Smarte Sicherungslogik für das Stellwerk der nächsten Generation

Zur Erlangung des akademischen Grades Doktor-Ingenieur (Dr.-Ing.) genehmigte Dissertation von M.Sc. Frederik Düpmeier, geb. am 20.12.1987 in Karlsruhe

Erstgutachter: Prof. Dr.-Ing. Andreas Oetting, Darmstadt
Zweitgutachter: Prof. Dr.-Ing. Jörn Pachl, Braunschweig

Tag der Einreichung: 20. April 2022
Tag der Disputation: 7. Juli 2022

TECHNISCHE UNIVERSITÄT DARMSTADT

Institut für Bahnsysteme und Bahntechnik

Düpmeier, Frederik: Smarte Sicherungslogik für das Stellwerk der nächsten Generation
Darmstadt, Technische Universität Darmstadt
Jahr der Veröffentlichung auf Tuprints: 2022
URN: urn:nbn:de:tuda-tuprints-220880
Tag der mündlichen Prüfung: 07.07.2022

Kurzfassung

Kapazitätssteigerungen, eine höhere Pünktlichkeit und eine Steigerung der Rollout-Geschwindigkeit von innovativen Technologien im Bereich der Leit- und Sicherungstechnik gehören zu den zentralen Herausforderungen, vor denen die Eisenbahn als Kernbaustein einer nachhaltigen Mobilität steht. Hierzu wird medial und auch in der Fachwelt der Einführung des Europäischen Zugbeeinflussungssystems ETCS eine wichtige Rolle zugesprochen. Erste Praxiserfahrungen zeigen jedoch, dass die isolierte Einführung von ETCS zur Erzielung der gewünschten positiven Effekte auf den Eisenbahnbetrieb nicht ausreichend ist. Stattdessen muss die Leit- und Sicherungstechnik im Systemverbund weiterentwickelt werden. Neben beispielsweise einer hinreichend genauen Ortung und einer leistungsfähigen Kommunikationstechnologie ist auch eine optimierte Sicherungslogik im Stellwerk, die optimal auf die Anforderung der zukünftigen Systemlandschaft abgestimmt ist, von zentraler Bedeutung. Die Sicherungslogik ist dabei für die sichere und effiziente Zuweisung von Infrastrukturressourcen an Zugfahrten verantwortlich und überwacht sicherheitskritische Zustandsänderungen auf Seiten der Eisenbahninfrastruktur.

Im Rahmen dieser Doktorarbeit wurde ein Ansatz für eine solche „smarte“ Sicherungslogik unter der Bezeichnung „smartLogic“ von Grund auf (Grüne Wiese) systematisch entwickelt. Die smartLogic basiert dabei auf einem generischen und topologieunabhängigen Ansatz, der es unter anderem ermöglicht, Gleise in beliebiger Ausdehnung zu belegen und freizugeben, zusätzliche Sicherheitsanforderungen zur Laufzeit der Sicherungslogik in die Logik zu integrieren und auf Basis der zur Verfügung stehenden Informationen über die aktuelle Betriebssituation risikobasiert über die Zulassung von Zugfahrten zu entscheiden. Parallel zur Arbeit ist eine pretotypische Software-Implementierung der smartLogic im Eisenbahnbetriebsfeld Darmstadt entstanden. Erste Kapazitätsuntersuchungen unter deren Nutzung zeigen, dass signifikante Zeiteinsparungen durch die smartLogic erzielbar sind, die zu einer deutlichen Erhöhung der Kapazität oder der Pünktlichkeit, insbesondere in Knotenbereichen, beitragen können.

Abstract

Capacity increases, improved punctuality, and a faster rollout of innovative technologies in the field of railway control, command and signalling (CCS) are among the main objectives to improve the competitiveness of the railway system as a sustainable mode of transportation. The European Train Control System (ETCS) is arguably the best known innovative technology in the field of CCS. However, early practical experience has demonstrated that an isolated rollout of ETCS within an environment of traditional CCS technologies is not sufficient to achieve the above-mentioned objectives. Instead, the CCS technology must be improved holistically, as an interdependent and interrelated system. In addition to for instance a precise localisation technology and a performant communication technology, an optimized safety logic as the core of the interlocking system is necessary that would be able to interact with the neighbouring systems in an optimal way. The safety logic is responsible for the safe assignment of infrastructure resources to train movements and supervises status changes of infrastructure components.

The main contribution of this doctoral dissertation is a systematic greenfield development of a new “smart” safety logic under the label “smartLogic”. The smartLogic is based on a generic and topology-independent approach. Among other features, it enables the assignment and release of arbitrarily long track sections to trains, the dynamic integration of additional safety requirements into the safety logic during its runtime, and making risk-based decisions based on all available information about the current operating situation. Accompanying the dissertation, a software pretotype was implemented in the Railway Operations Centre Darmstadt (EBD). Initial assessments with the smartLogic pretotype show significant time savings, which can contribute to significant capacity increases and improved punctuality, especially in nodes.

Danksagung

Während der Arbeit an dieser Dissertation konnte ich mich glücklicherweise jederzeit auf die Unterstützung aus dem Kollegen-, Familien- und Freundeskreis verlassen. Für diese wertvolle Unterstützung bin ich sehr dankbar.

Besonders möchte ich meinem Doktorvater, Herrn Prof. Oetting, für die Betreuung während des gesamten Bearbeitungszeitraums danken sowie Herrn Prof. Pachl für die Übernahme des Zweitgutachtens. Ein großer Dank gilt auch Georg Friedrich Bolz für das Korrekturlesen und die fachlichen Diskussionen zu den inhaltlichen Kernkapiteln sowie zusammen mit Werner Iberl und den studentischen Hilfskräften Lars Schulze-Falck, Christopher Bernjus und Carolin Becker für die Entwicklung des Demonstrators im Eisenbahnbetriebsfeld Darmstadt, bei der sich alle Beteiligten mit großem Einsatz eingebracht haben. Mein Dank gilt auch den heutigen und ehemaligen Kollegen am Institut für Bahnsysteme und Bahntechnik der TU Darmstadt, die immer für Fragen offen waren und für ein gutes Arbeitsklima gesorgt haben. Insbesondere möchte ich Sebastian Schön als Mentor und Peter Knuth für die jederzeit schnelle IT-Unterstützung danken.

Für das Gelingen einer umfangreichen wissenschaftlichen Arbeit hat auch die private Unterstützung einen großen Wert. Deshalb gilt mein großer Dank meiner Frau und meinem Sohn, die besonders in der Schlussphase der Bearbeitungszeit häufig auf mich verzichten mussten. Nicht zuletzt möchte ich mich auch bei meinem Vater bedanken, der mich während des gesamten Studiums und auch während der Anfertigung der Doktorarbeit unterstützt und beraten hat.

1 Einleitung

Vorbemerkung:

Während meiner in dieser Arbeit thematisierten Forschung zum Konzept einer neuen Sicherungslogik („**smartLogic**“) seit 2016 haben die Anstrengungen zur Digitalisierung der Leit- und Sicherungstechnik stetig zugenommen. Dabei rückte auch das Thema der Sicherungslogik als ein zentraler Bestandteil der zukünftigen Architektur der infrastrukturseitigen Sicherungstechnik zunehmend in den Fokus. In der Schweiz wurde mit dem Branchenprogramm smartRail 4.0 ein großangelegtes Programm gestartet. Etwas später folgte auch die Deutsche Bahn mit der „Digitalen Schiene“. Auf europäischer Ebene gibt es mittlerweile die Kollaborationsplattform RCA, auf der gemeinsam an der zukünftigen digitalen Bahn gearbeitet wird. Diese Dissertation liefert auf wissenschaftlicher Basis einen Ansatz für die Gestaltung zukünftiger Sicherungslogiken und möchte somit einen Beitrag für die aktuelle Diskussion und Entwicklungsarbeit leisten.

1.1 inhaltliche Hinführung und Aufgabenstellung

Im Zuge des Klimawandels nimmt die Bedeutung des Verkehrsträgers Bahn trotz kurzfristiger Nachfragerückgänge, wie durch die Corona-Pandemie, wieder zu. Durch diesen Trend erhöhen sich auch die Zugzahlen, besonders auf stark nachgefragten Korridoren. Insbesondere in Ballungsräumen ist der Platz für zusätzliche Infrastruktur jedoch begrenzt. Eine Möglichkeit zur Kapazitätserhöhung stellt die intensivere Nutzung der bestehenden Infrastruktur dar.

Physikalisch stößt die Infrastruktur derzeit nicht an ihre Grenzen, denn die Züge verkehren noch mit weit größeren Abständen zueinander als es ihrem Bremsweg entspricht. Dieser Umstand hat technologische Gründe. Der Abstand zwischen den Zügen wird maßgeblich von der Leit- und Sicherungstechnik vorgegeben. Ortungsungenauigkeiten, Latenzzeiten in der Kommunikation und Reaktionszeiten der technischen Komponenten bzw. der beteiligten Personen führen zu Verzögerungen bei der Allokation und Freigabe des Fahrwegs. Zudem ist der Fahrweg immer noch häufig in große räumliche Abschnitte unterteilt, die nur als Ganzes belegt und freigemeldet werden können.

Für die genannten Problemfelder werden derzeit viele innovative Lösungen erforscht oder bereits in der Praxis erprobt. Selbst wenn jedoch die einzelnen Komponenten wie die Ortungs- oder Übertragungstechnologie oder das Zugbeeinflussungs- bzw. -steuerungssystem mit modernen, innovativen Systemen optimiert werden, bleibt die Sicherungslogik im Stellwerk (Stellwerkslogik) zentraler Bestandteil der Eisenbahnsicherungstechnik und hat damit auch einen großen Einfluss auf die Performance des Gesamt-Systems Eisenbahn. So müssen beispielsweise Fahrstraßen nach dem Eingang einer neuen Zugortungsinformation (z. B. Position Reports vom Zug) auch zeitnah (teil-)aufgelöst werden können oder die Sicherungslogik muss flexible Durchrutschwege zulassen können. Ohne die Anpassung der Sicherungslogik können andere innovative Systeme ihre Vorteile häufig nicht ausspielen, weil sie von der Sicherungslogik bei der Ausnutzung ihres Funktionsumfangs eingeschränkt werden. Insbesondere in großen Knoten ist eine flexible Nutzbarkeit der Infrastruktur auch deshalb essenziell, um im Falle verspäteter Züge oder technischer Ausfälle (Folge-)Verspätungen zu vermeiden.

In dieser Arbeit soll aus den oben genannten Gründen eine innovative Sicherungslogik als zentraler Bestandteil der infrastrukturseitigen Sicherungstechnik für die Eisenbahn entworfen werden, die eine Maximierung der Kapazität im Zusammenspiel mit weiteren bevorstehenden oder zu erwartenden

Innovationen im Bereich der Leit- und Sicherungstechnik, wie dem European Train Control System (ETCS), erlaubt. Ein solcher Neuentwurf der Sicherungslogik ist möglich, da heute durch die genannten innovativen Umsysteme und mittlerweile verfügbare Sensortechnik gesicherte Daten ein deutlich genaueres Bild des aktuellen Betriebsgeschehens liefern und eine präzisere Steuerung erlauben als zur Konzeptionszeit der klassischen Stellwerkslogiken.

Um eine Voreingenommenheit beim Erarbeiten innovativer Lösungen durch die bestehende Technik und existierende Ansätze für die Sicherungslogik zu vermeiden, wurde für die Entwicklung der neuen Sicherungslogik „smartLogic“ vorgegeben, dass sie nicht auf der klassischen Stellwerkslogik aufbauen, sondern auf der „Grünen Wiese“ entwickelt werden soll. Zudem soll die in dieser Arbeit zu erarbeitende neue Sicherungslogik so konzipiert werden, dass sie eine schnelle und kostengünstige Umsetzung ermöglicht, um von den Ergebnissen schnell profitieren zu können. Dabei steht angesichts eines Mangels an Planungs- und Zulassungskapazitäten insbesondere auch die Verringerung des Planungs- und Zulassungsaufwandes im Fokus.

1.2 Gliederung der Arbeit

Die ausführliche Herleitung der Vorgehensweise dieser Arbeit erfolgt in Kapitel 3.6. Um den Lesenden bereits zu Beginn einen Überblick über den Aufbau der Arbeit zu geben, findet sich in diesem Kapitel eine kurze Übersicht.

Das 2. Hauptkapitel der Arbeit enthält eine kompakte Darstellung relevanter Grundlagen für das Verständnis der Thematik rund um die Sicherungslogik als Kern der infrastrukturseitigen Sicherungstechnik sowie zu weiteren Themen, die für die Erarbeitung einer neuen Sicherungslogik von Relevanz sind. Zudem werden weitere Arbeiten vorgestellt, die sich mit einer Weiterentwicklung von Stellwerken bzw. der Sicherungslogik beschäftigen. Da der Entwurf der neuen Sicherungslogik in dieser Arbeit jedoch auf der grünen Wiese erarbeitet werden soll (vgl. Kapitel 1.1), dienen diese bisherigen Arbeiten nicht zur Identifizierung einer Forschungslücke, sondern zur späteren Einordnung der Ergebnisse dieser Arbeit in den Kontext des aktuellen Stands des Wissens.

Im 3. Hauptkapitel wird die genaue Zielsetzung der Arbeit ausführlich hergeleitet. Aus der Zielsetzung werden die Anforderungen an die Arbeit bestimmt und eine inhaltliche Abgrenzung vorgenommen. Weiterhin wird die grundsätzliche Methode anhand der Anforderungen ausgewählt und daraus die generelle Vorgehensweise für die gesamte Arbeit hergeleitet.

Mit den Hauptkapiteln 4-8 folgen die inhaltlichen Hauptkapitel gemäß der in Kapitel 3 hergeleiteten Vorgehensweise, die sich grob am Prozess zur Entwicklung sicherheitskritischer Systeme aus EN 50126 orientiert. Demnach wird im 4. Hauptkapitel zunächst auf die Systemdefinition eingegangen. Im 5. Hauptkapitel folgt für das eingegrenzte System eine ausführliche Gefährdungsanalyse, auf deren Basis im 6. Hauptkapitel die funktionalen Anforderungen an die Sicherungslogik bestimmt werden können. In den Hauptkapiteln 7 und 8 folgt die eigentliche Entwicklung der neuen Sicherungslogik, wobei im 7. Hauptkapitel auf die Strukturmodellierung eingegangen und das benötigte Datenmodell bzw. Domänen-Modell hergeleitet wird und im 8. Hauptkapitel die Verhaltensmodellierung erfolgt. Anschließend enthält Hauptkapitel 9 eine kurze Beschreibung des Anwendungsdemonstrators der entworfenen Logik im Eisenbahnbetriebsfeld Darmstadt anhand eines Anwendungsbeispiels der Funktionsweise der smartLogic, bevor abschließend im 10. Hauptkapitel das Fazit der Arbeit und der Ausblick folgen.

1.3 Struktur der inhaltlichen Hauptkapitel 4 bis 8

Zur besseren Orientierung der Lesenden sind die inhaltlichen Hauptkapitel der Arbeit (die Hauptkapitel 4 bis 8) immer nach dem gleichen Schema strukturiert, das dem grundsätzlichen Aufbau wissenschaftlicher Arbeiten folgt. Zunächst wird die Zielsetzung des Hauptkapitels ausführlich beschrieben. Anschließend werden die spezifischen Anforderungen an das Hauptkapitel aus den globalen Anforderungen aus Kapitel 3.5 und der Zielsetzung des jeweiligen Hauptkapitels hergeleitet und daraus eine Methode und Vorgehensweise für das Hauptkapitel entwickelt. Da sich die Systemdefinition im 4. Hauptkapitel an den Vorgaben aus EN 50126 orientiert, wird dort auf eine Methodendiskussion verzichtet.

In den darauffolgenden Kapiteln des jeweiligen Hauptkapitels werden jeweils die zuvor bestimmte Methode angewandt und die Ergebnisse beschrieben. Im drittletzten Kapitel des jeweiligen Hauptkapitels folgt eine Diskussion der Ergebnisse, die im vorletzten Kapitel mit den Erkenntnissen anderer Arbeiten zur jeweiligen Thematik der Hauptkapitel verglichen werden. Dieser Vergleich erfolgt aufgrund des „Grüne Wiese"-Ansatzes der Arbeit bewusst erst am Schluss und nicht am Beginn des Hauptkapitels (siehe zur Begründung auch Kapitel 3.6.2). Als letztes Kapitel eines Hauptkapitels folgt eine Zusammenfassung.

1.4 Hinweise zum Verständnis der Arbeit

Die Arbeit enthält drei nummerierte Gliederungsebenen. Zusätzlich existieren bis zu zwei unnummerierte Gliederungsebenen, die normalerweise unterhalb der dritten nummerierten Gliederungsebene angesiedelt sind, in Ausnahmefällen aber auch direkt Kapitel höherer Gliederungsebenen strukturieren können. Die erste nummerierte Gliederungsebene wird als „***Hauptkapitel***" bezeichnet, die zweite als „***Kapitel***" und die dritte als „***Unterkapitel***". Die erste unnummerierte Gliederungsebene wird als „***Abschnitt***" bezeichnet, die zweite unnummerierte Gliederungsebene als „***Unterabschnitt***".

Rückwärtsverweise in der Arbeit werden unabhängig von der nummerierten Gliederungsebene, auf die sie verweisen, mit „vgl. Kapitel [Nr]" eingeleitet. Vorwärtsverweise werden mit „siehe Kapitel [Nr]" eingeleitet. Oftmals wird auf die globalen Anforderungen aus Kapitel 3.5 und die zugrundeliegenden Zieldimensionen referenziert. Um den Text nicht zu überfrachten, wird dabei zum Teil auf einen Verweis auf Kapitel 3.5 verzichtet. Die globalen Anforderungen und Zieldimensionen haben deshalb jeweils eine Kurzbezeichnung, die in Tab. 7 fett gedruckt ist. Die Verweise darauf werden im Text *kursiv* geschrieben. Verweise zu anderen Inhalten von Tabellen oder Listen aus demselben Kapitel wie der Verweis werden zur schnellen Orientierung ebenfalls *kursiv* geschrieben.

Einige Begriffe, die in der Arbeit verwendet werden, können von verschiedenen Personen oder in verschiedenen Kontexten unterschiedlich verstanden werden. Deshalb ist der Arbeit ein umfangreiches Glossar angefügt, in dem diese Begriffe für die Verwendung in der Arbeit definiert werden. Glossar-Begriffe werden an der Stelle, wo sie im Text inhaltlich eingeführt werden, **fett** gedruckt. Weitere Begriffe, die im Text inhaltlich eingeführt werden, aber nicht im Glossar vorkommen, werden an der Stelle ihrer Einführung ***kursiv*** gedruckt. Bei ***kursiv*** eingeführten Begriffen handelt es sich in der Regel um Fachbegriffe, die in externen Quellen (z. B. ETCS-Spezifikation) eindeutig definiert werden und somit keinen Interpretationsspielraum erlauben.

Abkürzungen werden beim ersten Auftreten eingeführt. Um die Verständlichkeit der einzelnen Kapitel zu erleichtern, können sie zudem an geeigneten Stellen erneut eingeführt werden.

In der Arbeit wird gemäß den aktuell gültigen Sprachregelungen das generische Maskulinum verwendet.[1]

Diese Dissertation beinhaltet Erkenntnisse, die im Verlauf der Bearbeitung der Promotion bereits auf Konferenzen vorgestellt wurden. Hierzu sind die Veröffentlichungen [Düpmeier 2018], [Düpmeier & Oetting 2018], [Düpmeier 2020] und [Düpmeier 2021] entstanden. Der Demonstrator wurde auf Basis der Ergebnisse dieser Arbeit von einem Projektteam aus technischen Mitarbeitern und studentischen Hilfskräften entwickelt.

Während der Anfertigung der Disseration wurden die in Tab. 1 gelisteten erfolgreich abgeschlossenen studentischen Arbeiten mit thematischem Bezug zum Promotionsthema betreut oder mitbetreut, deren Ergebnisse naturgemäß in unterschiedlichem Maße die eigenen Überlegungen beeinflusst haben, ohne dass dies durch einzelne Zitate abgebildet werden kann.

Tab. 1: Übersicht betreuter Abschlussarbeiten

Autor	Titel	Abschluss
Stefan Dillmann	A Formal Model of a Railway Operating Procedure with Moving Blocks and Dynamic Speed Profile	10/2017
Kostantin Koch	Untersuchung von Verhaltensmöglichkeiten eines automatisierten, regelbasierten Stellwerks bei Abweichungen vom Regelbetrieb	05/2018
Patrick Rauscher	Entwicklung eines Prüf-Verfahrens für eine formale Eisenbahn-Sicherungslogik	06/2018
Felix Grau	Entwicklung konkreter Testfälle auf einer geeigneten Eisenbahninfrastruktur für das Testen einer formalisierten Eisenbahnsicherungslogik	11/2018
Andreas Kleimann	Konzeptentwicklung und Implementierung eines Ortungsaggregators für die Ortung von Modellzügen im Eisenbahnbetriebsfeld und eines Korrekturalgorithmus für die Fahrzeugsteuerung des Eisenbahnmodells	11/2020
Diego Merkel	Auswirkungen einer regelbasierten Sicherungslogik auf die Kapazität von ausgewählten Eisenbahnbetriebssituationen	10/2021

[1] Hintergrund ist nicht, dass der Autor eine Abneigung gegenüber dem Gendern verspürt, sondern dass er bei der Erstellung der Arbeit nicht durchgängig auf das Gendern geachtet hat und deswegen aus Gründen der Einheitlichkeit ganz auf das Gendern verzichten möchte.

2 Grundlagen, Stand des Wissens

In diesem Hauptkapitel werden bestehende Technologien und Spezifikationen sowie aktuelle Projekte und Forschungsansätze vorgestellt, die für die vorliegende Forschungsarbeit von Relevanz sind. Dabei liegt der Fokus auf dem Bereich der infrastrukturseitigen Eisenbahnsicherungstechnik, dessen zentraler Bestandteil die in dieser Arbeit zu entwickelnde Sicherungslogik sein soll. Weiterhin werden Modellierungswerkzeuge vorgestellt, die für die Modellierung der Logik von Relevanz sind.

Diese Dissertation ist in einem Zeitraum von über fünf Jahren entstanden, in dem die zugrundeliegende Thematik in Fachkreisen und in der Öffentlichkeit immer mehr an Bedeutung gewonnen hat („Digitale Schiene“). Aus diesem Grund haben sich während der Bearbeitungszeit zahlreiche (z. T. parallele) (Forschungs-)Initiativen und Projekte weiterentwickelt. Im vorliegenden Hauptkapitel werden daher auch Arbeiten vorgestellt, die erst im Laufe der Bearbeitungszeit der Dissertation entstanden sind. Diese Vorgehensweise wurde mit dem Ziel gewählt, die vorliegende Dissertation möglichst vollständig in die Forschungslandschaft zum Zeitpunkt der Abgabe der Arbeit einzuordnen.

Gewöhnungsbedürftig dürfte für geübte Leser wissenschaftlicher Arbeiten sein, dass der Bezug zur Literatur im weiteren Verlauf der Arbeit nicht zu Beginn eines Hauptkapitels erfolgt. Dies liegt in der expliziten Anforderung an die Forschungsarbeit begründet, das Thema der Sicherungslogik von der „Grünen Wiese“ kommend zu betrachten (siehe Kapitel 1.1 und 3.6.2). Es soll daher gerade nicht die bestehende Literatur als Ausgangspunkt der Entwicklungen dieser Arbeit genommen werden. Stattdessen findet sich am Ende der inhaltlichen Hauptkapitel jeweils ein Unterkapitel „Vergleich mit alternativen Ansätzen“, in dem die wesentlichen Unterschiede des in dieser Arbeit vorgestellten Forschungsansatzes zu den im 2. Hauptkapitel vorgestellten bestehenden oder sich in der parallelen Entwicklung befindlichen Ansätzen erläutert werden.

Zunächst beschäftigt sich Kapitel 2.1 mit den Grundlagen der bisherigen Stellwerkslogiken im deutschsprachigen Raum, um ein Grundverständnis für die klassische Sicherungstechnik zu erhalten. Aus Ressourcengründen wird nur kurz auf Unterschiede ausländischer Logiken eingegangen. Kapitel 2.2 erweitert dann den Blick auf die anderen Komponenten der infrastrukturseitigen Sicherungstechnik und erläutert aktuelle Innovationen in diesem Bereich, da diese Komponenten voraussichtlich die Umsysteme der zu erarbeitenden Sicherungslogik bilden. In Kapitel 2.3 erfolgt ein Benchmark, in dem andere Ansätze aus der Praxis und aus der Forschung zur Weiterentwicklung der Sicherungslogik vorgestellt werden. Einige dieser Entwicklungen werden seit einigen Jahren unter dem gemeinsamen Framework der Reference CCS Architecture (RCA) entwickelt, der sich ein eigenes Kapitel (Kapitel 2.4) widmet.

Unter anderem da die Sicherungslogik die sichere Zuweisung der Infrastrukturressourcen an die Fahrzeuge sicherstellt und auch Statusänderungen der Infrastruktur überwacht, ist eine digitale Abbildung der Infrastruktur erforderlich. Kapitel 2.5 stellt deshalb verschiedene bestehende Infrastrukturdatenmodelle vor. Anschließend werden in Kapitel 2.6 Methoden für den sicherheitskritischen Entwurf der smartLogic analysiert.

Das Hauptkapitel schließt in Kapitel 2.7 mit einer Zusammenfassung zum aktuellen Stand des Wissens.

2.1 Stand der Technik: Bisherige Stellwerkslogiken im deutschsprachigen Raum

Das vorliegende Kapitel geht auf die bisherigen Evolutionsstufen der Stellwerkstechnik ein. Dieser Hintergrund ist erforderlich, um Potenziale einer neuen Sicherungslogik als Kernbestandteil der

infrastrukturseitigen Sicherungstechnik abschätzen zu können (siehe Kapitel 3). Als Quellen für die Aussagen im vorliegenden Kapitel und für eine eingehendere Betrachtung wird auf die einschlägige Fachliteratur verwiesen: [Maschek 2018], [Pachl 2020], [Pachl 2016] sowie [Theeg et al. 2020].

2.1.1 klassische Sicherungsprinzipien zur Vermeidung der Grundgefährdungen

Stellwerke dienen dazu, den Fahrweg für Züge einzustellen und zu sichern sowie den Fahrzeugen die Benutzung der Infrastruktur zu erlauben. Sie werden vom Fahrdienstleiter (Fdl) oder Weichenwärter (Ww) gemäß den Vorgaben des betrieblichen Regelwerkes bedient. Für die Sicherungsaufgabe enthalten Stellwerke eine interne Logik, die **Stellwerkslogik**, auf deren Basis die Stellwerke Handlungen des Bedieners zulassen oder verhindern. Die Stellwerkslogik wird im Zuge sich wandelnder Aufgabenteilung zwischen den einzelnen Komponenten der infrastrukturseitigen Sicherungstechnik in neueren Arbeiten häufig auch „**Sicherungslogik**“ genannt. Die technische Sicherung des Bahnbetriebs ist insbesondere notwendig, da sich der Mensch alleine als nicht zuverlässig genug erwiesen hat.

Klassische Stellwerkslogiken sind darauf fokussiert, die bekannten Grundgefährdungen im Bahnbetrieb – Entgleisung und Kollision mit einem anderen Eisenbahnfahrzeug – zu verhindern. Bei Entgleisungen stehen dabei die Ursachen überhöhte Geschwindigkeit und Umstellen eines Fahrwegelements unter dem Zug im Vordergrund. Bei Kollisionen werden Auffahrunfälle, Frontalzusammenstöße und Flankenfahrten unterschieden (vgl. sicherungstechnische Anforderungen 1. Ordnung in [Trinckauf 2013]).

Zu jeder dieser Grundgefährdungen hat sich im deutschsprachigen Raum ein Sicherungsprinzip herausgebildet. Abb. 1 enthält eine Übersicht der Grundgefährdungen und der zugehörigen Sicherungsprinzipien, die bei MASCHEK „**Schutzfunktionen**“ [Maschek 2009]) genannt werden. Dabei wird in Deutschland traditionell zwischen Bahnhofsbereichen und der freien Strecke unterschieden. In anderen Ländern wird zum Teil eine andere Unterteilung verwendet oder komplett auf eine Unterteilung verzichtet.

	Gefährdung (Schutzziel)	**Betriebsstelle**	**freie Strecke**
	Auffahrunfall (Folgefahrschutz)	Prüfen auf Freisein durch **Hinsehen**, Bahnhofsblock	Prinzip des **Streckenblock**s
	Gegenfahrt (Gegenfahrschutz)	Prüfen auf Freisein durch **Hinsehen**, Bahnhofsblock	Prinzip der **Erlaubnis**
	Flankenfahrt (Flankenschutz)	Verschluss der **Flankenschutz-elemente**	*keine Weichen vorhanden*
	Umstellen eines Fahrweg-elements unter dem Zug (Entgleisungsschutz)	**Verschluss** der Fahrweg- und DWeg-Elemente	*keine Weichen vorhanden*
	Überhöhte Geschwindigkeit (Entgleisungsschutz)	Signalisierung der richtigen Geschwindigkeit	

Abb. 1: Hauptgefährdungen und zugehörige klassische Sicherungsprinzipien
Quelle: Institut für Bahnsysteme und Bahntechnik, TU Darmstadt

Um die Sicherheit zu gewährleisten, darf die Technik einem Zug (bzw. dem Tf des Zuges) die Befahrung eines Infrastrukturabschnitts nur erlauben, wenn alle zur Erfüllung der aufgeführten Sicherungsprinzipien erforderlichen Voraussetzungen erfüllt sind. Als Mittel zur Übermittlung einer solchen **Fahrerlaubnis** haben sich in den meisten Fällen optische Signale durchgesetzt. Deshalb spricht man vom Prinzip der Signalabhängigkeit. Die Fahrtstellung des (Haupt-)Signals und die *signalisierte Geschwindigkeit* sind von den Voraussetzungen für eine sichere Befahrung des nachfolgenden Gleisabschnitts abhängig.

Das Hauptsignal (Startsignal) erlaubt dem Triebfahrzeugführer (Tf) unter Beachtung der signalisierten Geschwindigkeit (zur Vermeidung der Gefährdung „*überhöhte Geschwindigkeit*“) über den nachfolgenden Gleisabschnitt bis zum nächsten Hauptsignal (Zielsignal) zu verkehren. Befinden sich in diesem Gleisabschnitt Weichen, ist deren Lage aufgrund der Signalabhängigkeit fest definiert. Ein solcher Gleisabschnitt mit Weichen oder anderen beweglichen Fahrwegelementen wird als **Fahrstraße** bezeichnet. Neben dem Gleisabschnitt, dessen Befahrung mit der Fahrtstellung des Startsignals bis zum Zielsignal gestattet wurde, der häufig als **Fahrweg** bezeichnet wird[2] (vgl. [Widmann 2022]), gehören zur Fahrstraße auch **Flankenschutzelemente**, die zur Vermeidung der Gefährdung „*Flankenfahrt*“ dienen, sowie Elemente im Durchrutschweg.

Der ***Durchrutschweg*** ist die Schutzstrecke hinter dem Zielsignal, die erforderlich ist, damit sich der Zug mit einer betrieblich praktikablen Geschwindigkeit an das Zielsignal annähern kann, ohne im Falle eines unerwarteten Passierens des Zielsignals sich selbst oder andere Zugfahrten zu gefährden. Das Ende des für die Zugfahrt gesicherten Gleisabschnitts wird auch als **Gefahrpunkt** bezeichnet.

In Topologie-Bereichen mit Weichen oder anderen beweglichen Fahrwegelementen müssen diese Elemente zur Vermeidung der Gefährdung „*Umstellen eines Fahrwegelements unter dem Zug*“ gegen Umstellen gesichert werden, solange einer Eisenbahnfahrzeugbewegung die Befahrung des Elements erlaubt ist. In Deutschland und weiteren Ländern wird dafür auf das Prinzip des ***Fahrstraßenverschlusses*** zurückgegriffen. Alle Elemente einer Fahrstraße werden vor oder mit Fahrtstellung des Signals verschlossen sowie die gesamte Fahrstraße festgelegt. Die Festlegung darf erst nach Durchfahrt des Zuges (oder Halt bei Einfahrt in einen Bahnhof) wieder aufgelöst und der Verschluss aufgehoben werden. Bei neuern Stellwerken ist jedoch die schrittweise Auflösung einzelner Elemente der Fahrstraße möglich, sobald diese Elemente nach einer Befahrung wieder als frei gemeldet werden (***Teilfahrstraßenauflösung***). Ist eine Fahrstraße festgelegt, lässt sie sich vor der Durchfahrt des Zuges ohne manuellen Eingriff in die Sicherungslogik mittels einer sogenannten „***Hilfshandlung***“ nicht mehr verändern. Im britischen System tritt die Fahrstraßenfestlegung üblicherweise erst mit der Annäherung des Eisenbahnfahrzeugs an das Signal ein. Dies hat den Vorteil, dass eine Rücknahme der Fahrstraße unproblematisch noch solange möglich ist, bis sich der Zug tatsächlich im Bremswegabstand vor dem Beginn der Fahrstraße befindet.

Zur Gewährleistung des *Folgefahrschutzes* zur Vermeidung der Gefährdung „*Auffahrunfall*“ gibt es international verschiedene Lösungen. Mittlerweile hat sich das ***Fahren im festen Raumabstand*** weitgehend durchgesetzt. Hierfür wird die Gleistopologie in feste Abschnitte (***Blockabschnitte, Streckenblock***) aufgeteilt, die jeweils von Signalen begrenzt sind. Das Signal am Beginn des Blockabschnitts kann technisch gesichert die Fahrt erst dann erlauben, wenn der nachfolgende Abschnitt frei ist. Hierfür muss der vorausfahrende Zug die Zugschlussstelle passiert haben, seine Vollständigkeit bestätigt sein und das Signal am Ende des Blockabschnitts Halt zeigen. Um unnötige Bremsungen zu vermeiden, muss das Signal am Beginn des Blockabschnitts bereits auf Fahrt stehen,

[2] wobei der Begriff „Fahrweg“ in verschiedenen Fachkontexten leicht unterschiedlich verwendet wird, siehe Glossar

bevor der Zug den Beginn des Bremsweges auf dieses Signal erreicht hat. Aufgrund der langen Bremswege bei der Eisenbahn gilt daher die grobe Faustregel, dass ca. zwei Blockabschnitte zwischen zwei Zügen für einen flüssigen Bahnbetrieb frei sein müssen.

Das Prüfen auf Freisein kann im Bereich der freien Strecke durch die Blocklogik erfolgen. Bei eingleisigen Strecken existiert zusätzlich eine Abhängigkeit, die verhindert, dass von beiden Seiten in das Streckengleis eingefahren werden kann, um die Gefährdung „*Gegenfahrt*“ zu verhindern. In Deutschland wird hierfür das ***Erlaubnisprinzip*** genutzt. Das Erlaubnisprinzip stellt sicher, dass eine Strecke jeweils nur aus einer Richtung befahren werden kann, bis die Erlaubnis gewechselt wird und ein Befahren in der anderen Richtung erlaubt ist. Im Bahnhofsbereich ist dagegen auch mit nicht vollständig gesicherten Fahrzeugbewegungen zu rechnen. Aus diesem Grund musste früher das ***Freisein durch Hinsehen*** geprüft werden. Heute existieren meist infrastrukturseitige ***Gleisfreimeldeanlagen*** in Form von Achszählern oder Gleisstromkreisen.

Die Einhaltung des übermittelten Signalbegriffs inkl. übermittelter Geschwindigkeit kann durch Zugbeeinflussungssysteme (***Automatic Train Protection*** (**ATP**)) oder umfangreichere Zugsteuerungssysteme (***Automatic Train Control*** (**ATC**)) überwacht werden. Klassische in Deutschland verwendete Zugbeeinflussungssysteme sind die **Punktförmige Zugbeeinflussung (PZB)** sowie die **Linienförmige Zugbeeinflussung (LZB)**. In Kapitel 2.2.2 wird auf das neuere ATC „European Train Control System“ (ETCS) näher eingegangen.

Neben den hier vorgestellten Sicherungsprinzipien zur Vermeidung der in Abb. 1 aufgeführten Hauptgefährdungen besitzen heutige Stellwerke noch weitere Sicherungsprinzipien, um zusätzlichen Gefährdungen zu begegnen. Hierzu gehört zum Beispiel die ***Bahnübergangssicherungstechnik*** zur Vermeidung von Kollisionen mit anderen Verkehrsteilnehmern an Bahnübergängen oder die Vorgabe niedriger Geschwindigkeiten bei Einfahrt in ein Stumpfgleis. Auch die hinter diesen weiteren Sicherungsprinzipien stehenden funktionalen Sicherheitsanforderungen werden bei der Identifizierung der funktionalen Anforderungen an die neu zu entwickelnde Logik im 6. Hauptkapitel der heutigen Stellwerkstechnik zur Sicherung der Vollständigkeit in einem systematischen Verfahren berücksichtigt. Eine detaillierte Beschreibung aller dieser Sicherungsprinzipien würde an dieser Stelle der Arbeit allerdings den Rahmen sprengen und ist zum Verständnis der nachfolgenden Hauptkapitel auch nicht erforderlich.

Damit der Betrieb im Störungsfall von Teilen der Sicherungstechnik nicht gänzlich zum Erliegen kommt, enthalten Stellwerke zudem in der Regel **Rückfallebenen**. Diese ermöglichen die Nutzung eines Teils der Schutzfunktionen des Stellwerks, während ein anderer Teil durch die menschlichen Bediener übernommen werden muss.

2.1.2 bekannte Stellwerkstechniken

Die Stellwerkslogik kann mittels verschiedener Techniken im Stellwerk implementiert werden. Zunächst wurden mechanische Umsetzungen in mechanischen und elektromechanischen Stellwerken realisiert. Anschließend kamen Implementierungen mit elektronischen Relais auf. Seit den 1980er-Jahren existieren auch Stellwerkslogiken, die in Software abgebildet sind und in rechnergestützten Stellwerken laufen, die als elektronische Stellwerke (ESTW) bezeichnet werden.

Die Logik ist dabei im Wesentlichen auf zwei verschiedene Arten implementiert. Bei sogenannten „***Fahrstraßenstellwerken***“ sind alle sicherungstechnischen Abhängigkeiten für jede signaltechnisch gesicherte Fahrmöglichkeit (Fahrstraße) einzeln fest vorgeplant und entsprechend realisiert. Mechanische und elektromechanische Stellwerke sind Fahrstraßenstellwerke, aber auch Teile der Relaisstellwerke und der ESTW. Relaisstellwerke und ESTW sind darüber hinaus häufig als

sogenannte „***Spurplanstellwerke***“ ausgeführt. Bei Spurplanstellwerken sind die Abhängigkeiten nicht im Einzelnen fest vorgegeben. Stattdessen wird die Gleistopologie (der Spurplan) im Falle von Relaisstellwerken mittels generischer Baugruppen nachgebildet, so dass die Abhängigkeiten aus dem Spurplan heraus identifiziert werden. Im ESTW werden die Baugruppen mit Datenobjekten abgebildet und die Abhängigkeiten entsprechend mit einem Suchalgorithmus identifiziert.

Auch bei Spurplanstellwerken sind die Freiheitsgrade begrenzt. Fahrstraßen bilden sich zwischen den vorgeplanten festen Start- und Zielpunkten (i. d. R. Hauptsignale) immer auf die gleiche Weise. Nur bestimmte, vorprojektierte Abweichungen existieren, wie verkürzte Durchrutschwege für bestimmte Einfahrgeschwindigkeiten. Das aktuelle Betriebsgeschehen wird nur vereinzelt, z. B. bei Zwieschutzweichen, berücksichtigt.

Durch Unfälle und technologische Entwicklungen wurden die Anforderungen an den Funktionsumfang der Sicherungslogik und die Beschaffenheit der technischen Umsetzung immer wieder erweitert. So muss sichergestellt werden, dass die Stellwerkslogik auch im Falle von Störungen die Sicherheit gewährleistet. Hieraus resultiert zum einen das Prinzip der Fehleroffenbarung, das besagt, dass eine Fehlfunktion nicht unbemerkt bleiben darf. Zum anderen stellt das „Fail Safe“-Prinzip sicher, dass das Stellwerk nach einem Fehler in einen sicheren Zustand übergeht. Dieser Übergang in einen sicheren Zustand bedeutet in der Regel, dass zunächst im betroffenen Bereich keine Fahrzeugbewegung mehr zugelassen wird und bereits erteilte Fahrerlaubnisse wieder zurückgenommen werden, z. B. indem das Signal auf Halt fällt. Erst nach dem Klären der Ursache der Störung und geeigneten Ersatzmaßnahmen durch den Fdl oder Ww, der damit eine zusätzliche Sicherheitsverantwortung übernimmt, kann der Betrieb wieder aufgenommen werden.

2.2 aktuelle technologische Entwicklungen im Rahmen des digitalen Bahnbetriebs

Die in dieser Arbeit zu entwickelnde Sicherungslogik entsteht als Bestandteil der Eisenbahn-Leit- und Sicherungstechnik (LST) im Kontext aktueller technologischer Entwicklungen im Bereich ihrer Umsysteme. Die Europäische Union (EU) hat für die Zukunft der LST eine Strategie veröffentlicht, in der sie einige zentrale Entwicklungen nennt, die sie als sogenannte „Game Changer“ bezeichnet [ERA 2015, S. 6]. Es handelt sich um Technologien, die aus Sicht der EU zu einer deutlichen Steigerung des Marktanteils des Verkehrsträgers Schiene beitragen können. Auch die RCA-Gruppe, ein Zusammenschluss von Eisenbahninfrastrukturunternehmen (EIU) hat in einem Whitepaper solche Zukunftstechnologien gelistet [EUG & EULYNX 2018] [EUG & EULYNX 2019] (siehe auch Kapitel 2.4). Im Bereich der Umsysteme der Sicherungslogik geben Zukunftstechnologien und Bestandstechnik zumindest einen technologischen Rahmen für die Entwicklung der Sicherungslogik vor, in der sich die neu zu entwickelnde Sicherungslogik verorten muss[3]. Das vorliegende Kapitel gibt daher einen kompakten Überblick über diese Zukunftstechnologien.

Zu den sogenannten „Game Changers“ gehören ein modernes Kommunikationssystem (FRMCS) (hochverfügbar und mit geringen Latenzzeiten), eine präzise und hochverfügbare Ortung, Automatic Train Operation (ATO, ab Grade of Automation 2), ETCS Level 3 [ERA 2015] und eine einheitliche Hardwareplattform, die unabhängig von den Software-Komponenten zugelassen werden soll [EUG & EULYNX 2019]. Als Voraussetzung für das Zielbild wird ETCS mit Führerstandsignalisierung angesehen [EUG & EULYNX 2019].

[3] Die Funktionsweise der Umsysteme wird dabei im Sinne des „Grüne Wiese“-Ansatzes (vgl. Kapitel 1.1 und siehe auch Kapitel 3.6.2) bei der Entwicklung der Sicherungslogik nicht als unveränderlich betrachtet, sollte aber auch nicht gänzlich unbetrachtet bleiben, um eine realistische Umsetzungsmöglichkeit für die zu entwickelnde smartLogic sicherzustellen.

2.2.1 die Vision des Digitalen Bahnbetriebs / Digitale Schiene

Durch den Megatrend „Industrie 4.0“ befindet sich die Eisenbahnbranche derzeit in einer Aufbruchsstimmung, die alle Teile des Systems Bahn umfasst. So hat unter anderem die Deutsche Bahn AG (DB) eine großangelegte Digitalisierungsoffensive bis 2030 unter dem Titel „**Digitaler Bahnbetrieb**“ angekündigt [DB AG 2018]. Eines der Hauptziele ist dabei die Steigerung der Leistungsfähigkeit der Eisenbahninfrastruktur.

Bei der Erreichung dieses Ziels steht vor allem die Leit- und Sicherungstechnik im Fokus, die unter dem Titel „**Digitale Schiene**“ modernisiert werden soll (vgl. www.digitale-schiene-deutschland.de). In der Diskussion sind insbesondere Level 2 des Europäischen Zugsicherungssystems ETCS (siehe Kapitel 2.2.2) und Automatic Train Operation (ATO) (siehe Kapitel 2.2.7). ATO soll dabei aufbauend auf ETCS über ein genaueres Abfahren optimaler Fahrkurven zum Ziel von bis zu 20 % mehr Zügen auf den bestehenden Schienen beitragen [ebd.]. Als weitere Maßnahme sollen sogenannte „**digitale Stellwerke**“ **(DSTW)** eingeführt werden (siehe Kapitel 2.2.5). In einer Machbarkeitsstudie wurde eine Rollout-Strategie für die Komponenten ETCS und DSTW bis zur Mitte des 21. Jahrhunderts entworfen [McKinsey & Company 2018].

In die Vision des Digitalen Bahnbetriebs reiht sich auch diese Dissertation zur Entwicklung einer neuen Sicherungslogik („smartLogic“) ein.

2.2.2 European Train Control System (ETCS)

Das Europäische Zugsicherungssystem **European Train Control System (ETCS)**[4] bildet als zentraler Bestandteil des ***European Rail TrafficManagement Systems (ERTMS)*** die Basis der zukünftigen Eisenbahnsicherungstechnik an der Schnittstelle zwischen der fahrzeugseitigen und der infrastrukturseitigen Sicherungstechnik. Die Ausrüstung mit ETCS ist von der EU für bestimmte Fahrzeugneubeschaffungen und neue Infrastrukturprojekte vorgeschrieben [Europäische Kommission 2016]. Die Einführung von ETCS wird deshalb mittlerweile in immer mehr Ländern innerhalb und außerhalb der EU geplant bzw. vorangetrieben [Unife 2021].

Primärquelle für die folgenden Beschreibungen sind die **System Requirements Specification (SRS)**, die von der Europäischen Eisenbahnagentur ERA veröffentlicht werden [ERA 2016]. Es sei zudem auf die Sekundärquellen [Stanley 2011], [Trinckauf et al. 2020] und [Schnieder 2021] verwiesen.

ETCS ersetzt die Funktion der bisherigen Zugbeeinflussungssysteme (auch als Altsysteme oder in der ETCS-Terminologie als ***Class B-Systeme*** bezeichnet) wie PZB und LZB in Deutschland. Primäre Aufgabe von ETCS ist sicherzustellen, dass die Fahrzeuge innerhalb der Parameter der von der infrastrukturseitigen Sicherungstechnik zugewiesen Fahrerlaubnis (**Movement Authority (MA)**) bleiben.

Versionen und Levels

Es gibt mehrere Versionen der ETCS-Spezifikationen, die im Laufe der Entwicklung entstanden sind. Die Ausführungen in diesem Kapitel beziehen sich auf Baseline 3 mit Version 3.6.0 der SRS.

Die ETCS-Spezifikationen unterscheiden verschiedene Ausrüstungsstufen der Infrastruktur (ETCS-Levels). Bei ETCS Level 1 erfolgt die Übermittlung der Fahrerlaubnis von der infrastrukturseitigen Sicherungstechnik an die Fahrzeuge in der Regel über im Fahrweg verbaute

[4] Neue Glossar-Begriffe sind fett, andere neu eingeführte Begriffe sind kursiv geschrieben (vgl. Kapitel 1.4). Bei Letzteren handelt es sich in diesem Unterkapitel vorwiegend um Begriffe, die nur im ETCS-Kontext gebräuchlich sind und dort klar definiert sind, so dass eine gesonderte Erläuterung im Glossar als nicht nötig angesehen wurde.

Datenbalisen.[5] Diese Datenbalisen sind zum Teil schaltbar und es ist möglich, von jedem heute existierenden Stellwerk den angelegten Signalbegriff abzugreifen und mittels der Balise zu übertragen.

Bei ETCS Level 2 erfolgt die Übermittlung dagegen über Funk. Kommunikationspartner des Fahrzeuges ist hier das sogenannte „***Radio Block Center*** **(RBC)**“ (bei der DB auch „***ETCS-Zentrale***“ genannt), welches wiederum mit dem Stellwerk in Verbindung steht. Das RBC kann vom Stellwerk die Aufgabe des Folgefahrschutzes übernehmen.

Da Level 1 in Deutschland vor allem dort verbaut wird, wo ETCS zusammen mit älteren Stellwerken betrieben werden soll, mit denen Level 2 nicht kompatibel ist (vgl. Tab. 1 in [BMVI 2017b]), wird in dieser Arbeit davon ausgegangen, dass ETCS Level 2 die Grundlage für die zukünftige Schnittstelle der neuen Sicherungslogik zum Fahrzeug bildet (siehe Kapitel 4.5.2). Zudem ist Level 2 oder höher bzw. ein äquivalentes System auf Basis der Führerstandsignalisierung auch die anvisierte Version für die RCA und den Digitalen Bahnbetrieb der DB [DB AG 2018b; DB AG 2018; EUG & EULYNX 2018]. Daher beziehen sich die folgenden Ausführungen sofern nicht anders gekennzeichnet auf ETCS Level 2.

ETCS Level 3 entspricht Level 2 mit dem Unterschied, dass zusätzlich zur Fahrerlaubnis auch die vollständige Ortung der Fahrzeuge inkl. Zugvollständigkeitsmeldung über Funk erfolgen kann, so dass infrastrukturseitige Gleisfreimeldeanlagen wie Achszähler oder Gleisstromkreise in der Theorie entfallen können und theoretisch das Fahren im wandernden Raumabstand (Moving Block, siehe Kapitel 2.2.3) möglich wird. Bis heute gibt es allerdings außer auf Regionalstrecken mit homogenen Fahrzeugeinsatz noch keine wirtschaftliche Anwendung von ETCS Level 3. Da die Nachrichten für die Kommunikation zwischen Fahrzeug und infrastrukturseitiger Sicherungstechnik bei ETCS Level 2 und 3 identisch sind, ist für diese Arbeit eine weitere Differenzierung zwischen diesen beiden Levels nicht zielführend.

Betriebsmodi

Ein ETCS-Fahrzeug befindet sich zu jedem Zeitpunkt in einem ETCS-Betriebsmodus. Für eine vollständige Beschreibung der Betriebsmodi wird auf die Literatur verwiesen. An dieser Stelle soll jedoch auf einige Details eingegangen werden, die für die Entwicklung der Sicherungslogik relevant sind.

Der normale Betriebsmodus für Zugfahrten ist ***Full Supervision*** **(FS)**. Im Modus FS garantiert das Fahrzeug mit hinreichender Sicherheit innerhalb der Parameter der MA zu bleiben, d. h. alle Vorgaben der MA, insbesondere der übermittelte Gefahrpunkt und das erlaubte Geschwindigkeitsprofil werden überwacht. Die Führungsgrößen werden im Führerstand angezeigt. Für den Betrieb in ETCS Level 1 wurde mit ***Limited Supervision*** **(LS)** ein weiterer Betriebsmodus für den regulären Fahrbetrieb von Zugfahrten geschaffen, auf den an dieser Stelle mit derselben Begründung wie zum Ausschluss von ETCS Level 1 im vorigen Abschnitt nicht näher eingegangen werden soll.

Für Rangierfahrten ist der Modus ***Shunting*** **(SH)** vorgesehen. Es können Vorgaben für den Rangierbereich sowie eine einzuhaltende Höchstgeschwindigkeit übermittelt werden, die von ETCS überwacht werden.

Für Rückfallebenen gibt es mehrere Betriebsmodi. Hierbei wird insbesondere zwischen ***On Sight*** **(OS)** und ***Staff Responsible*** **(SR)** unterschieden. Letzterer Modus entspricht einer Befehlsfahrt, wobei auch hier eine Maximalgeschwindigkeit und bestimmte Fahrtbegrenzungen, die zum Beispiel über Balisen

[5] Es gibt weitere Übertragungswege, auf die hier mangels Relevanz für die vorliegende Arbeit nicht weiter eingegangen werden soll.

übermittelt werden können, überwacht werden. Im Gegensatz dazu entspricht On Sight einer Fahrt mit Full Supervision mit dem Unterschied, dass kein freies Gleis garantiert wird und somit auf Sicht gefahren werden muss. Alle anderen Parameter werden aber wie bei FS überwacht.

ETCS kann auch den Stillstand des Fahrzeugs überwachen (z. B. Modus ***No Power*** **(NP)**).

Position Report und Zugdaten

Zur Ortung sendet das Fahrzeug in regelmäßigen Abständen oder nach Anforderung Positionsmeldungen (ETCS-***Position Report***). Der Abstand kann von der Infrastruktur vorgegeben werden. Im Position Report kann angegeben werden, ob eine gesicherte Information darüber vorliegt, ob der Zug vollständig ist oder nicht. Weiterhin werden Informationen zum aktuellen Zustand des Fahrzeugs bzw. des Zuges (oder allgemeiner ausgedrückt: der überwachten Fahrzeugbewegung) übermittelt (aktuelles Level, aktueller Modus etc.).

Es wird dabei immer die gefahrene Distanz relativ zum letzten Ortungsbezugspunkt, der gemäß der aktuellen Spezifikation eine Balisengruppe ist (***Last Known Balise Group*** **(LRBG)**), und die aktuelle Ortungsungenauigkeit angegeben. Zur Ortung muss auch die Fahrtrichtung bekannt sein. Die meisten Balisen sind daher Teil einer Balisengruppe, in der anhand der Nummerierung der Balisen innerhalb der Gruppen die Fahrtrichtung bestimmt werden kann. Wenn ein Fahrzeug neu aufrüstet und die Fahrtrichtung unbekannt ist, muss es sich die Richtung zunächst „erfahren“, in dem es im Modus SR bis über die nächste Balisengruppe fährt. In Bahnhöfen sind unter anderem deshalb zahlreiche Balisengruppen vorhanden.[6]

Neben dem Position Report können vom Fahrzeug auch die Zugdaten abgefragt werden, wie z. B. die Zugart. Diese Zugdaten basieren jedoch derzeit häufig auf Eingaben des Tf, die potenziell fehleranfällig sein können.

Positionsberechnung

Die ETCS-Spezifikation kennt verschiedene Positionsangaben, die vor allem für die Berechnung der Bremskurven durch das ETCS-Bordgerät von Bedeutung sind. Das ***Estimated Front End*** bezeichnet den Punkt, an dem die Zugspitze nach interner Ortungsrechnung sich wahrscheinlich gerade befindet. Das ***Max Safe Front End*** bezeichnet dagegen den Punkt, den nach der internen Ortungsberechnung zuzüglich Sicherheitszuschlag die Zugspitze mit hinreichender Wahrscheinlichkeit maximal bereits erreicht haben kann, und das ***Min Safe Front End*** den Punkt, den die Zugspitze mit hinreichender Wahrscheinlichkeit mindestens bereits passiert haben muss. Das Estimated Front End wird zur Berechnung der Betriebsbremskurven verwendet und das Max Safe Front End für die sicherheitskritischen Berechnungen, wie die Berechnung der Notbremskurve vor einem Gefahrpunkt.

Weiterhin existiert das ***Min Safe Rear End***, aus welchem mittels der sicheren Zuglänge die Position berechnet wird, die von der entsprechenden Fahrzeugbewegung auf jeden Fall bereits passiert wurde. Es wird u. a. für die Berechnung des Zeitpunkts zum Beschleunigen nach einer temporären Langsamfahrstelle oder einem Weichenbereich verwendet. ***Estimated Rear End*** und ***Max Safe Rear End*** können ebenfalls berechnet werden, erfüllen derzeit aber keine Funktion.

Abb. 2 zeigt verschiedene Fahrzeugpositionen aus dem ETCS-Regelwerk. Die Position wird immer relativ zum letzten Ortungsreferenzpunkt (***Last Relevant Balise Group*** (**LRBG**)) angegeben. Das sichere Gesamtausmaß der Fahrzeugbewegung und damit das Ausmaß der notwendigen Belegung der Infrastruktur wird durch das Min Safe Rear End und das Max Safe Front End gebildet. Im

[6] Und um die Ortungsungenauigkeit zu verringern.

Position Report wird allerdings das Estimated Front End übertragen, aus dem das Max Safe Front End mittels standardisierter Formel berechnet werden kann. Statt der Position des Zugschlusses wird die Zuglänge im Position Report übertragen, zusammen mit einer Information, ob diese Länge als sicher angenommen werden kann und die Zugintegrität sicher gewährleistet ist (vgl. Aussage oben zur Angabe der sicheren Zugintegrität).

Abb. 2: ETCS-Fahrzeugpositionsangaben in Bezug zum letzten Ortungsreferenzpunkt (LRBG)
[Eigene Darstellung nach dem ETCS-Regelwerk [ERA 2016]]

Fahrerlaubnis (MA)

Mit der MA erlaubt die infrastrukturseitige Sicherungstechnik einem Fahrzeug auf der Infrastruktur zu verkehren. Die wichtigsten Informationen der MA sind die Zielpunkte. Es wird unterschieden zwischen der End of Authority und der Supervised Location.

Die ***End of Authority*** **(EoA)** ist Bestandteil jeder Fahrerlaubnis und wird relativ zum letzten bekannten Ortungsreferenzpunkt (LRBG) angegeben. ETCS berechnet die Betriebsbremskurven so, dass das Fahrzeug in der Regel vor diesem Punkt mit der angenommenen Position der Zugspitze (Estimated Front End) zum Halten kommt. Die EoA stellt also für das Fahrzeug den für das Ziel der Bremsung anzusteuernden Punkt dar. Die Zielgeschwindigkeit muss nicht Null sein. Ist sie größer als Null, wird der Zielpunkt als ***Limit of Authority*** **(LoA)** bezeichnet. Die LoA kann auch befristet werden. Kann das Fahrzeug die LoA nicht vor Ablauf dieser Zeit passieren, muss es anhalten.

Abb. 3 veranschaulicht die genannten Punkte.

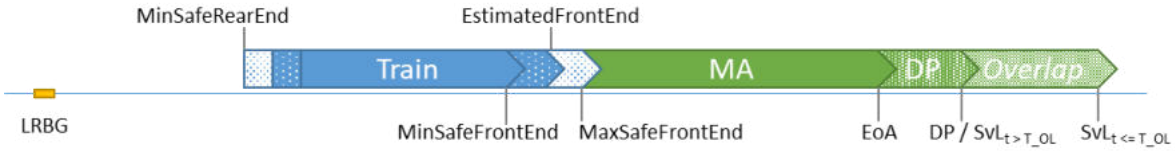


Abb. 3: ETCS-Positions- und Zielpunkte in Abhängigkeit vom letzten Ortungsreferenzpunkt (LRBG)
Bis zum Ablauf des Auflösetimers (T_OL) befindet sich die SvL am Ende des OL, danach springt sie an den DP.
[Eigene Darstellung]

Hinter der EoA bzw. LoA kann dem Fahrzeug ein zusätzlicher sicherer Fahrweg zugesichert werden, um schnellere Anfahrten zu ermöglichen. Das Ende dieses Fahrwegs wird als ***Supervised Location*** **(SvL)** bezeichnet. ETCS stellt sicher, dass das Fahrzeug mit hinreichender Sicherheit die SvL nicht passiert. ETCS berechnet dazu die flacheren Notbremskurven auf die SvL und überwacht die Annäherung mit der sicheren Zugspitze (Max Safe Front End), bei der zur angenommenen Position der Zugspitze die Ortungsungenauigkeit hinzuaddiert ist.

Die SvL kann entweder als permanent gültiger ***Danger Point*** **(DP)** übermittelt werden oder in Form eines ***Overlaps*** **(OL)**, der in der Regel nach Ablauf einer angegebenen Zeitspanne seine Gültigkeit verliert. Für den Overlap kann deshalb ein Auflösetimer mit der Dauer ***T_OL*** definiert werden, abhängig von einem Auflösepunkt, bei dessen Befahrung der Timer gestartet wird. Die SvL befindet sich, falls ein Overlap vorhanden ist, bis zu dessen Auflösung am Ende dieses Overlaps und ansonsten am Danger Point. Das Fahrzeug muss seine Bremsung so berechnen, dass es vor dem Danger Point

zum Stehen kommt, wenn es nicht ausschließen kann, dass es den Overlap nach Ablauf von T_OL benötigen würde. Die SvL kann auch am Ort der EoA liegen, wenn weder ein gesonderter Danger Point noch ein Overlap angegeben ist.

Es ist auch möglich, die Fahrerlaubnis in mehrere ***Segmente*** zu unterteilen. Für die Segmente kann ein Timer gesetzt werden, um abzubilden, dass das befahrene Segment nach Passieren einer festgelegten Position nur für eine bestimmte Zeit zur Verfügung steht. Der Timer wird gestoppt, wenn das Fahrzeug einen definierten Ort erreicht. Kann diese Zeit nicht eingehalten werden, muss das Fahrzeug vor Beginn des Segments bremsen. Die Segmente sind nur für diesen Zweck vorhanden und dürfen nicht mit den unabhängig definierbaren Segmenten des Geschwindigkeitsprofils, Neigungsprofils oder Modusprofils verwechselt werden.

An der EoA kann eine sogenannte ***Release Speed*** erlaubt werden. Das Fahrzeug kann dann nach Unterschreiten der Release Speed die Bremskurve mit dem Estimated Front End verlassen und mit der Release Speed weiterverkehren, bis die Notbremskurve erreicht ist. Diese Funktion ist aufgrund der Ortungsungenauigkeit vorgesehen, um dem Tf die Annäherung an den Zielpunkt (z. B. ein Hauptsignal oder eine Blechtafel) auf Sicht zu ermöglichen. Das Fahrzeug überwacht neben dem Einhalten der Notbremskurve auch das Einhalten der Release Speed und dass das Fahrzeug mit dem Min Safe Front End nicht die EoA passiert.

Neben den Zielpunkten und zugehörigen Parametern kann die MA mit weiteren Informationen präzisiert werden. Mittels des ***Static Speed Profile*** **(SSP)** wird das infrastrukturseitig zulässige Geschwindigkeitsprofil übermittelt, welches das Fahrzeug bzw. die Fahrzeugbewegung neben ihrer eigenen zulässigen Höchstgeschwindigkeit überwacht. Weiterhin können mit einem ***Mode Profile*** Moduswechsel nach festgelegten gefahrenen Distanzen (ebenfalls relativ zur LRBG) vorgegeben werden.

Dem Fahrzeug können auch Informationen über die Strecke mitgeteilt werden, die diesem unter anderem eine bessere Berechnung der Bremskurven ermöglichen. Hierzu gehört beispielsweise das Gradientenprofil, Informationen zur Haftreibung der Schienen, aber auch Informationen zum Überhöhungsfehlbetrag, die Position von Bahnsteigen etc. Weiterhin können sicherheitsrelevante Vorgaben, z. B. zur für die Befahrung notwendigen Fahrzeugausrüstung oder zum Vornehmen notwendiger Handlungen, wie Pfeifen, übermittelt werden.

Insgesamt können mit der MA zahlreiche Parameter übermittelt werden, die sehr flexible Vorgaben für Fahrerlaubnisse zulassen. In den praktischen Umsetzungen von ETCS werden allerdings bisher nur wenige Parameter tatsächlich genutzt.

Einordnung der Kapazitätspotenziale von ETCS für den digitalen Bahnbetrieb

Da das Heben von Kapazitätspotenzialen eine wichtige Zielsetzung der Vision der digitalen LST ist, wird im Folgenden kurz darauf eingegangen, welchen Beitrag gemäß der Literatur ETCS hierzu leisten kann und welche Voraussetzungen dafür existieren.

Häufig wird ETCS in seiner kapazitativen Wirkung in Level 1 mit der PZB und in Level 2 mit der LZB mit CIR-ELKE II gleichgesetzt (vgl. z. B. [BMVI 2017b]). Es gibt jedoch zahlreiche Unterschiede, die auch in der Praxis zu spürbaren Kapazitätsunterschieden führen, wobei sich die Einführung von ETCS sowohl positiv als auch negativ auswirken kann, abhängig vom Anwendungsszenario und den eingesetzten Umsystemen (vgl. z. B. [Büker 2017; Wirth & Schöbel 2020; Goers et al. 2019; Schmidt 2019; Kümmling & Wanstrath 2021]).

ETCS bietet sowohl in Level 1 als auch in Level 2 bzw. 3 die Möglichkeit, wesentlich mehr Informationen an die Fahrzeuge zu übermitteln als die genannten Class B-Systeme. Somit können in

der Theorie sowohl die Umsysteme in den Fahrzeugen als auch die Umsysteme auf Seiten der infrastrukturseitigen Sicherungstechnik ein detaillierteres Bild der Realität erhalten. Dieser Umstand bringt jedoch erst einen Vorteil, wenn die Umsysteme diese zusätzlichen Informationen auch effektiv nutzen können (z. B. Nutzung differenzierter Angaben des Überhöhungsfehlbetrags [Staffel 2020]). Es sind auch „deutlich kürzere Durchrutschwege ohne Begrenzung der Einfahrgeschwindigkeit“ möglich, „wenn auf eine Doppelausrüstung mit konventioneller Leit- und Sicherungstechnik verzichtet wird“ [Kümmling & Wanstrath 2021, S. 17].

Weiterhin hat die Berechnungsformel der Bremskurven einen entscheidenden Einfluss auf die durch ETCS erzielbare Kapazität (vgl. z. B. [Fehlauer & Kahl 2019; Feltz et al. 2017; Goers et al. 2019; Schnieder 2021]). Häufig sind diese Bremskurven trotz der genauen verfügbaren Informationen flacher als bei Altsystemen. Kapazitätserhöhende Bremskurvenmodelle stellen daher einen der in der Einleitung zu diesem Unterkapitel genannten „Game Changer“ dar [ERA 2015, S. 6].

Eine weitere wichtige Einflussgröße in Bezug auf die Kapazität von ETCS Level 2 bzw. 3 ist die Ortungsungenauigkeit. Eine präzise Ortung ist daher für das Heben von ETCS-Kapazitätspotenzialen unabdingbar [Trinckauf et al. 2020, S. 86–88; Schnieder 2021, S. 71–73]. Auch „Funklaufzeiten und die Verarbeitungszeiten der ETCS-Fahrzeuggeräte [spielen] eine Rolle.“ [Kümmling & Wanstrath 2021, S. 17]

Aus den in diesem Abschnitt genannten Gründen wird in der Fachöffentlichkeit vermehrt auch die Notwendigkeit einer angepassten Stellwerkslogik bzw. Sicherungslogik diskutiert (vgl. z. B. [Schmidt & Grabowski 2018; Kuttig-Trölenberg et al. 2021]) bzw. wurden Projekte zum Entwurf einer solchen Logik ins Leben gerufen (siehe Kapitel 2.3).

2.2.3 Moving Block, Hochleistungsblock und das Erfordernis präziserer Ortung

ETCS Level 3 unterstützt das Konzept des Fahrens im wandernden Raumabstand (engl. „Moving Block“) (vgl. Kapitel 2.2.2). Im Vergleich zum klassischen Fahren im festen Raumabstand, bei dem die Zugfolge mittels örtlich fester Blöcke erfolgt, geht beim Moving Block der Sperrzeitbestandteil der Fahrzeit im Blockabschnitt gegen Null, so dass theoretisch die Züge im absoluten Bremswegabstand (zuzüglich Sicherheitszuschläge und Kommunikationszeiten) aufeinander folgen könnten [Pachl 2020 S. 19f und 32; Büker et al. 2020]. Praktisch bleibt jedoch durch verschiedene diskrete Einflussgrößen wie Übertragungsintervallen bei der Übertragung von Fahrerlaubnis- und Ortungsinformationen sowie Zuschläge für Ortungsungenauigkeiten ein Restbestandteil der Fahrzeit im Blockabschnitt bestehen, auch wenn dieser nicht mehr an feste räumliche Blöcke gebunden ist (siehe auch *Hochleistungsblock*, unten).

Für eine gewinnbringende Nutzung des „Moving Block“-Verfahrens sind demnach eine präzise Zugortung und eine kontinuierliche Kommunikation der Zugposition sowie der Zugvollständigkeit erforderlich. Bisher gibt es nur auf einzelnen Strecken mit homogenem Betriebsprogramm realisierte Anwendungsfälle, da insbesondere noch keine organisatorisch und finanziell praktikable Technologie zur Sicherung der Zugvollständigkeit bei einem hinreichenden Anteil der verkehrenden Züge (zumindest auf Mischverkehrsstrecken) gefunden wurde. Zudem ist der praktische Kapazitätsvorteil durch Moving Block aus mehreren Gründen strittig [Pachl 2020, S. 32].

Zum einen reduzieren – wie oben angesprochen (zumindest derzeit noch) – eine ungenaue Zugortung und längere Kommunikations- und Systemverarbeitungszeiten durch die erforderliche regelmäßige Übermittlung von Zugposition und Zugvollständigkeit im Vergleich zur Nutzung klassischer, ortsfester Gleisfreimeldeanlagen wie Gleisstromkreise und Achszähler den Vorteil durch die wegfallenden Fahrzeit im Blockabschnitt wieder beträchtlich [Büker et al. 2019; Hennig et al. 2021]. Zum anderen

ist ein Folgen im absoluten Bremswegabstand nur solange möglich, wie keine Weiche (oder ein anderes Fahrwegelement, welches umgestellt werden muss,) passiert wird. Grund ist, dass für den Stellvorgang Zeit benötigt wird und sich das umzustellende Fahrwegelement zu diesem Zeitpunkt nicht im Bremsweg des nachfolgenden Zuges befinden darf, falls während des Umstellens ein Problem auftritt (vgl. z. B. [Büker et al. 2020]). Auch ein Halt des vorderen Zuges, z. B. an einem Haltepunkt, stellt ein Problem für den nachfolgenden Zug dar, wenn dieser im absoluten Bremswegabstand folgt.

Als oft diskutierte Alternative zu Moving Block gibt es daher Konzepte, bei denen die ortsfesten Blöcke um weitere Blöcke ergänzt werden, die in engem räumlichen Abstand aufeinander folgen („***Hochleistungsblock***“) und mit (***Teilblöcke***) oder ohne (***virtuelle Blöcke***) ortsfester Gleisfreimeldung ausgestattet sind (vgl. z. B. [Hennig et al. 2021]). Wenn die zusätzlichen Blöcke mit einer Gleisfreimeldeanlage ausgestattet sind, müssen die darauf verkehrenden Fahrzeuge, im Gegensatz zur Zugvollständigkeitserkennung beim Moving Block, nur mit Führerstandsignalisierung ausgerüstet sein. Die zusätzlichen Gleisfreimeldeanlagen bei Teilblöcken im Vergleich zu virtuellen Blöcken verursachen allerdings Kosten und stellen potenzielle Störungsquellen dar.

Trotz der oben genannten Einschränkungen sind Kapazitätsvorteile durch Moving Block in bestimmten Situationen denkbar. Zum Beispiel, wenn der nachfolgende Zug schneller ist als der vorausfahrende, aber zusätzliche Halte hat (z. B. schneller Regionalzug folgt auf Güterzug). In diesem Fall könnte der schnelle Regionalzug nach einem Halt immer bis zum absoluten Bremswegabstand auf den vorausfahrenden Güterzug aufrücken, bevor er zum nächsten Halt wieder bremsen würde.

Ein weiterer Vorteil von Moving Block ergibt sich dadurch, dass die Freimeldung der Infrastruktur nicht mehr an feste Punkte geknüpft ist, an denen eine Gleisfreimeldegrenze vorhanden ist. Es können daher beliebige Bestandteile der Gleistopologie belegt und freigemeldet werden. Hierdurch entsteht zusätzliche Flexibilität ohne zusätzliche Komplexität. Ein weiterer Vorteil ist die Eliminierung möglicher Störquellen in Form der Elemente der Gleisfreimeldeanlagen, die gerade bei Hochleistungsblöcken zahlreich sind, und damit eine Vereinfachung des Systems. Beispielsweise vereinfacht sich mit Moving Block auch die Planung und Zulassung, da keine Planung der Blöcke mehr erfolgen muss (vgl. z. B. [Schmidt 2019]).

Für die Zukunft kann davon ausgegangen werden, dass durch die zunehmende Ausstattung von Fahrzeugen mit Fahrzeugbussystemen oder Einzelwagen-Ortungsmöglichkeiten, z. B. für Zwecke der präventiven Instandhaltung der Fahrzeuge, für immer mehr Fahrzeugbewegungen die Zugvollständigkeit fahrzeugseitig festgestellt werden kann. Zudem ist es wahrscheinlich, dass präzisere Ortungsmöglichkeiten durch die Fusion von Sensordaten (vgl. z. B. [Winter et al. 2018]) oder FiberOpticSensing (vgl. z. B. [Zeilinger 2019]) marktfähig werden. Aus diesem Grund kann angenommen werden, dass „Moving Block“-Verfahren in Zukunft eine größere Rolle spielen werden. Aufgrund der hohen Umrüstungskosten und der zahlreichen Marktteilnehmer auf Seiten der EVUs und der Wagenhalter ist allerdings auf absehbare Zeit nicht davon auszugehen, dass alle Fahrzeuge „Moving Block“-fähig sein werden. Daher sollte außerhalb von homogen betriebenen Nebenstrecken sowohl von Moving Block-fähigen als auch nicht Moving Block-fähigen Fahrzeugen ausgegangen werden.

2.2.4 Future Railway Mobile Communication System (FRMCS)

Wie bereits in Kapitel 2.2.2 und 2.2.3 angeklungen, basiert der ETCS-Modus „Full Supervision“ auf dem Prinzip der Führerstandsignalisierung, wobei in den höheren Ausrüstungslevels 2 und 3 als Übertragungsweg die Funkkommunikation vorgesehen ist. Hierfür wird ein leistungsfähiges Kommunikationssystem benötigt. In ERTMS ist dafür GSM-R vorgesehen, welches jedoch bei einer

hohen Anzahl an Fahrzeugen, mit denen gleichzeitig kommuniziert werden muss, an die Grenze seiner Leistungsfähigkeit stößt. Zudem ist davon auszugehen, dass sich durch weitere zu erwartende Zukunftstechnologien die Anforderungen an die Bandbreite, die Anzahl der Kanäle und die Latenzzeit weiter erhöhen. Es ist auch davon auszugehen, dass GSM-R etwa um 2030 abgängig sein wird (vgl. zum Thema [Brand & Nänni 2019]).

Aus diesen Gründen wird derzeit über das Nachfolgesystem von GSM-R beraten. Die Technologie steht dabei zum Zeitpunkt des Verfassens dieser Arbeit noch nicht endgültig fest. Daher existiert die generische Bezeichnung „***Future Railway Mobile Communication System***“ (FRMCS).

Aus Sicht der Sicherungslogik, die in dieser Arbeit erarbeitet werden soll, kann angenommen werden, dass unabhängig von der konkreten Technologie in naher Zukunft ein FRMCS zur Verfügung stehen wird, welches die Kommunikation mit ausreichend vielen Fahrzeugbewegungen bei ausreichend niedriger Latenz und ausreichend hoher Bandbreite ermöglicht. Deshalb wird auf eine vertiefte Vorstellung möglicher FRMCS-Technologien verzichtet.

2.2.5 EULYNX und Digitale Stellwerke (DSTW)

Eine weitere Zukunftstechnologie, die einen wichtigen Bestandteil der Strategie des Digitalen Bahnbetriebs darstellt, ist ein neues modulares Schnittstellen-System für die Komponenten der infrastrukturseitigen Sicherungstechnik, das von der Deutschen Bahn „**Digitale Stellwerke**“ **(DSTW)** genannt wird (vgl. z. B. [Bührsch et al. 2022]). Die DB hatte hierzu zunächst ein Projekt mit dem Titel „NeuPro“ vorangetrieben [Leining & Elsweiler 2013], das mittlerweile auf europäischer Ebene von einer Gruppe von Eisenbahninfrastrukturunternehmen (EIU) weitergeführt wird, die sich als **EULYNX** bezeichnet (vgl. https://eulynx.eu/).

Ziel ist es, die bisherigen Stellwerksfunktionen zu modularisieren und zwischen den einzelnen Komponenten standardisierte Datenschnittstellen zu etablieren. **Feldelemente** wie Weichen und Signale, die sich unmittelbar am Gleis befinden, sind nicht mehr fest mit dem Stellwerkskern verbunden, sondern verfügen über eigene Steuerungssysteme, sogenannte „**Object Controler**“ **(OC)**, die über eine ringförmige Datenleitung miteinander und mit dem Stellwerkskern verbunden sind. Hierdurch entstehen neue Herausforderungen im Bereich der IT-Sicherheit, es bieten sich aber auch mehrere Vorteile (basierend u. a. auf [Bührsch et al. 2022, S. 225]):

- Die standardisierten Schnittstellen zu den Feldelementen ermöglichen, Feldelemente und Stellwerkskerne verschiedener Hersteller miteinander zu verbinden. Hierdurch können die Lebenszeiten der einzelnen Komponenten voneinander entkoppelt werden. Durch die Standardisierung sollen außerdem die Produktionskosten sinken.
- Feldelemente können einfacher und zustandsbasiert gewartet und ausgetauscht werden. Die Diagnose wird erleichtert.
- Deutlich größere Stellentfernungen sind möglich. Zukünftig ist geplant, je Netzbezirk der DB Netz AG nur noch einen Technikstandort zu unterhalten [Bührsch & Schlichting 2018, S. 218]. Theoretisch ist zudem die Zuordnung der Feldelemente zur zentralen Sicherungslogik/Stellwerkskern veränderbar. Bei Ausfall des Stellwerkskerns könnte das Feldelement somit theoretisch einem anderen Stellwerkskern zugeordnet werden. Dies könnte auch insgesamt für eine größere Flexibilität, beispielsweise in Hinblick auf die Überwachung durch Bedienpersonal genutzt werden.

Im Fokus von EULYNX liegen alle Schnittstellen, die im Kontakt mit dem Stellwerkskern stehen, der darüber entscheidet, ob Fahrzeugbewegungen auf der Eisenbahninfrastruktur zugelassen werden dürfen oder Stellelemente ihren Status ändern dürfen. Neben den Schnittstellen zu Feldelementen sind somit beispielsweise auch die Schnittstelle zu Nachbarstellbereichen und zur Bedienoberfläche im Kontrollzentrum, die nicht Teil des Stellwerkskerns sind, im Betrachtungsraum. Die innere Funktionsweise des Stellwerkskerns (Sicherungslogik) wird jedoch durch EULYNX nicht betrachtet.

Mittlerweile existieren erste (Teil-)Implementierungen von DSTWs [Deutsche Bahn AG 2019].

2.2.6 Trennung Zulassung Hardwareplattform und Software

Als weitere wichtige Zukunftstechnologie wird in [EUG & EULYNX 2019] eine Trennung von Hardwareplattform und Software genannt. Klassischerweise wurden Stellwerke über Jahrzehnte als technische Einheiten zugelassen, die von ihren Eigenschaften her nicht verändert werden durften. Dieses Prinzip wurde auch noch auf die ersten computerbasierten (elektronischen) Stellwerke übertragen, so dass die Hardwareplattform bei diesen Stellwerken in der Zulassung fest vorgegeben ist. Die schnelle Weiterentwicklung von Computerhardware und damit verbunden die schnelle Abgängigkeit entsprechender Hardwarekomponenten und der damit verbundene hohe Zulassungsaufwand stellt dieses Verfahren jedoch in Frage.

Darum rückt eine Trennung von Hardwareplattform und Software in den Fokus. Das Ziel ist, eine leistungsfähige, standardisierte Hardwareplattform zu entwickeln, auf der sicherungstechnisch geprüfte Software jederzeit sicher ausgeführt werden kann. Mittels Hardware-Abstraktionsschichten soll sichergestellt werden, dass die logischen Softwarebestandteile unabhängig von der Hardwareplattform spezifiziert werden können [EUG & EULYNX 2019, S. 6]. Eine mögliche Umsetzung können sogenannte „***Commercial-off-the-Shelf***"-Steuerungen sein (vgl. z. B. [Sezgün 2017]).

2.2.7 Automatic Train Operation (ATO)

Eine weitere Zukunftstechnologie, die in den letzten Jahren in der Fachöffentlichkeit breit diskutiert wurde und Thema auf zahlreichen Tagungen war, ist das automatisierte Fahren (engl. **Automatic Train Operation (ATO)**). Da das Thema recht breit ist, soll an dieser Stelle nur kurz auf Aspekte von ATO eingegangen werden, die eine Schnittmenge mit der infrastrukturseitigen Sicherungstechnik haben.

ATO ist der Oberbegriff für Technologien, bei denen ein Softwaresystem Aufgaben des Tf im Zusammenhang mit dem Führen eines Eisenbahnfahrzeuges übernimmt. Es werden verschiedene Level der Automatisierung unterschieden, die „***Grades of Automation***" **(GoA)** genannt werden. In der Regel werden die in Tab. 2 aufgeführten GoA unterschieden (vgl. z. B. [smartRail 4.0 2018]).

Die unterschiedlichen GoA haben verschiedene Vorteile (vgl. z. B. [Abrach et al. 2019]). Erst bei GoA 3 und 4, das zum Zeitpunkt der Erstellung dieser Arbeit auf Hauptbahnen mit Mischverkehr noch nicht etabliert ist, reduziert sich das benötigte Personal. Bereits in GoA 2 übernimmt jedoch das ATO-System die Fahrzeugsteuerung.

Tab. 2: Grades of Automation beim automatisierten Fahren (angelehnt an [smartRail 4.0 2018])

GoA	Bedeutung
GoA 1	Tf fährt selbst, wird aber überwacht (wird meist nicht als ATO, sondern als Zugbeeinflussung / Automatic Train Protection (ATP) betrachtet)
GoA 2	ATO-Bordgerät übernimmt die Zugsteuerung, Tf überwacht jedoch permanent die Strecke und das Verhalten des Bordgeräts
GoA 3	es ist kein Tf mehr an Bord, es gibt aber noch Zugbegleitpersonal, das bestimmte Handlungen (z. B. Türen schließen) übernimmt und im Notfall eingreifen kann (z. B. nach einer Notbremsung)
GoA 4	Zug kann ohne Bordpersonal verkehren (vollautomatisiertes Fahren)

Durch die Übernahme der Fahrzeugsteuerung durch das ATO-System verändern sich die Fahrkurven, da ein automatisches System ein anderes Fahrverhalten hat als ein Mensch. Das Fahrverhalten des Systems basiert auf Berechnungen, während das Fahrverhalten des Menschen auf Erfahrung und bestimmten präferierten Verhaltensweisen basiert. Da die Erfahrungen und Verhaltensweisen von Menschen unterschiedlich sind, kommt es im Vergleich zum automatisierten System zu einer größeren Streuung der Fahrkurven. Dies kann zu einer verringerten Kapazität führen, insbesondere, wenn aufgrund von knappen Zugfolgefällen eine hohe Präzision bei der Einhaltung der vorgegebenen Soll-Fahrkurven erforderlich ist [Flamm et al. 2019]. Zudem entfallen bei ATO Reaktionszeiten der Triebfahrzeugführer [Kümmling & Wanstrath 2021, S. 17], z. B. bei unerwarteten Signal-aufwertungen. Aus diesem Gründen wird auf einigen dicht befahrenen S-Bahn-Stammstrecken in Deutschland derzeit eine Einführung von ATO GoA 2 befürwortet [Beyer et al. 2019; Kümmling & Wanstrath 2021]. Eine Hürde bei GoA 2 ist jedoch die Aufrechterhaltung der Aufmerksamkeit des Tf, dessen Aufgabenbereich stark beschränkt würde [Stoll et al. 2019, 122f].

Bei GoA 3 und 4 sind im Regelbetrieb keine personalbedingten Streuungen der Fahrkurven zu erwarten, da in der Regel das Bordpersonal nicht in die Steuerung des Fahrzeugs eingreift. In der Rückfallebene können sich jedoch Unterschiede ergeben [Üyümez 2019].

2.2.8 Zusammenfassung der technologischen Ausgangsbasis für die smartLogic

Auf Basis der Erkenntnisse der vorangegangenen Unterkapitel von Kapitel 2.2 kann davon ausgegangen werden, dass auf Basis zukünftig voraussichtlich zur Verfügung stehender Technologien für die Entwicklung der neuen Sicherungslogik folgende Annahmen getroffen werden können:

- Die Fahrzeugbewegungen werden überwiegend mit ETCS mit Führerstandsignalisierung ausgestattet sein.
- Die europaweit spezifizierten ETCS-Nachrichten können von der Mehrzahl der Fahrzeugbewegungen gelesen und verarbeitet werden.
- Ein Großteil der Fahrzeugbewegungen kann hinreichend sicher und mit akzeptabler Toleranz bzgl. der Ortungsgenauigkeit vollständig (Zugspitze bis Zugende) geortet werden.
- Es existiert ein hochverfügbares Kommunikationssystem mit hinreichend kleinen Latenzzeiten, um eine schnelle Kommunikation zwischen Fahrzeug- und Infrastruktur zu ermöglichen.
- Mit Feldelementen verschiedener Hersteller kann über standardisierte Schnittstellen kommuniziert werden.

- Es existiert eine standardisierte, generische Hardwareplattform, auf der eine sicherungskritische Software wie die Sicherungslogik ohne inhaltliche Anpassung aufgesetzt werden kann.
- Es verkehren Fahrzeugbewegungen mit und ohne Tf im Zuständigkeitsbereich der Sicherungslogik.

2.3 aktuelle Ansätze zur Neu- bzw. Weiterentwicklung der Sicherungslogik

Während in Kapitel 2.2 aktuelle Entwicklungen im Bereich der Umsysteme der Sicherungslogik vorgestellt wurden, werden in diesem Kapitel aktuelle Entwicklungen und Forschungsarbeiten zum Thema der Sicherungslogik bzw. Stellwerkslogik (vgl. zu den Begriffen Kapitel 2.1.1) selbst vorgestellt.

Aufgrund der Aufgabenstellung, wonach eine neue Eisenbahnsicherungslogik auf der „Grünen Wiese“ entwickelt werden sollte, dienen die Informationen in diesem Kapitel nicht der Identifizierung einer Forschungslücke. Stattdessen sollen sie eine Einordnung der Ergebnisse dieser Arbeit im Kontext des aktuellen Stands der Technik und Forschung ermöglichen. Die einzelnen Projekte und Forschungsarbeiten werden daher an dieser Stelle nur grundsätzlich vorgestellt, während am Ende der inhaltlichen Hauptkapitel 4 bis 8 jeweils ein Kapitel „Vergleich mit alternativen Ansätzen“ existiert, das einen detaillierteren Vergleich der hier vorgestellten Projekte und Forschungsarbeiten mit den in den inhaltlichen Hauptkapiteln dieser Arbeit entwickelten Lösungen enthält (vgl. zur Struktur der inhaltlichen Hauptkapitel Kapitel 1.3).

2.3.1 Projekte von Eisenbahninfrastrukturunternehmen (EIU)

Stellwerkssysteme werden üblicherweise von Herstellern aus der Branche der Signalbauindustrie entwickelt und hergestellt. Dabei können sie entweder selbstständig neue Stellwerkstypen entwerfen oder auf Basis von Anforderungsdokumenten der EIU tätig werden. In ersterem Fall haben die Firmen ein Interesse daran, ihre Innovationen zu schützen. Daher sind wenig detaillierte Informationen über die nächsten Entwicklungsschritte der Signalbauindustrie bekannt. Aus diesem Grund fokussiert das vorliegende Kapitel auf aktuelle Projekte der EIU.

smartRail 4.0 (Schweiz)

In der Schweiz wird seit Mitte der 2010er-Jahre am Branchenprogramm **smartRail 4.0** gearbeitet. Bestandteil ist auch ein neuer Stellwerkstyp, der unter dem Label „***ETCS-Stellwerk***“ firmiert (vgl. [Schmidt & Grabowski 2018] und [SBB AG 2018]; auf der Webseite www.smartrail40.ch gibt es zudem eine umfangreiche Dokumentensammlung zum Thema). Ziel des ETCS-Stellwerks ist es, die Funktionsweise des Stellwerks auf die Erfordernisse von ETCS zu optimieren und möglichst generisch zu halten. Weiterhin sollen die Lebenszykluskosten durch eine deutliche Vereinfachung der Technik reduziert werden und die Migrationsfähigkeit in Bezug auf die bestehende Technik (insbesondere die Feldelemente) bestehen bleiben. Zur Erreichung der genannten Ziele enthält das ETCS-Stellwerk eine schlanke Sicherungslogik, die unabhängig von der konkreten Topologie ist und die topologischen Daten aus einer sicheren Datenquelle einliest.

Die Überlegungen zum ETCS-Stellwerk fließen in die später initiierte Reference CCS Architecture (RCA) mit ein, die in Kapitel 2.4 detaillierter vorgestellt wird. Da es sich bei RCA und smartRail 4.0 – wie auch in der vorliegenden Arbeit – um „Grüne Wiese“-Ansätze handelt, werden die Unterschiede zur smartLogic in den Literaturvergleichskapiteln zu den jeweiligen Hauptkapiteln (jeweils das vorletzte Kapitel des Hauptkapitels, vgl. Kapitel 1.3) näher erläutert werden. Die Konzepte in

smartRail 4.0 basieren jedoch in der Regel nicht auf einer ausführlichen wissenschaftlichen Herleitung, sondern auf der Erfahrung der beteiligten Experten. Die vorliegende Arbeit hat daher den Anspruch, wissenschaftlichen Hintergrund zu liefern und Alternativen aufzuzeigen sowie in Detailpunkten für zukünftige Designentscheidungen eine Entscheidungshilfe zu bieten.

Digitale Schiene (Deutschland)

Auch in Deutschland existiert bei der Deutschen Bahn eine Arbeitsgruppe, die sich mit der Zukunft der Stellwerkstechnik beschäftigt und zur Verwirklichung der Vision des „**Digitalen Bahnbetriebs**“ (vgl. Kapitel 2.2.1) unter der Bezeichnung „**Digitale Schiene Deutschland**“ beiträgt. Seit 2020 arbeitet diese Gruppe im Rahmen der RCA mit smartRail 4.0 eng zusammen. Auf eine gesonderte Vorstellung wird daher verzichtet.

2.3.2 Projekte auf europäischer Ebene

Auch auf europäischer Ebene gab und gibt es bereits mehrere Ansätze, die Stellwerkstechnik neu zu denken. Dabei steht auch der Aspekt einer europäischen Vereinheitlichung im Fokus, um Skaleneffekte zu erzielen.

