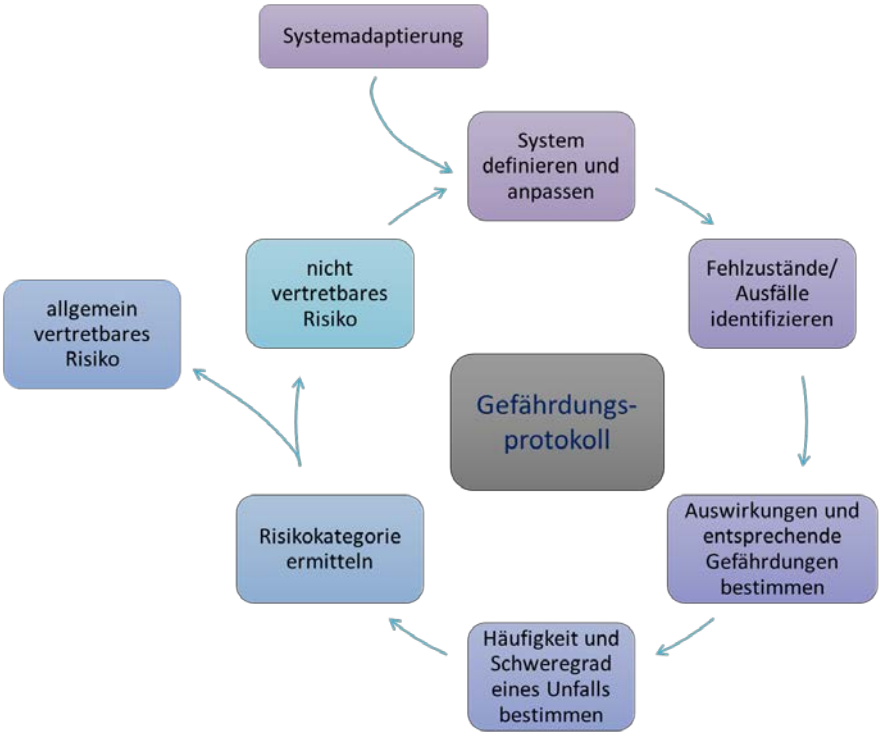
Deutsches Zentrum für
Schienenverkehrsforschung beim
Eisenbahn-Bundesamt

Berichte
des Deutschen Zentrums
für Schienenverkehrsforschung

Bericht 21 (2022)

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

Zusammenfassung



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"

Zusammenfassung

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.220005.02

Dresden, Februar 2022

Inhaltsverzeichnis

1 Einleitung 6

2 Systemdefinition 8

2.1 Produktorientierte Systemdefinition 8

2.2 Prozessorientierte Systemdefinition 9

3 Gefährdungsermittlung und –einstufung 10

4 Risikoevaluierung 13

4.1 Zugrundelegung von Regelwerken 13

4.2 Heranziehung eines Referenzsystems 15

4.3 Explizite Risikoabschätzung 16

5 Bestimmung der Sicherheitsanforderungen 17

5.1 Kategorien der Sicherheitsanforderungen 17

5.1.1 Funktionale Sicherheitsanforderungen 17

5.1.2 Technische Sicherheitsanforderungen 17

5.1.3 Kontextuelle Sicherheitsanforderungen 18

5.2 Sicherheitsanforderungen im Risikomanagementverfahren 18

5.2.1 Sicherheitsanforderungen aus der Systemdefinition 18

5.2.2 Sicherheitsanforderungen aus der Gefährdungsermittlung und -einstufung 18

5.2.3 Sicherheitsanforderungen aus der Risikoevaluierung 19

Abkürzungsverzeichnis 21

Abbildungsverzeichnis 21

Quellenverzeichnis 22

1 Einleitung

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.

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

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.

Ein Risikomanagementverfahren nach [CSM15] beginnt mit folgenden Verfahrensschritten:

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

Bei Feststellung einer sicherheitsrelevanten und signifikanten Änderung werden eine CSM-konforme Systemdefinition erstellt und potenzielle Gefährdungen identifiziert und bewertet. Die Gefährdungsermittlung soll alle Gefährdungen identifizieren, die aus dem System selbst und seinen Wechselwirkungen mit den interagierenden Systemen erwachsen können. Grundsätzlich werden alle sicherheitsrelevanten Abläufe und Tätigkeiten im System betrachtet und potenzielle Versagensarten einschließlich 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 daraus bei Eintreten der Gefährdung 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.

