ein nicht vertretbares Risiko (siehe Abschnitt 6.2.2 bzw. Anhang 5, Tabelle A.22 Nr. 3) vorgesehen. Dieses resultiert aus einem technischen Fehler im computergestützten Dispositionssystem. Die Ursache für den benannten Gefährdungsfall, der zu diversen katastrophalen Schadensausmaßen führen kann, liegt in fehlenden Anforderungen an ebendieses System begründet.

Als Referenzsystem eignet sich zur Bewertung dieses Risikos ein von anderen EVU eingesetztes Dispositionssystem. Hierfür wird das bereits bei einem weiteren, imaginären EVU anerkannte und eingesetzte computergestützte Dispositionssystem herangezogen.

Das im Rahmen der Nachweisführung für diesen Forschungsbericht referenzierte computergestützte Dispositionssystem kommt seit fünf Jahren bei diesem, zum Vergleich herangezogenen, imaginären EVU zum Einsatz. Dieses EVU betreibt SPV und SGV im Netz der deutschen Eisenbahnen des Bundes (EdB).

Zur Entscheidungsfindung, ob das referenzierte System über ähnliche

- Funktionen,
- Schnittstellen,
- Betriebsbedingungen und
- Umgebungsbedingungen

verfügt, müssen diese im zu bewertenden System zunächst identifiziert werden.

Notwendige Funktionen und Schnittstellen sind durch die in Kapitel 5 bzw. Anhängen 3 und 4 durchgeführte Systemdefinition vorgegeben. Darüber hinaus lassen sich Vorgaben des computergestützten Dispositionssystems im hier betrachteten fiktiven EVU aus Ergebnissen verschiedener Dissertationen (vgl. [JAC03], [KUC11], [NEU17], [WUR04]) extrahieren. Für real existierende EVU müssen die Vorgaben entsprechend der tatsächlich für die Praxisanwendung erforderlichen Funktionalitäten erweitert und angepasst werden. Tabelle 10 gibt die Vorgaben des fiktiven EVU sowie den Vergleich der Umsetzung im Referenzsystem des imaginären EVU wieder.

Tabelle 10 veranschaulicht, dass auch Abweichungen zwischen dem betrachteten System und dem Referenzsystem möglich sind. Mit dieser Diskrepanz gilt es sich genauer zu befassen. Gemäß Anhang I Punkt 2.4.4 der CSM-Verordnung [CSM15] muss bei Abweichungen der Grundsatz „Mindestens gleiche Sicherheit“ nachgewiesen werden. Im hier vorliegenden Beispielfall weist das Referenzsystem eine geringere Verfügbarkeit auf, als es im betrachteten System des fiktiven EVU definiert ist.

Der Nachweis mindestens gleicher Sicherheit lässt sich im vorliegenden Fall gemäß Vorgaben der Eisenbahn-Bau- und Betriebsordnung (EBO) §2 (2) [EBO19] durch eine Auswirkungsanalyse der Abweichung erbringen. Somit muss identifiziert werden, welche Wirkung eine größere Verfügbarkeit auf das Gesamtsystem hat. Ein System mit einer höheren Verfügbarkeit arbeitet vermehrt im funktionstüchtigen Zustand. Dementsprechend reduziert sich der Anteil der fehleranfälligeren Rückfallebene, in welcher manuelle Bedienhandlungen umzusetzen sind. Das betrachtete System verfügt damit für den Parameter Verfügbarkeit über bessere, d. h. sicherere Eigenschaften als das Referenzsystem. Damit ist der erforderliche Nachweis mindestens gleicher Sicherheit erbracht und das Verfahren beendet.

Das im fiktiven EVU zur Anwendung vorgesehene computergestützte Dispositionssystem kann unter Einhaltung der in Tabelle 10 definierten Vorgaben als angemessen sicher gelten, da die Risiken im imaginären EVU (Referenz-EVU) bereits als vertretbar angesehen sind. Abbildung 21 zeigt den beispielhaften Ablauf der Anwendung dieses Risikoakzeptanzgrundsatzes.

TABELLE 10: VORGABEN ZUM COMPUTERGESTÜTZTEN DISPOSTIONSSYSTEM

Vorgaben	**Vorgaben des computergestützten Dispositionssystems im fiktiven EVU (betrachtetes EVU)**	**Umsetzung im computergestützten Dispositionssystem des imaginären EVU (Referenz-EVU)**
Funktionen	Echtzeitverarbeitung und Realisierung der Dispositionsentscheidungen	Ja
	Wiedergabe Trassenbestellung	Ja
	Echtzeitwiedergabe und Verfolgung des Betriebsgeschehens des SGV und SPV	Ja
	Analyse des Betriebsgeschehens	Ja
	Konflikterkennung und Auswirkungsprognose	Ja
	Ermittlung und Eingabe Personal- und Fahrzeugeinsatz	Ja
	Umlaufplanerstellung und -bearbeitung	Ja
	Kapazitätsbedarfsanalyse	Ja
Schnittstellen	Übergabe von Störeinflüssen im befahrenen Netz	Ja
	Übergabe der Trassenbestellung an Netzbetreiber und deren Ergebnisse vice versa (Kurz- und Langfristplanung)	Ja
	Übergabe von übergeordneten Dispositionsentscheidungen des EIU (Priorisierungsentscheidungen im Netz)	Ja
	Übergabe der Dispositionsentscheidungen	Ja
Betriebsbedingungen	definierte Systemreaktionszeit	Ja
	definierte Exaktheit der Zugortung (räumlich und zeitlich)	Ja
	definierte Verfügbarkeit	Ja, aber geringere Verfügbarkeit
	Updatefähigkeit	Ja
	grafische und tabellarische Darstellungen	Ja
Umgebungsbedingungen	Implementierung der Software in definierte Rechner	Ja
	definierte Einspielmöglichkeit von Updates	Ja
	definierte Supportdienstleistungen (Incident Management)	Ja

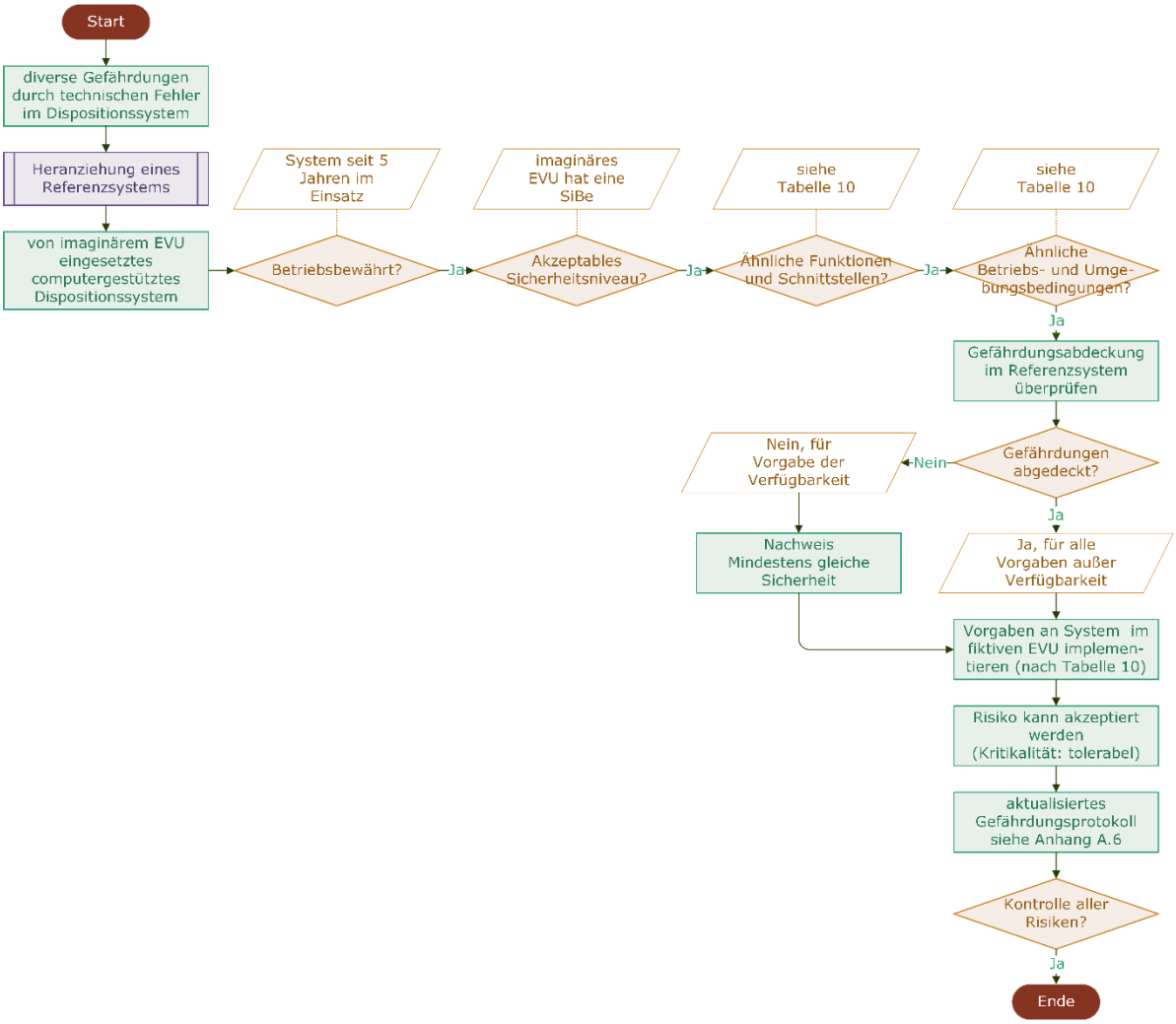


Abbildung 21: Ablauf der Anwendung der Heranziehung eines Referenzsystems und Risikoevaluierung im fiktiven EVU

6.2.3 Explizite Risikoabschätzung und -evaluierung

Bei der im Vorfeld durchgeführten Gefährdungsermittlung und -einstufung entstehen bei zwei Prozessschritten die Gefährdung *unbemerkter Ladungsverlust* durch technische Fehler des ZIS. Die als nicht vertretbar eingestuften Risiken gilt es mittels der expliziten Risikoabschätzung und -evaluierung zu beurteilen. Hierzu werden die harmonisierten Entwurfsziele gemäß [CSM15] herangezogen, da es sich beim ZIS um ein „programmierbares elektronisches technisches System“ nach [CSM15] handelt.

Beim ZIS kann aus folgenden (Fehl-)Funktionen ein katastrophaler Unfall resultieren:

- Erfassung der Beladungsdaten,
- Ermittlung des Gesamtzuggewichts,
- Übertragung der Beladungsdaten sowie
- Anzeige der Warnmeldung.

Bei den vier Funktionsausfällen wirken identische Sicherheitsbarrieren, weswegen die Ermittlung der Ausfallrate für die technischen Funktionen zusammengefasst wird. Wären keine identischen Barrieren vorhanden, müssten die Funktionsausfälle separat voneinander betrachtet werden und der in Abbildung 19 dargestellte Ablauf einzeln abgearbeitet werden.

Nachfolgend ist beispielhaft dargestellt, wie sich die Ausfallrate für technische Funktionen eines „elektrischen, elektronischen oder programmierbaren elektronischen technischen“ [CSM15] Eisenbahnsystems unter Berücksichtigung von zusätzlichen Sicherheitsbarrieren bestimmen lässt. Den weiteren Umgang mit diesen Ausfallraten thematisiert Kapitel 8. Basis für die angeführten Vorgänge und Kalkulationen bildet der Leitfaden für die Anwendung der harmonisierten Entwurfsziele der ERA [ERA17].

Beim Funktionsversagen kann es, wie bereits in Tabelle 8 definiert, zu einem Unfall mit mehreren Toten kommen. Dementsprechend darf lediglich ein höchst unwahrscheinliches Auftreten für dieses Funktionsversagen vorgesehen werden.

Ein Funktionsversagen des ZIS führt jedoch nicht unmittelbar zu einem Unfall. Die Barrieren

- Zug befindet sich nicht in Bewegung,
- kein (ausreichend großes) Leck vorhanden,
- Ladungsverlust wird bemerkt und
- Unfalleintritt ohne Verletzte und Tote

können das Risiko verringern.

Häufig werden die Wahrscheinlichkeiten für das Wirken der Barrieren in Expertenrunden ermittelt. Da im Rahmen des Forschungsprojekts allein ein fiktives EVU betrachtet wird, können die Angaben hier ebenfalls nur hypothetisch erfolgen. Konkrete Herleitungen und zugrundeliegende Methoden seien an dieser Stelle nicht näher beleuchtet. Die Angaben dienen lediglich dem übergeordneten Ziel, die Auswirkung von Sicherheitsbarrieren zu bestimmen. Es werden die in Abbildung 22 angegebenen Wahrscheinlichkeiten definiert.

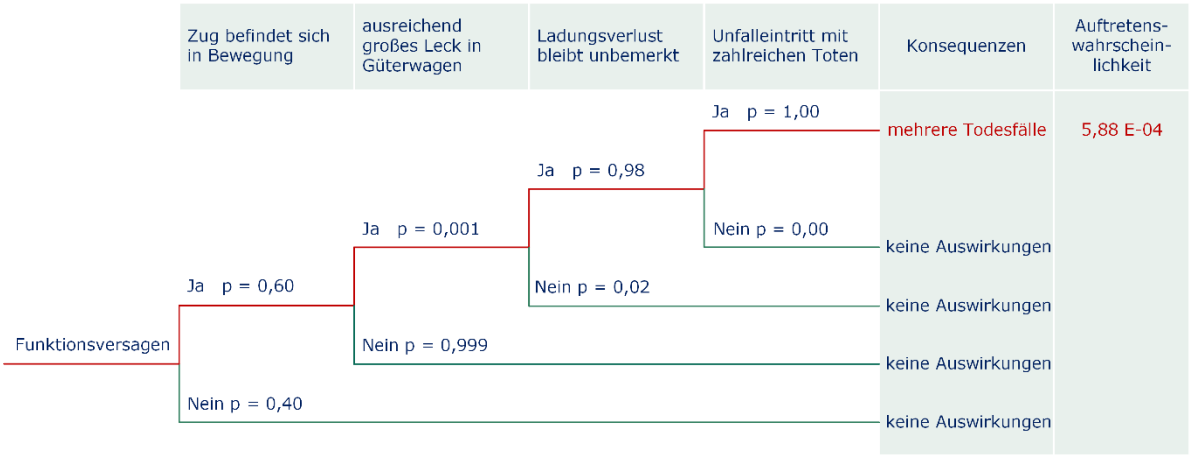


Abbildung 22: Ereignisbaum für Funktionsversagen des ZIS

Es ergibt sich ein kritischer Pfad mit einer Auftretenswahrscheinlichkeit von $P(kritischer\ Pfad) = 5{,}88 \cdot 10^{-4}$. Durch Anwendung der Formel 4 kann die zulässige Ausfallrate für alle Funktionen des ZIS bestimmt werden (siehe Formel 4). Für diese Ausfallrate gilt es den Nachweis (siehe Kapitel 8) zu erbringen.

$$DT(Funktion_x\ des\ ZIS) = \frac{1{,}00 \cdot 10^{-9}\ h^{-1}}{5{,}88 \cdot 10^{-4}} = 1{,}701 \cdot 10^{-6}\ h^{-1} \qquad (4)$$

Die Anwendung und Einhaltung der ermittelten Ausfallraten verringern als Schutzmaßnahme das Risiko für die genannten Fehler. Die zugehörige Dokumentation erfolgt im überarbeiteten Gefährdungsprotokoll

(siehe Anhang A7, Tabelle A.23). Es ergibt sich ein allgemein vertretbares Risiko für die Fehler im Gefährdungsprotokoll Nr. 6 und 8. Abbildung 23 stellt den praktischen Ablauf der Anwendung der harmonisierten Entwurfsziele für das Beispiel des technischen Zugintegritätssystems dar.

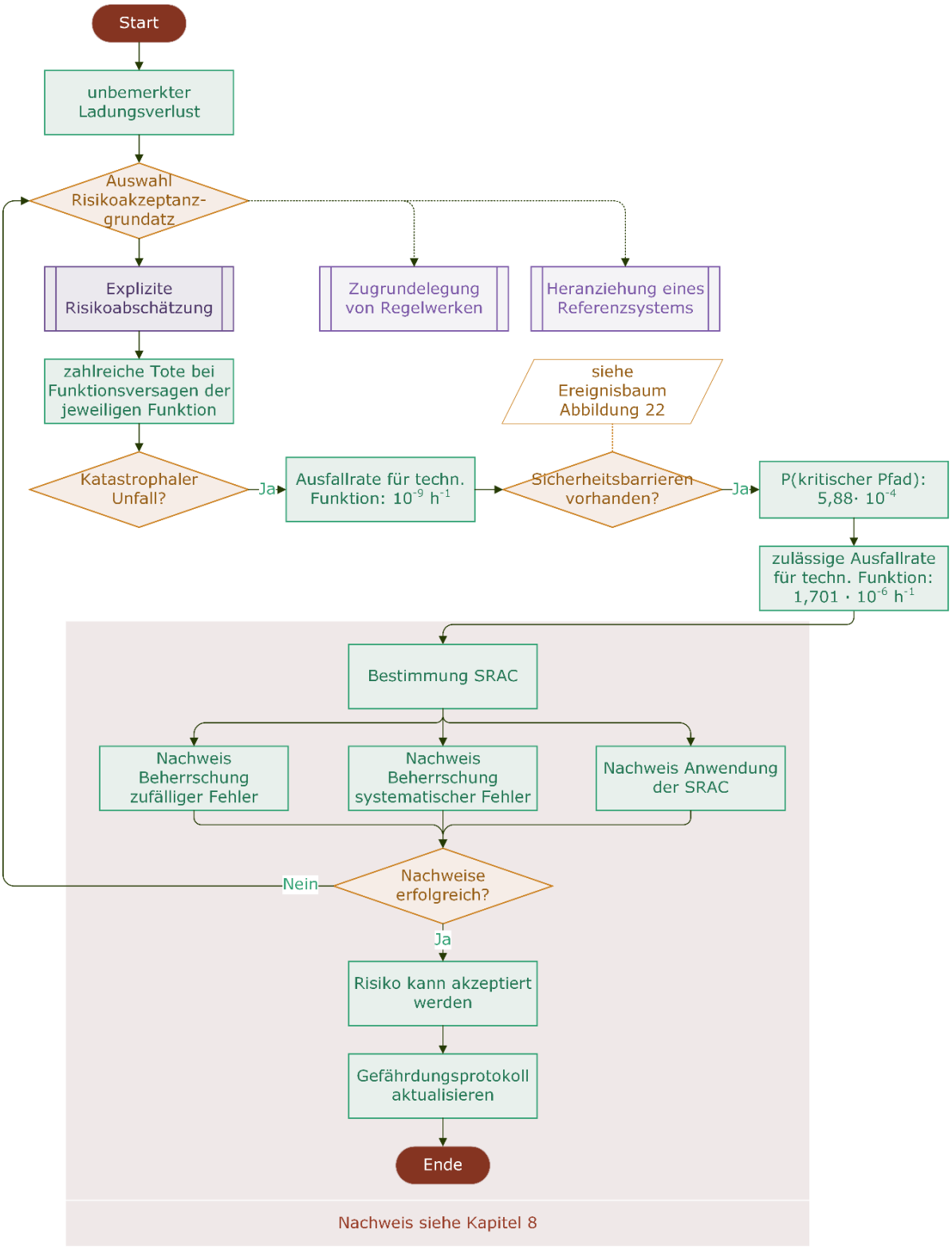


Abbildung 23: Ablauf der Anwendung der expliziten Risikoabschätzung und -evaluierung im fiktiven EVU

7 Bestimmung der Sicherheitsanforderungen

7.1 Methodisches Vorgehen

Bei einer sicherheitsrelevanten und signifikanten Änderung am Eisenbahnsystem muss neben der umfassenden Betrachtung des vom untersuchten System bzw. von der Änderung ausgehenden Risikos auch die Einhaltung der allgemeinen Sicherheitsanforderungen an das Gesamtsystem beurteilt werden. Hierfür ist die Ermittlung von Sicherheitsanforderungen und der Nachweis der Umsetzung von daraus abgeleiteten Sicherheitsmaßnahmen notwendig.

7.1.1 Kategorien der Sicherheitsanforderungen

Nach der DIN EN 50126-2 [EN262] können Sicherheitsanforderungen in drei Kategorien unterschieden werden:

- funktionale Sicherheitsanforderungen,
- technische Sicherheitsanforderungen und
- kontextuelle Sicherheitsanforderungen.

Funktionale Sicherheitsanforderungen

Funktionale Sicherheitsanforderungen bezeichnen Forderungen an die Ausübung eines definierten Prozessschritts. Dies umfasst sowohl das „erwartete funktionale Verhalten [der] sicherheitsbezogenen Funktion [als auch] das Verhalten der sicherheitsbezogenen Funktion bei Ausfällen“ [EN262]. Funktionale Sicherheitsanforderungen werden quantitativ und qualitativ definiert.

Den Nachweis qualitativer Sicherheitsanforderungen kann der Vorschlagende für interne Prozesse eigenverantwortlich erbringen. In diesem Fall wird der Nachweis mittels Anwendungsvorschriften oder dem Prozessablauf selbst geführt.

Die Definition eines Notfallmanagementsystems ist z. B. eine solche qualitative Sicherheitsanforderung. Hierbei wird der Nachweis über die vorhandenen Dokumentationen des Notfallmanagementsystems sowie dessen Wirken in Notfallübungen und bei real existierenden Notfällen erbracht.

Bei technischen Komponenten ist der Hersteller im Rahmen der Systementwicklung dafür zuständig, den funktionalen Sicherheitsnachweis zu erbringen. In diesem Fall bestehen die funktionalen Sicherheitsanforderungen aus quantitativen und qualitativen Bestandteilen. Insbesondere die CENELEC-Normenreihe DIN EN 5012x regelt die Nachweisführung von funktionalen Sicherheitsanforderungen für Bahnanwendungen und gilt in diesem Fall als Standardregelwerk.