Eurointerlocking

Von 1999 bis 2006 gab es bereits das Projekt „***Eurointerlocking***“ (in manchen Quellen auch „Euro-Interlocking“) des internationalen Eisenbahnverbandes UIC [Europäische Kommission 2021]. Die genauen Ergebnisse dieses Projektes sind leider derzeit nicht abrufbar. Auf der Projekthomepage des Fördermittelgebers Europäische Kommission werden als Ergebnisse des Projekts standardisierte Datenaustausch- und Dateiformate sowie ein Anforderungsmanagement-Tool („DOORS“) genannt.

INESS

Ein weiteres von der EU gefördertes Projekt wurde vom internationalen Eisenbahnverband UIC von 2008 bis 2012 unter dem Titel „***Integrated European Signalling System***“ **(INESS)** durchgeführt. Quelle für die folgenden Angaben ist der Abschlussbericht des Projektes [Buseyne 2017] sowie die Projekthomepage (www.iness.eu). Das Projekt versteht sich als Ergänzung zu den bisherigen ERTMS-Bestandteilen ETCS und GSM-R. Der Autor dieser Arbeit konnte jedoch keine Informationen über konkrete Realisierungen von INESS-Stellwerken finden.

Zu INESS gehörten die folgenden Teilprojekte (Work Streams):

- (A – Project Management)
- B – Business Modell: Es wurde ein Lebenszykluskostenmodell entwickelt, mit dessen Hilfe Kostentreiber identifiziert und Einsparpotenziale aufgezeigt wurde.
- C – System Design: Es wurde ein einheitliches, XML-basiertes Datenmodell mit dem Namen „European Unified Data Model for Railway Infrastructures (EUDRI)“ auf der Basis von RailML (siehe Kapitel 2.5.3) geschaffen.
- D – Generic requirements: Es wurden ca. 1000 generische funktionale Anforderungen definiert, die ein INESS-Stellwerk erfüllen muss. Basis bildeten die Ergebnisse aus dem Eurointerlocking-Projekt. Fokus lag im Zusammenspiel mit ETCS Level 1 und 2 und auf der Harmonisierung der verschiedenen Stellwerksansätze. Es war nicht Ziel des Projektes, die Funktionsweise der Sicherungslogik im Stellwerk neu zu denken. Ein Ergebnis des Teilprojekts ist auch ein formales Verifizierungstool, welches

Umsetzungsmodelle für die Sicherungslogik in Hinblick auf die Erfüllung der funktionalen Anforderungen prüft.

- E – Functional architecture & interfaces: Ergebnisse dieses Teilprojekts sind eine Stellwerksarchitektur, Schnittstellendefinitionen (FFFIS) und eine Untersuchung möglicher Rückfallebenen.
- F – Testing & Commissioning: Es wurde unter anderem ein Test- und Inbetriebnahme-Handbuch erstellt.
- G – Safety case process: Es wurden Hilfestellungen bzw. ein Werkzeugkasten für die Durchführung des CENELEC-Prozesses erarbeitet, um die erforderlichen Dokumentationen etc. effizient durchführen zu können.
- (H - Dissemination, Exploitation, Training & Coaching)

Shift2Rail

Shift2Rail ist ein großangelegtes Förderprogramm der EU. Das „Innovation Programme“ 2 beschäftigt sich mit der Leit- und Sicherungstechnik. Darin gibt es die folgenden Forschungs- und Innovationsbereiche:

- Communication System (TD 2.1)
- Automatic Train Operation (ATO) (TD 2.2)
- Moving Block (TD 2.3)
- Safe Train Positioning (TD 2.4)
- Train Integrity (TD 2.5)
- new laboratory test framework (TD 2.6)
- standardised engineering and operational rules (TD 2.7)
- Virtual Coupling (TD 2.8)
- Traffic Management System (TD 2.9)
- Smart radio-connected all-in-all wayside objects (TD 2.10)
- Cyber Security (TD 2.11)

Allerdings beschäftigt sich keiner der Forschungs- und Innovationsbereiche explizit mit der Funktionsweise der Sicherungslogik im Stellwerk (vgl. https://shift2rail.org/research-development/).

2.3.3 Forschungsarbeiten

Auf Seiten der Forschung gab es in den letzten Jahren ebenfalls mehrere Arbeiten, die sich mit einer generischen Beschreibung bzw. Weiterentwicklung der Stellwerkslogik beschäftigten und im Folgenden vorgestellt werden sollen.

generische Beschreibung des Eisenbahnbetriebs und der erforderlichen Schutzfunktionen

Spätestens seit dem Aufkommen leistungsfähiger Computer bietet es sich an, die Funktionsweise der Eisenbahnsicherungstechnik formal zu beschreiben, um sie in Software nachbilden zu können. Daher gibt es bereits mehrere formale Modelle. Im deutschsprachigen Raum forschen insbesondere die TU Braunschweig sowie die ETH Zürich an diesem Thema. Dabei stand zunächst die formale Nachbildung der bestehenden Sicherungstechnik im Fokus, aber zunehmend auch eine Vereinfachung der Regeln durch Reduzierung auf die generischen sicherungstechnischen Kernfunktionen.

Die Dissertation von Michael MEYER ZU HÖRSTE an der TU Braunschweig aus dem Jahr 2003 [Meyer zu Hörste 2003] enthält eine generische Funktionsliste von Funktionen der Leit- und Sicherungstechnik

(LST) und damit auch von Stellwerksfunktionen. Hergeleitet wird diese generische Funktionsliste von zuvor in der Arbeit identifizierten Gefährdungen für Zugfahrten. Diese Gefährdungen wurden in der Arbeit in einer eigenen Liste zusammengestellt, die auch spezifischere Gefährdungen außerhalb der Grundgefährdungen (vgl. Kapitel 2.1.1) enthält, wie z. B. einen Erdrutsch. Die Möglichkeit eines Betriebs mit ETCS Level 3 mit Moving Block wird bereits mitberücksichtigt. Mittels Petri-Netzen werden grundlegende Prozesse verdeutlicht.

Eine weitere Arbeit zu diesem Thema an der TU Braunschweig ist die Dissertation von Gunnar BOSSE aus dem Jahr 2010 [Bosse 2010]. Diese Arbeit ist auf die generische, länderübergreifende Beschreibung von Betriebsverfahren fokussiert, enthält dafür aber auch eine generische Beschreibung der Aufgaben der Sicherungstechnik. Die Arbeit führt eine Risikoanalyse als Ausgangspunkt der generischen Beschreibung durch und orientiert sich an den Prozessen aus EN 50126 und EN 50129. Mittels der Risikoanalyse werden über Ereignisketten funktionale Anforderungen an das generische Referenzsystem identifiziert, die natürlichsprachlich notiert werden. Dabei werden jeweils potenzielle Ausfälle von Systemkomponenten betrachtet. Ergebnis ist ein umfangreicher Funktionskatalog. Die Funktionen werden dabei in „Betriebliche (Teil-)Funktionen“, „Subsystemfunktionen“, „Prüf- und Kontrollfunktionen“, „Abfangfunktionen“ und „Schadensbegrenzungsfunktionen“ unterschieden [Bosse 2010, S. 96]. Die verwendete Methode wird ausführlich beschrieben. Die damit gewonnenen Ergebnisse sind in Form von Beispielen enthalten.

Auch die Dissertation von Silko HÖPPNER an der ETH Zürich beschäftigt sich mit einer „generische[n] Beschreibung von Eisenbahnbetriebsprozessen“ [Höppner 2015]. Die sehr umfangreiche Arbeit baut auf der Dissertation von BOSSE auf und nutzt die Modellierungssprache UML als Beschreibungsmittel. Das entstandene Modell beginnt mit den Kernfunktionen des Eisenbahnbetriebs im Falle eines einfachsten anzunehmenden Eisenbahnsystems (Ringstrecke mit einem Fahrzeug) und wird schrittweise erweitert bis „ein Zustand erreicht wird, in dem bei zusätzlicher Systemerweiterung keine Änderung der Verfahrensabläufe nötig ist“ [Höppner 2015, S. II]. Dabei geht HÖPPNER davon aus, dass das Eisenbahnnetz in diskrete Fahrwegabschnitte unterteilt ist. HÖPPNER greift auf die in [Maschek 2009] identifizierten Schutzfunktionen zurück [Höppner 2015, S. 158]. Der Fokus der Arbeit liegt aber auf den Betriebsprozessen und nicht auf sicherungstechnischen Details.

Dissertation von Daria Menzel

Daria MENZEL (geb. Bachurina) hat in ihrer Ende 2018 an der TU Dresden verteidigten Dissertation ein „generisches Konzept zur Fahrzeugbewegungssicherung“ entwickelt. Dabei handelt es sich um eine algorithmische Beschreibung der wichtigsten Regeln zur Fahrzeugbewegungssicherheit, wie sie bisher von Stellwerken sichergestellt wird. Prämisse war, dass die generische Logik so einfach wie möglich gehalten werden soll. Die Doktorarbeit wurde leider wegen eines Sperrvermerks noch nicht allgemein zugänglich veröffentlicht, so dass für die Zusammenfassung in diesem Kapitel auf die Informationen zurückgegriffen wurde, die in den Veröffentlichungen [Bachurina 2018] und [Menzel 2019] enthalten sind.

Die Arbeit fokussiert auf den Schutz vor den klassischen Grundgefährdungen Entgleisung und Kollision mit einem anderen Eisenbahnfahrzeug, die bereits in Abb. 1 in Kapitel 2.1.1 vorgestellt wurden. Dabei wurde zunächst ein möglichst einfaches Basis-Konzept entwickelt, welches nachfolgend für komplexere Anwendungsfälle erweitert wird. Das Konzept basiert auf einer generischen Darstellung der Topologie. Diese setzt sich aus Fahrwegelementen zusammen, die in stellbare Fahrwegelemente (z. B. Weiche) und nicht stellbare Fahrwegelemente (z. B. einfaches Gleis zwischen zwei Weichen) unterschieden werden.

Die Grundannahme ist, dass für jedes Fahrwegelement die gleichen Funktionen zu erfüllen sind. Die Elemente müssen umgestellt werden können, die Endlage muss überwacht werden und der Besetztzustand muss erfasst werden. Bei nicht stellbaren Fahrwegelementen spielt zwar nur der Besetztzustand eine Rolle; um das Modell generischer zu machen, werden die übrigen Funktionen jedoch trotzdem vorgesehen, sind aber inaktiv. Die Funktionen sind sowohl für Fahrwegelemente als auch für Flankenschutzelemente oder Elemente im Flankenschutzraum oder Durchrutschweg relevant.

Diese generischen Funktionen werden im Konzept des sicherungstechnischen Tripols zusammengefasst (siehe Abb. 4). Jedes Fahrwegelement bildet einen Tripol, der aus drei Knoten (A, B und C) besteht und bis zu vier Fahrmöglichkeiten bietet: A nach B, B nach A, A nach C und C nach A. Jede dieser vier Fahrmöglichkeiten bildet eine sogenannte „Basisfahrstraße“ des Tripols, deren Befahrbarkeit von der Ist-Lage des Tripols abhängt. Bei nicht stellbaren Fahrwegelementen kann die Ist-Lage nicht verändert werden. Deshalb sind zwei Basis-Fahrstraßen nicht als Fahrweg verfügbar.

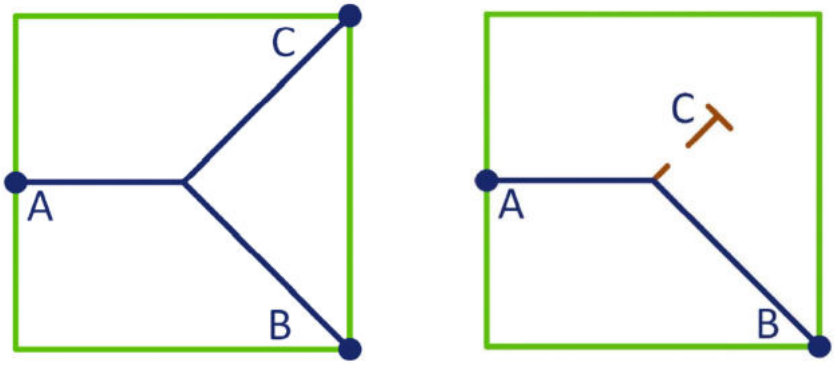


Abb. 4: Sicherungstechnischer Tripol
(links für stellbare Fahrwegelemente, rechts für nicht stellbare Fahrwegelemente)
Quelle: [Menzel 2019]

Ein freizugebender Fahrweg für einen Zug wird nun aus einer Verkettung der Basisfahrstraßen gebildet. Die Länge des freizugebenden Fahrwegs hängt dabei von betrieblichen Überlegungen ab.

Mit dem Konzept können sowohl eine klassische ortsfeste Signalisierung, als auch eine Führerstandsignalisierung mit ortsfesten und ohne ortsfeste Gleisfreimeldegrenzen realisiert werden. Weiterhin kann die Logik von einem zentralen infrastrukturseitigen System (analog heutiger Stellwerke) oder einem dezentralen auf den Fahrzeugen und Feldelementen angesiedelten System umgesetzt werden.

Das Konzept von MENZEL bietet damit einen sehr generischen Ansatz zur Fahrzeugbewegungssicherung im Schienenverkehr. Allerdings bleiben in Unkenntnis der eigentlichen Dissertation leider einige Fragen offen. Beispielsweise wie komplexere Zusammenhänge wie bei Kreuzungsweichen integriert werden können (z. B. mittels voneinander abhängiger Tripole?). Eine Einschränkung könnte die diskrete Aufteilung der Gleistopologie in Fahrwegelemente sein, die vermutlich auch nur eine diskrete Zuteilung der Infrastruktur auf die einzelnen Fahrzeugbewegungen erlaubt, da jeder Tripol nach [Menzel 2019] nur als Ganzes belegt oder unbelegt sein kann. Die in den aufgeführten Veröffentlichungen zur Dissertation enthaltenen Informationen bilden zudem nicht alle Sicherheitsanforderungen ab. Beispielsweise wurde die Einhaltung der zulässigen Geschwindigkeiten oder die Einbindung von Bahnübergängen nicht thematisiert. Es sei nochmals darauf hingewiesen, dass möglicherweise die noch nicht allgemein veröffentlichte Dissertation einige dieser Fragen beantwortet.

Masterarbeit von Leonhard Authier und David Etienne

Auch in der Masterarbeit von Leonhard AUTHIER und David ETIENNE an der ETH Zürich aus dem Jahr 2017 ([Authier & Etienne 2017]) wurde eine Sicherungslogik entworfen, die mit einem „Satz minimal notwendiger Regeln“ (Aufgabenstellung zu [Authier & Etienne 2017]) auskommt, um der steigenden Komplexität der Sicherheitskonzepte für den Bahnbetrieb zu begegnen.

Die Arbeit fokussiert auf ein sehr einfaches Szenario einer zweigleisigen Kreis-Strecke mit einem Betriebsbahnhof. Die Infrastruktur besteht aus Gleisen (Kanten im Modell) sowie Weichen, Kreuzungen und Prellbocke (Knoten). Es wurde angenommen, dass jederzeit ein vollständiges Informationsbild über die Topologie, den Status der Infrastrukturelemente sowie den Status der vorhandenen Fahrzeuge inkl. Positionsmeldung existiert. Weiterhin wurde angenommen, dass jederzeit eine Kommunikation zwischen allen einzelnen Fahrzeugen und allen einzelnen Infrastrukturelementen möglich ist.

Die Sicherungslogik soll die Gefährdungen Entgleisung wegen überhöhter Geschwindigkeit oder falsch gestellter Weiche, Kollision zwischen zwei Eisenbahnfahrzeugen und Fahrt gegen einen Prellbock verhindern.

Elemente des Gleises können sogenannte „***Exclusive Components***“ sein, wenn sie nur von einem Zug gleichzeitig genutzt werden können, z. B. Weichen oder Kreuzungen oder zwei Gleisabschnitte, deren Fahrzeugbegrenzungslinien sich überschneiden. Exclusive Components können den Status frei oder reserviert haben.

Zugfahrten belegen auf der Infrastruktur ihre Länge sowie ihren Bremsweg. Am Ende des Bremsweges befindet sich ein virtueller Stopp-Punkt. Auf dem Gleis können sich Hindernisse befinden. Ein solches Hindernis kann z. B. der virtuelle Stopp-Punkt einer anderen Zugfahrt oder ein Prellbock sein, aber auch eine Exclusive Component, die nicht für die betrachtete Zugfahrt reserviert ist. Ein Element kann zugleich für eine Zugfahrt ein Hindernis sein und für eine andere nicht (z. B. Weiche je nach Lage). Durch Umstellen eines solches Elements wird das Hindernis aufgelöst.

Einer Zugfahrt wird immer das nächste Hindernis mitgeteilt und ihr damit erlaubt, bis zu diesem Punkt zu fahren. Der Zug reserviert sich dabei seine Exclusive Components selbst. Dabei kann er dispositive Vorgaben aus der Zentrale bekommen, die aber keinen Einfluss auf die Sicherungstechnik haben.

Auch diese Arbeit verfolgt den Ansatz zunächst von einem engen Anwendungsfeld (zweigleisige Kreisstrecke mit Betriebsbahnhof) auszugehen, das als Basis für spätere Erweiterungen dienen soll. Dabei entfernt die Arbeit sich mit dem Konzept des virtuellen Stopp-Punktes von den klassischen Sicherungsprinzipien, die auf eingestellte Fahrstraßen und damit die explizite Freigabe eines bestimmten Gleisabschnitts setzen, und verfolgt einen neuen Ansatz.

dezentrale Ansätze

Mehrere Forschungsarbeiten wie [Fantechi et al. 2016] oder [Menzel et al. 2020] verfolgen einen dezentralen Ansatz, bei dem die Sicherungslogik auf die Feldelemente bzw. in die Fahrzeuge verteilt wird. Die Abstandshaltung regeln die Fahrzeuge dabei in der Regel untereinander durch direkte Kommunikation. Die Infrastrukturelemente werden vom Fahrzeug reserviert, wenn das Fahrzeug das jeweilige Infrastrukturelement benötigt.

Vorteil einer dezentralen Lösung ist vor allem die Vermeidung von Komplexität durch die Vermeidung zentraler Strukturen. Weiterhin können Veränderungen an der Infrastruktur ohne große Probleme vorgenommen werden, da keine zentrale Logik angepasst werden muss. Ein dezentrales System ist zudem robuster, da ein kritischer Fehler auf mehreren dezentralen Systemkomponenten auftreten

müsste, um die Verwendbarkeit des gesamten Systems einzuschränken. Allerdings wird bei den meisten Anwendungen zumindest noch ein Domain-Server benötigt, der die Netzwerkelemente (Infrastrukturelemente und Fahrzeuge im Betrachtungsbereich) mit ihren Kommunikationsadressen kennt. Ein dezentraler Ansatz bietet sich besonders für Regionalstrecken mit wenig Verkehr an, da hier der Abstimmungsaufwand und insbesondere die Konkurrenz um Infrastrukturressourcen zwischen den einzelnen Zugfahrten gering ist.

2.4 Reference CCS Architecture (RCA)

Wichtig für die Gestaltung einer zukünftigen Sicherungslogik ist auch die Architektur, in die sie eingebettet ist. Seit 2018 gibt es Bestrebungen, mit der **Reference CCS Architecture (RCA)** eine europaweit standardisierte Architektur für die infrastrukturseitige Leit- und Sicherungstechnik (LST, engl. CCS = „Command, Control, and Signalling“) zu definieren. Diese Initiative soll im vorliegenden Kapitel näher vorgestellt werden.

2.4.1 Hintergrund und Motivation

Die RCA wird von der RCA-Gruppe, einem Zusammenschluss von EIU aus der ERTMS Users Group (EUG) und der EULYNX-Gruppe, entwickelt. Das Whitepaper der RCA-Gruppe [EUG & EULYNX 2018] erläutert die Motivation der RCA, die im Folgenden kurz zusammengefasst wird.

Bereits seit den 1990er-Jahren wird am ERTMS-Standard für die Leit- und Sicherungstechnik gearbeitet. Seit der letzten Dekade werden auch verstärkt ETCS-Ausrüstungsprojekte umgesetzt. Jedoch zeigte sich bei bisherigen Implementierungen, dass durch ERTMS anvisierte Verbesserungen mittels seiner Komponenten ETCS und GSM-R alleine nicht oder nicht im gewünschten Maße realisiert werden können. So kann die Kapazität von Eisenbahnstrecken bei ungünstigen Voraussetzungen mit ETCS sogar sinken (vgl. auch Kapitel 2.2.2). Für ETCS-Ausrüstungsprojekte gibt es aufgrund dieses Umstandes und der immer noch hohen Kosten keinen eindeutig positiven Business Case. Dies verlangsamt die europäische Umsetzung.

Es existieren verschiedene Ursachen für die praktischen Probleme bei der Umsetzung von ETCS-Projekten, die an dieser Stelle nicht alle aufgezählt werden sollen. Eine wichtige Ursache ist jedoch, dass in Europa viele Bestandsstrecken mit historisch gewachsener Bestandsinfrastruktur umgerüstet werden sollen. Bei diesem Umrüstungskonzept muss die ETCS-Infrastruktur mit einer Vielzahl bestehender technischer Systeme zusammenarbeiten, die aufgrund ihres Alters nicht für die Zusammenarbeit mit ETCS ausgelegt sind. Die Möglichkeiten von ETCS können somit nicht vollumfänglich genutzt werden und Restriktionen der Bestandssysteme werden auf ETCS übertragen. Es existiert daher in der Fachwelt mittlerweile vielfach die Auffassung, dass auf ETCS angepasste Leit- und Sicherungstechnik erforderlich ist, um mit ETCS die bestmögliche Kapazität erzielen zu können und einen positiven Business Case für die ETCS-Einführung zu erreichen (vgl. z. B. [Schmidt & Grabowski 2018; Kuttig-Trölenberg et al. 2021]). (Hierzu möchte auch die vorliegende Arbeit beitragen.)

In der Vergangenheit wurde bereits der Versuch unternommen, ein europaweit standardisiertes Stellwerk zu entwickeln (vgl. INESS in Kapitel 2.3.1). Jedoch erwies sich dieses Vorhaben aufgrund der zahlreichen unterschiedlichen Anforderungen in den verschiedenen Ländern als extrem komplex. Ein weiterer Nachteil einer so weitreichenden Standardisierung ist, dass Innovationen, die von Zulieferer-Firmen entwickelt werden, kaum noch möglich sind. Eine fehlende Standardisierung begünstigt dagegen Kompatibilitätsprobleme zwischen verschiedenen Komponenten verschiedener Hersteller, so dass eine Herstellerbindung entsteht, die Wettbewerb behindert und somit zu höheren

Kosten führt. Deshalb wird bei der RCA analog zu EULYNX (vgl. Kapitel 2.2.5) auf die Entwicklung einer Systemarchitektur mit genau festgelegten Schnittstellen zwischen den Komponenten gesetzt. Dies ermöglicht Herstellern, einzelne Komponenten zu entwickeln, die mit dem Gesamtsystem auf verlässliche Weise verbunden werden können. Innovationen können somit leichter in einzelne Komponenten eingebracht werden. Voraussetzung ist jedoch, dass die Systemarchitektur und die Schnittstellen so gestaltet sind, dass sie den Komponenten großen Spielraum ermöglichen. Weiterhin ist Voraussetzung, dass die Komponenten jeweils getrennt voneinander einen Sicherheitsnachweis erhalten können. Durch dieses Konzept soll ein Business Case für ERTMS geschaffen werden.

2.4.2 Anforderungen an und Annahmen für die Architektur

Auf Seite 2 des Whitepapers werden die wichtigsten Anforderungen und Annahmen für die RCA gelistet [EUG & EULYNX 2018, S. 2]:

- es sollen standardisierte Schnittstellen zwischen den Systemkomponenten verwendet werden
  - ETCS Level 2 oder höher als Schnittstelle zu den Fahrzeugen (vgl. Kapitel 2.2.2)
  - EULYNX-Schnittstellen zur Infrastruktur (vgl. Kapitel 2.2.5)
- die RCA soll bereit sein für die Zukunftstechnologien ATO (vgl. Kapitel 2.2.7), ETCS Level 3 (vgl. Kapitel 2.2.3), FRMCS (vgl. Kapitel 2.2.4) und satellitenbasierte Ortungssysteme
- die infrastrukturseitige Sicherungstechnik soll deutlich vereinfacht werden und standardisierte Systemkomponenten enthalten
- die RCA soll eine verbindliche, modulare Architektur definieren, die verschiedene Konfigurationen für Migrationsstrategien und Ausführungen für verschiedene Anwendungsfälle ermöglicht
- existierende Systeme sollen eingebunden werden können, um die Migrationsfähigkeit zu erhöhen
- Abwärts- und Aufwärtskompatibilität soll sichergestellt werden, um die Kompatibilität mit zukünftigen, weiterentwickelten Systemen zu ermöglichen

2.4.3 Architektur

Abb. 5 zeigt die Systemarchitektur der RCA. Zu den folgenden Erläuterungen vergleiche [ERTMS Users Group & EULYNX 2020b].

Die Architektur besteht aus zwei Kommunikationszirkeln, dem sicherheitskritischen (pink dargestellt), für dessen infrastrukturseitigen Teil auch der Begriff **„Advanced Protection System“ (APS)** existiert, und dem nicht sicherheitskritischen (türkis dargestellt). Die Architektur ist zudem in mehrere Ebenen unterteilt.

Ganz oben steht die Planung der Fahrzeugbewegungen („***Planning System***“). Dies kann die Vorabplanung im Rahmen der Fahrplan-Erstellung beinhalten, aber auch die Planung des Life-Betriebs, die Verspätungen und sonstige Abweichungen vom Fahrplan umfassen (Disposition). Ganz unten stehen die ausführenden Elemente: Fahrzeuge und Feldelemente der Infrastruktur sowie Personen, die am Gleis arbeiten. Diese äußeren Schichten gehören nicht mit zur RCA, sondern stellen ihre Umsysteme dar (weiß dargestellt).

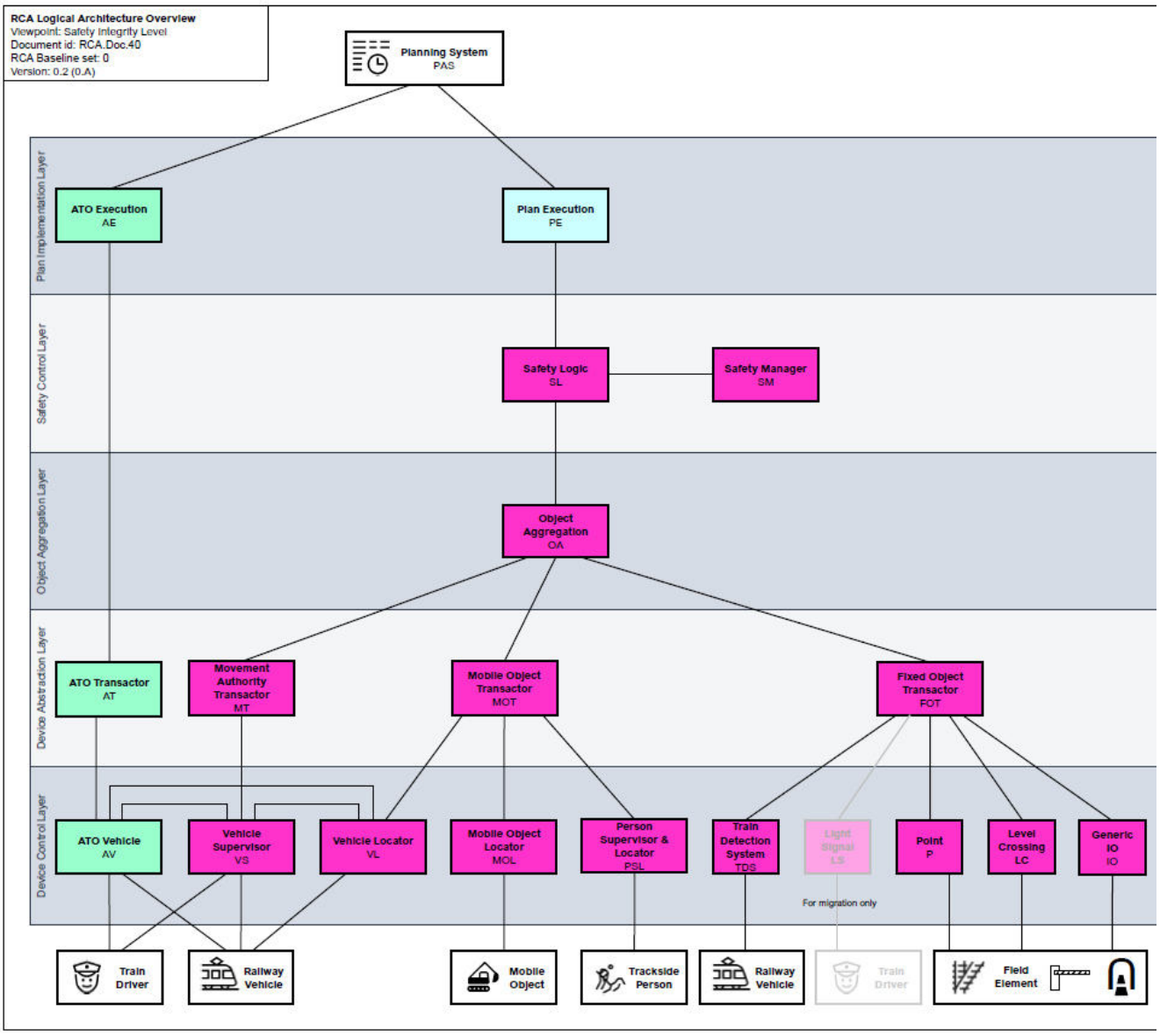


Abb. 5: Überblick über die RCA-Architektur (Ausschnitt)

Von Seiten der Planung (oben) kommend, stellt die Fahrzeugbewegungskontrolle („***Plan Execution***“ bzw. „***ATO Execution***“) die oberste Schicht dar, die im Fokus der RCA ist. Hier werden die Anweisungen für die Fahrzeuge auf Basis der Planungen des Planning Systems generiert. Dies können auf der nicht sicherheitskritischen Seite (türkiser Zirkel) entweder Zeitschranken sein, die von den Fahrzeugen eingehalten werden sollen oder genaue Fahrkurven. Die Diskussion, welches der beiden Konzepte sich hier durchsetzt, ist noch offen. Auf der sicherheitskritischen Seite (pinker Zirkel) handelt es sich um Zuweisungen der Infrastruktur für eine bestimmte Fahrt oder eine Stellanweisung für Stellelemente.

Die Zuweisungswünsche oder Stellanweisungen werden auf der nächsten Ebene („***Safety Control***“) einer Zulassungsprüfung unterzogen. Dabei entscheidet die Komponente Sicherungslogik („***Safety Logic***“), ob der Wunsch des TMS zu einem unsicheren Zustand des Systems führen könnte. In diesem Fall wird der Wunsch abgewiesen. Andernfalls wird der Wunsch des TMS als Anweisung an die untergeordneten Ebenen weitergeben. Die zweite Komponente auf dieser Ebene ist das Modul „***Safety Manager***“. Dieses Modul ist für die Überwachung des sicheren Zustands zuständig. Es ist seitens der RCA derzeit (Stand Mitte 2021) noch nicht entschieden, ob die Trennung in Safety Logic und Safety Manager beibehalten wird.

Unterhalb der Sicherungslogik folgen im sicherheitskritischen Zirkel die Objekt- und Geräteabstraktionsschicht („***Object Aggregation***“ and „***Device Abstraction***“). Die übergeordnete Sicherheitsschicht arbeitet nur mit generischen Regeln und abstrakten Repräsentationen der physischen Objekte. Diese werden in den beiden Zwischenschichten vom abstrakten Objekt über das konkrete Objekt zum konkreten Gerät hin verknüpft und in für die Feldelemente verständliche Nachrichten umgewandelt. Diese Trennung hat den Vorteil, dass die Sicherheitsebene getrennt von der konkreten Ausprägung der beteiligten Objekte generisch definiert werden kann. Die generische Definition soll u. a. die Zulassung vereinfachen.

Die darunter folgende Ebene der Gerätesteuerung („***Device Control***“) ist zwar noch Teil der RCA, sie befindet sich allerdings nicht mehr an zentraler Stelle, wie die übergeordneten Ebenen, sondern direkt an den Feldelementen. Hier werden die konkreten Aufträge für die Feldelemente empfangen und verarbeitet. Bei den Fahrzeugen sind dies die ETCS- bzw. ATO-„***On Board Unit***“ (OBU) (in der RCA als „***Vehicle Supervisor***“ bezeichnet). Zudem weist die RCA die Ortungsmöglichkeit des Fahrzeugs als getrennte Komponente auf („***Vehicle Locator***“), da sie auf Ebene der Geräteabstraktion von einer anderen Komponente angesteuert wird als die Fahrerlaubnis-verarbeitende OBU. Bei den Infrastruktur-Feldelementen geschieht die Ansteuerung über **Object Controller**. Zusätzlich kennt die RCA noch eine dritte Art von Feldelementen, die für Beschäftigte am Gleis gedacht sind und diese schützen sollen.

2.4.4 Modellierungskonzepte

Im Dokument „Domain Knowledge“ [ERTMS Users Group & EULYNX 2020a] sind die grundlegenden Prinzipien, nach denen die RCA aufgebaut ist bzw. funktioniert, beschrieben. Diese Prinzipien werden im Folgenden als Modellierungskonzepte bezeichnet. An dieser Stelle sollen einige für den weiteren Verlauf der Arbeit wichtige Konzepte kurz erläutert werden. Die Konzepte sind parallel zur Entwicklung der smartLogic entstanden und decken sich in einigen Teilen mit dem Datenmodell der neuen Sicherungslogik, während es in anderen Bereichen Unterschiede gibt. Auf Details wird in Kapitel 7 näher eingegangen.

Die Modellierungskonzepte sind verschiedenen Domänen zugeordnet, die in Abb. 6 dargestellt sind. Die „***Topology domain***“ enthält den Aufbau des topologischen Modells, die „***Safety Logic domain***“ Grundlagen für die Funktionsweise der Sicherungslogik, die „***Operational Plan domain***“ Konzepte für die Modellierung des Verhaltens der Fahrzeugbewegungen sowie Vorgaben für den Fahrplan. Die „***Incident domain***“ bildet unerwartete Ereignisse ab und die „***Object Realisation domain***“ verknüpft die Safety Logic mit den physischen Objekten, die wiederum an der Topologie verortet werden. Die „***Maintenance and Monitoring domain***“ wurde bisher nicht näher betrachtet.

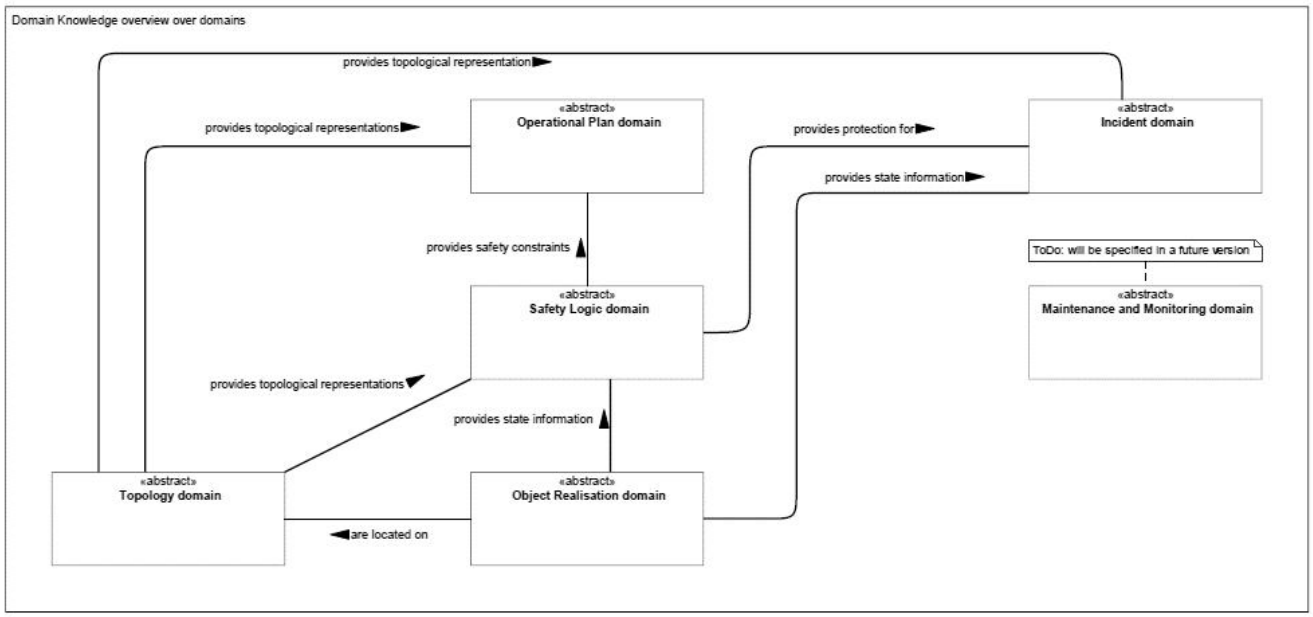


Abb. 6: Domänen der RCA-Modellierungskonzepte
Quelle: [ERTMS Users Group & EULYNX 2020a, S. 7]

Topologie

Die Topologie der RCA basiert bisher nicht auf dem neuen Standard des Rail Topo Models (siehe Kapitel2.5.2), sondern auf einem klassischen Knoten-Kanten-Modell (siehe Kapitel 2.5.1). Die Knoten (***Track Node***) sind demnach Verzweigungspunkte der Topologie und die Gleise zwischen den Verzweigungspunkten Kanten (**Track Edge**). Ein beliebiger zusammenhängender Teil einer Track Edge wird als „**Track Edge Section**“ bezeichnet. Demgegenüber steht das generische Konstrukt einer „**Track Area“**, das einen beliebigen Teil des Gleises bezeichnet, der sich über mehrere Track Edges erstrecken und auch nichtzusammenhängend oder verzweigend sein kann. Vollständig zusammenhängende Track Areas werden als „***Contiguous Track Area***“ bezeichnet. Enthält eine Contiguous Track Area keine Verzweigung, handelt es sich um eine „***Linear Contiguous Track Area***“.

Fahrzeug / Fahrzeugbewegung

Jede Art von gleisgebundener Fahrzeugbewegung wird als „**Movable Object“ (MOB)** modelliert. Kann die Bewegung einem Fahrzeug zugeordnet werden, handelt es sich um ein „***Resolved MOB***“, ansonsten um ein „***Unresolved MOB***“.

Sicherungslogik

Die Sicherungslogik verhindert auf generische Weise, dass einem Fahrzeug die Nutzung eines Fahrwegs erlaubt werden kann (z. B. vom TMS), der nicht sicher befahrbar ist. Zur Abgrenzung zum ETCS-Begriff „Movement Authority“ (MA) verwendet die RCA für die zu prüfende Fahrerlaubnis während der internen Verarbeitung den Begriff „**Movement Permission**“ **(MP)**. Erst nach positiver Prüfung wird die MP als MA an das Fahrzeug geschickt.

Bevor eine MP genehmigt werden kann, muss ihr Fahrweg auf Gefahren geprüft werden. Gefahren können dabei auf unterschiedliche Weise modelliert werden. Stellbare Fahrwegelemente müssen in der richtigen Lage sein, sonst sind sie nicht befahrbar. Zur Modellierung dieser Abhängigkeit verwendet die RCA sogenannte „**Drive Protection Sections“ (DPS)**. Eine DPS markiert die Track Area (dt. Gleisabschnitt) des stellbaren Fahrwegelements, die nicht befahrbar ist, wenn das Element nicht den richtigen Status bzw. die richtige Lage hat (im Fall der Weiche ist das der Bereich, der nicht

befahren werden kann, während die Weiche umgestellt wird). Von den nicht befahrbaren Gleisabschnitten sind Gleisabschnitte abzugrenzen, in denen eine gegenseitige Abhängigkeit der Befahrbarkeit existiert, also in denen bei Belegung des einen Gleisabschnitts durch ein MOB der andere Gleisabschnitt nicht befahrbar ist. Hierzu gehört z. B. der Raum zwischen dem Weichenanfang und dem Grenzzeichen einer Weiche. Diese Gleisabschnitte werden „**Allocation Section**“ **(AS)**, in der neusten Version des Dokuments auch „**Allocation Area**“ **(AA)**, genannt, wobei mehrere abhängige AS eine „**Allocation Section Group**“ **(ASG)** bilden. Die beiden Konzepte sind am Beispiel einer Weiche in Abb. 7 verdeutlicht.

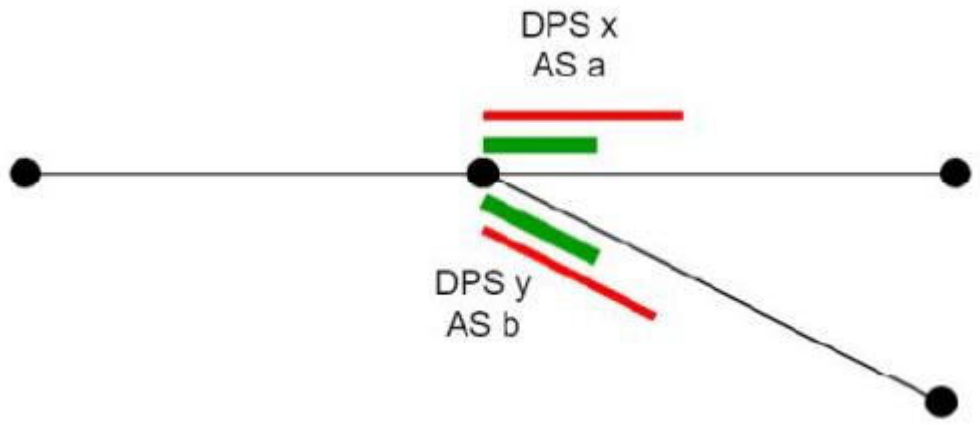


Abb. 7: Drive Protection Section (grün) und Allocation Section (rot)
Quelle: [ERTMS Users Group & EULYNX 2020a, S. 19]

Weitere Einschränkungen der Benutzbarkeit der Infrastruktur, deren Einhaltung von der Sicherungslogik kontrolliert werden muss, können über sogenannte „**Usage Restriction Areas**“ **(URA)** abgebildet werden. Hierzu zählen z. B. Geschwindigkeitsbegrenzungen.

Der Flankenschutzraum wird über sogenannte „***Risk Paths***“ abgedeckt. Es handelt sich um eine Contiguous Track Area, die sich bis zu einem schützenden Flankenschutzelement, dem Gleisende oder einem anderen Fahrzeug, welches vollüberwacht ist, erstreckt. Von jeder AS einer ASG, die ganz oder teilweise Teil der MP ist, geht ein Risk Path aus.

Incidents

Um unerwartete Ereignisse (***Incidents***) werden dreidimensionale Gefahrenbereiche (***Incident Areas***) gelegt, die nicht an den Gleisen, sondern unabhängig von den Gleisen verortet werden. Als Folge von Incidents können Reaktionen definiert werden, die bei Eintritt eines bestimmten Incidents ausgelöst werden.

2.4.5 Ausblick und Bewertung

Aufgrund der breiten Aufstellung der RCA-Initiative im Bereich der europäischen Bahnen und der bewussten Verortung der RCA in der Landschaft bestehender Initiativen, wie auch der angestrebten Kompatibilität zum Programm Shift2Rail der Europäischen Kommission, schätzt der Autor dieser Arbeit die Erfolgsaussichten der RCA als hoch ein. Es wird daher damit gerechnet, dass die infrastrukturseitige Sicherungstechnik sich in den nächsten Jahren schrittweise in Richtung der Überlegungen der RCA weiterentwickelt. Gleichsam befindet sich die RCA derzeit noch in der Entwicklungsphase. Die Ergebnisse dieser Dissertation können daher als Impuls in die weitere Entwicklung einfließen.

2.5 Infrastrukturdatenmodelle

Für die Modellierung der neuen Sicherungslogik ist ein zugrundeliegendes Infrastrukturdatenmodell nötig, um Konzepte wie den Zielpunkt einer Fahrerlaubnis beschreiben zu können. Im vorliegenden Kapitel werden verschiedene bestehende Infrastrukturdatenmodelle vorgestellt. Am Ende der Vorstellung des jeweiligen Modells erfolgt eine kurze Zusammenfassung von Vor- und Nachteilen. Eine ausführlichere Diskussion der Zusammensetzung des für diese Arbeit verwendeten Infrastrukturdatenmodells erfolgt im 7. Hauptkapitel.

Zu betrieblichen Eisenbahn-Infrastrukturdatenmodellen gehört in der Regel die Abbildung der Gleistopologie. Zum besseren Verständnis der Vor- und Nachteile der unterschiedlichen Modelle soll deshalb zunächst in Kapitel 2.5.1 auf Grundlagen zur Modellierung der Gleistopologie eingegangen werden. Anschließend folgt die Vorstellung der einzelnen Modelle und abschließend in Kapitel 2.5.7 ein Fazit.

2.5.1 Grundlagen zur Modellierung der Gleistopologie

Zur Verortung von Infrastrukturelementen, zur Routensuche und für viele weitere Zwecke wird eine Abbildung der Gleistopologie im Datenmodell benötigt. Bei der Gleistopologie handelt es sich um Wegebeziehungen, denen Eisenbahnfahrzeuge folgen können. Die Fahrzeuge können sich über die Gleise nur vor und zurück bewegen und von einem Gleisstrang an bestimmten Verzweigungspunkten (vor allem Weichen) das Gleis wechseln. Dabei ist ein Wechsel nicht in jeder Beziehung, also nicht von jedem Gleis auf jedes andere Gleis möglich, da z. B. Weichen nicht von einem Schenkel zum anderen direkt befahren werden können. Es sind in Einzelfällen auch Teile des Gleises denkbar, die nur in eine Richtung befahren werden dürfen, z. B. Ablaufberge. Die genannten Eigenschaften der Gleistopologie müssen durch das topologische Modell abgebildet werden können.

In diesem Unterkapitel sollen die Grundlagen einiger verbreiteter topologischer Modelle erläutert werden, die das Verständnis der in den weiteren Unterkapiteln dieses Kapitels beschriebenen Infrastrukturmodelle erleichtern. Dabei soll zunächst im ersten Abschnitt auf die klassischen topologischen Modelle eingegangen werden, während im zweiten Abschnitt ein etwas neuerer Ansatz vorgestellt wird, der dem UIC-Standard Rail Topo Model (RTM) (siehe Kapitel 2.5.2) zugrunde liegt. Abschließend sollen im dritten Abschnitt die Vor- und Nachteile des dem RTM zugrundeliegenden Topologiemodells erläutert werden.

Klassische Modelle für die Modellierung der Gleistopologie

[Radtke 2014] enthält eine anschauliche Einführung zur Modellierung der Gleistopologie, auf der die Ausführungen dieses Abschnitts basieren. Die Modellierung der Gleistopologie erfolgt demnach standardmäßig mit den Mitteln der Graphentheorie (häufig auch als Knoten-Kanten-Modell bezeichnet). Dabei befinden sich an den Verzweigungen der Topologie, wie an Weichen, Knoten und die dazwischenliegenden Teile des Gleises, nachfolgend als **Gleissegmente** bezeichnet, bilden die Kanten. Diese Vorgehensweise ist beispielhaft in Abb. 8 dargestellt. Gleis 201 könnte demzufolge ein Stumpfgleis sein und die Gleise 1 und 2 zwei parallelverlaufende Bahnhofsgleise.

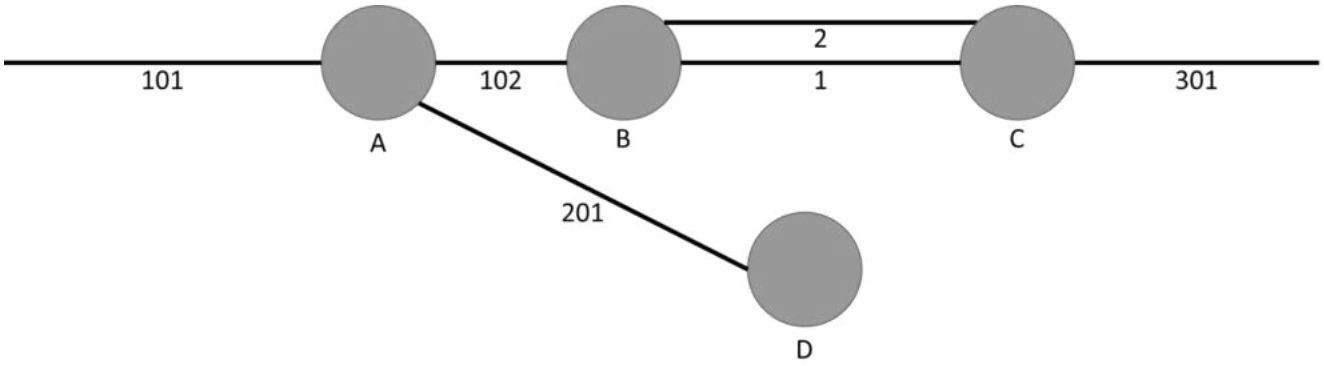


Abb. 8: Intuitives topologisches Knoten-Kanten-Modell
[Eigene Darstellung auf Basis von [Radtke 2014, S. 51]]

Eigenschaften der einzelnen Gleise bzw. der Verzweigungen, wie zulässige Geschwindigkeiten, können auf unterschiedliche Weise im Modell angegeben werden. RADTKE unterscheidet

- ***kantenbezogene Modelle***, bei denen die Eigenschaften in den Kanten gespeichert werden
- ***knotenbezogene Modelle***, bei denen spezielle Knoten existieren, die den Wechsel der Eigenschaft markieren (z. B. ein Geschwindigkeitswechselknoten)

Bei *kantenbezogenen Modellen* besteht die Gefahr, dass Informationen redundant hinterlegt sein müssen (z. B. muss die Geschwindigkeit in jeder Kante gespeichert werden). *Knotenbezogene Modelle* sind dagegen komplexer, da es viele verschiedene Arten von Knoten geben kann, die sich auch an anderen Stellen als an Verzweigungen der Topologie (und Betrachtungsenden bzw. Gleisenden) befinden können. [Radtke 2014, S. 50]

Bei beiden Formen entstehen Probleme an Verzweigungen, da es nicht möglich ist, spezifische Eigenschaften der einzelnen Fahrbeziehungen, wie die grundsätzliche Befahrbarkeit (z. B. ist es nicht möglich an Knoten A von Gleis 201 auf Gleis 102 zu wechseln) oder die jeweils erlaubte Geschwindigkeit in den Weichensträngen ohne Hilfskonstrukte wie Listen abzubilden, welche die erlaubten Fahrbeziehungen und zugehörige Geschwindigkeiten enthalten.

Um diese Probleme zu lösen, werden Verzweigungspunkte in manchen Modellen mit mehreren Knoten modelliert. Beim Colon-Graphen existieren z. B. immer zwei Knoten und ein Übergang zwischen zwei Kanten ist nur über beide Knoten zugelassen. Abb. 9 zeigt ein Beispiel. Der Übergang von 103 nach 102 ist demnach nicht möglich, da nur der Knoten B2 passiert werden würde, nicht aber der Knoten B1.

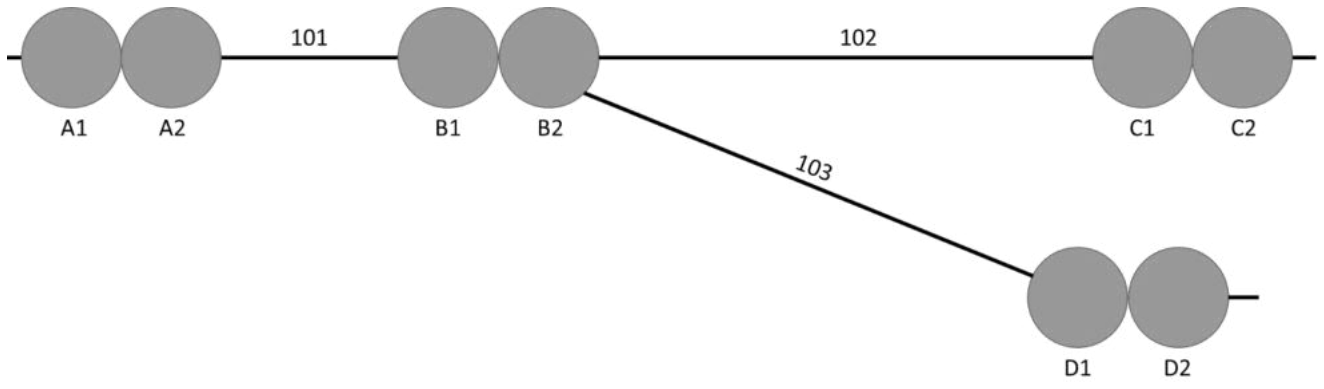


Abb. 9: Beispiel für einen Colon-Graphen
[Eigene Darstellung auf Basis von [Radtke 2014, S. 51]

Bei kantenbezogenen Modellen müsste zur Angabe von Weichengeschwindigkeit zudem der Verzweigungspunkt auch aus mehreren Kanten bestehen. Eine einfache Weiche hätte dann z. B. einen Knoten am Weichenanfang und jeweils einen am Weichenende der beiden Zweige und dazwischen zwei Kanten, an denen die zulässige Geschwindigkeit hinterlegt werden könnte. Abb. 10 enthält hierfür ein Beispiel. Eine Kombination mit dem Colon-Graphen wäre ebenfalls möglich, um Nichtbefahrbarkeiten abzubilden.

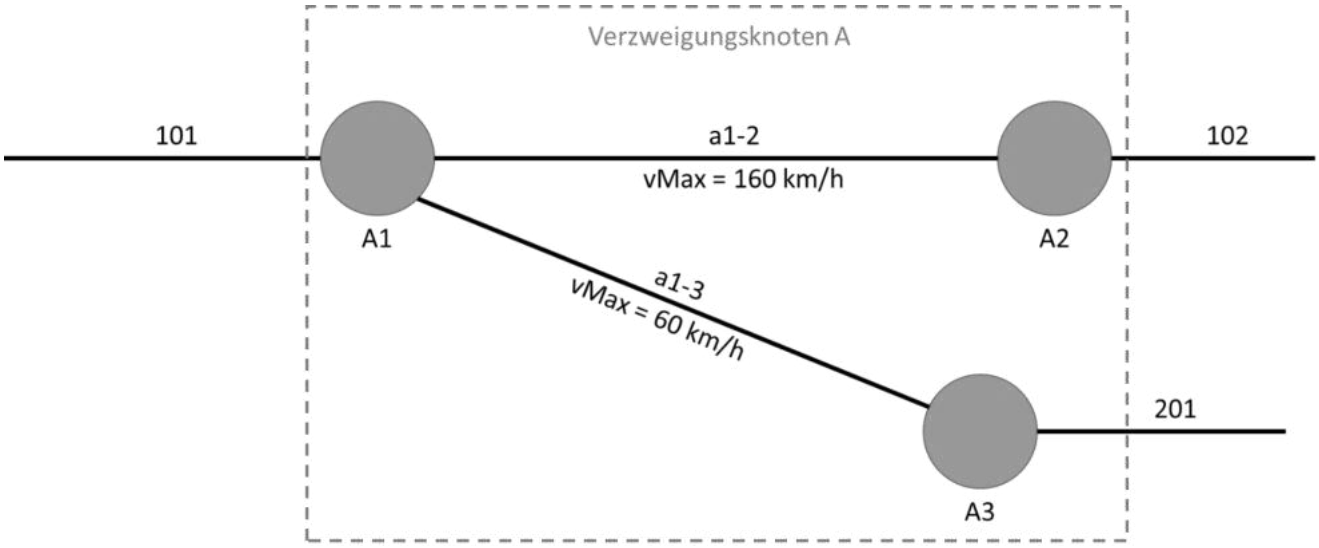


Abb. 10: Modellierung von Verzweigungspunkten mit mehreren Knoten
[Eigene Darstellung]

Gély et al (2010)

Eine weitere Möglichkeit, die topologischen Beziehungen zu modellieren wurde 2010 von GÉLY ET AL vorgeschlagen [Gély et al. 2010]. Hierbei werden die Gleise nicht als Kanten, sondern als Knoten modelliert. Dadurch würde das Modell skalierbarer, da mehrere Knoten zusammengefasst werden können. Somit sei eine mikroskopische und makroskopische Ansicht des gleichen Modells möglich.

Im Konzept von GÉLY ET AL sind alle physischen Elemente des Gleises Knoten und die Kanten zwischen den Knoten stellen die Befahrbarkeit dar, wie in Abb. 11 dargestellt.

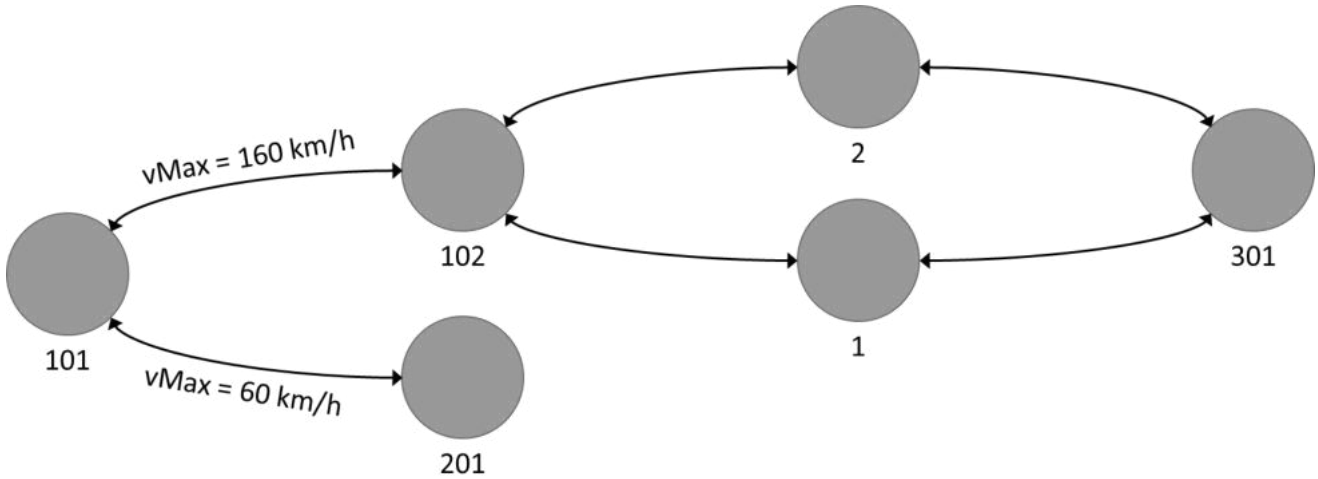


Abb. 11: Modellierung der Gleise als Knoten und der Übergänge zwischen den Gleisen als Kanten
[Eigene Darstellung nach Gély et al. 2010, S. 200]

Eine Weiche existiert in diesem Modell nicht als eigenständiges topologisches Element, sondern wird nur über die Verknüpfung der drei Gleisstränge abgebildet. (Die physischen Elemente repräsentieren rein das Gleis vom jeweiligen Weichenanfang bis zum nächsten Weichenanfang, die Weichen selbst haben also im topologischen Modell keine physische Ausdehnung.) Bei den Kanten handelt es sich um gerichtete Kanten. Es können sich also zwischen zwei Knoten zwei Kanten befinden, wenn ein Übergang vom einen physischen Element auf das andere in beiden Richtungen möglich ist; dies muss nicht immer der Fall sein. In Abb. 11 sind die beiden gerichteten Kanten jedoch aus Vereinfachungsgründen zu einer beidseitig gerichteten Kante zusammengefasst.

Da ein Gleissegment, also ein topologischer Knoten im Modell nach GÉLY ET AL, physisch jedoch auch nach der Logik des RTM eine eindimensionale Ausdehnung hat, müssen die beiden Enden des Gleissegments eindeutig identifizierbar sein. Ansonsten könnten zum Beispiel Punktobjekte auf dem Gleissegment nicht eindeutig verortet werden. Daher hat das Gleissegment zur Verbindung der Befahrbarkeitskanten (Positioned Relation) zwei Anknüpfungspunkte A und B und dazwischen eine definierte Länge. Die Befahrbarkeitskanten enthalten dann jeweils als Ursprung und als Ziel einen Zeiger auf ein Gleissegment (= Knoten im Modell) und den Hinweis auf das verknüpfte Ende ‚A' oder ‚B'. Abb. 12 verdeutlicht dies schematisch.

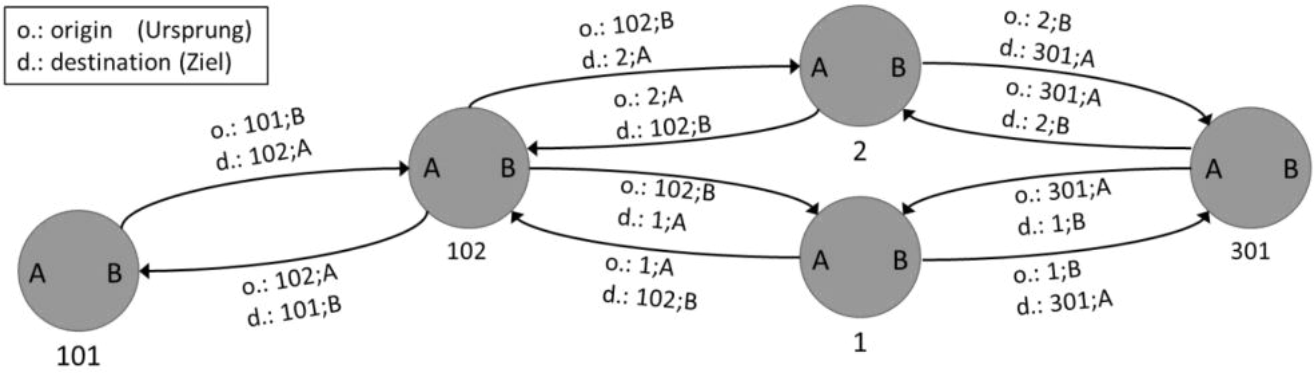


Abb. 12: Richtungsbezogene Verknüpfung der Gleissegmente
[Eigene Darstellung]

In den Befahrbarkeitskanten können auch weitere Informationen wie die zulässige Geschwindigkeit gespeichert werden.

Vor- und Nachteile

Die von GÉLY ET AL beschriebene Form der Modellierung der Gleistopologie bietet den Autoren zufolge gegenüber der intuitiveren klassischen Systematik, die im ersten Abschnitt beschrieben wurde, folgende Vorteile (vgl. hierzu [Gély et al. 2010] und [IRS 30100:2016]):

- alle physischen Elemente seien konsistent als Knoten modelliert (beim klassischen Modell sind sie teilweise Knoten und teilweise Kanten)
- alle physischen Elemente erbten von derselben Oberklasse, da sie alle als Knoten modelliert werden; Attribute könnten so leichter und konsistenter Gruppen von physischen Elementen über die Oberklassen zugeordnet werden
- über die Kanten könnten die Fahrbeziehungen mit dazugehörigen Eigenschaften konsistent und einfach dargestellt werden, Hilfskonstrukte wie Fahrwegtabellen würden nicht benötigt

- das Netzwerk sei skalierbar, da mehrere Knoten mit ihren Verbindungskanten zu einem Knoten zusammengefasst werden könnten, während im klassischen System bei einer Zusammenfassung Knoten und Kanten in einer Verletzung der grundsätzlichen Modellregeln gemeinsam zusammengefasst werden müssten

Als Nachteil steht den Vorteilen vor allem gegenüber, dass das Konzept etwas komplizierter und nicht so intuitiv wie das klassische Konzept zur Modellierung der Gleistopologie ist.

Die Überlegungen von GÉLY ET AL dienen als Grundlage für die Definition des Rail Topo Models (RTM), das in Kapitel 2.5.2 näher erläutert wird.

2.5.2 Rail Topo Model (RTM)

In der Eisenbahnbranche existieren derzeit viele verschiedene Infrastrukturdatenmodelle mit unterschiedlichen Anwendungszwecken und deshalb auch unterschiedlichem Aufbau. Ein erklärtes Ziel des internationalen Eisenbahnverbandes UIC ist es, die Austauschbarkeit von Infrastrukturdaten zwischen den verschiedenen Datenmodellen zu erhöhen. Hierfür muss die Beschreibung der Gleistopologie miteinander kompatibel sein. Aus diesem Grund wurde das ***Rail Topo Model*** **(RTM)** von der UIC als eigenständiger Standard für gleistopologische Datenmodelle festgelegt [IRS 30100:2016]. Es handelt sich dabei nicht um ein vollständiges Datenmodell, sondern um ein Metamodell, welches eine Struktur für die Topologiedaten vorgibt. Das RTM ist in der Unified Modelling Language (UML) als Klassendiagramm notiert. Im Folgenden werden die wichtigsten Grundzüge des RTM kurz zusammengefasst.

Das RTM unterstützt beliebig viele Detailierungsgrade, z. B. eine Korridordarstellung mit Betriebsstellen und Strecken oder eine mikroskopische Darstellung mit einzelnen Gleisen und Weichen. Zwischen diesen Ebenen besteht die Möglichkeit, Daten zu aggregieren bzw. disaggregieren, so dass je nach Anwendungsfall nur ein Teil der Daten übertragen werden muss, dabei aber immer auf die gleiche Datenbasis zurückgegriffen wird. Physische Elemente können als Punkte, lineare Objekte oder flächige Objekte definiert werden.

Um die Flexibilität des Rail Topo Models in Bezug auf die unterschiedlichen Anforderungen verschiedener geografischer Verortungssysteme zu erhöhen, unterstützt das RTM verschiedene Möglichkeiten, physische Elemente zu verorten, die als Referenzsysteme bezeichnet werden. Hierzu gehören

- die lineare Verortung (***Linear referencing***), z. B. entlang von Kilometrierungsachsen,
- die Verortung auf ein Geo-Koordinatensystem (***Positioning***) und
- Bildkoordinaten (***Screen Coordinates***) für die Anzeige auf Plänen oder Anzeigegeräten.

Das RTM basiert auf dem Knoten-Kanten-Modell nach [Gély et al. 2010], bei dem die Kanten keine physischen Objekte (die Gleise) repräsentieren, sondern nur die Verbindung zwischen den physischen Objekten. Die Gleise sind stattdessen jeweils Knoten (vgl. Kapitel 2.5.1). Das RTM kennt in seiner Topologie-Modellierung demnach keine Unterscheidung zwischen Weichen und einfachen Gleisen. Eine Weiche besteht vielmehr aus drei Gleisen, die eine Fahrbeziehung zueinander haben, die über die Kanten abgebildet sind. Die Kanten sind gerichtet. Es kann also zwei gegensätzlich gerichtete Kanten zwischen den Knoten geben, die unterschiedliche Eigenschaften haben. Eine Rückfallweiche kann beispielsweise eine Fahrbeziehung in eine Richtung zulassen, in die andere aber nicht. Vergleiche zur Modellierung des RTM auch [Wunsch & Jaekel 2017]. Abb. 13 verdeutlicht die topologische Modellierung im RTM.

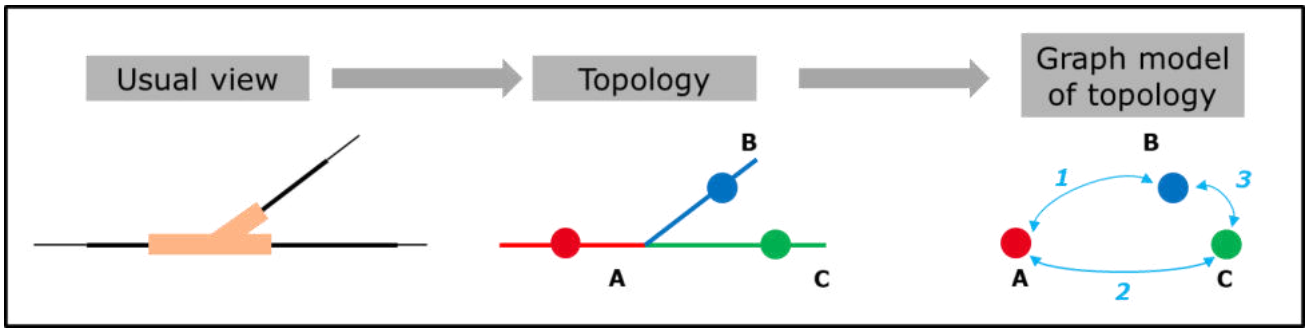


Abb. 13: topologische Modellierung im Rail Topo Model (RTM)
Quelle: [IRS 30100:2016] (grafisch nachgebessert)

Das Rail Topo Model ist von der UIC als Standard definiert worden und damit für die erforderliche Modellierung der Topologie im Rahmen dieser Arbeit auf jeden Fall relevant. Sein Aufbau ist so gestaltet, dass er einen möglichst vielfältigen Einsatz zulässt. Allerdings ist das Modell aktuell noch nicht weit verbreitet und es besteht zu älteren Modellen aufgrund unterschiedlicher Knoten-Kanten-Modelle ein Kompatibilitätsproblem. Das im RTM gewählte Knoten-Kanten-Modell bietet jedoch Vorteile gegenüber klassischen Knoten-Kanten-Modellen bei denen Weichen Knoten und Gleise dazwischen Kanten sind. So lässt sich die Befahrbarkeit der Weichen mit allen dazugehörigen Eigenschaften wie eingeschränkten Geschwindigkeiten für jede mögliche Verbindung leicht als Kanteneigenschaften modellieren und es benötigt keine Hilfskonstrukte wie Befahrbarkeitstabellen. Zudem können Daten zwischen den verschiedenen Detailierungsgraden korrekt aggregiert bzw. disaggregiert werden.

2.5.3 RailML

RailML (Railway Markup Language) ist ein Datenmodell für das Eisenbahnwesen, welches von einem eigetragenen Verein namens railML.org entwickelt wird. Er besteht aus Interessierten Entwicklern aus verschiedenen europäischen Ländern und ist unabhängig von EIUs, EVUs, Herstellern oder staatlichen Organisationen. Die Organisationen aus den genannten Bereichen werden allerdings von railML.org als Partner gelistet. Ziel ist die Schaffung eines Datenformats, das den internationalen Austausch eisenbahnbezogener Daten ermöglicht. Die Internetseite www.railml.org dient als Plattform für alle offiziellen RailML bezogenen Veröffentlichungen. Eine Dokumentation findet sich auch im Wiki der genannten Internetseite. RailML ist OpenSource.

Das Modell ist als XML-Schema definiert und besteht aus den vier Subschemas Fahrplan (***Timetable***), Fahrzeug (***Rollingstock***), Infrastruktur (***Infrastructure***) und Sicherungstechnik (***Interlocking***). Die Subschemas enthalten Vorgaben zur Beschreibung verschiedener Objekte aus dem Eisenbahnwesen wie ein Gleis oder einen Controller eines Stellelements. Zur Beschreibung gehören die Attribute mit ihren Eigenschaften. Ab Version 3.0 bzw. 3.1 soll RailML bei der Topologiemodellierung kompatibel zum Rail Topo Model sein.

Abb. 14 zeigt das Interlocking-Subschema der RailML 3. Zum Interlocking gehören die einzelnen zu steuernden Elemente (***Assets***), die physischer (z. B. Weichen) aber auch logischer (z. B. Fahrstraßen, Durchrutschwege und Gefahrpunkte) Natur sein können. Weiterhin gehören die Bedienplätze (***Controller***) und die einzelnen Stellwerksinstanzen (***Signal Boxes***) dazu, ebenso wie die EIU, die für die betrachtete LST verantwortlich sind.

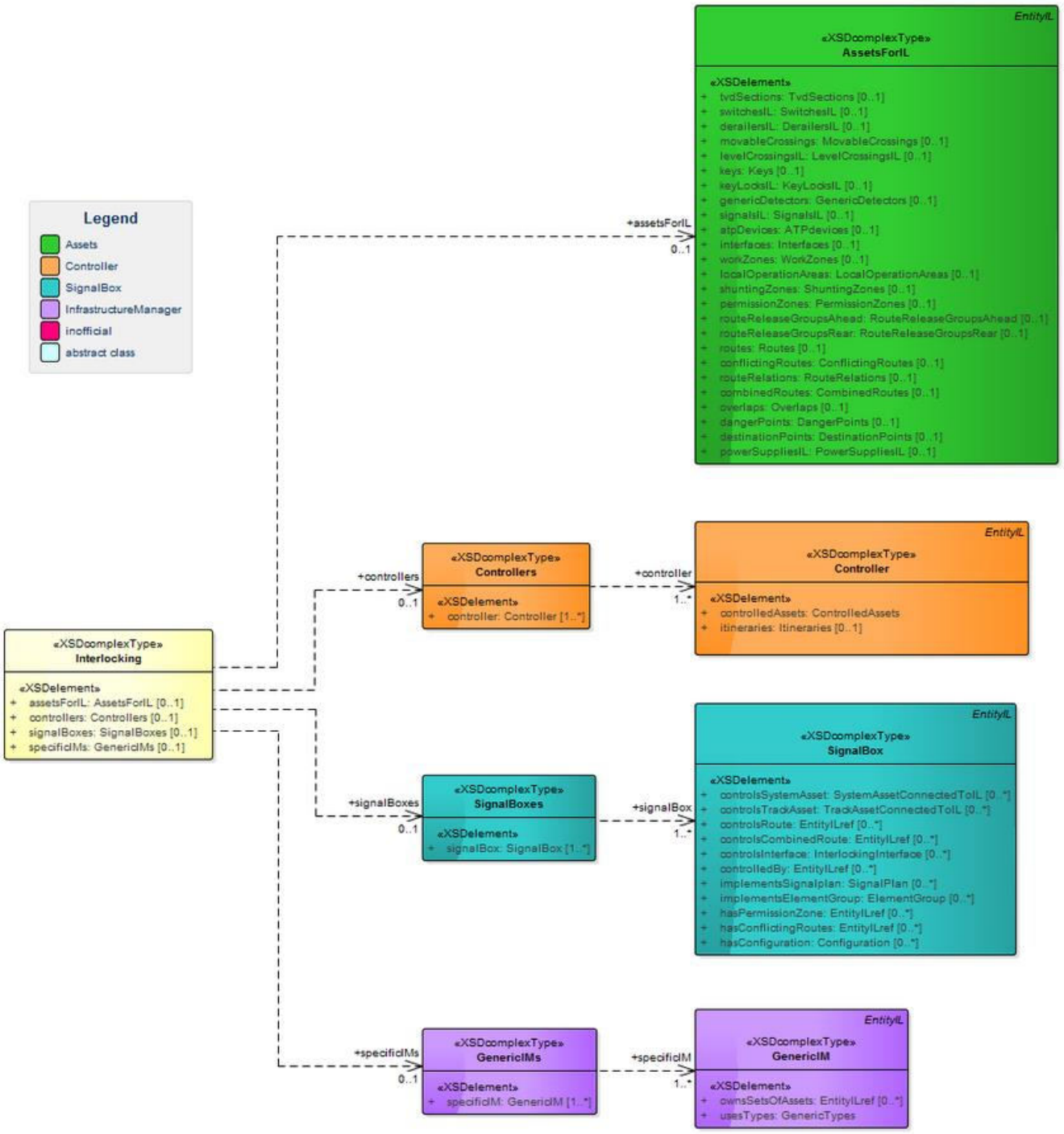


Abb. 14: Interlocking-Subschema der RailML 3.1
Quelle: https://wiki3.railml.org/DataModel/3.1/IL/ (abgerufen am 24.09.2021, 22:25 Uhr)

RailML ist zwar als internationales, standardisiertes, universelles Datenaustauschformat für den Eisenbahnsektor angelegt, kann diese Rolle allerdings derzeit nicht erfüllen, da von Seiten der Eisenbahnunternehmen und anderen etablierten Organisationen keine verbindlichen Beschlüsse zu seiner konsequenten Nutzung bestehen. Weiterhin fehlen für produktive Anwendungen häufig noch Details, die nicht zeitnah international abgestimmt werden können. Es bleibt abzuwarten, ob eine Forcierung von RailML in Zusammenhang mit dem RTM durch die UIC zu einer stärkeren Verwendung von RailML führen wird.

2.5.4 PlanPro

Das ***PlanPro***-Format ist wie RailML XML-basiert und deckt den Bereich der LST-Planung ab. Es ist in Deutschland seit 2009 entstanden und wurde in die u. a. bei der DB verbreitete Planungssoftware ***ProSig*** ab Version 7 EPU integriert. Es dient dem Austausch von LST-Planungsdaten zwischen verschiedenen Akteuren, die am Planungsprozess beteiligt sind. Zudem können verschiedene Arten von Plänen aus den PlanPro-Daten generiert werden. Somit wird das Datenmodell während des Planungsprozesses immer weiter angereichert und redundante Informationen in verschiedenen Plänen und damit eine potenzielle Fehlerquelle werden vermieden.

PlanPro besteht aus mehreren XML-Schema-Dateien, die verbindliche Vorgaben für die auszutauschenden Daten enthalten. Dabei sind auch Details wie die Art des Fundaments eines Signals oder dessen Signalschirm spezifiziert, aber auch sicherungstechnisch relevante Daten zu den Signalbegriffen. Ab Version 1.9.0 wird auch die ETCS-Aursrüstungsplanung unterstützt.

PlanPro verwendet ein klassisches Knoten-Kanten-Modell, welches auf zwei Abstraktionsebenen existiert (vgl. Abb. 15). Auf der topologischen Ebene repräsentieren topologische Knoten (***TOP-Knoten***) verzweigende Fahrwegelemente, Gleisenden, Digitalisierungsenden und Betrachtungsenden. Neben der topologischen Ebene gibt es auch eine geografische Ebene. TOP-Knoten sind dabei immer auch geografische Knoten (***GEO-Knoten***). Eine TOP-Kante kann aber durch weitere GEO-Knoten in mehrere GEO-Kanten unterteilt sein, um die Gleislage abzubilden.

Mit den TOP- bzw. GEO-Kanten sind in der Regel eine Höhenlinie und eine Streckenlinie verknüpft. Die Streckenlinie verläuft bei zweigleisigen Strecken mittig zwischen den zugehörigen TOP-Kanten. Infrastrukturelemente können je nach Typ als punktförmiges oder lineares Objekt an TOP-Kanten oder Strecken verortet werden. Dabei wird der Abstand zum Beginn der Kante bzw. Strecke und ggf. der seitliche Abstand zur Kante oder Streckenlinie angegeben.

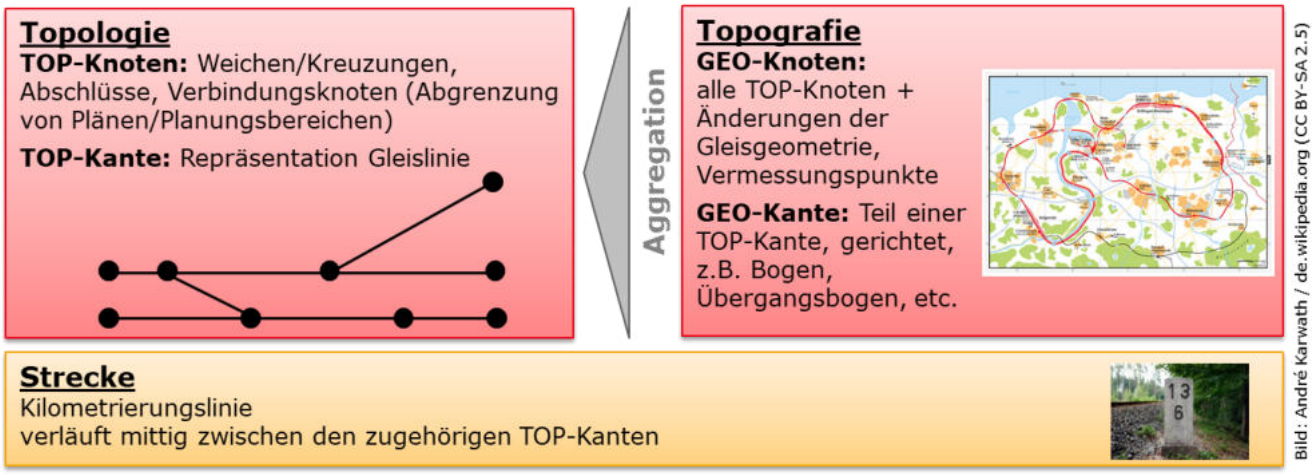


Abb. 15: Abbildung des Gleisnetzes in PlanPro
[Eigene Darstellung]

Infrastrukturobjekte können zusätzlich zu ihrer physischen, verorteten Repräsentation in Form von Punkt- oder Bereichsobjekten als Stellelemente definiert werden. Das Stellelement ist dann ein separates Objekt des Modells, welches mit dem physischen Objekt verbunden wird. Stellelemente bilden die LST-Ansicht des Infrastrukturelements. Sie können Stellbereichen und ESTW-Zentraleinheiten zugeordnet werden. Über diese Objekte können sie wiederum zu Bedienbezirken und Bedienzentralen oder logischen Gruppen wie Weichenlaufketten zusammengefasst werden.

PlanPro enthält damit ein sehr umfassendes Modell für Planungszwecke, welches allerdings rein infrastrukturbezogen ist und keine Datenstrukturen für die Modellierung von Zugfahrten bereithält. Der Anwendungsbereich ist damit enger als bei RailML. PlanPro wird bereits real eingesetzt. Damit sind Daten aus der Praxis vorhanden bzw. können über das Planungstool ProSig erzeugt werden. Allerdings ist die Datenverfügbarkeit derzeit noch auf einem niedrigen Niveau, da viele Stellwerksbereiche noch keine digitalisierten Planungsunterlagen haben. Aufgrund des verwendeten topologischen Knoten-Kanten-Modells ist PlanPro derzeit nicht mit dem Rail Topo Model kompatibel.

Weitere Informationen zu PlanPro finden sich unter anderem in [DB Netz AG 2015; Buder & Oelschläger 2014b; Buder & Oelschläger 2014a; Maschek 2017]. Das Schema kann unter fahrweg.dbnetze.com/fahrweg-de/unternehmen/dienstleister/PlanPro heruntergeladen werden.

2.5.5 XML-ISS

Die DB verwendet mit ***XML-ISS*** noch ein weiteres XML-basiertes Datenformat, welches vor allem für die Fahrplanerstellung, aber auch für die Erstellung von Echtzeit-Prognosen in den Betriebszentralen genutzt wird. Das Format ist in diesem Bereich bei der DB verbreitet und es existieren umfangreiche Datensätze des Streckennetzes.

Das XML-ISS-Format ist wesentlich weniger umfangreich als das PlanPro-Format, da für den Zweck der Fahrplanerstellung viele Planungsdaten irrelevant sind. Es enthält dafür auch für die Fahrplanerstellung relevante Datenstrukturen, die in PlanPro nicht vorhanden sind. Hierzu zählen z. B. vordefinierte Umleitungsstrecken. Im Bereich der LST sind nur die wichtigsten Informationen wie die vorhandenen Fahrstraßen und Signale, welche die Fahrdynamik beeinflussen können, vorgesehen. ETCS ist bereits enthalten.

Die Infrastruktur ist in sogenannte „***Spurplanbetriebsstellen***“ unterteilt, welche die drei Elemente ***Spurplanabschnitt***, ***Bahnhofsgleise*** und ***Betriebsstellenfahrwege*** enthält. Spurplanabschnitte repräsentieren Gleise zwischen Weichen und sind einer Strecke zugeordnet. Sie enthalten ***Spurplanknoten***, die wiederum Infrastrukturelemente wie Weichen (eine Weiche besteht aus mehreren Spurplanknoten für Weichenanfang, Weichenstamm und Weichenabzweig) Bahnübergänge oder Informationspunkte repräsentieren. Informationspunkte repräsentieren ortsgebundene Informationen wie zum Beispiel Geschwindigkeitswechsel. Sie sind immer mit einem bestimmten Gleis verknüpft.

Betriebsstellenfahrwege sind die regulären Fahrmöglichkeiten auf der Infrastruktur, in der Regel beschränkt auf Zugfahrten. Sie beginnen und enden an einem der drei Spurplanknoten ***Halteplatz***, ***Prellbock*** oder ***Betriebsstellengrenze***. Betriebsstellenfahrwege sind daher nicht identisch mit Fahrstraßen, die an einem Signal beginnen und enden. Der Verlauf von Betriebsstellenfahrwegen wird durch sogenannte „***Wegweiser***“ definiert. Diese repräsentieren eine bestimmte Weichenlage, die für den Betriebsstellenfahrweg erforderlich ist. Dabei wird für jede Weiche im Betriebsstellenfahrweg hinterlegt, ob diese im Stamm, links abzweigend oder rechts abzweigend befahren wird.

Zusätzlich sind im sogenannten „***Ordnungsrahmen***“ die Strecken, Betriebsstellen und Bahnsteige näher beschrieben. Strecken gliedern sich in Streckenabschnitte, denen die Betriebsstellen zugeordnet sind. Es können auch potenzielle Langsamfahrstellen definiert werden. Die Streckenabschnitte enthalten zudem eine Reihe genereller Daten zu diesem Streckenabschnitt. Dasselbe gilt für die Betriebsstellen. Den Betriebsstellen sind die Bahnsteige und diesen Bahnsteigkanten zugeordnet. Weiterhin gibt es die ***Stammdaten***, die unter anderem Daten wie Wertebereiche oder für die Fahrplangestaltung und Anschlussdisposition wichtige Informationen wie Übergangszeiten enthalten.

XML-ISS erfüllt damit alle Anforderungen für die Fahrplanung und Disposition. Der Umfang der Datenspezifikationen ist jedoch für diese Anwendungsfälle ausgelegt, so dass für darüberhinausgehende Anwendungsfälle Definitionen fehlen, beispielsweise zur Beschreibung der LST auf mikroskopischer Ebene.

2.5.6 Weitere Datenmodelle

SCHUBERT ET AL stellen in [Schubert et al. 2016] neben dem RTM mehrere weitere Modelle vor, welche Infrastrukturobjekte beschreiben und die Verortung von Geodaten ermöglichen. Im ***Mapdata 3.1-***Modell existieren hierzu verschiedene Layer, in denen eine unterschiedliche Verortung stattfinden kann: Dies sind die Verortung über dreidimensionale Raumkoordinaten mit Angabe einer Standardabweichung zur Transparenz über Koordinatengenauigkeiten, ein Topologie-Layer ähnlich dem des RTMs (vgl. Kapitel 2.5.2) und ein Geometrie-Layer zur Beschreibung des dreidimensionalen geometrischen Verlaufs des Gleises.

Das Mapdata 3.1-Modell wird um die ***Railway Infrastructure Map*** erweitert, die weitere Objekte definiert, die in Zusammenhang mit der Schieneninfrastruktur abgebildet werden. Die Objekte sind zunächst unabhängig von ihrer Verortung. Sie können als ***Point Element*** (Punktobjekt), ***Way Element*** (Linienobjekt) und ***Aggregation Element*** (Gruppierungselement) definiert werden. Punktobjekten kann dabei genau eine Geo-Koordinate zugewiesen werden, während Linienobjekte eine geordnete Sequenz von Positionskoordinaten zugewiesen werden kann, die entlang einer oder mehrerer Gleiskanten verortet werden. Das Gruppierungselement „ist ein komplexes Element, welches durch mehrere Punkt- und Linienelemente beschrieben werden kann, wie z. B. ein Bahnhofsbereich“ [Schubert et al. 2016, S. 9].

Die vorgestellten Modelle sind jedoch wenig verbreitet und bieten für die Sicherungslogik keine signifikanten Vorteile gegenüber den anderen Modellen. Sie werden daher hier nicht detaillierter betrachtet.

2.5.7 Fazit zu den bestehenden Datenmodellen

Die Nutzung von bestehenden Infrastrukturdatenmodellen für die Entwicklung der smartLogic kann Vorteile haben, da es wahrscheinlicher ist, dass passende Daten zukünftig auch bereitgestellt werden können. Auf der anderen Seite sollte das Infrastrukturdatenmodell die Funktionsweise der smartLogic auch möglichst nicht einschränken.

Alle bekannten Modelle außer dem RTM als topologischem Meta-Modell wurden zur Abbildung der bestehenden Infrastruktur mit festen Fahrstraßen etc. entworfen. Da das Konzept der Fahrstraße und auch einige weitere etablierte Konzepte in der vorliegenden Arbeit in Frage gestellt werden sollen, erscheint eine vollständige Verwendung eines der genannten Modelle nicht sinnvoll zu sein. Stattdessen sollte im 7. Hauptkapitel auch ein Infrastrukturdatenmodell für die smartLogic erarbeitet werden. Es sollte dabei jedoch geprüft werden, welche Elemente der anderen Modelle in dieses Modell übernommen werden können.

Beim RTM handelt es sich um einen vereinbarten Standard für die Modellierung der Gleistopologie mit Vorteilen gegenüber klassischeren Topologiemodellen. Deshalb erscheint es sinnvoll, diesen Standard möglichst einzuhalten.

Am meisten Daten liegen in Deutschland derzeit im XML-ISS-Format vor, da diese Daten deutschlandweit der Fahrplanerstellung zugrundeliegen. Jedoch sind die Daten aufgrund ihrer Ausrichtung für die Fahrplanerstellung und Disposition in Hinblick bzgl. der LST-Komponenten

weniger detailliert als z. B. PlanPro. PlanPro ist dagegen auf die LST-Planung ausgerichtet und so konzipiert, dass zukünftig Planungsdaten für Zwecke der Sicherungslogik mit relativ geringem Aufwand übernommen werden könnten. Allerdings liegen derzeit noch wenig PlanPro-Daten von realen Betriebsstellen vor.

2.6 Methoden für den sicherheitskritischen Entwurf

In der Arbeit soll eine neue Sicherungslogik entwickelt werden. Um eine hohe Qualität der Entwicklung sicherzustellen, ist es zielführend, bewährten Entwicklungsmethoden – soweit möglich – zu folgen und verbreitete Methoden beispielsweise für die Phase der Modellierung zu verwenden. In diesem Kapitel sollen zunächst in Kapitel 2.6.1 entsprechende, mögliche Entwicklungsmethoden besprochen werden und anschließend in Kapitel 2.6.2 gängige Modellierungsarten vorgestellt werden, die im Rahmen der Entwicklungsmethoden verwendet werden können.