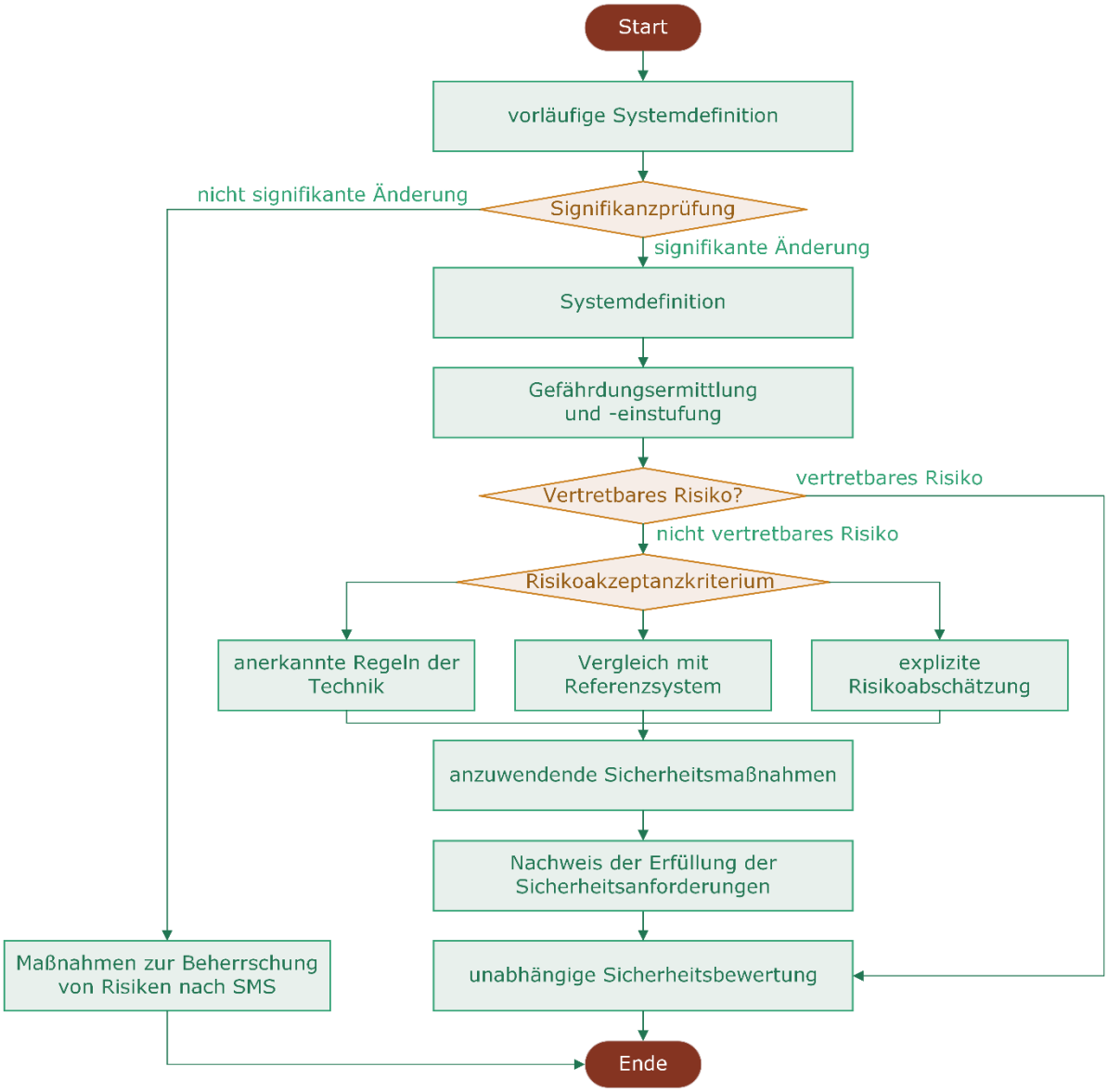


Abbildung 1: Ablauf des Risikomanagementverfahrens nach [CSM15]

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 vonstattengehen kann.

2 Systemdefinition

Eine Systemdefinition kann sowohl produkt- als auch prozessorientiert erfolgen. Änderungen am Eisenbahnsystem werden durch einen Vorschlagenden definiert und eingebracht, dessen Rolle in [CSM15] festgelegt ist. Dieser muss eigenständig 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, welche für das Risikomanagementverfahren gar nicht von Bedeutung sind, zeitaufwändig betrachtet werden.