Technische Sicherheitsanforderungen

Technische Sicherheitsanforderungen werden für einzelne physische Komponenten des Systems definiert und „umfassen technische Beschränkungen für den Entwurf/die Installation/die Nutzung“ [EN262] der Komponenten. Die Verwendung von hitzebeständigem Material aufgrund von Gefährdungen durch Feuer ist eine bezeichnende technische Sicherheitsanforderung.

Ihr Nachweis kann z. B. durch physische Vor-Ort-Kontrollen erbracht werden. Gleichfalls gilt die Dokumentation des Entwicklungsprozesses nach DIN EN 5012x als Nachweis für technische Sicherheitsanforderungen. Bei der Beurteilung von betrieblichen und organisatorischen Änderungen spielen systembedingt technische Sicherheitsanforderungen eine untergeordnete Rolle.

Kontextuelle Sicherheitsanforderungen

Kontextuelle Sicherheitsanforderungen „decken die den Betrieb und die Instandhaltung betreffenden Sicherheitsanforderungen ab“ [EN262]. Schulungsanforderungen und Instandhaltungsintervalle sind typische kontextuelle Sicherheitsanforderungen. Aus ihnen werden u. a. sicherheitsbezogene Anwendungsbedingungen (SRAC – Safety Related Application Conditions) abgeleitet.

Ihre Einhaltung kann analog zu qualitativen funktionalen Sicherheitsanforderungen vom Vorschlagenden selbst mittels Nachweisdokumenten aufgezeigt werden.

7.1.2 Sicherheitsanforderungen im Risikomanagementverfahren

Im Rahmen des Risikomanagementverfahrens werden Sicherheitsanforderungen an unterschiedlichen Abschnitten eruiert. Nachfolgend sollen verschiedene Arten umzusetzender Sicherheitsmaßnahmen und deren Nachweismöglichkeiten entsprechend dem Ablauf des Risikomanagementverfahrens vorgestellt werden.

Sicherheitsanforderungen aus der Systemdefinition

Zu Beginn des Risikomanagementverfahrens werden bei der Systemdefinition bereits umzusetzende Sicherheitsmaßahmen spezifiziert. Die Ausgestaltung und Implementierung des SMS stellt eine solche Sicherheitsmaßnahme dar. Weiterhin gelten Schnittstellen zu interagierenden Systemen im erweiterten Sinne ebenfalls als Sicherheitsmaßnahmen. Dies ist dann der Fall, wenn Aufgaben und Prozesse aus Sicherheitsgründen ausgelagert werden. Ein Beispiel im fiktiven EVU wäre die Durchführung von Weiterbildungsmaßnahmen durch einen externen Ausbildungsträger aufgrund eines fehlenden geeigneten internen Ausbilders. In diesem Fall wird der Sicherheitsmangel bei einer internen Schulung im Prozess erkannt und eine entsprechende Reaktion eingeleitet. Dies ist entsprechend im Prozess *Schulungsprogramm* (siehe Anhang 4, Abschnitt 4.2) veranschaulicht.

Typischerweise werden bei der Systemdefinition qualitative funktionale, technische sowie kontextuelle Sicherheitsanforderungen bestimmt und im System integriert. Der Nachweis der Erfüllung erfolgt direkt bei der Implementierung dieser Anforderungen im System. Eine zusätzliche Nachweisführung ist daher nicht notwendig.

Sicherheitsanforderungen aus der Gefährdungsermittlung und -einstufung

Im Rahmen der Gefährdungsermittlung und -einstufung können zusätzliche Sicherheitsanforderungen determiniert werden, um nicht allgemein vertretbare Risiken zu reduzieren. Die zusätzlichen Anforderungen werden in diesem Arbeitsschritt direkt im System implementiert und im Gefährdungsprotokoll hinterlegt. Ein Nachweis der Erfüllung wird analog zur Systemdefinition über die Implementierung der Maßnahmen im betrachteten System geführt.

Sicherheitsanforderungen aus der Risikoevaluierung

Während der Anwendung der drei Risikoakzeptanzgrundsätze werden ebenfalls notwendige Sicherheitsanforderungen definiert. Diese unterscheiden sich in Abhängigkeit der angewandten Risikoakzeptanzgrundsätze.

1. Zugrundelegung von Regelwerken

   Bei der Zugrundelegung von Regelwerken muss gemäß Anhang I Punkt 2.3.5 b) der CSM-Verordnung [CSM15] die Anwendung des betrachteten Regelwerks als Sicherheitsanforderung im Gefährdungsprotokoll erfasst werden.
   Der jeweilige Nachweis hängt vom Regelwerk und seinen Festlegungen ab.

2. Heranziehung eines Referenzsystems

   Sicherheitsanforderungen werden „aus Sicherheitsanalysen oder aus einer Bewertung der Sicherheitsdokumentation des Referenzsystems abgeleitet“ [CSM15] und im Gefährdungsprotokoll erfasst. Je nach Kategorie der Sicherheitsanforderung erfolgt anschließend der Nachweis durch den Vorschlagenden selbst oder bei technischen Systemen durch den Systemhersteller. Dabei müssen vor allem die ähnlichen Funktionen, Schnittstellen sowie Betriebs- und Umgebungsbedingungen erfüllt werden.

3. Explizite Risikoabschätzung – Harmonisierte Entwurfsziele

   Im Zuge der Anwendung der harmonisierten Entwurfsziele für „elektrische, elektronische und programmierbare elektronische technische“ [CSM15] Eisenbahnsysteme werden quantitative und qualitative funktionale Sicherheitsanforderungen für Funktionen des betrachteten Systems definiert. Jegliche unterstellte Sicherheitsbarrieren müssen ebenfalls als Sicherheitsanforderung angesehen werden. Hintergrund dessen ist, dass bei einem fehlenden Wirken dieser Barrieren das Risiko des Systems höher ist als das allgemein vertretbare Risiko, welches über die harmonisierten Entwurfsziele definiert wird.
   Folgende Belege müssen im Nachweis der Erfüllung der Sicherheitsanforderungen erbracht werden:
   - Nachweis der Erfüllung der harmonisierten Entwurfsziele (Beherrschung zufälliger Fehler),
   - Nachweis der Beherrschung von systematischen Fehlern und
   - Nachweis der sicheren Integration des technischen Systems in das betrachtete Eisenbahnsystem.

   Die Voraussetzungen der erfolgreichen Nachweisführung gelten u. a. dann als erfüllt, wenn ein DIN EN 5012x-konformer Entwicklungsprozess erfolgreich durchlaufen wird, da in ebendiesem Entwicklungsprozess zweckmäßige Nachweisführungen definiert sind.

7.2 Sicherheitsanforderungen und -maßnahmen im fiktiven EVU

Eine detaillierte Definition und Nachweisführung der Sicherheitsmaßnahmen in den Prozessschritten Systemdefinition und Gefährdungsermittlung und -einstufung kann aufgrund der bereits skizzierten Belege vernachlässigt werden. Wichtig ist, dass die zusätzlichen Anforderungen im System implementiert und im Gefährdungsprotokoll hinterlegt sind.

Für das im Forschungsprojekt betrachtete fiktive EVU lassen sich bei der Gefährdungsermittlung und -einstufung zusätzliche Anforderungen für zwei Gefährdungen definieren. Dies betrifft Nr. 1 und 2 in Tabelle 5 (siehe auch Anhang A5, Tabelle A.22). Zur Reduzierung der Häufigkeit des Gefahrenfalls wird das SMS im *Kompetenzmanagement* angepasst. Infolgedessen müssen die im Rahmen der Mitarbeiterkompetenz definierten Kenntnisse, Fertigkeiten, Erfahrungen und nachzuweisende Qualifikationen für die Berufsgruppe Disponent um die Anforderungen an die Durchführung des Notfallmanagements erweitert

werden. Das Verfahren zur Bewertung der Befähigung der Mitarbeiter wird ebenso wie das Schulungsprogramm aktualisiert. Im Zuge von ohnehin implementierten Überwachungsmaßnahmen des *Kompetenzmanagements* wird deren Umsetzung durch das Personalmanagement überwacht.

7.2.1 Nachweis bei Zugrundelegung von Regelwerken

Im Ergebnis der Zugrundelegung von Regelwerken ergeben sich Gegenmaßnahmen entsprechend der Umsetzung nach Tabelle 9. Im überarbeiteten Gefährdungsprotokoll wird folgende Schutzmaßnahme definiert: *Anwendung der Umsetzungsempfehlung des [VCI17].*

Der Gefahrgutbeauftragte ist im Zuge seiner verantwortungsvollen Aufgaben für die Umsetzung und Kontrolle der definierten Anforderungen zuständig und dokumentiert dies im Rahmen seiner Pflichten nach [GBV21]. Auch für das hier relevante Schnittstellen-Management (vgl. Anhang I Punkt 1.2 der CSM-Verordnung [CSM15]) mit dem EIU, welches für Abstellorte, die nicht im Verantwortungsbereich des fiktiven EVU liegen, ist der Gefahrgutbeauftragte verantwortlich.

7.2.2 Nachweis bei Heranziehung eines Referenzsystems

Als Referenzsystem wird das bereits bei einem weiteren imaginären EVU anerkannte und eingesetzte computergestützte Dispositionssystem herangezogen (siehe Abschnitt 6.2.2). Die Ähnlichkeit der beiden Systeme stellt Tabelle 10 dar. Ebendiese Charakteristika gelten als Sicherheitsanforderungen, da sonst nicht gewährleistet ist, dass Gefährdungen des computergestützten Dispositionssystems „durch ein ähnliches System angemessen abgedeckt“ [CSM15] werden.

Für den Nachweis der Anforderungen ist primär der Betreiber, welcher in diesem Fall das fiktive EVU ist, zuständig. Das fiktive EVU muss das computergestützten Dispositionssystem unter exakt den definierten Kriterien einsetzen und dies dokumentieren. Der Nachweis der Einhaltung der Funktionen und Betriebsbedingungen wird vorwiegend durch den Hersteller des computergestützten Dispositionssystems erbracht.

7.2.3 Nachweis bei expliziter Risikoanalyse

Die Anwendung der harmonisierten Entwurfsziele, wie in Abschnitt 6.2.3 vorgestellt, induziert mehrere funktionale Sicherheitsanforderungen für Funktionen des ZIS. Beispielhaft ist die sicherheitsrelevante Funktion *Erfassung der Beladungsdaten* in Tabelle 11 zusammen mit dem deklarierten Sicherheitsziel und den Sicherheitsanforderungen basierend auf den berücksichtigten Barrieren zusammengefasst. Für die anderen Funktionen *Ermittlung des Gesamtzuggewichts, Übertragung der Beladungsdaten* sowie *Anzeige der Warnmeldung* gelten identische Anforderungen, da sich das Schadensausmaß und die Sicherheitsbarrieren zwischen den Funktionen nicht unterscheiden.

Auch die Anforderungen, die an die berücksichtigten Barrieren gestellt werden, müssen zwingend eingehalten werden, da sonst das berechnete Entwurfsziel der Funktionen zu niedrig und die Sicherheit des ZIS nicht gewährleistet ist.

TABELLE 11: ENTWURFSZIEL UND SICHERHEITSANFORDERUNGEN FÜR FUNKTION ERFASSUNG DER BELADUNGSDATEN

Entwurfsziel	$DT(Erfassung\ der\ Beladungsdaten) = 1{,}701 \cdot 10^{-6}\ h^{-1}$
Sicherheitsanforderungen aus definierten Barrieren	Einhaltung der vorhandenen Fahr- und Umlaufpläne
	Einsatz der berücksichtigten Güterwagen und deren Wahrscheinlichkeit für ein Leck
	Einhaltung der herangezogenen Exposition der Güterwagen hinsichtlich der Einwirkung Dritter
	Einhaltung der unterstellten Umgebungsbedingungen einer Güterzugfahrt

Gemäß CENELEC-Normenreihe DIN EN 5012x sind für die Entwicklung von Bahnanwendungen sowohl der Betreiber als auch der Hersteller zuständig. In den Entwicklungsphasen 1 (Konzept) bis 4 (Festlegung von Systemanforderungen) definiert der Betreiber, der im vorliegenden Fall das fiktive EVU ist, die RAMS-Anforderungen an das ZIS und übergibt diese dem Hersteller. Der Hersteller ist im Zuge der Phasen 5 (Architektur und Aufteilung von Systemanforderungen) bis 9 (Systemvalidierung) für die Implementierung und Nachweisführung der Übereinstimmung des zu entwickelnden Systems mit den RAMS-Anforderungen zuständig. Speziell in Phase 6 (Entwurf und Implementierung) wird vom Hersteller der Sicherheitsnachweis geführt. Dieser begründet, „dass das System die festgelegten Sicherheitsanforderungen erfüllt“ [EN126] und besteht aus den in Abbildung 24 dargestellten Komponenten. Der Sicherheitsnachweis dokumentiert somit den Nachweis der Erfüllung der harmonisierten Entwurfsziele sowie der Beherrschung von systematischen Fehlern.

Abbildung 24: Bestandteile des Sicherheitsnachweises gemäß [EN126]

Für die sichere Integration des ZIS in das betrachtete Bahnsystem sind beide Akteure gemeinsam verantwortlich. Zum einen definiert der Hersteller Verfahren für die Installation, die Inbetriebnahme, den Betrieb und die Instandhaltung sowie Schulungsmaßnahmen und den Abnahmeprozess. Diese Vorgaben gelten ebenfalls als Sicherheitsanforderungen. Zum anderen ist der Betreiber selbst für den Abnahmeprozess verantwortlich. Durch diesen wird der Nachweis geführt, dass das ZIS sicher integriert ist.

8 Zusammenfassung und Ausblick

Im Forschungsprojekt „Anwendung der CSM-Verordnung 402/2013/EU für das Teilsystem Verkehrsbetrieb und Verkehrssteuerung“ wurde für die betriebliche und organisatorische Änderung eines neu in den deutschen Schienenverkehr eintretenden, fiktiven EVU das Risikomanagementverfahren gemäß [CSM15] beispielhaft durchlaufen. Der Fokus lag dabei auf der Darstellung des methodischen Vorgehens.

Hierfür wurden in Kapitel 5 mehrere Methoden zur Erstellung einer CSM-konformen Systemdefinition eingeführt und diese anhand des fiktiven EVU beispielhaft vorgestellt. Dies beinhaltete eine strukturelle Unterteilung des Systems sowie die Abgrenzung zu anderen Systemen unter Identifikation von notwendigen Schnittstellen. Darauf aufbauend wurden Prozesse im fiktiven EVU definiert und in Prozessablaufdiagrammen dargestellt. Bei der Erarbeitung der Systemdefinition wurde bewusst auf einzelne Verknüpfungen der Komponenten und Prozesse untereinander verzichtet. Dies ist damit begründet, dass das gesamte Risikomanagementverfahren nach der CSM-Verordnung im Rahmen dieses Forschungsprojekts durchlaufen werden sollte. Dementsprechend war es zunächst notwendig, entsprechende Risiken in der Systemdefinition zu bestimmen. Solche potenziellen Risiken betreffen nachfolgend benannte Sachverhalte:

- Es werden keine detaillierten Anforderungen betreffend der ordnungsgemäßen Sicherung, guten Beleuchtung und angemessenen Unzugänglichkeit von Abstellorten von Güterzügen beim Transport von Gefahrgütern spezifiziert.
- Es werden keine Anforderungen an das computergestützte Dispositionssystem definiert.
- Es werden keine Sicherheitsanforderungen für das innovative technische Zugintegritätssystem aufgeführt.

Diese Auflistung stellt lediglich einen kurzen Einblick in die betrachteten potenziellen Gefährdungen des beschriebenen Systems dar.

In der auf der Systemdefinition aufbauenden Gefährdungsermittlung und -einstufung (siehe Kapitel 6) wurden ebendiese nicht allgemein vertretbaren Risiken herausgearbeitet. Hierfür wurde die grundsätzliche Verfahrensweise der Gefährdungsermittlung und -einstufung präsentiert. Insbesondere die Methoden

- FME(C)A,
- Ereignisbaumanalyse sowie
- Risikomatrix

wurden vorgestellt. Sie dienen der Ermittlung von Fehlern und Gefährdungen einschließlich ihrer Auswirkungen. Darauf aufbauend erfolgte eine musterhafte Herausarbeitung des Gefährdungsprotokolls für die genannten Risiken. Somit konnte das Vorgehen zur Einstufung der Gefährdungen, die aus der betrachteten Änderung hervorgehen, exemplarisch beschrieben werden.

Es sei an dieser Stelle nochmals betont, dass die für das fiktive EVU gesammelten Erkenntnisse für real existierende EVU unterschiedlich und daher nicht unmittelbar übertragbar sind. Durch differente Anwendungsbedingungen oder abweichende Prozesse und Sicherheitsmanagementmaßnahmen lassen sich andere Gefährdungen, Schäden oder Eintrittswahrscheinlichkeiten identifizieren. Auch variierende Fehler und Ausfälle können sich ergeben.

Die Gefährdungsermittlung gemäß Anhang I Punkt 2.2 [CSM15] erfüllt nicht nur den Zweck des Nachweises des ordnungsgemäß durchgeführten Risikomanagementverfahrens. Wie in Kapitel 6.2.1 verdeut-

licht wurde, dient die Ermittlung potenzieller Gefährdungen dem anwendenden EVU auch dazu, die eigenen Prozesse zu analysieren und ggf. Anpassungen des SMS oder der implementierten Komponenten und Tätigkeitsabläufe vorzunehmen. Damit entsteht ein praktisches Werkzeug zur Wahrung und stetigen Verbesserung der Sicherheit im Eisenbahnsystem.

Die Gefährdungsermittlung und -einstufung ist jedoch nur dann aussagefähig, wenn die Systembeschreibung und die ermittelten Daten für Häufigkeit und Schadensausmaß eines Unfalles hinreichend belastbar sind. Je konkreter das System beschrieben oder je umfassender die Datenbasis für die Ermittlung von Häufigkeit und Schadensausmaß eines Unfalls sind, desto genauer lässt sich das Ergebnis der daraus resultierenden Risikoabschätzung bestimmen. Entsprechend wird im günstigen Fall die Dunkelziffer der Risiken so gering sein, dass eine Gefährdung belastbar bestimmt wird. Idealerweise sind ausreichend große statistische Auswertungen zur Bestimmung der definierten Größen vorhanden. Dies ist jedoch insbesondere bei neuen Systemen in der Realität selten gegeben bzw. gestaltbar. Daher empfiehlt es sich, das Risikomanagementverfahren auf Basis einer breit aufgestellten Expertise unter Anwendung von systematischen Methoden durchzuführen. Ebenfalls wird hier die Notwendigkeit einer ausführlichen Systemdefinition deutlich. Nur wenn das System einschließlich seiner Komponenten und definierter Prozesse ausreichend bekannt ist, können dessen Gefährdungen vollumfänglich ermittelt werden. Diese wesentlichen Randbedingungen dienen dazu, in gewisser Weise die Vollständigkeit und Richtigkeit der Einschätzungen sicherzustellen.

Bei großer Ungewissheit hinsichtlich der Kriterien einer Gefährdung sollte, wie in Risikoanalysen allgemein üblich, zur sicheren Seite entschieden werden. Daraus resultiert im Zweifelsfall eine Einstufung als größeres Risiko. Entsprechend wird die betrachtete Gefährdung beim Durchlaufen des Risikoanalyseprozesses weiter berücksichtigt und ihre potenziellen Auswirkungen näher untersucht.

In der auf diesen Erkenntnissen aufbauenden Risikoevaluierung (siehe Kapitel 7) wurden die nicht vertretbaren Risiken mittels Anwendung der drei Risikoakzeptanzgrundsätze

- Anwendung der Regelwerke,
- Analyse der Ähnlichkeit mit Referenzsystemen sowie
- Ermittlung von Szenarien und Sicherheitsmechanismen durch die explizite Risikoabschätzung

näher betrachtet. Dafür wurden die Abläufe zur Anwendung der Risikoakzeptanzgrundsätze charakterisiert. Anhand von konkreten Beispielen wurden die entscheidenden Kriterien zur Anwendung der einzelnen Risikoakzeptanzgrundsätze demonstriert.

Im Ergebnis jeder Anwendung der Risikoakzeptanzgrundsätze war für das fiktive EVU die Bestimmung allgemein vertretbarer Risiken unter Voraussetzung der Einhaltung der im Zuge dessen definierten Sicherheitsmaßnahmen (siehe Kapitel 8) möglich. Das wesentliche Ziel bestand darin, entsprechende Sicherheitsanforderungen und umzusetzende Sicherheitsmaßnahmen zu definieren, damit schlussendlich der erstmalige Betrieb von Eisenbahnverkehr in Deutschland durch das fiktive EVU mit vertretbaren Risiken vonstattengehen kann. Diesbezüglich wurden Kategorien von Sicherheitsanforderungen und deren Nachweismöglichkeiten vorgestellt. Zudem stellte Abschnitt 8.1.2 den Umgang mit diversen Sicherheitsanforderungen in den unterschiedlichen Abschnitten des Risikomanagementverfahrens nach der CSM-Verordnung vor.

Im nicht in den Ausführungen des Forschungsprojekts enthaltenen, nachfolgenden Schritt würde das fiktive EVU „eine unabhängige Bewertung der Eignung sowohl der Anwendung des in Anhang I dargelegten Risikomanagementverfahrens als auch seiner Ergebnisse“ [CSM15] durch eine anerkannte Bewertungsstelle veranlassen. Ihre Arbeiten sowie deren Ergebnisse dokumentiert die Bewertungsstelle im Sicherheitsbewertungsbericht.