2.6.1 Entwicklungsmethoden

Für den Entwicklungsprozess sicherheitskritischer Komponenten existiert mit dem V-Modell ein Vorgehensmodell als genormte Entwicklungsmethode (siehe erster Abschnitt). Da es sich bei dieser Arbeit um ein Forschungsprojekt handelt, an dessen Ende zwar Erkenntnisse für die Entwicklung einer neuen Sicherungslogik stehen soll, aber kein Produktivsystem entwickelt wird, muss das Vorgehen in dieser Arbeit nicht zwangsläufig streng der Norm folgen. Eine alternative grundsätzlich denkbare Entwicklungsmethode wäre es, den Entwicklungsprozess deutlicher agiler zu gestalten (zweiter Abschnitt). Auch hybride Ansätze werden in der Fachwelt diskutiert (siehe dritter Abschnitt).

Dieses Unterkapitel stellt die Unterschiede dieser Entwicklungsmethoden vor. Eine Auswahl der verwendeten Entwicklungsmethode erfolgt in Kapitel 3.6.

V-Modell

Der Entwurf sicherheitskritischer Systeme im Eisenbahnwesen, wie der Sicherungslogik, muss grundsätzlich den Euro-Normen [DIN EN 50126-1:2017; DIN EN 50128:2011; DIN EN 50129:2018 + AC:2019] folgen. Das grundsätzliche Vorgehen ist in der [DIN EN 50126-1:2017, 44f] vorgegeben und entspricht dem bekannten ***V-Modell***, welches in Abb. 16 dargestellt ist.

Der Ablauf des Entwicklungsprozesses gemäß dem V-Modell beginnt nach der groben Konzeptionierung mit einer Systemdefinition, auf welche eine Risikoanalyse folgt. Darauf aufbauend werden Systemanforderungen definiert. Hierbei handelt es sich um funktionale Anforderungen und Anforderungen aus der Risikoanalyse an die Zuverlässigkeit des Systems und seine Prozesse (Akzeptanzkriterien). Die Systemanforderungen werden dann ggf. auf Subsysteme aufgeteilt. Anschließend folgen Entwurf und Implementierung. Die späteren Phasen von der Herstellung über den Betrieb bis zur Außerbetriebnahme und Entsorgung sind nicht Teil der vorliegenden Arbeit und werden daher hier nicht weiter beschrieben.

Jeder Arbeitsschritt ist umfangreich zu dokumentieren und alle Dokumente müssen einen Freigabeprozess mit verschiedenen Beteiligten durchlaufen. Erkenntnisse aus späteren Entwicklungsphasen, in denen frühere Phasen regelmäßig validiert werden, werden iterativ in die Ergebnisdokumentation der früheren Phasen eingearbeitet und ab diesem Zeitpunkt im weiteren Prozess berücksichtigt.

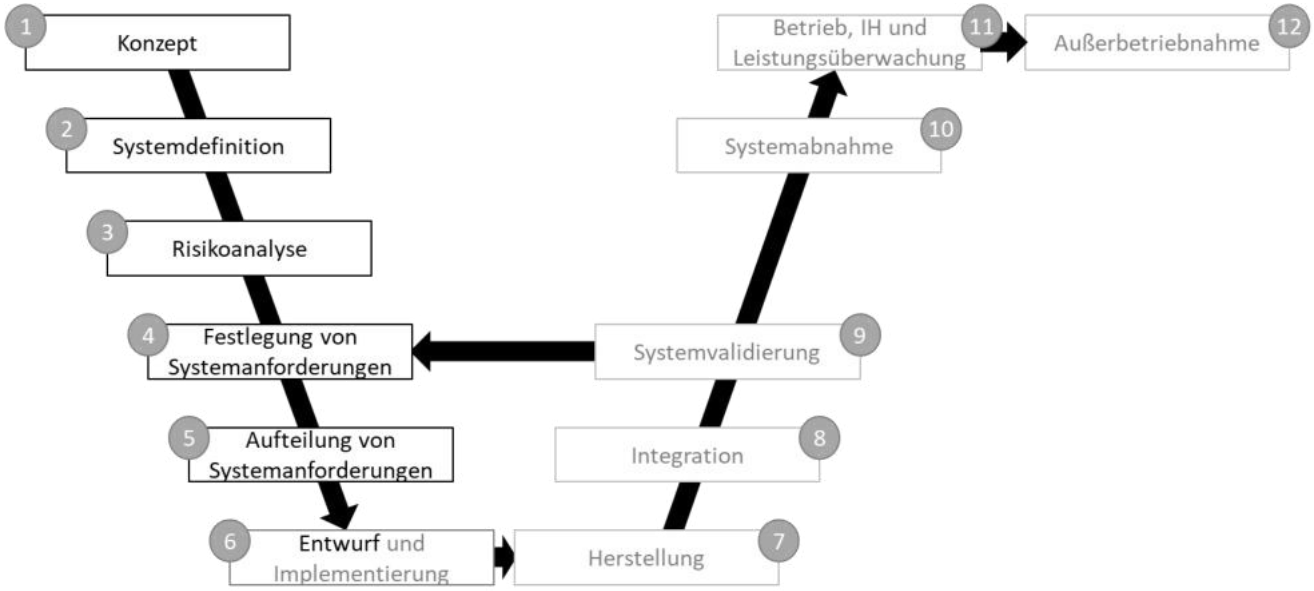


Abb. 16: V-Zyklus-Darstellung des Lebenslaufs eines sicherheitskritischen Systems
Eigene Darstellung nach [DIN EN 50126-1:2017, S. 45], die nicht betrachteten Stufen sind ausgegraut

Agile Methode

Bei der ***agilen Methode*** erfolgt keine vollständige Funktionsanalyse zu Beginn, sondern es wird zunächst eine für einfache Anwendungsfälle bereits lauffähige Version einer Sicherungslogik mit Basisfunktionalität geschaffen, die dann in weiteren Arbeits-Iterationen (Sprints) erweitert wird. Hierbei kann jeweils verifiziert werden, ob das bisher Entwickelte den Anforderungen der späteren Nutzer entspricht.

Diese Entwicklungsmethode hat grundsätzlich verschiedene Vorteile, die typisch für agile Arbeitsansätze sind und vor allem auf Nachteilen des V-Modells beruhen (vgl. zu Vor- und Nachteilen von Wasserfall- und agilem Ansatz Kapitel 1.4 in [Kuster et al. 2019]). So birgt das V-Modell die Gefahr, dass sich das Entwicklungsteam in den frühen Phasen, vor allem bei der Anforderungsdefinition, „verkünstelt“ und den Rahmen zu groß spannt, indem möglichst jede erdenkliche Anforderung an das spätere System integriert werden soll. Dieses Risiko steht vor allem dem Ziel einer geringen Komplexität der zu entwickelnden Sicherungslogik entgegen (Kriterium der möglichst optimalen Zielerfüllung) und auch den Kriterien auf Basis der äußeren Rahmenbedingungen in dieser Arbeit aus Kapitel 3.6.1.

Im Bereich der Eisenbahnsicherungstechnik ist das geschilderte Problem zum Beispiel bei ETCS zu sehen, welches einen umfangreichen Katalog an Funktionalitäten enthält, von denen in der Regel nur wenige wirklich genutzt werden. Dieser Umstand macht insbesondere die ETCS-Bordsysteme teuer, die aus Gründen der Interoperabilität alle spezifizierten Funktion beherrschen müssen, selbst wenn sie infrastrukturseitig nirgends genutzt werden.[7]

Bei der konkreten Umsetzung von ETCS zeigt sich jedoch ein weiteres Problem. So waren die erarbeiten umfangreichen Spezifikationen im Realbetrieb immer noch nicht ausreichend, um alle Anwendungsfälle so abzudecken, dass sie von den Eisenbahnunternehmen wirtschaftlich genutzt werden konnten. So mussten trotz umfangreicher Überlegungen in frühen Phasen des

[7] Zur Verteidigung des umfangreichen ETCS-Spezifikationen sei noch bemerkt, dass der umfangreiche Funktionskatalog derzeit auch notwendig ist, damit alle nationalen Regeln befolgt werden können. Das Problem ist hier also vor allem die fehlende Harmonisierung der Regelwerke.

Entwicklungsprozesses später große Änderungen umgesetzt werden (z. B. Mode LS in Baseline 3). Der vermeintliche Vorteil des V-Modells, alles bedacht zu haben, kommt also in der Realität selten zum Tragen, da sich trotz der umfangreichen Vorarbeit häufig noch Schwachstellen in der praktischen Umsetzung finden, die zu größeren Änderungen führen.

Die agile Methode hat dagegen den Vorteil, dass früh mit der Umsetzung begonnen wird und auch bereits früh für den späteren Nutzer sichtbare Ergebnisse produziert werden. Dieses Vorgehen ermöglicht eine stetige Validierung der Umsetzung der Ziele des Nutzers. Somit können Fehlentwicklungen früh erkannt und Korrekturen im Entwicklungsprozess vorgenommen werden.

Ein weiterer Nachteil des V-Modells gegenüber der agilen Methode liegt ebenfalls in der frühen vollständigen Analyse und Festlegung der funktionalen Anforderungen. Es besteht die Gefahr innovative Entwicklungsansätze durch zu viel alt Bewährtes, welches aus Gründen der Vollständigkeit „vorsichtshalber“ übernommen wird, zu unterdrücken. Der agile Ansatz, wonach ein früh lauffähiges System schrittweise erweitert wird, sorgt dagegen dafür, dass neue Funktionsanforderungen erst dann aufgestellt und berücksichtigt werden, wenn sie auch zur Umsetzung der im aktuellen Entwicklungsschritt gewünschten Funktionalität erforderlich sind.

Eine rein agile Methode kann jedoch den Nachteil haben, dass durch die frühe Entwicklung erster lauffähiger Versionen das Anforderungsmanagement zu kurz kommt, so dass später festgestellte Anforderungen nicht mehr in das erstellte Grundkonzept integriert werden können. Des Weiteren besteht die Gefahr, dass durch die Abweichung zum in der Norm beschriebenen Vorgehen die Akzeptanz der Ergebnisse bei der späteren Nutzung zur Erstellung eines marktreifen Produktes geschmälert wird.

Hybride Ansätze, Smart Engineering

Es sind auch Mischformen zwischen dem V-Modell und einer agilen Methode möglich (vgl. Kapitel 1.4.3 in [Kuster et al. 2019]). Auch für den Bereich sicherheitskritischer Software wie der Sicherungslogik argumentieren HAMETNER und SÜNDER, dass agile Methoden innerhalb des in den Normen [DIN EN 50126-1:2017; DIN EN 50128:2011; DIN EN 50129:2018 + AC:2019] vorgeschriebenen Verfahrens durchaus möglich sind [Hametner & Sünder 2017].

ESCHBACH ET AL definieren eine solche hybride Vorgehensweise in der Bahntechnik als „***Smart Engineering***“ [Eschbach et al. 2017]. Hierbei heben sie insbesondere die Bedeutung einer gründlichen Anforderungsdefinition für die zu entwickelnde Software (***Requirements Engineering***) hervor, um „aufwändige Korrekturen in späteren Entwicklungsphasen“ zu vermeiden [Eschbach et al. 2017, S. 447]. Demnach ist es also wichtig, bereits früh einen möglichst vollständigen Überblick über die späteren Anforderungen an das System zu erhalten, um die Fehler bei der Systemarchitektur möglichst zu vermeiden. Die spätere Entwicklung auf der geschilderten Grundlage kann dann allerdings agilen Prinzipien folgen.

Teil des Requirements Engineerings ist nach ESCHBACH ET AL. auch das Managen des Umgangs mit späteren Änderungswünschen. Demnach ist darauf zu achten, dass alle relevanten Stakeholder frühzeitig eingebunden werden. Für die eigentliche Softwareentwicklung empfehlen Eschbach et al die modellbasierte Softwareentwicklung [Eschbach et al. 2017, S. 450]. Zudem empfehlen sie die klare Definition von Systemgrenzen und Schnittstellen sowie die frühzeitige Entwicklung von Prototypen und Mockups, „um frühzeitig Rückmeldung von Stakeholdern zu bekommen“ [Eschbach et al. 2017, S. 448].

2.6.2 Modellierungsarten

Zur Beschreibung von Modellen können natürlichsprachliche (z. B. ein Glossar oder eine textuelle Beschreibung), semiformale (z. B. Pseudocode), formale (z. B. mathematische Notation) und grafische Beschreibungen (z. B. UML) verwendet werden (siehe Quellen im nachfolgenden Abschnitt). Im ersten Abschnitt sollen die Vor- und Nachteile dieser Beschreibungsarten anhand der Literatur diskutiert werden. Der zweite Abschnitt geht näher auf die grafische Modellierung ein, die im Rahmen der Arbeit überwiegend verwendet wird und diskutiert die Vor- und Nachteile verschiedener grafischer Modellierungsarten. Im dritten Abschnitt werden dann Details der grafischen Modellierungssprache UML erläutert, die in den Hauptkapiteln 7 und 8 als Beschreibungsmittel ausgewählt und verwendet wird.

Vor- und Nachteile der grundsätzlichen Modellierungsarten

Vor- und Nachteile der verschiedenen in der Einleitung zu Kapitel 2.6.2 genannten Beschreibungsmöglichkeiten diskutieren z. B. [Eigner et al. 2014, 63f], [Balzert 2009] sowie [Rupp 2007, S. 221–223] (wobei RUPP nur Diagramme und die textuelle Notation diskutiert).

Demnach haben formale Modellierungssprachen den Vorteil, dass die Beschreibung bei korrekter Definition des Modells in jedem Fall eindeutig ist. Allerdings sind sie für externe Betrachter häufig schwerer zu lesen. Daher wird bei semiformalen Modellierungssprachen auf Kosten der Eindeutigkeit und formalen Korrektheit die Lesbarkeit erhöht.

Grafische Modelle sind in der Regel sehr übersichtlich und ermöglichen eine schnelle Diskussion des Sachverhaltes. Insbesondere Zusammenhänge zwischen verschiedenen Teilen des Modells können gut veranschaulicht werden. Damit sie eindeutig sind, benötigt es allerdings ein ausführlich definiertes Rahmenmodell zur Definition aller verwendeten Begriffe. Zudem: „[Diagramme] verführen [...] oft dazu, Designentscheidungen vorwegzunehmen“ [Rupp 2007, S. 222].

„Textuelle Formulierungen sind dagegen „einfach“ und damit am schnellsten anzuwenden, „flexibel“ und „universell“ einsetzbar [Balzert 2009, S. 481]. Allerdings kann eine natürlichsprachliche Formulierung auch schnell mehrdeutig sein, wenn ihr eine unpräzise und uneinheitliche Wortwahl zu Grunde liegt [ebd.].

Grafische Modellierungssprachen

Für die Modellierung der Softwarearchitektur (***Strukturmodellierung***) und die Modellierung des Softwareverhaltens (***Verhaltensmodellierung***) existieren unterschiedliche Modellierungssprachen, von denen die Wichtigsten in den beiden nachfolgenden Unterabschnitten vorgestellt werden sollen.

Strukturmodellierung

Für die Strukturmodellierung stellt SIMSION in Kapitel 3.4.3 von [Simsion 2007] das ***Entity-Relationship-Modell*** **(ERM**, engl. **E-R)** mit verschiedenen Varianten, die sehr einfache ***Crow's foot notation*** (auch ***Martin-Notation***), ***Object-Role Modeling*** und die weit verbreitete ***Unified Modelling Language*** **(UML)** als gebräuchlichste grafische Notationsarten vor.

Die *Crow's foot notation* sowie *Object-Role Modeling* sind demnach sehr einfache Modelle, die beispielsweise keine Informationen zu den Eigenschaften der Objekte (= Attribute) darstellen können. Ihr Anwendungsgebiet ist daher auf die Beschreibung einfacher Sachverhalte begrenzt [Simsion 2007, 49f].

Die *Unified Modeling Language* ermöglicht mit einer Reihe verschiedener Diagrammtypen, die aus demselben Datenmodell heraus erzeugt werden, dieses zu notieren und für verschiedene

Anwendungsfälle darzustellen. Weiterhin ist die UML weltweit gebräuchlich, leicht verständlich und aus Teilen der Diagramme ist für die Erstellung eines Demonstrators direkt Java-Code generierbar. Zudem existiert eine Reihe mächtiger Werkzeuge für die UML-Modellierung, mit denen große Modelle übersichtlich und konsistent erstellt werden können. (Für weitere Informationen zur UML wird auf die einschlägige Fachliteratur verwiesen, z. B. [Kleuker 2018].)

Eine ebenfalls weit verbreitete grafische Modellierungssprache ist das *Entity-Relationship-Modell*. Im Vergleich zur UML beschränkt es sich allerdings auf die Darstellung von Objekten und deren Attributen und Beziehungen zueinander. Es gibt auch kein dahinterliegendes Datenmodell, welches die Nutzung der im ERM beschriebenen Objekte in anderen Darstellungsweisen zulässt. (Für weitere Informationen zu ERM wird auf die einschlägige Fachliteratur verwiesen, z. B. [Gadatsch 2019].)

UML ist von der ***SysML (Systems Modeling Language)*** abzugrenzen, welche häufig bei der Modellierung sicherheitskritischer Systeme zur Anwendung kommt und eine Abwandlung von UML darstellt. SysML eignet sich besonders für die Systementwicklung, wenn ein komplexes System aus verschiedenen Software- und physischen Komponenten und deren Zusammenwirken beschrieben werden soll, während UML mehr für die Softwareentwicklung verwendet wird (vgl. [Eigner et al. 2014, S. 63]). (Für weitere Informationen zur SysML vgl. [OMG 2019].)

Verhaltensmodellierung

Für die Verhaltensmodellierung sind vor allem ***Ereignisgesteuerte Prozessketten*** **(EPK)**, ***Business Process Model and Notation*** **(BPMN)**, ***Petri-Netze*** und ebenfalls die ***UML*** gebräuchlich [Drescher et al. 2017, Kapitel 3.1].

EPKs werden besonders für einfache Abläufe verwendet, die aus einer Folge von Bedingungen und Ereignissen, Funktionen und Konnektoren (zum Aufspalten der Kontrollflüsse) bestehen. Aufgrund der geringen Zahl an Darstellungsmöglichkeiten sind EPKs sehr übersichtlich, zugleich jedoch sind sie auf die Darstellung von Abläufen innerhalb einer Softwarekomponente beschränkt. Vergleiche z. B. [Nüttgens & Rump 2002].

BPMN enthält einen deutlich umfangreicheren Zeichenkatalog als EPKs. Anders als bei EPKs handelt es sich auch um eine formale Notation, die theoretisch in einen Softwareprozess umgewandelt werden kann. BPMN wird jedoch vorwiegend für die Abbildung von Geschäftsprozessen verwendet und ist in der Softwareentwicklung weniger verbreitet. Vergleiche https://www.bpmn.org/.

Petri-Netze sind formale Modelle, die auch grafisch dargestellt werden können. Im Unterschied zu den bisher vorgestellten Modellen liegt der Fokus nicht auf der anschaulichen Darstellung von sequentiellen Prozessen, sondern auf der formal korrekten Modellierung von komplexen Prozessen, insbesondere von nebenläufigen Systemen. Vergleiche [Priese & Wimmel 2008].

Die *UML* enthält wie bei der Strukturmodellierung eine Reihe verschiedener Diagrammtypen für Verhaltensdiagramme mit denen z. B. Prozessabläufe, die Interaktionen verschiedener Softwarekomponenten oder die Zustandsübergänge in einem System modelliert werden können. Die UML ist damit sehr ausdrucksstark und vielfältig einsetzbar. Die Diagramme können auf das Datenmodell aus der Strukturmodellierung zurückgreifen, wenn diese ebenfalls mit UML erfolgt ist. Die UML ist in der Softwareentwicklung sehr weit verbreitet. Vergleiche [OMG 2017] und [Kleuker 2018].

Ausführlicherer Hintergrund zur UML

Wie bereits im vorigen Abschnitt beschrieben, ist die UML eine weit verbreitete grafische Modellierungssprache. Sie wurde von der Object Management Group (OMG) entwickelt und wird von

dieser auch weiterentwickelt. [OMG 2017] enthält die Spezifikation der UML in Version 2.5.1. Über die UML gibt es zudem zahlreiche Fachbücher, von denen an dieser Stelle auf [Kleuker 2018] verwiesen werden soll.

Die UML kennt insgesamt 14 Diagrammarten, die vorwiegend zur Beschreibung von Softwaresystemen verwendet werden und sich in Struktur- und Verhaltensdiagramme aufteilen (vgl. Abb. 17). Die Strukturdiagramme beschäftigen sich mit der Beschreibung der im Modell verwendeten Datenkonstrukte sowie der Systemarchitektur, während sich die Verhaltensdiagramme mit der Funktionsweise des modellierten Systems beschäftigen. Die einzelnen Diagramme stellen dabei nur verschiedene Sichten auf ein konsistentes Modell dar.

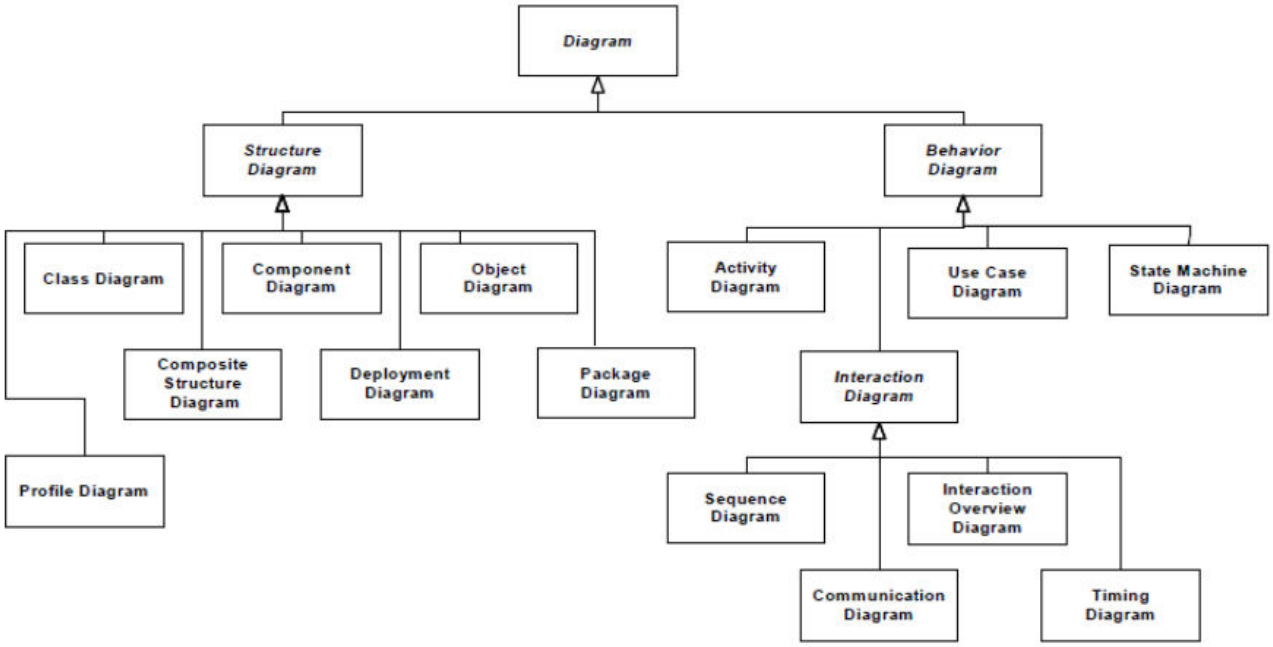


Abb. 17: Diagrammarten der UML
Quelle: [OMG 2017, S. 685]

UML-Strukturdiagramme

Das bekannteste und am weitesten verbreitete UML-Strukturdiagramm ist das UML-***Klassendiagramm***. Es dient zur Beschreibung der verwendeten **Objekttypen** im Modell, die in der objektorientierten Modellierung **Klassen** genannt werden. Jeder Modellbegriff (also Objekttyp) wird in Form einer Klasse mit seinen ***Attributen*** und ***Funktionen*** sowie den Abhängigkeiten zu anderen Begriffen modelliert. Zudem können viele hilfreiche weitere Details zu den einzelnen Modellelementen modelliert werden.

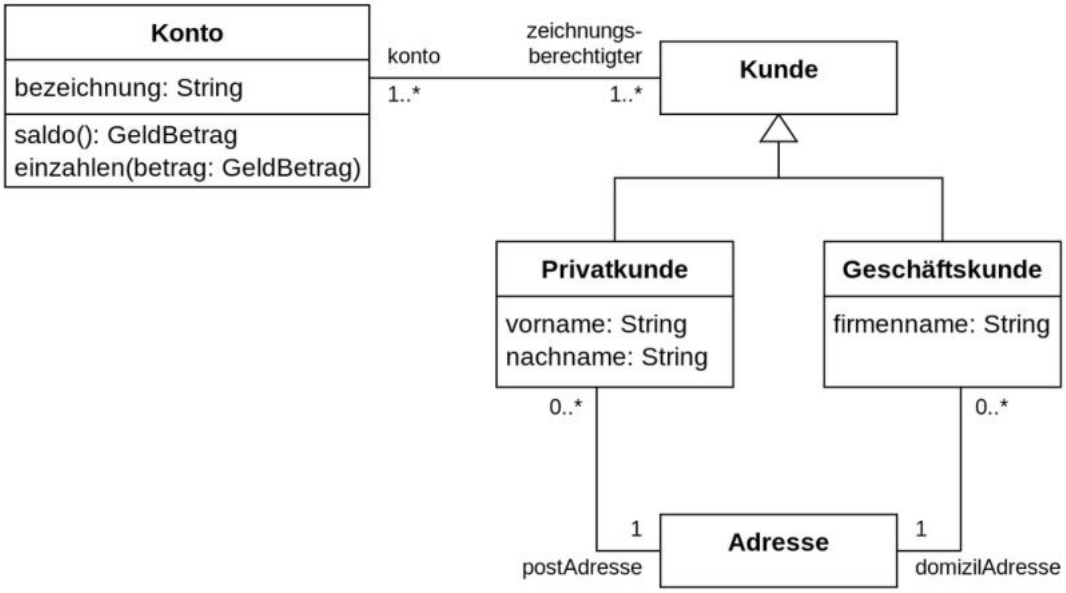


Abb. 18: Beispiel für ein UML-Klassendiagramm aus der Wikipedia
Quelle: Stkl, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

Die einzelnen Blöcke im Beispiel aus der Wikipedia (Abb. 18) sind die Klassen. Nach der Bezeichnung können zu jeder Klasse in der nächsten Zeile Eigenschaften in Form von Attributen angegeben werden. Jedes Attribut hat einen Attributtyp, der das Datenformat der im Attribut speicherbaren Werte enthält („String“ ist der Attributtyp für einen Fließtext). Die Klassen geben Schablonen vor, aus denen zur Laufzeit **Objekte** erzeugt werden können. Beispielsweise könnte ein Objekt vom Typ „Privatkunde“ mit vorname=“Erna“ und nachname=“Mueller“ existieren. Im einer weiteren Zeile können zu einer Klasse Funktionen angegeben werden, die diese Klasse ausführen kann. Im Beispiel sind dies bei der Klasse „Konto“ die Funktionen „saldo“, die keinen Eingangsparameter benötigt und eine Ausgabe von Typ „GeldBetrag“ enthält, und die Funktion „einzahlen“, die als Eingangsparameter eine Variable „betrag“ vom Typ „GeldBetrag“ benötigt.

Ein Attribut kann auch ein Zeiger auf ein anderes Objekt sein. Die Beziehungen zwischen den Objekten sind im Klassendiagramm mit Verbindungslinien oder Pfeilen eingezeichnet. Es werden verschiedene Arten von Verbindungslinien unterschieden. Im Beispiel ist ausgehend von „Privatkunde“ und „Geschäftskunde“ jeweils ein ***Vererbungspfeil*** zu „Kunde“ zu sehen. Der Vererbungspfeil gibt an, dass „Kunde“ eine allgemeinere, sogenannte „***Oberklasse***“ (auch „***Basisklasse***“) der beiden anderen Klassen ist, während „Privatkunde“ und „Geschäftskunde“ spezielle Formen (***Unterklassen***) von „Kunde“ sind. Die anderen Pfeile sind ***Assoziationen***, die angeben, dass eine bestimmte Art von Verbindung zwischen diesen Klassen besteht. Die Zahlen geben dabei an, wieviele Objekte der jeweils anderen Art mit dem Objekt verknüpft sein können (***Kardinalität***). Im Beispiel hat beispielsweise jeder „Privatkunde“ genau eine „Adresse“, während eine Adresse keinem, einem oder bis zu endlich vielen „Privatkunden“ zugewiesen sein kann.

Die übrigen sechs UML-Strukturdiagrammen sind weniger weit verbreitet als das Klassendiagramm. Das ***Paketdiagramm*** und das ***Verteilungsdiagramm*** beziehen sich auf die Softwarestruktur, die in dieser Arbeit nicht näher betrachtet wird. Das ***Kompositionsstrukturdiagramm*** beschreibt den Aufbau von Systemen aus Teilsystemen und das ***Komponentendiagramm*** die Wechselwirkungen dieser Systeme. Das ***Profildiagramm*** wird für die Metamodelle genutzt wird. Das ***Objektdiagramm*** zeigt die vorhandenen Objekte (= Instanzen der Objektklassen) zu einem bestimmten Zeitpunkt der Laufzeit.

Für genauere Erläuterungen zum Klassendiagramm und zu den im Folgenden vorgestellten weiteren UML-Strukturdiagrammen wird auf die oben genannte, einschlägige Standardliteratur verwiesen.

UML-Verhaltensdiagramme

Für die Beschreibung von Prozessen sind innerhalb der UML das ***Aktivitätsdiagramm*** und das ***Sequenzdiagramm*** vorgesehen. Beim Sequenzdiagramm liegt dabei der Fokus auf der Interaktion verschiedener Systemkomponenten, während beim Aktivitätsdiagramm die einzelnen logischen Aktionen, die zu einer Aktivität gehören, im Vordergrund stehen. Das ***Zustandsdiagramm*** bezieht sich nicht auf Prozesse, sondern auf die Beschreibung der Übergänge des modellierten Systems oder seiner Komponenten zwischen verschiedenen Systemzuständen. Weitere sogenannte ***Interaktionsdiagramme*** stellen beispielsweise mögliche Interkationen zwischen verschiedenen Systemkomponenten dar. Eine Sonderrolle hat das ***Anwendungsfalldiagramm***, welches sich auf die übergeordnete Darstellung der verschiedenen Funktionalitäten des Systems bezieht.

Im Folgenden soll das UML-Aktivitätsdiagramm näher beschrieben werden, das im späteren Verlauf der Arbeit von Bedeutung ist. In Abb. 19 findet sich ein Beispiel aus der Wikipedia.

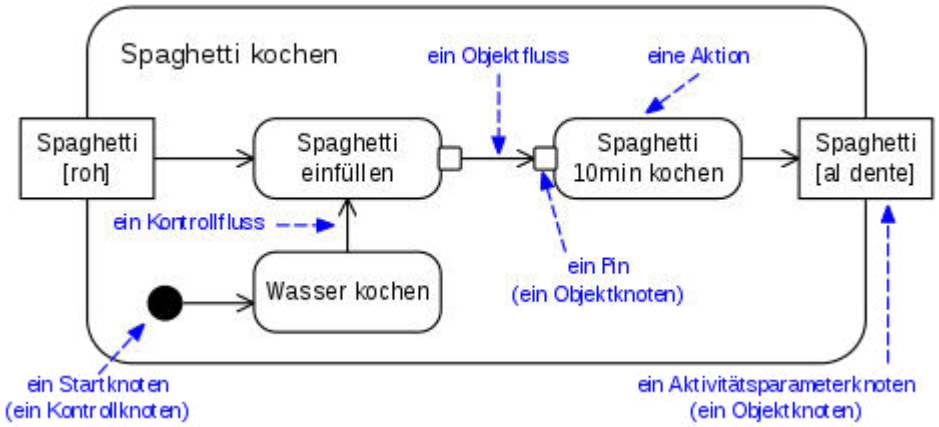


Abb. 19: Beispiel für ein UML 2.0-Aktivtätsdiagramm aus der Wikipedia
Quelle: Gubaer, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

Das *Aktivitätsdiagramm* stellt die Unterteilung eines Prozesses bzw. einer ***Aktivität*** in einzelne ***Aktionen*** dar. Der äußere Rahmen stellt dabei die Aktivität dar (im Beispiel „Spaghetti kochen“) und die kleineren Kästchen die Aktionen. Sogenannte „***Kontrollflüsse***“ (schwarze Pfeile zwischen den Aktionen) verbinden die Aktionen, so dass die Reihenfolge, in denen diese ausgeführt werden, ersichtlich wird. Ein Kontrollfluss kann sich beliebig verzweigen und wieder vereinigen. Nach Verzweigungen können entweder beide Stränge parallel weiterverfolgt werden (durch einen schwarzen Balken dargestellt) oder im Falle von ***Entscheidungsknoten*** (durch eine Raute dargestellt) je nach Bedingung nur ein Strang weiterverfolgt werden. Bei Vereinigungen bedeutet der schwarze Balken, dass auf alle eingehenden Kontrollflüsse gewartet werden muss, während bei einer Raute ein eingehender Kontrollfluss ausreichend ist, damit der Prozess weiterläuft.

Werden im Rahmen des modellierten Prozesses Nachrichten an benachbarte Systeme geschickt, werden diese ebenfalls im Aktivitätsdiagramm in einem je System abgegrenzten Bereich (als „***Schwimmbahnen***“ bezeichnet) dargestellt. Zusätzlich wird seit der UML 2.0 mit sogenannten „***Objektflüssen***“ der Austausch von Objekten zwischen den Aktionen modelliert. Zur Unterscheidung von den Kontrollflüssen beginnen und enden die Objektflüsse in sogenannten „***Pins***“ (Objektknoten). Dies gilt auch für den Eingang der Objekte in die und den Ausgang aus der Aktivität über

Aktivitätsparameterknoten. Objekte können in „***Central Buffer Nodes***“ bzw. „***Data Stores***“ temporär zwischengespeichert und zusammengefasst werden.

Einzelne Aktionen aus einem übergeordneten Aktivitätsdiagramm können in weiteren Aktivitätsdiagrammen verfeinert werden. Dies ermöglicht die Darstellung des Gesamtprozesses in verschiedenen Aggregationsstufen. Eine solche Aktion nennt sich „***Call Behaviour Action***“ (vgl. zum UML-Aktivitätsdiagramm [Kleuker 2018; OMG 2017]).

2.7 Zusammenfassung zum Stand des Wissens

In diesem Kapitel soll der in den vorigen Kapiteln dieses Hauptkapitels beschriebene Stand des Wissens in Bezug auf die Entwicklung der neuen Sicherungslogik „smartLogic“ zusammengefasst und eingeordnet werden. Dabei wird zunächst ausführlicher auf die Entwicklung der bisherigen Stellwerkstechnik sowie ihrer Umsysteme eingegangen, woraus sich der Bedarf für eine neue Sicherungslogik herleitet. Anschließend folgt eine (aufgrund des Grüne Wiese-Ansatzes) kurze Zusammenfassung zu aktuellen Arbeiten, die sich mit der Sicherungslogik beschäftigen. Die weiteren Abschnitte fassen die Erkenntnisse zu den Infrastrukturdatenmodellen und Methoden für den sicherheitskritschen Entwurf zusammen.

Entwicklung der bisherigen Stellwerkstechnik und Bedarf für eine neue Sicherungslogik

Da die aktuell in der Praxis vorzufindenden Sicherungslogiken eine stetige Weiterentwicklung aus den Anfängen der Eisenbahn darstellen, beginnt das Hauptkapitel in Kapitel 2.1 mit einer Übersicht des heutigen Stands der Stellwerkstechnik und den grundsätzlichen Sicherungsprinzipien. Bei der Weiterentwicklung der Stellwerkstechnik wurde kontinuierlich aus Unfallereignissen gelernt und das hohe Maß an Sicherheit erreicht, das wir heute vorfinden. Dieses Maß an Sicherheit darf auch durch zukünftige Innovationen nicht gefährdet werden. Allerdings zeigen die Erkenntnisse aus Kapitel 2.2, dass sich die technische Umgebung der Sicherungslogik weiterentwickelt hat und auch in den nächsten Jahren zahlreiche technologische Neuerungen zu erwarten sind. Gleichzeitig wurde die Sicherungslogik (noch) nicht vollumfänglich an den aktuellen Stand der Technik ihrer Umsysteme angepasst.

Die Diskrepanz zwischen dem Stand der Sicherungslogik und dem technischen Stand der Umsysteme zeigt sich beispielsweise in der Nutzung der verfügbaren Informationen über eine Zugfahrt. So liegt dem Blockprinzip die lange Zeit schwierige Ortbarkeit der Zugfahrten zu Grunde. Die klassischen optischen Signale wurden in Folge der Schwierigkeit der Datenübermittlung von der Infrastruktur an die fahrenden Züge erfunden. Die klassische Sicherungslogik der mechanischen Stellwerke – dort häufig als Stellwerkslogik bezeichnet – und der darauf aufbauenden Stellwerke in Form der Verschlusslogik und der Blockabhängigkeiten wurden entsprechend vor dem Hintergrund dieser eingeschränkten Verfügbarkeit von Informationen entwickelt. Festgelegte Infrastrukturbereiche (Fahrstraßen) werden auf Basis fest definierter Bedingungen für jeweils eine Zugfahrt gesperrt und wieder freigegeben (aufgelöst), wenn diese Zugfahrt einen definierten Ort vollständig erreicht hat (Prinzip der Fahrstraßenlogik).

Im Zuge der technologischen Neuerungen bei den Umsystemen der Sicherungslogik – wenn auch noch nicht immer in ausgereifter Form, aber doch so ausgeprägt, dass von ausgereiften Systemen in den nächsten Jahren ausgegangen werden kann – sind wesentlich mehr Informationen über die Zugfahrten und den Status der Infrastrukturelemente (z. B. Diagnosedaten) verfügbar. Außerdem können über ETCS deutlich mehr Informationen an die Fahrzeuge übertragen werden und somit

präzisere Vorgaben für die Befahrung der Gleisinfrastruktur je nach aktueller Betriebssituation gemacht werden.

Unter anderem durch die zusätzlichen Informationen können klassische Sicherungsprinzipien wie die Fahrstraßenlogik oder die Blocklogik bei der Entwicklung einer neuen Sicherungslogik in Frage gestellt werden. Bisher wurden Sicherungslogiken jedoch nur punktuell an die zusätzliche Informationsverfügbarkeit angepasst (z. B. Teilfahrstraßenauflösung, Anpassungen an LZB CIR-ELKE II). Auch bei Spurplanstellwerken sind die Freiheitsgrade für die Fahrstraßenbildung begrenzt. Fahrstraßen bilden sich vom vorgegebenen festen Start- zum Zielsignal immer auf die gleiche Weise. Nur bestimmte, vorprojektierte Abweichungen existieren, wie verkürzte Durchrutschwege für bestimmte Einfahrgeschwindigkeiten, und das aktuelle Betriebsgeschehen wird nur vereinzelt, z. B. bei Zwieschutzweichen, berücksichtigt. Ist eine Fahrstraße festgelegt, lässt sie sich ohne Hilfshandlung nicht mehr verändern.

Zahlreiche Funktionen von ETCS können weder mit Fahrstraßenstellwerken noch mit bestehenden Spurplanstellwerken (in Relais- oder ESTW-Bauart) genutzt werden, beispielsweise

- das Nutzen von vollüberwachten Fahrzeugen zur Gewährung des Flankenschutzes,
- das Übermitteln von Fahrprofilen von beliebigen zu beliebigen Punkten im Schienennetz mit gefahrpunktorientierten Geschwindigkeitsprofilen,
- das dynamische Anpassen des Durchrutschweges je nach verbleibender Geschwindigkeit des Fahrzeugs beim Bremsvorgang und
- das dynamische Verändern der Fahrstraße mit Zustimmung des Fahrzeugs bei geänderter Betriebssituation.

Ohne eine Anpassung der Sicherungslogik an die technologischen Neuerungen bei den Umsystemen wie ETCS lassen sich durch solche Neuerungen häufig die Kapazitätspotenziale nicht heben (vgl. z. B. Kapitel 2.2.2, Absatz „Einordnung der Kapazitätspotenziale von ETCS für den digitalen Bahnbetrieb“ oder die Kapitel 2.2.3 beschriebene bisherige Umsetzung der Hochleistungsblöcke für deren Realisierung zur effektiven Nutzung zahlreiche Gleisfreimeldeeinrichtungen erforderlich sind, die Kosten verursachen und eine potenzielle Quelle für Störungen sind). Nach Ansicht des Autors erfordert die heutige Stellwerkstechnik zudem, den Betrieb in manuellen Rückfallebenen häufiger durchzuführen, als es notwendig wäre[8]. Manuelle Rückfallebenen sind in aller Regel zeitintensiv und fehleranfällig (vgl. [Maschek 2013, 18f, 26ff; Braband 2013, S. 594]). Durch die genauen Informationen, die heute bereits vorliegen oder demnächst zur Verfügung stehen werden, könnte der Rückgriff auf solche manuellen Rückfallebenen allerdings nach Ansicht des Autors dieser Arbeit in zahlreichen Situationen vermieden werden.

Aus den zuvor genannten Gründen kann die These aufgestellt werden, dass es noch Verbesserungspotenzial im Bereich der Sicherungslogik gibt, insbesondere, wenn die Sicherungslogik grundsätzlich von ihren Zielen her unter den Vorzeichen der heute bereits vorhandenen und absehbar zukünftig zu erwartenden Innovationen neu gedacht wird („Grüne Wiese“-Ansatz).

Aktuelle Ansätze innovativer Sicherungslogiken

In den letzten Jahren wurden bereits mehrere Ansätze zur Neu- bzw. Weiterentwicklung der Sicherungslogik erarbeitet, die in Kapitel 2.3 vorgestellt wurden. Die dort vorgestellten Arbeiten

[8] Ist eine der vordefinierten Bedingungen für das Einlaufen einer Fahrstraße nicht verfügbar, kommt ein Signal in Deutschland nicht auf Fahrt. Dieser Umstand hat zur Folge, dass eine mehr oder weniger manuelle Rückfallebene zum Tragen kommt, in der technische Schutzfunktionen außer Kraft gesetzt und durch manuelle Handlungen des Betriebspersonals ersetzt werden müssen.

liefern wertvolle Impulse für eine Neugestaltung der Sicherungslogik. Keiner dieser Ansätze ist jedoch bereits so ausgereift, dass er tatsächlich in der Praxis umgesetzt wurde. Mögliche Gründe sind eine fehlende Migrationsfähigkeit und, dass nur ein Teilbereich des erforderlichen Funktionsumfangs einer Sicherungslogik abgedeckt wird.

Eine Sonderrolle nimmt die in Kapitel 2.4 vorgestellte, großangelegte RCA ein, die sich parallel zur Erstellung dieser Arbeit in der Entwicklung befand und deren Entwicklung zum Zeitpunkt der Abgabe dieser Arbeit noch nicht abgeschlossen ist, da sie möglicherweise in der Zukunft einen Standard bilden wird. Aus diesem Grund sollte insbesondere bei der Erstellung des Datenmodells soweit wie möglich auf eine Kompatibilität zur RCA geachtet werden. Die RCA-Komponenten „Safety Logic“ und „Safety Manager“, die sich thematisch mit der in dieser Arbeit zu entwickelnden smartLogic überschneiden, sind jedoch zum Zeitpunkt des Verfassens dieser Arbeit noch nicht im Detail ausgearbeitet, so dass die Ergebnisse dieser Arbeit in die weiteren Entwicklungen der an der RCA beteiligten EIU miteinfließen könnten.

Infrastrukturdatenmodell

Bei der Erarbeitung des Datenmodells für die Entwicklung der smartLogic bietet es sich aus Gründen der Einfachheit, aber auch aus Gründen der Migrationsfähigkeit hin zu einer neuen Sicherungslogik an, neben der Kompatibilität zur RCA auch zu prüfen, inwieweit bestehende Infrastrukturdatenmodelle, die in Kapitel 2.5 vorgestellt wurden, verwendet werden können. Die in Kapitel 2.5.7 zusammengefassten Erkenntnisse lassen vermuten, dass eine vollständige Verwendung eines der bestehenden Modelle die Entwicklung der Funktionsweise der neuen Sicherungslogik einschränkt und damit dem Ziel der Entwicklung einer möglichst optimalen Sicherungslogik auf der „Grünen Wiese“ widerspricht. Aus diesem Grund ist es sinnvoll, auch das Infrastrukturdatenmodell im Rahmen der Erarbeitung des Datenmodells für die smartLogic im Kontext ihrer Modellierung zu erarbeiten (siehe 7. Hauptkapitel). Es scheint dabei sinnvoll, auf eine Kompatibilität zum Standard des Topologie-Metamodells „Rail Topo Modell“ zu achten.

Methoden für den sicherheitskritischen Entwurf

Abschließend ging Kapitel 2.6 auf verschiedene Methoden für den sicherheitskritischen Entwurf von Systemen ein. Als Entwicklungsmethode wurde das V-Modell vorgestellt, welches gemäß [DIN EN 50126-1:2017] für die Entwicklung sicherheitskritischer Eisenbahnsysteme vorgesehen ist, und der agilen Arbeitsweise sowie einem hybriden Ansatz gegenübergestellt. Auf dieser Basis kann im Rahmen der Methodendiskussion im 3. Hauptkapitel die Vorgehensweise für die Entwicklung der smartLogic festgelegt werden. Zudem wurden verschiedene Modellierungsmethoden mit ihren Vor- und Nachteilen vorgestellt, die als Entscheidungsgrundlage im Kontext der Anforderungen an die jeweilige Anwendung der Modellierung in den inhaltlichen Hauptkapiteln dienen kann.

3 Herleitung der Zielsetzung sowie der grundsätzlichen Methode und Vorgehensweise

Wie in Kapitel 2 erläutert, sind die in heutigen Stellwerken verbauten Sicherungslogiken aus der stetigen Weiterentwicklung der sicherungstechnischen Anforderungen über die Jahrzehnte hinweg entstanden. Dieser Prozess ist robust, da evolutionär in kleinen Schritten von einem sicheren System zum nächsten noch sichereren System übergegangen wurde. Bei der Entwicklung einer neuen Sicherungslogik stellen sich daher hohe Anforderungen an den Entwicklungsprozess.

Um Effizienzprobleme zu vermeiden, sollte dieser Entwicklungsprozess konsequent von der globalen Zielsetzung hergeleitet werden. Da die genaue Abgrenzung der Aufgaben der Sicherungslogik innerhalb der infrastrukturseitigen Sicherungstechnik von der Zielsetzung abhängen sollte, wird die Zielsetzung zunächst für die gesamte infrastrukturseitige Sicherungstechnik hergeleitet und später auf die Sicherungslogik eingegrenzt.

Dementsprechend werden die globalen Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik in Kapitel 3.1 hergeleitet. Die anschließende Eingrenzung der Ziele auf die Sicherungslogik erfolgt in Kapitel 3.2. Der mögliche Bearbeitungsumfang dieser Arbeit wird dabei von äußeren Einflüssen, wie dem zur Verfügung stehenden Zeitbudget für diese Arbeit, zusätzlich begrenzt. Deshalb werden in Kapitel 3.3 inhaltliche Abgrenzungen vorgenommen. Um die Sicherungslogik so zu entwickeln, dass sie die Zielsetzung optimal erfüllt, sind Anforderungen an die zu entwickelnde Sicherungslogik zu bestimmen. Hierfür werden Verbesserungspotenziale bestehender Sicherungslogiken identifiziert, die gleichzeitig Nutzenpotenziale für die in dieser Arbeit zu entwickelnde, neue Sicherungslogik „smartLogic“ darstellen (Kapitel 3.4). Die zur Realisierung der Nutzenpotenziale identifizierten Anforderungen werden als globale Anforderungen bezeichnet, da sie, im Gegensatz zu den spezifischen Anforderungen an die einzelnen Hauptkapitel, für die gesamte Arbeit relevant sind.

Auf Basis der in Kapitel 3.5 identifizierten Anforderungen muss ein geeigneter Entwicklungsansatz als grundsätzliche Methode für diese Arbeit hergeleitet werden, woraus die grundsätzliche Vorgehensweise folgt. Hiermit beschäftigt sich Kapitel 3.6. Im Kapitel 3.7 folgt eine Zusammenfassung des 3. Hauptkapitels.

3.1 Globale Ziele für die infrastrukturseitige Sicherungstechnik

In diesem Kapitel soll die globale Zielsetzung für die Neuentwicklung von Komponenten der infrastrukturseitigen Sicherungstechnik hergeleitet werden. Die Bestimmung der Zielsetzung erfolgt zunächst global für die gesamte infrastrukturseitige Sicherungstechnik, da – wie in der Einleitung zum 3. Hauptkapitel bereits erwähnt – daraus in den folgenden Kapiteln die genaue Abgrenzung für eine neue Komponente Sicherungslogik erst noch hergeleitet wird. Auf die Zielsetzung für die Neuentwicklung der Komponente Sicherungslogik an sich wird dann detailliert in Kapitel 3.2 eingegangen.

Zur Bestimmung der Zielsetzung für die Neuentwicklung der Komponenten der infrastrukturseitigen Sicherungstechnik wird auf anerkannte Methoden aus der Industrie zur Verbesserung von Produktions- und Geschäftsprozessen, wie dem Lean Management und dem Qualitätsmanagement, zurückgegriffen. Diese Methoden, wie beispielsweise die Wertstromanalyse, sind zwar häufig nicht eins zu eins auf den Produktionsprozess „Durchführung von Fahrzeugbewegungen auf der Eisenbahninfrastruktur“ übertragbar, da es sich beim betrachteten Produkt um eine Dienstleistung handelt (Beförderungsdienstleistung), bieten aber dennoch geeignete grundsätzliche Ansatzpunkte, die sich auf den speziellen, hier vorliegenden Anwendungsfall übertragen lassen.

Haupt-Nutznießer der Eisenbahn ist der Kunde, daher wird zunächst in Kapitel 3.1.1 auf die Ziele der Kunden an den Bahnbetrieb und damit auch an die infrastrukturseitige Sicherungstechnik eingegangen. Anschließend wird die Betrachtung der Ziele durch eine Stakeholder-Analyse vervollständigt, um auch die Ziele anderer Beteiligter am Bahnbetrieb zu berücksichtigen.

3.1.1 Ziele aus Sicht der Kunden

Ausgangspunkt eines Verbesserungsprozesses sollte – wie in der Einleitung bereits erwähnt – immer der Nutzen für den Kunden sein (vgl. z. B. [Bertagnolli 2018, S. 9]). Diese Arbeit folgt als wissenschaftliche Arbeit einem gesamtgesellschaftlichen Blickwinkel, so dass nicht der direkte Kunde eines Eisenbahninfrastrukturbetreibers (EIU) (i. d. R. Eisenbahnverkehrsunternehmen (EVU)) im Vordergrund steht, sondern der Endkunde (Passagier, Güterverkehrskunde). Deshalb werden in diesem Unterkapitel zunächst die Ziele aus der Sicht der Endkunden betrachtet (erster Abschnitt) und anschließend hergeleitet, wie diese Ziele durch die Gestaltung der infrastrukturseitigen Sicherungstechnik beeinflusst wird.

Allgemeine Ziele der Endkunden

Der Endkunde möchte im Falle der Eisenbahn bekanntlich, dass er (oder sie) als Passagier bzw. seine Güter möglichst kostengünstig von einem Ort zum anderen befördert werden. Aus Sicht des Endkunden steigert sich der Wert dieser Beförderungsdienstleistung (und damit die Bereitschaft einen höheren Preis zu bezahlen) im Personenverkehr vor allem

- je kürzer er für diese Beförderungsleistung benötigt, wobei hier sowohl der auf die Eisenbahn entfallende Teil der Reisezeit als auch die gesamte Reisezeit von Haustür zu Haustür betrachtet werden müssen, und
- je höher der Komfort seiner Reise ist.

Auf der anderen Seite wird der Wert der Beförderungsdienstleistung für den Kunden vermindert

- durch Unpünktlichkeit, insbesondere bezogen auf die gesamte Wegstrecke, und
- durch Komfortmängel.

Im Güterverkehr sind vor allem der Transportpreis und die Pünktlichkeit relevant [BVU 2014, S. 109], wobei sich die Pünktlichkeit wieder auf die Kosten aus Sicht der Güterverkehrskunden und damit den von den Kunden empfundenen Preis auswirken kann [Oetting & Keck 2015]. Die Transportzeit ist häufig etwas weniger wichtig, da viele Firmen im Zweifel auch etwas früher bestellen können, sofern die Güter dann verlässlich zur erwarteten Zeit ankommen.

Umweltaspekte werden für einige Endkunden ebenfalls immer wichtiger. Ein Teil der Umweltaspekte spiegelt sich in anderen genannten Zielen wider, z. B. der Energieverbrauch in den Kosten, umweltschonende Verkehrsverlagerungseffekte in der Attraktivität des Schienenverkehrs, betriebliche Schallminderung durch das Vermeiden unnötiger Bremsvorgänge oder der Flächenverbrauch durch die Optimierung der Nutzung bestehender Infrastrukturen. Andere Umweltwirkungen wie der Energiemix der Fahrzeuge lassen sich nicht über die infrastrukturseitige Sicherungstechnik beeinflussen.

Einfluss der infrastrukturseitigen Sicherungstechnik auf das Erreichen der Ziele der Kunden

Um im weiteren Verlauf der Arbeit die zu entwickelnde neue Sicherungslogik als zentrale Komponente der infrastrukturseitigen Sicherungstechnik so zu gestalten, dass die oben genannten Ziele (Preis bzw. niedrige Kosten, Reisezeit, Pünktlichkeit und Komfort) möglichst optimal erreicht werden, muss der

Einfluss, den die Gestaltung der infrastrukturseitigen Sicherungstechnik auf das Erreichen dieser Ziele hat, bestimmt werden.

Im marktwirtschaftlichen Normalfall hängt der von den Kunden zu zahlenden Preis maßgeblich von den Kosten ab. Deshalb stellen die Kosten der infrastrukturseitigen Sicherungstechnik einen wichtigen Einfluss auf das Erreichen der Ziele der Kunden dar. Im Falle der Eisenbahn ist es üblich, dass Teile der Kosten auch vom Steuerzahler über staatliche Zuschüsse gedeckt werden. Weil jedoch im Sinne eines gesamtgesellschaftlichen Blickwinkels auch die Belastung der Steuerzahler zu minimieren ist, führt dieser Umstand nicht dazu, dass geringe Kosten ein weniger wichtiges Ziel werden.

Da in jeder Lebenszyklusphase Auswirkungen auf die Kosten existieren, ist es wichtig, den gesamten Lebenszyklus der Komponenten der infrastrukturseitigen Sicherungstechnik im Blick zu haben, vom Entwurf über die Planung, die Herstellung und Installation sowie den Betrieb bis zur Entsorgung (analog zu den Lebenszyklusphasen aus der Sicherheitsnachweiserstellung in [DIN EN 50126-1:2017]). Tab. 3 enthält für die globalen Ziele und die jeweils relevanten Lebenszyklusphasen daraus folgende Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik.

Nicht jede Lebenszyklusphase der Sicherungstechnik ist für jedes globale Ziel relevant. Bei einigen Zielen in Tab. 3 fehlen daher einzelne Lebenszyklusphasen. So wirkt sich beispielsweise die Planungsphase der Sicherungstechnik nicht direkt auf die Pünktlichkeit aus, da in dieser Phase die fahrenden Züge noch nicht beeinflusst werden. (Eine schlechte Planung kann zwar zu einer verlängerten Reisezeit führen, das dahinterliegende Ziel bezieht sich jedoch auf die Lebenszyklusphase „Betrieb“, z. B. dass die Planung eine möglichst hohe Geschwindigkeit im Betrieb ermöglichen soll.) Bei der Instandhaltungs-Phase wird angenommen, dass sie nur kurzfristig andauert und sich daher nicht auf die Reisezeit, sondern auf die Pünktlichkeit auswirkt. Da die Sicherungstechnik nicht direkt den Komfort beeinflusst, sondern nur mittelbar über ihre Funktionsweise Auswirkungen auf den Betriebskomfort hat, wird angenommen, dass nur die Betriebs- sowie die Instandhaltungsphase Auswirkungen auf das Komfort-Ziel haben.

Tab. 3: Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik

globales Ziel	**Lebenszyklusphase der Sicherungstechnik**	**Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik**
Kosten	Planung	einfache Projektierung, einfache Anpassbarkeit an neue Gegebenheiten bzw. Örtlichkeiten, Aufrüstbarkeit bei neuen Anforderungen, kurze Zulassungsprozesse
Kosten	Herstellung, Installation	geringe Komplexität, lange Lebenszeit, wenig Hardware
Kosten	Betrieb	einfache und ergonomische Bedienung, möglichst geringe aber gleichmäßige Auslastung der benötigten Arbeitskräfte, geringer Stromverbrauch, geringe Anforderungen an technische Begleitsysteme, Energieverbrauch der Fahrzeuge minimieren, geringe Produktionskosten pro Verkaufseinheit durch hohe Kapazität
Kosten	Instandhaltung	einfach zu wartende Technik, geringe Ausfallrate, verschleißarme Hardware

Kosten	Entsorgung	möglichst gut recyclebar, lange Lebenszeit, wenig Hardware
Reisezeit	Herstellung, Installation + Entsorgung	möglichst geringe Einschränkungen des Betriebs
Reisezeit	Betrieb	möglichst geringe Einschränkungen der maximalen Fahrzeuggeschwindigkeit, Wartezeiten vermeiden, möglichst viele Fahrzeugbewegungen ermöglichen (ermöglicht schnelle Direktverbindungen für Kunden)
Pünktlichkeit	Herstellung, Installation + Entsorgung	*siehe Reisezeit in den Lebenszyklusphasen Herstellung, Installation + Entsorgung*
Pünktlichkeit	Betrieb	hohe Verfügbarkeit, geringstmögliche Auswirkungen von Abweichungen auf den Regelbetrieb
Pünktlichkeit	Instandhaltung	geringstmögliche, planbare Auswirkungen auf den Betrieb
Komfort	Betrieb, Instandhaltung	möglichst viele Fahrzeugbewegungen ermöglichen (ermöglicht komfortable Direktverbindungen) (Kapazität)

Als zusätzliches Ziel ist noch die *Aufrechterhaltung der Sicherheit* zu sehen. Dieses Ziel taucht in Tab. 3 nicht auf, da bereits ein hohes Maß an Sicherheit besteht und auch gesetzlich vorgegeben ist. Dieses Maß muss gemäß dem Prinzip mindestens gleicher Sicherheit (vgl. [EBO:2019-04-05 §2]) mindestens gehalten werden und geht somit als Vorgabe in den weiteren Entwicklungsprozess ein. Dabei wird nicht ausgeschlossen, dass es zu weiteren Verbesserungen der Sicherheit kommen kann (vgl. Kapitel 5 zur Gefährdungsanalyse), eine Verbesserung der Sicherheit wird aber aufgrund des bereits hohen bestehenden Sicherheitsniveaus nicht prioritär gegenüber den weiteren identifizierten Zielen behandelt.

Außer dem prioritären Ziel der Aufrechterhaltung der Sicherheit kann keine eindeutige Rangfolge der identifizierten Ziele hergeleitet werden. Beispielsweise ist die Reisezeit nicht eindeutig wichtiger als die Pünktlichkeit oder der Komfort. In Fällen, in denen die Ziele miteinander in Konflikt stehen, muss daher eine Balance zwischen den Anforderungen der einzelnen Ziele gefunden werden.

3.1.2 Stakeholder-Analyse

Die in Kapitel 3.1.1 genannten Ziele wurden aus der Sicht der Kunden hergeleitet, die maßgeblich für die Annahme des betrachteten Produktes sind. Dennoch sollte der Vollständigkeit halber eine Stakeholder-Analyse durchgeführt werden, in der auch die Interessen anderer Interessensgruppen festgestellt und soweit möglich berücksichtigt werden können (vgl. zur Theorie der Stakeholder-Analyse [Kamiske 2015b]).

Typische Gruppen von Stakeholdern neben den Kunden sind demnach (Hauptgruppen aus [Kamiske 2015b], eigenständige Erweiterung um Beispiele für auf den Anwendungsfall bezogene konkrete Gruppen als Unterpunkte):

- Shareholder / Gesellschafter
  - Politik
  - Steuerzahler (vertreten durch die Politik)

- Belegschaft
  - Fahrdienst
  - Instandhaltung (IH)
  - Planungsabteilungen
    - Infrastruktur
    - Fahrplan
- Lieferanten
  - Signalindustrie
  - Computerhardwareindustrie
  - Software-Dienstleister
  - Ingenieurbüros
- staatliche Institutionen
  - Eisenbahnbundesamt (EBA)
  - European Railway Agency (ERA) / Europäische Union (EU)
  - Bundesstelle für Eisenbahnunfalluntersuchung (BEU)
  - Justiz
  - Bundesnetzagentur
- Zivilgesellschaft
  - Anwohner von Bahnstrecken
  - Umweltverbände

Zudem ist die Besonderheit zu beachten, dass aus Sicht der Eisenbahninfrastrukturunternehmen die Kunden nicht direkt die Endkunden sind, sondern die Eisenbahnverkehrsunternehmen. Im vorigen Kapitel wurde bewusst von den Endkunden als primäre Kunden ausgegangen, dennoch bleibt zu untersuchen, ob es aus Sicht der Kundengruppe EVU weitere Anforderungen gibt, die nicht bereits durch deren Kunden, die Endkunden, abgedeckt sind.

Einige Interessen der Stakeholder sind offensichtlich (insbesondere auf einer abstrakten Ebene), für andere ist eine vertiefte Analyse sinnvoll (insbesondere je konkreter die Interessen werden). Nachfolgend werden die Interessen der einzelnen Stakeholder-Gruppen zusammengefasst und daraus Ergänzungen für den Anforderungskatalog hergeleitet.

Shareholder

Die meisten Eisenbahnunternehmen sind heutzutage gemäß ihrer Organisationsform als wettbewerbs- und gewinnorientierte Unternehmen aufgestellt. Das grundsätzliche Interesse der Shareholder solcher Unternehmen in einer Marktwirtschaft ist typischerweise (entweder kurz- oder langfristig) einen möglichst großen Gewinn zu erzielen. Hierzu können zum einen die Erlöse gesteigert werden, z. B. indem mehr Beförderungsleistung angeboten oder die Auslastung verbessert werden kann. Zum anderen können die Kosten minimiert werden. Im Falle von Eisenbahninfrastrukturunternehmen tritt jedoch häufig der Sonderfall auf, dass die Unternehmen dem Staat gehören. In dieser speziellen Konstellation können weitere Ziele durch die Politik als Vertretung des Staates und seiner Bürger definiert werden. In einer Demokratie kann angenommen werden, dass sich die von der Politik definierten Ziele grundsätzlich am Wählerwillen orientieren. Dieser ist jedoch nicht homogen und wird je nach Partei unterschiedlich vertreten.

Die derzeitige Politik rückt hierbei vor allem neben dem finanziellen Ergebnis zwei weitere Ziele in den Vordergrund. Zum einen sollen vor allem aus Umweltgründen möglichst viele Menschen mit der Eisenbahn fahren. Hierfür spielt die Kapazität der Eisenbahn eine wichtige Rolle, aber auch die

Attraktivität für die Kunden. Diese Ziele sind in Tab. 3 bereits enthalten. Zum anderen wird das Thema „Erhöhung der Pünktlichkeit“ häufig erwähnt. Auch dieses Ziel ist in der Kundensicht bereits enthalten.

Ein weiteres Interesse der Politik wird von dieser nicht so sehr in den Vordergrund gerückt, hat aber ebenfalls eine große Wichtigkeit. Da die Bahn vor allem zur Erreichung der Klimaziele als umweltfreundliches Verkehrsmittel präsentiert werden soll, ist ihre Ökobilanz ebenfalls im Interesse der Politik. Zwar weist die Bahn grundsätzlich bereits niedrigere Emissionen als andere Verkehrsmittel auf. Dennoch gibt es in diesem Bereich noch einiges Potenzial, beispielsweise bei der Art der Energieversorgung. Wie in Kapitel 3.1.1 bereits beschrieben wurde, spiegeln sich jedoch auch diese Ziele bereits in anderen Zielen wieder oder wurden als für die Entwicklung der Sicherungslogik nicht relevant klassifiziert.

Es werden daher keine weiteren globalen Ziele aus den Zielen der Shareholder heraus definiert.

Belegschaft

Für die Belegschaft gibt es ebenfalls einige typische Ziele, die für alle Unternehmen gleich sind und die Motivation des Personals beeinflussen. Diese Ziele werden z. B. von der Arbeitswissenschaft untersucht und orientieren sich an den generellen Bedürfnissen der Menschen (vgl. hierzu einschlägige Werke der Arbeitswissenschaft wie [Schlick et al. 2018]). So kommt dem Arbeitsplatzerhalt eine hohe Bedeutung zu. Gleichsam wird eine ergonomische Gestaltung des Arbeitsplatzes bzw. der zu erfüllenden Tätigkeiten eine Rolle spielen, aber auch, inwieweit der Arbeitsplatz nur mit extrinsischer Motivation verbunden wird oder auch intrinsische Motivation hervorruft.

Eine vollständige Analyse solcher Ziele würde den Rahmen der Arbeit sprengen. Es kann aber aus der genannten Literatur gefolgert werden, dass es wichtig ist, die Belegschaft in die Entwicklung neuer Systeme miteinzubinden, vor allem bei den Schnittstellen, an denen sie mit diesen Systemen in Kontakt treten. Zwar kann aufgrund der bereits heute in neueren Stellwerken praktizierten Trennung von Bedienplatz und Sicherungslogik davon ausgegangen werden, dass im Regelfall keine direkte Benutzerinteraktion zwischen dem Menschen und der smartLogic stattfinden wird, allerdings ist dennoch davon auszugehen, dass Auswirkungen auf die Belegschaft, wie die Zahl der benötigten Arbeitsplätze, existieren. In den letzten Jahren herrscht im Bereich der Mitarbeiter des Fahrdienstes Fachkräftemangel [Anzenhofer 2019]. Eine Reduzierung des Bedienungsaufwandes und eine flexible Zuordnung der Aufgaben zu den verfügbaren Fachkräften ist daher wünschenswert. Da sich dieses Ziel auch auf die Kosten auswirkt, ist es ebenfalls bereits in Tab. 3 enthalten.

Auch außerhalb des Fahrdienstes gibt es Stakeholder aus der Belegschaft, die mit dem System zu tun haben. So muss das System von der Instandhaltung gewartet werden. Hierfür sind vor allem ein einfacher und klarer Aufbau und ein wartungsarmes System von Vorteil, denn auch in dieser Berufsgruppe herrscht Fachkräftemangel [Anzenhofer 2019]. Die Ziele aus Sicht der Instandhalter spiegeln sich bereits in den Zielen der hohen Verfügbarkeit und geringen Auswirkungen von Instandhaltungsmaßnahmen in Tab. 3 wieder.

Außerdem wird die Arbeit von Planern vom System beeinflusst, da heutige Stellwerke von diesen geplant und projektiert werden müssen. Derzeit gibt es ebenfalls zu wenige Planer [Verkehrsrundschau 2019]. Auch das Ziel einer effizienteren Planung wurde bereits durch die Kundensicht definiert, da sich eine effiziente Planung auch auf die Kosten auswirkt.

Die Ziele der Belegschaft sind also im Wesentlichen über ihren Einfluss auf die Kosten bereits berücksichtigt oder werden als nicht relevant für diese Arbeit angesehen. Es werden daher keine weiteren globalen Ziele aus den Zielen der Belegschaft heraus definiert.

Lieferanten

Ziele der Lieferanten sind üblicherweise im Wesentlichen das Sichern einer möglichst hohen Gewinnmarge, eine möglichst gleichmäßige Auslastung und stabile Lieferbeziehungen, die Planbarkeit für alle Seiten ermöglichen.

Lieferanten der Eisenbahninfrastrukturunternehmen für die infrastrukturseitige Sicherungstechnik sind in erster Linie die Firmen der Signalindustrie, aber zunehmend auch Hardware- und Softwarehersteller aus der Computerbranche. Aufgrund des langwierigen Zulassungsprozesses von Produkten und der vergleichsweise geringen Stückzahlen bei der Eisenbahn gibt es nur wenige Hersteller. Es ist aktuell üblich, Stellwerkssysteme inklusive aller daran angeschlossenen Feldelemente von einem Hersteller als monolithische Blackbox zu übernehmen. Dieses Vorgehen führt zu hohen Preisen, insbesondere bei der Instandhaltung, und stellt damit einen Widerspruch zu einem der zentralen Ziele aus Sicht des Kunden, nämlich niedrige Kosten und damit verbunden ein niedriger Preis für die Nutzung der Verkehrsdienstleistung, dar.

Um diese Abhängigkeit zu verringern, verfolgen einige Infrastrukturbetreiber bereits die Standardisierung von Schnittstellen zwischen Elementen der infrastrukturseitigen Sicherungstechnik (vgl. Kapitel 2.2.5). Gleichsam muss aus den hier und in anderen Arbeiten angestellten Überlegungen zu einer neuen Sicherungslogik auch ein Produktivsystem geschaffen werden und dafür sind die Zulieferer wichtige Partner. Deshalb ist es prinzipiell sinnvoll, auch ihre Zielsetzung im Blickfeld zu behalten.

Die Zielsetzung der Lieferanten steht aufgrund der gewählten gesamtgesellschaftlichen Sicht allerdings nicht im Vordergrund für die Überlegungen in dieser Arbeit. Daher werden keine weiteren globalen Ziele aus der Zielsetzung der Lieferanten heraus definiert.

Staatliche Institutionen

Staatliche Institutionen spielen im Bereich der Eisenbahn eine wichtige Rolle. Dies ist zum einen durch die hohen Sicherheitsanforderungen begründet, denn der Staat trägt Sorge für seine Bürger. Zum anderen spielen wettbewerbsrechtliche Regeln eine Rolle, die durch die Monopolstellung der Eisenbahninfrastrukturunternehmen ebenfalls dauerhaft staatlich überwacht werden.

Stakeholder aus sicherheitstechnischer Hinsicht sind vor allem das Eisenbahnbundesamt (EBA) als deutsche und die European Railway Agency (ERA) als europäische Aufsichtsbehörde sowie die Bundesstelle für Eisenbahnunfalluntersuchung (BEU), die zur Aufgabe hat, Unfälle zu analysieren und Empfehlungen zur zukünftigen Unfallverhinderung zu geben. Die Anforderung der Sicherheit wurde bereits aus Kundensicht erläutert. Des Weiteren haben die genannten Stellen ebenso wie die Justiz ein Interesse an transparenten Verfahren und einer lückenlosen Dokumentation aller sicherheitsrelevanter Prozesse. Diese Interessen müssen auch bei einer Neuentwicklung der Sicherungslogik gewährleistet werden. Die ERA wacht außerdem über die europäische Interoperabilität zwischen den nationalen Eisenbahnnetzen. Die Interoperabilität darf durch Neuentwicklungen seitens der infrastrukturseitigen Sicherungstechnik nicht beeinflusst werden.

Schließlich müssen Wettbewerbsverzerrungen durch die Funktionsweise der sicherungstechnischen Komponente verhindert werden. Hierüber wacht die Bundesnetzagentur (BNetzA). Die Aufrechterhaltung der Interoperabilität und die Vermeidung von Wettbewerbsverzerrungen werden

als weitere Ziele in den Katalog der globalen Ziele für die infrastrukturseitige Sicherungstechnik mit aufgenommen.

Zivilgesellschaft

Schließlich nimmt auch die Zivilgesellschaft Einfluss auf die Belange der Eisenbahn. Dieser Umstand äußert sich vor allem in Form von Lobbyarbeit der Kunden und einiger Umweltverbände für die Bahn sowie Anwohnerinitiativen und Naturschutzverbände gegen die Bahn, da sie Schallbelastung, Zerschneidungswirkung, Unfallgefahren oder einen negativen Einfluss auf die Biodiversität befürchten. Die Ziele der ersten Gruppe dürften in den Zielen der Kunden bereits enthalten sein. Die Ziele der zweiten Gruppe sind insofern relevant, dass ein bereits weiter oben definiertes Ziel der vorliegenden Arbeit ein mehr an Zugverkehr ist, welches den Interessen der genannten Gegner der Eisenbahn widerspricht. Allerdings sind weitere bereits oben definierte Ziele auch deckungsgleich mit den Zielen dieser Gruppen, zum Beispiel optimierte Energieverbräuche. Andere Ziele wie geringere Zerschneidungswirkungen oder ein Einfluss auf die Biodiversität werden durch die infrastrukturseitige Sicherungstechnik voraussichtlich nur unwesentlich beeinflusst und werden an dieser Stelle vernachlässigt.

Es werden daher aus den Zielen der Stakeholder der Zivilgesellschaft keine weiteren Ziele für das Projekt definiert.

Eisenbahnverkehrsunternehmen (EVU)

Die Eisenbahnverkehrsunternehmen sind die direkten Kunden der Eisenbahninfrastrukturunternehmen, die die infrastrukturseitige Sicherungstechnik primär betreiben. Es wurde davon ausgegangen, dass die von den Endkunden ausgehende Analyse auch den Großteil der Ziele der EVU berücksichtigt. Allerdings könnte es noch weitere Ziele der EVU geben, die noch nicht über die Endkunden abgedeckt sind.

Ansatzpunkt ist dabei die Kostenseite, da die Umsatzseite durch die Endkunden gut abgedeckt wird. Ein Problem für die EVU sind vertikale Verlagerungen innerhalb der Gesamtproduktionskosten entlang der Produktionskette zu Lasten der EVU. Diese Verlagerung ist auch ein häufig diskutierter Sachverhalt im Zuge der ETCS-Einführung. Hierbei befürchten die EVU, dass sie durch die hohen Kosten der ETCS-Fahrzeugausrüstung stärker belastet werden (vgl. [VDV 2018, S. 4]).

Da die vorliegende Arbeit rein die infrastrukturseitige Sicherungstechnik betrachtet und davon ausgegangen wird, dass notfalls Ausgleiche geschaffen werden können, wird dieses zusätzliche Ziel des Stakeholders EVU nicht weiter betrachtet.

Fazit

Die bereits in Kapitel 3.1.1 identifizierten und in Tab. 3 aufgelisteten Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik müssen durch die Stakeholder-Analyse nur geringfügig ergänzt werden. So wurden die Ziele „*Vermeidung von Wettbewerbsverzerrungen*“ und „*Aufrechterhaltung der Interoperabilität*“ durch die Betrachtung der Sichtweise der BnetzA hinzugefügt.

3.2 Ziele der Entwicklung der neuen Sicherungslogik

In diesem Kapitel sollen aus den globalen Zielen für die Neuentwicklung von Komponenten der infrastrukturseitigen Sicherungstechnik (vgl. Kapitel 3.1) die spezifischen Ziele für die in dieser Arbeit zu entwickelnde, neue Sicherungslogik „smartLogic“ hergeleitet werden. Diese spezifischen Ziele

bestimmen die Aufgabenstellung für die vorliegende Arbeit und bilden die Basis für die Herleitung der konkreten Anforderungen an die Entwicklung der smartLogic im nachfolgenden Kapitel 3.5.

Zur Bestimmung der spezifischen Ziele sind die globalen Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik aus Tab. 3 dahingehend zu untersuchen, inwiefern sie durch die neu zu entwickelnde Sicherungslogik beeinflussbar sein können. Hierfür ist eine Abgrenzung der Aufgaben der Komponente Sicherungslogik innerhalb der infrastrukturseitigen Sicherungstechnik erforderlich. Diese Abgrenzung ist jedoch bisher nicht fest vorgegeben, sondern kann noch durch die Anforderungen an die Sicherungslogik beeinflusst werden. Um diesen logischen Zirkelschluss zu durchbrechen, werden im folgenden Abschnitt zunächst Annahmen für den Zuständigkeitsbereich der Sicherungslogik getroffen, die später im Rahmen der Systemdefinition in Kapitel 4 detailliert werden. Auf Basis dieses Zuständigkeitsbereiches wird im darauffolgenden Abschnitt hergeleitet, welche Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik für die Komponente Sicherungslogik nicht relevant sind. Anschließend werden die verbleibenden Ziele für die Gestaltung der Sicherungslogik zusammengefasst.

Zuständigkeitsbereich der Sicherungslogik

Aufbauend auf den Zuständigkeitsbereichen bisheriger Stellwerkslogiken (vgl. Kapitel 2.1) und der Zuständigkeiten der Komponenten „Safety Logic“ und „Safety Manager“ in der RCA-Architektur (vgl. Kapitel 2.4.3) kann allgemein ausgesagt werden, dass die Sicherungslogik dafür zuständig ist, die Sicherheit von Zustandsänderungen im Bahnbetrieb wie Fahrerlaubnisse und geplante Statusänderungen von Infrastrukturelementen sicherzustellen sowie auf ungeplante Ereignisse mit Sicherheitsreaktionen zu reagieren. Die **Sicherheitsreaktion** dient dabei der Vermeidung von Gefährdungen, die in Folge des ungeplanten Ereignisses auftreten können.

Für die Gestaltung der Sicherungslogik nicht relevante Ziele

Einige der in Kapitel 3.1 identifizierten Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik sind gemäß des so festgelegten Zuständigkeitsbereiches für die Sicherungslogik nicht relevant. Im Folgenden werden die Gründe dafür hergeleitet.

Gemäß den Überlegungen aus Kapitel 2.2.6 wird dabei angenommen, dass die Sicherungslogik eine Software-Komponente ist, die auf einer sicheren (Computer-)Hardwareplattform läuft. Die Software kann demnach also unabhängig von der Computerhardware betrachtet werden. Die Performance der Hardwareplattform und ihre spezifischen Eigenschaften sind daher nicht im Fokus dieser Arbeit. Alle in Kapitel 3.1 definierten Ziele, die sich ausschließlich auf die Hardware beziehen, sind daher für die Komponente Sicherungslogik grundsätzlich nicht relevant.

Eine Ausnahme von der im vorigen Absatz formulierten Aussage zur Relevanz der auf Hardware bezogenen Ziele bilden solche Ziele, die durch die Arbeitsweise der Software Sicherungslogik beeinflusst werden. (Es wird angenommen, dass der Einfluss der Sicherungslogik auf den Parameter „*Stromverbrauch*“ vernachlässigt werden kann.[9]) Hierbei sticht basierend auf dem grundsätzlichen Aufbau der infrastrukturseitigen Sicherungstechnik (Kapitel 2.1) sowie aktuell bestehenden oder diskutierten Modifikationen (Kapitel 2.2, 2.2.8 und 2.4) – ohne an dieser Stelle zu viel Vorgriff auf die Systemdefinition in Kapitel 4 zu nehmen – das Ziel „*wenig Hardware*“ heraus. Der Umfang der benötigten Hardware wird stark durch die Funktionsweise der Sicherungslogik beeinflusst.

[9] An dieser Stelle handelt es sich um den Stromverbrauch durch die Software Sicherungslogik; mögliche Restriktionen der Anzahl gleichzeitig umlaufender Stellelemente durch den zur Verfügung stehenden Strom fallen hier nicht darunter, sondern wären eine funktionale Anforderung an die Logik und damit Thema in Kapitel 6.

Beispielsweise hängt sie davon ab, ob die Sicherungslogik Fahren im wandernden Raumabstand „Moving Block“ unterstützt oder ob und in welchem Maße Flankenschutz durch (Sperr-)Signale hergestellt werden muss. Deshalb wird das Ziel „*wenig Hardware*“ für die Komponente Sicherungslogik übernommen.

In der RCA-Architektur wird auch der Bereich des Kontrollzentrums strikt von der Komponente Sicherungslogik getrennt. Diese Trennung ist auch bereits in heutigen ESTW realisiert. Die Benutzeroberfläche ist nicht Teil dieser Arbeit. Daher wird die Zielsetzung bezüglich der Art der Bedienung für die Komponente Sicherungslogik (*„einfache und ergonomische Bedienung“*) als nicht relevant angenommen. Relevant ist dagegen das Ziel, wonach eine möglichst gleichmäßige Belastung der Arbeitskräfte erreicht werden soll, da dieses Ziel durch die Sicherungslogik beeinflusst werden kann, indem beispielsweise Kontrollbereiche flexibel zugeschnitten werden können.

Da die Sicherungslogik gemäß ihrer Aufgabenstellung nicht selbst Entscheidungen treffen soll, welche Arten von Zugfahrten priorisiert die Infrastruktur nutzen dürfen, – denn diese Entscheidung ist nicht sicherheitskritisch, – kann das Ziel der *„Verhinderung von Wettbewerbsverzerrung“* ebenfalls außer Acht gelassen werden. In klassischen Stellwerken werden solche Entscheidung durch den Fahrdienstleiter oder ein Leitsystem getroffen.

Zusammenfassung der relevanten Ziele für die Gestaltung der Sicherungslogik

Tab. 4 gibt eine Übersicht über die Relevanz der Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik für die Komponente Sicherungslogik. Um die Übersichtlichkeit zu erhöhen und die Komplexität zu vermindern, werden ähnliche relevante Ziele dabei zu Zieldimensionen zusammengefasst.

Tab. 4: Ziele für die Gestaltung der Komponente Sicherungslogik

Ziele für die Gestaltung der infrastrukturseitigen Sicherungstechnik	Relevanz für die Komponente Sicherungslogik	Zieldimension
einfache Projektierung		geringer Planungs- und Genehmigungsaufwand
einfache Anpassbarkeit an neue Gegebenheiten bzw. Örtlichkeiten		
Aufrüstbarkeit bei neuen Anforderungen		
kurze Zulassungsprozesse		
geringe Komplexität		
lange Lebenszeit		lange Nutzungszeiten (der Komponenten)
wenig Hardware		geringer Hardwareeinsatz
verschleißarme Hardware	*nicht im Fokus*	
möglichst gut recyclebar	*nicht im Fokus*	
einfache und ergonomische Bedienung	*nicht im Fokus*	
möglichst geringe aber gleichmäßige Auslastung der benötigten Arbeitskräfte		geringer Arbeitskräfteeinsatz
geringer Stromverbrauch	*nicht im Fokus*	
geringe Anforderungen an technische Begleitsysteme	*nicht im Fokus*	

minimaler Energieverbrauch der Fahrzeuge		Energieeffizienz
einfach zu wartende Technik, geringe Ausfallrate	*nicht im Fokus*	
möglichst geringe Einschränkungen der maximalen Fahrzeuggeschwindigkeit		hohe Kapazität
Wartezeiten vermeiden		
möglichst viele Fahrzeugbewegungen ermöglichen		
möglichst geringe Einschränkungen des Betriebs bei Instandhaltungsmaßnahmen		hohe Robustheit
planbare Auswirkungen auf den Betrieb		
hohe Verfügbarkeit, geringe Ausfallraten		
geringstmögliche Auswirkungen von Abweichungen zum Regelbetrieb		
Verhindern von Wettbewerbsverzerrungen	*nicht im Fokus*	
Aufrechterhalung der Interoperabilität		Interoperabilität

Die Aufgabenstellung an die Arbeit sieht also vor, dass eine neue Sicherungslogik so entwickelt werden soll, dass sie bei geringem Planungs- und Genehmigungsaufwand eine möglichst hohe Kapazität auf der bestehenden Infrastruktur bei gleichzeitig möglichst robustem und energieeffizientem Betrieb ermöglicht. Dabei soll die Logik einen geringen und flexiblen Arbeitskräfteeinsatz ermöglichen sowie einen geringen Hardwareeinsatz mit langer Nutzungszeit der Komponenten.

3.3 inhaltliche Abgrenzungen

Aufgrund der zeitlichen Rahmenbedingungen der Arbeit ist wie in jeder wissenschaftlichen Arbeit eine inhaltliche Abgrenzung vorzunehmen.

In Bezug auf den Reifegrad der Ergebnisse wurde entschieden, die Logik nur bis zur Entwicklungsphase der Modellierung (entspricht dem Teil „Entwurf“ im Schritt „Entwurf und Implementierung“ im V-Modell, vgl. Kapitel 2.6.1) zu entwickeln, da bis zu diesem Schritt die inhaltliche Konzeptionsarbeit im Vordergrund steht und die Modellierung eine gute Ausgangsbasis für eine spätere Produktentwicklung bietet. Eine feinere Spezifikation unter Einhaltung der CENELEC-Normen für die Entwicklung sicherungskritischer Software ergibt keinen Sinn, da die vorgeschriebenen Prozesse mit den verfügbaren Ressourcen nicht vollständig durchgeführt werden können. Um die Ergebnisse zu demonstrieren wird jedoch noch ein Software-Demonstrator der Sicherungslogik im Eisenbahnbetriebsfeld Darmstadt implementiert.

Inhaltlich beschränkt sich die Arbeit auf die Modellierung der wichtigsten (Basis-)Prüfprozesse zur Aufrechterhaltung eines sicheren und funktionierenden Bahnbetriebs. Insbesondere sollen Rückfallebenen und Übergangsprozesse zu anderen Stellbereichen mit Alttechnologien nur am Rande betrachtet werden. Die Basisprüfprozesse werden basierend auf einer ausführlichen Betrachtung der funktionalen Anforderungen ausgewählt. Bei der Bestimmung dieser funktionalen Anforderungen sollen aber möglichst keine Abgrenzungen vorgenommen werden.

Weiterhin beschränkt sich die Arbeit bei der Sicherheitsbetrachtung auf den Bereich der **funktionalen Sicherheit** zum Schutz gegen unbeabsichtigte Ereignisse, da der Themenbereich des Schutzes vor gezielten Angriffen (**Security**) ein eigener komplexer Forschungsbereich ist, dessen Berücksichtigung den Rahmen der Arbeit sprengen würde.

Bezüglich der verwendeten Hardwareplattform wird, wie bereits in Kapitel 3.2 festgestellt, davon ausgegangen, dass eine generische Plattform verwendet werden kann, so dass auf die Gestaltung dieser Hardwareplattform nicht näher eingegangen werden muss.

Weiterhin wird davon ausgegangen, dass die benötigten Daten (z. B. zur Topologie und zu den Fahrzeugen) vorhanden sind. Wie diese Daten erfasst werden, ist nicht Teil dieser Arbeit.

Im Rahmen der Nutzenpotenzialanalyse müssen ebenfalls Einschränkungen vorgenommen werden. So kann aus Ressourcengründen keine umfangreiche statistische Erhebung sowie Beobachtungs- und Interview-Reihe durchgeführt werden. Da die Erarbeitung der Logik jedoch systematisch erfolgt, wird angenommen, dass eine exemplarische Beobachtung sowie ein Expertenworkshop ausreichend sind, um Anforderungen an die zu entwickelnde Logik definieren zu können. Eine systematische Kapazitätsuntersuchung der in dieser Arbeit zu entwickelnden Sicherungslogik kann ebenfalls nicht geleistet werden und bleibt ein Thema für zukünftige Arbeiten.

Weiterhin kann im Rahmen der Arbeit die Bestimmung von Zahlenwerten, beispielsweise für den Einfluss der einzelnen Risikofaktoren auf das Prüfergebnis der Sicherungslogik oder für zulässige Wertebereiche für zu prüfende Variablen, nicht erfolgen. Hintergrund ist, dass diese Daten komplex zu erheben sind. Die Werte liefern außerdem keine Erkenntnisse für die Erarbeitung des grundsätzlichen Konzeptes der neuen Sicherungslogik.

3.4 Identifikation von Nutzenpotenzialen einer neuen Sicherungslogik

Um zur Erreichung der in der Aufgabenstellung in Kapitel 3.2 identifizierten Ziele Anforderungen an die Entwicklung bzw. Gestaltung der neuen Logik formulieren zu können, kann es hilfreich sein, mögliche Potenziale für die Verbesserung der Sicherungslogik zu identifizieren, die einen Nutzen in Hinblick auf die Erreichung der Ziele versprechen. Nachfolgend werden in Kapitel 3.4.1 verschiedene Methoden zur Identifikation der Verbesserungspotenziale hergeleitet und anschließend in den Kapiteln 3.4.2 bis 3.4.5 die Ergebnisse als Resultat der Anwendung der in Frage kommenden Methoden beschrieben.

3.4.1 Methoden

Um ein technisches System wie die Sicherungslogik zu verbessern, müssen auch die Prozesse analysiert werden, in die das System eingebunden ist bzw. zu deren Umsetzung es beiträgt. Zur Identifikation von Verbesserungspotenzialen und damit von Nutzenpotenzialen für die smartLogic kommen daher Methoden aus dem Qualitätsmanagement in Betracht, dessen Aufgabe die Verbesserung von Produktionsprozessen ist. Demnach bestehen vor allem die folgenden Möglichkeiten [vgl. Kamiske 2015a]:

- Beobachten des Produktionsprozesses
- statistische Erhebungen von Problemen/Schwachstellen, z. B. mittels Fehlersammelliste
- Interviews, insbesondere von Experten und am Betrieb Beteiligten
- prozessbasiertes Benchmarking

Da Verbesserungspotenziale in Hinblick auf die Sicherungslogik untersucht werden sollen, ist eine *Beobachtung des* relevanten *Produktionsprozesses* der Durchführung von Fahrzeugbewegungen auf der Eisenbahninfrastruktur nur an Orten sinnvoll, an denen die Auswirkungen der Arbeitsweise der Sicherungslogik deutlich werden und im Zusammenhang mit dem aktuellen Betriebsgeschehen beobachtet werden können. Diese Zusammenhänge werden über die Meldeanzeigen an den Bedienplätzen der Fahrdienstleiter und Disponenten in den Stellwerken bzw. den Betriebszentralen deutlich.

Die Durchführung einer *statistischen Erhebung* zum Zwecke der Identifikation von Nutzenpotenzialen wird aufgrund des hohen Aufwandes als nicht verhältsnismäßig eingeschätzt. Es wird angenommen, dass die anderen oben genannten Möglichkeiten aus [Kamiske 2015a] hinreichend sind, um die wichtigsten Verbesserungspotenziale aufgrund der Häufigkeit ihres Vorkommens zu identifizieren.