2.1 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, 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 Mitarbeitergruppen, die keinen Einfluss auf den allgemeinen (sicherheitsrelevanten) Eisenbahnbetrieb haben, müssen nicht zum Bestandteil der produktorientierten Systemdefinition im Sinne des Risikomanagementverfahrens gehören. Sie haben keinen Einfluss auf die Sicherheit im Bahnsystem 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 Mitarbeitergruppe 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 2). Während diese Form der Darbietung eine grundsätzliche Übersichtlichkeit gewährt, kann es insbesondere für Unbeteiligte zu Interpretationsspielräumen kommen.

Anhand der produktorientierten Systemdefinition können folgende Aspekte entsprechend 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).

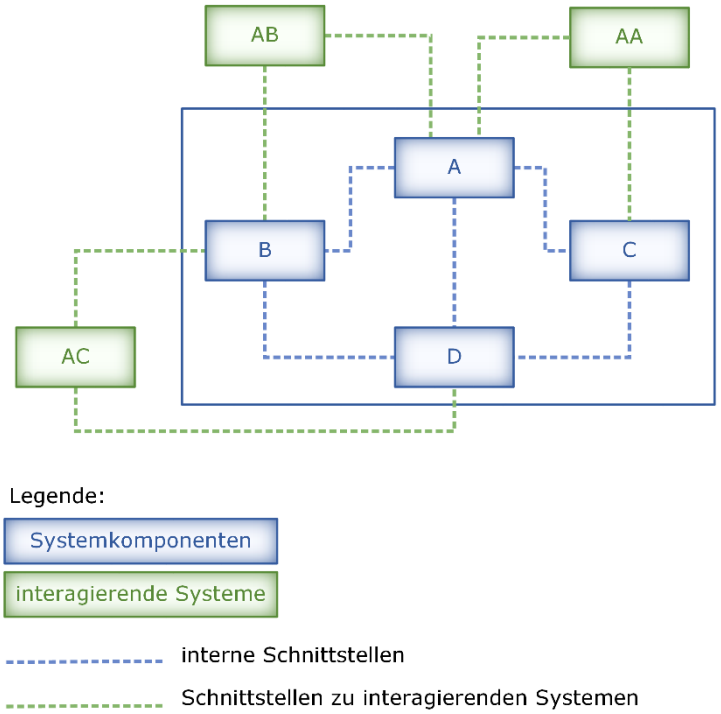


Abbildung 2: Beispielhafte Darstellung einer produktorientierten Systemdefinition

2.2 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 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 Anhang I Punkt 2.1.2 [CSM15] betrachtet werden:

- Funktionen des Systems einschließlich 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 ggf. 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 3 exemplarisch wiedergibt. Auch hier lassen sich Fehlinterpretationen nicht ausschließen.

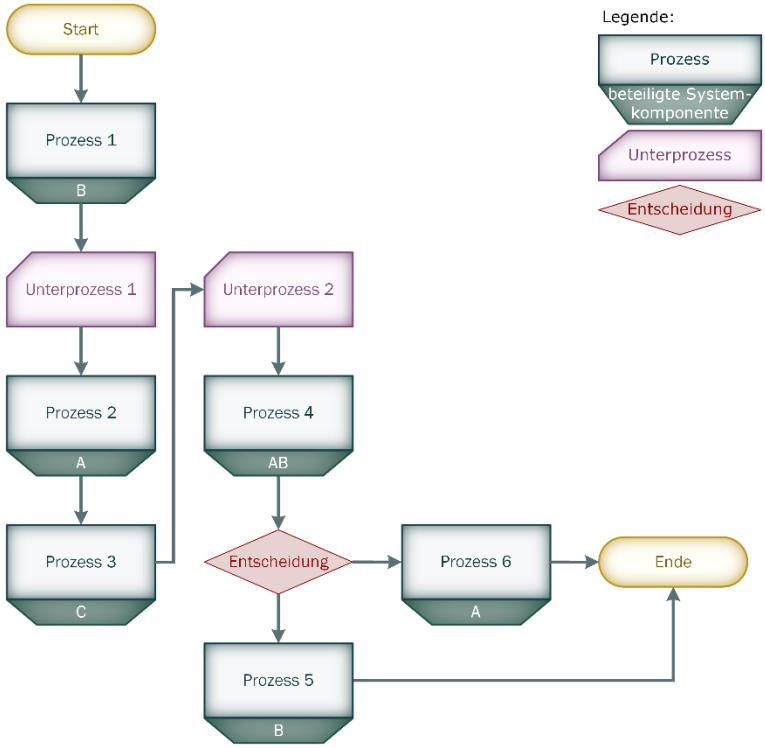


Abbildung 3: Beispielhafte Darstellung einer prozessorientierten Systemdefinition