Abkürzungsverzeichnis

ADN	Accord européen relatif au transport international des marchandises Dangereuses par voie de Navigation intérieure (dt.: Europäisches Übereinkommen für die Beförderung gefährlicher Güter auf dem Binnenwasserweg)
ADR	Accord européen relatif au transport international des marchandises Dangereuses par Route (dt.: Europäisches Übereinkommen über die Beförderung gefährlicher Güter auf der Straße)
AuB	Auftraggeber und Besteller
BGL	Bundesverband Güterkraftverkehr Logistik und Entsorgung e. V.
CENELEC	Comité Européen de Normalisation Électrotechnique (dt.: Europäisches Komitee für elektrotechnische Normung)
CSM	Common Safety Methods (dt.: gemeinsame Sicherheitsmethoden)
Dispo	Disposition
DT	Design Target (dt.: Entwurfs-/Sicherheitsziel)
EB	Eisenbahnbetrieb
EBA	Eisenbahn-Bundesamt
EBO	Eisenbahn-Bau- und Betriebsordnung
ECM	Entity in Charge of Maintenance (dt.: für die Instandhaltung zuständige Stelle)
EdB	Eisenbahnen des Bundes
EI	Eisenbahninfrastruktur
EIU	Eisenbahninfrastrukturunternehmen
ERA	European Union Agency for Railways (dt.: Europäische Eisenbahnagentur)
EVU	Eisenbahnverkehrsunternehmen
Fdl	Fahrdienstleiter
FM	Fahrzeugmanagement
FMEA	Failure Mode and Effects Analysis (dt.: Fehlzustandsart- und –auswirkungsanalyse)
FMECA	Failure Mode and Effects and Criticality Analysis (dt.: Fehlzustandsart-, -auswirkungs- und Kritikalitätsanalyse)
FME(C)A	siehe FMECA
GVZ	Güterverkehrszentrum
IHE	(externe) Instandhaltungseinrichtung
LE	Leitungsebene

MA	Mitarbeiter
PM	Personalmanagement
RAMS	Reliability, Availability, Maintainability, Safety (dt.: Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit)
RID	Règlement concernant le transport international ferroviaire de marchandises Dangereuses (dt.: Ordnung über die internationale Eisenbahnbeförderung gefährlicher Güter)
RPZ	Risikoprioritätszahl
SGV	Schienengüterverkehr
SiBe	Sicherheitsbescheinigung
Sifa	Sicherheitsfahrschaltung
SMS	Sicherheitsmanagementsystem
SPFV	Schienenpersonenfernverkehr
SPNV	Schienenpersonennahverkehr
SPV	Schienenpersonenverkehr
SRAC	Safety Related Application Condition (dt.: sicherheitsbezogene Anwendungsbedingung)
TAV	Technikbasiertes Abfertigungsverfahren
Tf	Triebfahrzeugführer
TSI OPE	technical specifications for interoperability relating to the operation and traffic management subsystem (dt.: Technische Spezifikationen für die Interoperabilität des Teilsystems „Verkehrsbetrieb und Verkehrssteuerung“)
VCI	Verband der Chemischen Industrie e.V.
VDV	Verband Deutscher Verkehrsunternehmen e. V.
Ww	Weichenwärter
Zb	Zugbegleiter
ZIS	technisches Zugintegritätssystem

Abbildungsverzeichnis

Abbildung 1: Ablauf des Risikomanagementverfahrens nach [CSM15] ... 10
Abbildung 2: Bereiche des Sicherheitsmanagementsystem (SMS) nach [SMS18] ... 14
Abbildung 3: Beispielhafte Darstellung einer produktorientierten Systemdefinition ... 18
Abbildung 4: Beispielhafte Darstellung einer prozessorientierten Systemdefinition ... 19
Abbildung 5: Produktorientierte Systemdefinition, Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“ ... 20
Abbildung 6: Schematische Darstellung des Zugintegritätssystem (ZIS) ... 22
Abbildung 7: Teilprozess Fahrt durchführen und Fahrzeug abrüsten im SGV ... 23
Abbildung 8: Darstellung des Wirkungsmodells ... 26
Abbildung 9: Ablauf zur Erstellung des Gefährdungsprotokolls ... 27
Abbildung 10: Ablauf einer FMEA nach [DIN812] ... 29
Abbildung 11: Schematische Darstellung eines Ereignisbaums ... 31
Abbildung 12: Differente Darstellung eines Ereignisbaums ... 31
Abbildung 13: Ablauf zur Aufstellung einer Risikomatrix nach [EN126] ... 32
Abbildung 14: Reduzierter Ereignisbaum: falsch/fehlerhaft verarbeitete Dispositionsentscheidung ... 38
Abbildung 15: Ablauf der Anwendung der Risikoakzeptanzgrundsätze (vereinfachte Darstellung) nach [CSM15] ... 42
Abbildung 16: Ablauf *Zugrundelegung von Regelwerken* und Risikoevaluierung nach [CSM15] ... 43
Abbildung 17: Ablauf *Heranziehung eines Referenzsystems* und Risikoevaluierung nach [CSM15] 45
Abbildung 18: Ermittlung des Entwurfsziels bei implementierten Barrieren nach [ERA17] ... 46
Abbildung 19: Ablauf Explizite Risikoabschätzung und -evaluierung nach [CSM15] ... 48
Abbildung 20: Ablauf der Anwendung der Zugrundelegung von Regelwerken und Risikoevaluierung im fiktiven EVU ... 52
Abbildung 21: Ablauf der Anwendung der Heranziehung eines Referenzsystems und Risikoevaluierung im fiktiven EVU ... 55
Abbildung 22: Ereignisbaum für Funktionsversagen des ZIS ... 56
Abbildung 23: Ablauf der Anwendung der expliziten Risikoabschätzung und -evaluierung im fiktiven EVU ... 57
Abbildung 24: Bestandteile des Sicherheitsnachweises gemäß [EN126] ... 62
Abbildung A.25: Produktorientierte Systemdefinition, Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“ ... 82
Abbildung A.26: Schematische Darstellung des ZIS ... 86
Abbildung A.27: Symbole der Prozessablaufdiagramme ... 89
Abbildung A.28: Prozess: Einstellung von Personal ... 90

Abbildung A.29: Prozess: Schulungsprogramm 92
Abbildung A.30: Prozess: Erwerb von Fahrzeugen 93
Abbildung A.31: Prozess: Disposition 95
Abbildung A.32: Prozess: Fahrt vorbereiten, durchführen und Fahrzeug abrüsten im SPV 97
Abbildung A.33: Prozess: Fahrt vorbereiten, durchführen und Fahrzeug abrüsten im SGV 100
Abbildung A.34: Prozess: Instandhaltung von Fahrzeugen 101
Abbildung A.35: Prozess: Außerbetriebnahme von Fahrzeugen 102
Abbildung A.36: Ereignisbaum: falsch/fehlerhaft verarbeitete Dispositionsentscheidung 105

Tabellenverzeichnis

Tabelle 1: Kategorisierung der Häufigkeit des Gefahrenfalls nach [EN126] ... 33
Tabelle 2: Kategorisierung des Schadensausmaßes nach [EN126] ... 33
Tabelle 3: Risikokategorien nach [EN126] ... 33
Tabelle 4: Risikomatrix nach [EN126] ... 34
Tabelle 5: Auszug aus dem Gefährdungsprotokoll für Gefährdungen bei fehlendem Personal im Notfallmanagement und Bewertung der Schutzmaßnahmen ... 36
Tabelle 6: Auszug aus dem Gefährdungsprotokoll für Gefährdungen bei Dispositionstätigkeiten durch Fehler im computergestützten System ... 37
Tabelle 7: Auszug aus dem Gefährdungsprotokoll für Gefährdungen bei Abstellung eines Güterzugs mit Gefahrgut ... 39
Tabelle 8: Auszug aus dem Gefährdungsprotokoll für Gefährdungen bei technischem Fehler des ZIS ... 40
Tabelle 9: Vorgaben des zugrunde gelegten Leitfadens (Auszug) ... 49
Tabelle 10: Vorgaben zum computergestützten Dispostionssystem ... 54
Tabelle 11: Entwurfsziel und Sicherheitsanforderungen für Funktion Erfassung der Beladungsdaten ... 62
Tabelle A.12: Beispiele für sicherheitsrelevante Änderungen ... 75
Tabelle A.13: Abschätzung der Ausfallfolgen ... 76
Tabelle A.14: Abschätzung des Innovationsgrads ... 77
Tabelle A.15: Abschätzung der Komplexität ... 77
Tabelle A.16: Abschätzung der Überwachbarkeit ... 78
Tabelle A.17: Abschätzung der Umkehrbarkeit ... 78
Tabelle A.18: Matrix zur Signifikanzbewertung ... 79
Tabelle A.19: Zwischenergebnis der Signifikanzprüfung ... 80
Tabelle A.20: Ergebnis der Signifikanzprüfung – Schritt 1 ... 80
Tabelle A.21: Ergebnis der Signifikanzprüfung ... 81
Tabelle A.22: Gefährdungsprotokoll (Auszug) ... 103
Tabelle A.23: Überarbeitetes Gefährdungsprotokoll (Auszug) ... 106

Quellenverzeichnis

[AEG20] Allgemeines Eisenbahngesetz vom 27. Dezember 1993 (BGBl. I S. 2378, 2396; 1994 I S. 2439), geändert durch Artikel 3 des Gesetzes vom 9. Juni 2021 (BGBl. I S. 1737).

[CKB20] CERSS Kompetenzzentrum Bahnsicherungstechnik: Bericht 18045.05.01 – Auswertung der Online-Befragung zur Anwendung der Durchführungsverordnung (EU) Nr. 402/2013 für das Teilsystem Verkehrsbetrieb und Verkehrssteuerung, Dresden: März 2020.

[CSM15] 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, geändert durch Durchführungsverordnung (EU) 2015/1136 der Kommission vom 13. Juli 2015, berichtigt durch Berichtigung, ABl. L 70 vom 16.3.2016, S. 38 (2015/1136), August 2015.

[DIN812] DIN EN 60812: Fehlzustandsart- und -auswirkungsanalyse (FMEA), August 2015.

EBO19] Eisenbahn-Bau- und Betriebsordnung vom 8. Mai 1967 (BGBl. 1967 II S. 1563), die zuletzt durch Artikel 2 der Verordnung vom 5. April 2019 (BGBl. I S. 479) geändert worden ist.

[ECM19] Durchführungsverordnung (EU) 779/2019 der Kommission vom 16. Mai 2019 mit Durchführungsbestimmungen für ein System zur Zertifizierung von für die Instandhaltung von Fahrzeugen zuständigen Stellen gemäß der Richtlinie (EU)2016/798 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnung (EU) Nr. 445/2011 der Kommission, Mai 2019.

[EN126] DIN EN 50126-1: Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Generischer RAMS-Prozess; Deutsche Fassung EN 50126-1:2017, Oktober 2018.

[EN262] DIN EN 50126-2: Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 2: Systembezogene Sicherheitsmethodik; Deutsche Fassung EN 50126-2:2017, Oktober 2018.

[ERA17] European Union Agency for Railways: Guideline for the application of harmonized design targets (CSM-DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013, Mai 2017.

[EU798] Richtlinie (EU) 2016/798 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über Eisenbahnsicherheit, Mai 2016.

[GBV21] Gefahrgutbeauftragtenverordnung in der Fassung der Bekanntmachung vom 11. März 2019 (BGBl. I S. 304), die durch Artikel 3 der Verordnung vom 26. März 2021 (BGBl. I S. 475) geändert worden ist.

[GGB19] Gefahrgutbeförderungsgesetz vom 6. August 1975 (BGBl. I S. 2121), das zuletzt durch Artikel 13 des Gesetzes vom 12. Dezember 2019 (BGBl. I S. 2510) geändert worden ist.

[GGV21] Gefahrgutverordnung Straße, Eisenbahn und Binnenschifffahrt in der Fassung der Bekanntmachung vom 26. März 2021 (BGBl. I S. 481).

[HOL15] Holst, Niko; Geisler, Marc: Harmonisierte Design Targets für das Risikomanagementverfahren nach CSM-RA. In: ETR – Eisenbahntechnische Rundschau (2015), Nr. 10, S. 19–23.

[JAC03] Jacobs, Jürgen: Rechnergestützte Konfliktermittlung und Entscheidungsunterstützung bei der Disposition des Zuglaufs, Dissertation, Aachen: 2003.

[KUC11] Kuckelberg, Alexander: Mikroskopische Disposition spurgebundener Verkehrsmittel unter Echtzeitbedingungen, Dissertation, Aachen: 2011.

[NEU17] Neuber, Marco: Ein Beitrag zur operativen Zuglaufregelung unter besonderer Berücksichtigung vorausschauender Zugförderung bei der Umsetzung dispositiver Entscheidungen, Dissertation, Stuttgart: 2017.

[NTZ16] Eisenbahn-Bundesamt: Verwaltungsvorschrift für die Neue Typzulassung (NTZ) von Signal-, Telekommunikations- und Elektrotechnischen Anlagen (Stufe 2: Übergangsregelung für Signalanlagen zur Anwendung bei den Infrastrukturen der Eisenbahnen des Bundes) – VV NTZ ÜGR Stufe 2. Ausgabe 1.1, gültig ab 01.07.2016.

[RID21] Übereinkommen über den internationalen Eisenbahnverkehr (COTIF) Anhang C – Ordnung für die internationale Eisenbahnbeförderung gefährlicher Güter (RID), Januar 2021.

[SMS18] Delegierte Verordnung (EU) 2018/762 der Kommission vom 8. März 2018 über gemeinsame Sicherheitsmethoden bezüglich der Anforderungen an Sicherheitsmanagementsysteme gemäß der Richtlinie (EU) 2016/798 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EU) Nr. 1158/2010 und (EU) Nr. 1169/2010, Mai 2018.

[TfV19] Triebfahrzeugführerscheinverordnung vom 29. April 2011 (BGBl. I S. 705, 1010), die zuletzt durch Artikel 3 der Verordnung vom 26. November 2019 (BGBl. I S. 1958) geändert worden ist.

[TSI19] Durchführungsverordnung (EU) 2019/773 der Kommission vom 16.Mai 2019 über die technische Spezifikation für die Interoperabilität des Teilsystems „Verkehrsbetrieb und Verkehrssteuerung“ des Eisenbahnsystems in der europäischen Union und zur Aufhebung des Beschlusses 2012/757/EU, Mai 2019.

[VCI17] Verband der Chemischen Industrie e. V.: VCI-Leitfaden – Umsetzung der gesetzlichen Sicherungsbestimmungen für die Beförderung gefährlicher Güter (Kapitel 1.10 ADR/RID/ADN 2017). Stand: 19.10.2017.

[WIN18] Winter, Hanno: Alternative Lösungen zur Gleisfreimeldung, Folien zur 24. Sicherungstechnischen Fachtagung der Professur für Verkehrssicherungstechnik, 28.09.2018.

[WUR04] Wurst, Christian: Kapazitätssteuerung in Dienstleistungsunternehmen – Optimierungsansätze des Güterwagenmanagements, Dissertation, Kassel: 2004.

Anhänge

A1 Sicherheitsmanagementsystem im fiktiven EVU 73

A2 Sicherheitsrelevanz- und Signifikanzprüfung 75

A3 Produktorientierte Systemdefinition im fiktiven EVU 82

A4 Prozessorientierte Systemdefinition im fiktiven EVU 89

A5 Gefährdungsprotokoll 103

A6 Ereignisbaum: falsch/fehlerhaft verarbeitete Dispositionsentscheidung 105

A7 Überarbeitetes Gefährdungsprotokoll 106

A1 Sicherheitsmanagementsystem im fiktiven EVU

Nachfolgend werden ausgewählte Bereiche, welche für die Systemdefinition des fiktiven EVU besonders relevant sind, komprimiert beschrieben. Dies soll keine vollumfängliche Beschreibung des Sicherheitsmanagementsystems des fiktiven EVU darstellen. Die hier behandelten Erläuterungen dienen lediglich zum besseren Verständnis für die Systemdefinition. Insbesondere der in Punkt 5 des Anhang I der Verordnung [SMS18] dargelegte Bereich des Betriebs soll nachfolgend hinsichtlich der Systemdefinition des fiktiven EVU betrachtet werden. In den Prozessdefinitionen in den Anhängen A3 und A4 wird an zweckdienlichen Stellen auf das SMS und dessen Vorgaben eingegangen.

A1.1 Maßnahmen zur Beherrschung von Risiken

Die Verordnungen [SMS18] und [CSM15] können nie unabhängig voneinander betrachtet werden. Die Anforderungen der Verordnungen greifen ineinander und müssen stets im Kontext der diversen Anforderungen betrachtet werden. Dies betrifft insbesondere den Bereich der Beherrschung von Risiken im EVU.

Zudem werden im Rahmen des SMS Überwachungstätigkeiten zur Kontrolle der implementierten Sicherheitsmaßnahmen durchgeführt. Grundsätzlich bestehen bei dem hier betrachteten fiktiven EVU Verfahren, die dafür sorgen, dass jedwede Änderung betrieblicher, organisatorischer oder technischer Art dazu führt, dass das Verfahren gemäß [CSM15] durchlaufen und dokumentiert wird. Auch bei sicherheitsrelevanten, aber nicht signifikanten Änderungen werden die im Rahmen der Maßnahmen zur Beherrschung von Risiken geplanten Instrumente und Abläufe angewandt.

A1.2 Kompetenzmanagement

Um „sicher[zu]stellen, dass die Mitarbeiter mit Aufgaben, die die Sicherheit betreffen, zur Erfüllung der in ihre Zuständigkeit fallenden sicherheitsrelevanten Aufgaben befähigt sind“ [SMS18], werden für jede Berufsgruppe fest definierte Kenntnisse, Fertigkeiten, Erfahrungen und nachzuweisende Qualifikationen im fiktiven EVU definiert. Anforderungen an die Beschäftigten basieren auf der TSI OPE [TSI19] sowie auf Grundlage der tatsächlichen Betriebserfordernisse.

Darüber hinaus definiert das Kompetenzmanagement ein Verfahren, welches die Bewertung der Befähigung der Beschäftigten und entsprechende Handlungsweisen vorsieht. Das im Kompetenzmanagement entwickelte *Schulungsprogramm* ist explizit Bestandteil der Systemdefinition des fiktiven EVU.

Das Kompetenzmanagementverfahren regelt folgende, wesentlichen Sachverhalte:

- Kriterien für die Kompetenz des Personals für jede (insbesondere sicherheitsrelevante) Funktion im fiktiven EVU unter Berücksichtigung der Anforderungen der Aufgaben,
- Schulungsbedarf ermitteln und, soweit erforderlich, Schulungsprogramme für relevante Anforderungen für das Personal des fiktiven EVU bereitstellen,
- Nachweisführung, dass das Personal für die Aufgaben, die es ausführt, und für seine Verantwortlichkeiten die erforderlichen Kompetenzen aufweist sowie
- Überwachung der Leistungsfähigkeit des Personals des fiktiven EVU.

A1.3 Betriebsplanung und -steuerung

Für die Betriebsplanung werden Prozesse zur Beherrschung von Sicherheitsrisiken definiert. Diese umspannen die Tätigkeiten und Abläufe der Disposition sowie deren technische Unterstützungen.

A1.4 Verwaltung von Sachanlagen

Das SMS sorgt in seiner Ausgestaltung dafür, dass Sachanlagen, zu denen im Sinne dieser Systemdefinition des fiktiven EVU die Fahrzeuge gehören, einen stets sicheren Betriebszustand aufweisen. Hierzu gehören Verfahren zur Prüfung der Fahrzeuge sowie Identifikation und Beseitigung von Mängeln. Zur sicherheitsrelevanten Verwaltung der Sachanlagen zählt ebenfalls der Austausch von wesentlichen Informationen mit externen Instandhaltungseinrichtungen sowie deren Überprüfung.

A1.5 Auftragnehmer, Partner und Zulieferer

Das fiktive EVU verfügt über ein zweckmäßiges Lieferantenmanagement. Dieses regelt die Prüfung von und den Umgang mit ausgelagerten Tätigkeiten im Sinne von [SMS18] sowie dazugehörige Vertragsbedingungen. Somit lassen sich Ergebnisse von externen Instandhaltungseinrichtungen, Leasingunternehmen, Personaldienstleistern, Ausbildungsträgern und externen Logistikunternehmen als ordnungsgemäß und risikofrei ansehen. Es finden Interaktionen mit Auftragnehmern, Partnern und Zulieferern in der Systemdefinition (als Schnittstelle zu interagierenden Systemen) einschließlich regelmäßiger Kontrollen Berücksichtigung.

A1.6 Änderungsmanagement

Bei Anpassungen von Vorgängen im fiktiven Unternehmen erfolgt eine Inspektion des SMS einschließlich entsprechender Handlungsanweisungen und derer Realisierung. Hierzu gehört auch eine selbstgesteuerte Signifikanzprüfung der Änderung mit einem einhergehenden Risikomanagementverfahren gemäß [CSM15] bei signifikanten betrieblichen, organisatorischen und technischen Änderungen.

A1.7 Notfallmanagement

Die Wiederherstellung des Regelbetriebs ist im Eisenbahnsystem neben dem Schutz von Mensch und Umwelt eines der bedeutendsten Ziele bei Störungen und insbesondere bei Notfällen. Im Rahmen des SMS werden detaillierte Maßnahmen und Aktionspläne ausgearbeitet. Diese dokumentieren Handlungsanweisungen für definierte Störungen und deren ausführende Mitarbeiter mit ihren Zuständigkeiten und Befugnissen. Das Notfallmanagement wird im Einklang mit der TSI OPE [TSI19] aufgestellt.

A2 Sicherheitsrelevanz- und Signifikanzprüfung

Vor der Durchführung des Risikomanagementverfahrens gemäß CSM-Verordnung muss die Sicherheitsrelevanz und Signifikanz der betrachteten Änderung überprüft werden.

Im Folgenden soll die Bewertung der Sicherheitsrelevanz und Signifikanz der vorgeschlagenen Änderung (erstmaliger Betrieb von Eisenbahnverkehr in Deutschland) durch das fiktive EVU erfolgen. Der zugrunde gelegte Untersuchungsgegenstand entspricht dabei dem (vorläufigen) System, welches in Kapitel 3 beschrieben wird.

Im Rahmen einer forschungsbegleitenden, nicht repräsentativen Umfrage (vgl. [CKB20]) konnte identifiziert werden, dass verschiedene Methoden zur Sicherheitsrelevanz- und Signifikanzprüfung bei realen EVU angewandt werden. Diese Methoden sind gemäß Umfrage jedoch nicht immer selbsterklärend, unproblematisch oder einfach umzusetzen. Das Forschungsprojekt soll daher eine weitere Möglichkeit anbieten, wie Experten zu einer fundierten Entscheidung bezüglich. der Sicherheitsrelevanz und Signifikanz für eine zu bewertende Änderung kommen können.

Die hier vorgestellte Prüfung stellt lediglich ein eigenes Verfahren zur Prüfung der in der CSM-Verordnung definierten Kriterien zur „Expertenbewertung über die Signifikanz der Änderung“ [CSM15] vor. Alternative definierte Verfahren können zur Sicherheitsrelevanz- und Signifikanzprüfung gleichermaßen angewandt werden.