Als Experten für *Interviews* bieten sich Personen an, die mit der Funktionsweise der Sicherungslogik vertraut sind und somit Schwachstellen der bisherigen Sicherungstechnik aus eigener Praxiserfahrung benennen können. Dieser Personenkreis kann über die Lebenszyklusphasen der Sicherungslogik eingegrenzt werden. So sind in den Phasen des Entwurfs, der Planung, Herstellung und Installation die im Planungs- und Genehmigungsprozess vorgesehenen Personengruppen involviert. Diese Personengruppen sind Gutachter, Sachverständnisse, Mitarbeiter von Aufsichtsbehörden, Mitarbeiter von Herstellern von Sicherungstechnik und Mitarbeiter von Eisenbahninfrastrukturunternehmen. In der Phase des Betriebs haben vor allem Fahrdienstleiter und Instandhalter einen logischen Bezug zur Sicherungslogik. Fahrdienstleiter nehmen bei ihrer Tätigkeit täglich die Auswirkungen der Sicherungslogik auf den Betrieb wahr. Allerdings sehen sie aufgrund ihres räumlich und zeitlich begrenzten Einsatzes nur einen kleinen Ausschnitt des Gesamtgeschehens. Übergeordnete Stellen bei den Infrastrukturunternehmen haben dagegen einen umfassenderen Blick. Gutachter und Sachverständige werden in der Regel nur zur Abgabe von Einschätzungen zu bestimmten Teilsystemen oder genau umrissenen Sachverhalten beauftragt. Allerdings haben sie aufgrund ihrer externen Anstellung einen distanzierteren Blick auf den Sachverhalt als Beschäftige der einzelner Eisenbahnunternehmen.

Aus Ressourcengründen kann keine umfassende Interviewreihe durchgeführt werden. Das Einbeziehen von Akteuren direkt von den Eisenbahninfrastrukturunternehmen erscheint aufgrund deren umfassenden Blicks als Nutzer der technischen Systeme zur Identifizierung von Nutzenpotenzialen einer neuen Sicherungslogik am zielführendsten zu sein. Erster Ansprechpartner ist hierfür die DB Netz AG als Europas größtes Eisenbahninfrastrukturunternehmen (EIU).

Zur Vervollständigung wird abschließend auch ein *prozessbasiertes Benchmarking* durchgeführt.

3.4.2 Gespräch mit einem Leiter Signaltechnik

Um ein Feedback zu den bisherigen Erkenntnissen zu erlangen, wurde ein Interview mit dem Leiter Signaltechnik der DB Netz AG geführt. Bei dem Gespräch wurde zunächst nach Schwachstellen der aktuellen Signaltechnik gefragt und im zweiten Schritt wurden Fragen zur Wahl einer geeigneten Vorgehensweise für die Arbeit gestellt.

Zur Frage der aktuellen Schwachstellen verwies der Experte insbesondere auf Fahrstraßenausschlüsse durch Durchrutschwege. Hierdurch würden besonders im Verspätungsfall zusätzliche Verspätungsminuten aufgebaut. Die Durchrutschwege seien aus Sicht der interviewten Person aber unbedingt notwendig. Weiterhin wurde das Problem der hohen Investitionskosten unterstrichen. Aus diesem Grund solle eine weitere Kostensteigerung durch eine neue Sicherungslogik unbedingt vermieden werden. Ebenfalls wurde bestätigt, dass nachträgliche Anpassungen an der

Sicherungstechnik häufig nicht vorgenommen werden könnten, da dies erhebliche finanzielle Mittel durch den erforderlichen Planungs- und Zulassungsprozess erfordere. Somit sei es schwierig, nachträglich sich als ungünstig erweisende Projektierungen anzupassen.

Bezüglich der Vorgehensweise rät der Experte, die Gefährdungen als Ausgangspunkt zu nehmen und zuerst eine umfassende Funktionsanalyse durchzuführen, welche in einem folgenden Schritt wieder auf die zunächst relevanten Kernfunktionen eingegrenzt wird. Das im Interview vorgestellte Zielbild (vgl. Kapitel 3.1) würde in die richtige Richtung gehen. Es sei davon auszugehen, dass eine Umsetzung einer neuen Sicherungslogik aufgrund des erforderlichen, aufwendigen Sicherheitsnachweises zeitintensiv sei. Deshalb sei auf die Migrationsfähigkeit der zu erarbeitenden Lösung zu achten.

3.4.3 Beobachtung von Betriebspersonal

Um einen Einblick in die Betriebspraxis zu erlangen, erfolgte ein Besuch der Betriebszentrale des Regionalbereichs Mitte in Frankfurt am Main mit Beobachtung und anschließender Befragung eines erfahrenen Fahrdienstleiters der DB Netz AG.

Fragestellung

Zur Erarbeitung der Fragestellung für den Besuch bieten sich wiederum Instrumente aus dem Bereich des Qualitätsmanagements an. Bereits in der Antike dienten die sieben W-Fragen als Leitfaden für Beobachtungen und begleitende Gespräche [vgl. Rau 2015]. Im weiteren bzw. übertragenen Sinne können diese typischen Fragestellungen auch für Fragen an Prozessbeteiligte bei der Prozessoptimierung von Produktionssystemen genutzt werden [vgl. Lindner & Becker 2015, S. 300]. Tab. 5 listet die aus den W-Fragen und der globalen Zielsetzung (vgl. Kapitel 3.1) hergeleiteten Fragestellungen für die Beobachtung und die Befragung auf.

Tab. 5: Fragestellungen für Beobachtung und Befragung des Betriebspersonals

W-Frage	Typische Fragestellungen im Qualitätsmanagement nach [Rau 2015]	Fragestellung für die Beobachtung und die Befragung
Was?	Was ist der Fehler? Was läuft suboptimal?	Welche betrieblichen Ineffizienzen gibt es in Hinblick auf die Zielsetzung aus Kapitel 3.1? Wodurch wird Infrastruktur nicht optimal ausgenutzt? Wodurch verlängern sich Reisezeiten? Gibt es unnötige Hardware (z. B. unnötige Infrastrukturelemente)? Gibt es unergonomische Betriebsprozesse
Wie?	Wie äußert sich das Problem?	Was sind die Konsequenzen der Ineffizienz? Welche Auswirkungen hat das auf die Kapazität oder auf Verspätungsminuten?
Wer?	Wer ist betroffen?	Welche Zugfahrten / Zugarten / Verbindungen etc. sind betroffen?
Wo?	Wo (geografisch) ist der Fehler beobachtet worden bzw. ist das Problem aufgefallen?	In welchen Infrastrukturkonstellationen tritt das Problem auf?

Wann?	Wann ist das Problem aufgetreten? (Zeitpunkt, Zeitraum, Situation) Wie oft tritt das Problem auf? Gibt es Zyklen?	Welche (betrieblichen) Voraussetzungen müssen erfüllt sein, damit das Problem auftritt?
Wie viel?	Wie groß ist das Ausmaß des Problems?	Wie viele Züge sind betroffen? Wie groß ist das Ausmaß der Kapazitätseinbußen, der zusätzlichen Verspätungsminuten, etc.?
Warum?	Warum ist das Problem aufgetreten? Was verstärkt das Problem? Was reduziert das Problem?	Welchen Einfluss haben die Komponenten Technik, Personal und Regelwerk bei dem Problem? *Die genaue Analyse der Ursache war nicht Fokus der Beobachtung bzw. der Befragung*

Rahmenbedingungen

Beobachtung und ergänzende Befragung erfolgten in einem inoffiziellen Rahmen und werden hier daher anonymisiert beschrieben. Die in Tab. 5 genannten Fragestellungen dienten als interner Leitfaden und wurden nicht, wie in einem Fragebogen, Schritt für Schritt abgearbeitet, sondern situationsgerecht in einem offenen Gespräch eingebracht. Dies hat den Vorteil, dass dem Charakter einer Beobachtung entsprechend das aktuelle Betriebsgeschehen im Vordergrund steht und den Ausgangspunkt der Analyse bildet, im Gegensatz zu einer systematischen Untersuchung möglicher Fehlerquellen im Rahmen einer ganzheitlichen Untersuchung des Betriebs. Wie in Kapitel 3.4 eingangs beschrieben ist Letzteres nicht der Zweck der hier beschriebenen Nutzenermittlung.

Die Betriebszentrale (BZ) Mitte der DB Netz AG in Frankfurt am Main wurde zum einen aufgrund der räumlichen Nähe zu Darmstadt gewählt und zum anderen, da Verbesserungspotenziale beim aktuellen Stand der infrastrukturseitigen Sicherungstechnik, also elektronischen Stellwerken (ESTWs) identifiziert werden sollen, die i. d. R. von der BZ aus bedient werden. Um genügend Komplexität zu haben, soll ein größerer Stellbereich mit einigen Betriebsstellen untersucht werden, die unterschiedlich aufgebaut sind und somit verschiedene Betriebssituationen möglich machen. Idealerweise sollen über die betrachtete(n) Strecke(n) verschiedene Zugarten (Regionalverkehr, Fernverkehr, Güterverkehr) in engem Abstand aufeinander folgen. Gleichzeitig soll die Komplexität aber auch nicht zu groß werden, so dass der Überblick verloren gehen könnte. Aus letzterem Grund schied der Stellbereich des Frankfurter Hauptbahnhofs und der unmittelbaren Zuläufe aus. Aus den oben genannten Gründen wurde der Stellbereich Bad Vilbel gewählt, der die zweigleisige Hauptstrecke von Kassel über Marburg nach Frankfurt am Main („Main-Weser-Bahn“) im Abschnitt von Frankfurt am Main-West bis kurz vor Friedberg sowie Teile der Nebenstrecke nach Glauburg-Stockheim (Niddertalbahn) umfasst.

Auf der Hauptstrecke des gewählten Stellbereichs verkehrten zum Zeitpunkt der Beobachtung ICE- und RE-Züge stündlich im Wechsel sowie Regionalbahn- und S-Bahn-Züge. Zudem gibt es regen Güterverkehr. Bei Betriebsstörungen auf dem Korridor Frankfurt – Fulda – Kassel – Hannover bildet die Main-Weser-Bahn außerdem die Umleitungsstrecke. Neben dem Bahnhof Bad Vilbel befinden sich im Stellbereich die Bahnhöfe Nieder-Wöllstadt, Groß-Karben und Frankfurter Berg. Der Fahrdienstleiter wurde von der Leitung der BZ als erfahrener Fahrdienstleiter ausgewählt. Als Beobachtungszeitpunkt wurde die nachmittägliche Hauptverkehrszeit gewählt.

Beobachtungen

Bei der Beobachtung über zwei Stunden in der nachmittäglichen Hauptverkehrszeit von 16 Uhr – 18 Uhr traten die in Tab. 6 beschriebenen Situationen auf, die zunächst nach den in Kapitel 3.1 ermittelten Zielen verbesserungswürdig erscheinen. Dabei ist zu beachten, dass jede – auch kleine – Verspätung auf einem hochbelasteten Netz durch Kaskadeneffekte weitere Folgeverspätungen und Anschlussgefährdungen außerhalb des Betrachtungsraumes zur Folge haben kann.

Tab. 6: Ergebnisse der Betriebsbeobachtung

Vorgang	Ursache	angenommener Raum für Verbesserungen
Güterzüge mussten häufig (planmäßig) in ein Überholgleis einfahren	schnellerer Verkehr sollte passieren	erhöhter Energieverbrauch, verlängerte Beanspruchung von Infrastrukturressourcen
Personenzug musste durch einen verkürzten Durchrutschweg (D-Weg) langsamer einfahren	vorausfahrender Güterzug hatte eine geringfügige Verspätung, wodurch eine Weiche im planmäßigen D-Weg des Personenzuges noch belegt war	Verspätung für den Personenzug
Züge fahren generell häufig langsamer als technisch möglich	durch die Technik bedingte frühzeitige Signalisierung einer einschränkenden Geschwindigkeit	längere Fahrzeit als nötig
Personenzug wurde durch Güterzug ausgebremst	der Fahrdienstleiter vergaß, den Güterzug in die planmäßige Überholung zu nehmen	Verspätung für den Personenzug
Personenzug ist durch verspätete Fahrstraßenbildung geringfügig zu spät abgefahren	der Fahrdienstleiter vergaß, einen Dispositionshalt zu löschen	Verspätung für den Personenzug

Wie bereits geschildert, stellen diese Beobachtungen nur einen Momenteindruck aus der Beobachtung nur eines Fahrdienstleiters in einem relativ kurzen Zeitraum dar. Zudem ist nicht garantiert, dass durch eine neue Sicherungslogik das vermeintliche Verbesserungspotenzial auch tatsächlich realisiert werden kann, zum Beispiel bei planmäßigen Überholungen. Dennoch liefern diese Beobachtungen Indizien, an welchen Punkten eine neue Sicherungslogik ansetzen kann, um Verbesserungen im Bahnbetrieb zu erzielen.

Basierend auf den Beobachtungen kann angenommen werden, dass bei Überholungen die technisch bedingte Wartezeit gering gehalten und falls möglich ein vollständiger Stillstand des zu überholenden Zuges vermieden werden sollte. Weiterhin sollten möglichst nicht vor dem eigentlichen Gefahrpunkt eingeschränkte Geschwindigkeiten gefahren werden müssen. Das Potenzial für menschliche Fehlhandlungen sollte so gering wie möglich gehalten werden und Fehler möglichst unproblematisch nachträglich korrigiert werden können, z. B. indem für einen Zug möglichst spät noch der Fahrweg geändert werden kann. Schließlich erweist sich auch das Thema der Durchrutschwege als optimierungswürdig.

Befragung

Um den Eindruck aus der Beobachtung zu unterstützen, wurde zusätzlich der Fahrdienstleiter anhand der in Tab. 5 beschriebenen Fragestellungen befragt. Dabei konnten einige der Beobachtungen

untermauert werden. So habe aus Sicht des Fahrdienstleiters der Durchrutschweg (D-Weg) einen entscheidenden Einfluss auf die Endgeschwindigkeit und führe am häufigsten zu unerwünschten betrieblichen Situationen mit Fahrzeitverlust. An verschiedenen Stellen führten geringe betriebliche Abweichungen zur Notwendigkeit, verkürzte D-Wege zu wählen, welche mit einer verringerten Einfahrgeschwindigkeit einhergehen. Zwei dieser Situationen sind im Folgenden geschildert.

Eine typische Situation findet sich demnach in Betriebsstellen, die wie Frankfurter Berg aufgebaut sind. Dort gibt es zwischen den beiden durchgehenden Hauptgleisen ein in Mittellage liegendes drittes Gleis, in welches aus beiden Richtungen Züge geleitet werden können, um überholt zu werden. Abb. 20 zeigt den Gleisplan der Betriebsstelle Frankfurter Berg.

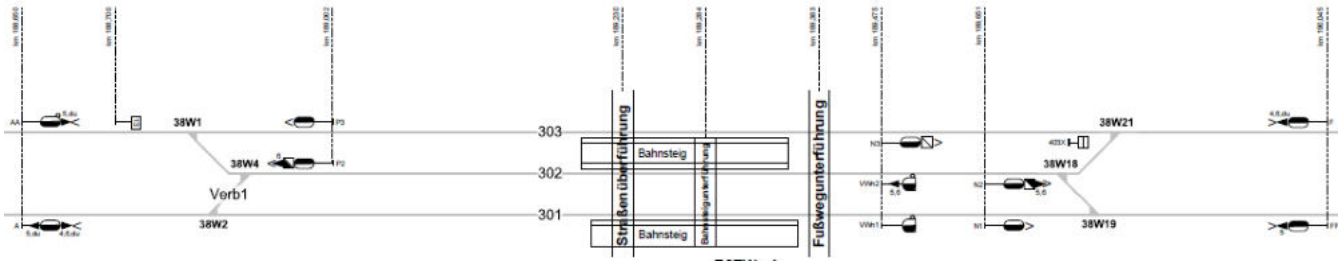


Abb. 20: Gleisplan Bahnhof Frankfurter Berg
Quelle: Trassenfinder (www.trassenfinder.de)

Bei Einfahrten in das Überholgleis wird zwar die Einfahrweiche unmittelbar, nachdem sie durch den einfahrenden Zug verlassen wurde, wieder freigegeben, die Weichenverbindung nach dem Zielsignal gehört aber noch zum Durchrutschweg. Dadurch werden bis zur Auflösung und Freigabe des D-Weges nach dem vollständigen Halt des Zuges und Ablauf der für die Auflösung festgelegten Zeit entweder Fahrten auf dem gegenüberliegenden Gleis verhindert oder nachfolgende Fahrten auf demselben Einfahrgleis, welche häufig die zuerst betrachtete Zugfahrt überholen sollen, eingeschränkt.

Bahnhöfe mit ähnlich aufgebauter Gleistopologie finden sich relativ häufig. So ist beispielsweise der Bahnhof Groß-Karben (Abb. 21) ähnlich aufgebaut. Auch im vierten sich auf der Strecke befindlichen Bahnhof Nieder-Wöllstadt (Abb. 22) tritt beim Überholgleis das Problem in leicht abgeänderter Form auf, da der D-Weg bei Einfahrten nach Gleis 3 gleichzeitig Einfahrten[10] nach bzw. Durchfahrten durch Gleis 2 verhindert.

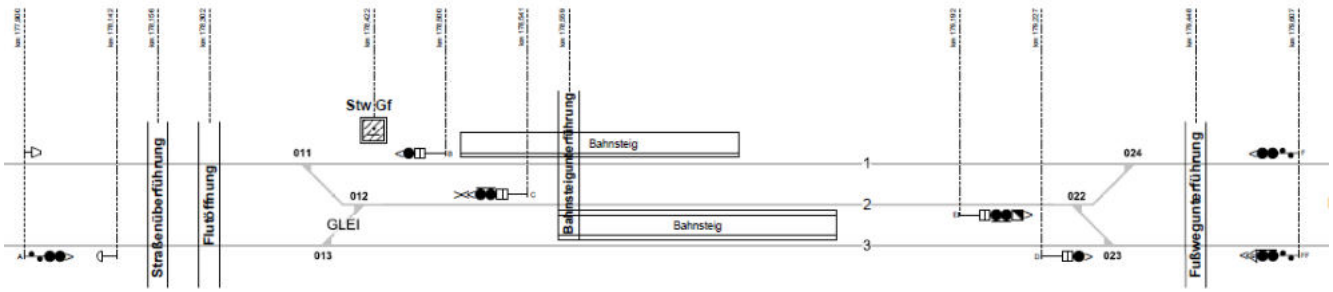


Abb. 21: Gleisplan Bahnhof Groß-Karben
Quelle: Trassenfinder (www.trassenfinder.de)

[10] In machen Anwendungsfällen dieser Art könnten Einfahrten auf Gleis 2 vor Auflösung des D-Weges der Fahrstraße nach Gleis 3 allerdings möglich sein, wenn überlappende D-Wege erlaubt sind und projektiert wurden.

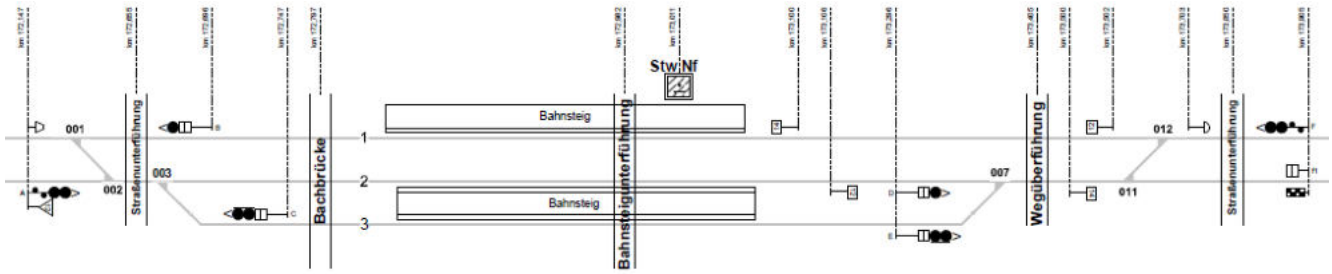


Abb. 22: Gleisplan Bahnhof Nieder-Wöllstadt
Quelle: Trassenfinder (www.trassenfinder.de)

Etwas komplexer ist die Situation am größeren Bahnhof Bad Vilbel. Der Gleisplan des Bahnhofs ist in Abb. 23 dargestellt. Die Einfahrsignale sind in der Darstellung abgeschnitten, um eine größere Darstellung zu ermöglichen.

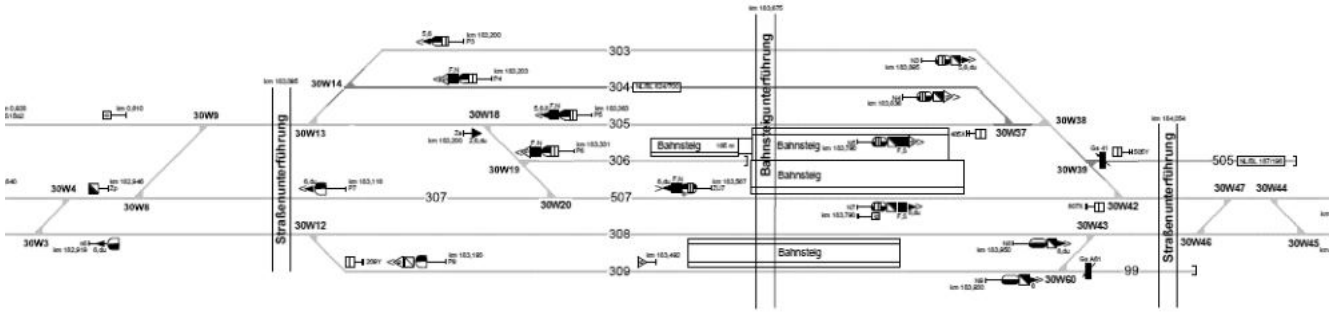


Abb. 23: Gleisplan Bahnhof Bad Vilbel
Quelle: Trassenfinder (www.trassenfinder.de)

Auch bei einem solchen Bahnhofslayout mit außen angeordneten Überholgleisen kann das bereits am Beispiel Frankfurter Berg geschilderte Problem auftreten. Eine Einfahrt in Gleis 309 aus Richtung Groß-Karben (links) würde z. B. eine nachfolgende schnelle Durchfahrt durch Gleis 308 verhindern, wenn nicht noch wie im vorliegenden Fall Platz für das Stumpfgleis 99 gewesen wäre.

Ein weiteres, aber selteneres Problem tritt in Bad Vilbel auf, wenn eine Einfahrt ins Gegengleis (über Weichen 30W46 und 30W47) erforderlich ist. In diesem Fall kann eine Einfahrstraße mit einem D-Weg über Weiche 30W46 in Linkslage gelegt werden, die mit normaler Einfahrgeschwindigkeit befahren werden kann und anschließend das direkte Stellen der Ausfahrstraße noch vor Auflösung des D-Weges ermöglicht. Allerdings kann dann bereits zum Zeitpunkt des Stellens der Einfahrstraße keine Zugfahrt im Gegengleis mehr stattfinden, da die Weiche 30W46 hierfür als Flankenschutz in Rechtslage benötigt wird. Dieser Fall erscheint zunächst sehr selten zu sein, da für seinen Eintritt viele spezielle betriebliche Bedingungen (Fahren im Gegengleis, dichte Zugfolge aus Richtung Groß-Karben (links) und gleichzeitig Gegenzug aus Richtung Frankfurter Berg (rechts)) erforderlich sind. Allerdings ist besonders bei verminderter Kapazität – worauf das Fahren im Gegengleis deutet – eine flexibel nutzbare Infrastruktur wünschenswert, denn gerade in diesem Fall sind knappe Zugfolgen, insbesondere bei Kreuzungen mit der Gegenrichtung wahrscheinlich.

In einer weiteren Betriebssituation, die in Bad Vilbel gelegentlich auftrat, verursachte ein zu langer Zug auf Gleis 305, der mit der Spitze vor Signal P5 steht, ein Flankenschutzproblem. Ursache war das vorgerückte Ausfahrsignal N5. Ragte der Zug über den Gleisfreimeldeabschnitt des Signals hinaus, bestand kein Flankenschutz für Ein- und Ausfahrten aus bzw. in Richtung Frankfurter Berg (rechts) in Gleis 303 oder 304, da kein weiteres Flankenschutzelement vor der Weiche 30W37 existierte. Das Problem wurde vom Betriebspersonal erkannt und gemeldet. Im konkreten Fall konnte das Problem mit einem zusätzlichen Sperrsignal vor der Weiche 30W37 gelöst werden, welches als zusätzliches

Flankenschutzelement fungiert. Der Einbau des zusätzlichen Sperrsignals wurde in Bad Vilbel möglich, da durch den viergleisigen Ausbau der Main-Weser-Bahn zwischen Frankfurt am Main-West und Bad Vilbel ohnehin eine neue Version der Stellwerkssoftware erarbeitet und installiert werden musste. Ansonsten wäre eine Behebung des Problems vermutlich aufgrund der erforderlichen Neuzulassung des Stellwerkssystems zu aufwändig gewesen.

Schlussfolgerungen

Trotz des Umstandes, dass es sich bei der Beobachtung und Befragung um eine kurze Momentaufnahme mit nur einem Probanden handelte, konnte der Autor dieser Arbeit einige Schlüsse daraus ziehen.

Der Besuch in der BZ unterstützt die Annahme, dass es im Bereich der Sicherungslogik noch Verbesserungspotenzial gibt, welches mit einer „smarten“ Logik gehoben werden könnte. Indiz hierfür sind die beobachteten Ineffizienzen im realen Betrieb, für die in Anbetracht der sich weiterentwickelnden Technologien (vgl. Kapitel 2.2) und der damit verfügbaren größeren Menge an Informationen, wie der exakten Zugposition und der Möglichkeit, präzise Vorgaben zum Fahrverhalten ins Triebfahrzeug zu übertragen, eine optimierte Lösung möglich erscheint.

Im Bereich der Fahrzeit- und Energieoptimierung erscheinen dynamische Durchrutschwege zielführend zu sein. Deren Länge sollte vom Bremsvermögen des Fahrzeuges, das (bzw. vor dem) durch den D-Weg geschützt wird, abhängig sein. Die Einfahrgeschwindigkeit sollte dabei nur soweit reduziert werden, wie es für die sichere Anfahrt auf den Gefahrpunkt tatsächlich notwendig ist. Eventuell durch den D-Weg beanspruchte Infrastrukturelemente sollten schnellstmöglich wieder freigegeben werden, wenn der Grund der Beanspruchung weggefallen ist. Fahrzeugseitig ist die dynamische D-Weg-Berechnung bei Systemen wie ETCS und Linienzugbeeinflussung (LZB) zum Teil bereits möglich, allerdings hält das Stellwerk in diesen Fällen zugunabhängig dennoch den kompletten D-Weg solange vor, bis es davon ausgeht, dass dieser auf keinen Fall mehr benötigt werden kann. Daher scheint eine Optimierung im Bereich der Sicherungslogik in Bezug auf D-Wege zielführend zu sein.

Aus den betrachteten Szenarien kann indirekt zusätzlich geschlussfolgert werden, dass aufgrund der ortsfesten Signalisierung die einschränkende Geschwindigkeit häufig deutlich früher von der Fahrzeugbewegung erreicht sein muss, als dies notwendig wäre, um die der Einschränkung zugrundeliegende Schutzfunktion zu erfüllen. Dieser Umstand kann bereits durch linienförmige Zugbeeinflussungssysteme wie LZB (in neueren Versionen) oder ETCS Level 2, ggf. bei Dunkelschaltung vorhandener ortsfester Signale geschickter gelöst werden (vgl. Kapitel 2) als in Bad Vilbel mit ortsfesten Signalen und PZB. Voraussetzung ist, dass diese Lösung im Stellwerk auch passend projektiert ist. Eine solche Optimierung der Einfahrgeschwindigkeiten sollte auch für die Neuentwicklung der Sicherungslogik im Rahmen dieser Arbeit im Fokus bleiben – gemäß der in Kapitel 3.1 beschriebenen Ziele möglichst ohne zusätzlichen Projektierungsaufwand.

Der Fall, in dem das zusätzliche Sperrsignal notwendig geworden ist, zeigt mehrere Probleme auf. Zum einen macht es deutlich, dass sinnvolle Änderungen, die durch das Betriebspersonal im laufenden Betrieb erkannt werden, – vermutlich kommt so etwas nicht nur im Stellbereich Bad Vilbel vor – nicht einfach behoben werden können. Stattdessen ist dafür ein aufwendiger Planungs- und Genehmigungsprozess erforderlich. Möglicherweise könnte durch bessere Simulationen des Betriebs vor Inbetriebnahme unter Einbezug von erfahrenem Betriebspersonal die Anzahl dieser Fälle reduziert werden. Ein vollständiges Ausbleiben solcher Fälle erscheint aber unwahrscheinlich, auch aufgrund der langen Lebenszeiten der Anlagen von mehr als dreißig Jahren und in diesem Zeitraum zwangsläufig auftretenden Änderungen der verkehrlichen Rahmenbedingungen bzw. des

Betriebsprogramms. Dies unterstützt das Ziel kürzerer Planungs- und Genehmigungszeiten und das möglichst einfache Ermöglichen flexibler Anpassungen an der Infrastruktur (vgl. Kapitel 3.1).

Zum anderen erscheint der Flankenschutz durch Sperrsignale generell hinterfragenswert zu sein. Im vorliegenden Fall beispielsweise besteht die Flankenschutzgefahr gar nicht, da die fragliche Gleisbeanspruchung durch einen Zug verursacht wird, der in die andere Richtung fährt. Allenfalls ein Rückwärtsrangieren unter Nichtbeachtung des bereits vorhandenen Sperrsignals am Hauptsignal N5 oder ein Abreißen eines Zugteils in einem Gleis mit Gefälle würde eine Flankenschutzgefahr darstellen. In diesen Fällen bliebe allerdings fraglich, ob das Sperrsignal sie überhaupt verhindern könnte, selbst, wenn es mit einem PZB-Magneten abgesichert wäre. Denn sowohl die rückwärts verkehrende Rangierfahrt, als auch der abgerissene Wagen wären nicht mit einem PZB-Magnet an erforderlicher Stelle ausgerüstet. Es handelt sich demnach auch um ein Verbesserungspotenzial in Bezug auf das Ziel einer möglichst geringen Anzahl von Infrastrukturelementen (Zieldimension *„geringer Hardwareeinsatz“*). Auch generell kann die Flankenschutzwirkung von Sperrsignalen in Frage gestellt werden, wie Unfälle im deutschen Eisenbahnnetz in den letzten Jahren zeigen (siehe Kapitel 5.4).

Auch der zweite oben beschriebene, flankenschutzbezogene Fall (mit der beabsichtigten Fahrt im Gegengleis) im Bahnhof Bad Vilbel zeigt, dass der Flankenschutz momentan nur unflexibel gehandhabt werden kann. So liegt die beabsichtigte Schutzwirkung im konkreten Fall darin, den Zug aus Richtung Frankfurter Berg (rechts im Gleisplan) vor einer Gefährdung von der Seite zu schützen. Dies könnte jedoch auch erreicht werden, wenn der aus Richtung der Gleisgruppe kommende Zug mit der nötigen Sicherheit garantieren würde, vor der relevanten Weiche zum Stehen zu kommen und ausgeschlossen werden kann, dass sich ein anderes, unkontrolliertes Fahrzeug der zu schützenden Zugfahrt nähern kann. Dies erscheint mit ETCS durchaus möglich, denn ETCS garantiert, dass ETCS-überwachte Fahrzeuge vor einem übertragenen Gefahrpunkt sicher zum Stehen kommen. Entscheidend ist dann, inwiefern garantiert werden kann, dass sich keine weiteren, unkontrollierten Fahrzeuge im Flankenschutzraum befinden.

3.4.4 Workshop mit der Fachabteilung Betrieb

Eine weitere Befragung von Experten der DB Netz AG fand im Rahmen eines Workshops mit Mitgliedern der Fachabteilung Betrieb statt. Die Fachabteilung ist unter anderem für die Aktualisierung der betrieblichen Regelwerke zuständig und betreut die Arbeit des operativen Betriebspersonals fachlich. Das betriebliche Regelwerk regelt die Handlungen des Betriebspersonals im Umgang mit der Sicherungstechnik und in der Kommunikation untereinander. In diesem Zusammenhang beschäftigt sich die Fachabteilung Bahnbetrieb auch mit betrieblichen Verbesserungspotenzialen in Zusammenhang mit dem Regelwerk oder der Leit- und Sicherungstechnik.

Im Workshop wurden verschiedene Szenarien diskutiert, die von der Fachabteilung Betrieb eingebracht wurden. Diese wurden anhand realer Gleispläne oder fiktiver Gleispläne aus dem Eisenbahnbetriebsfeld Darmstadt visualisiert.

Es konnten sieben Szenarien identifiziert werden, in denen von den Workshop-Teilnehmern realistische Verbesserungsmöglichkeiten durch eine optimierte Sicherungslogik innerhalb der infrastrukturseitigen Sicherungstechnik gesehen werden.

Szenario 1

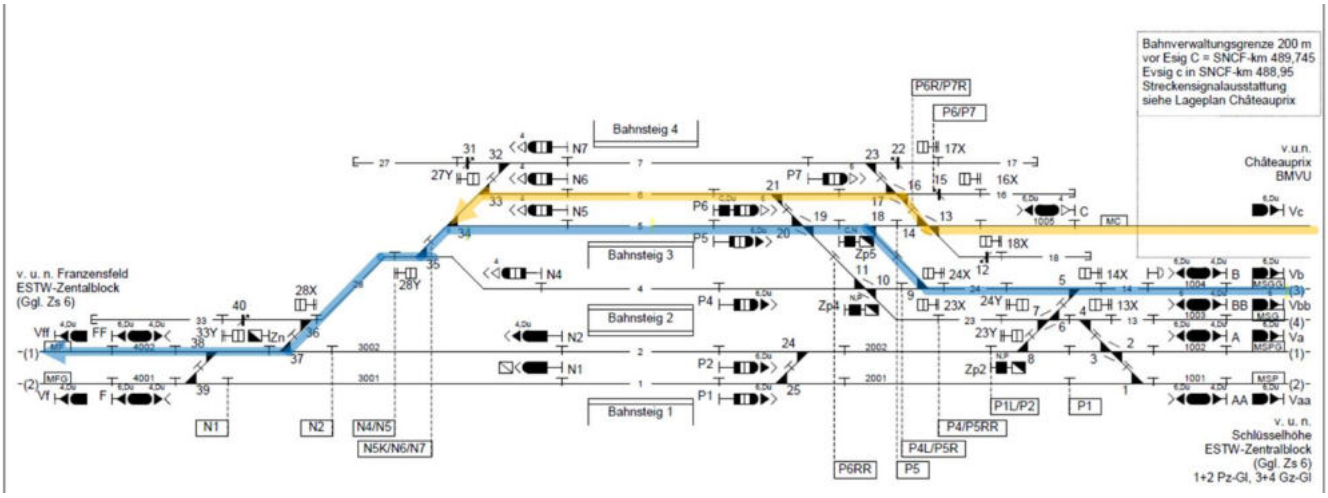


Abb. 24: Nutzenszenario 1 – flexible Gefahrpunktwahl
[Eigene Darstellung]

Szenario 1 skizziert die häufig vorkommende Überlappung eines Durchrutschweges einer Einfahrstraße mit einer anderen Fahrstraße (vgl. Abb. 24). Der Durchrutschweg (D-Weg) befindet sich hinter dem Fahrstraßenziel und stellt sicher, dass eine Fahrzeugbewegung mit ausreichender Sicherheit vor einem Gefahrpunkt zum Stehen kommt. Er darf sich daher nicht mit dem regulären Fahrweg einer anderen Fahrzeugbewegung überlappen.[11]

Um das skizzierte Problem zu lösen, können in modernen Stellwerken für Einfahrstraßen mehrere Durchrutschwege mit unterschiedlichen Längen projektiert werden. Kürzere Durchrutschwege bedingen bei punktuell überwachten Fahrzeugen, dass diese bereits am Beginn der Fahrstraße eine niedrigere Geschwindigkeit als bei längeren Durchrutschwegen erreicht haben müssen. Bei kontinuierlich überwachten Fahrzeugen mit Führerraumanzeige genügt es, wenn die Notbremskurve innerhalb des Durchrutschweges sicher zum Stillstand führt. Kürzere Durchrutschwege führen allerdings auch bei kontinuierlich überwachten Fahrzeugen zu einer geringeren Einfahrgeschwindigkeit oder einem früheren Bremseinsatzpunkt.

Bei komplexen Bahnhöfen müssten eine Vielzahl verschiedener Durchrutschwege und Gefahrpunkte projektiert werden, um alle Fahrmöglichkeiten mit der optimalen Geschwindigkeit fahren zu können. Jede dieser Fahrmöglichkeiten muss zugelassen und abnahmegeprüft werden. Aufgrund dieses Aufwandes werden nicht immer alle möglichen Durchrutschwege projektiert. Eine generische Logik könnte möglicherweise eine flexiblere Gefahr- und Durchrutschwegwahl ermöglichen, Projektierungs- und Zulassungsaufwand reduzieren sowie dadurch auch Kapazitätsvorteile realisieren.

[11] Überlappungen von zwei D-Wegen sind in Deutschland erlaubt, da die Wahrscheinlichkeit, dass beide D-Wege gleichzeitig in Anspruch genommen werden, als so gering angenommen wird, dass ausreichende Sicherheit als erreicht angesehen wird.

Szenario 2

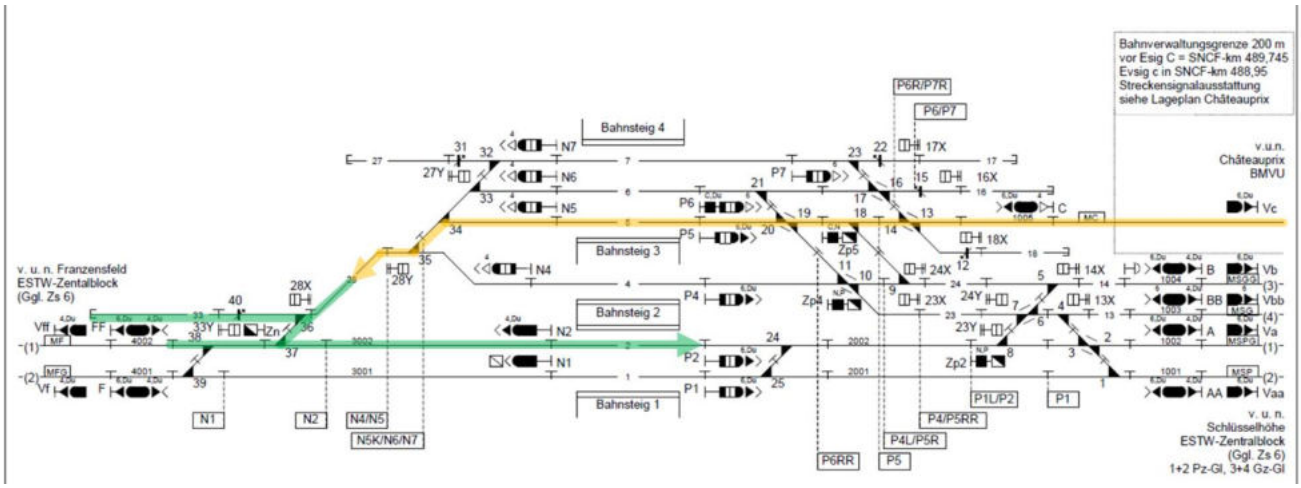


Abb. 25: Nutzenszenario 2 – flexible D-Weg-Länge
[Eigene Darstellung]

Das in Abb. 25 dargestellte Szenario 2 ähnelt Szenario 1, allerdings endet die für die einfahrende Zugfahrt (gelb) zur Verfügung stehende Infrastruktur nicht an einer Weiche oder einer Gleisfreimeldegrenze, sondern mitten auf dem Gleis. Hintergrund ist, dass aus entgegenkommender Richtung eine weitere Fahrzeugbewegung (grün) zugelassen werden soll, die aus einem Abstellgleis auf ein Hauptgleis rangieren möchte.

Idealerweise würde eine neue Sicherungslogik die Zuteilung der Infrastruktur genau so ermöglichen, dass beide Fahrzeugbewegungen möglichst wenig verlangsamt werden müssen (wobei hier durchaus definiert werden könnte, welche Fahrzeugbewegung gegebenenfalls stärker verlangsamt werden soll, wenn es zu Konflikten kommt). Hierfür wäre die Möglichkeit einer flexiblen Wahl der Länge des D-Weges optimal.

Szenario 3

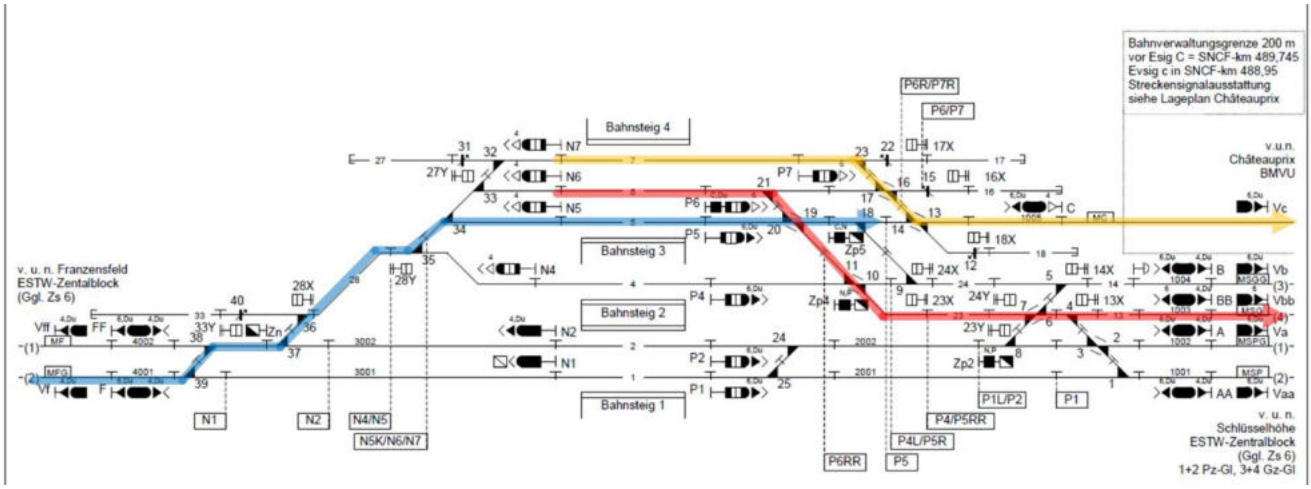


Abb. 26: Nutzenszenario 3 – dynamische Fahrstraßenziele
[Eigene Darstellung]

Szenario 3 ist ebenfalls eine Abwandlung von Szenario 1. Wie in Abb. 26 dargestellt ist, benötigen drei parallele Fahrzeugbewegungen Infrastrukturressourcen. Auch hierbei können bei heutigen Stellwerken wieder die Durchrutschwege zu theoretischen Ineffizienzen führen. So ist bei

gleichzeitiger Ausfahrt der gelben und roten Fahrzeugbewegung die Einfahrt der blauen Fahrzeugbewegung nicht möglich, da bereits kurz hinter dem Fahrstraßenziel der blauen Fahrzeugbewegung (an der Stelle des Signals P5) die Weiche 19/20 von der roten Fahrzeugbewegung beansprucht wird.

Ein Nutzenpotenzial einer neuen Sicherungslogik könnte entstehen, wenn die Sicherungslogik dynamisch das Fahrstraßenziel für die blaue Fahrzeugbewegung bzw. die Länge des D-Weges festlegen könnte und den D-Weg dann stückweise mit der Räumung der Fahrwegelemente hinter dem eigentlichen Zielpunkt nach hinten verschieben könnte. Ein ähnliches Prinzip ist in einigen hochbelasteten Knotenbahnhöfen bereits mit einer Vielzahl von Zugdeckungssignalen realisiert worden. Idealerweise könnte jedoch ein beliebiger Punkt auf dem Fahrweg als temporärer Zielpunkt bzw. Gefahrpunkt (Ende des D-Weges) dienen und die Fahrzeugbewegung würde eigenständig ihre Geschwindigkeit so wählen, dass sie bis zu diesem Gefahrpunkt zum Halten kommt.

Szenario 4

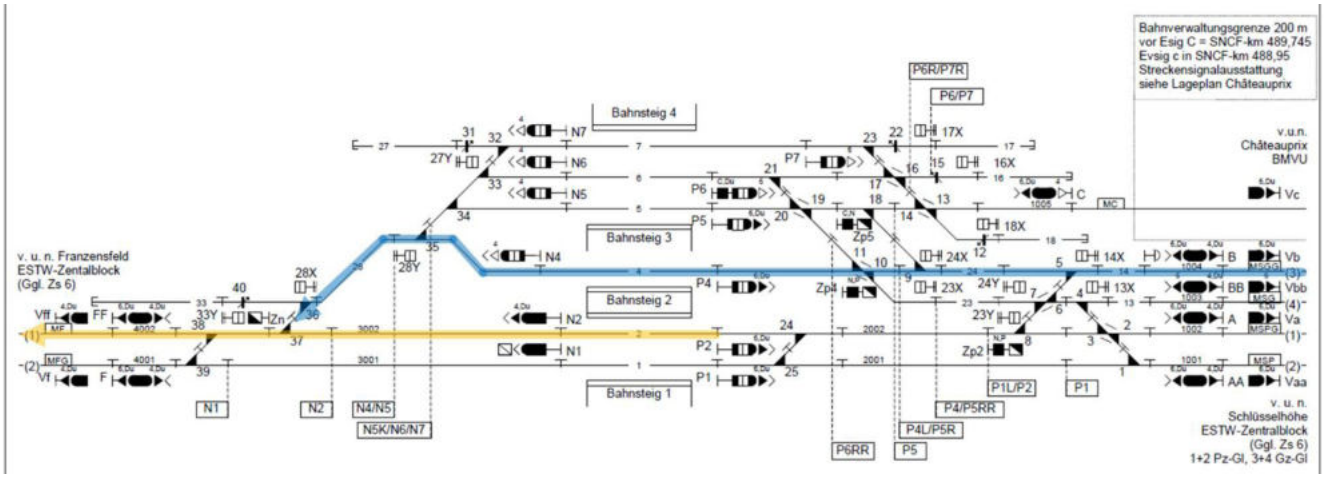


Abb. 27: Nutzenszenario 4 – vorzeitiges Vorrücken bis zum Gefahrpunkt
[Eigene Darstellung]

Szenario 4 betrachtet den entgegengesetzten Fall zu Szenario 3, die Ausfahrt von Eisenbahnfahrzeugen vom definierten Halteort aus auf die Strecke (vgl. Abb. 27). Heute ist die Ausfahrt in aller Regel (wenn nicht extra Zwischensignale projektiert sind) erst möglich, wenn die komplette Ausfahrstraße frei von anderen Fahrzeugen ist. Ein Nutzenpotenzial könnte realisiert werden, wenn die Ausfahrt bis zum aktuellen Gefahrpunkt bereits vorzeitig gestattet werden könnte, die dann regelmäßig verlängert wird, sobald der Gefahrpunkt sich verschiebt.

Szenario 5

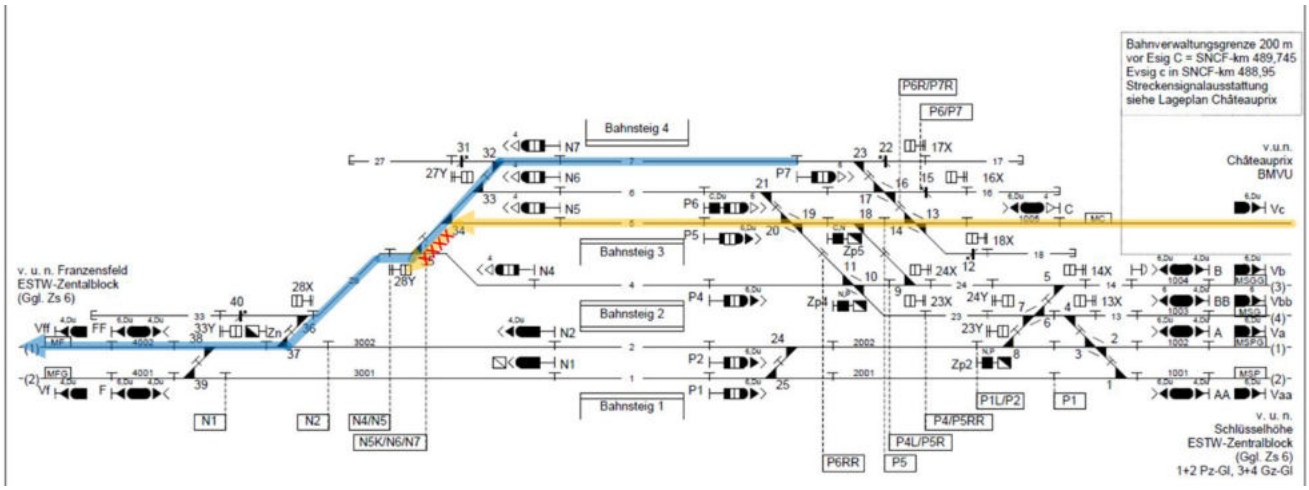


Abb. 28: Nutzenszenario 5: vorzeitige D-Weg-Rücknahme
[Eigene Darstellung]

Auch bei Szenario 5 findet eine Überlappung des Durchrutschweges der einfahrenden, in Abb. 28 gelb dargestellten Fahrzeugbewegung mit dem Fahrweg der ausfahrenden, blauen Fahrzeugbewegung statt. In diesem Szenario ist die Einfahrt der gelben Fahrzeugbewegung jedoch bereits weit fortgeschritten, so dass der Durchrutschweg nicht mehr benötigt wird.

Der Durchrutschweg wird bei modernen Stellwerken nach einer bestimmten Zeit wieder aufgelöst, in der garantiert werden kann, dass alle Fahrzeuge, welche die Einfahrstraße nutzen, entweder zum Stehen gekommen sind oder den Durchrutschweg in Anspruch genommen haben müssen. Verschiedene Fahrzeuge benötigen aufgrund ihrer unterschiedlichen Bremskraft unterschiedlich lange, um zum Stehen zu kommen. Daher könnte eine neue Sicherungslogik durch eine situationsabhängige Freigabe des Durchrutschweges eine frühere Nutzung desselben durch andere Fahrzeugbewegungen ermöglichen. Es sollte auch die Möglichkeit einer nachträglichen Verkürzung des Durchrutschweges in Betracht gezogen werden, wenn die einfahrende Fahrzeugbewegung eine bestimmte Geschwindigkeit unterschritten hat und somit nicht mehr den vollen Durchrutschweg benötigt.

Szenario 6

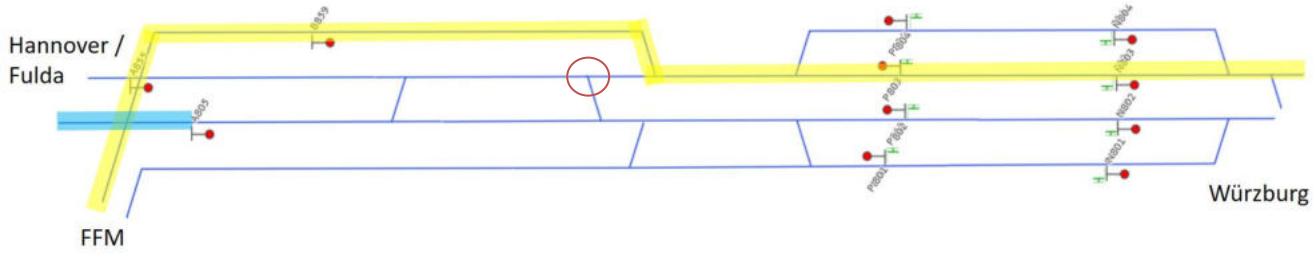


Abb. 29: Nutzenszenario 6: dynamische Gefährdungsabschätzung für Flankenfahrten
[Eigene Darstellung]

In der Abbildung zu Szenario 6 (Abb. 29) ist der Betriebsbahnhof Rohrbach abgebildet, in dem die Strecke aus Frankfurt auf die Schnellfahrstrecke Würzburg – Hannover trifft. Der Bahnhof veranschaulicht ein Problem von Fahrstraßenausschlüssen, die aufgrund von Flankenschutzmaßnahmen auftreten. Im vorliegenden Fall ist die rot umkreiste Weiche eine Zwieschutzweiche bei gleichzeitiger Einfahrt aus Richtung Fulda und Ausfahrt nach Frankfurt (jeweils

auf dem Regelgleis). Im beschriebenen Fall verhindert diese Zwieschutzeigenschaft die gleichzeitige Einstellung der beiden beschriebenen Fahrstraßen.

In anderen Fällen von Zwieschutzweichen wird der Flankenschutz häufig auf Signale übertragen. Dies ist jedoch im oben geschilderten Fall nicht möglich, da die durchgängigen Gleise der Schnellfahrstrecke mit mehr als 160 km/h befahren werden können und für diesen Fall ein physischer Flankenschutz durch Schutzweichen in der Eisenbahn-Bau- und Betriebsordnung (EBO) vorgeschrieben ist [EBO:2019-04-05 §14, Abs. 11].

Eine Verbesserung könnte möglich werden, wenn andere Möglichkeiten zur hinreichend sicheren Realisierung des Flankenschutzes von der Sicherungslogik in Betracht gezogen werden könnten. ETCS kann beispielsweise garantieren, dass ein vollüberwachter Zug bis zu einem Gefahrpunkt sicher zum Stehen gebracht wird und dort auch halten bleibt. So könnte er einen Flankenschutz darstellen, wenn sichergestellt ist, dass sich im Flankenschutzraum zwischen ihm und der zu schützenden Stelle keine weiteren Fahrzeuge befinden können. Weitere Potenziale durch eine neue Flankenschutzbetrachtung abweichend von definierten Flankenschutzelementen sind denkbar und sollten bei Überlegungen zu einer neuen Sicherungslogik berücksichtigt werden.

Szenario 7

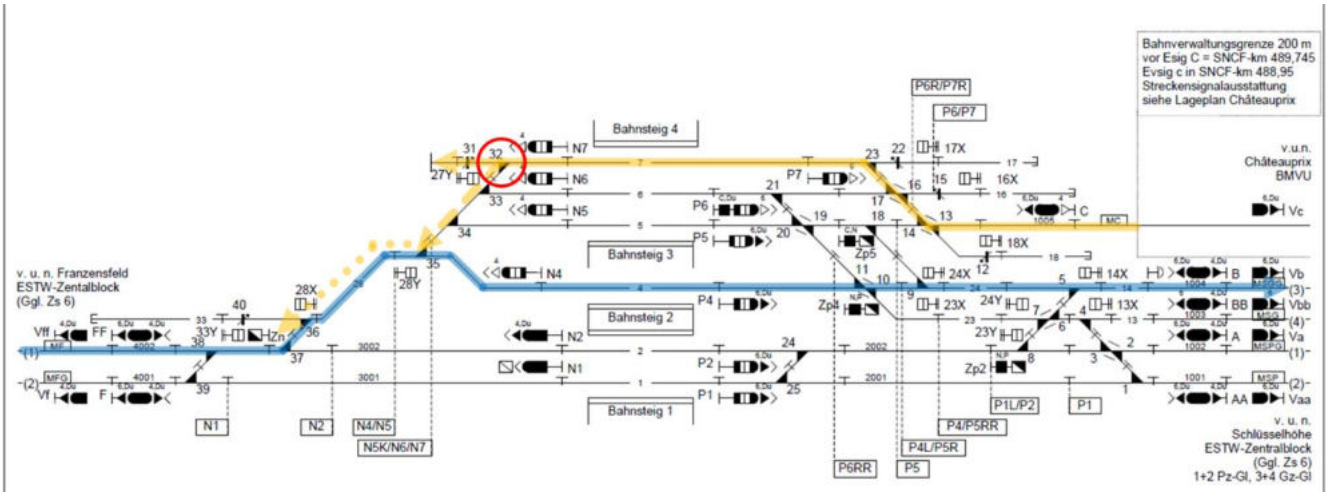


Abb. 30: Nutzenszenario 7: unnötige Flankenschutz-Einschränkungen vermeiden
[Eigene Darstellung]

In Szenario 7 muss bei konventioneller Technik Weiche 32 als Flankenschutzweiche für die blaue Zugfahrt in Rechtslage verschlossen werden. Hierdurch hat die Fahrstraße des gelben Zuges nur einen sehr kurzen D-Weg und kann dementsprechend nur langsam einfahren. Würde die Weiche in Linkslage liegen, wäre eine höhere Einfahrgeschwindigkeit möglich und der „D-Weg“ (Abstand bis zur SvL) könnte sogar noch verlängert werden, sobald der blaue Zug W35 passiert hat.

Die Sicherheit wäre bei Linkslage von W32 dennoch gewährleistet, solange der gelbe Zug vollüberwacht ist, da in diesem Fall ETCS garantiert, dass er rechtzeitig vor W35 zum Stehen kommt. Falls der gelbe Zug nicht vollüberwacht ist, könnte W32 weiterhin je nach Bedarf als Flankenschutzweiche verwendet werden.

Ein Kapazitätsnutzen könnte im Falle von Szenario 7 durch eine neue Sicherungslogik also erzielt werden, wenn der Flankenschutz auch auf den einfahrenden Zug verlagert werden könnte, sofern dieser vollüberwacht ist. Zudem könnte sich ein Nutzen durch die nachträgliche Verlängerung des D-Weges ergeben.

3.4.5 Benchmarking

Das prozessorientierte Benchmarking kann prinzipiell unternehmensintern und -extern erfolgen [vgl. hierzu Siebert et al. 2015]. Intern können dafür vergleichbare Prozesse im eigenen Unternehmen dienen, während extern klassischerweise zwischen konkurrenzbezogenem, branchenbezogenem und branchenunabhängigem Benchmarking unterschieden wird [ebd.].

Für das interne Benchmarking müsste es innerhalb des Eisenbahnsystems strukturell vergleichbare Prozesse zum untersuchten Prozess geben. Aufgrund der hohen Sicherheitsanforderungen, welche die Eigenschaften der Durchführung von Zugfahrten bestimmen, ist der betrachtetet Prozess jedoch weitgehend einzigartig.

Für das konkurrenzbezogene Benchmarking kommen die verschiedenen Eisenbahninfrastruktur-unternehmen der verschiedenen Länder in Betracht. Auf die dortigen sicherungstechnisch relevanten Teile der jeweiligen Produktionsprozesse sowie neue Ansätze wurde in Kapitel 2 bereits eingegangen. Für branchenbezogenes externes Benchmarking gilt die Erkenntnis zum internen Benchmarking, da es sich um deren Korrespondenz außerhalb des eigenen Eisenbahnsystems handelt.

Für das branchenunabhängige Benchmarking bieten sich Branchen mit ähnlichen Anforderungen an. Dies können andere sicherheitskritische Infrastrukturen, wie die Energieversorgung oder die Telekommunikationstechnologie sein, aber auch andere Verkehrsträger. Bei Letzteren vor allem die Luftfahrt, die ebenfalls sehr hohe Sicherheitsanforderungen hat, mehr als die Schifffahrt oder der Straßenverkehr.

Im Luftverkehr besteht anders als im Zugverkehr nicht die Möglichkeit, bei einem Problem in einen sicheren Zustand wie den Stillstand zu wechseln („Fail safe“). Aus diesem Grund wird im Luftverkehr ein „Fail operational“-Ansatz verfolgt, der mittels Redundanzen, einem sehr hohen Ausbildungsniveau und Notfallchecklisten kritische Ausfälle vermeidet. Ein Vorteil dieses Verfahrens im Vergleich zur Eisenbahnsicherungstechnik ist, dass der Betrieb auch im Störfall fortgeführt werden kann. Ein Nachteil sind die hohen Kosten durch die redundante Auslegung der Systeme und den umfangreichen Personaleinsatz.

Aus Sicht des Autors erscheint ein „Fail operational“-Ansatz auch für den Bahnverkehr insofern denkbar, dass bei klar eingrenzbaren Problemen nicht mehr zwangsläufig eine Störung zum Stillstand und einer manuellen Rückfallebene führen muss. Wenn die Einführung dieses Prinzips jedoch zu höheren Kosten führen würde, müsste eine genauere Abwägung der Vor- und Nachteile erfolgen. Da sich die Diskussion zu dieser Frage auf das Verhalten der Sicherungslogik in Rückfallebenen bezieht, sollte die Fragestellung im Kontext der Rückfallebenenbetrachtung näher untersucht werden.

3.5 globale Anforderungen an die neu zu schaffende Sicherungslogik

In diesem Kapitel werden aus den Zielen für die Komponente Sicherungslogik (Tab. 4 in Kapitel 3.2) Anforderungen an deren Funktionsweise und Gestaltung hergeleitet. Es wird die Bezeichnung „**globale Anforderungen**“ verwendet, da es für die Bearbeitung der einzelnen Arbeitsschritte weitere, spezifische Anforderungen geben kann, die dann in den jeweiligen Kapiteln zu diesen Arbeitsschritten beschrieben werden (in der Regel Unterkapitel x.2.1).

Zu jeder Zieldimension in Tab. 4 wurde mit Fachkollegen (Kollegen aus der Forschungsgruppe AG Signalling im Rahmen der Innovationsallianz zwischen Deutscher Bahn und TU Darmstadt unter Einbezug weiterer Fachkollegen der DB Netz AG sowie in Gesprächen auf Fachtagungen) ein Brainstorming mit der Fragestellung durchgeführt, welche Einflüsse sich auf den Zielerreichungsgrad der jeweiligen Zielfunktion auswirken und welche Anforderungen folglich zum Kontrollieren dieser

Einflüsse erforderlich sind. Ferner wurde die zuvor durchgeführte Nutzenpotenzialanalyse (Kapitel 3.4) zu Rate gezogen. Dabei wurde die Fragestellung untersucht, bei welcher dieser Zieldimensionen das Nutzenpotenzial ansetzt und welche Anforderungen erforderlich sind, um das identifizierte Verbesserungspotenzial bestmöglich erzielen zu können.

Außer der Kernanforderung der sicheren Logik, die in jedem Fall erfüllt sein muss, sind die Anforderungen dabei als Maximalforderungen an die zu entwickelnde Lösung für die neue Sicherungslogik zu verstehen. Im späteren Prozess dienen sie bei konkreten Designentscheidungen zur Logik als Abwägungsgrundlage, d. h. gegebenenfalls wird zwischen den einzelnen Anforderungen eine Abwägung getroffen. Eine Priorisierung der Zieldimensionen und der daraus folgenden Anforderungen erscheint global nicht sinnvoll zu sein, da sich aus den in Kapitel 3.1 identifizierten globalen Zielen keine eindeutige Rangfolge zwischen den Zielen herleiten lässt (mit Ausnahme der Kernanforderung Sicherheit) (vgl. Kapitel 3.1.1).

Tab. 7 gibt eine Übersicht über die globalen Anforderungen an die neue Sicherungslogik. Die fett markierten Wörter bilden die Kurzbezeichnung für die Identifikation der Anforderung in der folgenden Arbeit.

Tab. 7: Übersicht der globalen Anforderungen an die neue Sicherungslogik

Zieldimension	**Anforderung neue Sicherungslogik**
***Kernanforderung** sichere Logik*	*alle relevanten Schutzfunktionen (mind. zur Aufrechterhaltung des heutigen Sicherheitsniveaus) müssen abgedeckt werden*
geringer Planungs- und Genehmigungsaufwand	alle nicht sicherheitskritischen Funktionalitäten werden ausgegliedert (**schlanke** (Sicherungs-)**Logik**)
	sicherheitskritische Funktionalitäten werden auf ihren **sicherungskritischen Kern** beschränkt
	Funktionalitäten werden so **generisch** wie möglich beschreiben
	die Logik wird **topologieunabhängig** gestaltet
	Infrastrukturelemente können je nach Bedarf in der Logik hinzugefügt oder entfernt werden, ohne dass die gesamte Logik neu definiert werden muss (**flexible Infrastrukturzuordnung**)
Interoperabilität	die Logik verwendet soweit möglich generische **Standardschnittstellen** zu benachbarten Systemen
geringer Hardwareeinsatz	die Logik ist **nur** mit den **erforderliche**n **Infrastrukturelementen** verknüpft; jedes Infrastrukturelement ist auf seine Notwendigkeit hin zu überprüfen (z. B. Signale, Gleisfreimeldeeinrichtungen, zusätzliche Flankenschutzelemente, ggf. auch zentrale Überwachungssysteme)
geringer Arbeitskräfteeinsatz	die Logik arbeitet weitestgehend **automatisiert**
	die Zuständigkeitsbereiche sind während der Laufzeit flexibel zuschneidbar (**flexible Kontrollbereiche**)
Energieeffizienz	**unnötige Bremsvorgänge** sind zu **verhindern** (sofern dies durch die Sicherungslogik beeinflusst werden kann)
	der Fahrzeugbewegung wird **möglichst viel Freiraum** zum energieoptimalen Ausfahren ihrer Fahrerlaubnis gelassen
hohe Kapazität	die physisch (inkl. Sicherheitsmarge) **maximal mögliche Geschwindigkeit** wird nicht eingeschränkt
	Prüfanfragen werden schnell verarbeitet (**geringe Latenz**)

	es wird den Fahrzeugbewegungen nur so viel Infrastruktur zugewiesen, wie zur Aufrechterhaltung der Sicherheit unbedingt erforderlich ist (**minimale Infrastrukturbeanspruchung**)
	an Fahrzeugbewegungen zugewiesene Infrastruktur wird von diesen frühestmöglich wieder freigegeben (**frühestmögliche Infrastrukturfreigabe**)
hohe Robustheit	Rückfallebenen werden möglichst in die Logik integriert (**Rückfallebenenintegration**)
	Änderung bereits erteilter Aufträge sind solange wie möglich durch Regelhandlung zu ermöglichen (**Regelhandlungsgebot**)
	den Fahrzeugen wird **möglichst viel Freiraum** zum Reagieren auf kleinere Abweichungen gelassen
	Ausfälle von Teilsystemen führen nicht zur Nichtbenutzbarkeit des gesamten Systems (**Resilienz**)
	Funktionseinschränkungen (z. B. durch Wartungsarbeiten) können so kleinteilig wie möglich definiert werden (**modulare Außerbetriebnahme**)
lange Nutzungszeiten	die **Migrationsfähigkeit** zur bestehenden Technik wird gewährleistet
	zu erwartende neue Entwicklungen werden mitgedacht (**Zukunftsfähigkeit**)
[ohne]	alle sicherheitsrelevanten Aktivitäten werden **protokolliert**

Aus der *Kernanforderung* der sicheren Logik ergibt sich die Anforderung, dass alle relevanten Schutzfunktionen abgedeckt sein müssen, um das vorgegebene Maß an Sicherheit (SIL 4) zu erreichen. Relevant sind die Schutzfunktionen, wenn sie durch die Sicherungslogik beeinflusst werden können. Mit der genauen Abgrenzung dieser Funktionen beschäftigen sich die Hauptkapitel 5 und 6.

Aus der Zieldimension des *geringen Planungs- und Genehmigungsaufwands* folgt vor allem die Anforderung nach einer möglichst schlanken Logik, die sich auf die Kernfunktionalitäten, dem Entscheiden zwischen Zulassung und Zurückweisung einer Anfrage aus dem nicht sicherheitskritischen Bereich, beschränkt. Diese Anforderung ist auch in EN 50128 festgehalten. Demnach ist eine möglichst geringe Komplexität der sicherheitsrelevanten Software [DIN EN 50128:2011] anzustreben, damit die Sicherheitsnachweisführung nachvollziehbar bleibt. Zudem ist die generische Beschreibung zentral.

Aus der Anforderung der generischen Beschreibung folgt auch, dass die Logik unabhängig von konkreten Ausprägungen der Infrastruktur und der Fahrzeuge sein soll. Die smartLogic wird daher topologieunabhängig geplant. Der Spurplan bzw. eine Liste zulässiger Fahrwege und deren Geschwindigkeit, wie in vielen heutigen ESTW, sollte also ähnlich wie in Spurplanstellwerken nicht mehr direkter Bestandteil der Sicherungslogik sein. Stattdessen greift die Sicherungslogik für Funktionen wie die Zulässigkeitsprüfung einer MA auf den Spurplan aus einer signaltechnisch sicheren externen Quelle zu. Damit der Spurplan von der Sicherungslogik eingelesen werden kann, muss er in einem standardisierten Datenformat vorliegen. Dies gilt auch für weitere Schnittstellen und Daten, die von der Sicherungslogik verarbeitet werden müssen (z. B. Fahrzeugdaten).

Die Zieldimension des *geringen Hardwareeinsatzes* steht bereits für sich selbst. Sie unterstützt die Forderung nach Ablösung bzw. Verringerung von Infrastrukturelementen wie festen Signalen, infrastrukturanfälliger Gleisfreimeldesysteme und rein logikbedingter Schutzelemente.

Die Zieldimension „*geringer Arbeitskräfteeinsatz*“, vor allem aufgrund des geschilderten Fachkräftemangels, führt zu der Anforderung nach einem hohen Grad der Automatisierung, aber vor allem auch nach der möglichst gleichmäßigen Auslastung der Arbeitskräfte durch an das Verkehrsaufkommen angepasste Zuständigkeitsbereiche.

Die Anforderungen aus der Zieldimension „*Energieeffizienz*“ sind eng mit den Anforderungen aus dem Bereich der Zieldimension *Kapazität* verknüpft. Zum einen unterstützen sie sich gegenseitig, wenn es beispielsweise um das Vermeiden unnötiger Bremsvorgänge geht, zum anderen sind sie aber auch gegensätzlich, wenn es zum Beispiel um das sanfte Beschleunigen und Ausrollen lassen im Gegensatz zum straffen Beschleunigen und Bremsen geht. Da die Abwägung in solchen Zielkonflikten jedoch eine betriebliche Aufgabe ist und keine Sicherheitsimplikationen hat, soll die Sicherungslogik nur einen möglichst großen Spielraum für die Energieoptimierung eröffnen, indem sie wieder analog zu den Anforderungen aus der Zieldimension Kapazität die sicherungstechnisch notwendigen Einschränkungen auf ein Minimum reduziert.

Um einen solchen großen Entscheidungsspielraum zu ermöglichen, ist es aus Sicht der *Kapazität* vor allem entscheidend, dass für jede Fahrzeugbewegung nur die Infrastrukturressourcen exklusiv zugewiesen werden, die für die sichere Abwicklung der Fahrzeugbewegung erforderlich sind und dass diese Infrastrukturressourcen frühestmöglich für die Nutzung durch andere Fahrten wieder freigegeben werden. Hieraus folgt ebenfalls, dass die Sicherungslogik Fahrerlaubnisse von nahezu jedem Punkt zu jedem anderen Punkt auf der Infrastruktur zulassen muss und nicht mehr nur von einer fest vorgegebenen Menge an Punkten (Signalstandorten). Außerdem sollen Änderungen der Zuweisungen so lange wie möglich bei normaler Funktionsweise der Sicherungslogik durchführbar sein.

Die letztgenannte Anforderung folgt auch aus der Zieldimension *Robustheit*, denn es kann immer auch zu kurzfristigen Abweichungen vom (ggf. erst kurz zuvor festgelegten) Plan kommen (z. B. wenn das Fahrverhalten durch externe Einflüsse anders als geplant verläuft oder sich ein Fahrplanhalt durch Reisendeneinfluss unerwartet verlängert). Deswegen sollen grundsätzlich Festlegungen, die nicht ohne Weiteres rückgängig gemacht werden können, erst so spät wie nötig erfolgen. Weiterhin sollen Funktionen konsequent genutzt werden, welche die Rücknahme von Entscheidungen der Sicherungslogik aus betrieblichen Gründen im Falle geänderter äußerer Rahmenbedingung ermöglichen, z. B. die Rückgabe einer Fahrerlaubnis durch die Fahrzeugbewegung bei ETCS.

Weitere wichtige Anforderungen im Bereich der Zieldimension *Robustheit* zielen darauf ab, dass die Logik auch bei suboptimalen Bedingungen noch zuverlässig arbeitet. Dies kann erreicht werden, in dem Rückfallebenen für diese suboptimalen Bedingungen mit daraus resultierenden Einschränkungen (z. B. einer niedrigeren Geschwindigkeit) bereits in die Logik integriert werden. Dies würde auch dem „Fail Operational“-Ansatz im Luftverkehr (vgl. Kapitel 3.4.5) entsprechen, sollte aber nicht zu deutlich erhöhten Kosten führen. Idealerweise können für jede Sicherheitsanforderung mehrere Rückfallebenen definiert werden. ETCS bietet hierzu nicht nur niedrigere Geschwindigkeiten, sondern zum Beispiel auch die Möglichkeit ein Mode Profile mit abgeschwächten Fahrtmodi zu übertragen und jeweils durch den Tf quittieren zu lassen.

Aus der Zieldimension der *langen Nutzungszeit* lassen sich die Anforderungen Migrationsfähigkeit und Zukunftsfähigkeit herleiten. Migrationsfähigkeit bedeutet, dass die neue Logik mit verschiedenen technischen Versionen der einzelnen Umsysteme interagieren kann, so dass nicht die komplette Leit- und Sicherungstechnik auf einmal erneuert werden muss, da eine solche Erneuerung u. a. aufgrund von hohen Kosten nicht umsetzbar wäre. Die Anforderung der Migrationsfähigkeit wird auch von der RCA (vgl. Kapitel 2.4.2) und vom interviewten Experten der DB Netz AG (vgl. Kapitel 3.4.2) als

Wichtig erachtet. Die Anforderung der Zukunftsfähigkeit bezieht sich dagegen auf die Möglichkeit der Einbindung zukünftiger funktionaler Anforderungen, z. B. in Folge neuer Sicherheitsvorgaben, und möglicherweise in Zukunft zur Verfügung stehender neuer Technologien bei den Umsystemen der smartLogic.

Außerdem ist die rechtliche Anforderung der *Protokollierungspflicht* aller sicherheitsrelevanter Aktivitäten des zu entwickelnden Systems, die sich nicht direkt aus der Zielsetzung herleitet, aber juristisch vorgegeben ist, zu beachten.

Auf Basis dieser Anforderungen, insbesondere der dynamischen Fahrwegzuweisung und -rückgabe wurde die bereits in der Einleitung dieser Arbeit eingeführte Bezeichnung „smartLogic“ für die zu entwickelnde, neue Sicherungslogik gewählt.

3.6 grundsätzliche Methode und Vorgehensweise für die Entwicklung der neuen Sicherungslogik

Nachdem das Ziel der Arbeit und die Anforderungen an die Lösungen in den vorangegangenen Kapiteln dieses Hauptkapitels der Arbeit hergeleitet und beschrieben wurden, kann nun die grundsätzliche Methode für die Entwicklung der neuen Sicherungslogik festgelegt und daraus die grundsätzliche Vorgehensweise für diese Arbeit hergeleitet werden. Die Beschränkung auf die *grundsätzliche* Methode und Vorgehensweise erfolgt, da die Feinheiten zu den einzelnen Arbeitsschritten jeweils im Unterkapitel „Methode und Vorgehensweise“ der einzelnen Hauptkapitel zu den jeweiligen Arbeitsschritten hergeleitet werden.

Zunächst werden in Kapitel 3.6.1 geeignete Kriterien für die Auswahl der grundsätzlichen Methode und Vorgehensweise identifiziert. Vorgabe für die Arbeit ist, dass die neue Sicherungslogik auf der Grünen Wiese erarbeitet werden soll (vgl. Kapitel 1.1). Kapitel 3.6.2 analysiert deshalb, was diese Vorgabe für die Entwicklungsmethode in dieser Arbeit bedeutet. Als Teil der infrastrukturseitigen Sicherungstechnik ist die Sicherungslogik ein sicherheitskritisches System. Deshalb sind bei der Entwicklung Vorgaben aus Normen bzgl. des Entwicklungsprozesses zu beachten. Da es sich bei der vorliegenden Arbeit jedoch um eine wissenschaftliche Arbeit und nicht die Entwicklung eines Produktivsystems handelt, soll dennoch in Kapitel 3.6.3 zwischen verschiedenen grundsätzlichen Entwicklungsmethoden abgewogen und eine Entwicklungsmethode für die Arbeit festgelegt werden. Auf Basis der festgelegten Entwicklungsmethode können die einzelnen Arbeitsschritte der grundsätzlichen Vorgehensweise bestimmt (Kapitel 3.6.4) und die Reihenfolge dieser Arbeitsschritte hergeleitet werden (Kapitel 3.6.5). Abschließend erfolgt in Kapitel 3.6.6 eine Zusammenfassung der grundsätzlichen Vorgehensweise.

3.6.1 Kriterien

Zur Auswahl der geeignetsten Entwicklungsmethode und der daraus folgenden Vorgehensweise sind Kriterien zu definieren. Diese beruhen zum einen auf den definierten Zielen für die neue Sicherungslogik und den daraus hergeleiteten Anforderungen und zum anderen auf den äußeren Rahmenbedingungen der vorliegenden Dissertation und dem wissenschaftlichen Anspruch der Arbeit. Als Grundlage dienen die grundlegenden Projekterfolgsparameter Qualität, Kosten und Zeit.

Kriterien auf Basis der Zielsetzung:

- Methode und Vorgehensweise müssen sicherstellen, dass alle relevanten Schutzfunktionen durch die Sicherungslogik berücksichtigt werden, um das erforderliche Maß an Sicherheit (SIL 4) zu erreichen.

- Methode und Vorgehensweise müssen sicherstellen, dass mit hoher Wahrscheinlichkeit diejenigen Lösungen für konkrete Umsetzungsfragen identifiziert werden, welche die Ziele gemäß Kapitel 3.2 am besten erreichen oder zumindest eine qualifizierte Abwägung zwischen den möglichen Lösungen anhand der Ziele erlauben.
- Methode und Vorgehensweise sollen eine schnelle Nutzung der Ergebnisse bei der Entwicklung von Produktivsystemen ermöglichen.
- Die Arbeit soll durch einen neuen Ansatz einen Beitrag zur Debatte leisten.

Kriterien auf Basis der äußeren Rahmenbedingungen:

- Die Arbeit muss in der vorhandenen Zeit durchführbar sein.
- Die Arbeit muss im Wesentlichen durch den Autor alleine durchführbar sein (mit Unterstützung durch studentische Arbeiten und bei bestimmten Hilfstätigkeiten durch studentische Mitarbeiter und bei Implementierungsfragen z. B. durch einen Fachinformatiker).
- Methode und Vorgehensweise müssen das systematische Nachvollziehen aller getroffenen Entscheidungen ermöglichen.

3.6.2 Umsetzung des „Grüne Wiese"-Ansatzes

Ausgangspunkt für die Entwicklung der neuen Sicherungslogik kann entweder eine bestehende Logik sein, die weiterentwickelt wird, oder es handelt sich um eine Neuentwicklung auf Basis der hergeleiteten Ziele der Logik und somit um einen "Grüne Wiese"-Ansatz (vgl. hierzu [Lindner & Becker 2015, 312f]). Zwischen diesen beiden Extremen sind auch Abstufungen möglich.

Anspruch an diese Dissertation ist es, einen Ansatz auf der "Grünen Wiese" zu entwickeln (vgl. Kapitel 1.1), um eine Sicherungslogik entwerfen zu können, die möglichst optimal die in Kapitel 3.2 identifizierten Ziele erfüllt, ohne dass der Blick durch bestehende Lösungen verstellt wird. Ein solcher „Grüne Wiese"-Ansatz erscheint auch sinnvoll, da die Möglichkeit einer neuen Systemarchitektur nicht ausgeschlossen werden sollte (und auch in anderen Projekten bzw. Programmen zur Weiterentwicklung der infrastrukturseitigen Sicherungstechnik angedacht ist (vgl. RCA, Kapitel 2.4)) sowie eine Vielzahl von zusätzlich verfügbaren Informationen (z. B. durch ETCS, bessere Ortung und zusätzliche Sensoren) grundsätzliche Prinzipien bestehender Sicherungslogiken, wie die feste Blockteilung, in Frage stellen.

Dennoch sollte auch berücksichtigt werden, dass die bestehenden Sicherungslogiken auf Erfahrungen beruhen, die aus zahlreichen Betriebsjahren und vor allem Unfällen und gefährlichen Ereignissen gewonnen wurden, deren Wiederholung keine Option ist. Aus diesem Grund bietet es sich an zweistufig vorzugehen. Um den unvoreingenommenen Blick zu wahren, erfolgt zunächst die Entwicklung der neuen Sicherungslogik zur Ausschöpfung der größtmöglichen Effizienzgewinne auf der "Grünen Wiese" mit Hilfe einer systematischen Methode. Anschließend erfolgt jedoch eine Sichtung der bestehenden, bewährten Technik zur Vollständigkeitskontrolle, insbesondere der Sicherheitsanforderungen (vgl. erstes Kriterium auf Basis der Zielsetzung in Kapitel 3.6.1), sowie um eine schnelle Umsetzung der Ergebnisse bei der Entwicklung von Produktivsystemen zu ermöglichen (vorletztes Kriterium auf Basis der Zielsetzung).

3.6.3 V-Modell oder agile Methode?

In Kapitel 2.6.1 wurden das V-Modell, die agile Methode und mögliche Hybridformen für den Entwicklungsprozess sicherheitskritischer Systeme wie der Sicherungslogik vorgestellt. Nachfolgend soll hergeleitet werden, welche dieser Methoden in der weiteren Arbeit verwendet werden soll.

Für eine Inbetriebnahme eines späteren Produktivsystems ist eine Zulassung erforderlich. Hierzu müsste der Entwicklungsprozess den definierten Grundsätzen der dem V-Modell zugrundeliegenden Euronormen folgen. Bei der vorliegenden Arbeit handelt es sich allerdings um eine wissenschaftliche Arbeit, in deren Rahmen zwar Erkenntnisse für die Entwicklung eines Produktivsystems gewonnen werden sollen, aber nicht direkt ein Produktivsystem entwickelt wird. Aus diesem Grund muss der Entwicklungsprozess nicht streng den Normen folgen. Eine Entwicklung streng gemäß der Norm wäre auch durch eine einzelne Person, sowohl aus Zeitgründen als auch aufgrund der vorgeschriebenen Kontrollmechanismen durch weitere Fachexperten, gar nicht möglich (vgl. Kriterien auf Basis der äußeren Rahmenbedingungen in Kapitel 3.6.1 und inhaltliche Abgrenzungen in Kapitel 3.3).

Für eine wissenschaftliche Arbeit bietet es sich grundsätzlich an, eine agile Methode zu wählen, denn diese ermöglicht es, besser als das relativ statische V-Modell dynamisch auf neue Erkenntnisse zu reagieren. Das V-Modell scheint auch in Hinblick auf die in Kapitel 3.6.1 definierten Kriterien nicht optimal zu sein. Das zeigt sich besonders bei den Kriterien auf Basis der äußeren Rahmenbedingungen. Auch in Bezug auf das Kriterium der möglichst optimalen Zielerfüllung ist das V-Modell gegenüber der agilen Methode in Bezug auf das Ziel einer schlanken Sicherungslogik nicht zu bevorzugen.

Gleichwohl wurde in Kapitel 2.6.1 festgestellt, dass auch eine rein agile Methode nicht nur Vorteile hat. Demnach können größere Umplanungen notwendig werden, wenn einige der Schutzfunktionen erst nachträglich bei der Entwicklung der Logik berücksichtigt werden. Zudem kann es aufgrund des Kriterium der vollständigen Berücksichtigung aller relevanten Schutzfunktionen kein Zwischenprodukt geben, welches nicht alle Schutzfunktionen berücksichtigt. Deshalb könnte die Entwicklung eines Produktivsystems nach der Durchführung eines agilen Forschungsprojektes erschwert werden, wodurch die Erfüllung des Kritieriums der schnelle Nutzbarkeit der Ergebnisse beeinträchtigt wird.

Die hybride Methode nimmt in der Umsetzung des Smart Engineerings genau die problematischen Eigenschaften von V-Modell und agiler Methode in den Blick und entschärft die Nachteile dieser beiden Entwicklungsmethoden durch eine Kombination der beiden extremen Methoden. So wird durch das ausführliche Requirements Engineering im Rahmen einer gründlichen Systemdefinition dem Problem der Sicherstellung der vollständigen Umsetzung der relevanten Schutzfunktionen begegnet. Eine iterative Logikentwicklung im Rahmen der modellbasierten Softwareentwicklung nutzt dagegen den Vorteil der flexiblen agilen Methode. Die hybride Methode scheint daher für die vorliegende Arbeit am geeignetsten zu sein.

Für die Umsetzung im Rahmen der neuen Sicherungslogik ist zudem darauf zu achten, beim ausführlichen Requirements Engineering zwar die später noch benötigten oder möglicherweise dazukommenden funktionalen Anforderungen im Blickfeld zu haben, aber bei der Modellierung zu priorisieren, um die Zeit-Kriterien einhalten zu können. Diese Priorisierung kann iterativ unter Berücksichtigung der Interessen späterer Stakeholder der Sicherungslogik erfolgen. Mit dem Eisenbahnbetriebsfeld Darmstadt bietet sich zudem eine gute Möglichkeit, einen Demonstrator im Rahmen der Arbeit umzusetzen, wie im Ansatz des „Smart Engineering“ empfohlen.

3.6.4 Arbeitsschritte der grundsätzlichen Vorgehensweise

Auf Basis der gewählten Methode kann die grundsätzliche Vorgehensweise für diese Arbeit hergeleitet werden. Dafür muss Klarheit darüber bestehen, welche **Arbeitsschritte** in der Vorgehensweise enthalten sein müssen. Da die grundsätzliche Vorgehensweise gemäß des in Kapitel 2.6.1 vorgestellten hybriden Ansatzes des „Smart Engineerings“ den Schritten des V-Modells folgt, sind die wesentlichen Arbeitsschritte dadurch bereits vorgegeben.

Der erste Schritt ist die Konzepterstellung. Weiterhin sind eine Systemumgebung zu definieren, auf Basis einer Risikoanalyse Anforderungen an die Sicherungslogik festzulegen und auf die Systemkomponenten aufzuteilen und natürlich die spätere modellbasierte Entwicklung der eigentlichen Logik durchzuführen. Hierfür ist zudem ein wohldefiniertes Datenmodell erforderlich. Aus Gründen der Übersichtlichkeit wird dies als eigenständiger potenzieller Arbeitsschritt betrachtet (vergleiche unten).

Aufgrund der in Kapitel 3.6.1 definierten Kriterien, wonach Methode und Vorgehensweise eine schnelle Nutzung der Ergebnisse der Arbeit bei der Entwicklung von Produktivsystemen und einen wissenschaftlichen Beitrag zur Debatte ermöglichen sollen, erscheint es sinnvoll zur Veranschaulichung der Funktionsweise der neuen Sicherungslogik zusätzlich einen Demonstrator zu entwickeln.

Da die Umsetzung der Schritte des V-Modells aus den bereits in Kapitel 3.6.3 erläuterten Gründen nicht immer genau den genormten Anforderungen entspricht und der Zuschnitt der Arbeitsschritte für diese wissenschaftliche Arbeit zum Teil etwas abweichend sinnvoller erscheint (vgl. dazu die Erläuterungen bei den jeweiligen Schritten unten), werden zum Teil im weiteren Verlauf der Arbeit etwas abweichende Begrifflichkeiten verwendet. Die folgenden Arbeitsschritte sind daher mit der ursprünglichen Bezeichnung aus dem V-Modell und ggf. der im weiteren Verlauf der Arbeit abweichenden Bezeichnung überschrieben.

Konzeptphase

Zu Beginn des V-Modells steht die Konzeptphase. In dieser Phase ist das Vorhaben mit seiner Zielsetzung zu erläutern und daraus die Aufgabenstellung herzuleiten. Diese Inhalte finden sich im vorliegenden 3. Hauptkapitel dieser Arbeit.

Systemdefinition, System(umfeld)analyse

Wie in Kapitel 3.6.3 bereits erläutert, spielt die Verwendung einer klar definierten Systemumgebung eine wichtige Rolle. Hierzu ist an dieser Stelle zu klären, ob die Systemarchitektur des Gesamtsystems der digitalen Leit- und Sicherungstechnik, in das sich die Sicherungslogik einfügt, bereits aus einer in Kapitel 2 vorgestellten Architektur übernommen werden kann. Ein Kriterium auf Basis der Zielsetzung fordert bereits konkret: “Die neue Sicherungslogik soll so entwickelt werden, dass sie sich in die zukünftige Architektur der digitalen Leit- und Sicherungstechnik einfügen kann.“ (vgl. Kapitel 3.6.1).

Hierfür bietet sich aufgrund ihrer breiten internationalen Abstimmung vor allem die neue Reference CCS Architecture (RCA) als Grundlage an, die in Kapitel 2.4 vorgestellt wurde. Weitere so fein detaillierte international abgestimmte Architekturen sind gegenwärtig nicht bekannt. Die RCA definiert bereits die Aufgabe der Komponente Sicherungslogik und die Schnittstellen zu den benachbarten Systemen. Allerdings befindet sich die RCA zum Zeitpunkt der Erstellung dieser Arbeit noch in der Entwicklung und somit bestehen noch einige Definitionslücken. Zudem wurden im Rahmen der Bearbeitung dieser Arbeit bereits wesentlich vor Erscheinen der ersten Veröffentlichungen zur RCA Überlegungen zur zukünftigen Architektur der digitalen Leit- und

Sicherungstechnik in Hinblick auf die Rolle der Sicherungslogik darin angestellt und auch veröffentlicht, so dass eine Besprechung in einem eigenen Arbeitsschritt angemessen erscheint. In diesem Arbeitsschritt kann dann auch eine Abwägung zu weiteren bekannten bzw. möglichen Architekturen vorgenommen werden.

Risikoanalyse, Gefährdungsanalyse

In dieser Arbeit kann aufgrund des Umfangs keine vollständige Risikoanalyse gemäß den Vorgaben der Normen mit einem vollständigen RAMS-Prozess und der Definition der tolerierbaren Gefährdungsraten (engl. „Tolerable Hazard Rates“ THR) erfolgen. Eine Beschränkung auf die bekannten Hauptgefährdungen Entgleisung und Kollision mit anderen Schienenfahrzeugen (vgl. Kapitel 2.1.1) erscheint jedoch zu eng, da in den modernsten heutigen Stellwerken bereits wesentlich mehr potenziellen Gefährdungen begegnet werden kann (Anforderung der Migrationsfähigkeit) und davon auszugehen ist, dass zukünftig zusätzliche funktionale Sicherheitsanforderungen zur Vermeidung weiterer Gefährdungen hinzukommen könnten (Anforderung der Zukunftsfähigkeit). Zudem entspricht die Beschränkung auf die von heutiger Stellwerkstechnik beherrschten Gefährdungen nicht dem „Grüne Wiese“-Ansatz der Arbeit. Deshalb ist in der Vorgehensweise zumindest eine (im Vergleich zur Risikoanalyse vereinfachte) Gefährdungsanalyse[12] als Grundlage für die Definition der funktionalen Sicherheitsanforderungen an die smartLogic zu berücksichtigen.