3 Gefährdungsermittlung und –einstufung

Für die Identifizierung und Bewertung potenzieller Gefährdungen der 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 4 dargestellte Wirkungsmodell.

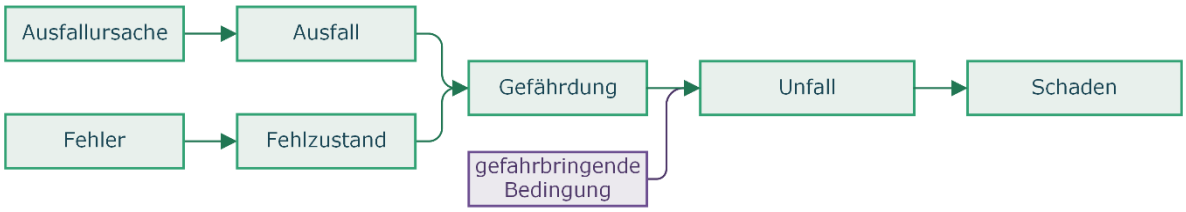


Abbildung 4: Darstellung des Wirkungsmodells

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. Es werden zudem 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 5 dargestellter Ablauf zur Anwendung. Sofern nicht vertretbare Risiken identifiziert werden, erfolgt eine erneute Überprüfung und ggf. Anpassung des betrachteten Systems, was eine abermalige 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.

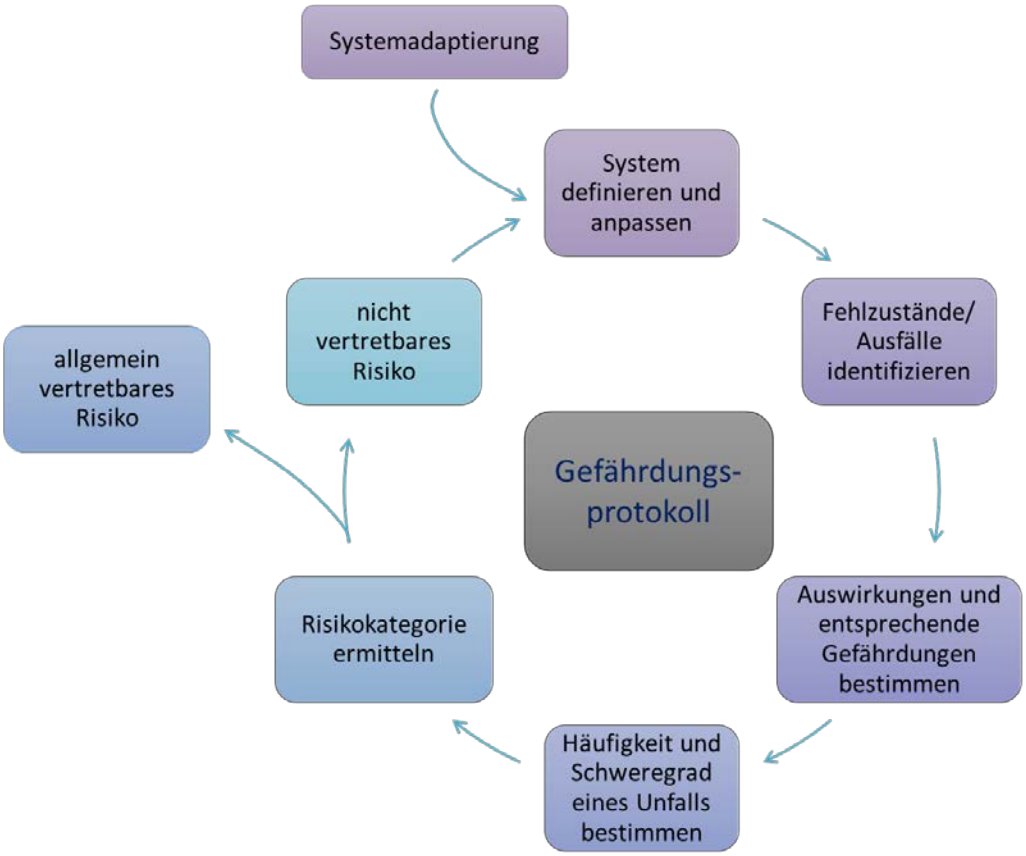


Abbildung 5: Ablauf zur Erstellung des Gefährdungsprotokolls

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 birgt aufgrund der Systemeigenschaften 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 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.