A2.1 Sicherheitsrelevanzprüfung

Bei der Sicherheitsrelevanzprüfung wird ermittelt, ob sich die betrachtete Modifikation ungünstig auswirken kann und dadurch die Sicherheit des Systems vermindern kann. Zur Verdeutlichung seien die nachfolgenden Beispiele (Tabelle A.12) genannt.

Beim Bewertungsgegenstand entsprechend der vorläufigen Systemdefinition kann im ungünstigen Fall die Sicherheit des Gesamtsystems beeinträchtigt sein. Es können Passagiere der eigenen Züge, Passagiere von anderen EVU und Personen im Umfeld der befahrenen Eisenbahnstrecken gefährdet werden.

TABELLE A.12: BEISPIELE FÜR SICHERHEITSRELEVANTE ÄNDERUNGEN

Beispiel	**Sicherheitsrelevanz**
Farbgebung der Sitzbezüge im Personenwagen	nicht sicherheitsrelevant
Umrüstung der Tritthöhe an Personenwagen	sicherheitsrelevant, da es die Sicherheit von Passagieren am Bahnsteig gefährden kann

A2.2 Signifikanzprüfung

A2.2.1 Schritt 1: Einschätzung der zu bewertenden Änderung

Die nachfolgend dargestellten Ausführungen dienen zur Beurteilung der Auswirkungen der Änderung auf das Eisenbahnsystem mittels der in [CSM15] definierten Kriterien. Hierfür werden die Signifikanzkriterien durch Experten eingeschätzt und anschließend einer quantitativen Bewertung zugeordnet. Die Kennzeichnung der jeweils zutreffenden Einschätzung erfolgt in den Tabellen A.13, A.14, A.15, A.16 und A.17 stets mit einem Kreuz in der Spalte *Auswahl*. Zudem wird die Auswahl entsprechend verbal begründet. So kann eine fundierte Entscheidungsgrundlage nachgewiesen werden.

A2.2.2 Bewertung der Folgen von Ausfällen

Kriterium: „Folgen von Ausfällen: Szenario des ungünstigsten anzunehmenden Falls (‚credible worst-case scenario') bei einem Ausfall des zu bewertenden Systems unter Berücksichtigung etwaiger außerhalb des zu bewertenden Systems bestehender Sicherheitsvorkehrungen" [CSM15].

TABELLE A.13: ABSCHÄTZUNG DER AUSFALLFOLGEN

Punkte	Ausfallfolgen	Beschreibung	Auswahl (X)
1	sehr gering	Es sind einzelne Personen betroffen. Es können lediglich leichte Verletzungen auftreten.	
2	gering	Es sind wenige Personen betroffen. Es können schwere Verletzungen auftreten.	
3	hoch	Es können viele Personen schwere Verletzungen erleiden oder einzelne Personen durch den Ausfall getötet werden.	
4	katastrophal	Es können viele Personen getötet werden.	**X**

Begründung für die Auswahl (**4 Punkte**):

Es sind zum einen Güterzüge betroffen, die mit einer Geschwindigkeit von mehr als 50 km/h mit einem anderen Eisenbahnfahrzeug zusammenstoßen können. Zum anderen sind Personenverkehrszüge betroffen, die bei hohen Geschwindigkeiten entgleisen können bzw. bei denen im Falle eines Zusammenstoßes mit anderen Eisenbahnfahrzeugen viele Personen getötet werden können.

Bewertung der Innovation

Kriterium: „innovative Elemente bei der Einführung der Änderung; dabei geht es nicht nur darum, ob es sich um eine Innovation für den Eisenbahnsektor als Ganzes handelt, sondern auch darum, ob es sich aus der Sicht der Organisation, die die Änderung durchführt, um eine Innovation handelt" [CSM15].

Eine Änderung, wie z. B. der Einsatz eines Fahrzeugtyps, kann demnach für ein EVU innovativ sein, da es keine Erfahrungen mit dem speziellen Fahrzeugtyp aufweist, während der Fahrzeugtyp bei anderen EVU bereits im Einsatz und anerkannt ist. Die Bewertung der Innovation ist stets eine individuelle Entscheidung für das einzelne EVU.

TABELLE A.14: ABSCHÄTZUNG DES INNOVATIONSGRADS

Punkte	Innovations-grad	Beschreibung	Auswahl (X)
0	gering	Die Änderung enthält keine oder nur wenige neue Elemente.	
1	hoch	Die Änderung enthält überwiegend neue Elemente.	**X**

Begründung für die Auswahl **1 Punkt**:

Die bestehenden Vorgaben von deutschen Regelwerken und Vorschriften finden für das fiktive EVU erstmalig Anwendung. Für die gesamten Prozesse liegen zum aktuellen Zeitpunkt keine Erfahrungswerte vor. Es bleibt deshalb ein hoher Innovationsgrad für die betrachtete Änderung festzuhalten. Gleichwohl stellt die Anwendung der Regelwerke und Vorschriften bei etablierten EVU keine Innovation dar.

Bewertung der Komplexität

Kriterium: Änderungsumfang und -auswirkungen

TABELLE A.15: ABSCHÄTZUNG DER KOMPLEXITÄT

Punkte	Komplexität	Beschreibung	Auswahl (X)
0	gering	Es werden keine oder nur wenige Element geändert oder hinzugefügt. Die Änderung bezieht sich auf ein einzelnes Element oder ein einzelnes Teilsystem mit wenigen betroffenen Schnittstellen bzw. Abhängigkeiten zu Nachbarsystemen.	
1	hoch	Es werden mehrere Elemente geändert oder hinzugefügt. Die Änderung bezieht sich auf mehrere Elemente oder ein oder mehrere Teilsysteme mit vielen betroffenen Schnittstellen bzw. Abhängigkeiten zu Nachbarsystemen.	**X**

Begründung für die Auswahl **1 Punkt**:

Es handelt sich bei der Änderung um die Aufnahme von Schienenpersonenverkehr (SPV) und Schienengüterverkehr (SGV) durch das fiktive EVU in Deutschland. Die Durchführung von Eisenbahnverkehr ist ein vielschichtiges Tätigkeitsgebiet, bei dem zahlreiche Schnittstellen zu anderen Teil- und Nachbarsystemen bestehen. Es ist daher gerechtfertigt die Komplexität der Änderung für das fiktive EVU als hoch einzustufen.

Bewertung der Überwachbarkeit

Kriterium: „Überwachung: Unmöglichkeit, die eingeführte Änderung über den gesamten Lebenszyklus des Systems hinweg zu überwachen und in geeigneter Weise einzugreifen“ [CSM15].

TABELLE A.16: ABSCHÄTZUNG DER ÜBERWACHBARKEIT

Punkte	Überwach-barkeit	Beschreibung	Auswahl (X)
0	hoch	Es besteht eine hohe Überwachbarkeit. Fehler des Systems werden mittelbar oder unmittelbar offenbart. Fail-safe-Systeme gehen im Fehlerfall in einen sicheren Zustand über. Dazu bedarf es einer inhärenten Fehleroffenbarung. Durch periodisch wiederkehrende oder prädiktive Instandhaltungsmaßnahmen wird die Sicherheit des Systems aufrechterhalten.	**X**
1	gering	Die Überwachbarkeit ist gering. Es sind Teilaspekte der Änderung nicht unmittelbar überwachbar. Eine Fehleroffenbarung ist nicht oder nur durch periodisch wiederkehrende Instandhaltungsmaßnahmen möglich.	

Begründung für die Auswahl **0 Punkte**:

Bei der Durchführung von Eisenbahnverkehr in Deutschland erfolgt eine Überwachung in Form von Dispositions-, Leit- und Sicherungssystemen (hier als interagierende Systeme definiert). Die Disposition gewährleistet eine fortlaufende Überwachung mit definierten und kontrollierten Prozessen. Darüber hinaus wurde im fiktiven EVU ein effektives SMS eingeführt. Daher kann davon ausgegangen werden, dass die Überwachbarkeit der Prozesse zur Durchführung des Eisenbahnverkehrs vorhanden ist.

Bewertung der Umkehrbarkeit

Kriterium: „Umkehrbarkeit: Unmöglichkeit, zu dem vor Einführung der Änderung bestehenden System zurückzukehren“ [CSM15].

TABELLE A.17: ABSCHÄTZUNG DER UMKEHRBARKEIT

Punkte	Umkehr-barkeit	Beschreibung	Auswahl (X)
0	leicht	Das System kann in den Zustand vor Einführung der Änderung zurückgeführt werden.	**X**
1	schwer	Das System kann nicht in den Zustand vor Einführung der Änderung zurückgeführt werden.	

Begründung für die Auswahl **0 Punkte**:

Es handelt sich um die Durchführung von Eisenbahnverkehr in Deutschland durch das fiktive EVU. Die Umkehrbarkeit der betrachtungsgegenständlichen Änderung ist gegeben, indem das EVU den Betrieb einstellen kann. Aufgrund der für das fiktive EVU angenommenen Randbedingungen kann diese Einschätzung für real existierende EVU abweichen.

A2.2.3 Zwischenergebnis aus Schritt 1

Das Zwischenergebnis aus den vorangegangenen Bewertungen ergibt sich aus einer qualifizierten Expertenschätzung. Hierfür wird die folgende Matrix (Tabelle A.18) zugrunde gelegt:

- Entlang der Abszisse (x-Achse) werden die Punkte aus der Bewertung der Folge von Ausfällen abgetragen (Ergebnis des Abschnitts 2.2.1.1).
- Entlang der Ordinate (y-Achse) wird die Summe aller Punkte aus der Bewertung der Vorhersehbarkeit der Ausfallfolgenbeherrschung, d. h.
  - Innovation,
  - Komplexität der Änderung,
  - Überwachbarkeit,
  - Umkehrbarkeit,

  abgetragen (Ergebnisse der Abschnitte 2.2.1.2 bis 2.2.1.5).

TABELLE A.18: MATRIX ZUR SIGNIFIKANZBEWERTUNG

Summe aller Punkte der Abschnitte 2.2.1.2 bis 2.2.1.5					
	4	E	S	S	S
	3	N	E	S	S
	2	N	N	E	S
	1	N	N	N	E
	0	N	N	N	N
		1	**2**	**3**	**4**
		Punkte aus Abschnitt 2.2.1.1			

Am Schnittpunkt von Abszissenwert und Ordinatenwert ergibt sich ein Vorschlag für die Signifikanzbewertung wie folgt:

- S: Die Änderung ist signifikant.
- N: Die Änderung ist nicht signifikant.
- E: Es ist eine Ermessensfrage, ob die Änderung als signifikant oder nicht signifikant eingestuft wird.

Somit sind die Bewertung der Ausfallfolgen einerseits und die Vorhersehbarkeit der Ausfallfolgenbeherrschung in eine angemessene Korrelation gesetzt.

Sicherheitliches Ermessen ist ein in Risiko- und Sicherheitsbetrachtungen gängiges Mittel in Bereichen, wo keine relevanten Grundsätze Anwendung finden können. Konkret ist sicherheitliches Ermessen gemäß Verwaltungsvorschrift Neue Typzulassung „die Beurteilung, ob die Sicherheit gewährleistet ist, wenn anerkannte Regeln der Technik für den zu bewertenden Fall nicht vorliegen oder davon abgewichen werden soll“ [NTZ16]. Da keine notifizierte nationale Vorschrift zur Bewertung der Signifikanzkriterien vorliegt,

kann dieses Mittel bei der Signifikanzprüfung zur Anwendung kommen. Es dient den Experten dazu, eine fundierte Grundlage zur Bewertung der Änderung zu finden. Zusätzliche Kriterien, die nicht in [CSM15] definiert sind, können hiermit berücksichtigt werden, sofern nicht direkt klar ist, dass eine Änderung signifikant oder nicht signifikant ist (Tabelle A.19). Eine Begründung der Expertenentscheidung ist in diesem Fall jedoch zwingend notwendig.

Ergebnis für den betrachtungsgegenständlichen Sachverhalt

Die Ergebnisse der betrachteten Sachverhalte sind in den Tabellen A.19 und A.20 dargestellt.

TABELLE A.19: ZWISCHENERGEBNIS DER SIGNIFIKANZPRÜFUNG

Achse	Kriterium	Punkte
x-Achse	**2.2.1.1 Folgen von Ausfällen**	**4**
	2.2.1.2 Innovation	1
	2.2.1.3 Komplexität	1
	2.2.1.4 Überwachbarkeit	0
	2.2.1.5 Umkehrbarkeit	0
Y-Achse	**Summe 2.2.1.2 bis 2.2.1.5**	**2**

TABELLE A.20: ERGEBNIS DER SIGNIFIKANZPRÜFUNG – SCHRITT 1

Summe aller Punkte der Abschnitte 2.2.1.2 bis 2.2.1.5					
	4				
	3				
	2				X
	1				
	0				
		1	**2**	**3**	**4**
		Punkte aus Abschnitt 2.2.1.1			

Fazit:

Die Änderung ist **signifikant**.

A2.2.4 Schritt 2: Berücksichtigung des Zusammenwirkens mit vorangegangenen Änderungen

Kriterium: „Additive Wirkung: Bewertung der Signifikanz der Änderung unter Berücksichtigung aller sicherheitsrelevanten Änderungen des zu bewertenden Systems, die in jüngster Zeit vorgenommen und nicht als signifikant beurteilt wurden“ [CSM15].

Hat es bereits früher Änderungen am System im Rahmen des betrachteten Sachverhalts gegeben, die als sicherheitsrelevant aber nicht signifikant eingestuft worden sind, so kann sich in der Gesamtbetrachtung mit der hier bewerteten Änderung eine Signifikanz ergeben.

Ergebnis für den betrachtungsgegenständlichen Sachverhalt:

Aufgrund der bereits identifizierten Signifikanz der Änderung (siehe Tabelle A.20) werden weitere, frühere Änderungen am System nicht betrachtet.

A2.2.5 Ergebnis der Signifikanzprüfung

Das Ergebnis der Signifikanzprüfung ist in Tabelle A.21 wiedergegeben.

TABELLE A.21: ERGEBNIS DER SIGNIFIKANZPRÜFUNG

Ist die Änderung sicherheitsrelevant? (siehe Abschnitt 2.1)	
☐ **Nein:** Das Risikomanagementverfahren gemäß [CSM15] ist nicht anzuwenden. *Bewertung abgeschlossen*	☒ **Ja:** Fortsetzung der Betrachtung. *weiter mit Signifikanzprüfung*
Ist die Änderung signifikant? (siehe Abschnitt 2.2.2 und 2.2.3)	
☐ **Nein:** Das Risikomanagementverfahren gemäß [CSM15] ist nicht anzuwenden. *Bewertung abgeschlossen*	☒ **Ja:** Es ist das Risikomanagementverfahren gemäß [CSM15] durchzuführen. *weiter mit Risikomanagementverfahren*

A3 Produktorientierte Systemdefinition im fiktiven EVU

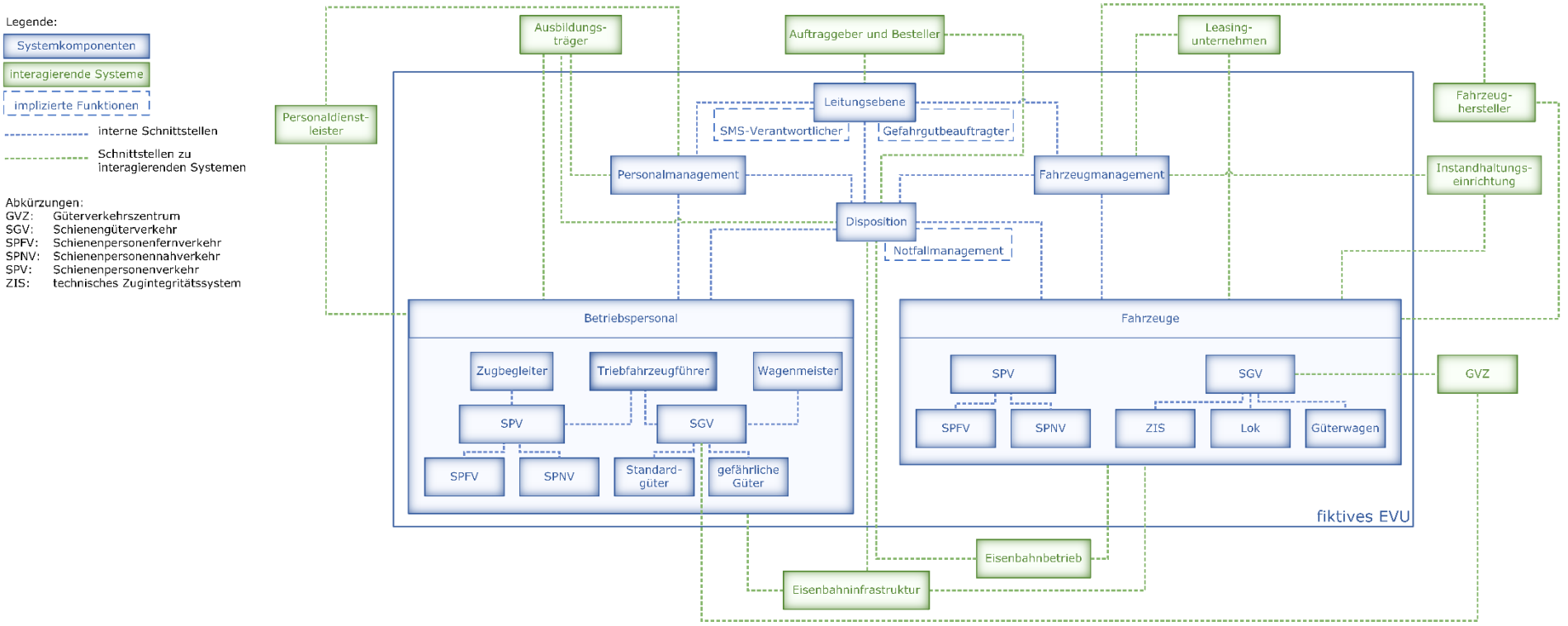


Abbildung A.25: Produktorientierte Systemdefinition, Teilsystem „Verkehrsbetrieb und Verkehrssteuerung“

A3.1 Leitungsebene

Die Leitungsebene ist die oberste Führungs- und Managementebene und beaufsichtigt alle untergeordneten Managementbereiche. Zu den sicherheitsrelevanten Aufgaben der Leitungsebene zählen:

- Vorgabe aller grundlegenden Anforderungen im SMS,
- Überwachung der
  - Eignung,
  - Wirksamkeit und
  - Einhaltung der definierten Verfahren, Methoden und praktischen Anwendungen im SMS,
- Organisation und Überwachung von untergeordneten Managementbereichen (z. B. Fahrzeug- und Personalmanagement).

Zusammenfassend verantwortet die Leitungsebene die Kontrolle der unterschiedlichen Ebenen des fiktiven EVU gemäß [SMS18].

Überdies ist der Leitungsebene die Funktion des Gefahrgutbeauftragten zugeordnet. Dieser überwacht die Einhaltung der Gefahrgutvorschriften (vgl. [GGB19], [RID21], [GGV21]).

A3.2 Fahrzeugmanagement

Die Aufgabe des Fahrzeugmanagements besteht darin, Fahrzeuge (Triebwagen, Triebzüge, Lokomotiven, Güterwagen) in einer ausreichenden Menge und Qualität zur Verfügung zu stellen, damit der sichere und fahrplanmäßige Eisenbahnbetrieb gewährleistet ist.

Über die eigens zu erbringende „Managementfunktion zur Beaufsichtigung und Koordinierung der [weiteren] Instandhaltungsfunktionen und zur Gewährleistung des sicheren Zustands des Fahrzeugs im Eisenbahnsystem“ [EU798] überwacht das Fahrzeugmanagement in gleichem Maße, wie es relevante Informationen mit der für die Instandhaltung zuständigen Stellen austauscht. Das Fahrzeugmanagement ist daher für das Sachanlagen- und Lieferantenmanagement (Verwaltung von Sachanlagen sowie Umgang mit Auftragnehmer, Partner und Zulieferer hinsichtlich der Fahrzeuge) zuständig.

Überdies ist das Fahrzeugmanagement dafür verantwortlich, dass die Fahrzeuge allein für ihren bestimmungsgemäßen Gebrauch eingesetzt werden. Hierfür existieren interne Richtlinien, welche bei der Disposition beachtet werden müssen und sich im SMS-Prozess *Betriebsplanung und -steuerung* wiederfinden.

A3.3 Personalmanagement

Das Personalmanagement verantwortet im Sinne des hier vorliegenden Betrachtungsbereichs insbesondere Beschäftigte, die an der Durchführung des Eisenbahnbetriebs beteiligt sind. Hierzu zählen das Betriebspersonal und die Disponenten. Unter den Zuständigkeitsbereich des Personalmanagements fallen auch alle weiteren Beschäftigte in den Bereichen Verwaltung, Management, Administration etc. des fiktiven EVU. Im Rahmen dieser Systemdefinition werden jedoch ausschließlich Berufsgruppen einbezogen, welche unmittelbar am Eisenbahnbetrieb beteiligt sind und somit einen direkten Einfluss auf die Sicherheit des Eisenbahnsystems haben.

Aufgabe des Personalmanagements ist es, die SMS-Prozesse u. a. im Bereich *Unterstützung* anzuwenden. Das Personalmanagement bestimmt den Personalbedarf und akquiriert ggf. neues Personal. Weiterhin muss das Personalmanagement die Kompetenzen der Beschäftigten des fiktiven EVU sicherstellen sowie überwachen und Schulungsprogramme für die jeweiligen Aufgaben durchführen. Die notwendigen Qualifikationen für die einzelnen Positionen werden vom Personalmanagement in Zusammenarbeit mit der Leitungsebene definiert (SMS-Prozesse *organisatorische Aufgaben, Zuständigkeiten, Rechenschaftspflichten und Befugnisse* und *Kompetenz*).

A3.4 Disposition

Die Disposition plant den Eisenbahnbetrieb in Abstimmung mit den Auftraggebern bzw. Leistungsbestellern und der übergeordneten Disposition des Eisenbahninfrastrukturbetreibers (SMS-Prozesse des Bereichs *Betrieb*, insbesondere *Betriebsplanung und -steuerung*). Die Disposition legt somit fest, welches Betriebspersonal mit welchen Fahrzeugen welche Leistungen erbringt und wie die Beförderungs- bzw. Transportleistungen detailliert erbracht werden.