Festlegen der Systemanforderungen, Funktionsanalyse

Dieser wichtige Arbeitsschritt bildet die Basis für das spätere Design und die Funktionsweise der Sicherungslogik im späteren Arbeitsschritt der modellbasierten Entwicklung. Im Ansatz des „Smart Engineerings“ entspricht dies dem (initialen) „Requirements Engineering“. Die Systemanforderungen setzen sich aus rein betrieblichen funktionalen Anforderungen und den funktionalen Sicherheitsanforderungen, die sich aus der Sicherheitsverpflichtung ergeben, zusammen. Erstere leiten sich aus den betrieblichen Funktionen der Sicherungslogik her (z. B. die Möglichkeit eine Weiche umzustellen) und Letztere aus der Gefährdungsanalyse.

Die funktionalen Anforderungen münden in Funktionen der zu erstellenden Sicherungslogik. Aufgrund der Zielsetzung der möglichst generischen Logik (vgl. Kapitel 3.2) ist die Zahl der aus den Anforderungen hergeleiteten Funktionen möglichst gering zu halten. Um dies zu erreichen ist eine Kategorisierung und anschließende Zusammenfassung zu generischen Funktionen eine mögliche Lösung. Wie in Kapitel 3.6.3 erläutert, ist außerdem zu erwarten, dass eine Priorisierung erfolgen muss. Daher wird der Schritt „Festlegen der Systemanforderungen“ aus dem V-Modell in dieser Arbeit zum Arbeitsschritt „Funktionsanalyse“ erweitert.

Aufteilung der Systemanforderungen

Da in der vorliegenden Arbeit nur die Komponente der Sicherungslogik innerhalb des Gesamtsystems der infrastrukturseitigen Sicherungstechnik betrachtet wird und keine zusätzliche Modulaufteilung der Sicherungslogik vorgenommen wird, ist in diesem Arbeitsschritt nur festzulegen, welche der zuvor definierten Anforderungen für die Komponente der Sicherungslogik eine Rolle spielen. Aufgrund der ebenfalls zu erfolgenden Priorisierung bei der Umsetzung (vgl. Kapitel 3.6.3) erscheint es jedoch zielführend, diesen Arbeitsschritt als Unterarbeitsschritt der Funktionsanalyse (siehe voriger Abschnitt) zu betrachten.

[12] Hier ist mit dem Begriff die Identifikation der zu betrachtenden Gefährdungen gemeint und nicht die später durchzuführende „betriebliche Gefährdungsanalyse“

Entwurfsphase / Logik-Erstellung

Dieser Arbeitsschritt bildet den Kern der Arbeit. Dabei wird gemäß der gewählten hybriden Methode (vgl. Kapitel 3.6.3) zunächst eine Basislogik geschaffen, die im Anschluss iterativ erweitert wird.

Herleitung des Datenmodells

Um die Logik in der Entwurfsphase zu beschreiben, werden unabhängig von der Beschreibungsart (z. B. natürlichsprachlich, grafisch oder formal) Begriffe benötigt, die für bestimmte Datenkonstrukte oder technische Konzepte stehen, z. B. „Weiche“ oder „Durchrutschweg“.

Zwar existieren für bestimmte Begriffe standardisierte oder rechtlich vorgeschriebene Definitionen, z. B. dass Bahnhöfe in Deutschland „Bahnanlagen mit mindestens einer Weiche [sind], wo Züge beginnen, enden, ausweichen oder wenden dürfen“ [EBO:2019-04-05, §4 Abs. 2], jedoch kann die Bedeutung im Ausland anders sein oder die Begriffsdefinition nicht mehr zu den Voraussetzungen der neuen Sicherungslogik im Umfeld der weiteren technologischen Entwicklungen im Bereich der Leit- und Sicherungstechnik passen, die in Kapitel 2.2 beschrieben wurden. Für viele Begriffe existiert zudem gar keine einheitliche Definition, sondern es existieren je nach Quelle und Kontext unterschiedliche Definitionen bzw. der Begriff wird unterschiedlich verwendet. Dabei bestehen die Unterschiede häufig nicht im Sprachlichen, sondern im Konzeptionellen. Unterschiedliche Definitionen sind auch die Folge von unterschiedlichen Umsetzungskonzepten.

Aus dem geschilderten Grund sollten die bei der Logik-Entwicklung verwendeten Begriffe klar definiert werden. Diese Definitionen können in einem Datenmodell (bzw. „Domänen-Modell“) zusammengefasst werden, welches der Strukturmodellierung der smartLogic entspricht (vgl. [Gadatsch 2019, S. 4]).

Die gewählte Definition eines Begriffes kann einen Einfluss auf das Verhalten der Logik haben. Zum Beispiel ermöglicht eine Aufteilung der Beanspruchung der Gleisinfrastruktur durch einen Zug in mehrere Bestandteile mit verschiedenen Sicherheitsanforderungen (z. B. Fahrweg, Durchrutschweg etc.) ein flexibleres Belegungsmanagement der Infrastruktur. Eine Weiche kann ebenfalls verschiedene Ausdehnung haben, je nachdem, welcher Aspekt (z. B. physisches Element, überschneidende Lichtraumprofile etc.) betrachtet werden soll.

Eigenschaften, wie die oben geschilderten, werden beispielsweise in den verschiedenen Datenmodellen, die in Kapitel 2.5 vorgestellt wurden, unterschiedlich definiert. Die Definition hängt dabei von den jeweiligen Anforderungen an das Modell ab. Das Kriterium des möglichst reibungslosen Einfügens in die zukünftige Systemarchitektur der digitalen Leit- und Sicherungstechnik spricht zwar dafür, ein bestehendes Datenmodell zu übernehmen. Das Datenmodell hat allerdings einen großen Einfluss auf den Definitionsspielraum, den die neue Sicherungslogik hat. Dadurch besteht die Gefahr, dass ein Festlegen auf ein bestehendes Datenmodell innovative Sicherungskonzepte verhindert oder einschränkt. Dies widerspricht dem Kriterium der möglichst optimalen Zielerfüllung und dem vorgegebenen „Grüne Wiese“-Ansatz.

Aus den genannten Gründen ist in der grundsätzlichen Vorgehensweise die Erstellung des Datenmodells als Arbeitsschritt zu berücksichtigen. Dabei sollte jedoch geprüft werden, inwieweit auf den bestehenden Datenmodellen aufgebaut werden kann, um bestehende Standards im Sinne der globalen Anforderungen der Unterstützung von Standardschnittstellen und der Migrationsfähigkeit zu unterstützen (vgl. Kapitel 3.5).

Demonstrator-Erstellung

Wie beschrieben, ist die Erstellung eines Demonstrators gemäß den Prinzipien des „Smart Engineering“ sinnvoll, um frühzeitig Stakeholdern auf einer niederschwelligen Ebene eine Beteiligung am Entwicklungsprozess zu ermöglichen und mögliche Vorteile durch das Projekt veranschaulichen zu können. Weiterhin erlaubt der Demonstrator bei geeigneter Gestaltung auch eine Evaluierung der Nutzenpotenziale der neuen Logik.

3.6.5 Reihenfolge der Arbeitsschritte

Schließlich ist die Reihenfolge der Arbeitsschritte in der grundsätzlichen Vorgehensweise zu diskutieren.

Grundsätzliche Überlegungen

Auch für die Reihenfolge der Arbeitsschritte lässt die beschlossene Orientierung am genormten V-Modell nur begrenzt Entscheidungsspielraum. Der vorgegebene Ablauf aus der Norm sollte soweit wie möglich eingehalten werden. Abweichungen sollten, sofern sie erforderlich sind, gut begründet werden.

Zu beachten ist zudem, dass gemäß dem V-Modell und vor allem gemäß der agilen Methode hier nicht eine rein sequentielle Reihenfolge definiert wird, sondern dass Änderungen und weitere Iterationen auch aus späteren Arbeitsschritten wieder eingeleitet werden können. Zu bestimmen ist demgemäß, in welcher Reihenfolge die initiale Bearbeitung erfolgen sollte, der auch die Beschreibung in dieser Dissertation folgt.

Einordnung des Arbeitsschritts „Herleitung des Datenmodells“

Entscheidungsbedarf entsteht bei der Einordnung des zusätzlichen Arbeitsschrittes „Herleitung des Datenmodells“, dessen Notwendigkeit in Kapitel 3.6.4 festgestellt wurde. Es wäre denkbar, diesen Arbeitsschritt unmittelbar auf die Systemdefinition folgen zu lassen, da es sich in gewisser Weise um eine weitergehende Systemdefinition im Sinne von Definitionen der beteiligten Elemente und Begrifflichkeiten handelt. Diese Platzierung hat jedoch den Nachteil, dass Überlegungen, die sich auf Basis des Arbeitsschrittes Funktionsanalyse für die Gestaltung der neuen Sicherungslogik ergeben, bezüglich der Gestaltung des Datenmodells in dessen initialen Entwurf nicht berücksichtigt werden können. Dieser Umstand könnte zu einem größeren Änderungsaufwand an grundsätzlichen Inhalten des Datenmodells führen. Eine Lösungsmöglichkeit wäre es, das Datenmodell erst nach der Funktionsanalyse zu erstellen, aber bereits während der Funktionsanalyse Begrifflichkeiten als spätere Bestandteile des Datenmodells sauber zu definieren, damit eine eindeutige Verwendung in der Funktionsanalyse gewährleistet ist.

Weiterhin könnte das Datenmodell (und damit die Strukturmodellierung) theoretisch vor oder hinter der Verhaltensmodellierung eingeordnet werden. Für das Verständnis der Verhaltensmodellierung ist ein Verständnis der verwendeten Begriffe allerdings zwingend erforderlich. Aus diesem Grund wird die Herleitung des Datenmodells nach der Funktionsanalyse, aber vor der Verhaltensmodellierung in die Arbeit eingeordnet. Zu beachten ist jedoch, dass das Datenmodell während der Verhaltensmodellierung noch erweitert werden kann, da die Erfordernisse der Verhaltensmodellierung einen Einfluss auf die Inhalte des Datenmodells haben (vgl Kapitel 3.6.4).

Einordnung des Arbeitsschritts „Demonstrator-Erstellung“

Neben dem Datenmodell ist die Einordnung des Arbeitsschrittes „Demonstrator-Erstellung“ in die Vorgehensweise durch die Struktur des V-Modells nicht fest vorgegeben. Zur Erstellung des Demonstrators wird zunächst die Logik benötigt, die darin implementiert wird. Gerade bei diesem Schritt sollte aber gemäß der agilen Komponente der gewählten hybriden Methode eine frühzeitige Entwicklung des Demonstrators erfolgen, damit schnell Feedback gesammelt werden kann, das dann in der weiteren Logik-Entwicklung genutzt werden kann. Die Demonstrator-Erstellung wird also zeitlich leicht versetzt, aber überwiegend parallel zum Arbeitsschritt „Logikerstellung“ angeordnet. In dieser Arbeit erfolgt die Beschreibung anschließend an die Logik-Entwicklung.

3.6.6 Zusammenfassung der gewählten Vorgehensweise

Gemäß der gewählten Entwicklungsmethode und der Diskussion in den vorangegangenen Unterkapiteln dieses Kapitels ergibt sich damit die in Abb. 31 dargestellte Vorgehensweise für die Erstellung der neuen Sicherungslogik, die nachfolgend kurz zusammengefasst wird.

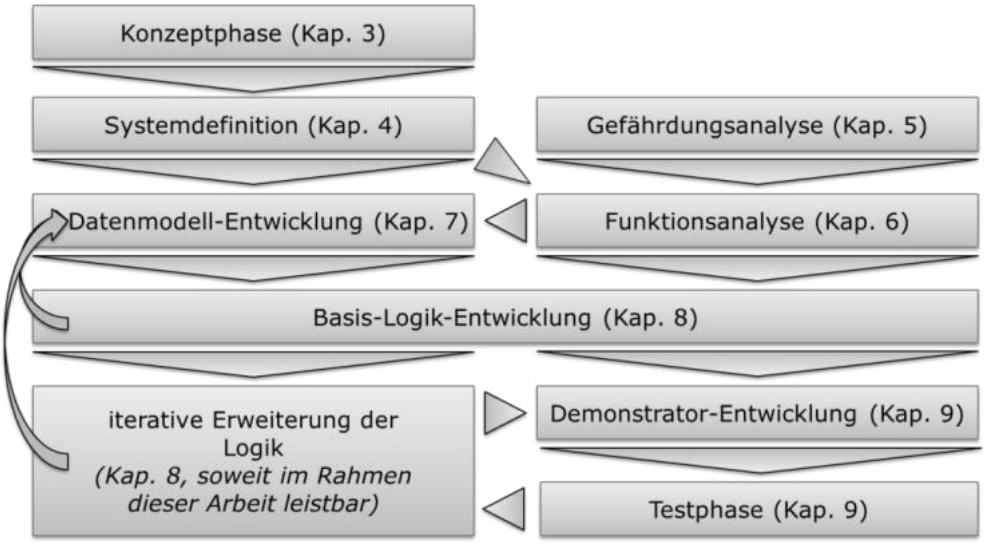


Abb. 31: Grundsätzliche Vorgehensweise
[Eigene Darstellung]

Die *Konzeptphase* ist Inhalt dieses Hauptkapitels. Die daraus folgende Wahl des Systemzuschnitts sowie der Systemumgebung erfolgt in Kapitel 4 *„Systemdefinition“*. Ausgangspunkt für die *Funktionsanalyse* in Kapitel 6, in der der funktionale Umfang der neuen Sicherungslogik abgesteckt wird, ist zum einen eine eingehende *Gefährdungsanalyse*[13], der sich Kapitel 5 widmet. Zum anderen stammen die funktionalen Anforderungen aus den betrieblichen Anforderungen an die Sicherungslogik, die sich aus dem Systemzuschnitt und damit aus der Systemdefinition ergeben.

Aus der Funktionsanalyse und der Systemdefinition wird ein erstes *Datenmodell* erstellt (Kapitel 7), welches der Strukturmodellierung der Logik entspricht. Wichtige Begriffe dafür werden bereits parallel zur Funktionsanalyse definiert und fließen später in die Erstellung des Datenmodells ein.

Nachdem diese Vorarbeiten erledigt sind, kann schließlich die *Basislogik* entwickelt werden. Sie umfasst die Verhaltensmodellierung der wesentlichen Funktionen der Sicherungslogik. Gemäß der gewählten hybriden Methode zwischen V-Modell und agiler Arbeitsweise kann die Logik nachfolgend

[13] im Sinne einer Gefährdungsidentifikation, nicht im Sinne einer „betrieblichen Gefährdungsanalyse“, vgl. auch Fußnote 12

iterativ erweitert werden. Bei der Logikentwicklung wird das Datenmodell ggf. um zusätzlich benötigte Begriffe erweitert. Die gesamte Logikentwicklung, die in dieser Arbeit geleistet werden kann, ist Thema von Kapitel 8. Kapitel 9 widmet sich der *Demonstrator-Entwicklung* und der *Testphase* mit dem Demonstrator.

U. a. durch die iterative Vorgehensweise kann es auch nachträglich zu Anpassungen in früheren Schritten, vor allem beim Datenmodell, kommen. Bei der Bearbeitung der einzelnen Schritte wird daher soweit möglich darauf geachtet, dass mögliche spätere Anforderungen bereits mitgedacht werden und durch möglichst generische Definitionen viel Raum besteht, nachträglich identifizierte Anforderungen einzuarbeiten.

3.7 Zusammenfassung

In der vorliegenden Arbeit soll eine neue Sicherungslogik als Kern der infrastrukturseitigen Sicherungstechnik entwickelt werden. In diesem Hauptkapitel wurde hierfür die Zielsetzung bestimmt sowie die grundsätzliche Methode und Vorgehensweise für die Entwicklung der neuen Sicherungslogik hergeleitet.

Zunächst wurden dafür aus den Interessen der am Bahnbetrieb beteiligten Personengruppen die globalen Ziele der Bahnproduktion und die Ziele der infrastrukturseitigen Sicherungstechnik im Speziellen bestimmt. Die Ziele wurden anschließend in Kapitel 3.2 auf die zu entwickelnde Sicherungslogik eingegrenzt und daraus die konkrete Aufgabenstellung für diese Arbeit hergeleitet. Demnach soll eine neue Sicherungslogik entwickelt werden, die eine optimale Kapazität der Infrastruktur und eine optimale Energieeffizienz ermöglicht sowie die Robustheit des Bahnbetriebs gegenüber Störungen erhöht. Dabei ist auf einen geringen Planungs- und Genehmigungsaufwand zu achten, um Kosten zu sparen und notwendige Änderungen der Sicherungstechnik schnell durchführen zu können. Um der knappen Ressource „qualifizierte Arbeitskräfte“ zu begegnen, soll der Arbeitskräfteeinsatz gering sein. Die zu entwickelnden Komponenten sollen bei geringem Hardwareeinsatz lange Nutzungszeiten aufweisen.

Aus Ressourcengründen wurden für die Zielsetzung inhaltliche Abgrenzungen vorgenommen. So soll die Logik nur bis zur Entwicklungsphase der Verhaltensmodellierung (Schritt „*Entwurf*“ im V-Modell) entwickelt werden und ein kleiner Demonstrator erstellt werden. Weiterhin beschränkt sich die Logik auf die wichtigsten Prüfprozesse, die zum Durchführen des Betriebs erforderlich sind, allerdings basierend auf einer ausführlichen Funktionsanalyse ohne Einschränkungen. Im weiteren Verlauf der Arbeit sollen im Rahmen der Funktionsanalyse diese Basis-Prozesse durch ein systematisches Verfahren bestimmt werden. Weiterhin werden im Rahmen der Arbeit keine speziellen Werte wie Risikoakzeptanzkriterien ermittelt.

Aufbauend auf der Aufgabenstellung wurden in einer Analyse mittels Betriebsbeobachtung, Interview und Experten-Workshop Verbesserungspotenziale der bestehenden Systeme und damit Nutzenpotenziale für die Erstellung einer solchen Sicherungslogik identifiziert. Demnach kann davon ausgegangen werden, dass es unter anderem noch Potenzial bei der Gestaltung der Durchrutschwege und der Nutzbarmachung von ETCS-Funktionen durch die Sicherungslogik gibt. Zudem besteht Potenzial, Flankenschutzbedingungen flexibler auszulegen und den Bahnbetrieb bei Abweichungen vom Regelbetrieb robuster zu gestalten, beispielsweise indem manuelle Rückfallebenen reduziert werden.

Für die Gestaltung der Sicherungslogik wurden aus den Zielen an die neue Logik und den identifizierten Nutzenpotenzialen spezifische Anforderungen an die neue Sicherungslogik und Kriterien zur Auswahl der Entwicklungsmethode und grundsätzlichen Vorgehensweise hergeleitet. Um

die Potenziale bestmöglich heben zu können, wird die neue Sicherungslogik im Wesentlichen eine Neuentwicklung auf der „Grünen Wiese“ sein, allerdings mit nachträglichem Vervollständigen durch die Literatur und empirische Beobachtungen. Die Arbeit folgt einem hybriden Ansatz zwischen V-Modell und einer agilen Methode. Dabei ist das Konzept des „Smart Engineering“ mit einem starken „Requirements Engineering“ Vorbild. Die aus diesen Rahmenbedingungen entstandene grundsätzliche Vorgehensweise für die gesamte Arbeit ist in Kapitel 3.6.6 in Abb. 31 dargestellt.

4 Systemdefinition (System(umfeld)analyse)

Gemäß der auf dem V-Modell basierenden gewählten Vorgehensweise (vgl. Kapitel 3.6.6) muss im Rahmen der Entwicklungsphase der *Systemdefinition* eine Analyse des Systemumfelds durchgeführt werden, in der der Zuständigkeitsbereich des betrachteten Systems „Sicherungslogik ‚smartLogic'" innerhalb der digitalen Leit- und Sicherungstechnik abgegrenzt und die benachbarten, externen Systeme, nachfolgend auch als „**Umsysteme**" bezeichnet, definiert werden. Hierzu gehört auch die Festlegung der Schnittstellen zwischen der Sicherungslogik und den Umsystemen. Mit dieser Aufgabe beschäftigt sich das vorliegende Hauptkapitel.

Das Hauptkapitel korrespondiert mit der Phase der Systemdefinition gemäß dem V-Modell in [DIN EN 50126-1:2017], stellt aber keine vollständige Durchführung dieser Phase dar (vgl. die Ausführungen zur grundsätzlichen Methode und Vorgehensweise in Kapitel 3.6. Nicht Bestandteil dieses Hauptkapitels ist eine interne Aufteilung des Systems in Module, die im V-Modell zur Phase der „Aufteilung von Systemanforderungen" gehört (vgl. Kapitel 2.7) und gemäß der in Kapitel 3.6 festgelegten Vorgehensweise im Rahmen der Funktionsanalyse in Kapitel 6 vorgenommen wird (vgl. zur Begründung Kapitel 3.6.4).

4.1 Ziel, Vorgehensweise und Aufbau des Kapitels

[DIN EN 50126-1:2017, S. 23] definiert analog zu IEC 60050-351:2013 ein System als „Menge miteinander in Beziehung stehender Elemente, die in einem bestimmten Zusammenhang als Ganzes gesehen und als von ihrer Umgebung abgegrenzt betrachtet werden". Unter dem Schritt der Systemdefinition versteht die Norm im Wesentlichen [DIN EN 50126-1:2017, S. 45]:

- die „Beschreibung der wesentlichen Eigenschaften und Funktionen des Systems" sowie
- die „Klärung der Schnittstellen mit anderen Systemen".

Weiterhin ist vorgesehen [ebd.], dass

- ein „RAM[14]- und Sicherheitsplan eingerichtet" wird,
- die „vorgesehenen Betriebsbedingungen (Instandhaltung, Umwelt usw.)" und
- die „Auswirkungen auf die RAMS[15]-Parameter benachbarter Systeme abgeleitet werden".

Eine Aufteilung des Systems in Komponenten ist nicht Teil der Phase der Systemdefinition (vgl. Kapitel 3.6.4) und deshalb nicht Teil dieses Hauptkapitels.

Die geforderten Dokumente wie der *RAM- und Sicherheitsplan* können aufgrund des großen Aufwandes im Rahmen dieser Forschungsarbeit nicht erstellt werden (zur Begründung vgl. die Erläuterungen in Kapitel 3.3 und 3.6.3). Für das Ziel dieser Arbeit in Hinblick auf die Beschreibung der neuen Logik sind die *Betriebsbedingungen* von untergeordneter Bedeutung, da davon ausgegangen werden kann, dass eine Hardwareplattform genutzt werden wird, die geeignete Betriebsbedingungen schafft. Gemäß der globalen Anforderung der Nutzung von Standardschnittstellen (vgl. Kapitel 3.5) wird zudem davon ausgegangen, dass die *Auswirkungen auf die RAMS-Parameter der benachbarten Systeme* (Umsysteme) nicht näher betrachtet werden müssen. Als Ziele dieses Hauptkapitels

[14] Reliability, Availability, Maintainability

[15] Reliability, Availability, Maintainability, and Safety

verbleiben somit die *Beschreibung der wesentlichen Eigenschaften und Funktionen des Systems* der Sicherungslogik smartLogic sowie die *Klärung der Schnittstellen mit anderen Systemen*.

Um eine Grundlage für Entscheidungsfindungen in Bezug auf die Systemdefinition zu haben, sind zunächst jedoch die spezifischen Anforderungen an die Systemdefinition aus den globalen Anforderungen herzuleiten. Dieser Schritt erfolgt in Kapitel 4.2.

Auf die Anforderungen folgt gemäß der vorgesehenen Reihenfolge in [DIN EN 50126-1:2017] die *Beschreibung des Systems*, wozu die Aufgabe der Sicherungslogik im Kontext der digitalen Leit- und Sicherungstechnik festzulegen ist. Hierzu gehört vor allem die Abgrenzung zu den Umsystemen (vgl. Kapitel 4.3). Ein wichtiger Bestandteil eines Softwaresystems ist auch die Verwaltung der benötigten Daten. Hierfür ist zu klären, wie diese Daten bereitgestellt werden. Für die Anwendung der smartLogic werden unterschiedliche Arten von Daten benötigt, die aus verschiedenen Quellen stammen, so dass es sinnvoll erscheint, diese Fragestellung in einem eigenen Unterkapitel zu behandeln (Kapitel 4.4). Ebenfalls eng mit der Definition der Systemgrenzen ist die Beschreibung der Kommunikation über diese Grenzen in Form der Schnittstellen zu den Umsystemen verbunden, der sich Kapitel 4.5 widmet.

Kapitel 4.6 beschreibt die aus den Ergebnissen der vorigen Unterkapitel resultierende Gesamtarchitektur der digitalen Leit- und Sicherungstechnik, also die Sicherungslogik im Kontext ihrer Umsysteme und Schnittstellen. Im Anschluss werden die Ergebnisse diskutiert (Kapitel 4.7) und vor dem Hintergrund alternativer Architekturen der digitalen Leit- und Sicherungstechnik, insbesondere der bereits in Kapitel 2.4 beschriebenen RCA, eingeordnet (Kapitel 4.8), bevor das Kapitel abschließend zusammengefasst wird (Kapitel 4.9). Wie in Kapitel 1.3 erwähnt, erfolgt der Vergleich mit der Literatur aufgrund des „Grüne Wiese“-Ansatzes bewusst erst am Ende des Hauptkapitels und nicht zu Beginn.

4.2 spezifische Anforderungen an die Systemdefinition der Sicherungslogik

Die spezifischen Anforderungen und damit die Entscheidungskriterien für das Treffen von Design-Entscheidungen in Bezug auf die Systemdefinition der Sicherungslogik ergeben sich primär aus den globalen Anforderungen an die neu zu schaffende Sicherungslogik, die in Kapitel 3.5 beschrieben wurden. Dazu wird für jede globale Anforderung überlegt, welchen Einfluss die Ergebnisse des vorliegenden Hauptkapitels in Hinblick auf die Erfüllung der jeweiligen globalen Anforderung haben könnten. Zusätzlich wurde zur Vervollständigung der spezifischen Anforderungen ein Brainstorming mit Fachkollegen durchgeführt.

Tab. 8 enthält eine Übersicht der globalen Anforderungen und der daraus hergeleiteten spezifischen Anforderungen, die anschließend unterhalb der Tabelle näher erläutert werden. Für die Systemdefinition sind nicht alle globalen Anforderungen von Relevanz. Bei nicht relevanten globalen Anforderungen ist dieser Umstand in kursiv vermerkt.

Tab. 8: spezifische Anforderungen an die Systemdefinition

Zieldimension	globale Anforderung	spezifische Anforderungen
Kernanforderung sichere Logik		alle Schutzfunktionen werden abgedeckt
geringer Planungs- und Genehmigungsaufwand	schlanke Logik	möglichst wenige nicht sicherheitsrelevante Funktionen werden abgedeckt, schlanke Schnittstellen
	Beschränkung auf sicherungskritischen Kern	*Anforderung primär für Funktionsanalyse (Kap. 6) relevant*

	generische Logik	Daten kommen aus externen Quellen, die Gleistopologie sowie vorhandene Infrastrukturelemente und weitere externe Systeme werden in generischer Form bei den Umsystemen berücksichtigt
	Topologieunabhängigkeit	Spezialfall von „generische Logik“
	flexible Infrastrukturzuordnung	Logik ist von den Infrastrukturelementen getrennt
Interoperabilität	Standardschnittstellen	Standardschnittstellen verwenden
geringer Hardwareeinsatz	nur erforderliche Infrastrukturelemente	bei der Entwicklung der Sicherungslogik werden nur Infrastrukturelemente berücksichtigt, die Auswirkungen auf die Sicherungslogik haben
geringer Arbeitskräfteeinsatz	hohe Automatisierung	Sicherungslogik und Bedienplatz sind getrennt
	flexible Kontrollbereiche	
Energieeffizienz	keine unnötigen Bremsvorgänge	*keine Relevanz der Anforderungen für die Systemdefinition festgestellt*
	Freiraum für Fahrzeuge	
hohe Kapazität	Ermöglichung maximaler Geschwindigkeit	*keine Relevanz der Anforderung für die Systemdefinition festgestellt*
	geringe Latenz	Schnittstellen sind so gestalten, dass eine schnelle Verarbeitung von Aufträgen für die Sicherungslogik möglich sind
	minimale Infrastrukturbeanspruchung	*keine Relevanz der Anforderungen für die Systemdefinition festgestellt*
	frühestmögliche Infrastrukturfreigabe	
hohe Robustheit	Rückfallebenenintegration	*keine Relevanz der Anforderungen für die Systemdefinition festgestellt*
	Regelhandlungsgebot	
	Freiraum für Fahrzeuge	
	Resilienz	*in diesem Hauptkapitel ist Resilienz nur eine Anforderung an die nicht betrachtete Hardwareplattform, auf der die Sicherungslogik läuft*
	modulare Außerbetriebnahme	modularer Aufbau der infrastrukturseitigen Sicherungstechnik
lange Nutzungszeiten	Migrationsfähigkeit	Architektur ist möglichst kompatibel zu bestehender Technik
	Zukunftsfähigkeit	Umsysteme und Schnittstellen generisch anlegen
[ohne]	Protokollierung	Ereignisse müssen sicher und unverfälschbar protokolliert werden

Die digitale Leit- und Sicherungstechnik muss als Gesamtes die *Kernanforderung* sicherstellen, wonach alle Schutzfunktionen abzudecken sind und somit kein unsicherer Zustand bedingt durch die LST eintreten kann. Bezogen auf die Sicherungslogik bedeutet dies, dass eine klare Abgrenzung der infrastrukturseitigen Sicherungstechnik von ihren Umsystemen erforderlich ist, die so gezogen sein muss, dass nicht sicherheitskritische Umsysteme entweder keinen[16] Einfluss auf die Sicherheit des Bahnbetriebs haben oder innerhalb klar definierter Parameter eine eigene Sicherheitsverantwortung besitzen (zu nennen ist für den letzteren Fall insbesondere die fahrzeugseitige Sicherungstechnik, die außerhalb des Betrachtungsraums dieser Arbeit liegt).

Aus der Kernanforderung kann jedoch nur ein minimaler Systemumfang der Sicherungslogik hergeleitet werden. Die Anforderung der *schlanken Logik* wirkt sich dagegen auf den maximalen Systemumfang aus. Demnach sind alle nicht sicherheitsrelevanten Funktionen in Komponenten außerhalb der Sicherungstechnik und damit der Sicherungslogik anzuordnen. Auch in Bezug auf die Infrastrukturelemente fordert eine Anforderung, dass *nur erforderliche Infrastrukturelemente* von der Sicherungslogik als Teil ihres Systemumfelds berücksichtigt werden sollen. Wenn die beiden letztgenannten Anforderungen in Konflikt mit der Kernanforderung stehen, ist jedoch die Kernanforderung der sicheren Logik höher zu bewerten.

Zwei weitere globale Anforderung fordern, dass die Sicherungslogik *generisch* und *topologieunabhängig* geplant werden soll. Die Logik soll demnach flexibel auf Änderungen an der Gleistopologie, bei den Infrastrukturelementen oder den weiteren externen Systemen sowie auf Änderungen der äußeren Rahmenbedingungen (wie zusätzlicher Anforderungen durch geänderte Regelwerke) anpassbar sein. Hieraus kann gefolgert werden, dass die Infrastrukturdaten (für eine räumliche Instanz) der Sicherungslogik nicht fest vorgegeben, sondern (möglichst auch während der Laufzeit) änderbar sein sollen. Somit müssen die entsprechenden Daten aus gesonderten externen Quellen kommen und können nicht Bestandteil der eigentlichen Logik sein.

Zudem fordert die globale Anforderung der *flexiblen Infrastrukturzuordnung,* dass auch die Ansteuerung der einzelnen Feldelemente klar von der generischen Sicherungslogik getrennt sein müssen, damit die Zuordnung der Feldelemente zu Zuständigkeitsbereichen der Logik flexibel erfolgen kann. Auch der Bedienplatz soll als eigene Komponente der infrastrukturseitigen Sicherungstechnik aufgrund der globalen Anforderungen der *hohen Automatisierung* und *flexiblen Kontrollbereiche* von der Sicherungslogik getrennt sein.

Bei der Abgrenzung der Sicherungslogik von den Umsystemen ist aufgrund der Anforderung der *geringen Latenz* auch auf die Ermöglichung einer schnellen Verarbeitung zu achten. Zudem soll eine geeignete *Protokollierung* durch den Systemaufbau sichergestellt werden. Die Kommunikationsprotokolle an sich sind jedoch nicht Teil dieser Arbeit, die sich auf funktionale Aspekte konzentriert (vgl. Kapitel 3.3).

Aufgrund der Annahme der Unabhängigkeit der entwickelten Sicherungslogik als Software von der verwendeten Hardwareplattform (vgl. Kapitel 3.2) sind Anforderungen, die sich im Kontext dieses Hauptkapitels ausschließlich auf die Funktionsweise dieser Hardwareplattform beziehen, nicht relevant, da sich die Arbeit nur auf die Softwareseite konzentriert. Hierzu gehört die Resilienz-Anforderung.

[16] Sicherheit bedeutet bekanntlich die Abwesenheit eines nicht tolerierbaren Risikos. Es darf also tatsächlich kein Einfluss auf die Sicherheit bestehen, da es sich bei der Sicherheit gemäß dieser Definition um einen Zustand handelt, der entweder erreicht ist oder nicht.

Bei Störungen oder erforderlichen Wartungsarbeiten soll keinesfalls das Gesamtsystem ausfallen, sondern nur Teilsysteme (*modulare Außerbetriebnahme*). Die Komponenten der infrastrukturseitigen Sicherungstechnik sollten also möglichst modular aufgebaut sein.

Für die Schnittstellen gibt es die Anforderung, dass möglichst generische *Standardschnittstellen* verwendet werden sollen. Hierfür ist eine Analyse von vorhandenen und – soweit heute absehbar – möglicherweise zukünftig existierenden Umsystemen bzw. von deren vermuteten Weiterentwicklungen erforderlich. Diese Analyse ist auch für die Migrationsphase bezogen auf die globale Anforderung der *Migrationsfähigkeit* sinnvoll. Hierzu stehen die Erkenntnisse aus Kapitel 2.2 zur Verfügung. Die Anforderung der Nutzung von Standardschnittstellen wird als wichtiger betrachtet als die Anforderung nach schlanken Schnittstellen aufgrund der globalen Anforderung der schlanken Logik. Falls jedoch Schnittstellen neu definiert werden müssen, sollen diese nicht umfangreicher sein als notwendig.

Im Sinne der globalen Anforderung der *Zukunftsfähigkeit* ist darauf zu achten, dass nachträglich auch noch neue Systeme als Umsysteme von der Sicherungslogik berücksichtigt werden können. Da die diese zukünftigen Systeme noch nicht bekannt sind, sollte auf eine möglichst generische Definition der Umsysteme geachtet werden.

Die globalen Anforderungen zu den Zieldimensionen *Kapazität*, *Energieeffizienz* und *Robustheit*, die sich auf die interne Funktionsweise der Sicherungslogik und nicht auf den Systemaufbau beziehen, werden als nicht relevant für die Systemdefinition angenommen. Sie sind stattdessen relevant für die nachfolgenden Hauptkapitel der Arbeit.

4.3 Beschreibung des Systems und Abgrenzung von den Umsystemen

In diesem Kapitel soll das System der Sicherungslogik smartLogic mit ihren wesentlichen Funktionen grob beschrieben werden. Angaben der Funktionen beschränken sich an dieser Stelle auf die grundsätzliche Aufgabe der smartLogic. Der genaue Funktionsumfang soll gemäß den Ergebnissen aus Kapitel 3.6.4 in Kapitel 6 bestimmt werden.

Die grundsätzlichen Funktionen ergeben sich zum einen aus der Aufgabenstellung für die smartLogic, die in Kapitel 3.2 hergeleitet wurde. Zum anderen hängen sie von der genauen Abgrenzung der smartLogic innerhalb der infrastrukturseitigen Sicherungstechnik ab.

In Kapitel 3.2 wurde die Aufgabe und damit grundsätzliche Funktion der Sicherungslogik so zusammengefasst, dass sie „dafür zuständig ist, die Sicherheit von Zustandsänderungen wie Fahrerlaubnisse und geplante Statusänderungen von Infrastrukturelementen sicherzustellen sowie auf ungeplante Ereignisse mit Sicherheitsreaktionen zu reagieren.“ Dabei wurde angenommen, dass „die Sicherungslogik eine Software-Komponente ist, die auf einer sicheren Hardwareplattform läuft.“ Weiterhin wurde bereits in der allgemeinen Festlegung der Abgrenzungen für diese Arbeit der Bereich der bewussten Angriffe auf den Bahnbetrieb ausgeklammert (vgl. Kapitel 3.3).

Gemäß der Definition der Aufgabe der Sicherungslogik aus Kapitel 3.2 ist die Sicherungslogik für die Aufrechterhaltung der Sicherheit im operativen Kontext zuständig. Ihre Aufgabe beschränkt sich also auf die Durchführung des Betriebs und nicht zum Beispiel bereits auf die Planung oder die Herstellung. Gleichzeitig wurde in Kapitel 4.2 im Sinne der globalen Anforderung der *schlanken Logik* die spezifische Anforderung aufgestellt, dass die Sicherungslogik „möglichst wenig nicht sicherheitsrelevante Funktionen“ mit abdecken soll. Diese nicht sicherheitsrelevanten Funktionen sind stattdessen Aufgabe der Leittechnik. Es ist daher eine genaue Abgrenzung der Sicherungslogik von der Leittechnik erforderlich, die in Unterkapitel 4.3.1 hergeleitet wird.

Eine Abgrenzung zu den Fahrzeugen macht u. a. aus Gründen der *Interoperabilität* Sinn, denn Fahrzeuge sollen sich möglichst mit *einem* Bordsystem durch ganz Europa und insbesondere durch Zuständigkeitsbereiche verschiedener Sicherungslogiken bewegen können. Es stellt sich in diesem Zusammenhang die Frage, welche sicherungstechnischen Funktionen im Fahrzeug und welche auf Seiten der Sicherungslogik angesiedelt sind. Dies wird in Unterkapitel 4.3.2 hergeleitet. Es ist grundsätzlich auch denkbar, dass das Fahrzeug direkt mit den Stellelementen kommuniziert (oder Fahrzeuge untereinander), ohne eine zentrale Sicherungslogik miteinzubeziehen. Deshalb wird die Abgrenzung der Sicherungslogik zu den Stellelementen in Kapitel 4.3.2 mitbetrachtet.

Auch die Beschaffenheit der Gleisinfrastruktur an sich, insbesondere des Bahnkörpers, hat einen Einfluss auf die Sicherheit. Unterkapitel 4.3.3 beschäftigt sich daher mit der Abgrenzung der Aufgaben zur Aufrechterhaltung der Sicherheit der Gleisinfrastruktur zu den Aufgaben der Sicherungslogik.

4.3.1 Abgrenzung von der Leittechnik

Wie bereits bei den spezifischen Anforderungen beschrieben wurde, muss die Sicherungslogik einerseits so zugeschnitten sein, dass sie einen unsicheren Zustand zuverlässig verhindert. Andererseits soll sie möglichst schlank gehalten sein, so dass nicht sicherheitsrelevante Funktionen in nicht sicherheitskritische Umsysteme ausgegliedert werden, die in Abgrenzung zur Sicherungstechnik als Leittechnik bezeichnet werden können.

Sicherungslogik und Leittechnik arbeiten im Betrieb direkt miteinander, die Abgrenzung zwischen ihnen ist jedoch nicht intuitiv klar. Beispielsweise hat die Entscheidung über die Reihenfolge von Fahrzeugbewegungen bei Belegungskonflikten einen sicherungstechnischen (es muss ausgeschlossen werden, dass zwei Fahrzeuge zur selben Zeit am selben Ort sind) und einen dispositiven Anteil (es muss entschieden werden, welche Fahrzeugbewegung Vorrang hat).

In diesem Unterkapitel soll die optimale Abgrenzung zwischen der Sicherungslogik und der Leittechnik hergeleitet werden. Zunächst werden dafür im ersten Abschnitt verschiedene Ansätze verglichen und ein Ansatz ausgewählt. Anschließend wird auf Basis dieses Ansatzes der daraus folgende Ablauf der Kommunikation zwischen der Sicherungslogik und der Leittechnik im zweiten Abschnitt beschrieben. Dabei stellt sich die Frage, wieviel die Sicherungslogik selbst entscheiden soll, also wie intelligent sie agieren soll. Hiermit beschäftigt sich der letzte Abschnitt.

Ansätze für die Abgrenzung zwischen Sicherungslogik und Leittechnik

Für die Abgrenzung zwischen der Sicherungslogik und der Leittechnik sind theoretisch mehrere Ansätze denkbar. Die beiden extremen Ansätze lassen sich wie folgt beschreiben:

1. Der dispositive Anteil könnte komplett in die Sicherungslogik integriert werden, so dass ein kombiniertes Leit- und Sicherungssystem entstehen würde, welches bereits bei der Entscheidungsfindung alle sicherheitsrelevanten Aspekte berücksichtigt und somit insgesamt sicherheitskritisch wäre.
2. Die Sicherungslogik fungiert als reines sicherheitskritisches Prüfsystem, welches alle sicherheitsrelevanten Entscheidungen der Leittechnik vor der Umsetzung durch die Fahrzeuge oder Stellelemente anhand eines einfachen generischen Regelsets in Bezug auf ihre Sicherheit überprüft. Das Leitsystem würde in diesem Fall die zu überprüfende Entscheidung in einer **Prüfanfrage** an das Prüfsystem schicken. Die Prüfung durch das Prüfsystem wäre in diesem Fall unabhängig von der Berechnung der optimalen Lösung und würde deren Optimalität nicht hinterfragen, sondern nur

überprüfen, ob durch die beabsichtigte Zustandsänderung ein unsicherer Zustand auftreten könnte.

Beim ersten Ansatz würde eine Schnittstelle zwischen Sicherungslogik und Leittechnik überflüssig werden. Allerdings müsste die komplette Entscheidungsfindungslogik für die dispositiven Probleme in die Sicherungslogik integriert werden, wodurch das Entstehen komplexer Entscheidungsregeln in der Sicherungslogik wahrscheinlich wäre und somit die Sicherheitsnachweisführung und damit Zulassung verkompliziert wird. Alternativ könnte im umgekehrten Fall die Leittechnik keine komplexen Entscheidungsregeln enthalten und würde somit suboptimale Entscheidungen treffen bzw. vorbereiten. Zudem bestünde die Gefahr, dass bei zukünftigen Veränderungen der Entscheidungsfindungsregeln der Leittechnik auch die Sicherungstechnik angepasst werden müsste. Hierdurch wäre ein neuer Zulassungsprozess erforderlich, der hohe Kosten verursachen würde und viel Zeit benötigte. Dieser Ansatz widerspricht damit der Anforderung der *schlanken Logik*.

Beim zweiten Ansatz wäre zwar ein zusätzliches System erforderlich, dafür würden jedoch die geschilderten Nachteile des ersten Ansatzes nicht auftreten. Somit wäre im Falle von Änderungen der dispositiven Regelungen keine langwierige und kostenintensive Zulassung der Sicherungslogik durch die Aufsichtsbehörden erforderlich.

Die beschriebene klare Trennung zwischen TMS und Sicherungslogik erfüllt die spezifischen Anforderungen für die Systemdefinition eindeutig am besten, da die Sicherungslogik in diesem Szenario genau so umfangreich gestaltet werden kann, wie es notwendig ist und keine nicht sicherheitsrelevanten Funktionen enthalten muss. Außerdem kann so auch der voraussichtliche zukünftige Standard der RCA eingehalten werden (vgl. Anforderung der Zukunftsfähigkeit)[17]. Daher wird der zweite Ansatz weiterverfolgt.

Ablauf der Kommunikation zwischen Sicherungslogik und Leittechnik

Das übergeordnete Leitsystem, welches keine Sicherheitsrelevanz mehr hat, wird als „**Traffic Management System**“ (TMS) bezeichnet (vgl. Kapitel 2.4.3). Zum Teil wird auch die erweiterte Bezeichnung „**Capacity and Traffic Management System**“ (CTMS) verwendet, bei der neben dem eigentlichen TMS noch die Fahrplanerstellung inbegriffen ist.

Abb. 32 verdeutlicht die Aufgabengebiete von TMS und Sicherungslogik am Beispiel einer Fahrerlaubnisanfrage. Das TMS entscheidet auf Basis seiner Optimierung, wann ein Zug eine Fahrerlaubnis bekommen soll und welche Vorgaben diese beinhalten soll (Distanz, die gefahren werden darf, erlaubte Maximalgeschwindigkeiten etc.). Bevor die Fahrerlaubnis an den Zug übermittelt werden kann, muss das TMS hierzu bei der Sicherungslogik mittels einer **Fahrerlaubnisanfrage** eine Genehmigung einholen. Die Sicherungslogik prüft die Entscheidung darauf, ob sie zu einem unsicheren Zustand führt und leitet sie erst nach positiver Prüfung an das Fahrzeug weiter.

Analog wird mit einem Stellbefehl verfahren. Auch dieser würde vom TMS zunächst an die Sicherungslogik als **Stellanforderung** zur Prüfung übermittelt werden und erst nach erfolgreicher Prüfung von der Sicherungslogik als **Stellbefehl** an die Stellelemente weitergegeben werden.

[17]Eine solche Sicherungslogik wurde unter anderem seit 2016 im Rahmen des später so benannten Schweizer Branchenprogramms „smartRail 4.0“ vorgesehen (vgl. hierzu Kapitel 2.3.1 und SBB AG 2018) und ist auch unter der Bezeichnung „Sicherungslogik“ (engl. „Safety Logic“, Abkürzung in beiden Sprachen „SL“) in die RCA eingeflossen (vgl. Kapitel 2.4 und ERTMS Users Group und EULYNX 2019).

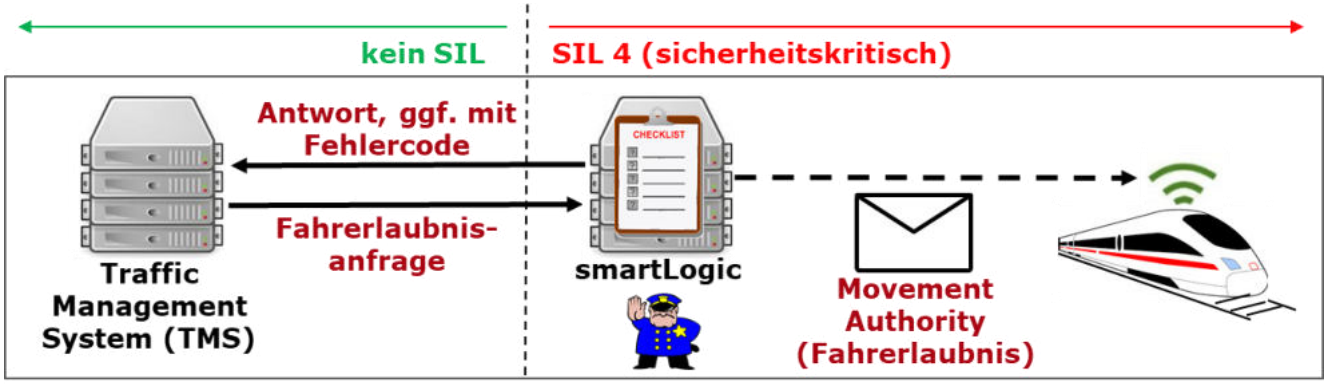


Abb. 32: Zusammenspiel von TMS und smartLogic
[Eigene Darstellung mit frei verfügbaren Cliparts]

Wieviel Intelligenz darf die Sicherungslogik haben?

Die genaue Abgrenzung zwischen Sicherungslogik und Leitsystem benötigt jedoch noch weiterer Erläuterung. Beispielsweise könnte die Sicherungslogik theoretisch bei einer nicht sicheren Prüfanfrage vom TMS selbstständig Kompensationsmaßnahmen, wie eine niedrigere Geschwindigkeit oder einen alternativen Fahrweg, auswählen (Lösungsmöglichkeit 1) anstatt die Prüfung mit negativem Ergebnis abzubrechen und die Entscheidung über mögliche Rückfallebenen dem Leitsystem zu überlassen (Lösungsmöglichkeit 2).

Durch das Vorgehen in Lösungsmöglichkeit 1 könnte wahrscheinlich aufgrund eingesparter Nachrichten besonders schnell auf das Problem reagiert werden. Allerdings würde die Anforderung der schlanken Logik verletzt, da für die Entscheidungsfindung durch die Sicherungslogik zusätzliche Komplexität in der Sicherungslogik notwendig wäre. Konsequenter wäre stattdessen Lösungsmöglichkeit 2, in der die Ablehnung der Prüfanfrage der Leittechnik nur mitgeteilt wird und die Leittechnik anhand ihrer Optimierungsregeln über das weitere Vorgehen und eine evtl. angepasste, erneute Prüfanfrage entscheidet.

Um den gewählten Ansatz der Aufgabentrennung zwischen Leittechnik und Sicherungslogik konsequent umzusetzen, sollte daher möglichst jegliche Entscheidungsgewalt – mit Ausnahme der Annahme oder Ablehnung einer Prüfanfrage durch die Sicherungslogik – bei der Leittechnik liegen.

4.3.2 Abgrenzung zur fahrzeugseitigen Sicherungstechnik und zu den Stellelementen

In diesem Kapitel wird die Aufgabenteilung zwischen fahrzeugseitiger und infrastrukturseitiger Sicherungstechnik sowie zu den Stellelementen bzw. deren Ansteuerungen („Object Controler“) diskutiert. Hierbei steht die grundsätzliche Fragestellung im Mittelpunkt, ob der umfangreichere Teil der Schutzfunktionen eher zentral (Zentralrechner auf Seiten der Infrastruktur) oder dezentral (Logik auf den Fahrzeugen und/oder auf den infrastrukturseitigen Feldelementen) übernommen werden soll. Diese Frage wird von Wissenschaft, Herstellern und Betreibern kontrovers diskutiert (vgl. z. B. [Fantechi et al. 2016; Guss 2016; Flamm & Scheier 2019]) und für den Bereich der Disposition z. B. [Cui et al. 2017], aus dem sich jedoch auch Argumente für den sicherheitsrelevanten Bereich übernehmen lassen, sowie den Abschnitt „dezentrale Ansätze“ in Kapitel 2.3.3).

Zunächst sollen die beiden Varianten in ihrer reinen Umsetzung vorgestellt werden. Anschließend erfolgt die Diskussion der Vor- und Nachteile. Zwischen rein zentralen und dezentralen Ansätzen sind auch hybride Ansätze denkbar, die im dritten Abschnitt besprochen werden. Abschließend folgt auf Basis der Diskussion im letzten Abschnitt die Wahl eines Ansatzes für das weitere Vorgehen.

Vorstellung der beiden (reinen) Ansätze

1. Beim zentralen Ansatz erfolgt die Kommunikation immer mit einer zentralen Infrastruktur (sowohl für die Leit- als auch für die Sicherungstechnik). Diese Infrastruktur ist für die Abstimmung der verschiedenen Zugfahrten untereinander verantwortlich und teilt die Ressourcen (zeitlich eingeschränktes Nutzungsrecht für Gleis- und sonstige Infrastruktur) zu. Weiterhin wacht die zentrale Infrastruktur darüber, dass die Zuteilung der Infrastrukturressourcen an die Fahrzeugbewegungen so geschieht, dass kein unsicherer Zustand eintritt (z. B. durch gleichzeitige Zuweisung der gleichen Infrastruktur an verschiedene Fahrzeuge oder einen falschen Status der Infrastruktur).
2. Beim dezentralen Ansatz stimmen sich die Fahrzeuge untereinander und/oder direkt mit den Stellelementen der Infrastruktur über deren Nutzung und Status ab. Zu unterscheiden ist dabei, ob es zumindest noch eine zentrale Verwaltungsinstanz gibt (Ansatz 2a), bei der die Fahrzeuge und Feldelemente registriert sind, oder ob die Fahrzeuge direkt miteinander kommunizieren und sich gegenseitig identifizieren müssen (Ansatz 2b).

Der Ansatz 2b ähnelt dem Individualverkehr, bei dem die Fahrzeuge als autonome Einheiten die Verkehrsinfrastruktur nutzen. Die Infrastruktur wird dabei nicht wie im Schienenverkehr exklusiv zugewiesen, sondern einem allgemeingültigen Regelwerk folgend von den Fahrzeugen genutzt. Die Eisenbahn unterscheidet sich jedoch durch die viel stärker limitierende Infrastruktur und die deutlich längere exklusive Beanspruchung der Gleise grundlegend vom Individualverkehr. Dies rechtfertigt die Annahme, dass zur möglichst optimalen Nutzung der Infrastruktur im Eisenbahnverkehr zumindest bei hohem Verkehrsaufkommen eine gewisse zentrale Planung erforderlich ist.

Vor- und Nachteile

In der Praxis finden derzeit dezentrale Verfahren wie der „Zugleitbetrieb“ ausschließlich auf einigen schwach befahrenen Nebenstrecken statt. Dezentrale Verfahren können dort wirtschaftliche Vorteile haben, wenn der Abstimmungsaufwand zwischen den Zügen gering ist, da auf zentrale Komponenten im Sinne der Zieldimension „*geringer Hardwareeinsatz*“ verzichtet werden kann (vgl. [Flamm & Scheier 2019]).

Auf Hauptstrecken nimmt dagegen der Abstimmungsaufwand stark zu, da viele Fahrzeugbewegungen über eine große Zahl stellbarer Feldelemente stattfinden. Würden die Fahrzeuge direkt und ohne Absprache mit einem zentralen Leitsystem (zur Möglichkeit eines zentralen Leitsystems und dezentraler Sicherungslogik siehe im übernächsten Absatz) die Infrastruktur allokieren, z. B. in Absprache mit dem Controller einer Weiche, wären entweder suboptimale Infrastrukturbeanspruchungen oder ein hoher Abspracheaufwand zwischen allen Beteiligten notwendig – zumindest dann, wenn es zu Abweichungen vom Fahrplan kommt.

Ein hoher Abspracheaufwand könnte in Hinblick auf die globale Anforderung der *geringen Latenz* nicht optimal sein. Allerdings sind Latenzzeiten ohne eine detaillierte Betrachtung der Hardwareplattformen und Kommunikationsinfrastruktur nur schwer quantifizierbar. Es kann jedoch davon ausgegangen werden, dass Latenzzeiten bei Übertragungen durch die Luft höher sind, als bei kabelgebundenen Übertragungen. Viele Funkübertragungen sind daher vor dem Hintergrund der Latenz-Anforderung nicht optimal.

Ein zentrales System kann bei zu geringer Dimensionierung auch zu einem Engpass (Flaschenhals) werden. Die zu übertragende Datenmenge, die Latenzzeiten und Bandbreiten der Kommunikationskanäle und die Performance der beteiligten Systeme sollten daher bei der Wahl zwischen zentralem und dezentralem Ansatz berücksichtigt werden.

Neben den Latenzzeiten hat die Frage einer dezentralen oder zentralen Logik auch auf die Flexibilität der Sicherungslogik bei notwendigen Veränderungen der Infrastruktur oder sonstiger Begebenheiten einen Einfluss (vgl. globale Anforderung der *flexiblen Infrastrukturzuordnung*). Dieser Einfluss hängt wesentlich von Aufbau und Funktionsweise der zentralen bzw. dezentralen Sicherungslogik ab. Würde eine dezentrale Logik beispielsweise ähnlich dem Spurplanprinzip bei Relaisstellwerken funktionieren, wäre es durchaus denkbar, dass einzelne Elemente ohne unverhältnismäßig hohen Aufwand hinzugefügt oder verändert werden können. Bei einer zentralen Logik könnte dies, z. B. bei Verwendung fester Fahrstraßentabellen, hingegen auch sehr kompliziert werden.

Ziel der Arbeit ist es jedoch, ein einfaches Prinzip zu finden. Von daher sollte im Falle einer zentralen Logik von einer möglichst einfachen Umsetzung ausgegangen werden, bei der die generische Sicherungslogik unabhängig von den konkreten Spurplandaten definiert ist und auf diese aus einer externen Quelle zugreift. Hierfür kann angenommen werden, dass flexible Änderungen an einer zentralen Stelle einfacher umzusetzen sind als bei einem dezentralen Konzept an mehreren Stellen. Dieses Argument wird umso stärker, wenn sich die Änderung nicht nur auf die beteiligten Infrastrukturelemente bezieht, sondern auf eine Änderung der generischen Grundlogik an sich.

Für die Anforderung der *Protokollierung* bietet eine zentrale Logik ebenfalls Vorteile, da nicht an jedem Feldelement eine erfolgreiche Protokollierung sichergestellt werden muss. Bei einem dezentralen System müssen die Kommunikationsströme für die Ursachenforschung bei Unfallereignissen erst genau ermittelt werden, während bei einem zentralen System diese in der Regel in der zentralen Stelle vorliegen.

Schwierig werden dezentrale Konzepte auch, wenn im Sinne der Anforderung *„Migrationsfähigkeit“* noch nicht alle Fahrzeuge mit der benötigten Technik ausgestattet sind. Während dieser Umstand im zentralen System durch einen größeren freigehaltenen Bereich mit einer angenommenen Position des nicht vollständig ortbaren Fahrzeuges durch eine konservative Positionsbestimmung kompensiert werden kann, wäre das dezentrale System vor Probleme gestellt. Natürlich wäre es möglich, dieses Problem mit entsprechenden zusätzlichen Fallunterscheidungen oder redundanter streckenseitiger Ortungstechnologie zu umgehen. Allerdings würde eine solche Umgehung wiederum zu einer nicht erwünschten Erhöhung der Komplexität der Sicherungstechnik führen (Anforderung der *schlanken Logik*).

Die Frage einer zentralen oder dezentralen Logik hat auch einen Einfluss auf die IT-Sicherheit, deren Betrachtung allerdings nicht Teil der Arbeit ist (vgl. Kapitel 3.5), weshalb es keine entsprechende Anforderung gibt. Der Vollständigkeit halber soll dennoch kurz darauf eingegangen werden. Bei einem Angriff sind zwei Gefahren zu unterscheiden. Zum einen existiert die primäre Gefahr eines Eingriffs, der zu einem Unfall führen kann, z. B. durch das Ändern eines Signalbegriffs. Zum anderen besteht die sekundäre Gefahr eines Betriebsstillstands aufgrund der Sicherheitsreaktion auf einen Angriff, um die primäre Gefahr zu vermeiden [AG CYSIS 2016]. Eine dezentrale Logik bietet aus Sicht der IT-Sicherheit den Vorteil, dass die Wahrscheinlichkeit großflächiger Folgen bei einem Angriff (bei einer ausreichend gut getrennten Kommunikationsarchitektur) geringer ist [AG CYSIS 2018]. Dagegen könnte es allerdings auch schwieriger sein, einen Angriff zu entdecken. Die Gefahr eines Betriebsstillstandes kann auch durch die redundante Auslegung einer zentralen Logik der Leit- und

Sicherheitstechnik reduziert werden. Das redundante Vorhalten der Logik dürfte wiederum bei wenigen zentralen Standorten einfacher sein.

Hybride Ansätze

Neben einer Festlegung auf eine rein zentrale oder dezentrale Architektur sind auch Hybridmodelle denkbar, bei denen Teilaufgaben der Sicherungstechnik zentral und andere Teilbereiche dezentral ausgeführt werden. Beispielsweise werden Ansätze diskutiert, in denen die Feldelemente zentral gesteuert und überwacht werden, die Fahrzeuge sich aber selbstständig um ihre Abstandshaltung kümmern, um Auffahrunfälle zu verhindern (vgl. z. B. [Flamm & Scheier 2019]). Hintergrund ist, dass bei der Kommunikation Latenzzeiten eingespart werden könnten, wenn die vorausfahrende Fahrzeugbewegung ihre aktuelle Position direkt an die nachfolgende Fahrzeugbewegung weitergibt.

Allerdings müssen beide Fahrzeuge auch weiterhin ihre Position an die zentrale Stelle melden und für eine sinnvolle und in Zukunft voraussichtlich verstärkt automatisiert durchgeführte ad hoc Disposition müssten Abstandsberechnungen auch von zentraler Seite aus durchgeführt werden. Insgesamt ist daher davon auszugehen, dass durch eine solche hybride Lösung mehr Kommunikation und Rechenaufwand entstehen. Es bleibt jedoch der Vorteil der geringeren Latenzzeiten bei Zugfolgefällen, die unmittelbar im Bremswegabstand aufeinander folgen.

Es wäre auch denkbar, das Leitsystem zentral und die Sicherungslogik dezentral anzulegen. In diesem Fall müssten sich die Fahrzeugbewegungen nicht untereinander darüber austauschen, wer welche Ressourcen in welchem Zeitraum nutzen darf. Allerdings müsste dann die Fahrzeugbewegung doppelt kommunizieren, sowohl mit dem zentralen Leitsystem, als auch mit den dezentralen Stellelementen. Hierbei würde im Vergleich zu einer ebenfalls zentralen Sicherungslogik wieder zusätzliche Kommunikation anfallen, insbesondere, falls eine Anfrage eines Stellelements durch eine Fahrzeugbewegung abgelehnt würde und die Fahrzeugbewegung nun erneut beim Leitsystem nach einer Alternative anfragen müsste.

Fazit

Die Diskussion zeigt, dass eine Koexistenz dezentraler und zentraler Leit- und Sicherungsansätze denkbar ist, je nach Art der betroffenen Strecke und Betriebsprogramm. Da jedoch die Mehrzahl der in Kapitel 3 geschilderten Optimierungspotenziale auf Hauptbahnen mit viel Verkehr gesehen werden, fokussiert diese Arbeit auf eine Architektur mit zentraler Sicherungslogik. Die Delegation des Folgefahrschutzes auf eine direkte Absprache zwischen Fahrzeugbewegungen in bestimmten Fällen (siehe hybrider Ansatz) wäre prinzipiell denkbar, wird allerdings an dieser Stelle als Spezialfall gesehen, der zwar nicht ausgeschlossen werden soll, aber im Folgenden aus Ressourcengründen nicht näher ausgeführt wird.

Abb. 33 fasst die wesentlichen Punkte der Diskussion (ohne die hybriden Ansätze) noch einmal zusammen.

Auch beim zentralen Ansatz haben die Fahrzeuge und Stellelemente eine Sicherheitsverantwortung. Sie sind zumindest dafür verantwortlich, die Parameter ihrer Fahrerlaubnis nicht zu überschreiten bzw. die Stellbefehle korrekt auszuführen und korrekte Informationen über ihren Status an die zentrale Sicherungslogik zu liefern. Diese Aufgaben sollten sie möglichst vollständig erfüllen, so dass keine unnötigen Ressourcen der Infrastruktur für sie reserviert werden müssen.

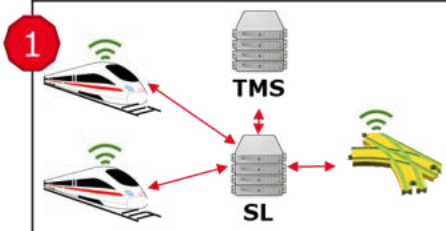
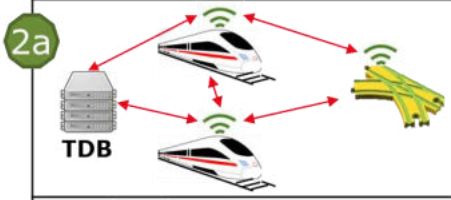
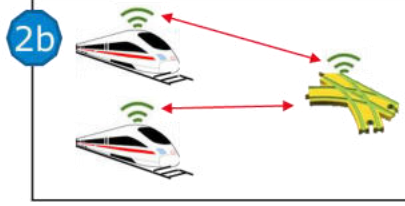
Ansatz	Vor- & Nachteile	mgl. Einsatzgebiete
	+ optimale Belegung der Infrastruktur möglich + Kommunikation schlank − angriffsgefährdet	(große) Knoten
	+ Züge können sich absprechen − viel Kommunikation ○ eher robust	▪ einfache Infrastrukturen ▪ längere Strecken-abschnitte zwischen Knoten
	+ schlanke Architektur − nicht kapazitätsoptimal − „Deadlock"-gefährdet + sehr robust	einfache Infrastrukturen

Abb. 33: Übersicht der Vor- und Nachteile zentraler bzw. dezentraler Logiken
[Eigene Darstellung]

4.3.3 Abgrenzung zur Sicherheit der Gleisinfrastruktur

Die Beschaffenheit des Bahnkörpers hat ebenfalls einen Einfluss auf die Sicherheit. Deshalb sollte abgegrenzt werden, wie die Grenze der Aufgaben der Sicherungslogik in Bezug auf die Sicherheit der Gleisinfrastruktur verläuft.

Wie bereits in der Einleitung zu Kapitel 4.3 festgestellt wurde, beschränkt sich die Sicherungstechnik auf die operative Einhaltung der Sicherheit während des Betriebes und nicht auf Einhaltung der Sicherheit während des Planungs- und Herstellungsprozesses der Eisenbahninfrastruktur. Demzufolge ist die Sicherungstechnik nicht für die Sicherheit des Bahnkörpers an sich verantwortlich. Sie kann allerdings Techniken umfassen, die während des Betriebes die Sicherheit des Bahnkörpers, zum Beispiel in Bezug auf Lageänderungen oder schädliche Naturereignisse wie Erdrutsche oder Unterspülungen, überwachen. Die Aufgabe der Sicherungslogik ist es dann, auf registrierte Abweichungen mit Maßnahmen zur Aufrechterhaltung der Sicherheit zu reagieren bzw. keine Fahrten in den gefährdeten Gleisbereich zuzulassen.

4.4 Datenquellen und Datenhaltung

Wie in Kapitel 4.1 festgestellt, gehört zur Abgrenzung des Systems auch der Bereich der Daten. Zu klären ist demnach, wie die benötigten Daten bereitgestellt und verwaltet werden sowie welche Daten benötigt werden, aus welchen Quellen die Daten kommen und in welcher Form sie zur Verfügung gestellt werden müssen. Bezogen auf die Verwaltung der Daten soll in Kapitel 4.4.1 zunächst geklärt werden, ob die Datenhaltung innerhalb oder außerhalb der smartLogic stattfinden soll. Welche Daten in welcher Qualität benötigt werden, soll nicht im Einzelnen, sondern nur allgemein in Kapitel 4.4.2 diskutiert werden, da eine Einzelbetrachtung an dieser Stelle der Arbeit zu umfangreich wäre. Stattdessen wird auf diese Einzelbetrachtung im Rahmen der Erarbeitung des Datenmodells in Kapitel 7 eingegangen.

Die Sicherungslogik benötigt unterschiedliche Daten, die aus unterschiedlichen Quellen stammen und unterschiedlich aufgebaut sind. Daher ist bezüglich der Quellen eine getrennte Analyse sinnvoll, die in den weiteren Unterkapiteln folgt. Dafür erschien keine bestimmte Reihenfolge erforderlich zu sein.

4.4.1 Datenhaltung innerhalb oder außerhalb der smartLogic

Wie in der Einleitung zu diesem Kapitel angeklungen, sollte zunächst geklärt werden, ob die Datenhaltung Bestandteil der smartLogic ist. In Kapitel 4.2 wurde als spezifische Anforderung für die Bewertung einer geeigneten Systemdefinition aus der globalen Anforderung der *generischen Logik* hergeleitet, dass die Datenmodule möglichst von der Sicherungslogik getrennt werden sollten. Dem entgegen steht die globale Anforderung der *geringen Latenz*, da die Latenzzeiten bei einer getrennten Anordnung länger sind.

Zahlreiche der in Kapitel 3 identifizierten Nutzenpotenziale basieren auf der Anforderung der generischen Logik. Da zwischen möglichen Datenhaltungssystemen und der Sicherungslogik keine Luftschnittstelle oder eine andere Schnittstelle mit hohen Latenzzeiten liegen muss, wird an dieser Stelle davon ausgegangen, dass akzeptable Latenzzeiten erzielt werden können. Zudem werden die Daten auch für das TMS benötigt. Somit ist in einer Abwägung der beiden Anforderungen die generische Logik ausschlaggebend und die Datenhaltung wird außerhalb der Sicherungslogik angeordnet. Die Latenzzeit sollte jedoch bei der Hardwarelösung und der genauen Gestaltung der Schnittstelle berücksichtigt werden.

4.4.2 Umfang und Qualität der benötigten Daten

Weiterhin kann der Umfang der benötigten Daten auf allgemeiner Ebene besprochen werden.

Mehr Daten führen prinzipiell zu genaueren Informationen, die wiederum zu einer optimierten Zuweisung der Infrastruktur an die einzelnen Zugfahrten und ein besseres Ausfahren der dazugehörigen Fahrerlaubnisse beitragen können. Aufgrund der Anforderung zu den Zieldimensionen „*hohe Kapazität*“ und „*hohe Robustheit*“ sollte daher die Logik mit möglichst vielen vorhandenen oder zukünftig voraussichtlich vorhandenen Daten arbeiten können.

Auf der anderen Seite wäre es nicht im Sinne der optimalen *Migrationsfähigkeit* und der *Robustheit*, wenn die smartLogic auf das Vorhandensein aller dieser Daten angewiesen wäre. Stattdessen sollte die smartLogic auch mit eingeschränkten Informationen umgehen können. Dies bedeutet, dass jeweils definiert sein sollte, welche Informationen auf jeden Fall benötigt werden und welche optional verfügbar sein können.

Bezüglich der Qualität der übermittelten Daten ist es erforderlich, dass die Informationen mit ausreichender Wahrscheinlichkeit zur sicheren Seite hin korrekt sind, z. B. dass die Position der Zugspitze hinreichend wahrscheinlich nicht vor dem übermittelten Punkt liegt oder die des Zugschlusses mit hinreichender Wahrscheinlichkeit nicht dahinter. Alternativ kann eine Angabe über die Güte der Information mitübermittelt werden, so dass die Sicherungslogik die Verwendbarkeit der Information bezogen auf die Güteanforderung für den jeweiligen Anwendungszweck prüfen kann.

4.4.3 Topologiedaten

In der bisherigen Arbeit wurde bereits hergeleitet, dass es sinnvoll ist, eine generische Grundlogik zu entwickeln, die unabhängig von der konkreten Ausprägung der Infrastruktur in Form der Topologie vor Ort ist. Hierzu wurde in Kapitel 3.5 auch eine globale Anforderung definiert. Die Grundlogik muss

jedoch mit der Infrastruktur vor Ort verknüpft werden. Die Topologie und die benötigten Infrastrukturdaten müssen also in einer geeigneten Quelle vorgehalten werden.

Auf Basis der Anforderungen können zwei Kriterien für die Gestaltung der Datenquelle aufgestellt werden:

Zum einen ist es für die Sicherheit sehr relevant, dass die gemeldete Topologie korrekt ist. Das heißt, es muss sichergestellt werden, dass die Infrastruktur vollständig und fehlerfrei erfasst wurde und immer aktuell ist. Zudem darf sie nicht manipulierbar sein. Zusammengefasst muss die Datenquelle sicher sein.

Zum anderen ist in Bezug auf die Latenzzeiten zu überlegen, wie oft und wann Daten mit der Sicherungslogik ausgetauscht werden. Dies spielt aus Performance-Gründen eine Rolle und ist für die Gestaltung der Schnittstelle relevant. Je häufiger der Zugriff erfolgt, desto wichtiger sind geringe Latenzzeiten in der Datenübertragung. Es kommen mehrere Möglichkeiten in Betracht.

- Bei jedem Prüfprozess wird die Topologie neu in die Sicherungslogik geladen, weil sich etwas geändert haben könnte.
- Bei der Durchführung von Prüfprozessen versichert sich die Sicherungslogik zu Beginn des Prozesses, dass keine Änderungen vorliegen.
- Die Infrastruktur- bzw. Topologiedatenquelle meldet sich, wenn Änderungen vorliegen.

Eines der grundlegenden Sicherheitsprinzipien der Eisenbahnsicherungstechnik besagt, dass Fehler sich offenbaren müssen (vgl. z. B. [Maschek 2013]). Dies ist erforderlich, um Folgefehler durch das Nichtentdecken eines Fehlers zu vermeiden. In diesem Sinne müsste für letzteren Fall zumindest sichergestellt werden, dass kein Ausfall der Datenquelle dazu führt, dass der Sicherungslogik vor einer wichtigen Entscheidung (wie der Durchführung eines Prüfprozesses) eine wichtige Information über die Infrastruktur vorenthalten wird. Aus diesem Grund ist zumindest eine Statussynchronisation im Rahmen von Prüfprozessen erforderlich. Es ist daher davon auszugehen, dass bei Prüfprozessen regelmäßiger Kontakt zur Topologiedatenquelle besteht. Daher sind hinreichend geringe Latenzzeiten notwendig.

Es wird in dieser Arbeit angenommen, dass eine Quelle für die Topologie existiert, welche die oben genannten Kriterien erfüllt. Wie diese Datenquelle genau aufgebaut ist und wie sie die Korrektheit und Manipulationsfreiheit der Daten sicherstellt, ist nicht Teil der Betrachtungen in dieser Arbeit.

4.4.4 Fahrzeugpositionen

Eine der größten Herausforderungen ist eine korrekte Ortung der Fahrzeuge. Eine solche Ortung ist für die Ressourcenzuteilung durch das Leitsystem gleichermaßen wie für den korrekten Beanspruchungsstatus der Infrastruktur wichtig. Je präziser die Ortung ist, desto weniger Infrastruktur muss aus Sicherheitsgründen einer einzelnen Fahrzeugbewegung gleichzeitig exklusiv zugewiesen werden. Dabei ist nicht nur die Zugspitze relevant, sondern auch der Zugschluss, um die Zugvollständigkeit sicherstellen und eine korrekte Freimeldung der Infrastruktur durchführen zu können.

Die Freimeldung erfolgte in der Vergangenheit über manuelles „Hinsehen“ und infrastrukturseitige Gleisfreimeldeeinrichtungen wie Achszähler und Gleisstromkreise. Mittlerweile sind diverse neuere Technologien in der Diskussion, die zum Teil auf Seiten der Infrastruktur und zum Teil auf Seiten der Fahrzeuge implementiert werden sollen (vgl. Kapitel 2.2.3).

Zum Zeitpunkt des Verfassens dieser Arbeit ist noch nicht absehbar, welche Technologie bzw. welche Technologien sich durchsetzen werden. Es ist auch möglich, dass sowohl infrastrukturseitige als auch fahrzeugseitige Technologien sich gegenseitig ergänzen werden, um eine hinreichende Genauigkeit der Positionsmeldung auch bei widrigen Umständen zu gewährleisten. Ein reines Verlassen auf den fahrzeugseitigen ETCS Position Report ist daher nicht zielführend.

Stattdessen wird angenommen, dass es als zusätzliche Komponente der Sicherungstechnik einen vorgelagerten **Ortungsinformationsaggregator** geben wird, der die zur Verfügung stehenden Ortungsinformationen bündelt und verlässliche Informationen zur Position der Zugspitze und zur Position des Zugschlusses liefert. Verlässlich meint hierbei im Falle der Zugspitze, dass ihre Position mit der notwendigen Wahrscheinlichkeit nicht vor dem gemeldeten Punkt liegt (vgl. „max safe front end“ bei ETCS) und im Falle des Zugschlusses mit der notwendigen Wahrscheinlichkeit nicht dahinter (vgl. „min safe rear end“ bei ETCS).

4.4.5 Fahrzeugdaten

Neben der Fahrzeugposition (und -integrität) können weitere Fahrzeugdaten vom Fahrzeug über ETCS ermittelt und verwertet werden. So können über das ETCS-Paket 11 „Validated Train Data“ unter anderem die Zugart (international train category), das Lademaßprofil, die Achslastkategorie, die Anzahl der Achsen, die unterstützten Stromsysteme und Zugsicherungssysteme, die Höchstgeschwindigkeit, der zulässige Überhöhungsfehlbetrag und die Zuglänge übertragen werden. Es ist aber auch denkbar, dass Fahrzeugdaten durch infrastrukturseitige Sensoren erfasst werden.

Viele dieser Informationen sind für die Leitebene zur Berechnung sinnvoller Fahrprofile von Bedeutung, allerdings könnten solche Fahrzeugdaten auch für die Sicherungslogik relevant sein. Besonders wichtig ist die eindeutige Identifizierung des Fahrzeugs. Gemäß der globalen Anforderung, wonach die physikalisch maximal mögliche Geschwindigkeit möglichst wenig eingeschränkt werden soll (*Ermöglichung maximaler Geschwindigkeit*), sind auch alle Informationen, die eine feinere Ausdifferenzierung der zulässigen Geschwindigkeit erlauben, von Interesse.

Ferner könnten infrastrukturseitig gewonnene Informationen über die Fahrzeuge verwertet werden, die dem Fahrzeug möglicherweise nicht hinreichend sicher bekannt sind, zum Beispiel beim Tunnelbegegnungsverbot die Zugart, die heute im Fahrzeug nur vom Tf eingegeben wird und damit fehleranfällig ist, oder auch eine ermittelte Zuglänge zum Abgleich mit der im Bordcomputer eingegebenen Länge. Auch Informationen zu Fahrzeugen, die von Sensoren wie Heißläuferortungsanlagen kommen, können für die Sicherungslogik von Relevanz sein.

Informationen zu den Fahrzeugen können auch erforderlich sein, um das Befolgen fahrzeugspezifischer Vorgaben sicherzustellen. Beispiele könnten Befahrbarkeitsverbote für bestimmte Abschnitte, z. B. ohne Oberleitung oder ohne Wirbelstrombremse sein, aber auch Informationen wie, dass Trittstufen nicht ausgefahren werden dürfen oder das an festgelegten Orten zu Pfeifen ist. Bei solchen fahrzeugspezifischen Vorgaben stellt sich jeweils die Frage, ob die Einhaltung der Vorgaben fahrzeugseitig oder infrastrukturseitig sichergestellt wird. Bei infrastrukturseitiger Sicherstellung müssen sichere Informationen zum Fahrzeug vorliegen, bei der fahrzeugseitigen Sicherstellung muss die Sicherungslogik die korrekte Übertragung aller Vorgaben an das Fahrzeug gewährleisten.

Um die Verfügbarkeit von Fahrzeugdaten zu erhöhen, sollten fahrzeugseitige und infrastrukturseitige Informationen kombiniert werden. Dies könnte wie bei der Ortung in einem Aggregator geschehen. Aufgrund der Anforderung der hinreichend sicher korrekten Daten, muss die Fahrzeugdatenaggregator-Komponente im sicherheitsrelevanten Bereich angeordnet sein. Das Projekt smartLogic geht davon aus, dass eine solche sichere Datenquelle für Fahrzeugdaten vorhanden ist.

Woher die Fahrzeugdaten dabei genau stammen, ist außerhalb des Betrachtungsraums dieser Arbeit (vgl. Kapitel 3.3).

4.4.6 Fahrplandaten

Auch die Fahrplandaten kommen wie die anderen Daten aus einer externen Quelle, deren Existenz vorausgesetzt wird. Allerdings werden Fahrplandaten gemäß der in Kapitel 4.3.1 hergeleiteten Aufteilung zwischen Leittechnik und Sicherungslogik nur für die Leittechnik benötigt. Die Sicherungslogik erhält gemäß ihrer Aufgabe als Kontrollinstanz zwischen dem TMS und den Stellelementen ihre Anfragen ausschließlich auf Basis der Echtzeit-Planung durch das TMS. Deshalb müssen die Fahrplandaten auch nicht wie die anderen Daten aus einer „signaltechnisch“ sicheren Quelle stammen.

4.5 Schnittstellen der Sicherungslogik zu den Umsystemen

Bestandteil der Phase der Systemdefinition ist nach [DIN EN 50126-1:2017] auch die Festlegung der Schnittstellen zu den Umsystemen. Die globalen Anforderungen fordern hierbei, möglichst auf Standardschnittstellen zurückzugreifen. Die Schnittstellen sollten sich vom Umfang her auf das Wesentliche beschränken, um späteren Obsoleszenz-Problemen vorzugreifen (vgl. [Klöters & Herten 2017]), ohne dabei jedoch die Funktionalität der Sicherungslogik einzuschränken. Im Mittelpunkt der Schnittstellenbetrachtung steht die zu entwickelnde Sicherungslogik als Kern der infrastrukturseitigen Sicherungstechnik. Im Folgenden wird die Ausgestaltung der Schnittstellen zur Sicherungslogik diskutiert.

4.5.1 … zu den Stellelementen

Die Schnittstelle von der Sicherungslogik zu den Stellelementen wurde klassischerweise direkt über Drahtzüge oder später Kupferkabel hergestellt. Beide Wege bedingen eine maximale Stellentfernung[18]. Ist die direkte Verbindung unterbrochen, fällt das verbundene Element in einen sicheren Zustand und das System muss in eine Rückfallebene übergehen. Im Rahmen der europäischen EULYNX-Initiative befindet sich in Deutschland derzeit die Anbindung der Stellelemente über einen ringförmigen Datenbus in der prototypischen Ausrüstungsphase (vgl. Kapitel 2.2.5).

Da eine neue Sicherungslogik alte Stellwerke ersetzen wird und alte Feldelemente nicht standardisiert ansteuerbar sind, muss kein Fokus auf die Migrationsfähigkeit zu möglichst vielen Alttechnologien in diesem Bereich gelegt werden. Stattdessen ist im Sinne der Anforderung der Zukunftsfähigkeit die Kompatibilität zur zukünftigen Standard-Technologie zur Ansteuerung der Feldelemente wichtig. Derzeit ist davon auszugehen, dass sich die EULYNX-Schnittstellen in den nächsten Jahren in Europa als Standard durchsetzen werden. In Deutschland wird das Konzept in den neuen digitalen Stellwerken (DSTWs) umgesetzt. Aus diesen Gründen erscheint es sinnvoll, bei der Sicherungslogik auf die EULYNX-Schnittstellen zu den Feldelementen zurückzugreifen.

Für die zusätzliche Herausforderung der IT-Sicherheit wird davon ausgegangen, dass eine entsprechende Schutzschicht existieren wird, die jedoch die Funktionsweise der Sicherungslogik an sich nicht beeinflussen wird. Derzeit gibt es intensive, erfolgsversprechende Forschungsbemühungen in diesem Bereich, welche die formulierte Annahme rechtfertigen (vgl. z. B. [Krauß et al. 2020]).

[18] Zu beachten ist, dass sich die Sicherungslogik nicht am Ort des Bedienplatzes befinden muss; Stellwerke können auch ferngesteuert werden.

4.5.2 … zum Fahrzeug

Die Schnittstelle zum Fahrzeug besitzt eine besondere Bedeutung, da sich das Fahrzeug über große Entfernungen bewegen soll und dabei normalerweise mehrere Infrastrukturbereiche und manchmal sogar mehrere Länder passiert. Gerade in letzterem Fall bemüht sich die Europäische Union seit Jahren mit dem europäischen Zugleit- und -sicherungssystem ERTMS und seinem Bestandteil ETCS eine einheitliche Schnittstelle zwischen Fahrzeug und Infrastruktur zu schaffen, die europaweit gültig ist (vgl. zu ETCS Kapitel 2.2.2). Deswegen ist es sinnvoll, analog der globalen Anforderung möglichst generische Standardschnittstellen zu verwenden, bei der Kommunikation zum Fahrzeug auf ETCS zurückzugreifen. ETCS bietet zudem bereits einen sehr großen Funktionsumfang, um Informationen zwischen Fahrzeug und Infrastruktur auszutauschen.

Eine vergleichbar flexible Schnittstelle, die für den Datenaustausch in Frage kommen würde, existiert derzeit nicht. Sollte sich durch die Logikentwicklung dennoch Anpassungsbedarf an der Schnittstelle ergeben, besteht die Möglichkeit über sogenannte „***Change Requests***“ Änderungsvorschläge für ETCS einzubringen.

ETCS verfügt über mehrere Kommunikationswege zwischen Infrastruktur und Fahrzeug. Hierzu gehören ***Balisen***, ***Euroloop*** und die ***Funkübertragung*** über das „*Radio Block Center*“ (RBC) als Funkzentrale. Wie die Daten übertragen werden, spiegelt sich im Betriebslevel wieder (vgl. Kapitel 2.2.2). Für die Entwicklung der neuen Sicherungslogik ist zu überlegen, mit welchem Betriebslevel die Sicherungslogik arbeiten können soll und ob bei Level 2 bzw. 3 eine Trennung zwischen Sicherungslogik und RBC noch sinnvoll ist.

Unterstützte ETCS-Betriebslevel

Betrieblich sind höhere ETCS Levels den niedrigeren überlegen (vgl. Kapitel 2.2.2). ETCS Level 3 ist jedoch vorerst als allein unterstütztes System unrealistisch (vgl. Kapitel 2.2.3). Bezogen auf die Schnittstelle Fahrzeug-Infrastruktur unterscheiden sich ETCS Level 2 und Level 3 allerdings ohnehin nicht, sondern nur in Bezug auf die Gleisfreimeldung (vgl. [ERA 2016]).

Haupthindernisse für ETCS Level 2 sind derzeit der aktuelle Funkkommunikationsstandard innerhalb von ERTMS (GSM-R), der jedoch mittelfristig durch das Future Railway Mobile Communication System (FRMCS) abgelöst werden soll (vgl. Kapitel 2.2.4), und ältere Stellwerke, die mit ETCS Level 2 nicht kompatibel sind (jedoch mit Level 1 im Modus „Limited Supervision“). Diese Hindernisse kommen jedoch aus Sicht der smartLogic nicht mehr zum Tragen, da von der Einführung eines FRMCS in absehbarer Zeit ausgegangen werden kann und die spezifischen Anforderungen von ETCS Level 2 bzw. 3 bei einer Neuentwicklung der Sicherungslogik bereits berücksichtigt werden können.

In dieser Arbeit wird als Schnittstelle zum Fahrzeug also hauptsächlich ETCS Level 2 bzw. ETCS Level 3 betrachtet. Im Sinne der Migrationsfähigkeit sollte im Laufe der Logik-Entwicklung zudem geprüft werden, inwieweit eine Kompatibilität mit ETCS Level 1 mit balisenbasierter Datenübertragung (bzw. Datenübertragung mittels Euroloop) gewährleistet werden kann.

Sinnhaftigkeit der Trennung zwischen RBC und Sicherungslogik

Die Trennung von Stellwerken und damit Sicherungslogik und RBC bietet den Vorteil, dass ETCS Level 2 mit einem RBC mit mehreren neuen und vor allem auch bestehenden Stellwerken zusammenarbeiten kann. Diese Zusammenarbeit ist bisher erforderlich, da ETCS i. d. R. auf Bestandsstrecken mit bestehenden Stellwerken verschiedener Bauarten aufgesetzt wurde bzw. wird. Nachteile der Trennung können in höheren Signallaufzeiten, einer geringeren betrieblichen Flexibilität

durch begrenzte Bewertungsmöglichkeiten in Folge einer begrenzten Schnittstelle und ggf. höheren Kosten liegen.

Da der Hauptgrund für die Trennung von Stellwerk/Sicherungslogik und RBC in Kompatibilitätsüberlegungen zu den bisherigen Stellwerken und nicht in betrieblichen oder operationellen Vorteilen liegt, erscheint eine solche Trennung für die Neuentwicklung der smartLogic nicht sinnvoll. Stattdessen wird davon ausgegangen, dass die Sicherungslogik direkt ETCS-kompatible Nachrichten generieren kann, die dann von einem einfachen Serialisierer in ETCS-Nachrichten umgewandelt werden und über die von ETCS bereitgestellten Kommunikationswege an die Fahrzeuge übermittelt werden können.

4.5.3 ... zum Traffic Management System

Für die Schnittstelle zwischen der Sicherungslogik und dem Traffic Management System (TMS) als Leittechniksystem gibt es noch keine definierte Standardschnittstelle. Über die Schnittstelle müssen gemäß der in Kapitel 4.3.1 hergeleiteten Aufgabenteilung zwischen Sicherungslogik und dem Leittechniksystem die Anträge für Zustandsänderungen der Infrastruktur bzw. von Fahrzeugen übermittelt werden, die anschließend von der Sicherungslogik in Hinblick auf ihre Auswirkungen auf die Sicherheit geprüft werden.

Die genaue Ausgestaltung der Schnittstelle hängt vom noch zu ermittelnden Funktionsumfang der Sicherungslogik ab (siehe Kapitel 6). Um die Einbettung der Sicherungslogik in ihre Umsysteme vollständig herleiten zu können, erscheint es jedoch sinnvoll, die Rahmenbedingungen für die Schnittstelle bereits an dieser Stelle der Arbeit zu analysieren.

Wie bereits in Kapitel 4.3.1 angeklungen ist, werden über die Schnittstelle auf jeden Fall Fahrerlaubnisanfragen und Stellanforderungen übermittelt. Um die über die Schnittstelle zu übertragenden Informationen bestimmen zu können, ist deshalb zu entscheiden, welche Aufgaben von der Sicherungslogik und welche vom TMS im Rahmen dieser Prüfung erledigt werden müssen. Nachfolgende Auflistung enthält beispielhaft einige solcher Aufgaben:

- Im Fall der Fahrerlaubnisanfragen sollen Fahrzeugbewegung von einem bekannten Punkt (der aktuellen Position des zu bewegenden Fahrzeugs) zu einem anderen in der Anfrage festgelegten Punkt zugelassen werden. Um diesen Zielpunkt zu erreichen sind gegebenenfalls mehrere Fahrwege verfügbar. Ist Letzteres der Fall, muss entweder das TMS oder die Sicherungslogik einen Fahrweg auswählen.
- Für die Fahrerlaubnis muss ein Profil erlaubter Geschwindigkeiten berechnet werden.
- Möglicherweise müssen Schutzelemente bestimmt und deren Status ebenfalls verändert werden.
- Gegebenenfalls müssen bei Nichtverfügbarkeit einzelner benötigter Ressourcen oder einschränkender äußerer Umstände Einschränkungen für die Fahrerlaubnis definiert werden.