[CSM15] definiert im 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.

4 Risikoevaluierung

Die Risikoevaluierung bildet den eigentlichen Fokus des Risikomanagementverfahrens nach der CSM-Verordnung. Hierzu werden die in [CSM15] definierten Risikoakzeptanzgrundsätze für alle in den vorherigen Schritten identifizierten Gefährdungen angewandt, die sich nicht der Kategorie *allgemein vertretbare Gefährdungen* zuordnen lassen.

Mit der Anwendung der Risikoakzeptanzgrundsätze wird das Ziel 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 6. Nachfolgend erfolgt eine detaillierte Beschreibung des notwendigen Vorgehens der Risikoevaluierung gemäß CSM-Verordnung.

4.1 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 [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]

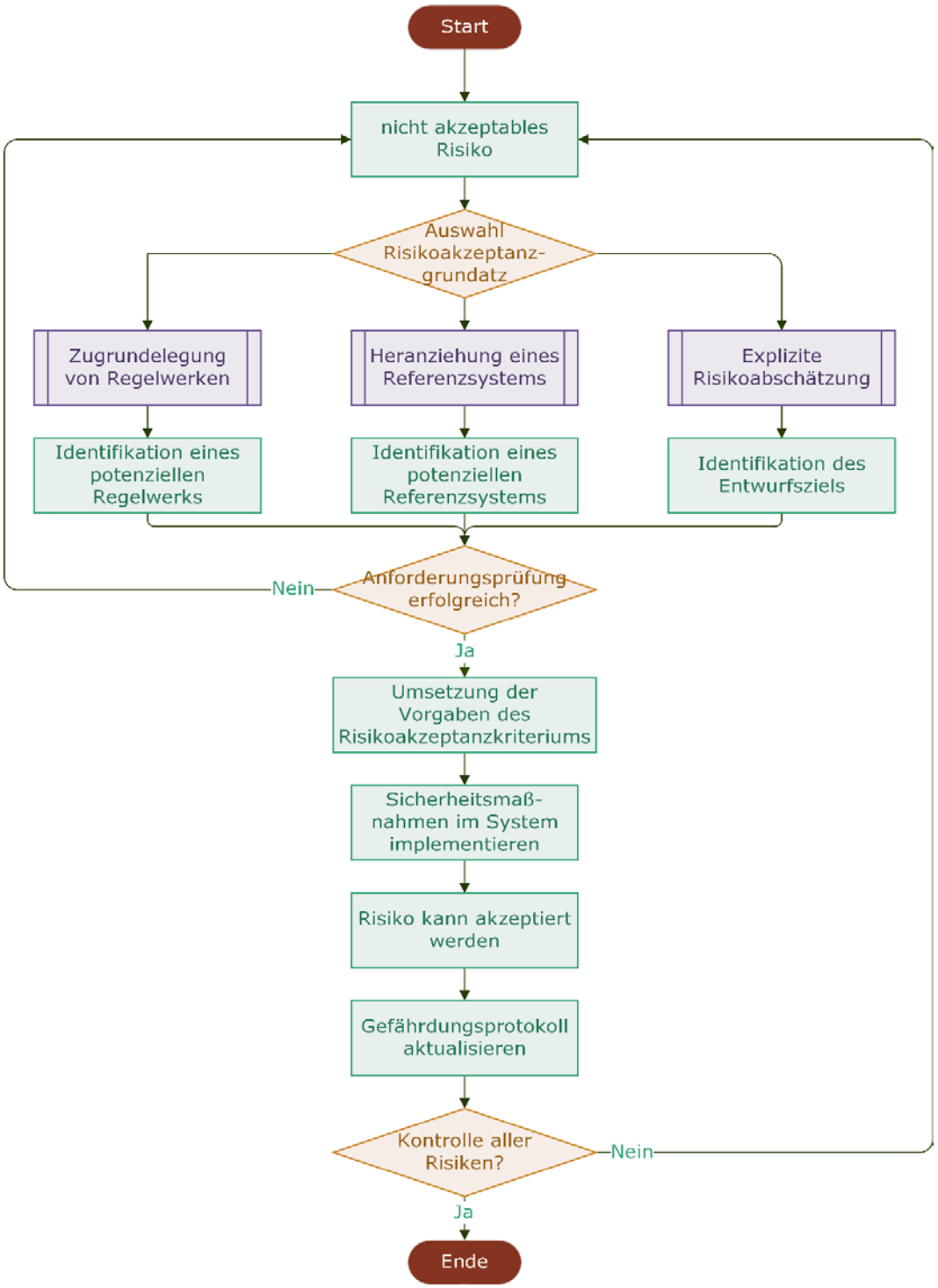


Abbildung 6: Ablauf der Anwendung der Risikoakzeptanzgrundsätze (vereinfachte Darstellung) nach [CSM15]

Für die Nutzung dieses Risikoakzeptanzgrundsatzes wird zunächst ein für die konkret betrachtete Gefährdung relevantes, anerkanntes und zugängliches Regelwerk ermittelt. Dazu gehören beispielsweise 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. Sofern bei Anwendung des herangezogenen Regelwerks die Gefährdung nicht vollumfänglich beherrscht wird, 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 der expliziten Risikoabschätzung zur Risikoreduktion notwendig sein.

4.2 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 eingesetzt werden.

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. Sofern die Gefährdung nicht vollumfänglich im herangezogenen Referenzsystem abgedeckt wird, sind geeignete Maßnahmen zu treffen. Dies kann die weiterführende Anwendung anderer Risikoakzeptanzgrundsätze sein.

4.3 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 (Design Targets).

Die CSM-Verordnung wurde hierzu im Jahr 2015 für „elektrische, elektronische und programmierbare elektronische technische“ [CSM15] Eisenbahnsysteme präzisiert. Dabei werden harmonisierte Entwurfsziele 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]. Ebenfalls definiert die CSM-Verordnung 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] Eisenbahnsysteme 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 kann der Sicherheitsbeitrag der Barrieren bestimmt und die notwendige Ausfallrate des technischen Systems ermittelt werden. Die Berechnungsgrundlage stellt der Leitfaden der ERA (European Union Agency for Railways) zur Anwendung der harmonisierten Entwurfsziele [ERA17] dar.

Das Risiko kann nach Anhang I 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.

5 Bestimmung der Sicherheitsanforderungen