Des Weiteren ist die Disposition dafür zuständig, die Instandhaltungstätigkeiten an den Fahrzeugen in den fahrplanmäßigen Betrieb des fiktiven EVU zu integrieren. Hierzu erfolgt eine Interaktion mit dem Fahrzeugmanagement

Zur Disposition gehört ebenfalls das Notfallmanagement. Dieses kommt insbesondere dann zum Tragen, wenn sich betriebshemmende Zustände einstellen oder technische Störungen ereignen. Ziel des Notfallmanagements ist es, den sicheren Betrieb in den genannten Fällen aufrechtzuhalten und den Betrieb möglichst schnell wieder in seinen ordnungsgemäßen Regelzustand zu führen. Hierfür existieren entsprechend des SMS konkrete Einsatz-, Alarm- und Informationspläne mit den jeweiligen Aufgaben und Zuständigkeiten.

A3.5 Betriebspersonal

A3.5.1 Triebfahrzeugführer

Triebfahrzeugführer sind für die sichere Durchführung der Zugfahrten verantwortlich. Im fiktiven EVU gibt es vier Gruppen von Triebfahrzeugführern je nach Einsatzbereich:

- Triebfahrzeugführer im SPNV,
- Triebfahrzeugführer im SPFV,
- Triebfahrzeugführer im SGV mit Standardgütern sowie
- Triebfahrzeugführer im SGV mit gefährlichen Gütern.

Triebfahrzeugführer müssen ihre Eignung entsprechend der Triebfahrzeugführerscheinverordnung [TfV19] nachweisen. Das im SMS enthaltene *Kompetenzmanagement* sorgt dafür, dass Kenntnisse, Fertigkeiten, Erfahrungen und nachzuweisende Qualifikationen entsprechend dem Betriebsaufgabenprofil definiert und überprüft werden.

A3.5.2 Zugbegleiter

Zugbeleiter, denen vielfältige Aufgaben zugeordnet sind, kommen im fiktiven EVU ausschließlich im SPV zum Einsatz. Sie sollen die aktive Betreuung der Fahrgäste vor, während und nach der Fahrt sicherstellen.

Die Rolle des Zugbegleiters kann sicherheitsrelevante Aufgaben beinhalten. Im SPFV übernimmt der Zugbegleiter die Aufgaben des Zugführers. Im SPNV übernimmt der Triebfahrzeugführer die Aufgaben des Zugführers.

Darüber hinaus sind Zugbegleiter im gesamten SPV für den sicheren Ablauf bei etwaigen Betriebsstörungen (z. B. bei Störungen am Fahrzeug) verantwortlich.

A3.5.3 Wagenmeister

Wagenmeister übernehmen im fiktiven EVU spezielle Aufgaben zur Gewährleistung der Betriebssicherheit und Verkehrstauglichkeit der Fahrzeuge im SGV.

A3.6 Fahrzeuge

Das fiktive EVU betreibt ausschließlich zugelassene Fahrzeuge. Somit ist sichergestellt, dass die Fahrzeuge den notwendigen Anforderungen an die Sicherheit im deutschen Eisenbahnverkehr genügen. Das fiktive EVU kann selbst der Halter der Fahrzeuge sein oder diese über Leasingunternehmen anmieten.

A3.6.1 Personenverkehr

Im SPV setzt das fiktive EVU ausschließlich Triebwagen mit einem technikbasierten Abfertigungsverfahren (TAV) ein. Die Triebwagen (SPNV) bzw. Triebzüge (SPFV) verfügen jeweils über alle für den vorgesehenen Betrieb notwendigen sicherungstechnischen Einrichtungen und können zusammengekuppelt werden, sofern die Baureihen kompatibel sind. In Mehrfachtraktion verkehrende Triebwagen bzw. Triebzüge werden in den folgenden Abschnitten als Triebwagenverband bezeichnet.

A3.6.2 Güterverkehr

Im SGV wird ein Güterzug stets aus einer Lokomotive und mehreren gekuppelten Güterwagen gebildet.

Die eingesetzten Lokomotiven verfügen über alle für den vorgesehenen Betrieb notwendigen sicherungstechnischen Einrichtungen.

Als Güterwagen kommen im fiktiven EVU diverse Gattungen zum Einsatz. Zudem unterhält das fiktive EVU Kesselwagen und Tragwagen für Tankcontainer. Diese werden ausschließlich für den Gefahrguttransport gemäß den rechtlichen Vorgaben (siehe [GGB19], [RID21], [GGV21]) eingesetzt.

A3.7 Technisches Zugintegritätssystem für Güterzüge

Das fiktive EVU setzt ein neuartiges System zur technischen Zugintegritätsidentifikation von Güterzügen ein. Dieses System soll neben der originären Aufgabe der Feststellung der Zugintegrität eines Güterzugs auch Ladungsverlust während der Zugfahrt detektieren und dem Triebfahrzeugführer mitteilen.

Das innovative technische Zugintegritätssystem (ZIS) ist ein rein hypothetisches System, welches allein aus dem Grund der Anwendung der expliziten Risikoabschätzung und -evaluierung nach [CSM15] im fik-

tiven EVU Anwendung findet. Intention des Einsatzes dieses neuartigen, in der Realität noch nicht eingesetzten Systems liegt ausschließlich in der Veranschaulichung des methodischen Vorgehens der Anwendung dieses Risikoakzeptanzgrundsatzes. Aus diesem Grund wird die Beschreibung der Komponenten und Funktionsweise des elektronischen Systems nur insoweit detailliert dargestellt, dass die explizite Risikoabschätzung und -evaluierung ermöglicht wird. Im Risikomanagementverfahren eines realen EVU müsste die Systemdefinition hingegen wesentlich umfangreicher gestaltet sein.

Es sei hierbei angemerkt, dass die Einführung eines solchen neuartigen Systems selbst schon eine eigenständige Änderung darstellt, welche ein autarkes Risikomanagementverfahren hervorruft.

Das ZIS basiert auf der fortdauernden Identifikation des Gesamtgewichtes des Zuges (vgl. [WIN18]). Neben der originären Aufgabe der Feststellung der Zugintegrität eines Güterzugs soll das System auch Ladungsverlust während der Zugfahrt detektieren und dem Triebfahrzeugführer melden. Dazu besteht das System aus den in Abbildung A.26 grün dargestellten Komponenten.

Abbildung A.26: Schematische Darstellung des ZIS

Jeder Güterwagen des fiktiven EVU verfügt über einen Beladungssensor, der die Zuladung des Güterwagens kontinuierlich misst. Über die von allen Beladungssensoren übertragenen Daten von Eigengewicht und Zuladung ermittelt die Auswerteeinheit kontinuierlich die Gesamtmasse des Güterzugs. Das ZIS gibt eine Warnmeldung an den Triebfahrzeugführer über eine Anzeige aus, sofern während der Fahrt eine Reduktion des Gewichts über einen definierten Schwellwert identifiziert wird. Dies kann beispielsweise durch Zugtrennung oder Ladungsverlust verursacht sein.

A3.8 Interagierende Systeme und deren Schnittstellen

Die folgende Beschreibung einzelner interagierender Systeme und deren Schnittstellen zum betrachteten System „Verkehrsbetrieb und Verkehrssteuerung“ des fiktiven EVU dient einzig zur Charakterisierung der Randbedingungen und Interaktionen von Systembestandteilen mit den interagierenden Systemen. Detaillierte Interaktionen zwischen Komponenten des fiktiven EVU und interagierenden Systemen können den Prozessbeschreibungen im Anhang 4 entnommen werden.

A3.8.1 Auftraggeber und Besteller

Das fiktive EVU führt planmäßige Zugfahrten ausschließlich im Auftrag von Dritten durch. Hierzu werden von diversen Auftraggebern und Bestellern zu erbringende Beförderungs- bzw. Transportleistungen im Sinne eines fahrplanmäßigen Angebots auf definierten Linien (im SPV) bzw. Touren (im SGV) vergeben.

A3.8.2 Instandhaltungseinrichtung

Das fiktive EVU ist die registrierte ECM (für die Instandhaltung zuständige Stelle – Entity in Charge of Maintenance) für die Fahrzeuge. Dabei werden die Instandhaltungsfunktionen

- Instandhaltungsentwicklung,
- Fuhrpark-Instandhaltungsmanagement und
- Instandhaltungserbringung

untervergeben und somit ausschließlich durch externe Instandhaltungseinrichtungen durchgeführt.

Es findet ein reger Informationsaustausch zwischen dem Fahrzeugmanagement des fiktiven EVU und der externen Instandhaltungseinrichtung statt. Die Instandhaltungsfunktionen erfolgen im Einklang mit der Durchführungsverordnung (EU) 2019/779 [ECM19].

Zur Auswahl und Überwachung der externen Instandhaltungseinrichtungen dient das Lieferantenmanagementsystem. Im Rahmen des Lieferantenmanagements werden die Risiken, welche aus den ausgelagerten Tätigkeiten resultieren können, kontrolliert.

A3.8.3 Eisenbahninfrastruktur

Der Begriff Eisenbahninfrastruktur beschreibt im Sinne dieser Systemdefinition alle durch Schienenfahrzeuge des fiktiven EVU befahrenen Gleise einschließlich der erforderlichen sicherungstechnischen Einrichtungen und sonstigen baulichen Anlagen. Zur Eisenbahninfrastruktur gehört ebenfalls der örtliche Bereich des jeweiligen GVZ einschließlich genutzter Abstellanlagen. Für die Unterhaltung der Eisenbahninfrastruktur sind externe Unternehmen (Infrastrukturbetreiber einschließlich ggf. beauftragter Dienstleister) zuständig. Auf Basis vertraglicher Beziehungen werden die Sicherheitsrisiken, welche sich aus der Eisenbahninfrastruktur ergeben, kontrolliert.

Die Bahnsicherungstechnik dient der Sicherung der Fahrzeugbewegungen von Eisenbahnfahrzeugen. Ausfälle der Bahnsicherungstechnik gehören nicht zum Betrachtungsgegenstand der Gefährdungsermittlung und -einstufung dieses Forschungsberichts.

Die Fahrzeuge des fiktiven EVU befahren die vorgesehenen Strecken im Netz der deutschen Eisenbahnen des Bundes (EdB). Lediglich Fahrzeuge, welche die notwendigen Eigenschaften (z. B. Ausrüstung mit spezieller Zugbeeinflussungseinrichtung, maximale Zuglänge, Radsatzlast) aufweisen, können eine bestimmte Strecke befahren. Es ist Aufgabe der Disposition, dafür zu sorgen, dass diese Randbedingungen bei den Zugfahrten des fiktiven EVU eingehalten werden.

Alle Fahrzeuge des fiktiven EVU werden, wenn sie sich nicht im Einsatz oder in der externen Instandhaltungseinrichtung befinden, in eine Abstellanlage verbracht. Im Rahmen des Projekts werden zur Vereinfachung der Abläufe und Beschreibungen gemäß Forschungsgegenstand sämtliche Nebengleise als Abstellanlagen bezeichnet.

A3.8.4 Eisenbahnbetrieb

Das fiktive EVU erbringt Verkehrsleistungen im deutschen Schienenverkehrsnetz, welches ebenfalls von weiteren Eisenbahnverkehrsunternehmen benutzt wird. Dementsprechend müssen Fahrzeugbewegungen anderer Schienenfahrzeuge und die übergeordnete Disposition des Infrastrukturbetreibers bei den Prozessen des fiktiven EVU berücksichtigt werden.

A3.8.5 Güterverkehrszentrum

Güterzugfahrten des fiktiven EVU verkehren ausschließlich zwischen Güterverkehrszentren. Im jeweiligen GVZ werden die Güterzüge be- und entladen sowie für die zu erbringenden Schienengüterverkehrsleistungen zusammengestellt. Die genannten Aufgaben fallen in den Zuständigkeitsbereich externer

Dienstleister, die damit beauftragt sind. Diese werden entsprechend des Lieferantenmanagements ausgewählt und überprüft. Somit ist sichergestellt, dass die mit ausgelagerten Tätigkeiten verbundenen Sicherheitsrisiken beherrscht werden.

A3.8.6 Ausbildungsträger

Sofern sich Schulungen nicht eigenständig im fiktiven EVU durchführen lassen, werden die erforderlichen Leistungen bei geeigneten Ausbildungsträgern eingekauft. Diese werden entsprechend des Lieferantenmanagements kontrolliert.

A3.8.7 Personaldienstleister

Personaldienstleister kommen zum Einsatz, wenn das fiktive EVU bestimmte Personale nicht selbst vorhält. Über eine Arbeitnehmerüberlassung stellt der Personaldienstleister entsprechend kompetente Personen zur Verfügung. Personaldienstleister selbst werden im Rahmen des SMS regelmäßig überprüft.

A3.8.8 Fahrzeughersteller

Sofern vom fiktiven EVU benötigte Schienenfahrzeuge käuflich erworben werden, erfolgt ein Direktbezug vom Hersteller.

A3.8.9 Leasingunternehmen

Sofern es für das EVU nicht zweckmäßig ist, die benötigten Schienenfahrzeuge käuflich zu erwerben, werden über externe Leasingunternehmen, die den Anforderungen des SMS des fiktiven EVU genügen, Fahrzeuge angemietet. In diesem Fall ist das Leasingunternehmen der Halter und als ECM vollumfänglich für die Instandhaltungsfunktionen zuständig.

A4 Prozessorientierte Systemdefinition im fiktiven EVU

Dieser Anhang umfasst die Charakterisierung der sicherheitsrelevanten Abläufe im fiktiven EVU und seinen interagierenden Systemen. Im Rahmen des Risikomanagements liegt der Fokus auf sicherheitsrelevanten Funktionsabläufen, sodass z. B. nicht alle Managementprozesse oder andere Verfahren, die gemäß [SMS18] definiert werden, in den Prozessdiagrammen wiedergegeben sind. Die Prozessablaufdiagramme enthalten die in Abbildung A.27 dargestellten Symbole, die anlassbezogen definiert werden.

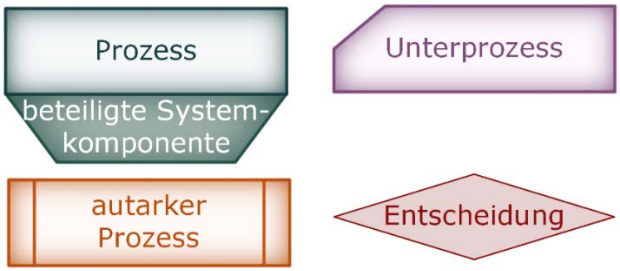


Abbildung A.27: Symbole der Prozessablaufdiagramme

Es sei an dieser Stelle nochmals darauf hingewiesen, dass die Systemdefinition des fiktiven EVU lediglich als Beispiel zur Durchführung des Risikomanagementverfahrens dienen soll. Entsprechend sind Prozesse der Übersichtlichkeit im Vergleich zu Prozessen realer EVU gekürzt oder abstrahiert. Weiterhin erfolgt in dieser initialen Charakterisierung noch keine abschließende Definition aller für die Gesamtbetrachtung erforderlichen Prozesse. Dies liegt darin begründet, dass verdeutlicht werden soll, welche sicherheitsrelevanten Vorteile das Verfahren aufweist. Darauf aufbauend können mittels der sich anschließenden Gefährdungsermittlung risikobehaftete Prozesse identifiziert und entsprechend angepasst werden.

A4.1 Einstellung von Personal

Der Prozess *Einstellung von Personal*, welches mit sicherheitsrelevanten Tätigkeiten im Bahnbetrieb betraut wird, steht im Mittelpunkt der nachfolgenden Ausführungen. Zu diesen Personalgruppen zählen das Betriebspersonal und Disponenten. Der Prozess zur Einstellung dieser Personalgruppen ist in Abbildung A.28 dargestellt. Für die Einstellung von neuem Personal ist das Personalmanagement zuständig. Die Bedarfserkennung steht dabei an erster Stelle. Dies kann z. B. dann der Fall sein, wenn zusätzliche Verkehrsleistungen erbracht werden sollen.

Nachdem der Bedarf identifiziert wird, erfolgt zunächst eine Definition der Anforderungen, welche an die neuen Beschäftigten gestellt werden. Diese dienen ebenfalls als Bewertungsgrundlage im Auswahlprozess. Basis für die Anforderungsdefinitionen sind die im Rahmen des Kompetenzmanagements für die jeweilige Berufsgruppe fest definierten Kenntnisse, Fertigkeiten, Erfahrungen und nachzuweisende Qualifikationen.

Grundsätzlich gibt es zwei verschiedene Möglichkeiten, um Personal an das fiktive EVU zu binden. Zum einen können sie sich in einem direkten Arbeitsverhältnis mit dem fiktiven EVU befinden (Unterprozess *Beschäftigung des Personals*). Zum anderen kann es bei einem Personaldienstleister angestellt sein und

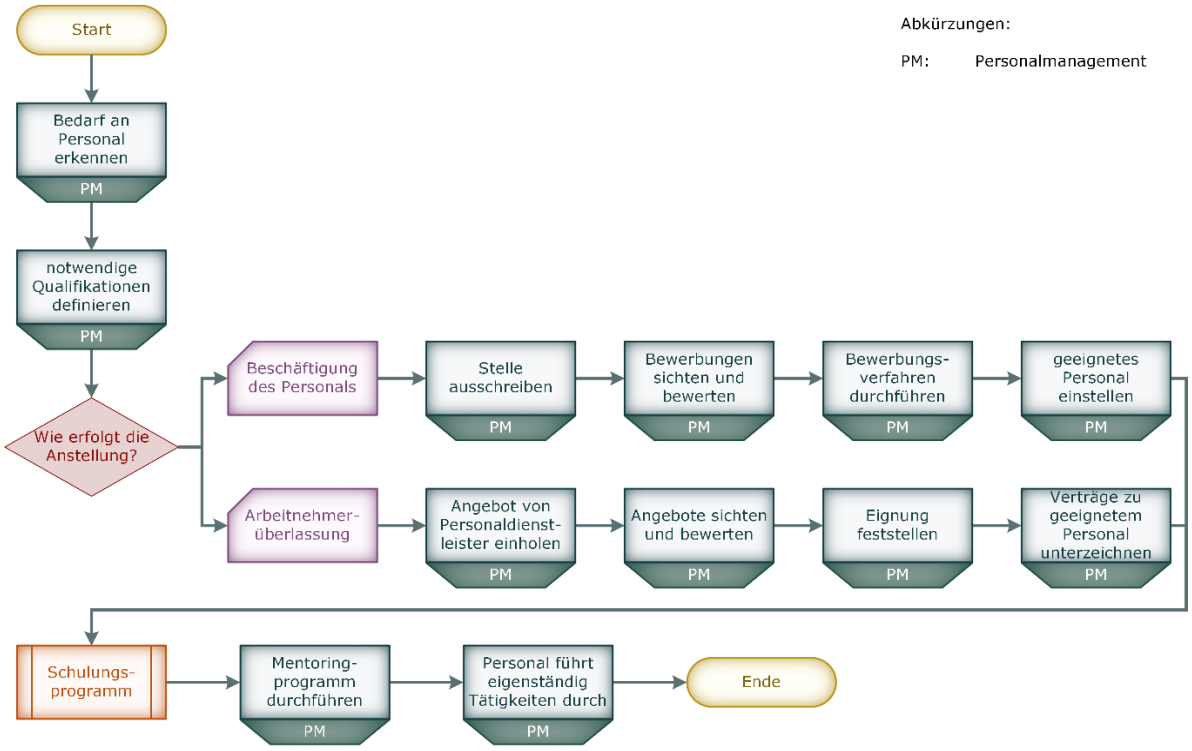


Abbildung A.28: Prozess: Einstellung von Personal

über eine Arbeitnehmerüberlassung Tätigkeiten beim fiktiven EVU ausüben. Lediglich Disponenten werden ausschließlich vom fiktiven EVU beschäftigt, sodass für diese Berufsgruppe der Unterprozess zur *Arbeitnehmerüberlassung* keine Gültigkeit besitzt.

A4.1.1 Beschäftigung des Personals

Die identifizierten Anforderungen an das gesuchte Personal werden in Stellenausschreibungen zusammengefasst. Wie diese organisiert werden sollen, ist nicht Gegenstand dieser Systemdefinition. Darauf eingehende Bewerbungen werden die gesichtet und hinsichtlich ihrer Eignung gemäß Kompetenzmanagement geprüft.

Qualifizierte Bewerbende werden in einem darauffolgenden Bewerbungsverfahren intensiv getestet. Dabei geht es u. a. um die Durchführung von Arbeitssimulationen und Leistungstests, um die angegebenen Kompetenzen bzgl. sicherheitsrelevanter Tätigkeiten der potenziellen Beschäftigten zu überprüfen. Zusätzlich werden in Bewerbungsgesprächen die Qualifikationen der Bewerber hinsichtlich ihrer Eignung für die zu besetzenden Stellen bewertet.

A4.1.2 Arbeitnehmerüberlassung

Soll oder kann das Personal nicht direkt beim fiktiven EVU angestellt sein, so werden die Qualifikationsanforderungen über ein Angebotsgesuch an externe Personaldienstleister übergeben. Diese Personaldienstleister sind entsprechend des Lieferantenmanagements ausgewählt und kontinuierlich überprüft, sodass sie geeignetes Personal anbieten können. Die eingehenden Angebote werden gesichtet und kritisch überprüft. Zusätzlich erfolgt bedarfsweise eine Überprüfung der potenziellen Kandidaten in ausgewählten Tests auf ihre tatsächliche Befähigung. Diese Eignungsfeststellung entspricht dabei nicht einem solchen Detaillierungsgrad wie beim Bewerbungsverfahren, da der Personaldienstleister für die Eignung

der Triebfahrzeugführer verantwortlich ist. Für einzelne Berufsgruppen, wie Triebfahrzeugführer, werden durch das fiktive EVU die Erfüllung der geforderten Fähigkeiten jedoch überprüft, um der Verantwortung bzgl. des sicheren Betriebs gerecht zu werden. Ist geeignetes Personal gefunden, werden entsprechende Verträge mit dem externen Personaldienstleister unterzeichnet.