Je nachdem, ob bereits das TMS für diese Aufgaben zuständig ist oder die Sicherungslogik, müssten mehr oder weniger Informationen über die Schnittstelle übertragen werden. Die beiden Extremfälle für die Fahrerlaubnisanfrage sehen demnach wie folgt aus:

1. Die Fahrerlaubnisanfrage an die smartLogic enthält nur den Zielpunkt und eine Fahrzeugreferenz. Alle anderen für die Erstellung der an das Fahrzeug zu

übertragenden Fahrerlaubnis benötigten Informationen müssten dann von der Sicherungslogik selbst zusammengestellt werden.

2. Die Fahrerlaubnisanfrage enthält bereits die komplette Fahrerlaubnis, die bei positiver Prüfung an das Fahrzeug übertragen wird, mit allen dazugehörigen Informationen (Geschwindigkeitsprofil, Modusprofil etc.) sowie die Fahrzeugreferenz und eine Beschreibung des kompletten zu befahrenden Weges.

Der erste Extremfall hätte den Vorteil seiner Schlichtheit auf Seite der Schnittstelle. Eine einfache Schnittstelle ist aus Obsoleszenz-Gründen wünschenswert (vgl. [Klöters & Herten 2017; Sezgün 2017]). Weiterhin muss die Sicherungslogik in jedem Fall den Status der beteiligten Feldelemente und auch z. B. das Geschwindigkeitsprofil prüfen, so dass ein gewisser Kommunikations- und Berechnungsaufwand auf Seiten der Sicherungslogik ohnehin anfällt. Eine Vorberechnung durch das TMS könnte zu unnötigen Doppelberechnungen führen.

Die globale Anforderung der *schlanken Logik* spricht dagegen für eine Auslagerung möglichst vieler Funktionen in die nicht sicherheitsrelevante Leitebene und eine Beschränkung der Sicherungslogik auf ihre reine Prüfaufgabe (vgl. insbesondere das Ergebnis der Überlegungen in Kapitel 4.3.1), wie es im zweiten Extremfall der Fall ist. Dieses Vorgehen hat auch den Vorteil, dass die komplette Entscheidungsgewalt, zum Beispiel bezüglich des konkreten Geschwindigkeitsprofils oder der Art von einschränkenden Maßnahmen bei eingeschränkter Ressourcenverfügbarkeit (z. B. Ausfall eines Flankenschutzelements), beim TMS liegt. So wäre es beispielsweise prinzipiell denkbar, dass aus leittechnischen Gründen eine niedrigere als die theoretisch mögliche Geschwindigkeit erlaubt werden soll und deshalb die Fahrerlaubnis mit diesem niedrigeren Geschwindigkeitsprofil beantragt wird.

Aufgrund der hohen Gewichtung der Anforderung der *schlanken Logik* in dieser Arbeit werden die Nachteile der komplexeren Schnittstelle in Kauf genommen und der zweite Extremfall weiterverfolgt. Auch hybride Lösungen erscheinen nicht zielführend, da sie in jedem Fall die Anforderung der *schlanken Logik* verletzen würden.

Um dem Obsoleszenz-Problem zu begegnen, sollte bei der Definition der Funktionen in Kapitel 6 auf eine möglichst generische Beschreibung geachtet werden. Zudem sollte bei der genauen Gestaltung der Schnittstelle darauf geachtet werden, dass keine nicht benötigten Informationen durch die Definition der Schnittstelle als obligatorisch vorgeschrieben werden und somit unnötig übertragen werden müssen. Es erscheint auch sinnvoll, dass sich Form und Inhalt der zu übertragenden Daten an den bekannten Schnittstellen von ETCS und EULYNX orientieren, da nach der Prüfung die Daten über diese Schnittstellen weitergegeben werden müssen.

GRAU hat in seiner Masterarbeit in Zusammenhang mit dieser Promotion den Aufbau der TMS-Schnittstelle im Kontext des Prozesses der Fahrerlaubnisprüfung in Kapitel 5 seiner Arbeit näher untersucht [Grau 2018].

4.5.4 … zum Bediener

Gemäß der globalen Anforderungen soll die Sicherungslogik weitestgehend automatisiert arbeiten (vgl. Kapitel 3.5). Dies gilt insbesondere auch für die Rückfallebenen, in denen nicht alle gewünschten Informationen vorliegen oder Stellelemente bzw. einzelne ihrer Status nicht verfügbar sind. Durch die einfache Aufgabenstellung der Sicherungslogik, zu überprüfen, ob Anfragen sicher sind und entsprechend Rückmeldungen zu geben, sind Deadlocks unwahrscheinlich. Dennoch können sie an dieser Stelle nicht ganz ausgeschlossen werden. Von daher sind in gewissen Ausnahmefällen Bedienhandlungen denkbar, welche in die Sicherungslogik eingreifen. In solchen Fällen, muss deren

Sicherheit (sichere Anzeige, wohlüberlegte Handlung, sichere Übertragung, sichere Protokollierung, sichere Authentifizierung) wie bei bisherigen elektronischen Stellwerken sichergestellt werden, wobei hier angenommen wird, dass diese Aufgabe beim Bedienplatzsystem angesiedelt ist.

4.5.5 ... zum Nachbarstellrechner

Aus verschiedenen Gründen (Performance, Ausfallsicherheit, Angriffssicherheit, andauernde Migration, Herstellerdiversifikation, ...) wird nicht eine Sicherungslogik für das komplette Netz zuständig sein. Daher muss es auch Schnittstellen zu den Nachbarstellwerken geben. Bisherige solche Schnittstellen und auch die EULYNX-Schnittstelle SCI-ILS basieren auf der Blocklogik, die in dieser Arbeit für die neue Sicherungslogik nicht mehr als gegeben angenommen wird. Aus Migrationsgründen ist eine Kompatibilität zu klassischen Blockschnittstellen aber sinnvoll und sollte bei der Zusammenstellung des Funktionsumfangs der neuen Sicherungslogik berücksichtigt werden.

Die Kommunikation zu einer weiteren (neuen) Sicherungslogik ohne Blocklogik sollte aber nicht über eine Blockschnittstelle erfolgen, da sonst die Vorteile des Wegfalls der Blöcke in diesem Übergang unnötigerweise nicht genutzt werden könnten. Aus diesem Grund ist eine neue Schnittstelle erforderlich. Diese spielt allerdings für die grundsätzliche Funktionsweise der zu entwickelnden Sicherungslogik keine Rolle und wird daher hier aufgrund der äußeren Rahmenbedingungen bei der Erstellung dieser Arbeit (vgl. Kapitel 3.6.1) nicht weiter diskutiert.

4.5.6 Weitere Schnittstellen

Es sind weitere Schnittstellen denkbar, beispielsweise zur Registrierung oder Deregistrierung externer Systeme, zur Meldung von Ereignissen oder zur Aktualisierung von Variablen durch externe Systeme wie beispielsweise Wetterüberwachungssysteme. Da der genaue Funktionsumfang jedoch erst noch ermittelt wird (siehe Kapitel 6), kann an dieser Stelle keine vollständige Liste erfolgen. Eine Liste könnte ohnehin nicht vollständig sein, da es in der Zukunft neue funktionale Anforderungen an die Sicherungslogik, beispielsweise durch die Entwicklung neuer Technologien, geben könnte. Vor diesen Hintergrund ist es sinnvoll, weitere Schnittstellen möglichst generisch zu halten. Dieser Aspekt wird in der weiteren Entwicklung berücksichtigt werden (siehe vor allem Kapitel 8.3.3).

4.6 Zusammenfassung der Einbettung der Sicherungslogik in die Gesamt-Architektur

Die im vorigen Teil dieses Hauptkapitels beschriebenen Überlegungen führen zur in Abb. 34 dargestellten Einbettung der Sicherungslogik in die Gesamt-Architektur der zukünftigen Leit- und Sicherungstechnik. Es handelt sich dabei um eine Übersichtsgrafik, die nicht den Anspruch erhebt alle Kommunikationsströme vollständig darzustellen.

Es wird streng unterschieden zwischen Komponenten, die sich im **sicherheitskritischen Bereich** befinden, für den gemäß Norm [DIN EN 50129:2018 + AC:2019, Anhang A] Sicherheitsintegritätslevel 4 (SIL 4) gilt, und Komponenten im **nicht sicherheitskritischen Bereich** (in der Abbildung mit „kein SIL“ bezeichnet). Die Trennung ist in der Abbildung durch eine gestrichelte Linie dargestellt.

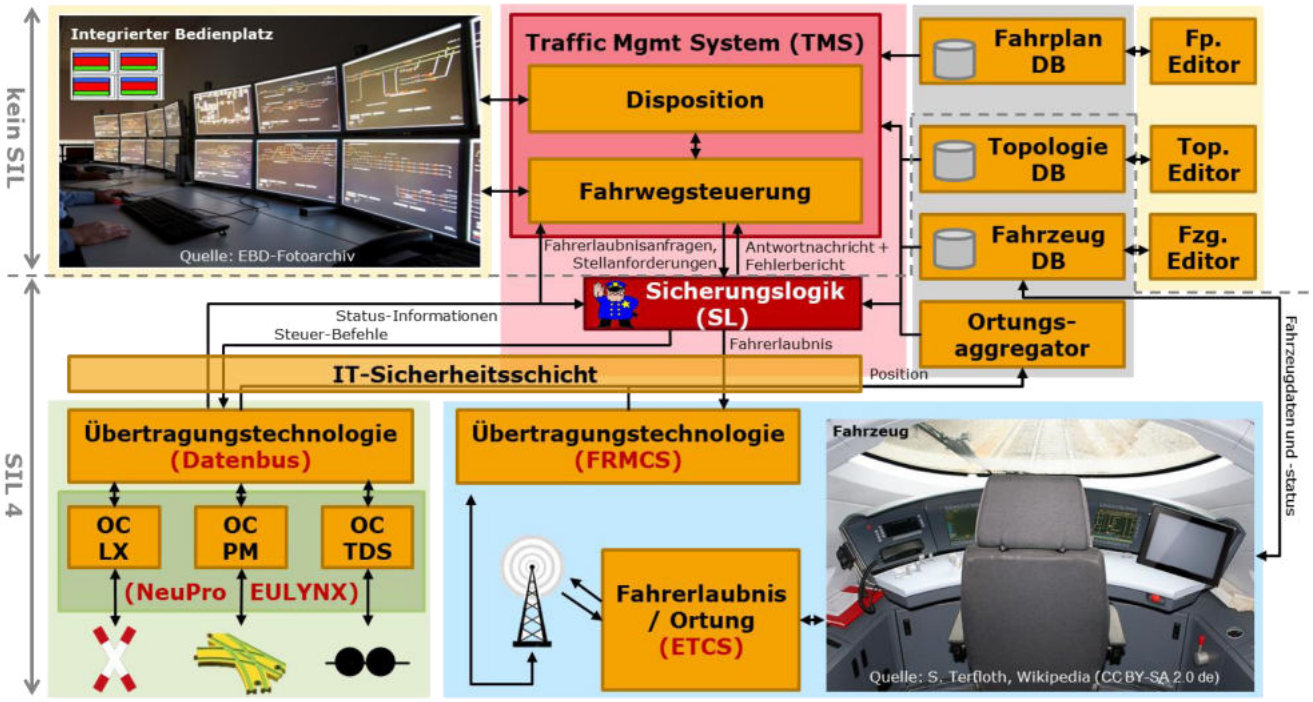


Abb. 34: Einbettung der Sicherungslogik in die Umsysteme
Weiterentwicklung aus: [Düpmeier 2018]

In der Mitte der Betrachtung steht die **Sicherungslogik (SL)** als zentrale Komponente der infrastrukturseitigen Sicherungstechnik. Ihre Aufgabe ist, jegliche Eingabe aus dem nicht sicherheitskritischen Bereich daraufhin zu überprüfen, ob sie zu einem unsicheren Zustand führt. Die gesamte „Intelligenz“ bezüglich der Wahl des optimalen Fahrwegs und der Bestimmung der optimalen Fahrerlaubnisse liegt jedoch in einem übergeordneten **Traffic Management System (TMS)** im nicht sicherheitskritischen Bereich. Die Sicherungslogik fungiert damit nur als „Türwächterin“, welche die Kommunikation zwischen dem TMS sowie den Komponenten der Außenanlage (grün dargestellt) und den Fahrzeugen (blau dargestellt) überwacht.

Das TMS umfasst dabei sowohl die **Fahrwegsteuerung**, die klassischerweise beim Fahrdienstleiter liegt (bzw. teilweise von der Zuglenkung übernommen wird), als auch Teile der übergeordneten **Disposition**, von deren fortschreitender Automatisierung ausgegangen wird. Die genaue Aufgabenteilung zwischen diesen beiden Bestandteilen des TMS ist allerdings für die Entwicklung der Sicherungslogik nicht relevant. Der rote Bereich orientiert sich an den bisherigen Aufgaben der Zentralstellen/Stellwerke und verdeutlicht somit, dass in der Zentralstelle eine neue Aufgabenteilung angestrebt wird. TMS und Sicherungslogik kommunizieren über eine noch zu entwickelnde Schnittstelle und tauschen zu prüfende Zustandsänderungswünsche des TMS und Antwortnachrichten mit detaillierten Fehlercodes der SL aus.

Das TMS ist nicht mit dem **Control Center** (in der Grafik gelb hinterlegt) zu verwechseln, in dem sich die menschlichen Aufsichtspersonen befinden. Dies ist eine separate Systemkomponente. Sie muss sich nicht am selben Ort befinden und ist ebenfalls über eine standardisierte Schnittstelle an das TMS angebunden, deren konkrete Ausgestaltung für die vorliegende Arbeit nicht von Relevanz ist.

Da die Sicherungslogik wie oben beschrieben unabhängig von der örtlichen Infrastruktur sein soll, muss die **Gleistopologie** aus einer sicheren Quelle (grau dargestellt) zugeliefert werden. Auch verwendbare **Fahrzeugdaten** müssen aus einer solchen sicheren Quelle stammen, wobei damit nicht festgelegt ist, ob dies das Fahrzeug selber oder eine entsprechende Datenbank ist. Woher die sicheren Daten stammen, wird hier generell nicht betrachtet, sondern es wird angenommen, dass diese zur

Verfügung stehen. Die Ortungsinformationen zu den Fahrzeugen stammen aus einem **Ortungsinformationsaggregator**, der seine Daten ebenfalls aus verschiedenen Quellen beziehen kann. Es werden Informationen zur Position der Zugspitze und des Zugschlusses geliefert mit einer Angabe wie sicher diese Informationen sind.

Es wird davon ausgegangen, dass die einzelnen Controller der **Infrastrukturobjekte** (in der Grafik grün hinterlegt) über standardisierte Schnittstellen über einen Datenbus angesteuert werden. Bezüglich der Schnittstellen wird auf die **EULYNX-Schnittstellen** zurückgegriffen (vgl. Kapitel 2.2.5). Schnittstellen zu möglichen weiteren externen Systemen auf der Infrastruktur (später in der Arbeit als Stakeholder-Systeme klassifiziert, vgl. Kapitel 8.3.3) wie Sensoren müssen ggf. noch entwickelt werden.

Als Schnittstelle zum **Fahrzeug** (in der Grafik blau hinterlegt) wird auf **ETCS** zurückgegriffen. Es wird davon ausgegangen, dass die Fahrzeuge Level 2 nutzen können. Die übermittelten Position Reports und Fahrzeugdaten dienen den entsprechenden Datenmodulen als Input. Eine separate Komponente **RBC** ist nicht mehr vorgesehen.

Die zu entwickelnde Sicherungslogik soll auch auf **automatisiertes Fahren (ATO)** in allen Automatisierungsstufen vorbereitet sein. Ob dabei die ATO-relevanten Daten über eine separate Schnittstelle, wie es derzeit europaweit angedacht ist (vgl. Kapitel 2.2.7), übertragen werden oder aus der ohnehin vorhandenen sicheren Fahrerlaubnis hergeleitet werden, spielt für die Gestaltung der Sicherungslogik keine Rolle.

Die Kommunikation erfolgt über eine geeignete **Übertragungstechnologie**. Für die Funkkommunikation zu den Fahrzeugen wird davon ausgegangen, dass ein leistungsfähiges **Future Railway Mobile Communication System (FRMCS)** zur Verfügung steht (vgl. Kapitel 2.2.4). Weiterhin wird davon ausgegangen, dass die **IT-Sicherheit** gewährleistet werden kann.

4.7 Ergebnisdiskussion

Die beschriebene Gesamt-Architektur verfolgt einen zentralen Sicherungsansatz über eine zentrale Sicherungslogik. Dies erfolgt vor allem, um eine schnelle Verarbeitung und eine gute Koordination der Fahrerlaubnisanfragen und Stellanforderungen zu ermöglichen. Die zentrale Stelle muss allerdings performant und redundant ausgeführt werden, um dem Risiko tiefgreifender Folgen durch einen technischen oder vorsätzlich herbeigeführten Ausfall vorzubeugen.

Durch die klare Trennung der sicherheits- und nicht sicherheitskritischen Aufgaben kann die Sicherungslogik optimal zugeschnitten werden. Diese Unterscheidung kann jedoch auch Doppelberechnungen notwendig machen. Ein Performance-Engpass wird hierdurch aufgrund der begrenzten Anzahl von Operationen jedoch nicht vermutet, so dass die Anforderung der schlanken Sicherungslogik höher gewichtet wurde.

Die externen Datenquellen für Fahrzeug- und Topologiedaten ermöglichen es, die Logik generisch auszuführen. Hierbei stellt sich die Frage, wie die Qualität dieser Daten gesichert werden kann. Diese Frage wurde in der vorliegenden Arbeit ausgeklammert. Von daher besteht ein Risiko für die zu entwickelnde Sicherungslogik darin, dass entsprechende sichere Quellen nicht vorhanden sind.

Die Verfügbarkeit der Daten kann durch die Möglichkeit der Kombination von fahrzeug- und infrastrukturseitigen Datenquellen, insbesondere bei der Ortung, erhöht werden. Um das Ziel der Robustheit bestmöglich zu erfüllen, muss die zu entwickelnde Logik jedoch auch mit der Nichtverfügbarkeit gewünschter Daten umgehen können.

Die beschriebene Systemdefinition der Sicherungslogik erfüllt die Anforderung, auf generische Standardschnittstellen zurückzugreifen, weitgehend. Bei der Schnittstelle zwischen SL und TMS besteht jedoch ein Obsoleszenzrisiko, welches im Folgenden durch geeignete Maßnahmen geringgehalten werden muss. Bei ETCS und EULYNX wird dieses Risiko geringer eingeschätzt, da die Schnittstellen bereits sehr ausgefeilt sind. Derzeit sind zwar noch einige Veränderungen durch „Change Requests“ zu erwarten, allerdings ist nicht davon auszugehen, dass dadurch die grundsätzliche Funktionsweise in Frage gestellt wird. Stattdessen handelt es sich um neue Funktionalitäten, die ergänzt werden, und somit kein Problem für die zu entwickelnde Sicherungslogik darstellen.

4.8 Vergleich mit alternativen Architektur-Ansätzen

Die hier erarbeitete Gesamt-Architektur wurde im Rahmen dieser Promotion bereits in den Jahren 2016 und 2017 erarbeitet und auf dem Scientific Railway Signalling Symposium 2017 vorgestellt (die Veröffentlichung des Tagungsbandes erfolgte allerdings erst 2018) [Düpmeier 2018]. Sie basiert unter anderem auf Überlegungen, die zuvor bereits bei den Schweizerischen Bundesbahnen (SBB) angestellt wurden. Die Überlegungen der SBB flossen mittlerweile in die **Reference CCS Architecture (RCA)** (vgl. Kapitel 2.4) ein, die von einer europäischen Initiative ausgehend eine europaweit standardisierte Architektur werden soll – aus Sicht des Autors mit guten Chancen sich durchzusetzen. Von daher ist an dieser Stelle vor allem ein Vergleich der erarbeiteten Architektur mit der RCA geboten.

Die RCA gliedert sich in mehrere Ebenen, die vertikal entlang des Prozesses der Genehmigung von Fahrzeugbewegungen angeordnet sind. Der Prozess startet dabei bei „Planning“, welches nicht direkt im Fokus der RCA ist und setzt sich über die Ebene der Fahrzeugbewegungskontrolle über die Sicherheitsebene, die Objektabstraktionsebenen bis zur Kontrolle der Feldelemente bzw. Fahrzeuge fort. Diese Gliederung existiert in dieser Klarheit in der entwickelten Architektur zwar nicht, dennoch finden sich die meisten dieser Stufen dort wieder. Ausgenommen werden müssen die beiden Objektabstraktionsebenen, die nicht aus der Sicherungslogik ausgegliedert wurden. Stattdessen sind sie in der Sicherungslogik integriert. Dies macht aufgrund der geforderten Topologieunabhängigkeit der Logik Sinn, um den generischen Teil der Logik klarer zu separieren. Allerdings müssen die Regeln zur Verknüpfung der generischen Regeln mit den beteiligten konkreten Objekten ebenfalls generisch sein, sonst könnten die Topologiedaten nicht generisch aus einer sicheren Quelle ausgelesen werden. Aus diesem Grund scheint die feine Unterteilung in der RCA auch nicht als zwingend.

Bei den Objekten wird bei der RCA nicht nur in Feldelemente, die analog der hier entwickelten Architektur über Object Controller angesteuert werden, und Fahrzeuge unterschieden, sondern bei den Fahrzeugen in eine überwachende und eine kontrollierende Instanz, den „Vehicle Supervisor“ und den „Vehicle Locator“. Des Weiteren werden Personen und mobile Objekte separat aufgeführt. Letztere haben aus Sicht des Autors allerdings viele Gemeinsamkeiten mit den Feldelementen. Sie werden später bei der Logikentwicklung als Stakeholder-Systeme betrachtet werden (siehe Kapitel 8.3.3).

Ein weiterer Unterschied findet sich direkt in der Ebene der Sicherungslogik. Hier wird der Sicherungslogik bei der RCA mit dem „Safety Manager“ eine zweite eigenständige Komponente zur Seite gestellt, welche die Zustandsüberwachung übernimmt, während die Sicherungslogik die Prüfung von Fahrerlaubnisanfragen und Stellanforderungen übernimmt. Die smartLogic ist dagegen gemäß der in Kapitel 3.2 festgelegten Zielstellung für beide Aufgaben zuständig, für deren Umsetzung jedoch naturgemäß unterschiedliche Prozesse notwendig sind.

Der Vorteil einer Trennung ist, dass die von außen angestoßenen Prozesse von den fortlaufenden Überwachungsprozessen logisch strikt getrennt sind. Allerdings gibt es auch viele Rückkopplungen

zwischen den beiden Arten von Prozessen. Ob eine Auslagerung sinnvoll ist, kann an dieser Stelle daher nicht abschließend beurteilt werden.

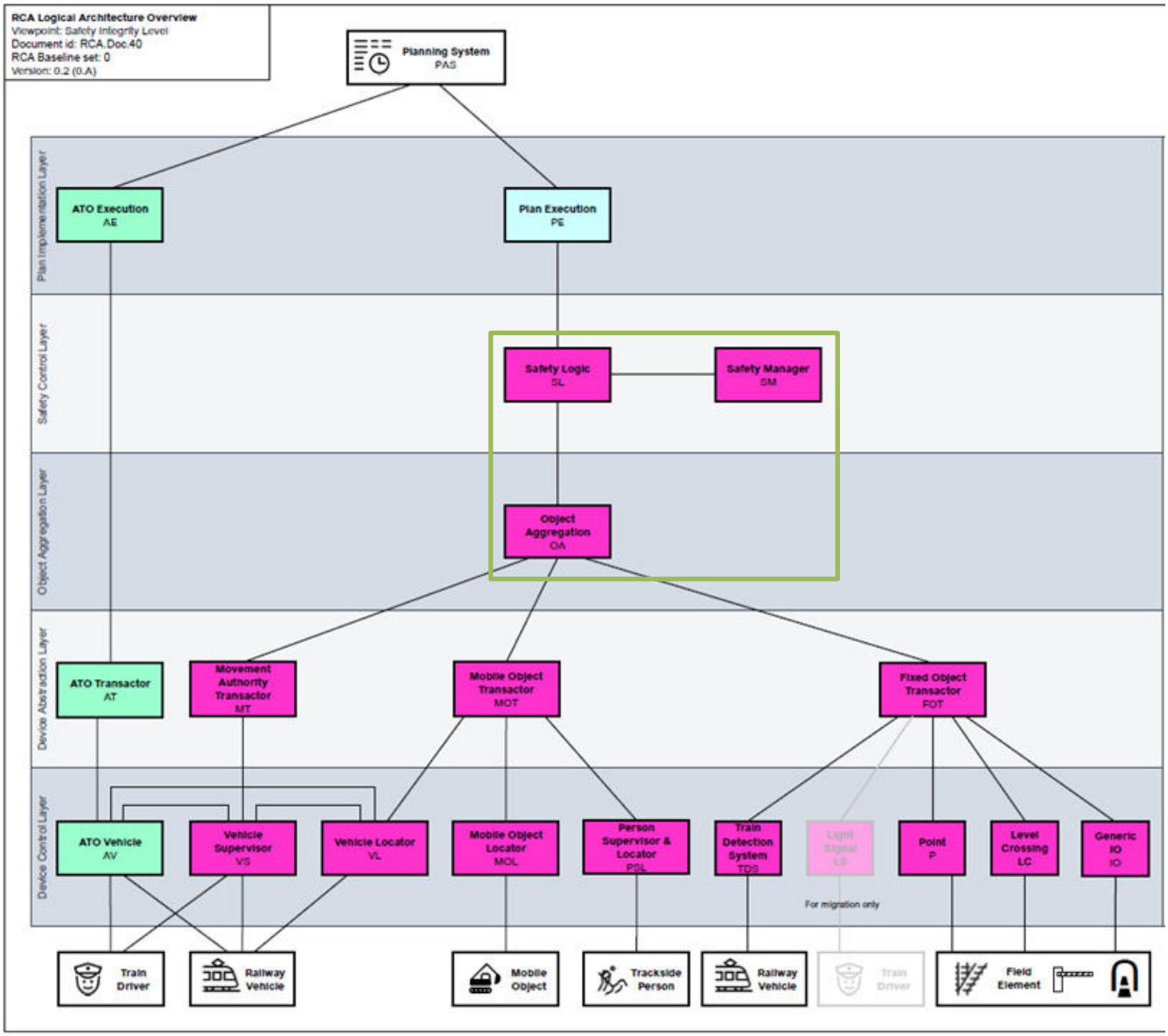


Abb. 35: Abdeckung der RCA-Komponenten durch die smartLogic
Quelle: Bearbeitung eines Ausschnitts von [ERTMS Users Group & EULYNX 2020c]; die grüne Markierung zeigt die ungefähre Abdeckung durch die smartLogic

Bei der RCA existiert ein separater ATO-Kanal, der bei der erarbeiteten Architektur nicht zwingend notwendig ist, da theoretisch das ATO-System sein Handeln zumindest im Regelbetrieb zum Preis von einigen betrieblichen Einschränkungen (z. B. müssten Fahrplanhalte immer mit einer End of Authority am Halteplatz verbunden werdeb) auch aus der ETCS-Fahrerlaubnis herleiten könnte. Die erarbeitete Architektur steht dem separaten ATO-Kanal allerdings auch nicht entgegen.

Insgesamt kann festgestellt werden, dass die erarbeitete Architektur grundsätzlich nah an der RCA ist. Die grüne Markierung in Abb. 35 zeigt in der RCA-Architektur, welche ihrer Komponenten durch die smartLogic nach der Systemdefinition in diesem Kapitel in dieser Arbeit abgedeckt werden. Eine Sonderrolle nimmt der Ortungsinformationsaggregator ein, der in der RCA nicht als eigene Komponente vorgesehen ist, sondern Teil der „Object Aggregation“ ist, während fahrzeugseitige

(„Vehicle Locator“) und infrastrukturseitige Ortung („Train Detection System“) jeweils als eigene Komponenten auftauchen.

4.9 Zusammenfassung

Im vorliegenden Hauptkapitel wurde eine Systemdefinition für die im weiteren Verlauf dieser Arbeit zu entwickelnde Sicherungslogik hergeleitet. Dabei wurden zunächst spezifische Anforderungen aus den globalen Anforderungen bestimmt, auf deren Basis die Architektur erarbeitet wurde. Zunächst wurde das System der Sicherungslogik näher beschrieben, indem es von den Umsystemen abgegrenzt wurde. Dabei kristallisierte sich eine klare Trennung zwischen der Sicherungslogik und dem Leitsystem heraus. In Bezug auf die Abgrenzung zur fahrzeugseitigen Sicherungstechnik und den Aufgaben der Stellelemente wurde ein zentraler Ansatz der Sicherungslogik befürwortet.

Ein intelligentes Traffic Management System (TMS) errechnet demnach Trassenslots für Eisenbahnfahrten. Aus diesen resultieren spezifische Stellanforderungen an die Feldelemente und Fahrerlaubnisanfragen für die Fahrzeuge. Aufgabe der Sicherungslogik ist es, diese Anforderungen des TMS, welches sich komplett im nicht sicherheitskritischen Bereich befindet, daraufhin zu überprüfen, ob sie zu einem unsicheren Zustand führen.

Wann ein unsicherer Zustand vorliegt, beurteilt die smarte Sicherungslogik anhand der aktuellen Betriebslage und mit allen mit hinreichender Sicherheit zur Verfügung stehenden Informationen. Die Informationen stammen dabei aus sicheren Datenquellen, die nicht Teil der Sicherungslogik sind, aber dennoch zum sicherheitskritischen Bereich gehören. Ein Ortungsinformationsaggregator berechnet aus verschiedenen Quellen für die Fahrzeuge die Konfidenzintervalle der Positionen der Zugspitze und des Zugschlusses. Die genaue Ausgestaltung der Datenquellen wird in der vorliegenden Arbeit nicht betrachtet, ihre Existenz wird aber vorausgesetzt.

Führt die Anfrage des TMS nicht zu einem unsicheren Zustand, wird sie über standardisierte Schnittstellen an die Fahrzeuge bzw. Feldelemente weitergeleitet. Bei der Kommunikation zum Fahrzeug wird dabei auf ETCS zurückgegriffen und bei der Kommunikation zu den Feldelementen auf die sich in der europäischen Abstimmung befindlichen EULYNX-Schnittstellen. Die Sicherungslogik erfüllt demnach eine Art Wächterfunktion zwischen dem TMS und den Fahrzeugen bzw. den Stellelementen.

5 Gefährdungsanalyse

Aufgabe der Eisenbahnsicherungstechnik ist die Verhinderung von Unfällen im Bahnverkehr. Ein Großteil der funktionalen Anforderungen an die Sicherungslogik ergibt sich daher aus den zu vermeidenden Gefährdungen im Bahnbetrieb. Mit diesen Gefährdungen beschäftigt sich das 5. Hauptkapitel dieser Arbeit, die als Grundlage für die Erarbeitung der einzelnen **funktionalen Sicherheitsanforderungen** (= Schutzfunktionen, welche die Sicherungslogik gewährleisten muss) im nächsten Arbeitsschritt, der Funktionsanalyse (siehe Kapitel 6), dienen.

5.1 Ziel und Aufbau des Kapitels

EN 50126 definiert eine **Gefährdung** (engl. „hazard“) als einen „Zustand, der zu einem Unfall führen kann“ [DIN EN 50126-1:2017, S. 15]. In der klassischen Eisenbahnsicherungstechnik wird die Kernaufgabe der Sicherungslogik (in bestehenden Stellwerken häufig als Stellwerkslogik bezeichnet), i. d. R. als Verhinderung von Entgleisungen und Kollisionen mit anderen Fahrzeugen verstanden (vergleiche Abb. 1 in Kapitel 2.1.1). Diese Gefährdungen für Eisenbahnfahrzeugbewegungen werden bereits sehr gut beherrscht, wie niedrige Unfallzahlen des statistischen Bundesamtes belegen.

Dennoch soll für die Entwicklung der neuen Sicherungslogik smartLogic gemäß dem „Grüne Wiese“-Ansatz und der Vorgehensweise im V-Modell eine ausführliche Gefährdungsanalyse erfolgen, damit die smartLogic auch für mögliche zukünftige funktionale Sicherheitsanforderungen vorbereitet ist (vgl. auch die globale Anforderung der Zukunftsfähigkeit in Kapitel 3.5).

Der Aufbau dieses Hauptkapitels folgt dem generellen Aufbau der inhaltlichen Hauptkapitel (vgl. Kapitel 1.3). Demnach werden im nachfolgenden Kapitel 5.2 zunächst Methode und Vorgehensweise diskutiert. Die darauf folgenden Kapitel des Hauptkapitels beschäftigen sich dann mit den einzelnen Arbeitsschritten der Gefährdungsanalyse gemäß der in Kapitel 5.2 hergeleiteten Vorgehensweise (systematische Herleitung von Gefährdungen im Bahnbetrieb (Kapitel 5.3), Erweiterung durch Auswertung von Unfallereignissen und Literatur (Kapitel 5.4), Vorstellung des so entstandenen vorläufigen Gefährdungskatalogs (Kapitel 5.5) und Ermittlung der Relevanz der Gefährdungen für die infrastrukturseitige Sicherungstechnik (Kapitel 5.6)). Anschließend werden die Ergebnisse diskutiert (Kapitel 5.7) und ein Vergleich mit alternativen Gefährdungskatalogen aus der Literatur gezogen (Kapitel 5.8). Das Kapitel schließt mit einer Zusammenfassung.

Die Sicherungslogik ist eine Komponente der **funktionalen Sicherheit**. Die Sicherheit gegen bewusste Angriffe von außen wird an dieser Stelle nicht extra adressiert, muss aber bei der anschließenden Entwicklung einer realen Umsetzung der Sicherungslogik berücksichtigt werden. Eine Mitbetrachtung der Angriffssicherheit an dieser Stelle wäre aufgrund der Schnelllebigkeit der Angriffsstrategien potenzieller Angreifer nur schwer möglich. Strategien zur Erhöhung der Sicherheit gegen Angriffe lassen sich jedoch im Nachhinein auf das System zur Sicherstellung der funktionalen Sicherheit aufsetzen (vgl. z. B. [Krauß et al. 2020]).

5.2 Methode und Vorgehensweise

In diesem Kapitel werden aufbauend auf der Zielsetzung des Hauptkapitels, die in Kapitel 5.1 beschrieben wurde, Methode und Vorgehensweise für die Erstellung der Gefährdungsanalyse diskutiert und festgelegt. Das Kapitel folgt dem üblichen wissenschaftlichen Aufbau, wonach zunächst aus den globalen Anforderungen aus Kapitel 3.5 spezifische Anforderungen an die Funktionsanalyse hergeleitet werden (Kapitel 5.2.1). Auf deren Grundlage werden anschließend Methode und

Vorgehensweise erarbeitet (Kapitel 5.2.2). Kapitel 5.2.3 fasst die gewählte Methode und Vorgehensweise zusammen.

5.2.1 spezifische Anforderungen an die Gefährdungsanalyse

Die spezifischen Anforderungen als Kriterien für die Auswahl einer geeigneten Methode und Vorgehensweise leiten sich aus den Anforderungen an die gesamte Arbeit (globale Anforderungen, vgl. Kapitel 3.5) und der Zielsetzung für dieses Hauptkapitel im Speziellen ab. Dazu wird für jede globale Anforderung überlegt, welchen Einfluss die Ergebnisse des Kapitels in Hinblick auf die Erfüllung der jeweiligen globalen Anforderung haben. Zusätzlich wurde zur Vervollständigung der spezifischen Anforderungen ein Brainstorming mit Fachkollegen durchgeführt.

Da sich die meisten globalen Anforderungen auf die Gestaltung der Sicherungslogik beziehen und die Gefährdungsanalyse nur eine notwendige Vorarbeit für diese darstellt, sind nur einige wenige globale Anforderungen für die Durchführung der Gefährdungsanalyse relevant, wie Tab. 9 zeigt, die eine Übersicht der daraus abgeleiteten spezifischen Anforderungen an die Gefährdungsanalyse enthält. Diese werden anschließend unterhalb der Tabelle näher erläutert. Bei nicht relevanten globalen Anforderungen ist dieser Umstand in kursiv vermerkt.

Tab. 9: spezifische Anforderungen an die Gefährdungsanalyse

Zieldimension	**globale Anforderung**	**spezifische Anforderungen**
Kernanforderung sichere Logik		alle für die Sicherungslogik relevanten Gefährdungen werden identifiziert
geringer Planungs- und Genehmigungsaufwand	schlanke Logik	möglichst viele Gefährdungen, die eindeutig nicht in den Bereich der Sicherungslogik fallen, werden ausgeschlossen
	Beschränkung auf sicherungskritischen Kern	*globale Anforderung primär für Funktionsanalyse (Kap. 6) relevant*
	generische Logik	Gefährdungen werden generisch formuliert
	Topologieunabhängigkeit	*keine Relevanz für die Gefährdungsanalyse festgestellt*
	flexible Infrastrukturzuordnung	
Interoperabiliät	Standardschnittstellen	*keine Relevanz für die Gefährdungsanalyse festgestellt*
geringer Hardwareeinsatz	nur erforderliche Infrastrukturelemente	*keine Relevanz für die Gefährdungsanalyse festgestellt*
geringer Arbeitskräfteeinsatz	hohe Automatisierung	*keine Relevanz für die Gefährdungsanalyse festgestellt*
	flexible Kontrollbereiche	
Energieeffizienz	keine unnötigen Bremsvorgänge	*keine Relevanz für die Gefährdungsanalyse festgestellt*
	Freiraum für Fahrzeug	
hohe Kapazität	Ermöglichung maximaler Geschwindigkeit	*keine Relevanz für die Gefährdungsanalyse festgestellt*
	geringe Latenz	
	minimale	

	Infrastrukturbeanspruchung	
	frühestmögliche Infrastrukturfreigabe	
hohe Robustheit	Rückfallebenenintegration	auch Gefährdungen, die sich aus Rückfallebenen ergeben, werden betrachtet
	Regelhandlungsgebot	*keine Relevanz für die Gefährdungsanalyse festgestellt*
	Freiraum für Fahrzeuge	
	Resilienz	
	modulare Außerbetriebnahme	
lange Nutzungszeiten	Migrationsfähigkeit	*keine Relevanz für die Gefährdungsanalyse festgestellt*
	Zukunftsfähigkeit	Suchraum nicht auf heutige Sicherheitsanforderungen beschränken
[ohne]	Protokollierung	*keine Relevanz für die Gefährdungsanalyse festgestellt*

Die wichtigste spezifische Anforderung ist die Sicherstellung der Vollständigkeit des Gefährdungskatalogs, die sich, wie im vorigen Kapitel beschrieben, direkt aus der *Kernanforderung* ergibt. Darum ist eine breite Erfassung potenzieller Gefährdungen sinnvoll.

Auf der anderen Seite sollten jedoch nach Möglichkeit auch Gefährdungen ausgeschlossen werden, deren Eintrittswahrscheinlichkeiten mit hinreichend großer Sicherheit (um mind. SIL 4-Niveau zu erreichen, vgl. EN 50129) nicht durch die Komponente Sicherungslogik beeinflusst werden können, die also nicht zu den für die Sicherungslogik relevanten Gefährdungen gehören. Andernfalls droht der Gefährdungskatalog zu umfangreich zu werden und die globale Anforderung der *schlanken Logik* würde verletzt sowie die äußeren Rahmenbedingungen aus Kapitel 3.6.1 wie die zur Verfügung stehende Bearbeitungszeit könnten zu stark beeinträchtigt werden.

Bei der Eingrenzung der Gefährdungen auf die für die Sicherungslogik relevanten Gefährdungen ist auf die deutlich stärkere Gewichtung der Kernanforderung der sicheren Logik zu achten. Es muss also sichergestellt werden, dass nur Gefährdungen ausgeschlossen werden, deren Eintrittswahrscheinlichkeit hinreichend gering ist, um mind. SIL 4-Niveau zu erreichen. Nicht ausgeschlossen werden sollten Gefährdungen, die in Folge möglicher Rückfallebenen auftreten können, um die *Rückfallebenenintegration* in die smartLogic zu ermöglichen.

Weiterhin sollten in Folge der Anforderung der *generischen Logik* die Gefährdungen möglichst generisch formuliert werden, um eine breite mögliche Ereignispalette abzudecken und die spätere Sicherungslogik nicht durch zu viel Spezifität auf bestimmte gefährliche Situationen zu verkomplizieren oder sogar mögliche gefährliche Ereignisse nicht abzudecken. Auch hier gilt jedoch, dass die Kernanforderung der sicheren Logik am höchsten zu gewichten ist, also das Kriterium der Vollständigkeit vorgeht.

Die weiteren globalen Anforderungen beziehen sich entweder auf den Funktionsumfang der Logik, die interne Funktionsweise, den Aufbau der Logik oder die Kompatibilität zu anderen Systeme. Da die Gefährdungsanalyse von den grundsätzlichen Gefahren im Bahnbetrieb ausgeht und nicht von der

konkreten Umsetzung der Sicherungslogik, werden diese Anforderungen als für die Gefährdungsanalyse nicht relevant betrachtet.

5.2.2 Erarbeitung der Methode und Vorgehensweise

In diesem Unterkapitel soll auf Basis der in Kapitel 5.2.1 identifizierten spezifischen Anforderungen eine geeignete Methode und Vorgehensweise für die Funktionsanalyse erarbeitet werden. Zunächst werden mögliche Ansätze für die generelle Methode zur Ermittlung der Gefährdungen identifiziert und bewertet. Anschließend werden die im ersten Abschnitt identifizierten Methoden jeweils näher betrachtet und eine detaillierte Vorgehensweise hergeleitet.

Generelle Methode und Vorgehensweise

Gefährdungen können prinzipiell auf zwei Arten ermittelt werden. Zum einen über eine systematische Betrachtung möglicher Ausfälle des Systems sowie möglicher Unfallereignisse, die im Bahnbetrieb entstehen können, z. B. mittels einer Failure Modes and Effects Analysis (FMEA). Zum anderen über eine Auswertung bekannter gefährlicher Ereignisse, die bereits zu einer Gefährdung oder sogar zu einem Unfall geführt haben. Vergleiche hierzu [Braband 2013, S. 570].

Die erste Art entspricht dem „Grüne Wiese“-Ansatz, denn durch die systematische Herleitung der Gefährdungen aus Ausfällen und möglichen Unfallereignissen kann eine Vorfestlegung auf althergebrachte Lösungen verhindert werden. Bei einer reinen Auswertung bereits stattgefundener Unfallereignisse ist dies dagegen weniger wahrscheinlich. Die Erkenntnisse daraus sind ja bereits in der aktuellen Sicherungstechnik verwirklicht. Wollte man sich auf die Auswertung der bekannten Unfallereignisse beschränken, wäre eine Gefährdungsanalyse an dieser Stelle gar nicht mehr notwendig. Zudem müssen nicht alle zukünftigen Ausfälle, die Sicherheitsrisiken bergen, in den bereits bekannten Unfallereignissen erkennbar sein.

Eine systematische Betrachtung ist demnach auf jeden Fall sinnvoll. Wie bereits in Kapitel 3.6.2 beschrieben, sind auch Mischformen aus Weiterentwicklung und „Grüne Wiese“-Ansatz möglich. Zur Sicherstellung der Vollständigkeit sollte deshalb nicht auf eine zusätzliche Auswertung der bereits bekannten Unfallereignisse verzichtet werden. Eine solche Auswertung kann weitere wichtige Erkenntnisse liefern und die systematische Untersuchung ergänzen.

Um den offenen Blick der systematischen Analyse nicht zu verstellen, sollte bezogen auf die Reihenfolge der Arbeitsschritte zunächst die eigene, systematische Untersuchung durchgeführt werden und dann die Auswertung der Unfallereignisse folgen. Als weiteren Schritt zur Sicherstellung der Vollständigkeit können die Ergebnisse mit bereits bekannten Gefährdungskatalogen abgeglichen und ggf. ergänzt werden. Dies erfolgt in Kapitel 5.5.

Systematische Herleitung von Gefährdungen

Die systematische Sammlung der Gefährdungen kann analog der nach EN 50126 vorgeschriebenen Risikoanalyse erfolgen (vgl. Vorgehen bei der Risikoanalyse für ETCS bei der Deutschen Bahn [DB Netz AG 2014]). Allerdings ist zu beachten, dass die Gefährdungsidentifikation dort bereits für ein vollständig definiertes System erfolgt, dessen Systemfunktionen bekannt sind, während sie im vorliegenden Fall als Grundlage für die Bestimmung des Funktionsumfangs der Sicherungslogik dienen soll. Hieraus und aus den eingeschränkten Ressourcen zur Bearbeitung der Arbeit ergeben sich einige Abweichungen zur Risikoanalyse. So können die vorgeschriebenen Dokumentationspflichten und Mehraugenprinzipien nicht alle vollständig eingehalten werden.

Gemäß dem Vorgehen bei Risikoanalysen sind zunächst die TOP-Gefährdungen zu definieren. Diese können aus den grundsätzlichen Unfallarten hergeleitet werden, die nach der in Kapitel 5.1 zitierten Definition von „Gefährdungen“ Zustände (bzw. Ereignisketten) sind, die zu einem Unfall führen können. Ein Unfall ist nach allgemeiner Definition ein unbeabsichtigtes Ereignis, durch das ein Schaden für Personen, Sachwerte oder die Umwelt entsteht (vgl. u.a. [EUB 2009, S. 3]).

Identifizierung der Gefährdeten

Für die Herleitung der Unfallarten ist es daher zunächst wichtig, sich Klarheit darüber zu verschaffen, wer durch den Bahnbetrieb geschädigt werden kann. Hierzu kann die Stakeholder-Analyse aus Kapitel 3.1.2 als Grundlage genommen werden, die entsprechend zu verfeinern ist. Zu klären ist, wer von den Stakeholdern mit dem Bahnbetrieb (hier ist damit die Durchführung des Bahnbetriebs gemeint) in Kontakt kommt und somit durch diesen potenziell geschädigt werden kann. Bahnbetrieb bezeichnet hier alle Prozesse, die unmittelbar mit der Bewegung von Eisenbahnfahrzeugen auf der Eisenbahninfrastruktur zusammenhängen (ohne vorgelagerte Prozesse wie Fahrplanerstellung, etc.)

Auf jeden Fall kommen die Kunden, die Fahrgäste sind, mit dem Bahnbetrieb in Kontakt. Sie sind in vielfältiger Weise durch diesen auch gefährdet. Nicht unmittelbar durch den Bahnbetrieb gefährdet sind die Stakeholder-Gruppen Shareholder und staatliche Institutionen, da sie in der Regel nicht unmittelbar am Bahnbetrieb teilnehmen. (Allerdings gibt es Ausnahmen, z. B. bei Vorortterminen. Dies wird hier allerdings vernachlässigt, da die Betroffenen in solchen Fällen wie Fahrgäste oder Personal an der Strecke gefährdet sind.) Die Eisenbahnverkehrsunternehmen spielen als Gruppe für diese Analyse ebenfalls keine Rolle, da sie sich in Bezug auf Beteiligte am Bahnbetrieb wiederum in die anderen Gruppen (**Fahrpersonal** = Beschäftigte in den Eisenbahnfahrzeugen, Personal an der Strecke) aufspalten und die Erkenntnisse zu diesen Gruppen somit die EVU umfassen. Weitere Gruppen benötigen eine ausführlichere Analyse.

Teile der Belegschaft kommen selbstverständlich mit dem Bahnbetrieb in Kontakt. Hierzu gehört vor allem das Fahrpersonal, welches ähnlich betroffen ist wie die Fahrgäste, und das Personal, welches an der Strecke arbeitet. Zu Letzterem gehört das örtlich ansässige Stellwerkspersonal[19], das Zugbildungspersonal[20], das Bahnhofspersonal sowie das Instandhaltungspersonal.

Lieferanten kommen je nach Art ihrer Lieferung ebenfalls mit dem Bahnbetrieb in Kontakt, allerdings in ähnlicher Weise wie das Instandhaltungspersonal, so dass sie mit diesem zusammengefasst werden können.

Die Zivilgesellschaft besteht aus verschiedenen Gruppen, die in unterschiedlichen Funktionen mit dem Bahnbetrieb in Kontakt kommen. An dieser Stelle ist entscheidend, ob sie dies als Gruppe in besonderer Weise tun. Dabei spielt keine Rolle, dass Mitglieder dieser Gruppe möglicherweise in anderer Funktion, z. B. als Fahrgäste mit dem Bahnbetrieb in Kontakt kommen. Kundenverbände sind dieser Definition folgend nicht direkt am Bahnbetrieb beteiligt, Anwohner dagegen schon. Umweltverbände vertreten als Gruppe die Interessen der Umwelt. Allerdings spielen sie als Personengruppe an dieser Stelle keine Rolle, da sie nicht direkt mit dem Bahnbetrieb in Kontakt kommen und so als Gruppe nicht direkt gefährdet sind – wenn man einmal von gefährlichen

[19] Da eine allgemeingültige Definition für das Stellwerkspersonal nicht gefunden werden konnte, werden zum Stellwerkspersonal in dieser Arbeit alle Beschäftige gezählt, die mit dem Stellwerk bzw. der Sicherungslogik unteragieren bzw. zur Erfüllung der Schutzfunktionen des Stellwerks einen Beitrag leisten. Hierzu zählen Fahrdienstleiter inkl. örtlich zuständiger Fahrdienstleiter, Weichenwärter, Schrankenwärter und von diesen beauftragte Mitarbeiter (z. B. Posten, Boten, Melder).

[20] Umfasst alle an der Zugbildung und sonstigen Rangierprozessen beteiligte Mitarbeiter, die nicht zum Stellwerkspersonal gehören (z. B. Rangierer, Rangierbegleiter, Wagenmeister, Rangiertriebfahrzeugführer) (Es kann Überschneidungen zum >Fahrpersonal geben.).

Protestaktionen absieht. Den Vertretern aus der Zivilgesellschaft kann auch die wichtige Gruppe der Nutzer anderer Verkehrsmittel (inkl. Fußgängern) zugeordnet werden. Diese kommen in der Regel an Bahnübergängen mit dem Bahnbetrieb in Kontakt.

Zusammengefasst sind also mögliche Unfallarten für Fahrgäste und Fahrpersonal, in Gleisnähe arbeitendes Personal (egal ob eigenes oder fremdes), Anwohner und andere Verkehrsteilnehmer zu untersuchen.

Bei den Sachwerten können u. a. Eisenbahninfrastruktur, Eisenbahnfahrzeuge, Transportgüter und Gepäck, Baustellen- bzw. Instandhaltungsmaterial, Fahrzeuge anderer Verkehrsmittel an Bahnübergängen, Haus- oder Nutztiere sowie nicht zur Bahn gehörende, sich an der Strecke befindliche Gegenstände oder Immobilien durch einen Unfall gefährdet werden.

Im Bereich der Umwelt können Pflanzen, wildlebende Tiere, der Boden, Gewässer oder die Luft geschädigt werden (vgl. zur Vollständigkeit die Definition von Umweltverschmutzung im Lexikon der Nachhaltigkeit [IHK 2015]). Der Austritt von Radioaktivität durch Unfälle im Bahnbetrieb – wenn man von Castor-Transporten absieht – ist im Regelfall nicht zu befürchten und wird deshalb nicht weiter untersucht.

Herleitung der Unfallarten

Für die gefährdeten Personengruppen können zur Bestimmung der Unfallarten die elf Themenfelder aus dem von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) empfohlenen Gefährdungskatalog, der von der Berufsgenossenschaft Rohstoffe und chemische Industrie (BG RCI) [BG RCI 2017] erstellt wurde, herangezogen werden. Für jedes der Themenfelder muss ermittelt werden, ob aus dem Bahnbetrieb eine Gefährdung für eine oder mehrere der gefährdeten Personengruppen besteht. Hierzu bietet sich eine FMEA an, wonach mögliche Ausfall- bzw. Versagensarten des Produktionssystems Eisenbahn zu analysieren sind (vgl. [Braband 2013, 570f]).

Die Risikoanalyse der DB Netz AG für ETCS enthält in Anlage 2 eine Checkliste möglicher Versagensarten [DB Netz AG 2014], die auch für die einzelnen Teilsysteme des betrachteten Produktionssystems angewendet werden können. Falls ein Ausfall nach einer der Versagensarten zu einer Gefährdung führen könnte, ist diese zu listen. Zur Beurteilung, ob ein Ausfall zu einer Gefährdung führt, sind neben den Personen auch die zuvor identifizierten Gefährdungsarten für Sachwerte und Umwelt zu betrachten.

Die Herleitung der Unfallarten gemäß dieser Methode wird in Kapitel 5.3 beschrieben.

Auswertung von Unfallereignissen

Ziel der Auswertung von Unfallereignissen ist die Vervollständigung des entwickelten Gefährdungskatalogs. Hierzu ist bei den Unfällen nicht die oberflächliche Ursache (z. B. Entgleisung, Zugkollision) relevant, sondern wie es zu ihr kam, was also die zugrundeliegende Ursache war.

Für die Auswertung bieten sich für Deutschland die ausführlichen Berichte der Bundesstelle für Eisenbahnunfalluntersuchung (BEU) an [BEU 2019]. Die Berichte sind mit dem Ziel verfasst, Lehren aus dem Unfallereignis für den Bahnbetrieb zu erzielen. Demzufolge mündet die Untersuchung in Handlungsempfehlungen für die am Bahnbetrieb beteiligten Akteure.

Zeitlich reichen die Berichte auf der Internetseite der BEU (bis 2017 Eisenbahnunfall-untersuchungsstelle des Bundes EUB) bis ins Jahr 2000 (Eisenbahnunfall von Brühl) zurück. Allerdings wurde die EUB erst 2008 eingerichtet, so dass es vor 2010 nur wenig Berichte gibt. Diese liefern jedoch einen guten Überblick über aktuelle Unfallereignisse. Ferner kann angenommen werden, dass die wesentlichen Erkenntnisse aus früheren Unfällen bereits in der aktuellen Generation

der Sicherungstechnik abgedeckt sind, da genügend Zeit vergangen ist, um entsprechende Sicherheitsempfehlungen als Lehre aus diesen Ereignissen umzusetzen. Daher erscheint die Auswertung der Unfallereignisse über den beschriebenen Zeitraum für das Ziel der Gefährdungsanalyse in dieser Arbeit ausreichend zu sein.

Die Auswertung der Unfallereignisse wird aus Kapazitätsgründen auf Deutschland beschränkt. Dies erscheint vertretbar, da die Betriebsverfahren und bisherigen Sicherungssysteme sehr national geprägt sind. Nichtsdestotrotz könnten Unfallereignisse aus anderen Ländern weiter zur Vervollständigung des Gefährdungskatalogs beitragen, allerdings wären zur genauen Analyse die jeweiligen Produktionsprozesse genau zu analysieren. Dies wird als sehr zeitintensiv eingeschätzt. Dagegen scheint die bereits hohe Sicherheit im deutschen Produktionsprozess dafür zu sprechen, dass eine Auswertung dennoch stattgefundener deutscher Unfallereignisse einen ausreichenden Erkenntnisgewinn zur Vervollständigung des Gefährdungskatalogs beisteuern können.

Bewertung der Zuständigkeit der Komponente Sicherungslogik

Bei der Sammlung der Gefährdungen wird zur Sicherstellung der Vollständigkeit des Gefährdungskatalogs zunächst nicht unterschieden, ob diese tatsächlich durch die zu entwickelnde Sicherungslogik verhindert werden können oder nicht. Diese Unterscheidung ist aber für die Bestimmung der funktionalen Sicherheitsanforderungen an die Komponente Sicherungslogik erforderlich. Kriterien hierfür sind, ob die Gefährdung bereits durch eine andere Komponente des Produktionssystems Eisenbahn zuverlässig verhindert wird oder ob sie nach eigener und der Einschätzung weiterer Fachkollegen außerhalb der Möglichkeiten einer infrastrukturseitigen Sicherungslogik liegt, weil es beispielsweise keine Detektionsmöglichkeit gibt und die Entwicklung einer solchen auch nach derzeitigem Stand nicht wahrscheinlich erscheint.

5.2.3 Zusammenfassung der gewählten Methode und Vorgehensweise

Als Ergebnis der in Kapitel 5.2.2 geschilderten Diskussion wird die in Abb. 36 dargestellte Methode und Vorgehensweise bei der Gefährdungsanalyse verfolgt.

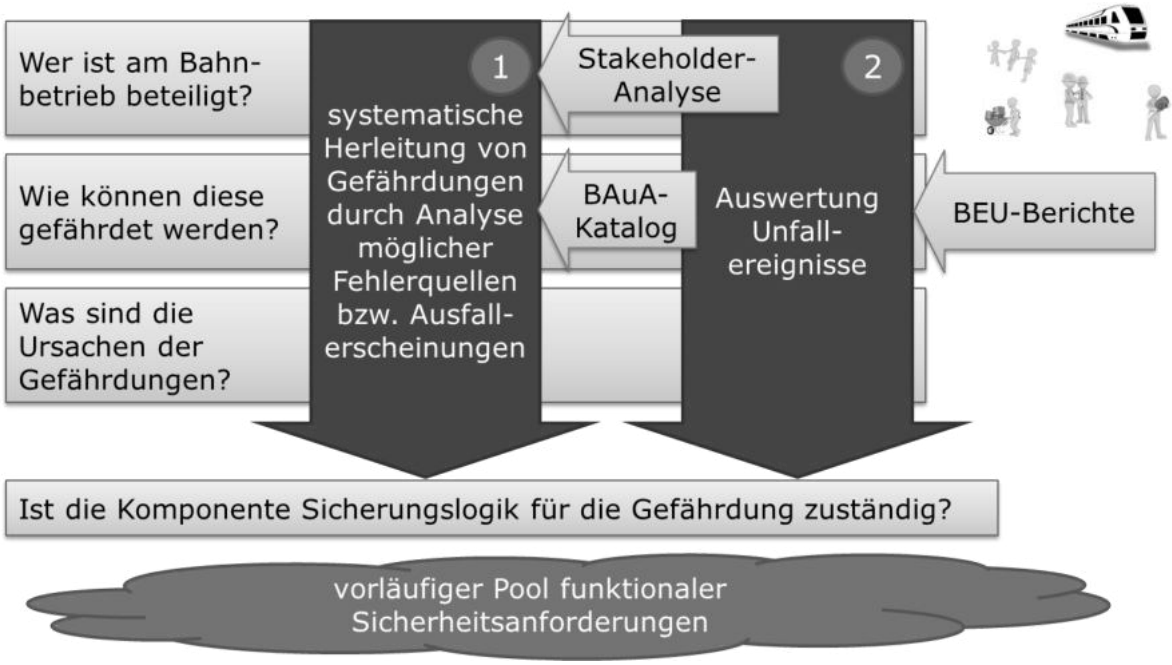


Abb. 36: Methode und Vorgehensweise bei der Gefährdungsanalyse
[Eigene Darstellung]

Zur Bestimmung der Gefährdungen werden zwei Ansätze verfolgt. Zunächst wird eine systematische Herleitung der Gefährdungen vorgenommen. Die so entstandene Menge an Gefährdungen wird im zweiten Schritt durch eine Auswertung von Unfallereignissen ergänzt.

Für die systematische Herleitung der Gefährdungen wird zunächst untersucht, wer unmittelbare Beteiligung am Bahnbetrieb beteiligt ist. Für diese Personen werden die grundsätzlich möglichen Gefährdungen anhand des von der BAuA empfohlenen Gefährdungskatalogs ermittelt. Weiterhin wird untersucht, inwiefern Sachgüter und die Umwelt gefährdet werden können. Anschließend wird anhand möglicher Ausfälle der am Bahnbetrieb beteiligten Systemkomponenten ein erster Gefährdungskatalog bestimmt.

Für die Auswertung der Unfallereignisse werden auf Basis der Unfallberichte der BEU/EUB Ursachen neuerer Unfälle analysiert und gegebenenfalls der Gefährdungskatalog ergänzt.

Anschließend folgt eine Bewertung, welche der gefundenen Gefährdungen im Zuständigkeitsbereich der Sicherungslogik liegen. Hieraus kann in der Funktionsanalyse ein vorläufiger Pool an sicherungstechnischen Anforderungen hergeleitet werden, deren Einhaltung durch entsprechende Prüfbedingungen von der Sicherungslogik sichergestellt werden muss.

5.3 systematische Herleitung von Gefährdungen

Der erste Schritt der Gefährdungsanalyse besteht gemäß der in Kapitel 5.2.3 beschriebenen Vorgehensweise aus einer systematischen Betrachtung möglicher Gefährdungen. Die systematische Betrachtung geht an dieser Stelle über den Zuständigkeitsbereich der späteren Sicherungslogik bewusst deutlich hinaus, um im Sinne des „Grüne Wiese“-Ansatzes nicht bereits zu voreingenommen durch die bisherige Aufgabenteilung innerhalb der infrastrukturseitigen Sicherungslogik zu sein.

Daher werden nur wenige, recht offensichtliche Gefährdungsarten in diesem Verfahrensschritt bereits ausgeschlossen, die zum in Kapitel 5.1 definierten Ziel, die Grundlage für die Definition der funktionalen Sicherheitsanforderungen der zu entwickelnden Sicherungslogik zu schaffen, definitiv nichts beitragen. Dieser Ausschluss erfolgt, damit die systematische Gefährdungsanalyse nicht unnötig komplex und unübersichtlich wird. Hierzu kann die Abgrenzung des Aufgabengebiets der Sicherungslogik als Teil der infrastrukturseitigen Sicherungslogik gemäß den Überlegungen in Kapitel 4.3 herangezogen werden. Demnach können Gefährdungsarten ausgeschlossen werden, die sich ausschließlich auf Sicherheitsaspekte innerhalb der Fahrzeuge beziehen. Diese müssen im Rahmen der Fahrzeugkonstruktion und des Baus der Fahrzeuge berücksichtigt werden. Die Beschaffenheit des Bahnkörpers wird allerdings nicht ausgeschlossen, da Techniken denkbar sind, die Gefährdungen aus diesem Bereich vermeiden oder deren Auswirkungen verringern können und eine Einbindung solcher Techniken in die Sicherungslogik prinzipiell denkbar ist, z. B. Heißläuferortungsanlagen.

Weiterhin werden Gefährdungsarten ausgeschlossen, die sich rein auf die Arbeitsplatzbeschaffenheit beziehen, sofern diese nicht einen unmittelbaren Einfluss auf den Eisenbahnbetrieb haben. Diese Gefährdungsarten müssen im Rahmen der Arbeitssicherheit berücksichtigt werden. Wenn betriebliche Sicherheitsziele, wie z. B. der Schutz von Beschäftigten auf Gleisbaustellen vor Gefährdungen durch Zugfahrten, betroffen sind, sind die Gefährdungsarten jedoch relevant.

Nachfolgend werden die möglichen (Primär-)Gefährdungen durch den Bahnbetrieb für den Menschen (Kapitel 5.3.1) sowie für Sachgüter und die Umwelt (Kapitel 5.3.2) hergeleitet. Kapitel 5.3.3 beschäftigt sich mit zusätzlichen Sekundärgefährdungen, die in Folge von Primärgefährdungen durch nicht verhinderte Schadensausmaßvergrößerungen entstehen können. Eine solche Sekundärgefährdung tritt ein, wenn die Sicherungstechnik durch eine Sicherheitsreaktion zur

Vermeidung einer Primärgefährdung das Schadensausmaß vergrößert (z. B. bei einem Nothalt bei einem Brand im Tunnel).

5.3.1 Gefährdungen für den Menschen

Zunächst wird untersucht, welche Gefährdungen für die menschlichen Stakeholder auftreten. Hierzu dient wie beschrieben der von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) empfohlene Gefährdungskatalog der BG RCI [BG RCI 2017] als Basis. Zu jedem dort gelisteten Gefährdungs-Themenfeld wird untersucht, welche am Bahnbetrieb beteiligten Personen Gefährdungen daraus ausgesetzt sind und welche Ursachen es dafür im Bahnkontext gibt. Hierzu werden die Tätigkeiten der einzelnen beteiligten Personengruppen betrachtet und jeweils ein Brainstorming durchgeführt. Die Ergebnisse sind in Tab. 10 dargestellt.

Tab. 10: mögliche Gefährdungen der am Bahnbetrieb Beteiligten und Ursachen

Gefährdungs-Themenfelder	Betroffene Stakeholder	Gefährdungsarten	Ursachen im Bahnkontext
Grundlegende organisatorische Faktoren	Alle	Begünstigung anderer Gefährdungsarten	Fehlen wichtiger Informationen oder Kenntnisse, Nichtentdecken von Fehlern und Fehlfunktionen, intransparente oder fehlende Zuständigkeiten und Prozesse, fehlerhaftes Einsetzen von Arbeitskräften, Fehlen von Schutzausrüstung, etc.
Gefährdung durch Arbeitsplatzgestaltung		*nicht im Fokus*	
Gefährdung durch ergonomische Faktoren		*nicht im Fokus*	
Mechanische Gefährdung	Alle	Stürzen, Überrollen, Kompression des Körpers, Quetschen	*siehe Tab. 11*
Elektrische Gefährdung	IH-Personal, Fahrgäste, Fahrpersonal (z. B. bei Evakuierung), andere Verkehrsträger (bei Kontakt mit Oberleitung)	Stromunfall an der Oberleitung, Stromunfall durch spannungstragende Teile im Fahrzeug oder an der Infrastruktur	Störung an der Oberleitung
Gefährdung durch Stoffe	Anwohner, Betriebs- und IH-Personal	Gefahrstoffunfall	*siehe Gefährdungen von Transportgütern (Tab. 12)*
Gefährdung durch Brände/Explosionen	Anwohner, Fahrgäste, Betriebs- und IH-Personal	Folgen durch Fahrzeugbrand oder Brand an der Strecke	Fahrzeugbrand, fehlerhafte Evakuierung, Flucht in Entrauchungsrichtung

Biologische Gefährdung		*nicht im Fokus*	
Gefährdung durch spezielle physikalische Einwirkungen	Anwohner, Fahrgäste, Betriebs- und IH-Personal	Schienenverkehrs-lärm, Überhitzung, Unterkühlung	Schienenverkehrslärm, Ausfall der Temperaturregulierung im Zug, Gleislagefehler durch Temperaturschwankungen
Psychische Belastungsfaktoren		*nicht im Fokus*	
Sonstige Gefährdungs- und Belastungsfaktoren		*bisher keine identifiziert*	

Der von der BAuA empfohlene Gefährdungskatalog listet vielfältige Themenfelder für Gefährdungen, jedoch sind nicht alle davon für die Sicherungslogik relevant. Wie bereits oben erwähnt, werden an dieser Stelle bereits alle Gefährdungen ausgeschlossen, die sich auf die **Arbeitsplatzgestaltung** beziehen. Der relevante physische Schutz von Personal an der Strecke oder im Zug zum Beispiel auf Gleisbaustellen wird dagegen in den Themenfeldern „mechanische Gefährdungen“ und „Gefährdungen durch spezielle physikalische Einwirkungen“ gesehen. **Ergonomische Faktoren** sind ebenfalls nicht im Fokus, da die Bedienoberfläche nicht Teil der Sicherungslogik ist (vgl. Kapitel 2.2.5, 0 und 4). **Psychische Belastungsfaktoren** können entweder ebenfalls durch die Arbeitsplatz-gestaltung verursacht werden oder durch den Eintritt belastender Ereignisse wie Unfälle. Deren Eintritt muss ohnehin verhindert werden. Eine Untersuchung der physischen Belastungsfaktoren bringt hier keinen Mehrwert für die Ermittlung der funktionalen Sicherheitsanforderungen an die Sicherungslogik. **Biologische Gefährdungen** werden ausgeschlossen, da sie entweder auf spezielle Transportgüter zurückzuführen wären (siehe auch Gefährdung durch Stoffe). In diesem Fall bräuchten diese Transportgüter aber ohnehin spezielle Sicherungsmaßnahmen, die nicht in den Bereich der infrastrukturseitigen Sicherungslogik fallen. Zum anderen können biologische Gefährdungen durch den Einsatz gefährdender Stoffe im Produktionsprozess entstehen. Auch in diesem Fall scheint die Gestaltung der zu entwickelnden Sicherungslogik hierauf keinesfalls einen Einfluss zu haben.

Gefährdungen durch Stoffe sind wahrscheinlicher als biologische Gefährdungen, da Gefahrstoffe deutlich häufiger transportiert werden, als biologisch gefährliche Stoffe. Als Transportgut sind sie über die allgemeine Schutzanforderung für Transportgüter (siehe unten bei Sachgütern) allerdings bereits abgedeckt und stellen zumindest für die Logik keine zusätzlichen Anforderungen dar. Auch die Verwendung von Stoffen mit gefährdenden Eigenschaften innerhalb der Produktion sicherungstechnischer Komponenten kann Gefährdungen durch Stoffe auslösen. Allerdings wird in dieser Arbeit davon ausgegangen, dass die zu entwickelnde Sicherungslogik auf einer sicheren Hardwareplattform läuft. Daher braucht das Themenfeld „Gefährdung durch Stoffe“ hier nicht weiter betrachtet zu werden.

Bei **elektrische**n **Gefährdungen** ist zunächst die bahnspezifische Gefahr durch die Oberleitung intuitiv präsent. Stromunfälle können auch an anderen spannungstragenden Teilen im Fahrzeug oder an der Infrastruktur hervorgerufen werden. Dies wird durch die Gestaltung der Hardware beeinflusst und die Verhütung fällt in den Bereich der allgemeinen, nicht eisenbahnspezifischen Vorsorge gegen Stromunfälle. Die reine Gefährdung aus der Gestaltung der Hardware wird hier daher nicht weiter betrachtet (vgl. „Gefährdungen durch Stoffe“). Die Oberleitung ist als Gefährdungsquelle dagegen durchaus relevant. Die Sicherungslogik sollte zumindest auf Fehlfunktionen der Oberleitung reagieren können und zum Beispiel Fahrten in Bereiche mit gestörter Oberleitung verhindern. Dieser Aspekt

wird ebenfalls bei der Gefährdung von Sachgütern auftauchen, da Oberleitungsstörungen oder Störungen an der korrespondierenden fahrzeugseitigen Technik die Fahrzeuge und die Infrastruktur gefährden können. Systeme mit Stromschienen werden aufgrund ihrer begrenzten Verbreitung an dieser Stelle nicht näher betrachtet.

Gefährdungen durch Brände spielen ebenfalls eine Rolle und sollten weiter betrachtet werden, wobei hier im Aufgabenbereich der Sicherungslogik vor allem die Folgen durch ein Brandereignis im Fahrzeug oder an der Strecke im Fokus stehen. Der eigentliche Brand wird eher nicht durch die Logik begünstigt, aber auf die Folgen kann die Sicherungslogik einen Einfluss haben, beispielsweise durch die Verhinderung von Fahrten in den Brandbereich oder die Evakuierung von Fahrzeugen aus gefährdeten Bereichen, wie es in der Schweiz bei ETCS mit der Reversing-Funktionalität vorgesehen ist.

Grundlegende organisatorische Faktoren bilden ein Sonderthemenfeld. Sie können andere Gefährdungen begünstigen, beispielsweise durch eine fehlerhafte Einweisung, eine fehlerhafte Fehlerkultur, ein unzureichendes Meldewesen oder intransparente und unvollständige Prozesse. Allerdings stellen sie von sich aus keine Primärgefährdung dar. Da in der vorliegenden Arbeit die Sicherungslogik als technische Komponente überarbeitet werden soll und nicht die organisatorischen Prozesse, wird eine vertiefte Betrachtung grundlegender organisatorischer Faktoren hier nicht vorgenommen. Es wird stattdessen davon ausgegangen, dass diesen Fehlerquellen bereits in den vorgeschriebenen Prozessen bei der Entwicklung und Bedienung sicherungstechnischer Komponenten im Eisenbahnbereich begegnet wird.

Mechanische Gefährdungen treten in vielfältiger Weise auf. Zum einen, wenn ein schwerwiegender Unfall, wie eine Entgleisung oder eine Kollision, passiert sind. Zum anderen auch durch Eigenschaften des normalen Betriebs, wie zu starkem Beschleunigen oder Abbremsen oder hoher Seitenbeschleunigung, zum Beispiel in S-Kurven. Dies kann zum Beispiel Stöße oder Stürze verursachen. Stürze können auch beim Ein- und Ausstieg eine Gefährdung darstellen, die durch vielfältige Ursachen ausgelöst werden kann. Tab. 11 enthält eine Übersicht der Ergebnisse eines Brainstormings über mögliche mechanische Gefährdungen, die für die verschiedenen am Bahnbetrieb Beteiligten auftreten können. Es sind dabei alle Phasen zu betrachten, in denen die jeweilige Personengruppe mit dem Bahnbetrieb in Berührung kommt.

Tab. 11: Übersicht mechanischer Gefährdungen

betroffene Stakeholder	mechanische Gefährdungen
Fahrgäste (während der Fahrt)	abruptes Abbremsen oder sonstige mechanische Gefährdung durch Entgleisung oder Kollision, zu schnelles Beschleunigen oder Bremsen, seitliche G-Kräfte in Bögen, bei Weichenverbindung oder in S-Kurven, Herausfallen aus dem Zug oder Herausstrecken von Gliedmaßen
Fahrgäste (beim Ein- und Ausstieg)	Sturz ins Gleisbett (bevor Zug da ist), Sog von vorbeifahrendem Zug, Gefährdung durch ungesicherte Ladung eines vorbeifahrenden Zuges, Gefährdung beim Zustieg bzw. Ausstieg über befahrene Gleise (planmäßig oder unplanmäßig, siehe Gefährdung Personal an der Strecke), Sturz in Spalt zwischen Fahrzeug und Bahnsteig, Einklemmen in Tür, Mitschleifen, Sturz ins Gleisbett bei Ausstieg (falls kein Bahnsteig vorhanden)
Fahrgäste (im Evakuierungsfall)	Sturz beim Ausstieg, Überrollen auf noch befahrenen Gleisen, Quetschungen bei Panik
Fahrpersonal	siehe Fahrgäste
Personal an der	Überrollen, Sog, Gefährdung durch ungesicherte Ladung, Schotterflug,

Strecke	Gegenstände an der Strecke, Eisabwurf, Einklemmen in bewegliches Infrastrukturelement
Anwohner	siehe Personal an der Strecke
andere Verkehrsteilnehmer	Kollision beim Überqueren der Gleise, Überrollen, Sog, Gefährdung durch ungesicherte Ladung

Die in [BG RCI 2017] vorgeschlagenen sonstigen Gefährdungs- und Belastungsfaktoren sind auf den Arbeitsschutz ausgerichtet und erscheinen für die Identifizierung von funktionalen Sicherheitsanforderungen wenig passend. Weitere, für den vorliegenden Anwendungsfall relevante sonstige Gefährdungen wurden nicht identifiziert.

5.3.2 Gefährdungen für Sachgüter und die Umwelt

Neben den Gefährdungen für den Menschen sind auch Gefährdungen für Sachgüter und die Umwelt zu betrachten. Hierzu wird der vorläufige Gefährdungskatalog entsprechend erweitert. Tab. 12 enthält für die einzelnen Arten von Sachgütern und Umweltgefahren einen Überblick der für sie relevanten Gefährdungen (Sammlung durch Brainstorming).

Tab. 12: Übersicht der Gefährdungen von Sachgütern und Umwelt

Gefährdetes Sachgut bzw. Umweltgefahr	Gefährdungen
Eisenbahninfrastruktur	Entgleisungen, Überschreiten der zulässigen Geschwindigkeit, Überschreiten der Grenzlinien (planmäßige Lademaßüberschreitung oder ungesicherte Ladung), Schäden an der Infrastruktur, Befahren durch ein nicht geeignetes Fahrzeug (z. B. zu hohe Achslast), Kollision mit Einrichtungen der Infrastruktur (z. B. in Deckungsstellen), Stromabnehmerfehlfunktion, Unzulässige Verwendung von Fahrzeugfunktionen mit Auswirkungen auf die Infrastruktur (z. B. Wirbelstrombremse, ausfahrbare Trittstufen, Schneepflug), Wettereinflüsse
Eisenbahnfahrzeuge	Entgleisung / Verlassen des Fahrwegs, Kollision mit anderem Eisenbahnfahrzeug, Kollision mit anderem Verkehrsteilnehmer, Kollision mit Gegenstand, Überschreiten der Grenzlinien, Schäden an der Infrastruktur, Befahren einer nicht geeigneten Strecke, falsches Stromsystem, Überspannungen, falsche Spurweite, Wettereinflüsse
Transportgüter inkl. Gepäck	mechanische Beschädigung durch Entgleisung, Kollision oder hohe Beschleunigung bzw. Abbremsung, Fahrzeugbrand, Aussetzung hoher Wärme- bzw. Kälteentwicklung, Wettereinflüsse (bei nicht dagegen geschützten Ladung)
Gegenstände an der Strecke (Baustellen, Instandhaltungsmaterial, Gegenstände von Anwohnern, etc.)	Schotterflug, ungesicherte Ladung, Sog
Fahrzeuge anderer Verkehrsmittel an Bahnübergängen	*siehe andere Verkehrsteilnehmer in Tab. 11*

Tiere	Schotterflug, ungesicherte Ladung, Sog, Gefahrgutunfall, Brand
Pflanzen	Gefahrgutunfall, Brand
Boden	Gefahrgutunfall
Gewässer	Gefahrgutunfall
Luft	Gefahrgutunfall, Abgase

5.3.3 Gefährdungen durch nicht verhinderte Schadensausmaßvergrößerung

Als weitere Kategorie, die nicht auf der oben beschriebenen Untersuchung basiert, erscheinen „nicht verhinderte Schadensausmaßvergrößerungen“ sinnvoll. Bei dieser Kategorie handelt es sich nicht um primäre Gefährdungen, sondern um sekundäre Gefährdungen, die erst zum Tragen kommen, wenn bereits eine primäre Gefährdung eingetreten ist.

Eine Schadensausmaßvergrößerung kann leicht durch ein nicht vollständig durchdachtes Sicherheitssystem eintreten, beispielsweise, wenn das Sicherheitssystem aufgrund einer Schutzfunktion das Entfernen des Fahrzeugs oder der Insassen aus einer Gefahrenzone erschwert. Ein typisches Beispiel ist die Notbremsung bei einem Brand in einem Tunnel. In diesem Beispiel wird dem Problem durch Notbremsüberbrückungsfunktionen und bei ETCS durch die Möglichkeit der Definition sogenannter „Non Stopping Areas“ (NSA) begegnet. Ein anderes Beispiel ist die Reversing-Funktion von ETCS, die das automatische Herausholen eines Zuges aus einer Gefahrenfunktion ermöglichen soll.

Weitere Schadensausmaßvergrößerungen können durch eine entsprechende Gestaltung von Infrastruktur und Fahrzeugen beispielsweise bezüglich Crashsicherheit, Sollbruchstellen und der Gestaltung von Rettungswegen verhindert werden. Die letztgenannten Beispiele, die sich rein auf infrastruktur- oder fahrzeugseitige Aspekte beziehen und keinen Einfluss auf den Betrieb haben, werden mangels Relevanz für den Funktionsumfang der smartLogic jedoch nicht weiter betrachtet.

Zur Systematisierung wird die Gefährdung durch eine nicht verhinderte Schadensausmaß-vergrößerung jeweils auf Basis ihrer Primärgefährdungen betrachtet. Zu beachten ist, dass die Schadensausmaßvergrößerungen nicht den Ausfall der Sicherungsmaßnahmen umfassen, welche die Primärgefährdungen vermeiden sollen. Diese Sicherungsmaßnahmen sind erst die Antwort auf den hier erstellten Gefährdungskatalog. Zudem geht es an dieser Stelle nicht darum, grundsätzliche sicherungstechnische Prinzipien wie das Gebot der Fehleroffenbarung aufzuzählen. Tab. 13 enthält eine Übersicht möglicher Schadensausmaßvergrößerungen nach der zugrundeliegenden Primärgefährdung (Sammlung jeweils durch Brainstorming).

Tab. 13: mögliche Schadensausmaßvergrößerungen nach Primärgefährdung

Primärgefährdung(en)	**mögliche Schadensausmaßvergrößerungen**
Stürzen	keine oder fehlerhafte Anweisungen (z. B. zur Ausstiegsseite), fehlerhafte Gestaltung von Bahnsteig oder Zug
Überrollen	keine oder fehlerhafte Anweisungen oder Warnhinweise, keine Fluchtmöglichkeiten, keine Sichtbarkeit der Arbeitskräfte, zu lange Schließzeit bei BÜ (diverse durch Regelmissachtung)
Sog	keine Vorankündigung von durchfahrenden

	Fahrzeugbewegungen, fehlerhafte Gestaltung des Bahnsteigs,
Einklemmen	keine oder fehlerhafte Anweisungen oder Warnhinweise
abruptes Abbremsen oder sonstige mechanische Gefährdung durch Kollision oder Entgleisung, etc.	keine Möglichkeit Fahrzeug aus Gefahrenzone herauszuholen, keine oder fehlerhafte Vorwarnung, keine Notstoppmöglichkeit
zu schnelles Beschleunigen oder Bremsen	keine Vorankündigung
Panik	keine oder fehlerhaft gestaltete Fluchtwege
Stromunfall / Beeinträchtigung der Oberleitung	Einlassen von Personen in nicht abgeschalteten und geerdeten Bereich
Gefahrstoffunfall	keine Möglichkeit Fahrzeug aus Gefahrenzone herauszuholen
Folgen durch Fahrzeugbrand	keine Möglichkeit Fahrzeug aus Gefahrenzone herauszuholen, fehlerhafte Evakuierung
Schienenverkehrslärm	*wird als nicht sicherheitsrelevant betrachtet*
Überhitzung	keine Möglichkeit Fahrzeug aus Gefahrenzone herauszuholen oder zu evakuieren (z. B. stundenlanges Ausharren in überhitztem Zug)
Unterkühlung	keine Möglichkeit Fahrzeug aus Gefahrenzone herauszuholen, keine ausreichende Ausrüstung für Ausfall der Heizung
diverse durch Regelmissachtung	sich nicht selbst-erschließende Regeln; zu großer Anreiz Regel zu brechen (z. B. geschlossener Reisendenübergang bevor Zug abgefahren ist, zu lange Schließzeit bei BÜ), keine verlässliche Statusanzeige (z. B. Restschließzeit bei BÜ)

5.4 Auswertung von Unfallereignissen bzw. gefährlichen Ereignissen

Gemäß der beschriebenen Vorgehensweise wird in einem zweiten Schritt der gefundene vorläufige Gefährdungskatalog aus der systematischen Herleitung von Gefährdungen durch eine Auswertung aktueller Unfallereignisse (bzw. gefährlicher Ereignisse, gemäß Definition der BEU, siehe unten) ergänzt. Hierzu dienen, wie in Kapitel 5.2.2 erläutert, die Untersuchungsberichte der Bundesstelle für Eisenbahnunfalluntersuchung (BEU, vormals Eisenbahnunfalluntersuchungsstelle des Bundes EUB) als Grundlage. Die vollständige Auswertung der Untersuchungsberichte findet sich in Anlage 4. Im Folgenden werden die Ergebnisse sowie wesentlichen Erkenntnisse für die weitere Arbeit zusammengefasst.

5.4.1 Datengrundlage

Die BEU (bzw. EUB) veröffentlicht gemäß ihren Statuten einen Bericht, wenn ein Unfall mit Todesfolge, Schwerverletzten oder mindestens fünf Leichtverletzten stattgefunden hat oder wenn sie bei einem gefährlichen Ereignis davon ausgeht, dass die Untersuchung des Ereignisses die Sicherheit des Eisenbahnbetriebs verbessern könnte. Gefährliche Ereignisse sind dabei Unfälle oder Ereignisse, die zu einem Unfall hätten führen können. EIU und EVU müssen dazu gefährliche Ereignisse melden

[EUB 2009]. Meldepflichtige Ereignisse sind in Tab. 6 aufgeführt. Die Ereignisarten entsprechen auch der Gliederung der Unfallberichte der BEU.

Tab. 14: Meldepflichtige Ereignisse gemäß [EUB 2009]

Kategorie	Ereignisart
Unfall	Kollision
	Entgleisung
	Personenunfall
	Bahnübergangsunfall (Zusammenprall)
	Fahrzeugbrand
	Sonstiger Unfall im Eisenbahnbetrieb
Störung	Vorbeifahrt eines Zuges am Haltbegriff
	Unzulässige Einfahrt in einen besetzten Gleisabschnitt
	Störung am Bahnübergang (sofern nicht von Straßenverkehrsteilnehmern verursacht)
	sicherheitsrelevante Störung am Fahrzeug
	Störung an der Infrastruktur, der zu einem Nothalt eines Zuges führt
	Störung durch betriebliche Fehlhandlung

Suizide sind ausdrücklich von der Meldepflicht ausgeschlossen.

Die damalige Eisenbahnunfalluntersuchungsstelle des Bundes hatte bis zum Stichtag der Auswertung am 23.10.2017 insgesamt 96 Berichte zu gefährlichen Ereignissen auf ihrer Website veröffentlicht [BEU 2019]. Danach folgende Berichte sind in der folgenden, systematischen Auswertung nicht enthalten. Allerdings wurden neuere Berichte im Laufe des Entwicklungsprozesses der smartLogic weiterhin verfolgt und Erkenntnisse daraus wurden somit ebenfalls (indirekt) im Entwicklungsprozess berücksichtigt.

5.4.2 Fehlerarten

Um Gefährdungen zu verhindern, muss die Sicherungslogik die Ursachen der Gefährdungen vermeiden. Daher liegt der Fokus der Auswertung nicht darauf, in welcher Ausprägung sich das gefährliche Ereignis zeigte, also z. B. ob das Ereignis eine Entgleisung oder eine Kollision zur Folge hatte. Vielmehr ist von Interesse, welcher Umstand auslösend für das Eintreten des gefährlichen Ereignisses war, also was der initiale Fehler war. Prinzipiell werden häufig zum einen menschliche (auch Human Factors) und technische Fehler (bzw. technische Defekte) (bei Hard- oder Software) unterschieden und zum anderen systematische und zufällige Fehler (vor allem im Bereich der Messtechnik gebräuchlich, aber auch auf die vorliegende Arbeit übertragbar, vgl. hierzu z. B. [Papula, S. 646]).

Zufällige Fehler treten innerhalb der erwarteten, statistischen Ausfallverteilung auf und sind nicht vorhersehbar. Daher muss durch die Sicherungstechnik die Wahrscheinlichkeit für das Auftreten zufälliger Fehler soweit gesenkt werden, bis zufällige Fehler hinreichend selten auftreten oder ihre Auswirkungen mit hinreichender Wahrscheinlichkeit beherrscht werden können. Die Wahrscheinlichkeit für rein durch zufällige Fehler verursachte Unfälle ist im Eisenbahnbetrieb sehr gering, wie auch die Auswertung der gefährlichen Ereignisse zeigen wird. Jedoch können Unfälle durch zufällige Fehler naturgemäß nicht vollständig ausgeschlossen werden.

Systematische Fehler sind Fehler, die sich bei gleicher Ereigniskonstellation jeweils auf die gleiche Art und Weise auswirken. Sie sind theoretisch vorhersehbar und somit vermeidbar. In der Praxis ist jedoch zu beachten, dass die menschlichen Handlungen der menschlichen Fehlerwahrscheinlichkeiten unterliegen. Systematische Fehler sind damit in der Realität ebenfalls nie vollständig verhinderbar.

Technische Fehler bzw. Defekte sind zunächst Fehlfunktionen an technischen Anlagen. Allerdings können nur bewusst akzeptierte zufällige Fehler an technischen Anlagen als rein technische Fehler betrachtet werden, da systematische Fehlfunktionen an technischen Anlagen auf menschlichen Fehlern beruhen, die im Laufe der Lebenszeit der technischen Anlage gemacht wurden, z. B. bei der Entwicklung, Herstellung, Installation oder Instandhaltung (vgl. hierzu z. B. [Badke-Schaub et al. 2008, S. 5] zur Ursache technischer Defekte).

Neben diesen menschlichen Fehlern, die sich in technischen Fehlfunktionen zeigen, treten direkte menschliche Fehler durch fehlerhafte Handlungen des Betriebspersonals. Diese können ihre Ursache in den klassischen Fehlerursachen des Menschen haben, wie z. B. Überforderung, fehlerhafter Wahrnehmung, Müdigkeit, etc. Eine Unterscheidung der gefährlichen Ereignisse auf Basis menschlicher Fehlerursachen wird hier allerdings nicht vorgenommen, da für die Entscheidung über den Funktionsumfang der neuen Sicherungslogik nur wichtig ist, an welchen Stellen menschliche Fehler auftreten, nicht aber, wodurch sie verursacht wurden.

Abzugrenzen sind allerdings menschliche Fehlhandlungen auf Basis von Fehlern im Regelwerk. Regelwerke regeln den Umgang der beteiligten Menschen untereinander und mit der einzusetzenden Technik. Ist das Regelwerk fehlerhaft, so wird hier angenommen, dass der Fehler primär nicht durch den das Regelwerk befolgenden Beschäftigten, sondern bereits bei der Regelwerkserstellung verursacht wurde. Tab. 15 enthält eine Übersicht der so abgegrenzten, grundsätzlichen Fehlerarten.

Tab. 15: grundsätzliche Fehlerarten

Ursachenart	Erläuterung
zufällige technische Fehlfunktion	Die Fehlfunktion tritt innerhalb der erwarteten Versagenswahrscheinlichkeit auf. Es handelt sich also um ein in Kauf genommenes Risiko.
technische Fehlfunktion aufgrund eines Konstruktionsfehlers	Der Fehler tritt aufgrund einer Fehlkonstruktion einer technischen Komponente auf.
technische Fehlfunktion aufgrund fehlerhafter Montage oder Instandhaltung	Die Fehlfunktion tritt aufgrund einer falschen Herstellung, Montage oder Instandhaltung auf. Auch Transportfehler der Komponenten können hierunter fallen. Zu unterscheiden ist wiederum, ob der Fehler bereits im Regelwerk für den entsprechenden Arbeitsschritt vorliegt.
Fehler im Regelwerk	Der Fehler kann bei genauer Befolgung des Regelwerkes auftreten.
Fehler des Betriebspersonals	Der Fehler tritt durch eine fehlerhafte menschliche Handlung oder ein fehlerhaftes Befolgen des Regelwerkes auf.