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.

5.1 Kategorien der Sicherheitsanforderungen

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

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

5.1.1 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 quantitative 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.

5.1.2 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.

5.1.3 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.

5.2 Sicherheitsanforderungen im Risikomanagementverfahren

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

5.2.1 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 bei einem 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.

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.

5.2.2 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.

5.2.3 Sicherheitsanforderungen aus der Risikoevaluierung

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

Zugrundelegung von Regelwerken

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

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.

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, das 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.

6 Fazit

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 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.

In der auf der Systemdefinition aufbauenden Gefährdungsermittlung und -einstufung wurden 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.

In der auf diesen Erkenntnissen aufbauenden Risikoevaluierung 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 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.

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

Abkürzung	Definition
CSM	Common Safety Methods (dt.: gemeinsame Sicherheitsmethoden)
DT	Design Targets (dt.: Entwurfs-/Sicherheitsziel)
ERA	European Union Agency for Railways (dt.: Europäische Eisenbahnagentur)
EVU	Eisenbahnverkehrsunternehmen
SMS	Sicherheitsmanagementsystem
SRAC	Safety Related Application Condition (dt.: sicherheitsbezogene Anwendungsbedingung)

Abbildungsverzeichnis

Abbildung 1:Ablauf des Risikomanagementverfahrens nach [CSM15] 7
Abbildung 2:Beispielhafte Darstellung einer produktorientierten Systemdefinition 9
Abbildung 3:Beispielhafte Darstellung einer prozessorientierten Systemdefinition 10
Abbildung 4:Darstellung des Wirkungsmodells 11
Abbildung 5:Ablauf zur Erstellung des Gefährdungsprotokolls 12
Abbildung 6:Ablauf der Anwendung der Risikoakzeptanzgrundsätze (vereinfachte Darstellung) nach [CSM15] 14

Quellenverzeichnis

[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.

[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.

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