A4.1.3 Schulungs- und Mentoringprogramm

Unabhängig vom Beschäftigungsverhältnis durchläuft das neue Personal zunächst ein Schulungsprogramm (siehe Abschnitt 4.2) sowie ein Mentoringprogramm.

Die Schulungsinhalte sind abhängig vom zukünftigen Einsatzgebiet der einzelnen Mitarbeitenden und werden im Rahmen des Kompetenzmanagements definiert.

Im Mentoringprogramm erfolgt ein direkter, berufsgruppenspezifischer Erfahrungs- und Wissenstransfer zwischen Bestandspersonal und Neupersonal. Neben vorwiegend theoretischen Grundlagen können so auch praktische Belange thematisiert werden. Damit lässt sich dafür sorgen, dass das neu zum Einsatz kommende Personal erst dann in eigenständiger Verantwortung tätig wird, wenn die dafür notwendigen Voraussetzungen in einem erforderlichen Maß vorhanden sind.

A4.2 Schulungsprogramm

Schulungsbedarf wird durch das Personalmanagement identifiziert. Hierzu ist ein effektives und praktikables *Kompetenzmanagement* eingeführt. Schulungen sind insbesondere dann notwendig, wenn neue Beschäftigte eingestellt werden oder dem Personal neue Funktionen und Aufgaben übertragen werden. Darüber hinaus besteht Bedarf an Weiterbildungen, sofern Defizite beim Personal identifiziert werden. Hierzu erfolgt eine regelmäßige Überwachung und Beurteilung des Personals durch das Personalmanagement. Weiterhin kann Schulungsbedarf aus sonstigen bevorstehenden Neuerungen und Weiterentwicklungen, z. B. der Einsatz neuer Triebfahrzeugbaureihen, resultieren. Mit Schulungen sollen Kenntnisse zu verschiedenen Punkten, wie

- Sicherheitsmanagement des fiktiven EVU,
- angewandte Betriebsverfahren insbesondere bei Störungen und Notfällen,
- technische Ausrüstungen der eingesetzten Fahrzeuge,

sichergestellt werden. Wird ein Bedarf an Weiterbildungen identifiziert, so entscheidet das Personalmanagement zunächst neben Schulungsinhalten und -umfängen darüber, auf welche Weise die Schulung durchführen werden soll.

Dabei lassen sich zwei grundsätzliche Varianten unterscheiden:

- interne Schulung durch geeignetes, kompetentes Personal oder
- Schulung durch externe Ausbildungsträger.

Abbildung A.29 stellt beide Weiterbildungsvarianten dar. Bei internen Schulungen werden zunächst qualifizierte und kompetente Beschäftigte ermittelt, die als Ausbilder und Ausbilderinnen fungieren können. Diese müssen fundierte und weitreichende Kenntnisse in dem zu schulenden Bereich nachweisen. Des Weiteren müssen sie ebenfalls didaktische Fähigkeiten besitzen, damit das zu vermittelnde Wissen den Schulungsteilnehmenden angemessen und zielführend weitergegeben werden kann. Anschließend wird das Schulungsprogramm determiniert und die bei der Schulungsdurchführung zum Einsatz kommenden Medien, z. B. Präsentationen und Weiterbildungsunterlagen, vorbereitet. Dies erfolgt durch den benannten Ausbilder in Zusammenarbeit mit dem Personalmanagement.

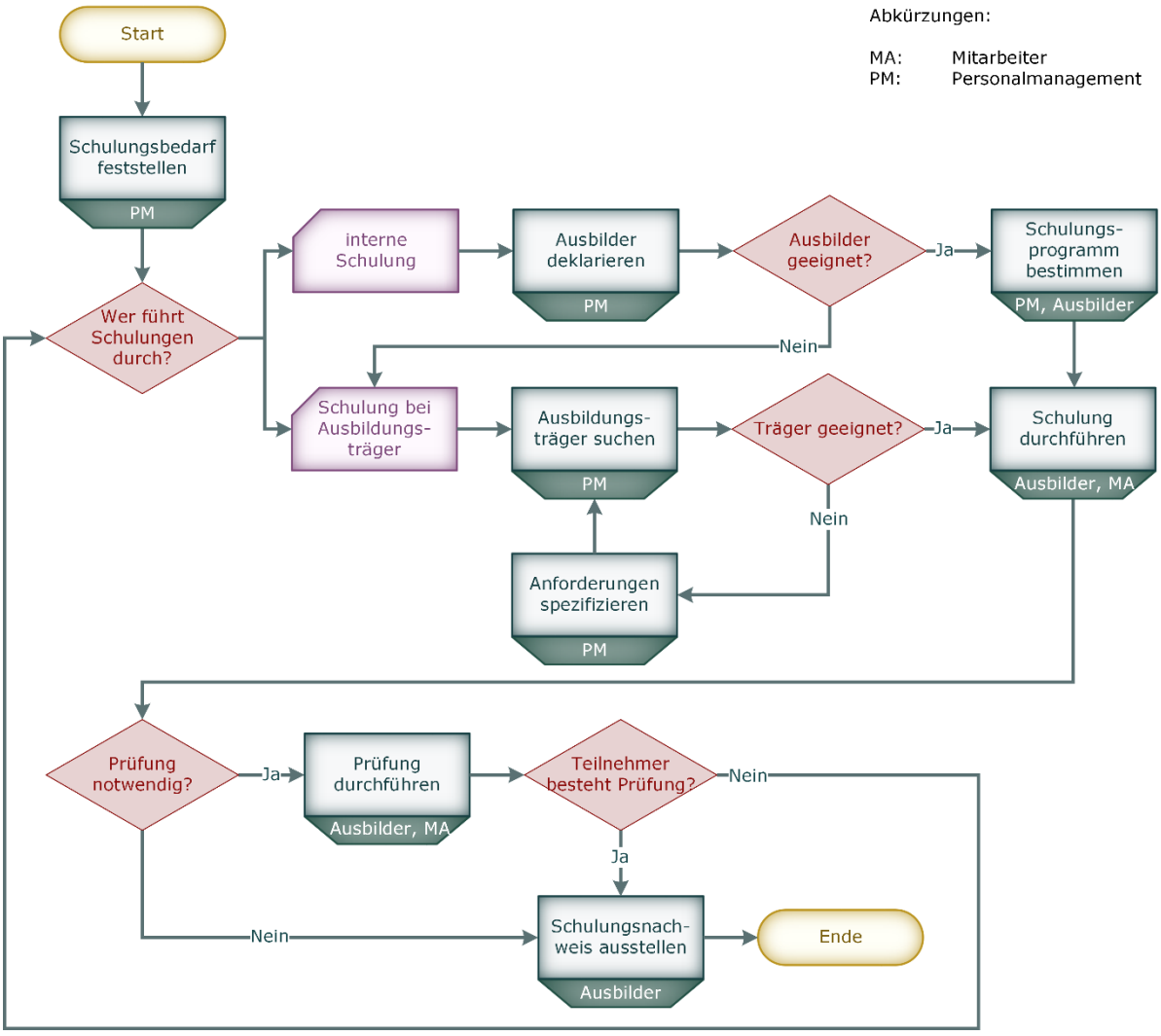


Abbildung A.29: Prozess: Schulungsprogramm

Sofern sich kein geeigneter interner Ausbilder finden lässt oder andere Motive dahinterstehen, wird ein geeigneter externer Ausbildungsträger engagiert. Hier werden die Prozesse des *Lieferantenmanagements* ebenfalls genutzt.

Die Weiterbildungsmaßnahme kann durchgeführt werden, sofern das Schulungsprogramm durch den internen Ausbilder definiert bzw. ein Programm bei einem externen Ausbildungsträger erschlossen ist. Bei einigen Weiterbildungen kann je nach Schulungskonzept eine abschließende Prüfung notwendig sein. Dabei gilt es zu kontrollieren, dass die Schulungsteilnehmenden zum Veranstaltungsende über das zu vermittelnde Wissen verfügen und dieses anwendungsorientiert einsetzen können. Insbesondere bei Triebfahrzeugführern sind solche Leistungsnachweise obligatorisch.

Sofern die Prüfung nicht bestanden wird, muss die Schulung wiederholt oder vertieft werden, um die Weiterbildungsziele zu erreichen. Bei einem erfolgreichen Abschlusstest sowie bei Schulungen, bei denen keine Prüfung erforderlich ist, wird als letzter Schritt der Schulungs-/Weiterbildungsnachweis ausgestellt. Dieser dient zur Nachweisführung für das Personalmanagement und den Beschäftigten selbst.

A4.3 Erwerb von Fahrzeugen

Identisch zu den Einstellungsprozessen, wird auch beim Erwerb von Fahrzeugen zunächst der Bedarf identifiziert. Hierfür ist das Fahrzeugmanagement in Zusammenarbeit mit der Leitungsebene und der Disposition verantwortlich. Dies gilt alle Fahrzeuge nach Abschnitt A3.6 in Anhang 3. Abbildung A.30 stellt den Prozess dar.

In Zusammenarbeit von Fahrzeugmanagement und Disposition gilt es, Anforderungen an die zu beschaffenden Fahrzeuge zu definieren. Diese richten sich bei Triebwagen im SPNV unter den aktuell gegebenen Rahmenbedingungen mehrheitlich nach dem jeweiligen Anforderungsprofil, das vom Aufgabenträger bzw. Leistungsbesteller des SPNV-Vergabeverfahren vorgegeben ist. Dazu gehören vor allem ausgeschriebene Fahrzeugkonzepte bzw. anderweitige Randbedingungen, z. B. durch die vorgesehenen zu befahrenen Strecken definierte Eigenschaften. Bei Triebzügen im SPFV gelten für das fiktive EVU vergleichbare Anforderungen. Hierbei sei darauf hingewiesen, dass dies von der üblichen Praxis abweicht. Für Lokomotiven und Güterzüge im SGV werden die Anforderungsspezifikationen ausschließlich vom fiktiven EVU bestimmt, wobei diese wiederum vom zukünftigen Einsatzgebiet und -zweck abhängig ist.

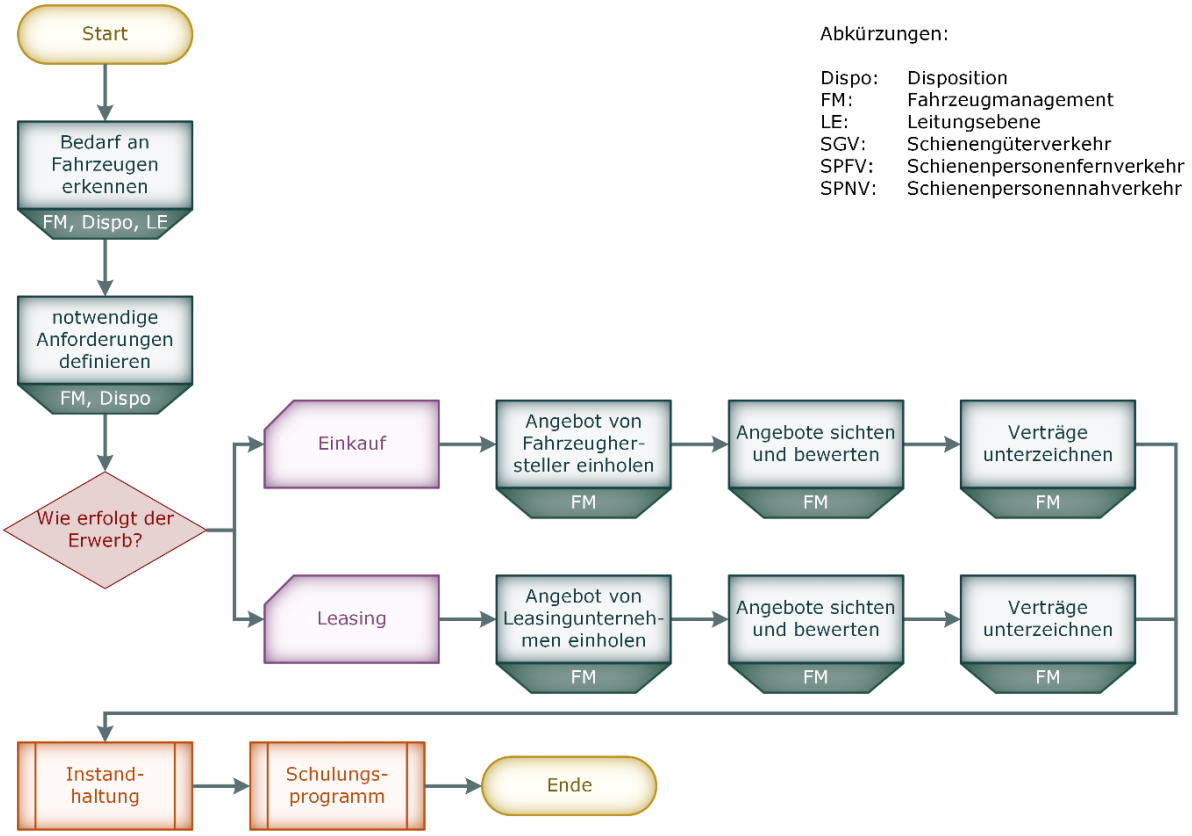


Abbildung A.30: Prozess: Erwerb von Fahrzeugen

Das Fahrzeugmanagement entscheidet gemeinsam mit der Leitungsebene, ob Triebwagen bzw. Lokomotiven und Güterwagen direkt vom Fahrzeughersteller eingekauft oder über eine Leasinggesellschaft angemietet werden. Der Ablauf des Erwerbsprozesses unterscheidet sich jedoch kaum. In beiden Fällen werden zuerst Angebote eingeholt und diese anschließend hinsichtlich der gestellten Anforderungen evaluiert, bevor es schließlich zu einer erforderlichen Vertragsunterzeichnung kommt. Die Rahmenbedingungen für die benannten Prozesse gibt das *Lieferantenmanagement* gemäß SMS vor.

Bevor ein neues Fahrzeug im fiktiven EVU den Betrieb aufnehmen kann, erfolgt in einer externen Instandhaltungseinrichtung eine weitreichende Inspektion nach dem autarken Prozess der *Instandhaltung* (siehe Abschnitt 4.6). Dabei wird insbesondere die Instandhaltungsentwicklungsfunktion realisiert.

Zudem erfolgen entsprechende Schulungsmaßnahmen für das Betriebspersonal beim erstmaligen Einsatz neuer Fahrzeuge und Fahrzeugeinrichtungen im fiktiven EVU.

A4.4 Disposition

Die umfangreichen Aufgaben der Disposition wurden bereits im Anhang 3, Abschnitt 3.4 erläutert. Die Tätigkeiten dienen:

- der „Erstellung und Durchführung von Zugfahrplänen“ [SMS18],
- dem „Betrieb von Zügen/Fahrzeugen unter verschiedenen Betriebsbedingungen ([hier] gestörter Betrieb und Notfälle)“ [SMS18],
- der „Anpassung des Betriebs bei Aufforderungen zur Außerbetriebnahme von Fahrzeugen und bei Meldungen ihrer Wiederinbetriebnahme durch die für die Instandhaltung zuständigen Stellen“ [SMS18],
- der „Kontrolle der Zuweisung von betriebssicherheitsrelevanten Zuständigkeiten [...] für die Koordinierung und Steuerung des sicheren Betriebs von Zügen und Fahrzeugen“ [SMS18],
- der „Kontrolle der betriebssicherheitssicherheitsrelevanten Kompetenzen [bzgl. der] nach Unfällen und Störungen geeignete[n] Maßnahmen“ [SMS18],
- der unverzüglichen Benachrichtigung der Notfalldienste,
- der Erbringung Erster-Hilfe-Leistungen sowie
- den Vorkehrungen für Notfälle mittels „Einsatz-, Alarm und Informationspläne[n]“ [SMS18].

Aus diesem Grund werden nachfolgend die Abläufe der verschiedenen Tätigkeiten näher beschrieben. Abbildung A.31 stellt eine gesamthafte Darstellung der Dispositionsprozesse in Unterprozesse und deren Zusammenwirken untereinander dar. Nachfolgend sollen die einzelnen Teilprozesse näher erläutert werden. Bei den Tätigkeiten der Disposition kommen computergestützte Systeme zum Einsatz, deren Anforderungen zunächst nicht näher ausgeführt werden. Dies hat den Hintergrund, dass Gefährdungen, die aus dem computergestützten Dispositionssystem resultieren mittels Heranziehung eines Referenzsystems evaluiert werden sollen.

A4.4.1 Disposition des Fahrplans

Ein Fahrplan dient der koordinierten Abwicklung des Betriebs innerhalb eines vorab definierten Verkehrsnetzes. Um die vorhandenen Strecken nutzen zu können, erfolgt nach Auftragseingang in Abhängigkeit des Verkehrs von Seiten des fiktiven EVU zuerst eine Definition von Anforderungen an die zu verkehrenden Fahrzeuge sowie eine Trassenanmeldung.

Als letzten Schritt der Fahrplandisposition findet eine Abstimmung mit dem Eisenbahninfrastrukturunternehmen (EIU) statt, in welcher Wiederherstellungsregelungen für einen gestörten Betrieb festzulegen sind. Diese werden anschließend vom EIU veröffentlicht.

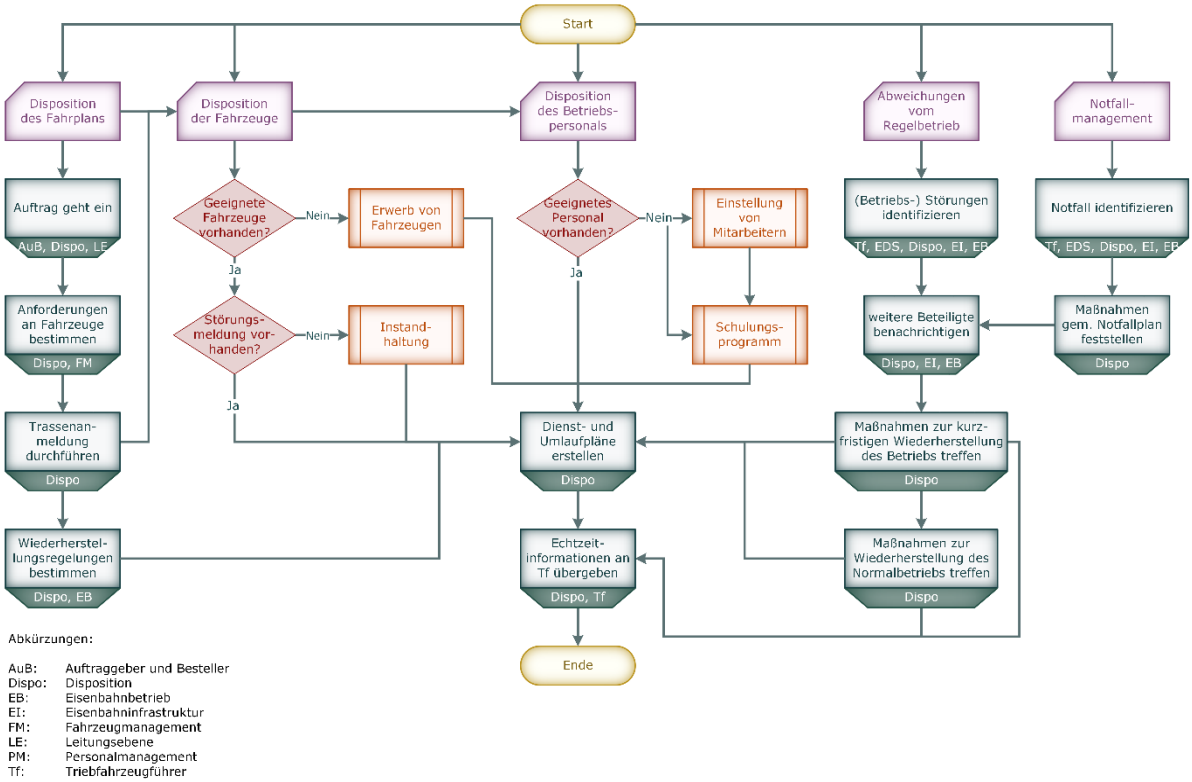


Abbildung A.31: Prozess: Disposition

A4.4.2 Disposition der Fahrzeuge

Im nächsten Schritt erfolgt die Prüfung, ob geeignete Fahrzeuge für die durchzuführenden Zugfahrten verfügbar sind. Ist dies nicht der Fall, werden in Abhängigkeit der zu erbringenden Leistungen die Prozesse des *Fahrzeugerwerbs* (siehe Abschnitt 4.3) angestoßen.

Die Disposition muss gleichfalls die Fahrzeuge, welche einer technischen Instandhaltung bedürfen, aus den Umlaufplänen der Zugleistungen nehmen. Die Information hierzu wird über die Fuhrparkinstandhaltungsmanagementfunktion durch die externe Instandhaltungseinrichtung und das Fahrzeugmanagement an die Disposition gegeben.

A4.4.3 Disposition des Betriebspersonals

Weiterhin bedarf es der Disposition des Betriebspersonals: die notwendigen Triebfahrzeugführer, im SPV ebenfalls die einzusetzenden Zugbegleiter sowie im SGV einzusetzende Wagenmeister müssen disponiert werden. Hierzu erfolgt im Verbund mit dem Personalmanagement eine Prüfung, ob geeignetes Personal zur Verfügung steht. Dies beinhaltet zudem die Kontrolle der Streckenkenntnis der Triebfahrzeugführer.

Tätigkeiten zur Disposition der Betriebspersonale und Fahrzeuge müssen auch situationsbedingt, z. B. bei Fahrplanabweichungen, tagtäglich und ad hoc stattfinden können.

Sind alle genannten Dispositionstätigkeiten erfolgreich umgesetzt worden, werden aktualisierte Dienst-, Umlauf- und Fahrpläne erstellt. Für die planmäßige betriebliche Umsetzung werden anschließend die Zuglaufdaten an den Triebfahrzeugführer übermittelt.