Für die Klassifizierung der gefährlichen Ereignisse wurde zudem noch betrachtet, ob das Ereignis bereits durch eine bekannte Technik hätte verhindert werden können, die theoretisch hätte eingebaut werden können (ohne an dieser Stelle wirtschaftliche Aspekte zu berücksichtigen).

5.4.3 Auswertung

Tab. 16 gliedert die 96 von der EUB zum Stichtag untersuchten gefährlichen Ereignisse nach den zugrundeliegenden Ursachen.

In der vorliegenden Arbeit wird nur die infrastrukturseitige Sicherungstechnik und im Speziellen die Komponente der Sicherungslogik betrachtet. Aus Vereinfachungsgründen ist daher eine detaillierte Unterscheidung von fahrzeugseitigen Fehlern nur insofern notwendig, wie sie theoretisch infrastrukturseitig detektierbar wären. Weitere fahrzeugseitige Fehler werden als „Fahrzeugmangel" zusammengefasst. Die gleiche Argumentation kann auch auf Mängel am Bahnkörper übertragen werden, die nachfolgend unter „Versagen des Bahnkörpers" zusammengefasst sind. Es handelt sich um Gleislagefehler oder Schienenbruch.

Tab. 16: EUB-untersuchte gefährliche Ereignisse nach Ursachengruppe

Ursachengruppe	Anzahl
fehlerhaftes Handeln des Stellwerkspersonals bei Abweichungen vom Regelbetrieb	13
Fahrzeugmangel (ohne Heißläufer)	11
Bahnübergang missachtet (Straßenverkehr)	9
nicht oder fehlerhaft detektierter Heißläufer	8
Versagen des Bahnkörpers	7
fehlerhafte Bremsprobe / Zugbildung	6
unzeitige Fahrstraßenauflösung durch das Stellwerkspersonal	5
Fahrfehler	5
Kollision mit Gegenstand oder Tier(en)	5
keine oder fehlerhafte Fahrwegprüfung durch das Stellwerkspersonal	4
keine oder fehlerhafte Freimeldung eines Bahnübergangs (durch Stellwerkspersonal)	3
fehlerhafte Beladung	3
fehlerhaftes Verhalten nach Zwangsbremsung (durch Tf)	2
Sperrsignal missachtet	2
fehlerhafte Bauplanung	2
fehlerhafte Bauausführung	2
Konstruktionsfehler (Fahrzeug)	2
fehlerhafte Zugabfertigung (Fahrpersonal)	1
Hauptsignal missachtet, keine Zwangsbremsung	1
Zugleitbetrieb	1
fehlerhaftes Verhalten eines Bahnübergangssicherungspostens	1
Konstruktionsfehler (Gleisfreimeldeanlage)	1
Erdrutsch	1
Stellwerksfehlfunktion	1

Am häufigsten erscheint in der Auswertung die Gruppe „fehlerhaftes Handeln des Stellwerkspersonals bei Abweichungen vom Regelbetrieb". Bei den zu dieser Gruppe gehörenden Ereignissen wurde jeweils das betriebliche Regelwerk durch ein oder mehrere Mitglieder des Betriebspersonals nicht oder

fehlerhaft befolgt. Warum das Betriebspersonal das Regelwerk fehlerhaft befolgte, ist an dieser Stelle – wie unter „Fehlerarten“ geschildert – nicht relevant (Die Berichte der BEU erhalten hierzu nähere Angaben.). Diese Gruppe ist der Fehlerart „Fehlern des Betriebspersonals“ zuzuordnen (vgl. Tab. 15), zu der einige weitere Ursachengruppen gehören, die aufgrund ihrer Häufigkeit und der direkten Relevanz für die Gestaltung der Sicherungslogik extra ausgewiesen wurden. Hierzu gehören die unzeitige Fahrstraßenauflösung, die nicht erfolgte oder fehlerhaft durchgeführte Fahrwegprüfung sowie die nicht erfolgte oder fehlerhaft durchgeführte Freimeldung eines Bahnübergangs (BÜ) durch das Stellwerkspersonal.

Die letzte Gruppe der Bahnübergangsunfälle wird von Bahnübergangsunfällen abgegrenzt, bei denen der BÜ zwar korrekt gesichert war, aber vom Straßenverkehrsteilnehmer missachtet wurde. Diese Gruppe bildet die dritthäufigste Ursachengruppe, wobei die BEU nicht in jedem dieser Fälle einen Untersuchungsbericht veröffentlicht. Die Eintrittswahrscheinlichkeit dieser Ereignisse könnte zwar möglicherweise durch eine ausgereiftere Bahnübergangssicherungstechnik beeinflusst werden, jedoch nicht durch die Sicherungslogik, da keine Fehlfunktion in ihrem Bereich vorlag. Deshalb wird diese Ursachengruppe zu den externen Einflüssen gezählt.

Zudem ist ein Unfall auf das fehlerhafte Verhalten eines Bahnübergangssicherungspostens zurückzuführen. Dieser wurde aufgrund des besonderen Akteurs gesondert ausgewiesen und gehört ebenfalls zu den „Fehlern des Betriebspersonals“. Weitere Ursachengruppen, die zu dieser Fehlerart gezählt werden können, sind auf Seiten des Fahrpersonals Fahrfehler der Tf, fehlerhaftes Verhalten nach Zwangsbremsung, Sperrsignal missachtet und fehlerhafte Zugabfertigung. Fahrfehler sollten eigentlich durch technische Sicherheitsmaßnahmen verhindert werden. Diese sind aber noch nicht lückenlos. In der Gruppe verbergen sich Unfälle bei Rangierfahrten, die weniger stark überwacht werden und auf Fahrfehler der Tf zurückzuführen sind, einem Fall von Zurückrollen und einem Fall von zu früher Beschleunigung. Außerdem gibt es nicht regelkonformes Verhalten bei der Zugbildung und bei Bauarbeiten.

Der Eisenbahnunfall von Hordorf wurde gesondert aufgeführt (Hauptsignal missachtet, aber keine Zwangsbremsung), da er mit hoher Wahrscheinlichkeit durch eine Zugbeeinflussungseinrichtung, wie sie heute bereits besteht, aber an der Unglücksstelle planmäßig nicht vorhanden war, hätte verhindert werden können [EUB 2011, S. 24]. Ein Unfall fand im Betriebsverfahren „Zugleitbetrieb“ statt. Dieser Unfall wurde ebenfalls gesondert aufgeführt, da es sich um ein Betriebsverfahren mit reduzierter Sicherheitstechnik handelt und somit keine Vergleichbarkeit zu den anderen Ereignissen besteht.

Am zweithäufigsten sind die Fahrzeugmängel. Eine vertiefte Ursachenanalyse, inwiefern diese aus Instandhaltungsmängeln, Materialmängeln oder Konstruktionsmängeln, etc. resultieren, erfolgte nicht, da die Konstruktion und Beschaffenheit der Fahrzeuge, wie oben beschrieben, für die Bestimmung des Funktionsumfangs der infrastrukturseitigen Sicherungstechnik als rein fahrzeugseitige Eigenschaften nicht relevant sind. Heißläufer sind gesondert aufgeführt, da für sie bereits Detektionseinrichtungen existieren, sie allerdings dennoch die vierthäufigste Ursachengruppe darstellen. Für jeden Heißläufer gibt es daher einen Fahrzeugmangel als Primärursache, aber auch eine nicht erfolgte oder fehlerhafte Detektion als Sekundärursache. Letztere ist für die vorliegende Arbeit relevanter und wurde daher näher betrachtet. Dabei zeigten sich mehrere Probleme auf der technischen Seite. So lagen die Heißläuferortungsanlagen zu weit auseinander, wurden aufgrund betrieblicher Besonderheiten umfahren oder die gemessene Temperatur war zwar auffällig, lag aber unter dem Schwellwert. In einem anderen Fall, wurde der Heißläufer zwar korrekt detektiert, aber vom Betriebspersonal nicht die vorgeschriebenen Maßnahmen ergriffen. Dieser Fall wurde zur besseren Abgrenzung der Fehlerarten nicht der Gruppe der nicht oder fehlerhaft detektierten

Heißläufer zugeordnet, sondern der Gruppe fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb.

Auch das Versagen des Bahnkörpers war in insgesamt sieben Fällen Ursache eines Unfalls. Zwei Ereignisse wurden als Konstruktionsfehler auf Fahrzeugseite klassifiziert und ein Ereignis als Konstruktionsfehler der Gleisfreimeldeanlage. Weiterhin gab es ein Ereignis, zu dem eine Stellwerksfehlfunktion signifikant beigetragen hat.

Als externe Einflüsse werden ein Erdrutsch und die Gruppe der Kollision mit Gegenständen oder Tieren gewertet. Auch hierbei können jedoch ein rechtzeitiges Erkennen der Gefahr und/oder Maßnahmen zur Verhinderung der Beeinträchtigung der Bahnanlage durch die Hindernisse eine Rolle spielen. Die externen Einflüsse fließen daher ebenfalls in die Gefährdungsanalyse mit ein.

Tab. 17 enthält eine Übersicht der Zuordnung der Unfallereignisse zu den Fehlerarten aus Tab. 15. Eine Unterscheidung zwischen Konstruktionsfehlern und Montage oder Instandhaltungsfehlern wird aufgrund der bereits oben erläuterten nicht vorhandenen Relevanz für die Erstellung einer neuen Sicherungslogik jedoch nicht vorgenommen. Gesondert aufgeführt sind außerdem Ereignisse, die durch den aktuellen Stand der Technik bereits verhinderbar gewesen wären, wenn diese auf der am Ereignis beteiligten Infrastruktur ausgerüstet gewesen wäre, sowie externe Einflüsse. Zu beachten ist auch, dass die Ursachen für die Ereignisse vielschichtig sein können. Jedes Ereignis ist in Tab. 17 aber nur einer Fehlerart zugeordnet. Die Zuordnung erfolgt auf Basis der oben beschriebenen Kriterien.

Tab. 17: Zuordnung der gefährlichen Ereignisse zu Fehlerarten

Fehlerart	Beispiele	Anzahl
zufällige technische Fehlfunktion		0
Konstruktionsfehler, fehlerhafte Montage oder Instandhaltung	Fahrzeugmangel, Infrastrukturversagen, Konstruktionsfehler, Stellwerksfehlfunktion, nicht oder fehlerhaft detektierte Heißläufer	30
Fehler im Regelwerk		*0*
betriebspersonalbedingt inkl. Bauarbeiten	Stellwerkspersonalfehler, Fahrpersonalfehler, Zugbildungsfehler, Fehler bei Bauarbeiten	49
durch Stand der Technik bereits verhinderbar	Hauptsignal missachtet und keine Zwangsbremsung, Zugleitbetrieb	2
externe Einflüsse	Kollision mit Gegenstand, Bahnübergang missachtet, Erdrutsch	15

Der Fehlerart „zufällige technische Fehlfunktion“ wurde kein Ereignis zugeordnet. Den Fehlern im Regelwerk wurde ebenfalls kein Ereignis zugeordnet, da der Fehler im Regelwerk bei keinem Ereignis als Hauptursache gezählt wurde. Allerdings zeigte sich, dass diese Zuordnung insofern problematisch ist, dass bei fast allen Unfällen ein anderes Regelwerk den Unfall hätte verhindern oder das Schadensausmaß abmildern können, mit entsprechenden Nebeneffekten auf die Kapazität[21]. Deshalb wurde diese Fehlerart *kursiv* gedruckt. Die betriebspersonalbedingten Fehler haben dagegen eine besonders große Bedeutung, denn hier könnte durch zusätzliche Automatisierung noch Potenzial für Sicherheitsverbesserungen liegen. Auch wenn Sicherheitsverbesserungen nicht das primäre Ziel der Arbeit sind, macht es trotzdem Sinn, die personalbedingten Fehler genauer zu analysieren. Tab. 18

[21] Zum Beispiel wurde nach dem Unfall in Bad Aibling das Regelwerk insofern geändert, dass der erste Zug nach Auftreten einer Störung und damit verbundener Zulassung der Zugfahrt ohne vollständige technische Sicherung auf Sicht fahren muss. Trotzdem wurde das Ereignis als betriebspersonalbedingter Fehler eingeordnet, da das bestehende Regelwerk auch nicht korrekt befolgt wurde.

zeigt die Ursachengruppen nach Personalgruppen gegliedert. Die meisten der betriebspersonalbedingten Fehler, die zu einem gefährlichen Ereignis führten, treten dabei in der Gruppe der Stellwerkspersonale auf, die in der bisherigen Sicherungstechnik eine regelmäßige Interaktion mit der Sicherungslogik der Stellwerke haben.

Tab. 18: betriebspersonalbedingte Ursachengruppen der gefährlichen Ereignisse nach Personalgruppe

Personalgruppe	Ursache	Ereignisse
Stellwerkspersonal	fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	13
	unzeitige Fahrstraßenauflösung	5
	keine oder fehlerhafte Fahrwegprüfung	4
	keine oder fehlerhafte Freimeldung eines Bahnübergangs	3
	GESAMT	25
Fahrpersonal	Fahrfehler	5
	fehlerhaftes Verhalten nach Zwangsbremsung	2
	Sperrsignal missachtet	2
	fehlerhafte Zugabfertigung	1
	GESAMT	10
Beladungs- und Zugbildungspersonal	fehlerhafte Bremsprobe / Zugbildung	6
	fehlerhafte Beladung	3
	GESAMT	9
Planung und Durchführung von Bauarbeiten	fehlerhafte Bauplanung	2
	fehlerhafte Bauausführung	2
	GESAMT	4
Posten	fehlerhaftes Verhalten eines Bahnübergangssicherungspostens	1

5.4.4 Erkenntnisse

Die Auswertung unterstützt, dass der Gefährdungskatalog nicht auf die klassischen sicherungstechnischen Gefährdungen der Verhinderung von Kollisionen durch Fahrstraßenausschlüsse, Folge- und Flankenschutz und Erlaubnisprinzip sowie Entgleisungen mittels Geschwindigkeitsüberwachung und Fahrstraßenverschluss begrenzt werden sollte.

Neben den bekannten Bahnübergangsunfällen fallen auch die Ursachengruppen Fahrzeugmangel und nicht oder fehlerhaft detektierte Heißläufer ins Gewicht. Insbesondere der zweiten Ursachenart wird bereits mittels verschiedener Ortungstechnologien wie Heißläufer- und Festbremsortungsanlagen begegnet. Einige der oben erfassten Ereignisse sind jedoch aufgrund von nicht regelwerkskonformen Reaktionen der beteiligten Menschen auf Warnhinweise zumindest nicht verhindert worden. In diesem Zusammenhang könnte eine zu prüfende direkte Integration vorhandener Messeinrichtungen

in die Sicherungslogik über eine geeignete Schnittstelle hilfreich sein und sollte im Weiteren untersucht werden. Gefährdungen, die sich aus Fahrzeugmängeln ergeben, sollten daher in einem vollständigen Gefährdungskatalog für die Ausarbeitung der funktionalen Sicherheitsanforderungen enthalten sein. Auch mögliche kontinuierliche Überwachungseinrichtungen für den Gleiskörper könnten wichtig sein, wie die Auswertung zeigt und sollten bei den Gefährdungen berücksichtigt werden.

Wichtig ist an dieser Stelle zu betonen, dass durch die obigen Erkenntnisse keine Aussage getroffen werden soll, ob und wann zusätzliche technische Sicherungseinrichtungen wirklich notwendig sind. Jedes Unfallereignis ist letztlich auf sehr spezielle Ereignisketten zurückzuführen. Auch wirtschaftliche Überlegungen sind aus Überzeugung des Autors zulässig. Denn eine wirtschaftlich betriebene Eisenbahnstrecke kann immer noch erheblich sicherer sein, als eine nicht mehr wirtschaftliche Eisenbahnstrecke, die z. B. durch Busverkehr ersetzt wurde. Jedoch sollte eine zu entwickelnde Sicherungslogik auf entsprechende Sicherheitsanforderungen vorbereitet sein, indem sie z. B. Schnittstellen für technische Überwachungseinrichtungen bereit hält.

Die größte identifizierte Ursachengruppe ist fehlerhaftes Handeln des Stellwerkspersonals bei Abweichungen vom Regelbetrieb. In der Rückfalleben werden sicherungstechnische Aufgaben von der Technik auf das Betriebspersonal verlagert. Die Zahl der gefährlichen Ereignisse in solchen Fällen unterstreicht die Anforderung, die sich bereits aus der Zieldimension der Robustheit an das Design der Sicherungslogik ergibt: Die Sicherungslogik sollte auch bei Abweichungen vom Regelbetrieb wie Störungen jeglicher Art noch den maximal möglichen Sicherungsumfang gewährleisten und manuelle Rückfallebenen, wann immer es geht, vermeiden.

Insgesamt sind mit Abstand am meisten Ereignisse der betriebspersonalbedingten Fehlerart zugeordnet. Davon liegen wiederum am meisten auf Seiten des Stellwerkspersonals. Insbesondere (regelmäßig oder unregelmäßig) durchzuführende, manuelle Räumungs- bzw. Fahrwegprüfungen scheinen erhöhtes Fehlerpotential zu bieten. Dies kann als weiterer Indikator dafür dienen, insgesamt auf eine möglichst hohe Automatisierung zu setzen, da im Gegenzug die technisch bedingten Ursachen klar in der Unterzahl sind. Für eine klare Aussage hierzu ist allerdings die vorliegende Studie nicht aussagekräftig genug. Dies ist auch nicht das Ziel der hier durchgeführten Gefährdungsanalyse. Der zuvor generierte vorläufige Gefährdungskatalog kann hingegen auf Basis der Auswertung der Unfallereignisse um den Aspekt der Rückfallebene erweitert werden.

Bei den weiteren betriebspersonalbedingten Ereignissen, die nicht dem Stellwerkspersonal zuzuordnen sind, muss noch untersucht werden, inwieweit diese auch durch die Komponente Sicherungslogik beeinflusst werden können (siehe Kapitel 5.5). Die Ereignisse der Gruppe Fahrfehler waren teilweise auf nicht ausreichende Überwachung bei punktförmigen Zugbeeinflussungssystemen zurückzuführen. Dieses Problem wird mit kontinuierlicher Überwachung, wie sie bei ETCS in höheren Leveln (aber auch bereits bei der LZB) eingesetzt wird, behoben.

Nach dem Untersuchungsstichtag veröffentlichte Unfallereignisse stützen die beschriebenen Erkenntnisse.

5.5 der vorläufige Gefährdungskatalog

Aus der systematischen Herleitung von Gefährdungen (Kapitel 5.3) und der Auswertung von gefährlichen Ereignissen (Kapitel 5.4) kann nun ein vorläufiger Gefährdungskatalog inkl. der identifizierten primären Ursachen entwickelt werden. Dafür ist eine sinnvolle Gliederung zu wählen. Abb. 37 enthält eine Übersicht des Gefährdungskatalogs mit den acht gewählten Hauptgefährdungen, die im Folgenden näher erläutert werden. Zur Hauptgefährdung „Kollision“ ist in der Abbildung die

nachgeordnete Systematik beispielhaft aufgeklappt. Die Hauptgefährdungen sind fett und mit grüner Linie dargestellt.

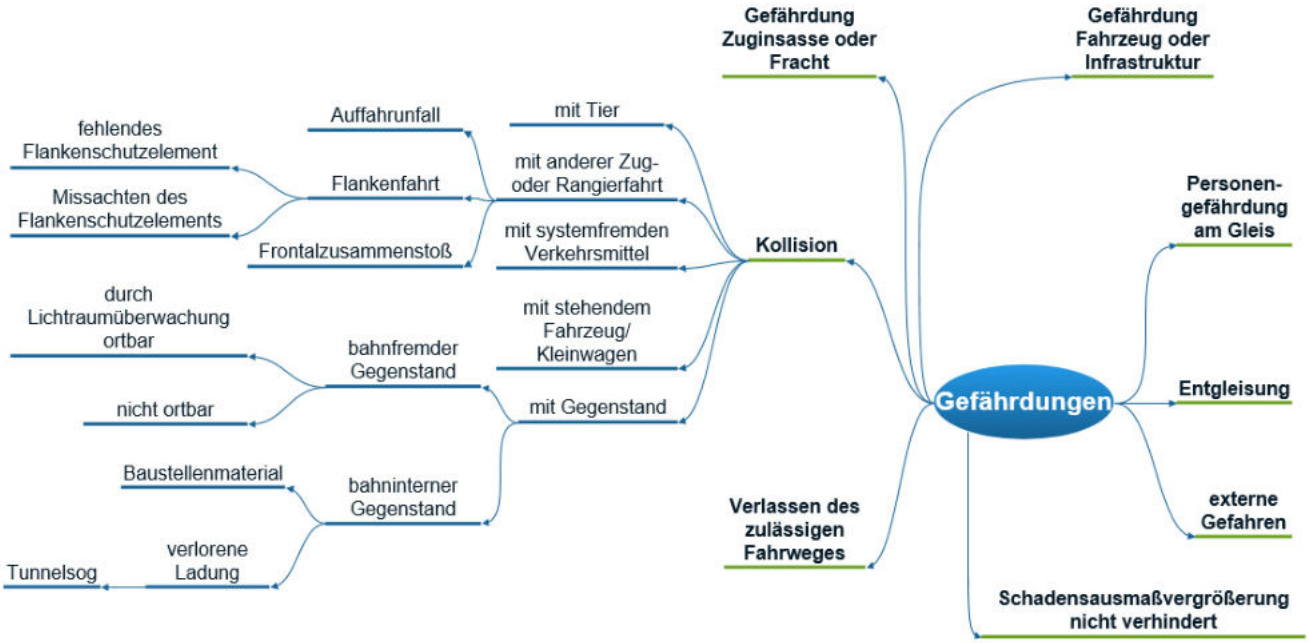


Abb. 37: Auszug aus der Gefährdungsübersicht (Hauptgruppe Kollision aufgeklappt) [Eigene Darstellung]

Die Einteilung der Gefährdungsübersicht hätte prinzipiell analog zur Vorgehensweise zur Identifizierung der Gefährdungen stattfinden können. Dann wären die Hauptgruppen „Gefährdungen für den Menschen“, „Gefährdungen von Sachgütern“ und „Gefährdungen der Umwelt“ gewesen. Diese Einteilung erscheint aber zur Herleitung der funktionalen Sicherheitsanforderungen weniger geeignet, da es viele Dopplungen geben würde. Stattdessen bietet es sich an, für die häufigsten tatsächlichen Unfallarten eigene Hauptgruppen zu definieren und die identifizierten Einzelgefährdungen und Ursachen zur feineren Untergliederung innerhalb dieser Hauptgruppen zu nutzen. Dies bietet auch den Vorteil, dass die Hauptgefährdungen als TOP-Gefährdungen für die im Rahmen einer anschließenden Produktentwicklung vorgeschriebene Risikoanalyse genutzt werden können.

Die Hauptgefährdungen **Kollision** und **Entgleisung** bedürfen als klassische Gefährdungen der Eisenbahnsicherungstechnik keiner ausführlichen Erläuterung. Der Gruppe „**Verlassen des zulässigen Fahrweges**“ sind verschiedene Arten von Gefährdung zugeordnet (beispielsweise Überfahren des Gleisendes, Fahrt in offene Deckungsstelle, Fahrt in ein nicht zulässiges Gleis, z. B. mit nicht eingehaltenem Lichtraumprofil, etc.). Häufig wäre die Folge ebenfalls eine Entgleisung oder aber auch die Beschädigung von Infrastruktur oder Fahrzeug. Aufgrund der Ähnlichkeit der aus dieser Gruppe folgenden funktionalen Sicherheitsanforderungen, wurden sie in einer eigenen Gruppe zusammengefasst.

Für einige Gruppen Gefährdeter würde die Einteilung nach tatsächlichen Unfallarten allerdings zu umfangreich werden. Beispielsweise für die spezifischen Gefährdungen von Zuginsassen, die sich nicht aus einer der vorgenannten Hauptgefährdungen ergeben. Deshalb wurde für diese eine eigene Hauptgruppe gebildet. Die Gefährdungen für die Zuginsassen sind umfangreicher als die für die transportierte Fracht. Die Gefährdungen für Letztere gehen aber häufig einher mit Gefährdungen für die Zuginsassen. Deshalb wurden sie mit der Hauptgruppe Gefährdungen für Zuginsassen zur Hauptgruppe „**Gefährdung Zuginsasse oder Fracht**“ zusammengefasst. Eine weitere solche Gruppe

Gefährdeter sind die Personen am Gleis. Hier macht es Sinn, alle Personen, die sich in Gleisnähe aufhalten, zusammenzufassen, denn für sie existieren häufig dieselben Gefährdungen. Die zugehörige Hauptgefährdungsgruppe ist „**Personengefährdung am Gleis“**.

Als extra Gruppe wurden auch die „**externen Gefahren**“ ausgewiesen. Hierzu zählen Umgebungseinflüsse, die eine Gefährdung für den Bahnbetrieb erzeugen können. Die Entstehung des Primärereignis kann dabei i. d. R. nicht durch die Gestaltung des Systems Eisenbahn beeinflusst werden. Jedoch können geeignete Präventionsmaßnahmen, eine rechtzeitige Detektion und eine schnelle und zielgerichtete Reaktion den Schadenseintritt verhindern oder begrenzen.

Hieran anknüpfend erhält die Gruppe „**Schadensausmaßvergrößerung nicht verhindert**“ die Gefährdungen, die insbesondere aus fehlerhaften oder nicht erfolgten Reaktionen auf Primärgefährdungen ergeben. Diese Gruppe basiert auf den Erkenntnissen aus Kapitel 5.3.3. Gefährdungen durch nicht verhinderte Schadensausmaßvergrößerungen können jedoch nicht nur in Folge von externen Gefahren entstehen, sondern auch in Folge von Gefährdungen aus den anderen Hauptgruppen.

5.6 Relevanz der Gefährdungen für die infrastrukturseitige Sicherungstechnik

Wie in der Einleitung zu Kapitel 5.3 beschrieben, ist vor allem durch die systematische Herleitung der Gefährdungen ein sehr umfangreicher Gefährdungskatalog entstanden. Nicht alle dieser Gefährdungen können durch die infrastrukturseitige Sicherungstechnik verhindert oder eingeschränkt werden. Daher ist der Zuständigkeitsbereich der infrastrukturseitigen Sicherungstechnik und ihrer Komponente Sicherungslogik abzugrenzen. Dabei soll jedoch nicht eine Vorfestlegung über den genauen Zuschnitt der Komponente Sicherungslogik innerhalb der infrastrukturseitigen Sicherungstechnik erfolgen. Die Abgrenzung soll demnach großzügig erfolgen, in dem Sinne, dass eher zu viele Gefährdungen als relevant betrachtet werden, als zu wenige. Ein Ausschluss muss begründet werden.

Um diesen Anforderungen gerecht zu werden, wurde jeder identifizierten Gefährdung in der Übersicht eine Farbe zugewiesen. Rote Gefährdungen müssen durch die infrastrukturseitige Sicherungstechnik zuverlässig (also mit der erforderlichen Wahrscheinlichkeit) verhindert werden. Orangene Gefährdungen können durch die infrastrukturseitige Sicherungstechnik teilweise verhindert oder ihre Auswirkungen bzw. Eintrittswahrscheinlichkeit verringert werden. Neutrale (schwarze) Gefährdungen können durch die infrastrukturseitige Sicherungstechnik nur gering oder nicht beeinflusst werden.

Bewertungsgrundlage bilden der aktuelle Stand der Technik und zukünftig absehbare oder vorstellbare Entwicklungen. Die Einschätzung erfolgte durch den Autor mit der Unterstützung von Kollegen und in Rücksprache mit Fachkollegen der DB Netz AG.

Abb. 38 enthält einen Ausschnitt aus der so klassifizierten Gefährdungsübersicht. Die vollständige Gefährdungsübersicht findet sich in Anlage 4.

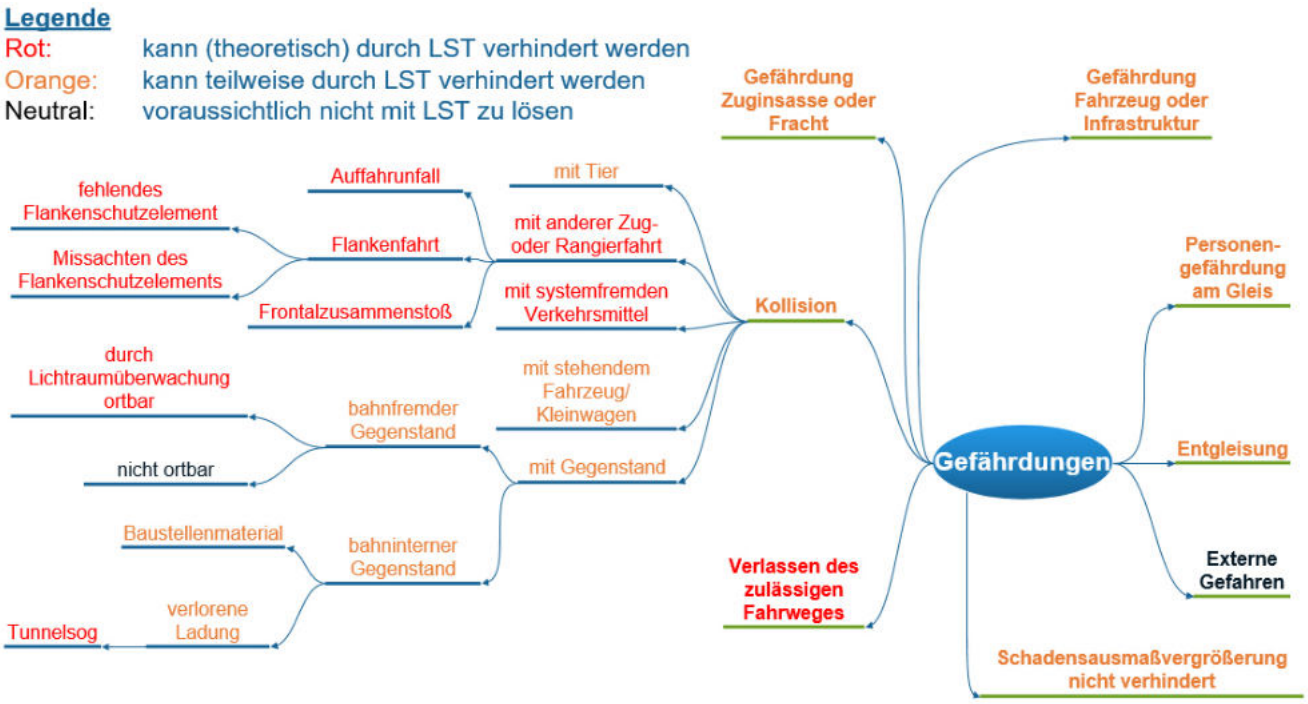


Abb. 38: Auszug aus der bzgl. Relevanz klassifizierten Gefährdungsübersicht (Hauptgruppe Kollision aufgeklappt) [Eigene Darstellung]

5.7 Ergebnisdiskussion

Der in Kapitel 5.6 verbliebene relevante Gefährdungskatalog rechtfertigt nicht mehr eine reine Fokussierung der infrastrukturseitigen Sicherungstechnik auf die Vermeidung von Entgleisungen und Kollisionen. Stattdessen ist es wichtig, dass eine zu entwickelnde Sicherungslogik gemäß den globalen Anforderungen aus Kapitel 3.5 auch zukunftssicher für mögliche zukünftige funktionale Sicherungsanforderungen ist. Die Auswertung der gefährlichen Ereignisse zeigt, dass mit weiteren solchen Anforderungen zu rechnen ist (vgl. Kapitel 5.4.4). Insbesondere in Bezug auf die Vermeidung von Fehlhandlungen des Betriebspersonals sollte geprüft werden, ob weitere Gefährdungspfade in die Prüflogik der Sicherungslogik integriert werden können. Dies gilt für den Regelbetrieb und vor allem auch für Rückfallebenen. Die Untersuchung unterstützt die Forderung, dass die zukünftige Sicherungslogik bei möglichst vielen Abweichungen vom Regelbetrieb noch (ggf. mit eingeschränkter Schutzfunktion) genutzt werden kann.

Die Auswertung von Unfallereignissen (vgl. Kapitel 5.4) rechtfertigt zudem die Aussage, dass mit einer angepassten Sicherungslogik in Zusammenhang mit ETCS auch die Zahl der verbleibenden Unfälle reduziert werden könnte.

5.8 Vergleich mit alternativen Ansätzen

Der Gefährdungskatalog wurde in dieser Arbeit aufgrund des gewählten „Grüne Wiese“-Ansatzes bewusst in einer eigenen Gefährdungsanalyse entwickelt. In diesem Kapitel soll der entwickelte Gefährdungskatalog kurz mit bestehenden Gefährdungskatalogen verglichen werden.

Wie bereits mehrfach zitiert, unterscheidet TRINCKAUF in [Trinckauf 2013] die Anforderungen an die Eisenbahnsicherungstechnik in Anforderungen erster und zweiter Ordnung. Anforderungen erster Ortung sind die Gewährleistung von Signalabhängigkeit, Folgefahrschutz und Gegenfahrschutz/Flankenschutz. Sie dienen damit zur Vermeidung von Entgleisung und Kollisionen

mit anderen Eisenbahnfahrzeugen. Zu den Anforderungen zweiter Ortung gehören die Sicherung von Gefahrenbereichen wie „Bahnübergangssicherung, Beschäftigte an Gleisbaustellen und Reisendensicherung am Bahnsteig“ sowie die Sicherstellung der Zugintegrität inkl. „Zugschlusserkennung, Bremsfähigkeitsüberwachung, Heißläuferfeststellung, Türkontrolle/-Ladungssicherung, Geschwindigkeitsanpassung bei fahrdynamischen Umgebungseinflüssen“. Der zugrundeliegende Gefährdungskatalog ist auf die historisch bekannten Gefährdungen und Unfallereignisse zurückzuführen. In dieser Arbeit wurden die Gefährdungen dagegen zunächst theoretisch hergeleitet und erst im zweiten Schritt durch tatsächliche Unfallereignisse ergänzt. Damit ist ein weiterer, nicht historischer Blickwinkel auf mögliche Gefährdungen enthalten. Dieser kann wertvoll sein, wenn es um mögliche zukünftig in die Sicherungslogik zu integrierenden funktionale Sicherheitsanforderungen geht, wie beispielsweise den Schutz von Fahrgästen beim Ein- und Ausstieg oder den Schutz von Personal am Gleis.

Maschek beschreibt in [Maschek 2009] ebenfalls eine systematische Herleitung von Gefährdungen und darauf aufbauend die „Schutzfunktionen“, die die Sicherungstechnik zu gewährleisten hat. Ausgangspunkt sind die Systemeigenschaften des Schienenverkehrs, deren lange Bremswege eine Kollisionssicherung und die Spurführung einen Schutz vor Entgleisung notwendig machen. Zu den Gefährdungen können nun Ursachen ermittelt werden, die mittels einer Fehlerbaumanalyse immer weiter heruntergebrochen werden können, bis ein geeigneter Detaillierungsgrad je nach Anwendungszweck erreicht ist.

Umfangreiche Gefährdungskataloge unterhalten auch die Unfalluntersuchungsbehörden. Der Katalog der deutschen Bundesstelle für Eisenbahnunfalluntersuchung wurde in Kapitel 5.4.1 vorgestellt und ist dort in die Entwicklung des hier erstellten Gefährdungskatalogs mit eingegangen. Der internationale Eisenbahnverband UIC führt zudem länderübergreifend eine Sicherheitsdatenbank und gliedert dort nach einem umfangreichen Schema in die Hauptgruppen Infrastruktur, Fahrzeuge, Faktor Mensch (Personal und Auftragnehmer), Bahnbenutzer, Wetter & Umwelt, Dritte und Sonstige („Nicht gekennzeichnet“) [UIC 2013]. Zudem veröffentlicht die UIC jährlich einen Sicherheitsbericht (vgl. für das Berichtsjahr 2016 [UIC 2017]). Der UIC-Ursachenbaum eignet sich aufgrund seiner umfangreichen Struktur gut zur weiteren Vollständigkeitskontrolle des entstandenen Gefährdungskatalogs.

Einen weiteren Gefährdungskatalog liefert WEHR in [Wehr 2017], der in Abb. 39 dargestellt ist.

<table>
<tr><th colspan="2">Im System</th><th>Von außen</th><th>Nach außen</th></tr>
<tr><td>Rollmaterial</td><td>Technische Mängel
Bremsstörungen
Zugtrennungen
Mangelhafte Verladung</td><td rowspan="3">• Naturgefahren
• Schienengleiche Eisenbahnkreuzungen
• Bahnfrevel</td><td rowspan="3">• Gefahrguttransporte
• Brand
• Erschütterungen
• Tunnelsicherheit</td></tr>
<tr><td>Infrastruktur</td><td>Schadhafte Anlagen</td></tr>
<tr><td>Betrieb</td><td>Unerlaubte Signalüberfahrung
unerlaubtes Einlassen in besetzten Gleisabschnitt
Fehlein-, -ausfahrt, Fehlleitung
Fahren ohne Fahrerlaubnis
Entrollen von Schienenfahrzeugen</td></tr>
</table>

Abb. 39: Gefährdungen für den Bahnbetrieb nach WEHR
Quelle: [Wehr 2017]

Der Gefährdungskatalog ist deutlich weniger umfangreich als der in dieser Arbeit entwickelte Gefährdungskatalog oder der Ursachenbaum der UIC-Sicherheitsdatenbank. Interessant für die vorliegende Arbeit ist vor allem die Untergliederung im Bereich Betrieb, die auch Aspekte wie „Fehlleitung“ aufführt, die auf dem ersten Blick nicht sicherheitsrelevant erscheinen, aber zu weiteren Fehlhandlungen führen können.

Auch MEYER ZU HÖRSTE liefert in seiner Dissertation einen Gefährdungskatalog (vgl. Abb. 40), dessen Herleitung er allerdings nicht systematisch beschrieben hat, wie dies in der vorliegenden Arbeit erfolgt ist. Der Gefährdungskatalog nach Meyer zu Hörste ist demnach auch weniger ausführlich und ist ebenfalls nicht zukunftsfest (vgl. die Anmerkung zu [Trinckauf 2013] oben).

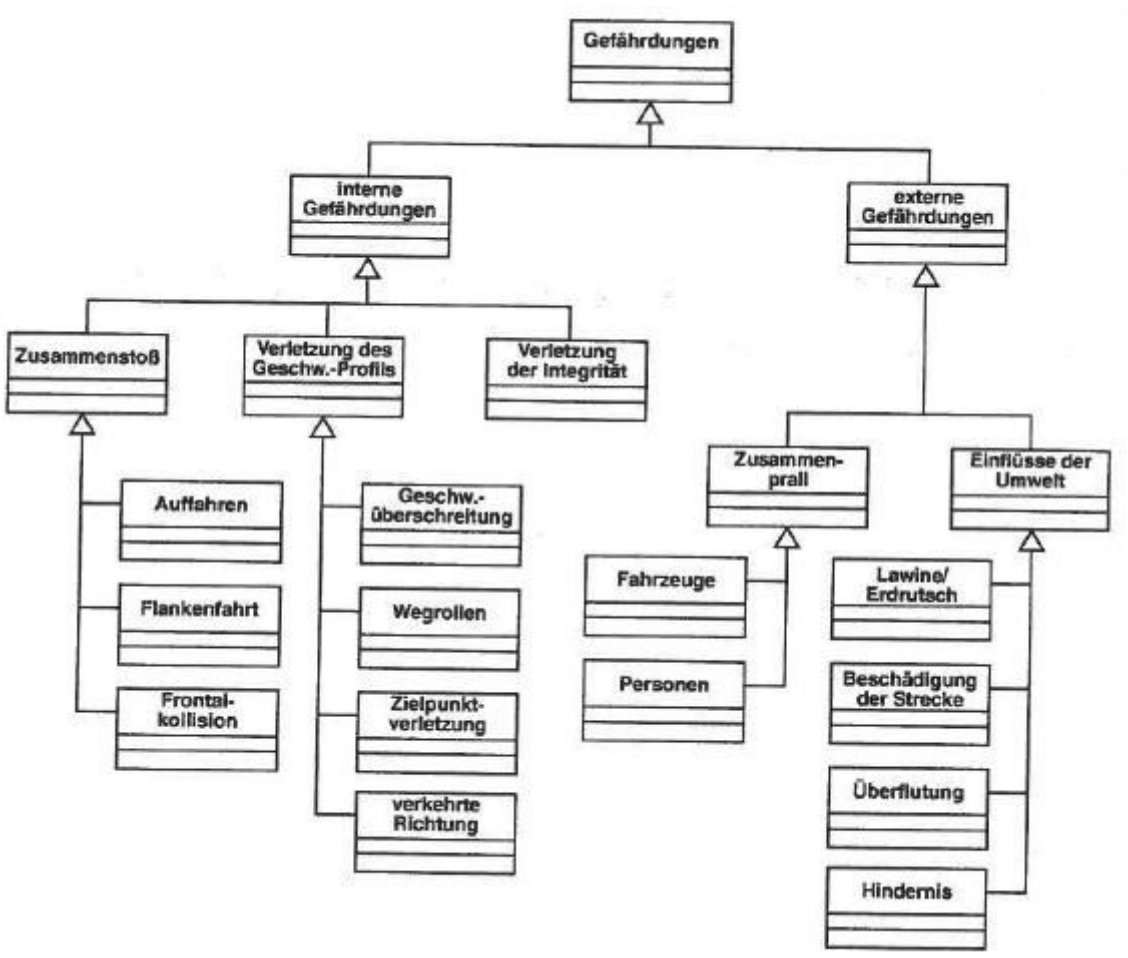


Abb. 40: Gefährdungen für den Bahnbetrieb nach MEYER ZU HÖRSTE
Quelle: [Meyer zu Hörste 2003]

Ein weiterer Gefährdungskatalog wird in der Dissertation von BOSSE hergeleitet (vgl. [Bosse 2010] und Kapitel 2.3.3). Die Dissertation enthält allerdings nicht den vollständigen Katalog und die Gefährdungen werden direkt mit den betrieblichen Funktionen verbunden, so dass ein Vergleich zwischen dem hier erarbeiteten Gefährdungskatalog mit dem Ergebnis der Arbeit von BOSSE schwierig ist.

5.9 Zusammenfassung

Im vorliegenden Hauptkapitel wurde in mehreren Schritten ein Gefährdungskatalog als Grundlage für die Festlegung der funktionalen Sicherheitsanforderungen an die smartLogic systematisch hergeleitet. Zunächst wurde hierfür ein erster Gefährdungskatalog erstellt, indem für die identifizierten

Beteiligten (Stakeholder) am Bahnbetrieb sowie betroffene Sachgüter und die Umwelt verschiedene Gefährdungsthemenfelder analysiert und mögliche Gefährdungen daraus abgeleitet wurden. Durch eine Auswertung von zurückliegenden Unfallereignissen bzw. gefährlichen Ereignissen und dem Vergleich mit alternativen Gefährdungskatalogen aus der Literatur konnte dieser erste Gefährdungskatalog soweit wie möglich vervollständigt werden. Anschließend wurden aus den gefundenen Gefährdungen diejenigen identifiziert, deren Eintritt durch die Gestaltung der infrastrukturseitigen Sicherungstechnik beeinflusst werden kann.

Im Vergleich zu alternativen Ansätzen unterscheidet sich der in dieser Arbeit entwickelte Gefährdungskatalog insbesondere durch den Einbezug von umfangreichen Überlegungen zum Schutz der Zuginsassen in allen Phasen ihres Kontakts mit dem Bahnbetrieb sowie durch den Einbezug der Gefährdungsgruppe „Schadensausmaßvergrößerungen nicht verhindert“. Zudem enthält er eine alternative Gliederung der Gefährdungen, die aus der systematischen Herleitung ausgehend von den Gefährdeten resultiert. Dies ermöglicht es, neben den klassischen Gefährdungen, die durch die Eisenbahnsicherungstechnik adressiert werden, weitere Gefährdungen in die Bestimmung des Funktionsumfangs der zu erstellenden Sicherungslogik miteinzubeziehen, die möglicherweise in Zukunft in Folge von neuen Sicherheitsanforderungen berücksichtigt werden müssen. Bei der Erstellung des Gefährdungskatalogs zeigte sich bereits, dass eine solche Ausdehnung der Menge der von der Sicherungslogik adressierten Gefährdungen sinnvoll sein kann, um die Eintrittswahrscheinlichkeit bestimmter Unfallereignisgruppen weiter zu verringern (vgl. Ergebnisdiskussion in Kapitel 5.7).

Der umfangreiche Gefährdungskatalog kann nicht mit abschließender Sicherheit als vollständig betrachtet werden, dennoch zeigt der Vergleich mit bestehenden Gefährdungskatalogen, dass von einer guten Abdeckungsquote der relevanten Gefährdungen ausgegangen werden kann.

6 Bestimmung der funktionalen Anforderungen (Funktionsanalyse)

Der festgelegten Vorgehensweise (vgl. Kapitel 3.6.6) folgend, sollen in diesem Hauptkapitel die funktionalen Systemanforderungen an die Sicherungslogik (im Weiteren auch kurz als „**funktionale Anforderungen**“ bzw. „**Funktionen**“ der Sicherungslogik bezeichnet) identifiziert werden, die in einem **Funktionskatalog** für die Entwicklung der smartLogic zusammengefasst werden können. Notwendige Funktionen können zum einen aus der Zielsetzung (vgl. Hauptkapitel 3) gemäß der Abgrenzung der Sicherungslogik innerhalb der infrastrukturseitigen Sicherungstechnik (vgl. Hauptkapitel 4) hergeleitet werden. Es handelt sich damit um betrieblich erforderliche Funktionen (= betriebliche funktionale Anforderungen). Zum anderen muss die Sicherungslogik die zur Aufrechterhaltung der Sicherheit erforderlichen aus der Gefährdungsanalyse in Hauptkapitel 5 hergeleiteten funktionalen Anforderungen (= funktionale Sicherheitsanforderungen) erfüllen.

Die Struktur des Hauptkapitels folgt dem allgemeinen Aufbau der Hauptkapitel in dieser Arbeit (vgl. Kapitel 1.3). Demnach wird das Ziel dieses Hauptkapitels im ersten Kapitel (6.1) näher erläutert. Aufbauend auf einer geeigneten Methode und Vorgehensweise für das Hauptkapitel, die in Kapitel 6.2 hergeleitet und beschrieben wird, werden die Gliederung und die Inhalte der weiteren Kapitel des Hauptkapitels festgelegt.

6.1 Ziel und Aufbau des Kapitels

Das globale Ziel der Sicherungslogik ist es, die Sicherheit von Zustandsänderungen im Bahnbetrieb, wie die Genehmigung von Fahrerlaubnissen und geplante Statusänderungen von Infrastrukturelementen, sicherzustellen sowie auf ungeplante Ereignisse mit Sicherheitsreaktionen zu reagieren (vgl. Kapitel 3.2 und 4.3). Die Kernanforderung der sicheren Logik aus Kapitel 3.5 fordert, dass alle notwendigen Schutzfunktionen durch die zu entwickelnde Sicherungslogik smartLogic abgedeckt werden müssen. Das bedeutet, die smartLogic muss bei jeder an sie gerichteten Anfrage bzw. bei jedem an sie gemeldeten Ereignis in Folge einer Änderung der Umweltsituation (z. B. Position Report, auffälliges Messergebnis eines infrastrukturseitigen Sensors etc.) sicherstellen, dass im Bahnbetrieb kein unsicherer Zustand auftritt oder zumindest – sofern ein unsicherer Zustand nicht vermeidbar ist – der Schaden minimiert wird (vgl. auch Kapitel 5.1).

Die Kernanforderung benennt jedoch die notwendigen Schutzfunktionen nicht im Detail. Diese Schutzfunktionen müssen daher aus dem in Kapitel 5 erstellten Gefährdungskatalog ermittelt werden (vgl. die Herleitung und Beschreibung der grundsätzlichen Vorgehensweise dieser Arbeit in Kapitel 3.6). Jede zu gewährleistende Schutzfunktion stellt eine **funktionale Sicherheitsanforderung** an die Entwicklung der smartLogic. Die zu entwickelnden Prozesse der smartLogic müssen die Einhaltung aller funktionalen Sicherheitsanforderungen bzw. Schutzfunktionen garantieren. Deshalb ist es Aufgabe dieses Hauptkapitels, die Schutzfunktionen zu identifizieren und in einem Funktionskatalog zusammenzufassen.

Unabhängig von den funktionalen Sicherheitsanforderungen bestehen, wie in der Einleitung zu diesem Hauptkapitel bereits angedeutet, auch **betriebliche funktionale Anforderungen** an die Sicherungslogik, die damit ebenfalls den Funktionsumfang der Logik beeinflussen[22]. Diese betrieblichen funktionalen Anforderungen ergeben sich nicht aus den Gefährdungen, sondern aus den gewünschten Funktionen, welche die Komponente Sicherungslogik der infrastrukturseitigen Sicherungstechnik angesichts ihrer Aufgabe im System zur Durchführung des Eisenbahnbetriebs

[22] Würde es nur funktionale Sicherheitsanforderungen geben, wäre die einfachste Lösung diese umzusetzen, gar nicht zu fahren.

erfüllen soll (vgl. hierzu die globalen Ziele aus Kapitel 3.1). „Gewünschten“ drückt dabei aus, dass die betrieblichen Anforderungen anders als die funktionalen Sicherheitsanforderungen beeinflussbar und im Umfang veränderbar sind. Sie bilden die Basis, um zu ermitteln, welche Anfragen zur Prüfung vom TMS an die Sicherungslogik gestellt werden können sollen und damit welche Prozesse es innerhalb der smartLogic geben muss, um diese Anfragen zu bearbeiten.[23]

Ziel dieses Kapitels sind daher die Bestimmung der betrieblichen funktionalen Anforderungen bzw. betrieblichen Funktionen (Kapitel 6.3) sowie die Identifikation und Beschreibung der funktionalen Sicherheitsanforderungen bzw. Schutzfunktionen (Kapitel 6.4) an die Logik. Diese beiden Gruppen bilden zusammen den Funktionskatalog möglicher Funktionen der Sicherungslogik. Das Kapitel bearbeitet damit Teile von Phase IV des Lebenszyklusprozesses aus [DIN EN 50126-1:2017] (vgl. Kapitel 3.6.4). Abb. 41 fasst den Unterschied zwischen den beiden Arten von funktionalen Anforderungen bzw. Funktionen zusammen.

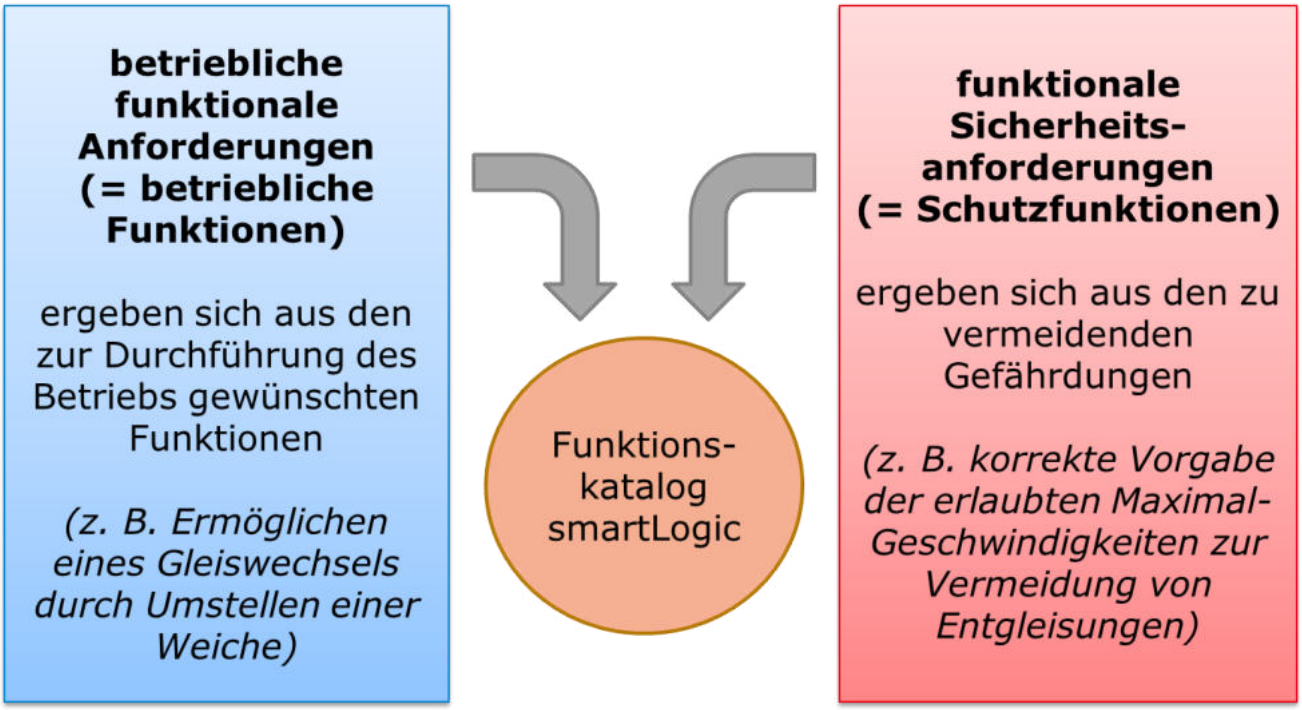


Abb. 41: Unterscheidung der funktionalen Anforderungen in betriebliche funktionale Anforderungen und funktionale Sicherheitsanforderungen
[Eigene Darstellung]

Der identifizierte Funktionskatalog bildet die Basis für die anschließende Logikentwicklung und bildet gemäß der Gesamt-Vorgehensweise, die in Kapitel 3.6.6 zusammengefasst wurde, den angestrebten Funktionsumfang der smartLogic ab. Da die Vollständigkeit des Funktionskatalog besonders wichtig ist, soll er den Überlegungen in Kapitel 3.6.2 folgend aus der Literatur ergänzt werden (Kapitel 6.5).

Gemäß den Abgrenzungen aus Kapitel 3.3 können allerdings aus Ressourcengründen nur die wichtigsten Basis-Funktionen in dieser Arbeit umgesetzt werden. Der im Rahmen der Arbeit näher ausgearbeitete **Funktionsumfang** enthält also nur einen Teil der Funktionen aus dem Funktionskatalog. Aus diesem Grund ist eine begründete Priorisierung vorzunehmen (Kapitel 6.6).

[23] Prozesse, die auf Änderungen der Umweltsituation reagieren, ergeben sich dagegen in der Regel aus den funktionalen Sicherheitsanforderungen.

Abschließend werden die Ergebnisse in Kapitel 6.7 und vor dem Hintergrund der Zielerreichung in Kapitel 6.8 diskutiert. In Kapitel 6.9 folgt ein Vergleich mit alternativen Zusammenstellungen funktionaler Anforderungen an Stellwerks- bzw. Sicherungslogiken (vgl. zum Vorgehen Kapitel 1.3). Kapitel 6.10 fasst das Hauptkapitel zusammen.

6.2 Methode und Vorgehensweise

In diesem Kapitel werden aufbauend auf der Zielsetzung des Hauptkapitels, die in Kapitel 6.1 beschrieben wurde, Methode und Vorgehensweise für die Durchführung der Funktionsanalyse diskutiert und festgelegt. Das Kapitel folgt dem üblichen wissenschaftlichen Aufbau, wonach zunächst aus den globalen Anforderungen aus Kapitel 3.5 spezifische Anforderungen an die Funktionsanalyse hergeleitet werden (Kapitel 6.2.1). Auf deren Grundlage werden anschließend Methode und Vorgehensweise erarbeitet (Kapitel 6.2.2). Kapitel 6.2.3 fasst die gewählte Methode und Vorgehensweise zusammen.

6.2.1 spezifische Anforderungen an die Funktionsanalyse

Zunächst sind die für die Funktionsanalyse spezifischen Anforderungen zu bestimmen. Sie dienen als Kriterien für die Auswahl einer geeigneten Methode und Vorgehensweise und leiten sich aus den globalen Anforderungen an die neu zu schaffende Sicherungslogik her (vgl. Kapitel 3.5). Dazu wird für jede globale Anforderung überlegt, welchen Einfluss die Ergebnisse des Kapitels in Hinblick auf die Erfüllung der jeweiligen globalen Anforderung haben. Zusätzlich wurde zur Vervollständigung der spezifischen Anforderungen ein Brainstorming mit Fachkollegen durchgeführt.

Tab. 19 enthält eine Übersicht der globalen Anforderungen und der daraus folgenden spezifischen Anforderungen an die Funktionsanalyse, die anschließend unterhalb der Tabelle näher erläutert werden. Bei nicht relevanten globalen Anforderungen ist dieser Umstand in kursiv vermerkt.

Tab. 19: spezifische Anforderungen an die Funktionsanalyse

Zieldimension	globale Anforderung	spezifische Anforderungen
Kernanforderung sichere Logik		alle Schutzfunktionen werden abgedeckt
geringer Planungs- und Genehmigungsaufwand	schlanke Logik	möglichst wenige nicht sicherheitsrelevante Funktionen werden abgedeckt
	Beschränkung auf sicherungskritischen Kern	Funktionsbestandteile mit nicht sicherheitskritischen Anteilen werden abgetrennt
	generische Logik	Funktionen werden möglichst generisch formuliert
	Topologieunabhängigkeit	
	flexible Infrastrukturzuordnung	Funktionen zur Neu-Zuordnung von Infrastrukturelementen werden vorgesehen
Interoperabilität	Standardschnittstellen	Anforderungen der Standard-Schnittstellen werden erfüllt
geringer Hardwareeinsatz	nur erforderliche Infrastrukturelemente	Funktionen vermeiden zusätzlichen Bedarf an Infrastrukturelementen
geringer Arbeitskräfteeinsatz	hohe Automatisierung	Funktionen vermeiden Benutzerinteraktion

	flexible Kontrollbereiche	Funktionen zur Neu-Zuordnung von Kontrollbereichen werden vorgesehen
Energieeffizienz	keine unnötigen Bremsvorgänge	Funktionen werden so formuliert, dass das Fahrzeug so wenig wie möglich eingeschränkt wird (möglichst flexiblen Bahnbetrieb ermöglichen)
	Freiraum für Fahrzeug	
hohe Kapazität	Ermöglichung maximaler Geschwindigkeit	
	geringe Latenz	*keine Relevanz für die Funktionsanalyse festgestellt*
	minimale Infrastrukturbeanspruchung	Funktionen werden so formuliert, dass das Fahrzeug so wenig wie möglich eingeschränkt wird (möglichst flexiblen Bahnbetrieb ermöglichen)
	frühestmögliche Infrastrukturfreigabe	
hohe Robustheit	Rückfallebenenintegration	Funktionen werden so formuliert, dass sie mit möglichst vielen möglichen Betriebssituationen kompatibel sind und auch Rückfallebenen umfassen (möglichst flexiblen Bahnbetrieb ermöglichen)
	Regelhandlungsgebot	
	Freiraum für Fahrzeuge	Funktionen werden so wenig restriktiv wie möglich formuliert (möglichst flexiblen Bahnbetrieb ermöglichen)
	Resilienz	unabhängige Sicherheitsanforderungen führen zu unabhängigen Funktionen
	modulare Außerbetriebnahme	
lange Nutzungszeiten	Migrationsfähigkeit	der Umfang der zu unterstützenden Alttechnik wird festgelegt
	Zukunftsfähigkeit	funktionale Anforderungen möglicher zukünftiger Technologien bei den Umsystemen werden berücksichtigt
[ohne]	Protokollierung	eine Protokollierung aller Ereignisse wird vorgesehen

Die *Kernanforderung* der sicheren Logik erfordert die Vollständigkeit des Funktionsumfangs in Bezug auf die Schutzfunktionen. Demgegenüber steht die Anforderung der *schlanken Logik*, die allerdings im Vergleich zur Kernanforderung niedriger zu gewichten ist (vgl. Kapitel 3.5). Die zu wählende Methode soll also sicherstellen, dass alle relevanten Schutzfunktionen durch die Logik abgedeckt sind, die Logik unter Einhaltung dieser Bedingung aber möglichst schlank bleibt. Hierzu sollen beispielsweise möglichst wenige nicht sicherheitsrelevante Funktionen in den Funktionskatalog aufgenommen werden. Zudem sollen im Sinne der globalen Anforderung der *Beschränkung auf [den] sicherheitskritischen Kern* die betrieblichen Funktionen so formuliert werden, dass Funktionsbestandteile mit nicht sicherheitskritischen Anteilen nicht Teil des Funktionskatalogs der smartLogic sind.

Für die Wahl der geeigneten Formulierung der Funktionen ergeben sich aus den in der obigen Tabelle identifizierten Anforderungen weitere Vorgaben. Die Funktionen sollen generisch (z. B. unabhängig von der konkreten Art des Infrastrukturelements) und unabhängig von der im Zuständigkeitsbereich der smartLogic existierenden Gleistopologie sowie den sonstigen existierenden Infrastrukturelementen

und externe Systemen formuliert werden (globale Anforderungen der *generischen Logik* und *Topologieunabhängigkeit*). Weiterhin sollen sie so formuliert werden, dass möglichst keine Benutzerinteraktion vorgesehen ist (globale Anforderung der *hohen Automatisierung*). Letzteres ist allerdings vor allem auch eine Frage der Umsetzung, die in Kapitel 8 thematisiert wird.

Es erscheint plausibel, dass nicht bei jeder Prüfung einer beantragten Statusänderung durch die Sicherungslogik alle Sicherheitsanforderungen eine Rolle spielen. Falls verschiedene Sicherheitsanforderungen im Rahmen der Prüfung in einem gemeinsamen Schritt der Prüfung, im Folgenden auch als **Prüfbedingung** bezeichnet (siehe zur ausführlicheren Herleitung des Begriffs auch Kapitel 6.2.2), zusammengefasst werden würden, um den Prozess zu vereinfachen (z. B. verschiedene Sicherheitsanforderungen, die sich auf die Geschwindigkeit beziehen), bestünde daher die Gefahr, dass die Verletzung einer Prüfbedingung dazu führen könnte, dass das Ergebnis der gesamten Prüfung negativ ist, obwohl die dahinterstehende nicht erfüllte Sicherheitsanforderung für diese Prüfung gar nicht relevant ist. Dieser Umstand würde u. a. die globalen Anforderungen der *Resilienz* und der *modularen Außerbetriebnahme* verletzen. Das Problem kann umgangen werden, wenn darauf geachtet wird, dass verschiedene Sicherheitsanforderungen zu unabhängigen Prüfbedingungen führen.

Verschiedene globale Anforderungen zu den Zieldimensionen „Energieeffizienz“, „hohe Kapazität“ und „hohe Robustheit“ beziehen sich auf den Umfang möglicher durch Sicherheitsanforderungen verursachter Einschränkungen und Vorgaben für Fahrzeugbewegungen (vgl. Anforderungen zum Stichwort „*möglichst flexiblen Bahnbetrieb ermöglichen*“). Um betrieblich die Infrastruktur bestmöglich nutzen zu können, ist entscheidend, dass durch die Formulierung der Schutzfunktionen die Fahrzeugbewegungen nur so wenig eingeschränkt werden wie möglich oder anders formuliert, nur so eingeschränkt werden, wie es nötig ist. Dem Traffic Management Systems (TMS) soll also ermöglicht werden, möglichst individuell auf die aktuelle Betriebssituation zugeschnittene Anfragen zu stellen.

Im Sinne der Anforderungen zur *Zieldimension der Robustheit* sollen möglichst viele Betriebssituationen durch die smartLogic abgedeckt werden, um eine *Rückfallebenenintegration* zu erreichen und das *Regelhandlungsgebot* bestmöglich umzusetzen. Es sollten z. B. Änderungen bereits erteilter Aufträge solange wie möglich durchführbar sein (oder die feste Auftragsverteilung spätestmöglich erfolgen). Weiterhin sollten Rückfallebenen berücksichtigt werden, also Situationen, in denen die Infrastruktur nicht vollständig zur Verfügung steht oder keine vollständige Informationslage über den Zustand der Infrastruktur und/oder der Fahrzeuge vorliegt. Die Berücksichtigung solcher Situationen verkompliziert die Logik zwar auf der einen Seite und widerspricht damit der Anforderung der schlanken Logik. Auf der anderen Seite erhöht sie aber auch die Nutzbarkeit der Logik in diesen Fällen, so dass keine manuellen Rückfallebenen erforderlich sind und die Kapazität durch die Rückfallebenenintegration nicht unnötig eingeschränkt wird. Da der Effekt durch die Rückfallebenenintegration auf die Zieldimensionen der Kapazität und der Robustheit als groß eingeschätzt wird, wird die erhöhte Nutzbarkeit der Logik in diesem Fall höher gewichtet als die Anforderung der schlanken Logik.

Einige globale Anforderungen geben auch Inhalte für den Funktionskatalog der Sicherungslogik vor. Demnach müssen funktionale Anforderungen von verwendeten *Standardschnittstellen* an die smartLogic erfüllt sein, sofern diese Anforderungen nicht über ein zwischenliegendes System (z. B. der Ortungsinformationsaggregator (vgl. Kapitel 4.4.4)) erfüllt werden. Ferner müssen Funktionen vorhanden sein, mit denen einzelne Infrastrukturelemente unterschiedlichen Kontrollbereichen bzw. Zuständigkeitsbereichen der smartLogic zugewiesen werden können, um einen flexiblen Personaleinsatz zu ermöglichen (*flexible Infrastrukturzuordnung* und *flexible Kontrollbereiche)*.

Schließlich soll der Funktionskatalog der smartLogic auch eine Migration der neuen Technik in einer Welt bestehender Technik ermöglichen (*Migrationsfähigkeit*) sowie bereits für mögliche zukünftige funktionale Anforderungen vorbereitet sein (*Zukunftsfähigkeit*). Die zu wählende Methode für die Funktionsanalyse muss also sicherstellen, dass möglichst wenige Anforderungen an die Technik der Umsysteme durch die Formulierung der funktionalen Anforderungen definiert werden. Gleichsam sollen auch keine nicht mehr erforderlichen Einschränkungen der Sicherungslogik durch Beschränkungen der Alttechnik übernommen werden. Dabei können Abwägungen zwischen den globalen Anforderungen der Migationsfähigkeit und Zukunftsfähigkeit sowie der globalen Anforderung der schlanken Logik nötig werden. In einem Konflikt sollte gemäß der Diskussion zum „Grüne Wiese"-Ansatz (vgl. Kapitel 3.6.2) im Zweifelsfall die Anforderung der schlanken Logik höher bewertet werden.

Die globale Anforderung nach einer *geringen Latenz* wird durch die Gestaltung der Systemarchitektur (vgl. Hauptkapitel 4) sowie die Abfolge und Ausgestaltung der Prozessschritte (vgl. Hauptkapitel 8) beeinflusst. Auf die Formulierung der Funktionen hat die Latenz-Anforderung jedoch keinen Einfluss, deshalb wird sie für dieses Hauptkapitel als nicht relevant eingestuft.

Aufteilung der spezifischen Anforderungen in Gruppen

Da im Falle der Funktionsanalyse aus den globalen Anforderungen eine große Anzahl von spezifischen Anforderungen hergeleitet wurden, erscheint es sinnvoll zu untersuchen, ob sie sich neben der Gliederung nach den zugrundliegenden Zieldimensionen in weitere Gruppen gliedern lassen.

Es fällt auf, dass sich einige spezifische Anforderungen rein auf den Umfang des Funktionskatalogs beziehen. Diese Anforderungen können von den spezifischen Anforderungen unterschieden werden, die sich auf die Formulierung der Funktionen beziehen. Die beiden spezifischen Anforderungen „*Funktionen vermeiden zusätzlichen Bedarf an Infrastrukturelementen*" und „*Funktionen vermeiden Benutzerinteraktion*" können keiner dieser beiden Gruppen eindeutig zugeordnet werden. Sie beziehen sich auf die inhaltliche Ausgestaltung der Funktionen und können damit sowohl den Umfang der Funktionen, als auch deren Formulierung berühren. Tab. 20 enthält eine Übersicht der oben beschriebenen spezifischen Anforderungen und ihre Zuordnung zu den drei genannten Gruppen.

Tab. 20: Aufteilung der spezifischen Anforderungen in Bezug auf Umfang und Formulierung der Funktionen

alle Schutzfunktionen werden abgedeckt	Umfang
möglichst wenige nicht sicherheitsrelevante Funktionen werden abgedeckt	
Anforderungen der Standard-Schnittstellen werden erfüllt	
Funktionen zur Neu-Zuordnung von Infrastrukturelementen werden vorgesehen	
Funktionen zur Neu-Zuordnung von Kontrollbereichen werden vorgesehen	
der Umfang der zu unterstützenden Alttechnik wird festgelegt	
funktionale Anforderungen möglicher zukünftiger Technologien bei den Umsystemen werden berücksichtigt	
eine Protokollierung aller Ereignisse wird vorgesehen	
Funktionsbestandteile mit nicht sicherheitsrelevanten Bestandteilen werden abgetrennt	Formulierung
Funktionen werden möglichst generisch beschrieben	
Funktionen werden so wenig restriktiv wie möglich formuliert	

unabhängige Sicherheitsanforderungen führen zu unabhängigen Funktionen	
Funktionen vermeiden zusätzlichen Bedarf an Infrastrukturelementen	Umfang und Formulierung
Funktionen vermeiden Benutzerinteraktion	
Funktionen werden so formuliert, dass sie mit möglichst vielen möglichen Betriebssituationen kompatibel sind und auch Rückfallebenen umfassen	

Weitere sinnvolle Gliederungen wurden an dieser Stelle nicht identifiziert.

6.2.2 Erarbeitung der Methode und Vorgehensweise

In diesem Unterkapitel soll auf Basis der in Kapitel 6.2.1 identifizierten spezifischen Anforderungen eine geeignete Methode und Vorgehensweise für die Funktionsanalyse erarbeitet werden. Für eine systematische Identifikation der Funktionen kann es hilfreich sein zu untersuchen, in welche Arten sich die Funktionen unterscheiden lassen, um für jede Art von Funktion eine systematische Bestimmung möglicher Funktionen für den Funktionskatalog der smartLogic durchführen zu können (erster Abschnitt). Für diese systematische Bestimmung werden für die verschiedenen Funktionsarten wiederum Methoden benötigt, die in den nachfolgenden Abschnitten hergeleitet werden (betriebliche Funktionen im zweiten Abschnitt und Schutzfunktionen im dritten Abschnitt). Wie bereits in Kapitel 6.1 erwähnt, ist die Vollständigkeit des Funktionskatalogs wichtig, weswegen anschließend an die systematische Bestimmung der Funktionen noch weitere Schritte zur Erhöhung der Vollständigkeit festgelegt werden sollen (vierter Abschnitt). Abschließend wird eine Methoden zur Kategorisierung und Priorisierung der bestimmten Funktionen festgelegt, um den Funktionskatalog auf einen im Rahmen der Arbeit umsetzbaren Funktionsumfang für die smartLogic einzugrenzen (sechster Abschnitt, vgl. ebenfalls Kapitel 6.1).

Unterscheidung verschiedener Arten von Funktionen

Funktionen des Funktionskatalogs wurden bereits in Kapitel 6.1 anhand ihrer Herleitung in betriebliche Funktionen und Schutzfunktionen unterschieden. Da eine große Anzahl von Funktionen zu erwarten ist, erscheint es sinnvoll, zu untersuchen, ob es weitere nützliche Unterscheidung der Funktionen in verschiedene Funktionsarten gibt. Nützlich kann eine Unterscheidung zum Beispiel dann sein, wenn sie für die Identifizierung der Funktionen hilfreich ist oder die präzise und stringente Formulierung der hinter der jeweiligen Funktionen stehenden funktionalen Anforderung durch das Aufstellen eines klaren Formulierungsschemas für verschiedene Arten von Funktionen ermöglicht. Mögliche Unterscheidungen der Funktionen nach Funktionsarten sollen daher in diesem Abschnitt untersucht werden. Eine zusammenfassende Grafik zu den Begriffen findet sich im letzten Unterabschnitt dieses Abschnitts (Abb. 42).

Abgrenzung von Prozessfunktionen und Subroutinen

Gemäß [Balzert & Liggesmeyer 2011, S. 109] spezifizieren funktionale Anforderungen, „welche Funktionalität oder welches Verhalten das Softwareprodukt unter festgelegten Bedingungen besitzen bzw. erfüllen soll.“ Es wird also zwischen funktionalen Anforderungen unterschieden, die eine Funktionalität bedingen und funktionalen Anforderungen, die sich auf das Verhalten bei der Ausführung von Funktionalitäten beziehen.

Bezogen auf die Unterscheidung von betrieblich funktionalen Anforderungen (betriebliche Funktionen) und funktionalen Sicherheitsanforderungen (Schutzfunktionen) kann angenommen werden, dass sich Erstere eher auf Funktionalitäten beziehen, wie beispielsweise „Die Sicherungslogik

soll das Umstellen von Stellelementen wie Weichen ermöglichen.“ oder „Die Sicherungslogik soll das Übermitteln von Fahrerlaubnissen an Züge ermöglichen.“.

Funktionalitäten können dabei von der smartLogic über Prozesse bereitgestellt werden. Ein **Prozess** wird je nach Anwendungsbereich unterschiedlich definiert. Bezogen auf eine Software wie die smartLogic wird im Rahmen eines Prozesses in Folge eines Auslösers (Prozessaufruf, z. B. durch Eingang einer Prüfanfrage vom TMS, vgl. Kapitel 4.3.1) eine Reihe von **Prozessschritten** durchgeführt, die in einem Ergebnis münden (vgl. z. B. verschiedene Prozessdefinitionen bei [Kaffenberger 2013]).

Prinzipiell wäre es denkbar, alle zur Bereitstellung der geforderten Funktionalitäten erforderlichen Prozesse als voneinander unabhängig zu betrachten. Es würde dann jeder Prozessschritt bis ins Detail für den jeweiligen Prozess definiert werden müssen. Es ist allerdings anzunehmen, dass einige Bestandteile der Prozesse, wie beispielsweise die Überprüfung der Syntax der auslösenden Prüfanfrage oder die Identifizierung beteiligter Infrastrukturelemente, bei mehreren Prozessen erforderlich sein werden. Aufgrund der Anforderung der *schlanken Logik* ist demnach ein möglichst modularer Aufbau der Prozesse wünschenswert. Dies kann erreicht werden, indem wiederkehrende Bestandteile von Prozessen in Unterprogramme ausgegliedert werden. Diese Unterprogramme werden im Weiteren in Abgrenzung zu den übergeordneten **Prozessfunktionen** (process functions, im Weiteren auch kurz als „Prozesse“ bezeichnet) als **Subroutinen** bezeichnet. Prozessfunktionen sind alle Funktionen, die direkt von außen aufgerufen werden. Subroutinen werden dagegen intern von den Prozessfunktionen oder von anderen Subroutinen aufgerufen und melden ihr Ergebnis wieder zurück an die aufrufende Funktion.[24]

Durch dieses Vorgehen ist insbesondere bei häufigen Verwendungen einiger Subroutinen eine deutlich schlankere Logik zu erwarten. Zudem wird ein Redundanzproblem vermieden. Eine Ausgliederung von Aufgaben in Subroutinen kann auch zur Vereinfachung der Prozessfunktionen dienen, selbst wenn die Subroutine von keiner weiteren Prozessfunktion mehr benötigt wird, da sie die Darstellung des Prozessablaufs vereinfachen kann. Diese Vorteile wiegen den Nachteil einer leicht komplexeren Struktur mit verschiedenen Funktionsarten aus Sicht des Autors deutlich auf.

Abgrenzung von Prüfbedingungen

Im Gegensatz zu den betrieblich funktionalen Anforderungen, die sich auf Funktionalitäten beziehen, beziehen sich die funktionalen Sicherheitsanforderungen (Schutzfunktionen) der Logik nicht nur auf Funktionalitäten (z. B. „Die Sicherungslogik muss bei Detektion eines Heißläufers den betroffenen Zug anhalten.“), sondern auch auf das Verhalten bei der Ausführung von Funktionalitäten, wie z. B. „Es muss sichergestellt werden, dass eine Weiche nur umgestellt werden darf, wenn sie nicht von einem Zug besetzt ist.“ Dabei werden Bedingungen formuliert, die für ein positives Ergebnis einer Prozessfunktion zu beachten und damit im Laufe des Prozesses zu prüfen sind. Diese Bedingungen werden im Folgenden als **Prüfbedingungen** bezeichnet (vgl. auch Kapitel 6.2.1).

Es stellt sich die Frage, wie Prüfbedingungen in die Prozesse eingebunden werden:

1. Die Prüfbedingungen könnten unmittelbar als Prozessschritt in die Prozesse eingebunden werden („Prüfe Prüfbedingung xy“).

[24] Diese Aufteilung ist auch in der Informatik verbreitet. Es gibt verschiedene Möglichkeiten, wie dies bei der Implementierung softwaretechnisch umgesetzt werden kann. Die vorliegende Arbeit beschäftigt sich jedoch nicht mit so tiefgehenden Fragen der Implementierung. Deshalb wird an dieser Stelle nicht näher auf mögliche softwaretechnische Umsetzungen eingegangen.

2. Die Prüfbedingungen könnten innerhalb eines Prozesses durch eine Subroutine abgeprüft werden.
3. Prüfbedingungen bilden eine neutrale dritte Art von Funktionen und könnten in den Prüfprozessen je nach Anwendungsfall entweder direkt als Prozessschritt oder als Subroutine eingebunden werden.

Gegen eine direkte Integration in die Prozesse als Prozessschritt (erster Ansatz) spricht, dass es Prüfbedingungen gibt, die in mehreren Prozessen abgeprüft werden müssen. Hier greift die gleiche Argumentation wie bei der Begründung der Subroutinen, denn es kann nicht davon ausgegangen werden, dass eine Prüfbedingung mit einem einzelnen Prozessschritt wie einer Statusabfrage erfüllt wird. Beispielsweise ist zur Sicherstellung des seitlichen Kollisionsschutzes (Flankenschutz) ein umfangreicherer Algorithmus zu erwarten.

Gegen die Formulierung von Prüfbedingungen in Form einer Subroutine (zweiter Ansatz) spricht allerdings, dass nicht pauschal davon ausgegangen werden kann, dass eine Prüfbedingung bei jedem Prozess in gleicher Weise prozessual abgeprüft wird. Beispielsweise muss in Hinblick auf die Flankenschutz-Prüfbedingung bei der Prüfung einer Fahrerlaubnisanfrage des TMS eine Risikobetrachtung erfolgen, mit welcher Wahrscheinlichkeit die Fahrzeugbewegung, für die die beantragte Fahrerlaubnis gelten soll, durch eine Flankenfahrt gefährdet wird. Dagegen impliziert die Prüfbedingung bei der Reaktion auf ein Problem im Tunnel, bei dem die ETCS-Funktion „Reversing“ genutzt werden soll, dass ggf. mehrere Fahrzeuge identifiziert und beeinflusst werden müssen, um den Flankenschutz für die Fahrzeugbewegung im Modus „Reversing“ zu gewährleisten.

Aus diesen Gründen wird der dritte Ansatz bevorzugt, bei dem die Prüfbedingungen je nach Anwendungsfall in den Prüfprozessen abgeprüft werden. Daher werden die Prüfbedingungen neben den Prüfprozessen und den Subroutinen als eigene Art in den Funktionskatalog aufgenommen. Es handelt sich (wie auch der Name sagt) als im Rahmen von Prozessfunktionen oder Subroutinen zu überprüfende Bedingungen. Eine Prozessfunktion muss dabei jeweils alle für sie relevanten Prüfbedingungen abdecken. Die Abdeckung kann entweder durch entsprechende prozessspezifische Prozessschritte oder durch eine in den Prozess eingebundene Subroutine erfolgen. (Wie dies sichergestellt wird, wird in Kapitel 8.2 erörtert.)

Funktionstypen gemäß der Anforderungsanalyse

Wie bereits in Kapitel 3.3 abgegrenzt wurde, wird die smartLogic als Softwaresystem betrachtet. Als weitere mögliche Unterscheidung von funktionalen Anforderungen bietet es sich daher an, auf die bewährte Methode der Anforderungsanalyse (engl. „Requirements Analysis“ als Teil des „Requirements Engineering“) aus der Softwareentwicklung zurückzugreifen. Die Anforderungsanalyse unterscheidet bezogen auf die Funktionalitäten drei verschiedene Typen von funktionalen Anforderungen, die in Tab. 21 aufgeführt sind (vgl. zur Anforderungsanalyse Kapitel 2.2 in [Kleuker 2013]).

Tab. 21: Funktionale Anforderungstypen nach [Kleuker 2013, S. 27]

Typ	Bezeichnung	Beschreibung
Typ 1	Selbständige Systemaktivität	das System führt den Prozess selbständig durch
Typ 2	Benutzerinteraktion	das System stellt dem Nutzer die Prozessfunktionalität zur Verfügung
Typ 3	Schnittstellenanforderung	das System führt einen Prozess in Abhängigkeit von einem Dritten (zum Beispiel einem Fremdsystem) aus, ist an sich passiv und wartet auf ein externes Ereignis

„Anforderungen vom Typ 1 beschreiben die zentrale Funktionalität [des Systems], die typischerweise von Anforderungen des Typs 2 oder 3 angestoßen werden.“ [Kleuker 2013, S. 28]. Mit Hilfe der Anforderungstypen 2 und 3 können benötigte Prozesse aus den Anforderungen der Schnittstellen zu den Umsystemen und aus den gewünschten Benutzerinteraktionen hergeleitet werden.

Gemäß den globalen Anforderungen an die Arbeit (vgl. Kapitel 3.5 und 6.2.1) sollen Benutzerinteraktionen (**Bedienfunktionen**) möglichst vermieden werden, da die Logik möglichst automatisiert arbeiten sollte. Sie sollten daher nur vorgesehen werden, wenn sie in Folge einer anderen funktionalen Anforderung zwingend benötigt werden. Kapitel 6.5.2 beschäftigt sich eingehender mit Bedienfunktionen.

Schnittstellenanforderungen sind insoweit zu berücksichtigen, als sie auf Standardschnittstellen zurückgehen (vgl. globale Anforderung der Verwendung von Standardschnittstellen). In anderen Fällen sollte gemäß der globalen Anforderung *Freiraum für Fahrzeuge* (vgl. Kapitel 3.5 und 6.2.1) die Sicherungslogik möglichst wenig durch Anforderungen bestehender Schnittstellen beeinflusst werden, damit nicht erforderliche Einschränkung der Nutzung der Infrastruktur in Folge der Schnittstellen vermieden wird.

Aus der Aufteilung nach funktionalen Anforderungstypen kann also gefolgert werden, dass die Standardschnittstellen als Quelle für mögliche Funktionen dienen können. Viele weitere Funktionen würden dem Typ 1 zugeordnet werden, während Bedienfunktionen keine wesentliche Rolle spielen.

inhaltliche Aufteilung der Prozessfunktionen in Prüf- und Reaktionsprozesse

Eine weitere Möglichkeit der Aufteilung ist eine Aufteilung nach inhaltlichen Aufgabenbereichen der smartLogic. In Kapitel 3.2 wurden als Aufgabe der smartLogic definiert, dass sie dafür zuständig ist, „die Sicherheit von Zustandsänderungen wie Fahrerlaubnisse und geplante Statusänderungen von Infrastrukturelementen sicherzustellen sowie auf ungeplante Ereignisse mit Sicherheitsreaktionen zu reagieren“. Demnach soll die smartLogic zum einen geplante Statusänderungen überprüfen. Ein solcher Prozess kann folglich als „**Prüfprozess**“ bezeichnet werden. Zum anderen soll sie auf ungeplante Ereignisse reagieren. Entsprechend kann ein solcher Prozess als „**Reaktionsprozess**“ bezeichnet werden.

In beiden Fällen handelt es sich um Prozesse, die über Schnittstellen von außen ausgelöst werden, jedoch sind diese Auslöser unterschiedliche Schnittstellen. Bei Prüfprozessen ist gemäß den Ergebnissen aus Kapitel 4.3.1 das Traffic Management System (TMS) der Auslöser, welches die Prüfung eines gewünschten betrieblichen Verhaltens mittels einer entsprechenden Nachricht beauftragt. Bei Reaktionsprozessen wird das Ereignis (z. B. eine unerwartete Zustandsänderung einer Weiche oder ein Sensormessergebnis wie beispielsweise von einer Heißläuferortungsanlage) durch ein beliebiges Umsystem über eine entsprechende Schnittstelle gemeldet und löst den Prozess aus.

Prüfprozesse können ein positives oder ein negatives Ergebnis haben, die zugrundeliegende Anfrage also genehmigen oder zurückweisen, falls ein unsicherer Zustand droht. Bevor das Ergebnis nicht vorliegt, verlässt das System nicht seinen aktuellen Zustand. Funktioniert der Prüfprozess korrekt, kann das System daher durch die beantragte Zustandsänderung mit hinreichender Sicherheit nicht in einen unsicheren Zustand geraten.

Reaktionsprozesse können dagegen nicht erst ergebnisoffen prüfen, ob die Zustandsänderung zu einem unsicheren Zustand führt, da dieser bereits unmittelbar droht oder sogar bereits eingetreten ist. Es kann also nicht der Eintritt der Zustandsänderung durch die Prüfung verhindert werden, sondern es können nur die Auswirkungen, die durch die Zustandsänderung ausgelöst werden, beeinflusst werden. Das Ergebnis des Prozesses ist das Einleiten von Maßnahmen zur Schadensbegrenzung, falls diese erforderlich sind. Dabei muss beachtet werden, dass diese Maßnahmen keine negativen Auswirkungen auf die Sicherheit an anderer Stelle (z. B. auf andere Fahrzeugbewegungen) haben dürfen. Aufgrund des geschilderten Unterschiedes erscheint es sinnvoll, diese beiden Arten von Prozessen in Hinblick auf die Identifizierung und Formulierung der Funktionen zu unterscheiden.

Zusammenfassung

Die Funktionen bzw. funktionalen Anforderungen werden in Prozesse (Prozessfunktionen), Subroutinen und Prüfbedingungen unterteilt. Die Prozesse können wiederum in Prüfprozesse und Reaktionsprozesse unterschieden werden. Abb. 42 veranschaulicht die verschiedenen Funktionsarten und ihre Herleitung.

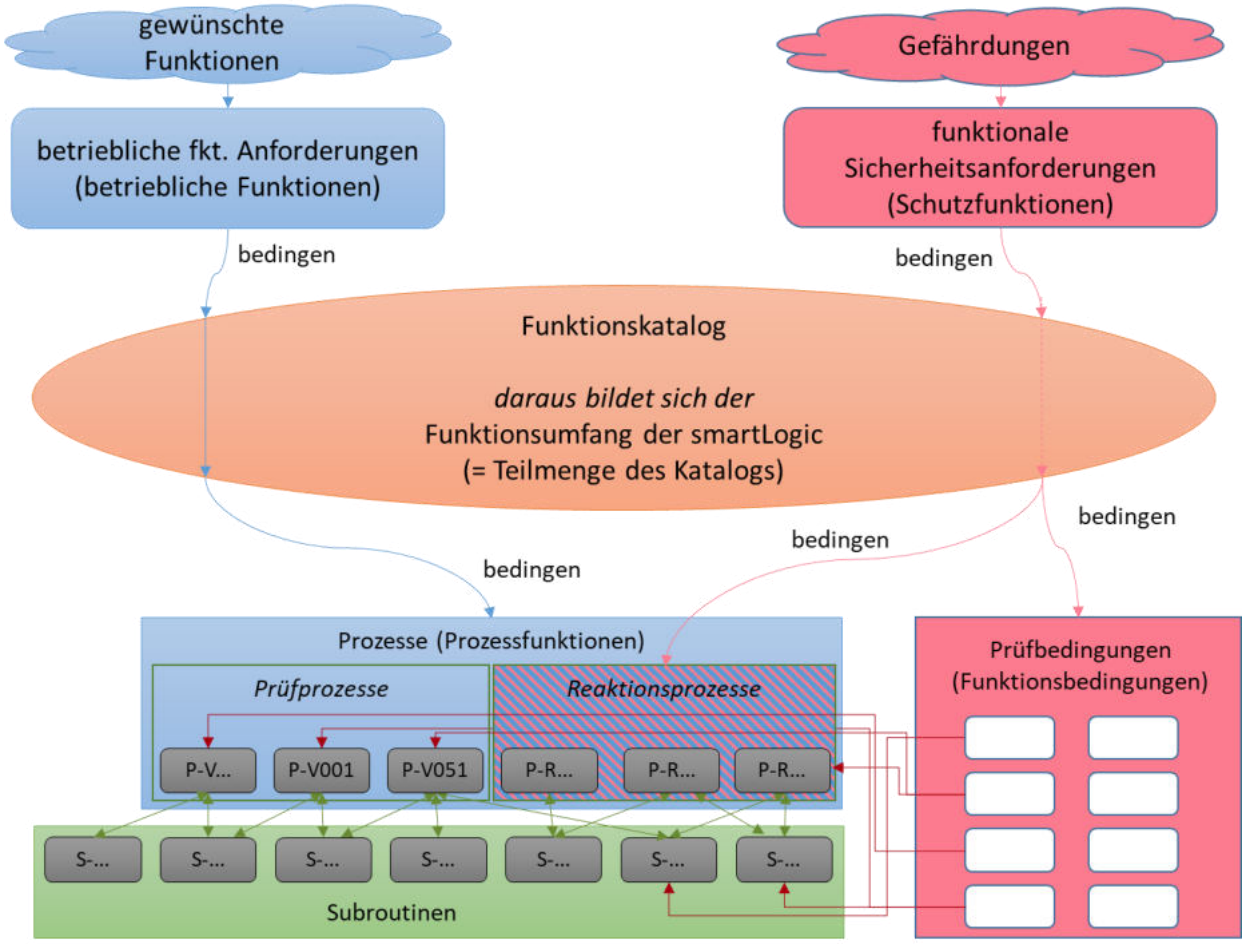


Abb. 42: Aufteilung der Funktionen der smartLogic in Funktionsarten und ihre Herleitung [Eigene Darstellung]

Eine Prozessfunktion der smartLogic prüft im Falle eines Prüfprozesses, ob alle für diesen Prozess relevanten Prüfbedingungen erfüllt sind. Im Falle eines Reaktionsprozesses leitet sie in Folge einer gemeldeten Zustandsänderung (Ereignis), sofern dies zur Aufrechterhaltung der Sicherheit erforderlich ist, notwendige Maßnahmen ein, um die Sicherheit zu gewährleisten bzw. ein mögliches Schadensausmaß zu verringern. Dabei sind wie bei den Prüfprozessen die Prüfbedingungen zu beachten. Die Prüfbedingungen reflektieren die auf das Verhalten des Prozesses bezogenen funktionalen Anforderungen, die zur Aufrechterhaltung der Sicherheit von allen Prozessen eingehalten werden müssen.