A4.4.4 Abweichungen vom Regelbetrieb und Notfallmanagement

Zusätzlich zu den regelmäßigen, planbaren Tätigkeiten werden Dispositionen bei Betriebsstörungen getätigt. Diese wurden bereits im Rahmen des SMS-Prozesses *Betriebsplanung und -steuerung* definiert. Zunächst gilt es alle auftretenden bzw. aufgetretenen Betriebsstörungen zu identifizieren und deren Ursachen, soweit möglich, zu bestimmen. Außerdem sind alle weiteren am Betrieb beteiligten Stellen, z. B. die betreffenden EIU und sonstige EVU, über die Störung zu benachrichtigen. Parallel erörtern und entscheiden die Disponenten konkrete Maßnahmen zur kurzfristigen Wiederherstellung des Betriebs. Grundsätzlich existieren hierfür bereits im Vorfeld definierte Wiederherstellungsregelungen, die es nutzbringend anzuwenden und in den Fahrplan einzupflegen gilt. Über die Weiterleitung von Echtzeitinformationen werden die getroffenen Maßnahmen an alle Beteiligten, allen voran den Triebfahrzeugführern, übermittelt und anschließend umgesetzt.

Die Tätigkeiten des Notfallmanagements weichen – von der Ausgangssituation abgesehen – kaum von den Abläufen bei Abweichungen vom Regelbetrieb ab. Die Maßnahmen zur Wiederherstellung des generellen Betriebs und des Regelbetriebs sind ebenfalls im Rahmen des SMS-Prozesses in einem Notfallplan definiert und werden situationsbedingt initiiert.

A4.5 Fahrt vorbereiten, durchführen und Fahrzeug abrüsten

A4.5.1 Personennah- und -fernverkehr

Der Prozess *Fahrt vorbereiten, durchführen und Fahrzeug abrüsten (im Personennah- und -fernverkehr)* ist in Abbildung A.32 dargestellt und beschreibt den umfassenden Ablauf der Fahrzeugbewegungen im SPNV und SPFV. Er beginnt und endet praxisgemäß am Abstellplatz des Fahrzeugs. Dieser ist einzunehmen, wenn die Zugfahrten beendet sind und damit die Beförderungs-/Transportleistung erbracht wurde. Ausnahmen bilden Aufenthalte in (externen) Instandhaltungseinrichtungen.

Fahrt vorbereiten

Der Triebfahrzeugführer/die Triebfahrzeugführerin muss zu Beginn seines Dienstes seine persönlichen Ausrüstungsgegenstände mitführen, z. B. die persönliche Schutzausrüstung gemäß Arbeitsschutzvorschriften.

Vor jedem Dienst erhält der Triebfahrzeugführer zudem einen Arbeitsauftrag und die für den Dienst relevanten Unterlagen. Diese werden vom Triebfahrzeugführer auf Vollständigkeit und – soweit er das überprüfen kann – auf Plausibilität überprüft. Im Fall festgestellter Abweichungen wird die Disposition umgehend informiert, woraufhin diese den Prozess der *Abweichungen vom Regelbetrieb* einleitet. Ergebnis dieses Prozesses ist ein neuer Arbeitsauftrag, welcher eine erneute Prüfung der Unterlagen herbeiführt. Erst wenn die Unterlagen dem Triebfahrzeugführer augenscheinlich korrekt und vollumfänglich vorliegen, können die nächsten Tätigkeiten stattfinden.

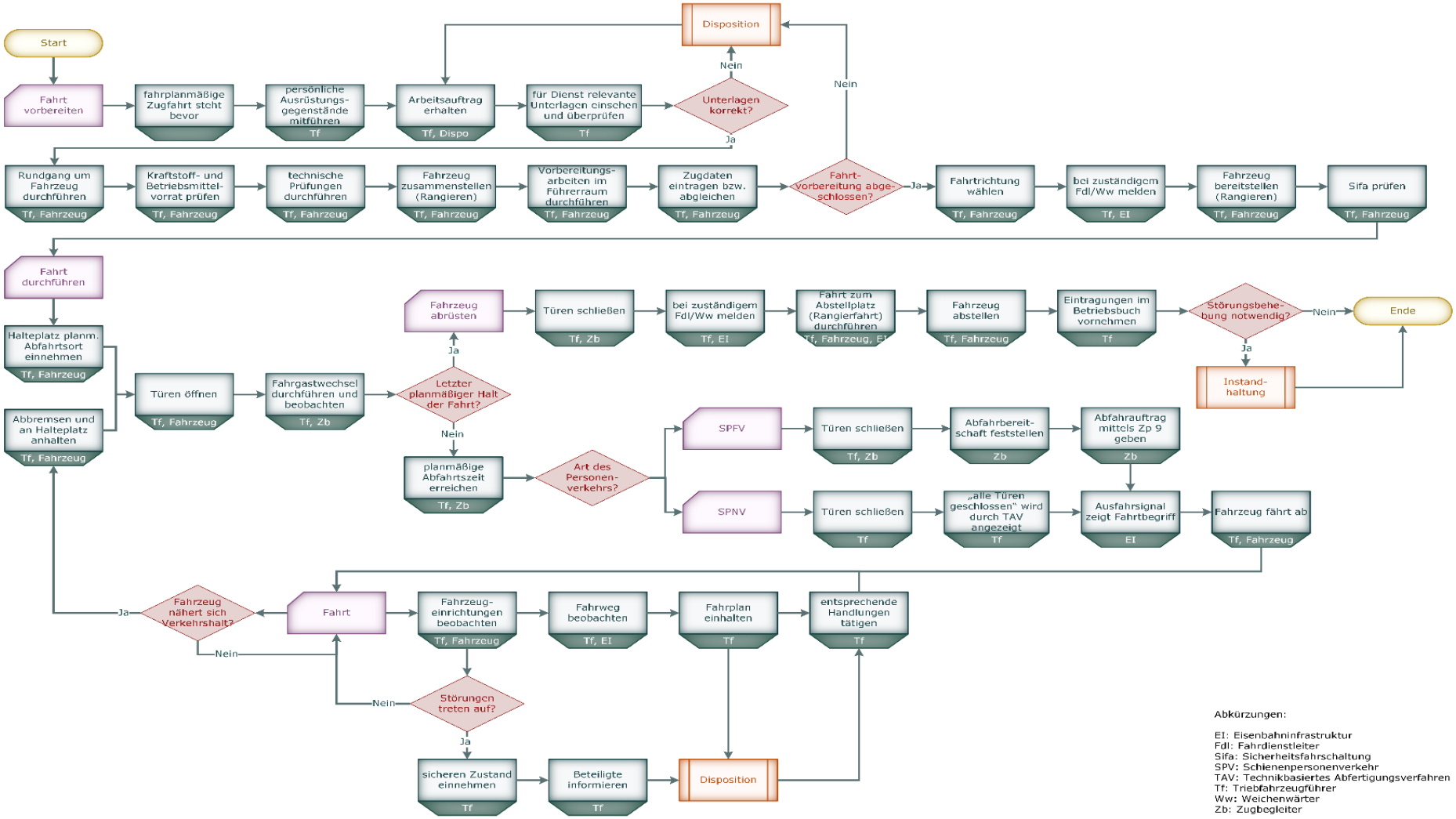


Abbildung A.32: Prozess: Fahrt vorbereiten, durchführen und Fahrzeug abrüsten im SPV

Es schließt sich der Rundgang um das Fahrzeug an, bei dem Kraftstoff- und Betriebsmittelvorräte sowie technische Funktionseinheiten überprüft werden. Sofern ein Triebwagenverband zusammengestellt werden muss, wird dies durch den Triebfahrzeugführer ausgeführt. Anschließend werden die Vorbereitungsarbeiten im Führerraum fortgesetzt. Hier erfolgen Prüfungen und Tests an den technischen Einrichtungen. Weiterhin werden die Komponenten im Führerraum in Betrieb genommen. Alle Tätigkeiten im Vorbereitungs- und Abschlussdienst sind für die jeweils eingesetzten Fahrzeuge in einer Vorschrift (Betriebsregelwerk) aufgelistet. Dieses Vorschriftenkonvolut wird, wie alle in Anwendung befindlichen Regelwerke, im Rahmen des *Änderungsmanagements* und der implementierten *Maßnahmen zur Beherrschung von Risiken* stetig hinsichtlich ihrer Aktualität, Vollständigkeit und Verständlichkeit überprüft und ggf. angepasst. Der Triebfahrzeugführer gibt zuletzt die erforderlichen Zugdaten ein bzw. überprüft diese. Können die Vorbereitungsarbeiten nicht vollumfänglich durchgeführt bzw. abgeschlossen werden, leitet der Triebfahrzeugführer analog zur Unterlagenkontrolle dispositive Tätigkeiten ein.

Nachdem die Fahrtrichtung gewählt wurde, wird die Abfahrbereitschaft dem zuständigen Fahrdienstleiter bzw. Weichenwärter gemeldet. Dieser stellt den Fahrweg zum definierten Halteplatz (Startplatz der folgenden Zugfahrt) ein und der Triebfahrzeugführer fährt als Rangierfahrt zu dieser Stelle. Während dieser Fahrt wird an einer geeigneten Stelle die Sicherheitsfahrschaltung (Sifa) getestet.

Fahrt durchführen

Nach Beendigung der Vorbereitungstätigkeiten befindet sich das Fahrzeug am Halteplatz des planmäßigen Abfahrtsortes. Im SPV erfolgt hier der Fahrgastwechsel. Dieser wird durch den Triebfahrzeugführer und/oder den Zugbegleiter beobachtet.

Die nachfolgenden Tätigkeiten unterscheiden sich hinsichtlich der Art des SPV. Im SPNV verfügt jeder Triebwagen über ein TAV, welches die Türschließung überwacht. Dem Triebfahrzeugführer wird im Führerraum der Zustand der geschlossenen Türen angezeigt. Im SPFV hat der Zugbegleiter in der Rolle des Zugführers die Aufgabe, die Abfahrbereitschaft des Zuges festzustellen und diese dem Triebfahrzeugführer mittels Signal Zp 9 anzuzeigen.

Sofern die Abfahrbereitschaft vorliegt und das Ausfahrsignal einen Fahrtbegriff anzeigt, kann der Zug abfahren. Es beginnt der Unterprozess *Fahrt*. Hierbei laufen diverse Abfolgen parallel und wiederkehrend ab. Dazu zählen:

- die Beobachtung der Fahrzeugeinrichtungen insbesondere der Führerraumanzeigen,
- die Streckenbeobachtung sowie
- die Einhaltung des Fahrplans.

Entsprechend der Feststellungen tätigt der Triebfahrzeugführer situationsgerechte Handlungen, wie z. B. die Geschwindigkeitsanpassung. Werden Störungen identifiziert, nimmt das Gesamtystem den sicheren Zustand ein und der Tf informiert alle Beteiligte (z. B. EIU, weitere EVU, Disposition). Die Disposition gibt gemäß dem in Abschnitt 4.4.4 benannten Abläufen Maßnahmen vor, welche der Triebfahrzeugführer entsprechend umzusetzen hat.

Nähert sich das Fahrzeug dem nächsten Verkehrshalt wird die Geschwindigkeit entsprechend verringert und das Fahrzeug hält am vorgesehenen Halteplatz. Der Fahrgastwechsel beginnt erneut, indem der Triebfahrzeugführer die Türen öffnet. Dieser Prozess wird solange durchlaufen, bis der letzte planmäßige Halt der Fahrt erreicht ist und das Fahrzeug abgerüstet wird.

Fahrzeug abrüsten

Die Fahrt zum Abstellplatz erfolgt für das Fallbeispiel des fiktiven EVU grundsätzlich als Rangierfahrt. Anschließend werden durch den Triebfahrzeugführer Tätigkeiten entsprechend des Betriebsregelwerks durchgeführt. Dazu gehören auch Eintragungen im Betriebsbuch, insbesondere durchgeführte Prüftätigkeiten und identifizierte technische Störungen. Handelt es sich bei zuletzt genannten um solche, die einer Instandsetzung bedürfen, wird der Prozess der *Instandhaltung* gestartet, anderenfalls schließt der Prozess ohne weitere Aktivität.

A4.5.2 Güterverkehr

Die Prozesse im SGV unterscheiden sich zum eben vorangestellten Ablauf im SPV nur in Einzelfällen. Auf diese Detailunterschiede konzentrieren sich die nachfolgenden Ausführungen. Der gesamte Ablauf der *Fahrtvorbereitung, -durchführung und der Fahrzeugabrüstung im SGV* ist in Abbildung A.33 dargestellt. Zur Demonstration der Prozesse im SGV gilt es zu unterscheiden, ob sich der Güterzug am Abstellplatz oder am Zielgleis der vorangegangenen Zugfahrt befindet.

Der Unterprozess, wenn sich der Güterzug in der Abstellanlage befindet, beinhaltet keine wesentlichen Abweichungen gegenüber den Verfahrensweisen im SPV. Auch hier werden Prüfungen und Inspektionen am Fahrzeug, den technischen Anlagen sowie den für den Dienst relevanten Unterlagen durchgeführt. Am Ende dieser Abfolge von Tätigkeiten des Triebfahrzeugführers wird der Güterzug am Halteplatz im GVZ bereitgestellt.

Sofern sich der Güterzug nach einer Fahrt im Zielgleis der Zugfahrt befindet, wird er als Rangierfahrt in den Nebengleisbereich gefahren und dort an definierter Position im GVZ zum Halten gebracht.

Hier wird der Güterzug von einem externen Logistikunternehmen übernommen, ent- und beladen sowie für die anstehende Fahrt zusammengestellt. Der Detailprozess der Be- und Entladung wird in dieser Systemdefinition nicht näher erläutert, da er außerhalb des Untersuchungsgegenstandes liegt. Dies liegt darin begründet, dass die Tätigkeiten nicht vom fiktiven EVU durchgeführt werden, sondern entsprechend des SMS-Prozesses *Auftragnehmer, Partner und Zulieferer* an externe Logistikunternehmer vergeben ist. Dem Triebfahrzeugführer und dem Wagenmeister werden abschließend nach Beladung die entsprechenden Beförderungspapiere übergeben.

Befinden sich im Wagenverband gefährliche Güter nach der Gefahrgutverordnung Straße, Eisenbahn und Binnenschifffahrt (GGVSEB) [GGV21], müssen die zugehörigen Begleit- und Beförderungspapiere dem Triebfahrzeugführer und Wagenmeister vor Ort durch den Auftraggeber bzw. Verlader übergeben werden. Es folgen mehrere Überprüfungen im Einklang mit [GGV21] bzw. [RID21]. Darüber hinaus muss der Triebfahrzeugführer gemäß § 31a GGVSEB „vor Antritt der Fahrt die schriftlichen Weisungen zu den bei einem Unfall oder Zwischenfall zu ergreifenden Maßnahmen“ [GGV21] sichten. Nur im Fall einer vollumfänglichen, positiven Beurteilung des Gefahrguts findet der Transport statt. Andernfalls informiert der Triebfahrzeugführer oder Wagenmeister die Disposition.

Bevor der Güterzug den Halteplatz am Ausfahrgleis einnehmen kann, ist zunächst die Prüfung der Betriebssicherheit und Verkehrstauglichkeit durch den Wagenmeister und den Triebfahrzeugführer erforderlich. Anschließend werden vorhandene Hand- und Feststellbremsen gelöst und das Spitzen- und Zugschlusssignal kontrolliert. Die Abfahrbereitschaft ist schließlich hergestellt und der Triebfahrzeugführer meldet sich beim zuständigen Fahrdienstleiter bzw. Weichenwärter zur Rangierfahrt für die Bereitstellung an.

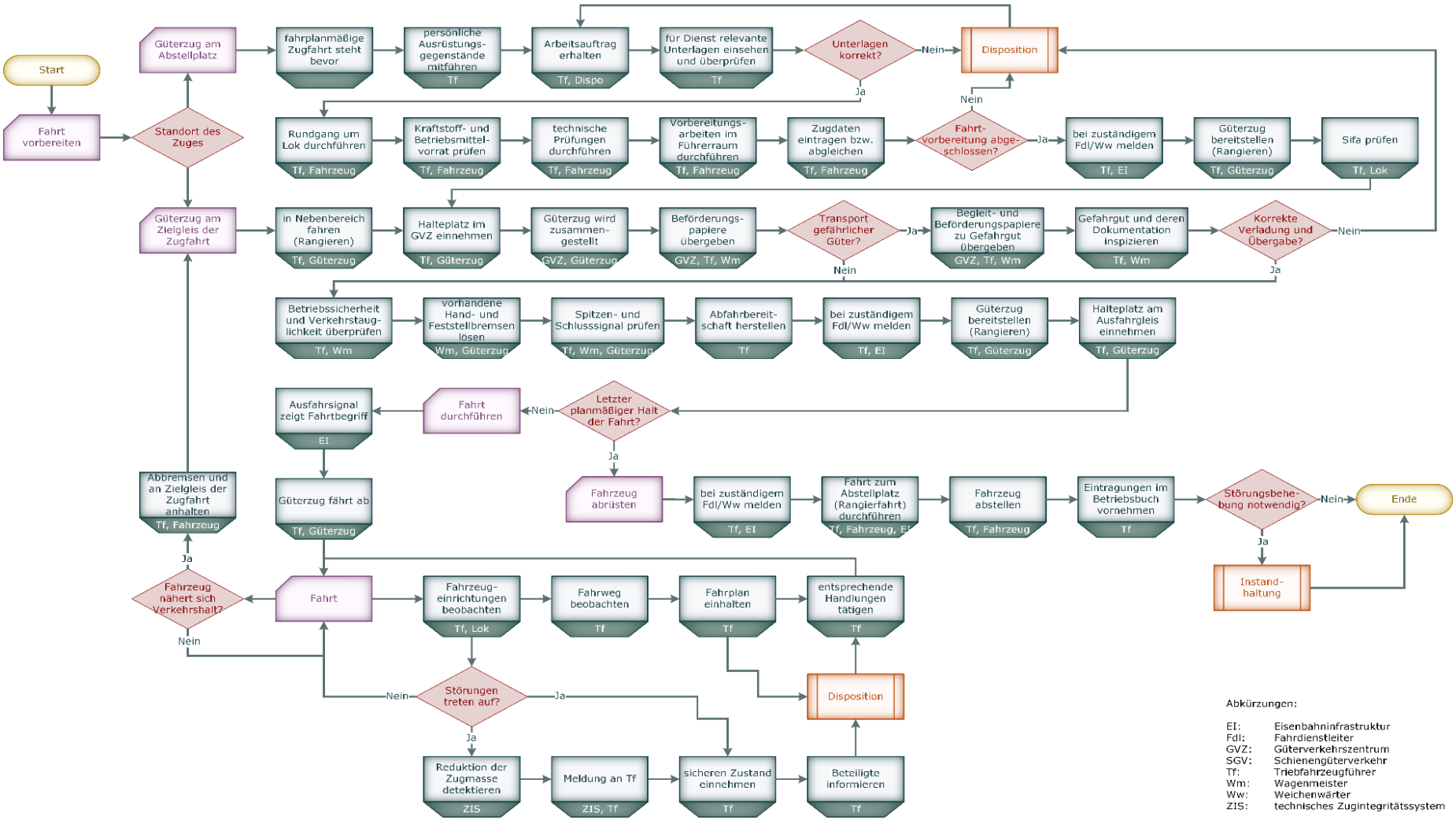


Abbildung A.33: Prozess: Fahrt vorbereiten, durchführen und Fahrzeug abrüsten im SGV

Sobald das Ausfahrsignal am Ausfahrgleis den Fahrtbegriff zeigt, fährt der Zug ab. Der Unterprozess *Fahrt* beginnt und dauert so lange an, bis sich der Zug dem nächsten Verkehrshalt nähert.

Besonderheit an diesem Unterprozess im SGV ist der Einsatz des ZIS. Dieses System detektiert kontinuierlich während der Zugfahrt eine potenzielle Reduktion des Zuggewichts und gibt eine entsprechende Warnmeldung an den Triebfahrzeugführer aus. Dieser führt situationsgerecht entsprechende Handlungen aus, um den sicheren Zustand einzunehmen und informiert die Beteiligten.

Nähert sich das Fahrzeug dem nächsten Verkehrshalt wird die Geschwindigkeit entsprechend verringert und der Güterzug hält am vorgesehenen Zielgleis. Die Besonderheit der Modellierung der Abläufe im SGV für diesen Forschungsgegenstand besteht darin, dass sich nach jedem Halt am Halteplatz des Güterverkehrsgleises der Prozess der Be- bzw. Entladung anschließt. Der Prozessablauf wird erst beendet, wenn der letzte planmäßige Halt der Fahrt stattgefunden hat. Anschließend kann der Güterzug zum Abstellplatz gefahren werden und der Vorgang zum Abrüsten wird analog zum SPV eingeleitet.

A4.6 Instandhaltung

Bei der Instandhaltung wird zwischen präventiver und korrektiver Instandhaltung unterschieden. Über die Instandhaltungsentwicklungs- sowie die Fuhrparkinstandhaltungsmanagementfunktion überwacht die externe Instandhaltungseinrichtung die präventiven Instandhaltungsvorgaben der Fahrzeuge des fiktiven EVU. Korrektive Instandhaltung wird notwendig, wenn sicherheitsrelevante Störungen während des Betriebs durch den Triebfahrzeugführer oder den Wagenmeister identifiziert werden. Der Prozess der *Instandhaltung* ist in Abbildung A.34 dargestellt. Aus als notwendig identifizierten Dispositionstätigkeiten resultiert, dass das Fahrzeug zur externen Instandhaltungseinrichtung gefahren wird. Dies erfolgt nach dem Prozess der *Fahrtdurchführung* (siehe Abschnitt 4.5). In der externen Instandhaltungseinrichtung werden die notwendigen Maßnahmen durch fachkundiges Instandhaltungspersonal durchgeführt und dokumentiert.

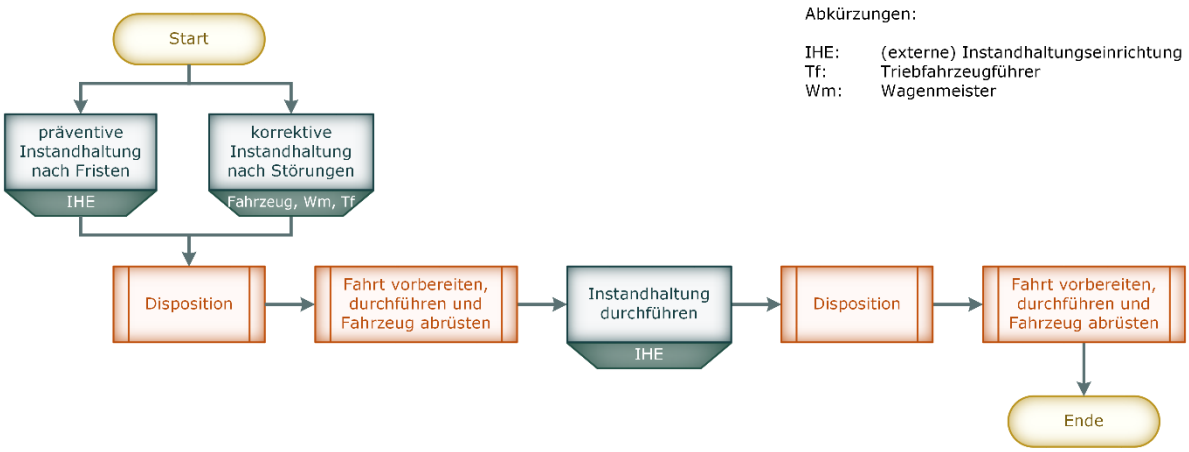


Abbildung A.34: Prozess: Instandhaltung von Fahrzeugen

Nach Beendigung aller Instandhaltungstätigkeiten steht das Fahrzeug wieder für den Bahnbetrieb zur Verfügung. Dafür finden *Dispositionsprozesse* statt (siehe Abschnitt 4.4), die dazu führen, dass das Fahrzeug am Abstellplatz stationiert wird. Das Fahrzeugmanagement ist im Rahmen der implementierten SMS-Prozesse dafür zuständig, die Tätigkeiten der externen Instandhaltungseinrichtung zu inspizieren.

A4.7 Außerbetriebnahme von Fahrzeugen

Der Außerbetriebnahmeprozess von Fahrzeugen wird eingeleitet, falls diese nicht mehr benötigt oder ein irreparabler Schaden festgestellt wurde. Der Prozess ist in Abbildung A.35 dargestellt.

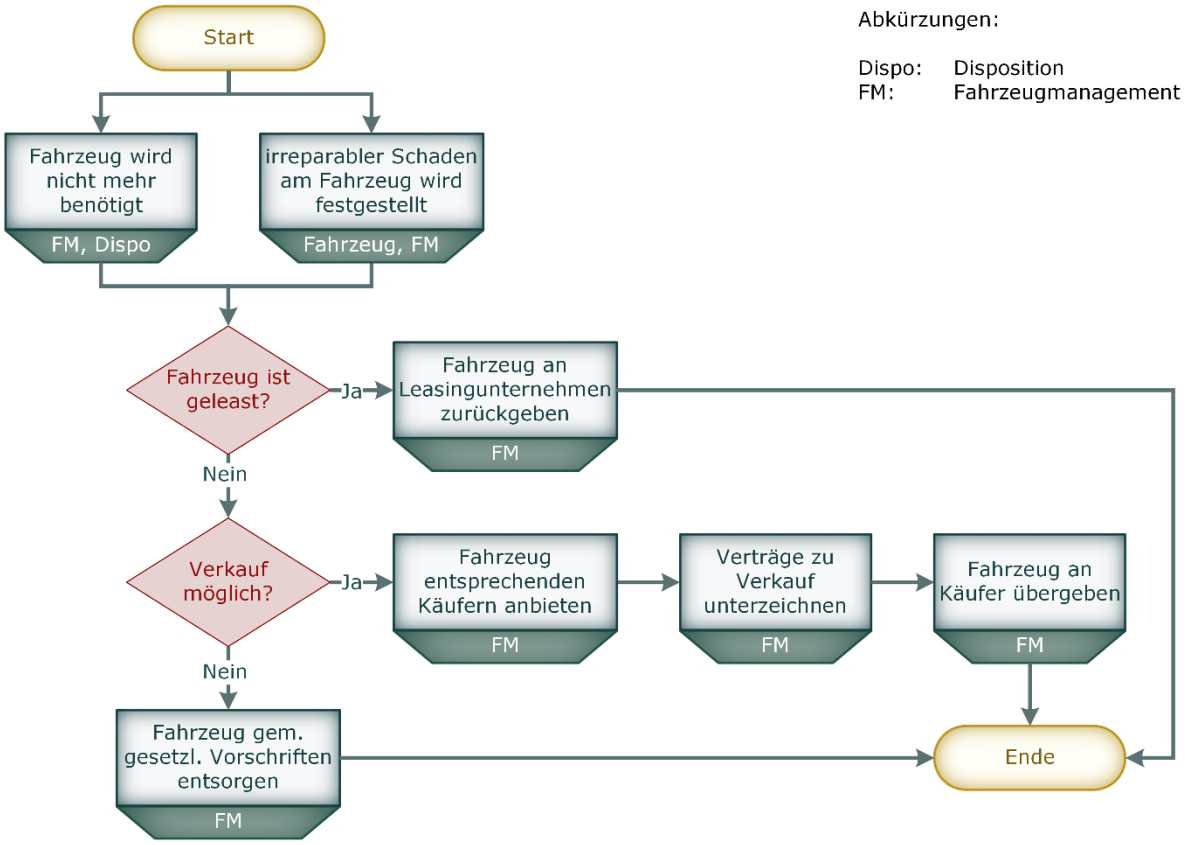


Abbildung A.35: Prozess: Außerbetriebnahme von Fahrzeugen

Die Außerbetriebnahme von Fahrzeugen ist abhängig von dessen Erwerb. Bei einem geleasten Objekt wird das Fahrzeug an das Leasingunternehmen zurückgegeben. Falls das Fahrzeug Eigentum des fiktiven EVU ist, erfolgt die Überprüfung, ob ein Verkauf möglich ist. Das Fahrzeugmanagement trifft diese Entscheidung. Bei getroffener Verkaufsentscheidung wird das Fahrzeug entsprechenden Interessenten angeboten und im Erfolgsfall die Fahrzeugübergabe vertraglich fixiert und anschließend umgesetzt. Anderenfalls erfolgt eine Entsorgung des ausgedienten Fahrzeugs unter Einhaltung der entsprechenden gesetzlichen Vorschriften. Dabei greift das SMS mit seinem *Sachanlagenmanagement*.

A5 Gefährdungsprotokoll

TABELLE A.22: GEFÄHRDUNGSPROTOKOLL (AUSZUG)

Nr.	Unter-prozess	Funktion	Ausfallursache/Fehler		Ausfall/Fehlzu-stand	Gefährdung	Unfall	Schadensausmaß		Häufigkeit		Kritikali-tät	Anwen-dung RAG
		Tätigkeit	Beschrei-bung	Kategorisie-rung		Auswirkung eines Ausfalls Fehlzustands	Folge der Gefähr-dung	Katego-risie-rung	Begrün-dung	Kategori-sierung	Begründung		
Prozess: Einstellung von Mitarbeitern													
1		Bedarf an Personal erkennen	Bedarf wird nicht er-kannt, Miss-manage-ment	organisatori-scher Fehler	fehlendes Personal im Notfallmanage-ment	notwendige Maßnahmen bei Störungen wer-den nicht getrof-fen	Folgeunfall	kata-strophal	zahlreiche Tote, extremer Umwelt-schaden	selten	Es wird angenommen, dass das Ereignis durch unvorhergese-hene längere Ausfälle, z. B. Schwangerschaft, Krankheit, irgendwann einmal eintreten kann.	uner-wünscht	–
2			Bedarf wird zu spät er-kannt	menschliches Fehlverhalten	Personal im Not-fallmanagement kann nicht rechtzei-tig eingestellt wer-den	notwendige Maßnahmen bei Störungen wer-den nicht getrof-fen	Folgeunfall	kata-strophal	zahlreiche Tote, extremer Umwelt-schaden	selten	Es wird angenommen, dass das Ereignis durch unvorhergese-hene längere Ausfälle, z. B. Schwangerschaft, Krankheit, irgendwann einmal eintreten kann.	uner-wünscht	–
Prozess: Disposition													
3	Disposi-tion des Fahrplans	Dienst- und Umlaufpläne erstellen	Fehler im computerge-stützten Sys-tem	technischer Fehler	Disposition wird falsch/fehlerhaft verarbeitet	diverse	Zugentgleisung, Kontamination der Umwelt (Gefahr-gutaustritt), Kolli-sion Fahrzeug mit Ladung	kata-strophal	zahlreiche Tote, extremer Umwelt-schaden	selten	Anforderungen an computergestütztes System nicht definiert, weshalb angenommen wird, dass das Ereignis irgendwann einmal auftreten wird.	uner-wünscht	Referenz-system
Prozess: Fahrt vorbereiten, durchführen und Fahrzeug abrüsten (im SGV)													
4	Fahrt vor-bereiten	Halteplatz am Ausfahr-gleis einneh-men	fehlende Definition zu Abstellorten bzgl. Siche-rung des Ge-fahrguts	organisatori-scher Fehler	Halteplatz ist nicht ausreichend gesi-chert, unbeleuchtet und/oder für Öf-fentlichkeit unzu-gänglich	Einwirkung von Dritten	Kontamination der Umwelt (Gefahrgutaustritt) bei unsachgemä-ßer Verwendung durch Dritte	kata-strophal	extremer Umwelt-schaden	wahrschein-lich	Aufgrund fehlender Definition zu Plätzen für das zeitweilige Ab-stellen von Fahrzeu-gen, wird angenom-men, dass das Ereignis oft auftreten wird.	untragbar	Regel-werk

Nr.	Unterprozess	Funktion	Ausfallursache/Fehler		Ausfall/Fehlzustand	Gefährdung	Unfall	Schadensausmaß		Häufigkeit		Kritikalität	Anwendung RAG
5	Fahrt durchführen	Zugtrennung detektieren	diverse	technischer Fehler	Reduktion des Zuggewichts wird nicht detektiert	unbemerkte Zugtrennung	kein Unfall durch Sicherheitsmechanismen (Gleisfreimeldung)					keine Gefährdung	–
6						unbemerkter Ladungsverlust	Zugentgleisung durch Ladung auf Strecke	katastrophal	zahlreiche Tote, extremer Umweltschaden	unwahrscheinlich	Es wird angenommen, dass das Ereignis ausnahmsweise auftreten kann.	unerwünscht	explizite Risikoabschätzung
7	Fahrt durchführen	Meldung Zugtrennung an Triebfahrzeugführer	diverse	technischer Fehler	Reduktion des Zuggewichts wird nicht gemeldet	unbemerkte Zugtrennung	kein Unfall durch Sicherheitsmechanismen (Gleisfreimeldung)					keine Gefährdung	–
8						unbemerkter Ladungsverlust	Zugentgleisung durch Ladung auf Strecke	katastrophal	zahlreiche Tote, extremer Umweltschaden	unwahrscheinlich	Es wird angenommen, dass das Ereignis ausnahmsweise auftreten kann.	unerwünscht	explizite Risikoabschätzung
9		Abbremsen und an Zielgleis der Zugfahrt anhalten	fehlende Definition zu Abstellorten bzgl. Sicherung des Gefahrguts	organisatorischer Fehler	Halteplatz ist nicht ausreichend gesichert, unbeleuchtet und/oder für Öffentlichkeit unzugänglich	Einwirkung von Dritten	Kontamination der Umwelt (Gefahrgutaustritt) bei unsachgemäßer Verwendung durch Dritte	katastrophal	extremer Umweltschaden	wahrscheinlich	Aufgrund fehlender Definition zu Plätzen für das zeitweilige Abstellen von Fahrzeugen, wird angenommen, dass das Ereignis oft auftreten wird.	untragbar	Regelwerk
10	Fahrzeug abrüsten	Fahrzeug abstellen	fehlende Definition zu Abstellorten bzgl. Sicherung des Gefahrguts	organisatorischer Fehler	Halteplatz ist nicht ausreichend gesichert, unbeleuchtet und/oder für Öffentlichkeit unzugänglich	Einwirkung von Dritten	Kontamination der Umwelt (Gefahrgutaustritt) bei unsachgemäßer Verwendung durch Dritte	katastrophal	extremer Umweltschaden	wahrscheinlich	Aufgrund fehlender Definition zu Plätzen für das zeitweilige Abstellen von Fahrzeugen, wird angenommen, dass das Ereignis oft auftreten wird.	untragbar	Regelwerk

A6 Ereignisbaum: falsch/fehlerhaft verarbeitete Dispositionsentscheidung

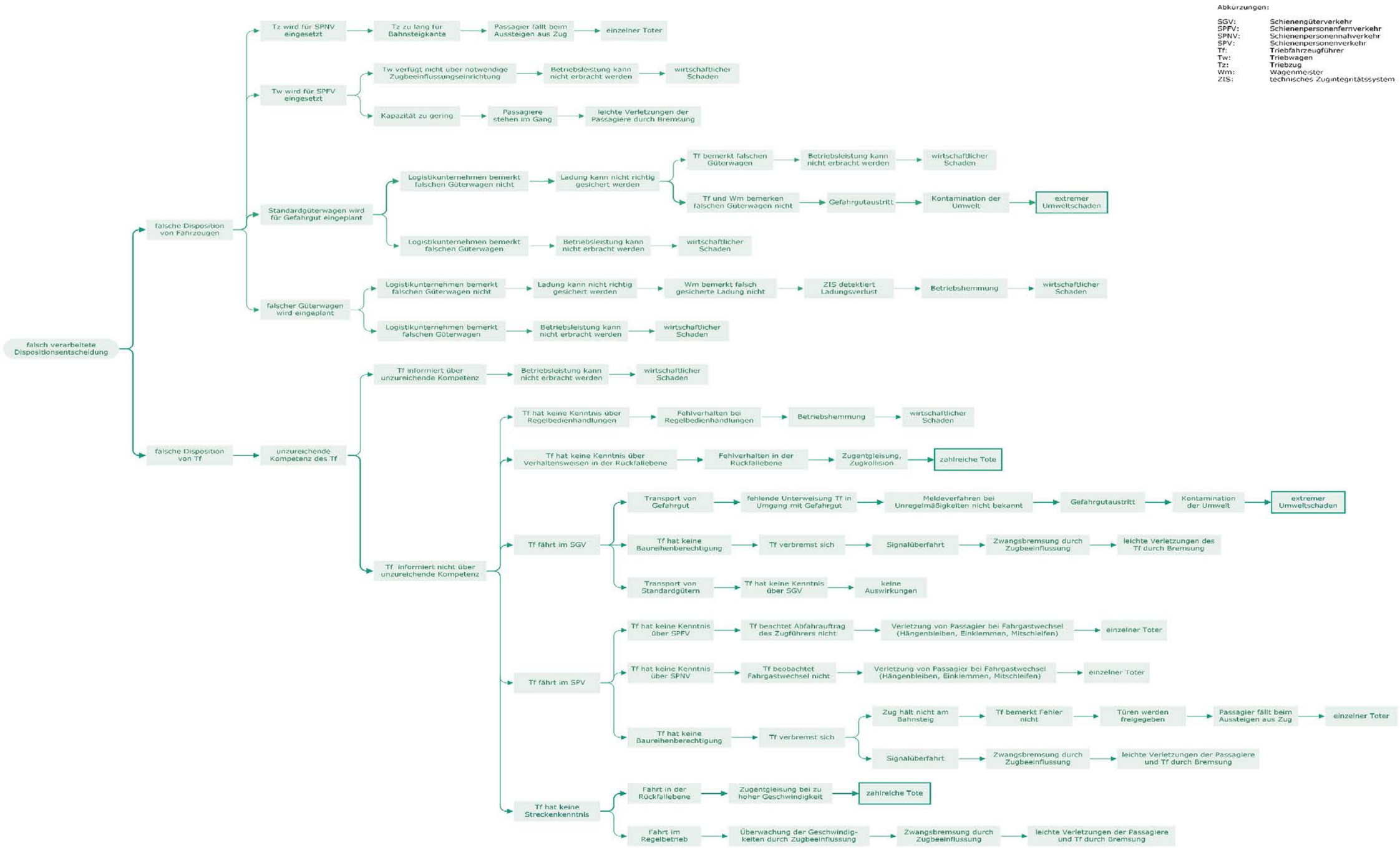


Abbildung A.36: Ereignisbaum: falsch/fehlerhaft verarbeitete Dispositionsentscheidung

A7 Überarbeitetes Gefährdungsprotokoll

TABELLE A.23: ÜBERARBEITETES GEFÄHRDUNGSPROTOKOLL (AUSZUG)

Nr.	Unter-prozess	Funktion	Ausfallursache/Fehler		Ausfall/Fehlzustand	Gefährdung	Unfall	Schadensausmaß		Häufigkeit		Kritikalität
Prozess: Disposition												
3	Disposition des Fahrplans	Dienst- und Umlaufpläne erstellen	Fehler im computergestützten System	technischer Fehler	Disposition wird falsch/fehlerhaft verarbeitet	diverse	Zugentgleisung, Kontamination der Umwelt (Gefahrgutaustritt), Kollision Fahrzeug mit Ladung	katastrophal	zahlreiche Tote, extremer Umweltschaden	selten	Anforderungen an computergestütztes System nicht definiert, weshalb angenommen wird, dass das Ereignis irgendwann einmal auftreten wird.	unerwünscht
		Schutzmaßnahmen: Anwendung der Vorgaben an das computergestützte Dispositionssystem gemäß Tabelle 10 Resultat: Risiko kann unter Einhaltung der Anforderungen an computergestütztes Dispositionssystem als allgemein vertretbar angesehen werden										tolerabel
Prozess: Fahrt vorbereiten, durchführen und Fahrzeug abrüsten (im Güterverkehr)												
4	Fahrt vorbereiten	Halteplatz am Ausfahrgleis einnehmen	fehlende Definition zu Abstellorten bzgl. Sicherung des Gefahrguts	organisatorischer Fehler	Halteplatz ist nicht ausreichend gesichert, unbeleuchtet und/oder für Öffentlichkeit unzugänglich	Einwirkung von Dritten	Kontamination der Umwelt (Gefahrgutaustritt) bei unsachgemäßer Verwendung durch Dritte	katastrophal	extremer Umweltschaden	wahrscheinlich	Aufgrund fehlender Definition zu Plätzen für das zeitweilige Abstellen von Fahrzeugen, wird angenommen, dass das Ereignis oft auftreten wird.	untragbar
		Schutzmaßnahmen: Anwendung der Umsetzungsempfehlung des [VCI17] (siehe Tabelle 9) Resultat: Anforderungen, Realisierungen und Überprüfungen verringern in erheblichem Ausmaß die Häufigkeit der Einwirkung durch Dritte; Risiko kann als allgemein vertretbar angesehen werden										tolerabel
6	Fahrt durchführen	Zugtrennung detektieren	diverse	technischer Fehler	Reduktion des Zuggewichts wird nicht detektiert	unbemerkter Ladungsverlust	Zugentgleisung durch Ladung auf Strecke	katastrophal	zahlreiche Tote, extremer Umweltschaden	unwahrscheinlich	Es wird angenommen, dass das Ereignis ausnahmsweise auftreten kann.	unerwünscht
		Schutzmaßnahmen: Anwendung und Einhaltung der zulässigen Ausfallraten für das jeweilige technische Funktionsversagen sowie der zugrunde gelegten Sicherheitsbarrieren Resultat: Risiko kann unter Einhaltung der Schutzmaßnahmen als allgemein vertretbar angesehen werden										tolerabel
8	Fahrt durchführen	Meldung Zugtrennung an Triebfahrzeugführer	diverse	technischer Fehler	Reduktion des Zuggewichts wird nicht gemeldet	unbemerkter Ladungsverlust	Zugentgleisung durch Ladung auf Strecke	katastrophal	zahlreiche Tote, extremer Umweltschaden	unwahrscheinlich	Es wird angenommen, dass das Ereignis ausnahmsweise auftreten kann.	unerwünscht
		Schutzmaßnahmen: Anwendung und Einhaltung der zulässigen Ausfallraten für das jeweilige technische Funktionsversagen sowie der zugrunde gelegten Sicherheitsbarrieren Resultat: Risiko kann unter Einhaltung der Schutzmaßnahmen als allgemein vertretbar angesehen werden										tolerabel

Nr.	Unter-prozess	Funktion	Ausfallursache/Fehler		Ausfall/Fehlzustand	Gefährdung	Unfall	Schadensausmaß		Häufigkeit		Kritikalität
9	Fahrt durchführen	Abbremsen und an Zielgleis der Zugfahrt anhalten	fehlende Definition zu Abstellorten bzgl. Sicherung des Gefahrguts	organisatorischer Fehler	Halteplatz ist nicht ausreichend gesichert, unbeleuchtet und/oder für Öffentlichkeit unzugänglich	Einwirkung von Dritten	Kontamination der Umwelt (Gefahrgutaustritt) bei unsachgemäßer Verwendung durch Dritte	katastrophal	extremer Umweltschaden	wahrscheinlich	Aufgrund fehlender Definition zu Plätzen für das zeitweilige Abstellen von Fahrzeugen, wird angenommen, dass das Ereignis oft auftreten wird.	untragbar
		Schutzmaßnahmen: Anwendung der Umsetzungsempfehlung des [VCI17] (siehe Tabelle 9) Resultat: Anforderungen, Realisierungen und Überprüfungen verringern in erheblichem Ausmaß die Häufigkeit der Einwirkung durch Dritte; Risiko kann als allgemein vertretbar angesehen werden										tolerabel
10	Fahrzeug abrüsten	Fahrzeug abstellen	fehlende Definition zu Abstellorten bzgl. Sicherung des Gefahrguts	organisatorischer Fehler	Halteplatz ist nicht ausreichend gesichert, unbeleuchtet und/oder für Öffentlichkeit unzugänglich	Einwirkung von Dritten	Kontamination der Umwelt (Gefahrgutaustritt) bei unsachgemäßer Verwendung durch Dritte	katastrophal	extremer Umweltschaden	wahrscheinlich	Aufgrund fehlender Definition zu Plätzen für das zeitweilige Abstellen von Fahrzeugen, wird angenommen, dass das Ereignis oft auftreten wird.	untragbar
		Schutzmaßnahmen: Anwendung der Umsetzungsempfehlung des [VCI17] (siehe Tabelle 9) Resultat: Anforderungen, Realisierungen und Überprüfungen verringern in erheblichem Ausmaß die Häufigkeit der Einwirkung durch Dritte; Risiko kann als allgemein vertretbar angesehen werden										tolerabel