Prozessfunktionen leiten sich zum einen aus den betrieblichen Funktionen her. Sie können aber auch in Folge von Schutzfunktionen notwendig werden. Beispielsweise könnten Schutzfunktionen die Durchführung geeigneter Maßnahmen zur Vermeidung einer Schadensausmaßvergrößerung bei Eintritt eines unerwarteten Ereignisses, wie eines Erdrutsches, fordern, welches von einem externen System registriert wird. Die Verarbeitung der zugrundeliegenden **Ereignismeldung** würde dann in einem Reaktionsprozess erfolgen. Dieser Prozess müsste über die Beachtung der entsprechenden Prüfbedingungen sicherstellen, dass alle erforderlichen Maßnahmen getroffen werden.

Prozessfunktionen und Prüfbedingungen werden im Funktionskatalog grundsätzlich getrennt aufgeführt. Falls also Prüfbedingungen eine Prozessfunktion erforderlich machen, wird die Prozessfunktion zusätzlich in den Funktionskatalog aufgenommen.

Subroutinen können Teile des notwendigen Prozesses zur Erfüllung der Prozessfunktionen abdecken. Weiterhin beinhalten sie die Umsetzung von Prüfungen, die durch Prüfbedingungen gefordert werden, für einen bestimmten Anwendungsfall der Prüfbedingung. In beiden Fällen sind die zugrundeliegenden funktionalen Anforderungen der Subroutine bereits durch die Prozessfunktion bzw. die Prüfbedingung im Funktionskatalog enthalten. Daher tragen die Subroutinen nur in Ausnahmefällen zur Vollständigkeit des Funktionskatalogs bei. Stattdessen stellt sich bei den Prozessfunktionen die Frage, welche Prozessschritte in Subroutinen ausgegliedert werden sollten. Diese Frage kann allerdings am besten im Rahmen der Verhaltensmodellierung der Logik in Kapitel 8 beantwortet werden. Deshalb ist die Definition der Subroutinen nicht Teil der Funktionsanalyse.

Ausnahmen vom Fazit des vorigen Absatzes könnten für Funktionen sinnvoll sein, die durch die Analyse der anerkannten Regeln der Technik identifiziert wurden und keine eigene Prozessfunktion darstellen und auch nicht durch Prüfbedingungen abgedeckt werden. Sie werden zur Sicherung der Vollständigkeit als Subroutinen in einer eigenen Kategorie in den Funktionskatalog mitaufgenommen.

Abb. 43 illustriert, wie die verschiedenen Funktionsarten aufgerufen werden können. Die Prozessfunktionen können über ein Prozessschnittstellen-Gateway vom TMS, einem anderen externen System (Umsystem) oder in seltenen Fällen direkt von einem Bediener ausgelöst werden. Das TMS löst dabei in der Regel Prüfprozesse und externe Systeme Reaktionsprozess aus. Am Prozessschnittstellen-Gateway kann auch die erforderliche Protokollierung angeschlossen werden, die alle Aktivitäten auf Grund der juristischen Protokollierungs-Anforderung (vgl. Kapitel 3.5) aufzeichnet. Die Subroutinen werden dagegen von den Prozessen aufgerufen. Sowohl Prozesse als auch Subroutinen enthalten eine Liste von Prüfbedingungen aus dem Pool aller Prüfbedingungen, deren Einhaltung sie sicherstellen müssen. Die für die jeweilige Prozessfunktion bzw. die jeweilige Subroutine relevanten Prüfbedingungen werden im Rahmen der Verhaltensmodellierung im 8. Hauptkapitel identifiziert.

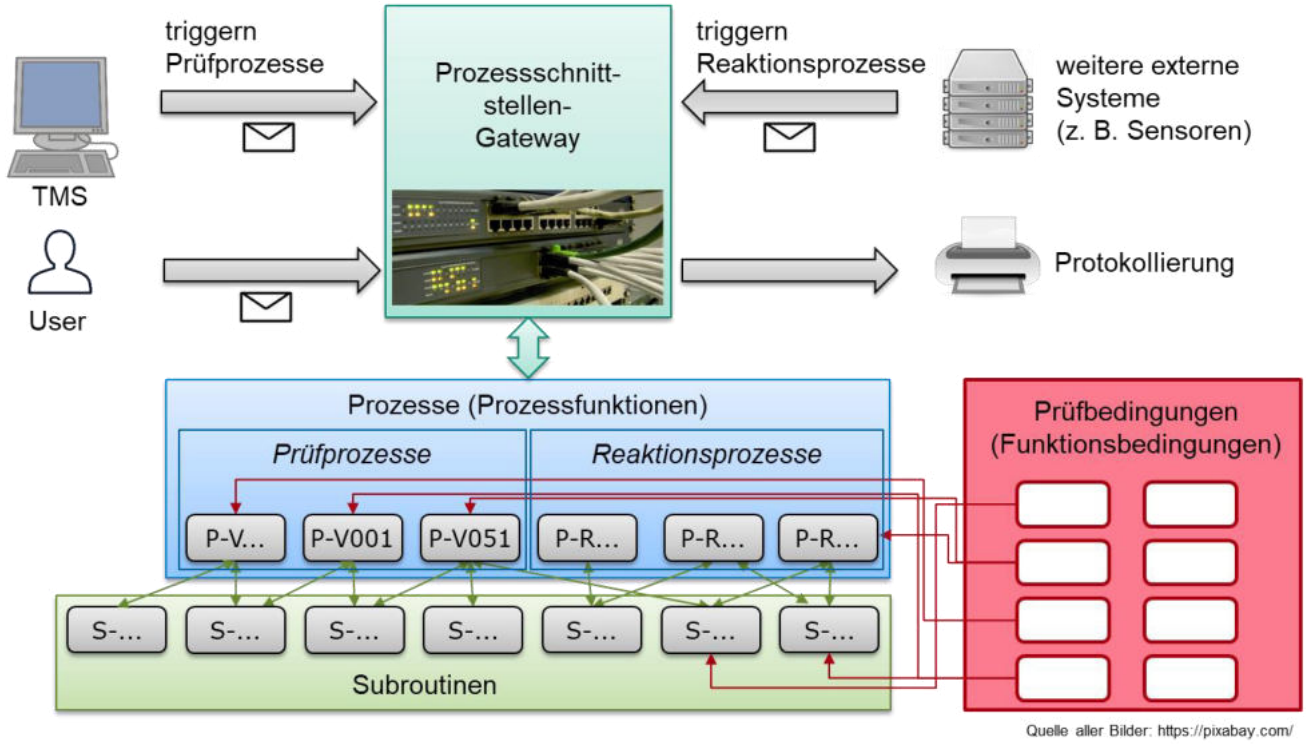


Abb. 43 Aufrufen der verschiedenen Funktionsarten
[Eigene Darstellung, Quelle der in der Abbildung verwendeten Grafiken: pixabay.com]

Bestimmung der betrieblichen Funktionen

Nach der Untersuchung möglicher Funktionsarten, können Methoden zur Identifikation der einzelnen Funktionen bestimmt werden. Der Funktionsumfang der Sicherungslogik setzt sich, wie bereits erwähnt, aus den gewünschten, betrieblichen Funktionen und den notwendigen Schutzfunktionen, um die Sicherheit zu gewährleisten, zusammen. Da zusätzliche betriebliche Funktionen neue Möglichkeiten für Gefährdungen erzeugen, ist der Umfang der notwendigen Schutzfunktionen vom Umfang der betrieblichen Funktionen abhängig. Es ist daher sinnvoll, bei der Bestimmung der erforderlichen Funktionen mit den betrieblichen Funktionen zu beginnen.

Die Menge der betrieblichen Funktionen soll aufgrund des Kriteriums der schlanken Logik klein gehalten werden, aber gleichzeitig auch die weiteren globalen Anforderungen erfüllen, von denen, wie in Kapitel 6.2.1 festgestellt, viele eher zu einer Vergrößerung des Funktionsumfangs führen, um einen möglichst flexiblen Bahnbetrieb zu ermöglichen. Um dennoch eine schlanke Logik zu erhalten, sollten zunächst alle nicht sicherheitskritischen Funktionalitäten aus der Sicherungslogik ausgegliedert werden und die verbleibenden Funktionen so generisch wie möglich definiert werden, ohne durch zu pauschale Festlegungen zu Betriebseinschränkungen zu führen (vgl. Beispiele in Kapitel 6.2.1).

Analog zum Abschnitt „Unterscheidung verschiedener Arten von Funktionen“ liegt es für das Identifizieren der Anforderungen für das Softwaresystem smartLogic nahe, wieder Methoden der Anforderungsanalyse in Betracht zu ziehen. Demnach können Anforderungen entweder über eine ausführliche Recherche und Analyse von bestehenden Systemen und Dokumenten hergeleitet oder systematisch aus den Interessen der Stakeholder des Systems ermittelt werden (vgl. [Pohl & Rupp 2015, S. 21]).

Die betrieblichen Funktionen können demnach zum einen von der globalen Zielsetzung und der Aufgabenstellung der Sicherungslogik innerhalb des Bahnproduktionsprozesses hergeleitet werden (vgl. Kapitel 3.2 und 4.3), wobei sie zusätzlich gegen die Liste der globalen Anforderungen aus

Kapitel 3.5 geprüft werden sollten. Zum anderen kommt die Bestimmung aus der Literatur bzw. per Benchmarking in Betracht. Gemäß dem hybriden Ansatz der Arbeit in Bezug auf die Abwägung zwischen Weiterentwicklung und Neuentwicklung auf der „Grünen Wiese“, sollte zunächst die Herleitung aus der Zielsetzung erfolgen und anschließend die Vervollständigung durch die Literatur und per Benchmarking.

Bei der Übernahme von funktionalen Anforderungen aus der Literatur bzw. aus bestehenden Systemen sollte jedoch geprüft werden, ob diese zusätzlichen Funktionen auch in der zukünftigen Systemumgebung noch benötigt werden (vgl. Abschnitt „Erhöhung der Vollständigkeit“). Die systematische Herleitung der betrieblichen Funktionen erfolgt in Kapitel 6.3 und die Vervollständigung mittels Literatur und zukünftiger Anforderungen in Kapitel 6.5.

Bestimmung der Schutzfunktionen

Neben den betrieblichen Funktionen, müssen auch die Schutzfunktionen als funktionale Sicherheitsanforderungen an die Logik und daraus folgend die Prüfbedingungen identifiziert werden.

Gemäß der *Kernanforderung der sicheren Logik* müssen die notwendigen Prüfbedingungen so vollständig wie möglich sein, um einen unsicheren Zustand hinreichend sicher zu vermeiden (während Vollständigkeit dagegen bei den betrieblichen Funktionen nur eine gewünschte Anforderung ist). Es ist jedoch schwierig, die Vollständigkeit zu beweisen, wenn nicht unmöglich, wie leider immer noch stattfindende Unfälle zeigen. Letztlich muss die finale Bestimmung aller notwendigen Prüfbedingungen bei der Markteinführung gemäß dem vorgeschriebenen Verfahren (vgl. [DIN EN 50126-1:2017]) durch ein Experten-Team erfolgen und durch ein unabhängiges Gutachter-Team bewertet werden. Dies kann und soll naturgemäß eine wissenschaftliche Dissertation nicht leisten. Dennoch ist es für die vorliegende Arbeit wichtig, einen möglichst vollständigen Katalog an Schutzfunktionen und daraus hergeleiteten Prüfbedingungen zu erhalten.

Auch für die Identifikation der notwendigen Schutzfunktionen sind prinzipiell die beiden im vorigen Abschnitt beschriebenen Methoden aus der Anforderungsanalyse denkbar. Das zentrale Interesse der Stakeholder ist im Falle der funktionalen Sicherheitsanforderungen die Gewährleistung der Sicherheit bzw. im Einzelfall die Vermeidung der Gefährdungen, die in der Gefährdungsanalyse in Kapitel 5 identifiziert wurden. Jede Zustandsänderung im Bahnbetrieb kann prinzipiell zu Gefährdungen führen, wenn eine durch die Zustandsänderung ausgelöste Kette an Ereignissen zu der Gefährdung existiert, die als ***Ereigniskette*** bezeichnet wird (vgl. Ereignisbaumanalyse in [Braband 2013, S. 572]). Entsprechende Ereignisketten müssen daher durch die Aufnahme entsprechender Schutzfunktionen in den Funktionskatalog unterbrochen werden.

Aufgrund des hybriden Vorgehens auf Basis des „Grüne Wiese“-Ansatzes (vgl. Kapitel 3.6.2) wird in dieser Arbeit der initiale Katalog an Prüfbedingungen zunächst systematisch aus den Ergebnissen der Gefährdungsanalyse hergeleitet und erst anschließend durch Literatur vervollständigt. Die ausführliche Methode für die systematische Herleitung wird in Kapitel 6.4.1 beschrieben. Mit Schritten zur Erhöhung der Vervollständigung der Prüfbedingungen beschäftigt sich zunächst der Abschnitt Erhöhung der Vollständigkeit in diesem Kapitel. Die Anwendung der dort vorgestellten Methode wird dann in Kapitel 6.5 beschrieben.

Erhöhung der Vollständigkeit

Wie am Beginn des Kapitels und in den vorigen beiden Abschnitten bereits erwähnt, bietet sich zur Erhöhung der Vollständigkeit des Funktionskatalogs ein Benchmark in Bezug auf die Funktionen bestehender Sicherungslogiken an. Hierfür kommen prinzipiell bisherige Stellwerke in Betracht, die derzeit die Sicherungslogik der infrastrukturseitigen Sicherungstechnik beinhalten. Die Funktionen

werden dabei in der Regel in Anforderungsdokumenten und Lastenheften beschrieben. Weiterhin stellen Umsysteme und das betriebliche Regelwerk Anforderungen an die Sicherungslogik.

Die genannten Quellen können als Primärquellen gelten, da sie den aktuellen Stand der Technik in für die Planung und Bedienung verbindlichen Dokumenten repräsentieren und durch ihren offiziell erfolgten akkreditierten Prüfprozess als zum Zeitpunkt der Zulassung weitgehend vollständig angesehen werden können. Sekundärquellen, wie Fachbücher, werden daher nicht zusätzlich betrachtet. Überwiegend aus Ressourcengründen beschränkt sich die Auswertung von Quellen zur Vervollständigung des Funktionskatalogs der Sicherungslogik in dieser Arbeit auf die deutsche Stellwerkstechnik.

Als Dokumentenquelle für die funktionalen Anforderungen an bisherige Stellwerke sieht der Autor dieser Arbeit das bereits etwas ältere Lastenheft für elektronische Stellwerke der DB Netz AG, als größte europäische Eisenbahninfrastrukturbetreiberin, als sinnvolle Quelle [DB Netz AG 2001] an. Dieses Lastenheft ist naturgemäß, vor allem in Bezug auf neue Technologien wie ETCS, lückenhaft, wenn man deren vollen Funktionsumfang nutzen möchte, wie es dem Ziel der vorliegenden Arbeit entspricht. Jedoch kann das Lastenheft dennoch zur Ergänzung des Funktionsumfangs herangezogen werden.

Neben dem Lastenheft für elektronische Stellwerke können Lastenhefte für Umsysteme herangezogen werden, die ebenfalls Anforderungen für ihr Umsystem Sicherungslogik oder häufig allgemeiner „Stellwerk“ stellen. Anforderungsdokumente für frühere Stellwerke werden nicht betrachtet, da davon ausgegangen wird, dass sich die Erkenntnisse aus früheren Generationen in der Entwicklung der aktuellen Generation von Stellwerken bereits wiederfinden.

Eine weitere mögliche Quelle ist das betriebliche Regelwerk, welches sich an den Bediener der technischen Anlagen bauartübergreifend richtet, da es zahlreiche Schutzfunktionen enthält, die entweder vom Stellwerk oder von dessen Bediner erfüllt werden müssen. Hier dient die Richtlinie 408 der Deutschen Bahn AG als Quelle [DB Netz AG 2017a]. Das Regelwerk ist auch eine gute Quelle, wenn es darum geht, zu prüfen, ob weitere menschliche Aufgaben automatisiert und in die Sicherungslogik integriert werden können (vgl. Erkenntnisse aus der Gefährdungsanalyse in Kapitel 5.7).

Eine Gefahr beim Vervollständigen des Funktionskatalogs durch das Heranziehen von Dokumenten, die auf bisherige Stellwerkstechniken ausgelegt sind, liegt allerdings darin, dass nicht mehr benötigte Vorschriften wieder in den Funktionsumfang der smartLogic übernommen werden und damit die globale Anforderung der schlanken Logik verletzt werden könnte. Deshalb ist jede aus diesen Dokumenten zusätzlich identifizierte Funktion bzw. Prüfbedingung kritisch auf ihre Notwendigkeit vor dem Hintergrund der neuen Sicherungslogik zu prüfen. Aus diesem Grund sollte die bestehende Literatur auch erst als zweiter Schritt nach der eigenständigen Herleitung aus der Gefährdungsanalyse zur Identifikation möglicher Funktionen der smartLogic genutzt werden. Schutzfunktionen, die aus Migrationsgründen Anforderungen der Umsysteme repräsentieren, sollten separat abgegrenzt werden, so dass eine Gegenüberstellung ihres Nutzens bei der Migration hin zur neuen Sicherungslogik und der dafür möglicherweise erforderlichen betrieblichen Einschränkungen erfolgen kann.

Da bestehende Regelwerke nur aktuelle und vergangene Technologien abdecken, aber in der Regel keine zukünftigen, bietet es sich außerdem an, funktionale Anforderungen an die Sicherungslogik aus derzeit in der Entwicklung oder in der Konzeptphase befindlichen zukünftigen Technologien herzuleiten. Erkenntnisse daraus können zur Sicherung der Zukunftsfestigkeit der zu entwickelnden Sicherungslogik genutzt werden.

Kategorisierung und Generalisierung

Wie bereits in Kapitel 6.1 festgestellt, ist aufgrund der ressourcenbedingten Eingrenzung auf die Modellierung der Basis-Funktionen in dieser Arbeit (vgl. Kapitel 3.3) eine Priorisierung der Funktionen erforderlich. Um die Priorisierung nicht im Einzelfall begründen zu müssen, erscheint es sinnvoll, die identifizierten Funktionen zunächst zu kategorisieren. Hierfür ist eine geeignete Methode festzulegen (erster Unterabschnitt). Zudem ist im Sinne der Anforderungen der *schlanken Logik* und der *generischen Logik* zu prüfen, ob eine generischere Formulierung der Funktionen und damit möglicherweise eine Zusammenfassung mehrerer Funktionen möglich ist (zweiter Unterabschnitt).

Kategorierung

Eine Kategorisierung ist nach verschiedenen Kriterien möglich. Intuitiv ist bei Schutzfunktionen bzw. den daraus folgenden Prüfbedingungen die Kategorisierung nach der Gefährdungsgruppe (z. B. Engleisung oder Kollision), die ihr zugrunde liegt (vgl. Kapitel 5.5). Bei dieser Einteilung kann es allerdings Überlappungen in dem Sinne geben, dass eine Prüfbedingung mehreren Gefährdungsgruppen zugeordnet werden kann. Es ist wahrscheinlich, dass bei dieser Einteilung ähnliche Prüfbedingungen in derselben Gruppe sind, aber nicht zwingend. Zum Beispiel könnten mehrere Kollisionsarten durch eine Prüfbedingung abgedeckt werden, welche Doppelbeanspruchungen eines Gleisbereichs mit verschiedenen Eisenbahnfahrzeugen ausschließt. Allerdings könnte zum Beispiel sowohl eine Gefährdung aus der Gruppe „Verlassen des zulässigen Fahrwegs“ als auch aus der Gruppe der „Personengefährdungen am Gleis“ zu einer generischen Prüfbedingung zur Einhaltung einer Befahrbarkeitssperre führen.

Da in jedem Fall alle Gefährdungen ausgeschlossen werden müssen, ist für eine Priorisierung die Einteilung nach Gefährdungsgruppen allerdings weniger geeignet. Eine Priorisierung kann daher nicht anhand einer Kategorisierung auf Basis von Eigenschaften der Prüfbedingungen erfolgen, sondern nur anhand deren Relevanz für die einzelnen Prüfprozesse bzw. den gewünschten betrieblichen Funktionsumfang. Deshalb sind weitere Kategorisierungen sinnvoll.

Es erscheint sinnvoll, zu überlegen, ob der Umfang der Prüfbedingungen in Hinblick auf den Anwendungsbereich der Logik reduziert werden kann. Der Anwendungsbereich kann dabei in räumlicher, zeitlicher und funktioneller Hinsicht eingegrenzt werden.

Da im Falle der smartLogic die räumliche Ausdehnung des Zuständigkeitsbereiches einer Instanz der Logik keine große Rolle spielt, da die Regeln generisch und topologieunabhängig formuliert werden sollen, ist vielmehr für den Funktionsumfang relevant, wie die Übergangsbereiche zu Nachbartechnologien gestaltet werden. Der dadurch beeinflusste Umfang der Kompatibilität zu Nachbartechnologien spielt für die Migrationsfähigkeit eine Rolle. Eine Kategorisierung nach Anwendungsbereich, in Hinsicht auf die ausschließliche Bedeutung innerhalb des der smartLogic zugewiesenen Stellbereichs oder in die verschiedenen Übergangsbereiche zu Alttechniken, erscheint daher sinnvoll.

Zeitlich gesehen spielt ebenfalls die Migrationsfähigkeit eine Rolle. Es kann angenommen werden, dass zusätzliche Funktionalitäten notwendig sind, um eine Abwärts- und Aufwärtskompatibilität zu Umsystemen zu gewährleisten.

Der funktionelle Anwendungsbereich erstreckt sich vor allem auf verschiedene Arten von Fahrzeugbewegungen. Von der „gewöhnlichen Fahrt“ – wobei dies hier nicht als fester Begriff definiert werden soll – sind beispielsweise Lademaßüberschreitungen und Fahrzeuge mit besonderen Anforderungen wie Schneeräumfahrzeuge zu unterscheiden. Auch eine Unterteilung in Bezug auf die unterstützten Rückfallebenen und damit den Umfang der Funktionsfähigkeit des Systems bei Ausfall

bzw. Nichtverfügbarkeit von Teilsystemen oder benötigten Informationen kann zum funktionellen Anwendungsbereich gezählt werden.

Eine Unterscheidung in Zug- und Rangierfahrten erscheint dem Autor demgegenüber zunächst nicht intuitiv und sollte nicht unüberlegt aus den bestehenden Regelwerken übernommen werden. Ihr Hintergrund liegt in verschiedenen akzeptierten Sicherheitsniveaus. Diese werden durch unterschiedliche Risiken in Hinsicht auf die beförderten Güter und Personen sowie den erlaubten Geschwindigkeitsbereich begründet. Eine Unterscheidung des Sicherheitsniveaus erscheint prinzipiell denkbar, es sollte allerdings geprüft werden, in welcher Form eine Berücksichtigung unterschiedlicher Sicherheitsniveaus am effektivsten erfolgen kann, auch in Hinblick auf die Anforderung der schlanken Logik.

Generalisierung

Um die globale Anforderung der generischen Logik erfüllen zu können, scheint es vor der Priorisierung auf Basis der Kategorisierung sinnvoll, nach Funktionen der gleichen Kategorie zu suchen, die mit einer generischeren Formulierung zusammengefasst werden können. Dabei ist darauf zu achten, dass keine Schutzfunktionen durch die generische Formulierung verloren geht und dass Prüfbedingungen nicht so allgemein gehalten sind, dass sie bei mehr Prüfprozessen zur Ablehnung einer Prüfanfrage führen würden als zur Aufrechterhaltung der Schutzfunktionen erforderlich.

So ist eine generische Formulierung, die beispielsweise vom Bezug auf konkrete Arten von Infrastrukturelementen abstrahiert (z. B. statt „die Weiche muss die richtige Lage haben“, „das stellbare Fahrwegelement muss den richtigen Status haben“), zwar wünschenswert, um die Logik schlank zu halten, es muss allerdings beachtet werden, dass trotz des fehlenden direkten Bezuges noch alle funktionalen Sicherheitsanforderungen von der generischen Formulierung abgedeckt werden (z. B. wenn „bei Seitenwind darf maximal 90 km/h gefahren werden“ zu „Wettereinschränkungen müssen beachtet werden“ wird, könnte die Information, dass Einschränkungen in Bezug auf den Wind zu beachten sind, verloren gehen).

Bei einer zu generischen Formulierung bestünde außerdem die Gefahr, dass Entscheidungen von der Sicherungslogik zu pauschal getroffen werden könnten (immer zugunsten der Sicherheit). Dadurch würden zu viele Anfragen abgelehnt und damit der Betrieb unnötig eingeschränkt, obwohl die abgelehnten Anfragen nicht tatsächlich zu einer Gefährdung geführt hätten. Beispielsweise, wenn die Schutzfunktion im Falle eines Tunnelbegegnungsverbotes dazu führte, dass sich gar keine Eisenbahnfahrzeuge im Tunnel begegnen könnten, anstatt dies auf bestimmte Konstellationen von Zugarten und bestimmte Geschwindigkeiten einzuschränken. In diesem Spannungsfeld der gegensätzlichen Anforderungen muss wiederum im Zweifel zugunsten der Sicherheit abgewogen werden.

6.2.3 Zusammenfassung der gewählten Methode und Vorgehensweise

Der Funktionsanalyse der smartLogic umfasst die Identifikation der betrieblichen Funktionen sowie der Schutzfunktionen, die im Funktionskatalog zusammengefasst werden. Weiterhin beinhaltet sie die Kategorisierung, anschließende Generalisierung und schließlich Priorisierung der Funktionen, woraus sich der in dieser Arbeit umzusetzende Funktionsumfang der smartLogic bestimmt. Die gewählte Vorgehensweise für die Funktionsanalyse ist in Abb. 44 dargestellt.

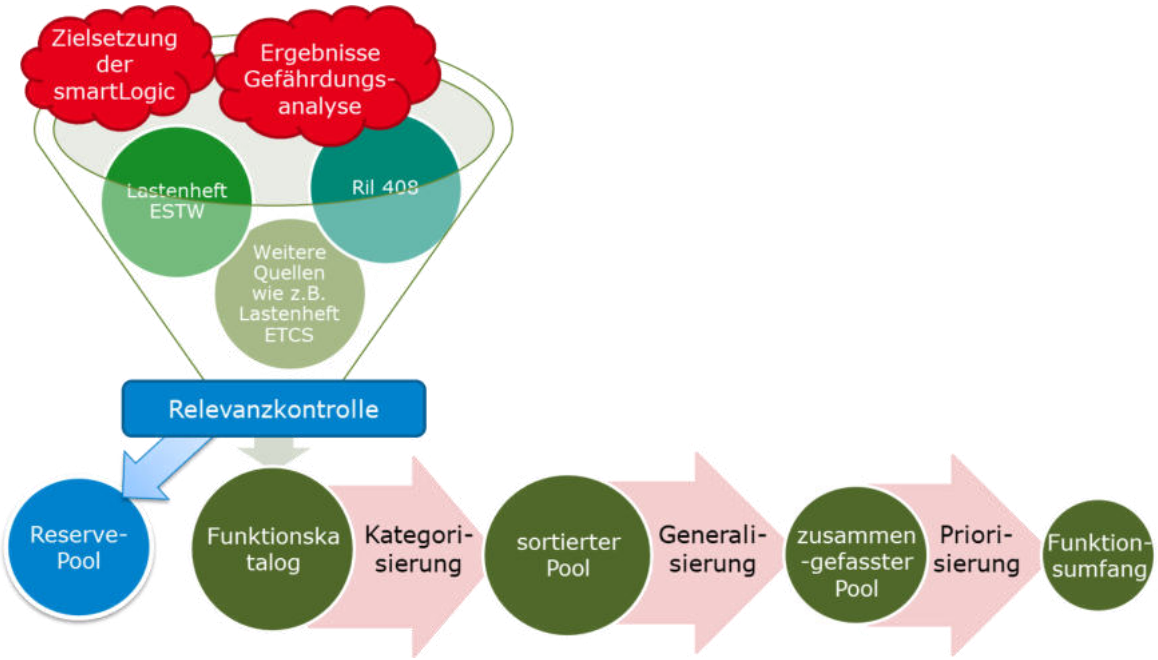


Abb. 44: Vorgehen Funktionsanalyse
Quelle: Eigene Darstellung

Zunächst werden in einem ersten Schritt die gewünschten betrieblichen Funktionen (betrieblich funktionale Anforderungen an die smartLogic) aus der Zielsetzung bestimmt, aus denen sich die Prüfprozesse ergeben (Kapitel 6.3). Im nächsten Schritt werden die möglichen Schutzfunktionen (funktionale Sicherheitsanforderungen) aus den Gefährdungen hergeleitet (Kapitel 6.4), die in der Gefährdungsanalyse im 4. Hauptkapitel identifiziert wurden und in Form von Prüfbedingungen und Reaktionsprozessen in den Funktionskatalog aufgenommen werden. Bei der Definition der einzelnen Prozesse und Prüfbedingungen wird auf eine möglichst generische Formulierung geachtet.

Zur Vervollständigung des Funktionskatalogs werden in einem weiteren Schritt zusätzlich bestehende Quellen ausgewertet. Dies sind vor allem das bereits ältere ESTW-Lastenheft [DB Netz AG 2001] sowie das betriebliche Regelwerk in Form der Ril 408 [DB Netz AG 2017a], außerdem Lastenhefte und Spezifikationen von Umsystemen sowie weitere Quellen der DB Netz AG (Systemdefinition des Teilsystems Zentraleinheit des ESTW-NeuPro bzw. heute DSTW-Kern [DB Netz AG 2017b], Lastenheft für BTSF 3 für ETCS [DB Netz AG 2016], Geschäftliche Anwendungsfälle für die Leitung und Sicherung des Bahnbetriebs [DB Netz AG 2013]).

Bei jeder durch die bestehenden Quellen zusätzlich definierten Funktion (Prozessfunktion oder Prüfbedingung) wird ermittelt, ob sie für die neue Sicherungslogik noch Relevanz besitzt. Dabei werden nur solche Funktionen aussortiert, die hinreichend sicher keine Relevanz für die neue Logik mehr haben. Um ganz sicher zu gehen, werden die aussortieren Funktionen in einem **Reservepool** gesammelt. Die anderen Funktionen werden in den Funktionskatalog aufgenommen (Kapitel 6.5).

Als nächster Schritt erfolgt die Kategorisierung der Funktionen nach verschiedenen Kriterien. Im Anschluss erfolgt ein weiterer Generalisierungsschritt, in dem auf Basis der besseren Übersichtlichkeit nach der Kategorisierung noch einmal versucht wird, die Funktionen generischer zu fassen. Abschließend wird eine Priorisierung auf Basis der Kategorisierung vorgenommen (Kapitel 6.6).

6.3 Betriebliche Funktionen und daraus folgende Prüfprozesse

Die betrieblichen Funktionen wurden in den vorherigen Kapiteln dieses Hauptkapitels als gewünschter Bestandteil des Funktionsumfangs von den zur Aufrechterhaltung der Sicherheit erforderlichen

Schutzfunktionen abgegrenzt. Sie bestimmen damit vor allem, welche Prüfprozesse die Sicherungslogik vorhalten muss, da in den Prüfprozessen die (i. d. R. vom TMS) gewünschten Zustandsänderungen des Systems auf ihre sicherungstechnische Zulässigkeit hin überprüft werden (vgl. Kapitel 4.6).[25] Zum Beispiel bedingt die betriebliche Funktion, den Fahrweg einstellen zu können (also vor allem Weichen umstellen zu können, um Zügen das Wechseln des Gleises zu ermöglichen), als betriebliche funktionale Anforderung, dass es einen Prüfprozess geben muss, der die Zulässigkeit der Zustandsänderung durch den Vorgang des Umstellens der Weiche ermittelt.

Im Folgenden soll zunächst in Kapitel 6.3.1 die Herleitung der betrieblichen Funktionen auf Basis der Erkenntnisse aus Kapitel 6.2.2 erfolgen. Anschließend ist festzulegen, wie die gemäß Kapitel 6.2.2 aus den betrieblichen Funktionen resultierenden Prozessfunktionen formuliert werden können. Hiermit beschäftigt sich Kapitel 6.3.2. Kapitel 6.3.3 fasst die Ergebnisse des Kapitels zusammen.

6.3.1 Herleitung

Wie bereits in der Einleitung zu diesem Kapitel erwähnt, leiten sich die betrieblichen Funktionen gemäß den Erkenntnissen aus Kapitel 6.2.2 aus der globalen Zielsetzung und der Aufgabe der Sicherungslogik bei der Erreichung dieser Zielsetzung her und fließen in Form von Prozessfunktionen (genauer Prüfprozessen) in den Funktionskatalog ein. Bei der Herleitung sind die in Kapitel 6.2.1 identifizierten Anforderungen zu beachten.

Ziel des Bahnbetriebs ist es, wie bereits in Kapitel 3.1 beschrieben, die Durchführung von Fahrzeugbewegungen auf der Eisenbahninfrastruktur zu ermöglichen, um Güter und Personen über das Schienennetz befördern zu können. Die grundlegenden betrieblichen Funktionen der bisherigen Stellwerke sind dabei, den Fahrweg einzustellen und Zugfahrten zuzulassen (vgl. Kapitel 2.1 und die Übertragung dieser Zielstellung auf die smartLogic in Kapitel 3.2). Die dazugehörigen betrieblichen Anforderungen können wie folgt formuliert werden:

- Einem Eisenbahnfahrzeug kann erlaubt werden, einen Teil der Infrastruktur zu nutzen.
- Einem Eisenbahnfahrzeug kann der gewünschte Fahrweg eingestellt werden.

Sollen Eisenbahnfahrzeuge nicht immer als untrennbare Einheiten verkehren, müssen Züge zudem gebildet bzw. getrennt werden können.

- Ein Zugverband kann gebildet (mehrere Zugteile oder einzelne Fahrzeuge vereinigt) oder getrennt werden.

Daraus leiten sich drei grundsätzliche Prüfprozesse her:

- Ausstellen einer Fahrerlaubnis
- Verändern des Status der stellbaren Fahrwegelemente (Controlled Track Elements)
- Veränderung der Fahrzeugzusammensetzung der Fahrzeugbewegungen (Zugtrennung und -vereinigung)

Mit diesen drei Prozessen auf Seiten der infrastrukturseitigen Sicherungslogik ist mit einem funktionierenden Fahrzeug auf einer existierenden und instandgehaltenen Infrastruktur prinzipiell Eisenbahnbetrieb möglich.

[25] Die betrieblichen Funktionen geben dagegen nicht vor, welche Prüfbedingungen innerhalb der Prüfprozesse zu prüfen sind – dies wird durch die Schutzfunktionen als funktionale Sicherheits¬anforderungen bestimmt.

Gemäß der Anforderung der schlanken Logik, könnte der betriebliche Funktionsumfang an dieser Stelle so belassen werden. Allerdings sind weitere spezifische und globale Anforderungen zu beachten (vgl. Kapitel 6.2.1). So werden in Tab. 20 zwei konkrete zusätzliche Prüfprozesse gefordert:

- Funktionen zur Neu-Zuordnung von Infrastrukturelementen (zum Zuständigkeitsbereich der smartLogic)
- Funktionen zur Neu-Zuordnung von Kontrollbereichen

Weitere in Tab. 20 enthaltene Anforderungen an den Umfang des Funktionskatalogs sind abstrakter; Tab. 22 enthält eine Übersicht dieser Anforderungen und der sich daraus ergebenden betrieblichen Anforderungen. Kursive Einträge sind zur Vollständigkeit enthalten, durch sie werden jedoch keine Prozessfunktionen für den Funktionskatalog begründet.

Tab. 22: spezifische Anforderungen an Umfang und Formulierung der funktionalen Anforderungen (Funktionen)

Anforderung aus Tab. 20	**ggf. notwendige betriebliche Anforderung**
alle Schutzfunktionen werden abgedeckt	*bezieht sich auf die Schutzfunktionen, siehe Kapitel 6.4*
möglichst wenig nicht sicherheitsrelevante Funktionen werden abgedeckt	*allgemeine Anforderung an den Umfang, begründet keine spezifische notwendige betriebliche Anforderung*
Anforderungen der Standard-Schnittstellen werden erfüllt	aus den gemäß Kapitel 4.5 relevanten Standardschnittstellen ergeben sich außer den bereits identifizierten Anforderungen, noch Reaktionsprozesse (siehe unten)
der Umfang der zu unterstützenden Alttechnik wird festgelegt	aus der Kompatibilität zur Unterstützung der Alttechnik folgen spezielle Funktionen zum Übergang in andere Stellbereiche, die in dieser Arbeit aus Ressourcengründen nicht detailliert betrachtet werden sollen (vgl. Kapitel 3.3)
funktionale Anforderungen möglicher zukünftiger Technologien bei den Umsystemen werden berücksichtigt	bei der Analyse möglicher zukünftiger Technologien im Bahnbetrieb wie ATO wurden zunächst keine zusätzlichen Prozesse für den Regelbetrieb identifiziert; eine gesonderte Analyse für Rückfallebenen erscheint jedoch sinnvoll, die in dieser Arbeit aus Ressourcengründen nicht erfolgen soll (vgl. Kapitel 3.3)
eine Protokollierung aller Ereignisse wird vorgesehen	*die Protokollierung wird an dieser Stelle ausgeklammert, da sie weder ein Prüf- noch ein Reaktionsprozess ist, sondern bei allen Prozessen mitläuft und die Entscheidungen festhält*
Funktionen vermeiden zusätzlichen Bedarf an Infrastrukturelementen	*definiert keine eigene Prozessfunktion, sondern sollte bei den anderen Prozessfunktionen beachtet werden*
Funktionen vermeiden Benutzerinteraktion	es wird davon ausgegangen, dass Benutzerinterkationen nur für Rückfallebenen erforderlich sind; sie werden demnach im Folgenden ausgeblendet
Funktionen werden so formuliert, dass sie mit möglichst vielen möglichen Betriebssituationen kompatibel sind und auch Rückfallebenen umfassen	ein Prozess zur nachträglichen Anpassung von bereits getroffenen Entscheidungen, insbesondere einer bereits ausgestellten Fahrerlaubnis, soll vorgesehen werden

Eine Analyse der Standardschnittstellen (vgl. Kapitel 4.5) mittels Durchsuchung der entsprechenden Spezifikationsdokumente, wie sie in Tab. 22 gefordert wird, führt zu den in Tab. 23 dargestellten weiteren potenziell notwendigen Prozessfunktionen. Dabei wurden ähnliche Nachrichten, die über

eine Schnittstelle ausgetauscht werden, wie verschiedene Fehlermeldungen oder Lesebestätigungen anderer Nachrichten, aggregiert. In der rechten Spalte findet sich zudem eine Einordnung bezogen auf die Prozessart bzw. die Relevanz für die smartLogic. Kursive Einträge sind zur Vollständigkeit enthalten, führen aber nicht zur Aufnahme weiterer Prozessfunktionen. Zusätzlich zu den Standardschnittstellen wurde die Schnittstelle zu den Datenquellen gemäß der Architektur aus Kapitel 4.6 ergänzt.

Tab. 23: von Standardschnittstellen geforderte potenzielle Prozessfunktionen

Schnittstelle	pot. notwendige Prozessfunktion	Prozessart / Relevanz
ETCS	Verarbeitung der Zugdaten	*diese Schnittstelle wird in der Architektur aus Kapitel 4 über die Fahrzeugdatenaggragtion abgedeckt*
	Verarbeitung von Position Reports	*diese Nachricht wird in der Architektur aus Kapitel 4 über den Ortungsinformationsaggregator abgedeckt*
	Start of a mission / Aufbau der Kommunikationssession	Prüfprozess
	End of mission / Abbau der Kommunikationssession	Reaktionsprozess, nur für die interne Datenverwaltung relevant, da das Fahrzeug hierduch nicht verschwindet
	Verarbeitung rangierbezogener Nachrichten	*Hierfür sollte die Notwendigkeit noch geklärt werden. Siehe Kapitel 8.3.5*
	Verarbeitung verschiedener Arten von Benachrichtigungen zur Bestätigung des Nachrichtenerhalts oder ausgeführter Handlungen	Subroutine, da diese Nachrichten nur als Reaktion auf vorausgehende Nachrichten, die im Rahmen eines Prozesses gesendet wurden, erfolgen
	Verarbeitung von fahrzeugseitigen Fehlermeldungen	Reaktionsprozesse
EULYNX SCI-TDS	Verarbeitung von Meldungen der infrastrukturseitigen Gleisfreimeldeeinrichtungen	*diese Schnittstelle wird in der Architektur aus Kapitel 4 über den Ortungsinformationsaggregator abgedeckt*
EULYNX SCI-PM	Stellbefehle der Weichen	*bereits oben bei den grundsätzlichen Prozessfunktionen abgedeckt*
	Verarbeitung von Status-Informationen der Weichen	Reaktionsprozesse, sofern nicht Teil der Prüfung von Stellbefehlen (dann Subroutine)
EULYNX SCI-LX	Kommando zum Bahnübergang schließen	*Vorgang ist nicht sicherheitskritisch, solange davon ausgegangen werden kann, dass ohne die Meldung „Bahnübergang geschlossen und gesichert" der Bahnübergang nicht befahren werden kann*
	Verarbeitung der Meldung Bahnübergang geschlossen und gesichert bzw. Einschaltbereitschaft des BÜ	Subroutine, da es im Rahmen von Prozessen geprüft werden muss
	Störmeldungen des Bahnübergangs	Reaktionsprozess (in Tab. 24 als Störmeldungen von Stakeholdern-Systemen zusammengefasst, siehe hierzu Kapitel 8.3.3)

Datenquellen inkl. Ortungs-informations-aggregator	Abfragen von Informationen	Subroutine, da das Abfragen im Rahmen von Prozessen erfolgt
	Verarbeiten von Informationsupdates	verschiedene Reaktionsprozesse

Die Vollständigkeit der Auflistung kann nicht alleine durch die beschriebene Vorgehensweise garantiert werden. Ein hoher Grad an Vollständigkeit wird aber durch die zusätzliche Literaturanalyse in Kapitel 6.5 erreicht, die wie bereits erwähnt aufgrund des „Grüne-Wiese"-Ansatzes erst nach dem Brainstorming durchgeführt wurde.

Weitere betriebliche Funktionen können identifiziert werden, wenn man vor- und nachgelagerte Tätigkeiten zur Aufrechterhaltung des Bahnbetriebs in der Betriebsphase der Sicherungslogik wie Instandhaltung und Bauarbeiten sowie besondere Fahrten, z. B. mit Spezialfahrzeugen, mitbetrachtet. Die Vollständigkeitskontrolle kann hier besonders gut über die Auswertung der in der Diskussion der Vorgehensweise (Kapitel 6.2.2) genannten Quellen erfolgen, wie sie in Kapitel 6.5 durchgeführt wird.

- Ermöglichen von Fahrbetrieb bei geplanten und ungeplanten Abweichungen vom Regelbetrieb wie z. B. Bauarbeiten an den Gleisen
- Ermöglichen des Aufgleisens und Ausgleisens von Baustellenfahrzeugen und neuen Fahrzeugen
- Ermöglichen von Fahrbetrieb bei Instandhaltungsarbeiten an der Infrastruktur
- Durchführung von Fahrten mit besonderen Anforderungen, z. B. Schneeräumung der Gleise oder Fahrten mit Lademaßüberschreitung

Nicht jeder dieser zusätzlichen betrieblichen Funktionen bzw. Funktionscluster muss auch zu einer eigenen Prozessfunktion der Sicherungslogik führen. Beispielsweise wäre es auch denkbar, dass z. B. die Funktion „Fahrbetrieb bei Bauarbeiten an den Gleisen" durch die Aufnahme zusätzlicher Prüfbedingungen im Prozess „Ausstellen einer Fahrerlaubnis" abgedeckt werden kann. Endgültig kann diese Zuordnung erst bei der Modellierung der Logik geklärt werden (Kapitel 8), daher erfolgt zunächst im Funktionskatalog nur eine vorläufige Zuordnung, die bei der Logikentwicklung überprüft wird.

6.3.2 Formulierung der Prozessfunktionen und Subroutinen

Aus Gründen der Verständlichkeit und Übersichtlichkeit ist es sinnvoll, für die einzelnen Funktionen im Funktionskatalog eine möglichst einheitliche Notation zu verwenden. Wie oben bereits erläutert, resultieren aus den betrieblichen Funktionen zunächst hauptsächlich Prozessfunktionen. Da Subroutinen allerdings ebenfalls Teile von Prozessen beschreiben, erscheint es plausibel, für sie ähnliche Formulierungen zu verwenden. Auf die Formulierung von Prüfbedingungen wird in Kapitel 6.4.2 eingegangen.

Da die Prozessfunktionen aus den funktionalen Anforderungen an die Sicherungslogik resultieren, können Methoden der Anforderungsanalyse zur Formulierung verwendet werden. Demnach kann die Notation entweder textuell oder formal, z. B. mit Diagrammen erfolgen (vgl. z. B. [Rupp 2007]).

Vor- und Nachteile der verschiedenen Beschreibungsmöglichkeiten wurden bereits in Kapitel 2.6.2. diskutiert. Die textuelle Beschreibung ist demzufolge am einfachsten umsetzbar. Da die in Kapitel 6.3.1 hergeleiteten betrieblichen Funktionen und daraus folgenden Prozessfunktionen sehr überschaubar sind und wenig Interpretationsspielraum lassen, erscheint eine textuelle Beschreibung an dieser Stelle ausreichend zu sein.

Zudem ist zu entscheiden, in welcher Sprache die Funktionen notiert werden sollen. Für den Autor umsetzbar ist entweder die deutsche Sprache als Amtssprache in Deutschland oder die international in der Forschung und in internationalen Organisationen als Arbeitssprache gebräuchliche englische Sprache. Da die Ergebnisse der Arbeit nicht auf den deutschsprachigen Raum begrenzt sein sollen, wird für die Notationen an dieser Stelle und im Folgenden die englische Sprache verwendet.

Die textuelle Beschreibung sollte ebenfalls einem klaren syntaktischen Schema folgen. Gängige Schemas aus der Anforderungsanalysen greifen für die textuelle Beschreibung von Anforderungen auf den Aufbau von natürlichsprachlichen Sätzen zurück (daher wird auch von natürlichsprachlichen Anforderungen gesprochen) (vgl. z. B. Kapitel 8 in [Rupp 2007] und Kapitel 19 in [Balzert 2009]). Natürlichsprachliche Sätze bestehen bekanntlich aus Subjekt, Prädikat, Objekt(en) und adverbialen Bestimmungen.

Das Subjekt der Prozessfunktion bzw. Subroutine (also der funktionalen Anforderung) ist das zu entwickelnde System, also die Sicherungslogik: „**Die Sicherungslogik** muss/soll …“. In diesem Fall ist das Subjekt jedoch wenig aussagekräftig, da immer die Sicherungslogik Subjekt ist. Aus Vereinfachungsgründen kann es daher auch weggelassen werden.

Das Prädikat enthält das Hauptverb. RUPP nennt dies „Prozesswort“ [Rupp 2007, S. 228]. Bei Prozessfunktionen ist immer eine Anfrage durch ein externes System, in der Regel das TMS, über eine festgelegte Schnittstelle der Auslöser. In diesem Fall besagt das Prozesswort schlicht, dass die Anfrage bearbeitet werden können muss: „process [request]“. Bei Subroutinen sind vielfältige Prozessworte möglich.

Üblicherweise wird in klassischen Anforderungsdokumenten, wie dem Lastenheft, dem Prozesswort ein Hilfsverb vorangestellt, welches die Verbindlichkeit der Anforderung definiert (Muss-Bestimmung vs. Kann-Bestimmung) (vgl. [Balzert 2009, S. 483]). Da eine Bewertung der Wichtigkeit erst im weiteren Verlauf im Rahmen der Priorisierung, die auch mehr als zwei Stufen enthalten kann, vorgesehen ist, wird auf eine solche Einteilung in Verbindlichkeiten an dieser Stelle verzichtet.

Der Objektteil beschreibt die zu verarbeitende Anfrage bzw. bei den Subroutinen, welche Informationen verarbeitet werden sollen. Dabei müssen die Substantive im Datenmodell definiert sein, das in Hauptkapitel 7 erarbeitet wird.

Der letzte Satzbestandteil sind die adverbialen Bestimmungen. Sie ermöglichen Einschränkungen des Satzinhalts auf bestimmte Rahmenbedingungen (z. B. örtlich, zeitlich, bzgl. der Art und Weise oder definierten Bedingungen).

6.3.3 Zusammenfassung

Tab. 24 enthält die gemäß der in diesem Kapitel beschriebenen Methode identifizierten und formulierten Prozessfunktionen. Für die Gesamtliste und weitere Details siehe Anlage 2. Für eine Übersicht der wichtigsten funktionalen Anforderungen an die Logik siehe Tab. 26 in Kapitel 6.7. In der zweiten Spalte von Tab. 24 ist angegeben, ob es sich um einen Prüf- (‚C‘) oder Reaktionsprozess[26] (‚R‘) handelt. Dabei ist zu beachten, dass nicht untersucht wurde, welche Bedienfunktionen möglicherweise für Rückfallebenen relevant sein könnten.

[26] Falls es sich um die Antwort auf eine von der smartLogic gesandte Anfrage, die im Rahmen eines Prüfprozesses gestellt wurde, handelt, kann die Verarbeitung der Antwort auch in die Prozessfunktion oder Shared Function integriert sein.

Tab. 24: Liste der mit der systematischen Methode identifizierten Prozessfunktionen

ID	C/R	Prozessfunktion	Bemerkung
F-E002	C	process train registration request	vgl. bei ETCS: „start of a mission“; siehe Kapitel 8.4.2; inkl. Baustellenfahrzeuge
F-E009	C	process stakeholder list update	siehe zum Konzept der Stakeholder-Systeme Kapitel 8.3.3, siehe auch Kapitel 8.5.2
F-E040	C	process status change requests for controlled track element	Stellanforderung, siehe Kapitel 8.5.5
F-E051	C	process movement authority request	Fahrerlaubnisanfrage, siehe Kapitel 8.5.3
F-E051a	*C*	*process movement authority requests for movable objects with special requirements*	*kann in F-E051 integriert werden*
F-E059	C	process movement authority change request	siehe Kapitel 8.5.4
F-E091	C	process train dividing request	siehe Kapitel 8.4.3
F-E092	C	process train joining request	
F-E140	C	process change of global paramter request (e.g. friction, breaking distance, weather indicator)	ähnlich zu F-E898 und F-E899
F-E257	C	process stakeholder status change request for external systems such as LX (if safety relevant)	ähnlich zu F-E040, wird als Spezialfall betrachtet
F-E806a	C	process area of responsibility change request	siehe Kapitel 8.4.5
F-E806b	C	process control area change request	
F-E898	C/R	insert restriction	siehe Kapitel 8.5.1
F-E899	C/R	update restriction	
F-E093	C/R	process vehicle transfer on track	wenn vor Eingleisung zum Einholen einer Erlaubnis: Prüfprozess; ansonsten: Reaktionsprozess
F-E003a	R	process “end of a mission” notification	nur für die Datenhaltung relevant
F-E006	R	process externally triggered status update of infrastructure attributes	bei (mglw. unerwarteten) Veränderungen an den Infrastrukturdaten
F-E007	R	process train position report	Update kommt über Ortungsinformations-aggregator
F-E008	R	process train information updates	
F-E074	R	process vehicle registration after leaving a locally controlled area	
F-E094	R	process vehicle transfer from track	wenn ein Fahrzeug eine Ausgleisung meldet
F-E107	R	process status updates of controlled track elements	z. B. neue Weichenlage

F-E108	R	process state reports of controlled track elements	z. B. über Zustand "Betriebsbereit"
F-E132b	R	process trackside monitoring system reports	
F-E242	*R*	*process a track clearance message*	*infrastrukturseitige Ortungsmeldung fließt in Ortungsinformations-aggregator, s. F-E007*
F-E258	R	process status updates of stakeholders	z. B. neuer Sensorwert
F-E259	R	process state reports of stakeholders	z. B. über Zustand "Betriebsbereit"
F-E749	*R*	*[placeholder for fallback modes]*	
F-E807	R	process infrastructure update	

6.4 Schutzfunktionen und daraus folgende Prüfbedingungen und Reaktionsprozesse

Neben den betrieblichen Funktionen muss die Sicherungslogik aufgrund der Kernanforderung der sicheren Logik die Schutzfunktionen erfüllen, die in diesem Kapitel hergeleitet werden sollen (vgl. Kapitel 6.1).

Die Schutzfunktionen werden gemäß der in Kapitel 6.2.3 beschriebenen, grundsätzlichen Methode dem „Grüne Wiese"-Ansatz folgend aus den Ergebnissen der Gefährdungsanalyse hergeleitet und fließen als Prüfbedingungen oder ggf. als Reaktionsprozess in den Funktionskatalog ein. Die zugrundeliegenden Gefährdungen wurden in der Gefährdungsanalyse in Kapitel 5 identifiziert. In diesem Kapitel wird zunächst in Kapitel 6.4.1 die Herleitung der Schutzfunktionen und der daraus folgenden Prüfbedingungen und Reaktionsprozesse auf Basis der in Kapitel 6.2.2 besprochenen, grundsätzlichen Methode weiter detailliert. Da Reaktionsprozesse auch Prozessfunktionen sind, bietet es sich an, bei den Reaktionsprozessen auf die Formulierungsregeln der Prozessfunktionen und Subroutinen in Kapitel 6.3.2 zurückzugreifen. Bei den Prüfbedingungen handelt es sich dagegen nicht um Prozesse, weshalb eine eigene Herleitung der Regeln für die Formulierung der Prüfbedingungen sinnvoll erscheint. Diese Herleitung der Formulierungsregeln für Prüfbedingungen erfolgt in Kapitel 6.4.2. Anschließend werden die Herleitung und die Formulierungsregeln in diesem Kapitel anhand von zwei Beispielen verdeutlicht (Kapitel 6.4.3 und 6.4.4).

Die Liste der identifizierten Schutzfunktionen findet sich aufgrund des Umfangs in Anlage 2. In Kapitel 6.5 erfolgt die Vervollständigung der Liste der Schutzfunktionen anhand der Literatur.

6.4.1 Herleitung

Wie in der Einleitung zu diesem Kapitel erwähnt, werden die Schutzfunktionen aus den Gefährdungen im Bahnbetrieb hergeleitet. Eine „Gefährdung entsteht durch ein mögliches räumliches und/oder zeitliches Zusammentreffen eines verletzungs- bzw. krankheitsbewirkenden Faktors einer Gefahrquelle." [BfGA 2020]. Zugrunde liegen ein oder mehrere verkettete Ereignisse, die zum unerwünschten Zusammentreffen führen. Diese bilden die möglichen Ursachen der Gefährdung. Die Wahrscheinlichkeit für das Eintreten dieser möglichen Ereigniskombinationen bzw. Ereignisketten müssen begrenzt werden. Die Wahrscheinlichkeit für das Eintreten der Gefährdung ergibt sich aus den multiplizierten Wahrscheinlichkeiten der Einzelereignisse der Ereigniskette (vgl. Ereignisbaumanalyse in [Braband 2013, S. 572]).

Es ist möglich, dass die Eintrittswahrscheinlichkeit für eine Gefährdung über eine Ereigniskette bereits ohne weitere technische Maßnahmen hinreichend klein ist, so dass das System (bei ausreichender Einschränkung der anderen Ereignisketten, die zu Gefährdungen führen) als sicher gelten kann. In vielen Fällen werden jedoch Maßnahmen erforderlich sein, um die Eintrittswahrscheinlichkeit zu senken. Dies kann zum Beispiel über Prüfbedingungen der Sicherungslogik erfolgen. Damit dient die Sicherungslogik als ***Barriere*** in den Ereignisketten (vgl. zu „Barriere“ [Braband 2013, S. 596]). In diesen Fällen, in denen die Sicherungslogik über eine Prüfbedingung einen signifikanten Anteil zur Reduzierung der Eintrittswahrscheinlichkeit einer Gefährdung beitragen kann, ergibt sich daher eine funktionale Sicherheitsanforderung an die Sicherungslogik.

Die wesentlichen Ursachen für die Gefährdungen wurden im Rahmen der Gefährdungsanalyse in Kapitel 5 erfasst. In Kapitel 5.6 wurde bereits jeweils bewertet, ob die Sicherungslogik einen Einfluss auf die Eintrittswahrscheinlichkeit der Gefährdung haben kann. Ist dies der Fall, besteht eine funktionale Sicherheitsanforderung und es sollte eine Prüfbedingung als Barriere formuliert werden.

Zu beachten ist, dass die funktionalen Sicherheitsanforderungen eine abstrakte Anforderung nach einer Barriere darstellen. Sie enthalten noch keine Aussage über die Umsetzung dieser Barriere. Dies wird erst über die genaue Formulierung der zugehörigen Prüfbedingung(en) konkretisiert.

6.4.2 Formulierung

Prüfbedingungen sollen gemäß ihrer Definition in Kapitel 6.2.2 eine Umsetzung der funktionalen Sicherheitsanforderungen (Schutzfunktionen) darstellen, indem die Schutzfunktionen in klar zu prüfende Sachverhalte übertragen werden. Für die Formulierung von Anforderungen an sicherheitskritische Systeme, wie sie von Prüfbedingungen abgedeckt werden, gibt es – anders als bei den gewünschten betrieblichen funktionalen Anforderungen – klare Vorgaben. [DIN EN 50126-1:2017, S. 72] fordert unter anderem, dass

- „sie vollständig, präzise, eindeutig, verifizierbar, prüfbar und vertretbar sind;“
- „sie so geschrieben sind, dass sie für das Verständnis der Personen, die die betreffenden Informationen in irgendeiner Phase des Lebenszyklus wahrscheinlich nutzen werden, förderlich sind;“

Daher ist, wie bei den Prozessen und Subroutinen, eine präzise Formulierung des Prüfgegenstandes der Prüfbedingung erforderlich. Für die Beschreibung ist entsprechend ein geeignetes Beschreibungsmittel und eine Syntax festzulegen. Zu letzterem gehört auch, mit welchen Parametern ggf. die Prüfbedingung präzisiert werden kann. Im Hinblick auf die Anforderungen der schlanken Logik kann zudem überlegt werden, ob die Anzahl der Prüfbedingungen durch generische Formulierung reduziert werden kann (vgl. Kapitel 6.2.1).

Beschreibungsmittel

Mögliche Beschreibungsmittel wurden bereits für die Prozessfunktionen und Subroutinen in Kapitel 6.3.2 diskutiert. Im Falle der sicherheitskritischen Prüfbedingungen sind auch die Anforderungen an die Formulierung von Anforderungen sicherheitsrelevanter Systeme in [DIN EN 50126-1:2017, S. 72]) zu beachten. Auch nach der genannten Norm ist es prinzipiell möglich für die Formulierung der Prüfbedingungen auf eine formale Modellierungssprache zurückzugreifen, die Prüfbedingungen textuell (natürlichsprachlich / „Prosa“) zu beschreiben oder grafisch zu notieren.

Da sich eine grafische Beschreibung insbesondere zur verständlichen Darstellung komplexer Sachverhalte, aber weniger zur Abbildung von Listen eignet, wird sie für den vorliegenden

Anwendungszweck ausgeschlossen. Eine formale Beschreibung wäre dagegen möglich, sofern sie sich auf ein wohl definiertes Modell stützt. Allerdings wäre die korrekte formale Beschreibung der funktionalen Anforderungen sehr aufwändig und würde möglicherweise bereits die Umsetzung vorwegnehmen. Für den vorliegenden Anwendungsfall wird die textuelle Beschreibung ebenfalls als akzeptabel angesehen, sofern sie ein stringentes Vokabular verwendet. Die textuelle Formulierung ist am schnellsten anzuwenden und erleichtert im Vergleich zur formalen Beschreibung die Diskussion des Sachverhaltes. Zudem wurden die betrieblichen Funktionen ebenfalls textuell formuliert (vgl. Kapitel 6.3.2). Aus diesen Gründen wird im Folgenden auf die textuelle Beschreibung zurückzugreifen.

Syntax für die Formulierung der Prüfbedingungen

Um eine Syntax für die konkrete Formulierung der Prüfbedingungen festzulegen, bietet es sich wie bei den Prozessfunktionen und Subroutinen an, auf die Erfahrungen der Anforderungsanalyse zurückzugreifen. Bereits in Kapitel 6.3.2 wurde erläutert, dass gängige Schemas für die textuelle Beschreibung von Anforderungen auf den Aufbau von natürlichsprachlichen Sätzen zurückgreifen. Wie bei den Prozessfunktionen und Subroutinen kann das Subjekt der Anforderung (das System smartLogic) aufgrund des geringen Erkenntnisgewinns aus Vereinfachungsgründen weggelassen werden.

Das Prädikat bzw. nach RUPP „Prozesswort“ [Rupp 2007, S. 228] enthält das Hauptverb. Da die Prüfbedingungen nicht direkt einen Prozess beschreiben, wie die Prozessfunktionen und Subroutinen, sondern die Einhaltung der Sicherheitsvorgaben, beschränken sich auch die Prozesswörter auf diese Aufgabe.

Eine Prüfbedingung kann prinzipiell positiv (Prozesswort „Sicherstellen“, engl. „*Ensure*“) oder negativ (Prozesswort „Verhindern“, engl. „*Prevent*“) formuliert werden. Prinzipiell können negative Formulierungen (***Negativbedingung***) in positive Formulierungen (***Positivbedingung***) umgewandelt werden (Z. B. „[Die Sicherungslogik muss] Verhindern, dass Personen der Übergang über ein Gleis erlaubt wird, wenn dieses Teil einer genehmigten Fahrerlaubnis ist“ und „[Die Sicherungslogik muss] Sicherstellen, dass Personen der Übergang über kein Gleis erlaubt wird, welches Teil einer genehmigten Fahrerlaubnis ist.“). Da die beiden Formulierungsweisen unterschiedliche Betonungen haben, sind sie in unterschiedlichen Fällen intuitiv (z. B. Negativbedinungen bei präventiver Gefährdungsvermeidung, Positivbedingungen im Fall von Zustandsänderungen). Bei der Transformation können leicht Fehler gemacht werden, z. B. wenn im zweiten Fall statt „kein Gleis“ „ein Gleis“ übernommen worden wäre. Dagegen sind keine negativen Auswirkungen für den Fall ersichtlich, dass beide Formulierungsweisen zugelassen werden. Aus diesem Grund enthält der Katalog an Prüfbedingungen Positiv- und Negativbedingungen.

Da es sich bei den Prüfbedingungen aufgrund der Relevanz für die Sicherheit grundsätzlich um Muss-Bestimmungen handelt, wird wie bei den Prozessfunktionen und Subroutinen auf den Zusatz eines Hilfsverbes verzichtet, welches die Verbindlichkeit der Prüfbedingung näher erläutert.

Der Objektteil beschreibt die eigentliche Prüfbedingung. Er enthält immer eine klare Aussage, bei der jedes Substantiv klar definiert sein muss. Diese Definitionen finden sich wie im Falle der Prozessfunktionen und Subroutinen im Datenmodell, das in Hauptkapitel 7 beschrieben wird.

Der letzte Satzbestandteil sind die adverbialen Bestimmungen. Sie ermöglichen Einschränkungen des Satzinhalts auf bestimmte Rahmenbedingungen (z. B. örtlich, zeitlich, bzgl. der Art und Weise oder definierter Bedingungen) und sollen im nächsten Abschnitt näher erläutert werden.

Einfügen geeigneter Parameter

Mittels der adverbialen Bestimmungen können Prüfbedingungen feiner formuliert werden. Durch eine solche feinere Ausdifferenzierung der Prüfbedingungen werden unnötige Einschränkungen vermieden (z. B. „Sicherstellen, dass Züge bei Wind *mit mehr als 90 km/h* die Geschindigkeit reduzieren“).

Bei der Nutzung der adverbialen Bestimmungen muss allerdings darauf geachtet werden, dass keine speziellen Schutzfunktionen durch die adverbiale Bestimmung aus dem Abdeckungsbereich der Prüfbedingung ausgeschlossen werden (z. B. würde die Ortsangabe „auf dem Bahnsteig“ bei „Verhindern, dass Personen *auf dem Bahnsteig* der Übergang über ein Gleis erlaubt wird“ unzulässigerweise Personen ausnehmen, die sich nicht auf dem Bahnsteig befinden). Weiterhin sollte im Sinne der globalen Anforderung der *generischen Logik* verhindert werden, dass durch die Verwendung von adverbialen Bestimmungen mehr Prüfbedingungen als erforderlich formuliert werden, die sich auch zu einer generischen Prüfbedingung zusammenfassen lassen (z. B. „Verhindern, dass Personen *auf dem Bahnsteig* der Übergang über ein Gleis erlaubt wird“ und „Verhindern, dass Personen *außerhalb von Bahnhöfen und Bahnübergängen* der Übergang über ein Gleis erlaubt wird“).

Gemäß der obigen Diskussion machen adverbiale Bestimmungen vor allem dann Sinn, wenn sie eine Fallunterscheidung in Bezug auf die Genehmigungsfähigkeit einer Anfrage ermöglichen, die bei unterschiedlichen Bedingungen zu unterschiedlichen Ergebnissen führt, weil durch diese Fallunterscheidung die Genehmigung zusätzlicher Fahrten bzw. Stellbefehle möglich wird. Die Genehmigungsfähigkeit einer Anfrage hängt von den Eintrittswahrscheinlichkeiten der Gefährdung über die betrachteten Ereignisketten ab. Eine genaue Betrachtung von Eintrittswahrscheinlichkeiten wird – wie in Kapitel 3.3 abgegrenzt – in der vorliegenden Arbeit nicht vorgenommen, da in jedem Einzelfall eine umfangreiche Recherche und ggf. weitere Maßnahmen zur Bestimmung der Eintrittswahrscheinlichkeit notwendig wären. Stattdessen werden die Eintrittswahrscheinlichkeiten als später festzulegende Parameter betrachtet, die jederzeit ohne Veränderung der Sicherungslogik angepasst werden können.

Mögliche Parameter, die über adverbiale Bestimmungen in die Prüfbedingung mitaufgenommen werden können, legen zum Beispiel einen Geschwindigkeitsbereich fest, in dem die Prüfbedingung gültig ist, da die Geschwindigkeit einen Einfluss auf die Prüfbedingungen hat.

Nachfolgend werden zwei Beispiele zur Anwendung der Formulierungsregeln beschrieben.

6.4.3 Beispiel 1: „keine Warnung vor Zugfahrt“

Als erstes Beispiel zur Anwendung der Formulierungsregeln kann durch Anwendung der in Kapitel 6.4.1 definierten Regeln aus der Gefährdung „keine Warnung vor Zugfahrt“ der Kategorie „potenzielle Schadensausmaßvergrößerung“ (identifiziert u. a. über die Primärgefährdung „Sog“ für Menschen am Bahnsteig oder am Gleis) die funktionale Sicherheitsanforderung (Schutzfunktion) hergeleitet werden, dass Menschen an Orten, an denen sie Zügen nahekommen, gewarnt werden müssen. Solche Berührungsorte sind die Bahnsteige und Bahnübergänge, aber auch die Strecke, wenn sich dort Menschen aufhalten. Durch die unterschiedlichen Orte ergeben sich aus der funktionalen Sicherungsanforderung also mehrere Prüfbedingungen.

Die Art und Weise der Warnung wird an dieser Stelle nicht festgelegt. Sie kann auch außerhalb der Funktionsweise der Sicherungslogik erfüllt werden, z. B. durch Personalschulungen. Die Sicherungslogik muss allerdings dafür vorbereitet sein, eine solche funktionale Sicherheitsanforderung durch geeignete Prüfbedingungen abprüfen zu können.

Als einschränkende Parameter zur Eingrenzung des Anwendungsbereiches der Prüfbedingung kommen Eigenschaften der beteiligten Zugfahrten in Betracht. So spielt die Geschwindigkeit bei der nicht erfolgten Warnung durch ein von der Sicherungslogik angesteuertes Warnsystem eine Rolle, da bei niedrigen Geschwindigkeiten die Gefahr vom Gefährdeten eher erkannt wird oder andere Möglichkeiten zur Warnung außerhalb des Kontrollbereichs der Sicherungslogik (z. B. durch den Tf) wahrscheinlicher zum Erfolg führen, z. B. ein Achtungspfiff. Es wäre also denkbar, dass eine Warnung durch die Sicherungslogik erst ab einer bestimmten Geschwindigkeit des durch den Warnbereich fahrenden Zuges sichergestellt werden müsste und vorher über andere Maßnahmen erfolgt. Wie hoch diese Geschwindigkeit wäre oder ob immer gewarnt werden muss, spielt für die Entwicklung der Sicherungslogik keine Rolle, da es sich nur um einen einstellbaren Parameter handelt. Ein weiterer solcher Parameter könnte auch die Zugart sein. Z. B. wäre es denkbar, dass die automatische Warnung für verschiedene Zugarten ab unterschiedlichen Geschwindigkeiten von der Sicherungslogik überwacht wird.

Die resultierende Prüfbedingung wäre also z. B. für die Personen am Bahnsteig: *Ensure that people at a platform are warned if a MA is issued to a train which is allowed to pass a platform with more than {TRAINTYPE|OP_CAUTION_VMAX}*.

Die Prüfbedingung kann auch gleichzeitig weitere Schutzfunktionen oder zumindest einzelne Anwendungsbereiche solcher Schutzfunktionen abdecken, z. B. der Personengefährdung am Gleis durch Überrollen.

6.4.4 Beispiel 2: „Masse / Achslast zu hoch“

Als weiteres Beispiel dient die Gefährdung, die durch eine Fahrt in ein Gleis verursacht wird, für welches ihre Achslast zu hoch ist. Hierdurch könnte es zu einer Entgleisung durch Infrastrukturversagen kommen oder die Infrastruktur könnte beschädigt werden.

Eine Ereigniskette zu dieser Gefährdung könnte z. B. eine Fahrzeugbewegung beinhalten, die eine Fahrerlaubnis in einen Abschnitt erhält, für den sie die zulässige Achslast überschreitet bzw. eine Fahrerlaubnis mit einer Geschwindigkeit, die für ihre Achslast und das entsprechende Gleis zu hoch ist. Es könnte aber auch eine falsche maximale Achslast des betroffenen Abschnitts oder der Fahrzeugbewegung im System hinterlegt sein. Die Fahrzeugbewegung könnte auch über einen Fahrweg erfolgen, für den sie gar keine Fahrerlaubnis hat und so auf das Gleis gelangen, dessen zulässige Achslast sie überschreitet.

Eine funktionale Sicherheitsanforderung, welche alle diese Pfade abdeckt, wäre zum Beispiel, die Einfahrt von Fahrzeugbewegung in ein Gleis zu verhindern, wenn dadurch die dort zulässige Achslast überschritten ist. Durch diese Sicherheitsanforderung nicht abgedeckt wäre allerdings der Fall, wenn die Achslastüberschreitung entsteht, während sich das Fahrzeug bereits auf dem betroffenen Gleis befindet. Dies könnte z. B. bei der Beladung geschehen. Eine weitere funktionale Sicherheitsanforderung wäre daher, bei der Beladung sicherzustellen, dass die zulässige Achslast nicht überschritten wird. Letzterer Fall fällt jedoch nicht in den Zuständigkeitsbereich der Sicherungslogik, da die Gefährdung nicht bei der Durchführung einer Fahrzeugbewegung auftreten würde. Erst wenn die Fahrzeuge sich in Bewegung setzen sollen, kommt die Sicherungslogik ins Spiel. Dann würde aber die zuerst definierte funktionale Sicherheitsanforderung greifen.

Ein einschränkender Parameter (mit begrenzter Wirkung) kann auch in diesem Beispiel die gefahrene Geschwindigkeit sein. So wäre es denkbar, dass die Eintrittswahrscheinlichkeit eines Schadens durch die Überschreitung der Achslast bei höheren Geschwindigkeiten wahrscheinlicher wird und somit bei

niedrigen Geschwindigkeiten noch akzeptiert werden kann. Demnach wäre es vorstellbar, dass für verschiedene Geschwindigkeiten unterschiedliche Grenzachslasten gelten.

Eine passende Prüfbedingung könnte daher lauten: *Prevent a vehicle from entering a track for which it exceeds the maximum permissible axle load for its allowed speed.*

Diese Prüfbedingung impliziert, dass es im zugrundeliegenden Datenmodell Informationen sowohl zur Achslast der Strecke als auch zur Achslast des Fahrzeugs gibt. Diese Daten müssen aus einer sicheren Quelle stammen. Zur Sicherstellung der Verfügbarkeitsanforderung an die Sicherungslogik sollte allerdings auch geregelt werden, was passiert, wenn die Daten nicht vorliegen.

Die Prüfbedingung könnte im Sinne der schlanken Logik auch generischer formuliert werden, indem mehrere Gefährdungen zusammengefasst werden, die sich auf das unzulässige Befahren eines Gleisabschnitts beziehen. Die Achslast wäre dann nur eine von mehreren Eigenschaften bzw. Befahrbarkeitsanforderungen des Gleisabschnitts, deren Einhaltung bei der Fahrerlaubnisausstellung durch die Sicherungslogik geprüft werden würde. Die zu prüfenden Befahrbarkeitsanforderungen könnten für jedes Gleissegement in der sicheren Quelle in einem generischen Datenformat gespeichert werden.

Entscheidend bei der Bewertung, ob die entsprechende identifizierte Sicherheitsanforderung (hier bzgl. der Einhaltung der zulässigen Achslast) in einer generischer formulierten Prüfbedingung aufgehen kann, ist allerdings, dass keine Information über die entsprechende Sicherheitsanforderung verloren geht. Anders als bei Weichen und Gleissperren, die beide stellbare Fahrwegelemente sind und damit bei Verwendung des letztgenannten Begriffs definitiv abgedeckt sind, ist der Begriff „Befahrbarkeitsanforderungen des Gleisabschnitts“ sehr generisch und es ist nicht eindeutig, welche Eigenschaften darunter fallen und zu beachten sind. Daher wird die identifizierte Sicherheitsanforderung auf der Anforderungsebene zunächst als eigene Prüfbedingung in den Funktionskatalog aufgenommen werden. Dadurch wird jedoch nicht ausgeschlossen, dass sie auf der Umsetzungsebene in einem Prüfprozess auf generische Weise abgeprüft wird (siehe Konzept der Restricted Areas in Kapitel 7.3.6).

6.5 Vervollständigung des Funktionskatalogs

Gemäß der in Kapitel 3.6 hergeleiteten Vorgehensweise werden zur Sicherstellung der bestmöglichen Vollständigkeit des Funktionskatalogs und damit des Funktionsumfangs der späteren Sicherungslogik diverse externe Quellen herangezogen, die in Kapitel 6.2.2 hergeleitet wurden und die anerkannten Regeln der Technik wiederspiegeln (Kapitel 6.5.1).

Bei der Analyse der Literatur stellte sich heraus, dass mit den System- und den Bedienfunktionen zwei weitere Gruppen von Funktionen sinnvoll sind, die durch die zunächst durchgeführte systematische Herleitung in Kapitel 6.3 und 6.4 nicht identifiziert wurden. Diesen ist ein eigenes Unterkapitel (Kapitel 6.5.2) gewidmet.

Die vollständige Liste der identifizierten Prüfbedingungen nach der eigenen Herleitung und nachträglichen Ergänzung durch das Benchmark findet sich in Anlage 2.

6.5.1 ...durch Einbeziehung der anerkannten Regeln der Technik

Die etablierte Eisenbahnsicherungstechnik und das dazugehörige betriebliche Regelwerk beinhalten die Erfahrung aus der bald 200-jährigen Entwicklungsgeschichte des Verkehrsträgers Eisenbahn (vgl. Kapitel 2.1). In dieser Zeit hat man immer wieder aus Unfalls- und Störungsereignissen gelernt und die Sicherungstechnik an entscheidender Stelle weiterentwickelt. Dies hat zu einem hochgradig

sicheren Betrieb geführt, allerdings auch zu einer gewissen Schwerfälligkeit in Hinsicht auf die Durchsetzung von Innovationen, die jahrzehntelang den Beweis antreten mussten, dass sie im Sicherheitsniveau mindestens das bisherige, hohe Level erreichen (vgl. Kapitel 3.1.1).

Gemäß ihrer Zielsetzung soll in dieser Arbeit jedoch der Entwurf der neuen Sicherungslogik so erfolgen, wie er unter den Gesichtspunkten der heutigen und zukünftig absehbaren technischen Möglichkeiten optimal wäre. Daher wurde die bisherige Sicherungstechnik, wie bereits in den Kapitel 3.6.2 und 6.2.2 erläutert, bewusst nicht als Ausgangsbasis für die Bestimmung des Funktionskatalogs verwendet. Es wäre jedoch fahrlässig, auf die bestehende Erfahrung gänzlich zu verzichten. Deshalb wird der bisherige Funktionskatalog, bestehend aus den in Kapitel 6.3 bestimmten betrieblichen Funktionen und den in Kapitel 6.4 bestimmten Prüfbedingungen, durch eine Auswertung zentraler Dokumente ergänzt.

Quellen und Vorgehensweise

In Kapitel 6.2.2 wurden sinnvolle Quellen diskutiert. Demnach wird zum einen das ESTW-Lastenheft berücksichtigt, welches einen guten Überblick über die sicherungstechnischen Funktionen der aktuellen Stellwerksgeneration bietet. Weiterhin werden die Systemdefinition des Teilsystems Zentraleinheit des ESTW-NeuPro, auch als DSTW-Kern bezeichnet [DB Netz AG 2017b], das Lastenheft BTSF 3 für ETCS [DB Netz AG 2016] sowie die geschäftlichen Anwendungsfälle für die Leitung und Sicherung des Bahnbetriebs [DB Netz AG 2013] verwendet. Ferner wird auch das betriebliche Regelwerk in Form der Richtlinie 408 der Deutschen Bahn AG untersucht.

Bei jeder dadurch zusätzlich gefundenen Funktion wird geprüft, ob sie unter den grundsätzlichen Prämissen der smartLogic [vgl. Düpmeier 2018] noch einen Nutzen in Hinblick auf die Beschränkung der Gefährdungen haben oder ob sie – soweit erkennbar – nicht mehr erforderlich sind. Um sicherzustellen, dass keine Funktion der bisherigen Sicherungstechnik fälschlicherweise aus dem Funktionsumfang der neuen Sicherungslogik gestrichen wird, können die als nicht mehr erforderlich eingestuften Funktionen zunächst in einen Pool aufgenommen werden, aus dem nach Abschluss der Entwicklung einer ersten Basislogik der smartLogic Testfälle generiert werden können, welche fälschlicherweise gestrichene Funktionen identifizieren.

Erkenntnisse

Die ergänzende Betrachtung der genannten Dokumente brachte vor allem zusätzliche Erkenntnisse in speziellen Anwendungsfällen der Sicherungslogik, wodurch auch spezielle Prüfbedingungen entstehen können. Zum Beispiel muss bei Schneeräumfahrten sichergestellt werden, dass der Schneeflug an den richtigen Stellen gehoben und gesenkt wird. Ferner müssen Trittstufen manchmal ausgefahren werden und manchmal dürfen sie es nicht. Auch die Wirbelstrombremse muss an bestimmten Orten eingesetzt werden bzw. darf nicht eingesetzt werden.

Weiterhin konnten einige technische Aspekte nachträglich identifiziert werden. So erlaubt das betriebliche Regelwerk prinzipiell überlappende Durchrutschwege und damit auch das potenzielle Auffahren von stumpf befahrenen Weichen. Das ESTW-Lastenheft schränkt dies allerdings auf Weichen ohne bewegliche Herzstückspitzen ein [DB Netz AG 2001, S. 14]. Weitere nachträglich identifizierte Prüfbedingungen beziehen sich auf spezielle Fälle, in denen der Stromabnehmer gehoben oder gesenkt werden muss.

Das Lastenheft enthält auch verschiedene Regeln, wie Signalbegriffe aufeinanderfolgen dürfen. Hintergrund ist, dass der Tf nicht durch widersprüchliche Informationen verwirrt werden soll. Wie in Kapitel 4 erläutert, wird bei der smartLogic primär von Führerstandsignalisierung ausgegangen. Auch hierbei besteht die Gefahr, dass der Tf durch mehrere hintereinander eingeblendete widersprüchliche

Informationen verwirrt wird. Allerdings gibt es vielfältigere Möglichkeiten, mögliche Missverständnisse auszuräumen. So kann beispielsweise eine Bestätigung für den neuen Zustand der Fahrerlaubnis eingeholt werden und/oder diese mit einer Textnachricht näher erläutert werden. Auch die Migrationsfähigkeit sollte beachtet werden. Es ist also zu prüfen, ob es in Übergangsbereichen doch noch optische Signale gibt, für die entsprechende Regeln zu beachten sind.

Da Lösungsstrategien an dieser Stelle der Arbeit jedoch noch nicht betrachtet werden sollen, kann für den zuletzt geschilderten Fall widersprüchlicher Informationen für den Tf zunächst eine allgemeinere funktionale Sicherheitsanforderung formuliert werden. Demnach muss der Bediener unter Berücksichtigung seiner menschlichen Auffassungsgabe immer die aktuelle Betriebssituation einwandfrei identifizieren können. Die Prüfbedingung, die sich aus dem geschilderten Anwendungsfall hierzu ergibt, kann zum Beispiel wie folgt formuliert werden: *In case of human interaction, prevent message sequences that might be misinterpreted due to human perception*.

Ein weiteres Beispiel sind Funktionsanforderungen an die Sicherungslogik, die sich aus Wettereinflüssen ergeben. Hiervon gibt es im betrieblichen Regelwerk zahlreiche Beispiele, wie Einschränkungen bei Wind oder Schnee und Eis. Das betriebliche Regelwerk gibt in solchen Fällen bestimmte Höchstgeschwindigkeiten vor. Auch hier kann zunächst verallgemeinert werden. Gemeinsam haben die Wetterregeln, dass zunächst ein Zustand definiert werden muss (durch einen menschlichen Bediener oder einen automatischen Sensor), in Folge dessen festgelegte Konsequenzen geprüft werden. Es wird angenommen, dass dieser Impuls in jedem Fall von einem externen System kommt (egal, ob die Ursprungsquelle der menschliche Bediener oder ein automatischer Sensor ist). Zur Erfüllung der Anforderungen muss es demnach möglich sein, für definierte Bereiche der Infrastruktur definierte Einschränkungen der Fahrerlaubnis festzulegen, die durch das Ansprechen einer entsprechenden Schnittstelle aktiviert bzw. deaktiviert und für den Zeitraum ihrer Gültigkeit von der Sicherungslogik überwacht werden.

Eine solche verallgemeinerte Anforderung kann auch genutzt werden, um Funktionsanforderungen im Falle von Rückfallebenen abzudecken. Mit solchen Funktionsanforderungen beschäftigen sich viele Regelungen des betrieblichen Regelwerks, die beispielsweise niedrige Geschwindigkeiten bei bestimmten technischen Defekten vorschreiben. Um der Entwicklung der neuen Sicherungslogik nicht vorzugreifen, werden die einzelnen Rückfallebenen hier allerdings nicht einzeln erfasst. Die Liste aus dem betrieblichen Regelwerk kann für die zukünftige Systemumgebung auch nicht als vollständig angesehen werden, da sie sich auf die aktuelle Systemumgebung bezieht, bei der zahlreiche Änderungen anstehen (vgl. das 4. Hauptkapitel). Zudem wurde in Kapitel 3.3 abgegrenzt, dass Rückfallebenen in dieser Arbeit nicht im Detail betrachtet werden. Bei der Logik-Entwicklung erfolgt daher nur eine kurze grundlegende Analyse des Themas Einbindung von Rückfallebenen in die smartLogic (siehe Kapitel 8.3.6). Die Anforderungen aus den Rückfallebenen bleiben allerdings im Reserve-Pool, um bei dieser Betrachtung zur Sicherung der Vollständigkeit herangezogen werden zu können.

6.5.2 Systemfunktionen und Bedienfunktionen

Die Literaturrecherche hat auch ergeben, dass neben der vorgeschrieben Protokollierungsfunktion, die in Kapitel 6.2.2 bereits erwähnt wurde, zwei weitere Gruppen an Funktionen noch fehlen, die sich nicht aus systematischen Herleitung ergeben, die in den Kapiteln 6.3 und 6.4 beschrieben wurde. Diese beiden Gruppen sollen im vorliegenden Unterkapitel näher erläutert werden.

Zum einen handelt es sich um die ***Systemfunktionen***. Diese sind erforderlich, damit die Sicherungslogik als Systemkomponente arbeiten kann. Hierzu gehören zum einen allgemeine

Systemfunktionen, die sicherungstechnischen Grundprinzipien folgen, wie z. B. sicherzustellen, dass das System sich immer in einem eindeutigen Zustand befindet, sowie einige spezifische Funktion (Art der Funktion gemäß Kapitel 6.2.2 in Klammern):

- Sicherstellen, dass die Sicherungslogik nur in ordnungsgemäß funktionierendem Zustand sicherheitsrelevante Entscheidungen trifft (Prüfbedingung)
- Selbstüberwachung der eigenen Funktionsweise (aus der oben genannten Prüfbedingung resultierende Subroutine)
- Sicherstellen, dass sich die Sicherungslogik immer in einem eindeutigen Zustand befindet (Anforderung an die Hardwareplattform (Out of Scope) und Prüfbedingung)
- Sicherstellen, dass die Sicherungslogik ihren Zustand korrekt und verständlich (insbesondere bei Benutzerinteraktion) kommuniziert (Prüfbedingung)
- Sicherstellen, dass der Zustand nicht durch äußere Einflüsse verfälscht werden kann (z. B. Stromausfall) (Anforderung an die Hardwareplattform, hier Out of Scope)
- Änderung des Zuschnitts des von der Logik kontrollierten Zuständigkeitsbereiches (Prozessfunktion, vergleiche globale Anforderungen)
- Verknüpfen bzw. Trennen der Sicherungslogik mit/von ihren Umsystemen (Prozessfunktion)
- Sicherstellen, dass alle erforderlichen Umsysteme registriert (angeschlossen) sind (Prüfbedingung)
- Sicherstellen, dass die von Umsystemen gelieferten Informationen verlässlich sind (Prüfbedingung)
- Sicherstellen, der Autorisierung aller angeschlossenen Systeme (Prüfbedingung)
- Sicherstellen, dass Benutzereingaben, bei denen unklar ist, ob sie zu einem unsicheren Systemzustand führen, nur im Rahmen eines hinreichend sicheren Prozesses erfolgen können (Prüfbedingung, Relevanz für die Gestaltung der smartLogic muss noch geprüft werden)

Als weitere spezielle Funktionsgruppe bieten sich die ***Bedienfunktionen*** an. Sie könnten auch den betrieblichen Funktionen zugeordnet werden, da jede Bedienerinteraktion eine Prozessfunktion darstellt und die Bediener keine Schutzfunktionen übernehmen sollen (vgl. Abschnitt Unterscheidung verschiedener Arten von Funktionen in Kapitel 6.2.2). Da es sich um eine recht spezielle Art von Funktionen handelt, erscheint jedoch die Definition einer eigenen Gruppe gerechtfertigt zu sein.

Da die smartLogic als Mittelsystem zwischen dem Traffic Management System (TMS) und den Feldelementen bzw. Fahrzeugen fungiert, soll sie im Regelbetrieb keine Bedienerinteraktion benötigen. Die Bedienfunktionen beziehen sich daher auf spezielle Aufgaben und Rückfallebenen und sind im Einzelfall noch einmal genau auf ihre Notwendigkeit hin zu untersuchen.

Die Bedienfunktionen begründen immer eine zusätzliche Prozessfunktion mit spezifischen Anforderungen. In diesem Prozess sollten die Bedienfunktionen ebenfalls soweit wie möglich gegen Prüfbedingungen geprüft werden. Jedoch ist zu beachten, dass Bedienfunktionen bei einem im Normalzustand automatisch arbeitenden System nur in Zusammenhang mit Systemfunktionen oder der Überbrückung einer automatischen Funktion Sinn ergeben. Die genaue Untersuchung der benötigten Bedienfunktionen erfolgt daher erst nach der Modellierung. Erst zu diesem Zeitpunkt ist klar, welche Prozessfunktionen wirklich umgesetzt werden und an welchen Stellen eine Überbrückung Sinn macht (siehe Kapitel 8.8.2).

Die Bedienfunktionen aktueller Stellwerke wurden zur Vollständigkeitssicherung in den Reserve-Pool übernommen.

6.6 Kategorisierung, Generalisierung und Priorisierung der betrieblichen Funktionen

Wie in der Diskussion der Vorgehensweise zu diesem Hauptkapitel (Kapitel 6.2.2) beschrieben, erfolgt für die Modellierung der Sicherungslogik aus Ressourcengründen eine Priorisierung der Funktionen des identifizierten Funktionskataloges (Kapitel 6.6.3). Um einen nicht auf den Einzelfall bezogenen Maßstab für die Priorisierung zu erarbeiten, ist jedoch zunächst eine Kategorisierung sinnvoll (Kapitel 6.6.1). Da die Priorisierung nicht mit einer Gefährdung der Sicherheit durch nicht geprüfte Prüfbedingungen einhergehen darf, erfolgt die Kategorisierung in Hinblick auf die betrieblichen Funktionen. Um den Funktionskatalog vor der Priorisierung zu vereinfachen erfolgt als weiterer Schritt nach der Kategorisierung eine Generalisierung der Funktionen, bei der ähnliche Funktionen soweit möglich zu einer generischen Funktion zusammengefasst werden (Kapitel 6.6.2).

6.6.1 Kategorisierung

Zur Kategorisierung wurden in der Diskussion in Kapitel 6.2.2 im Abschnitt „Kategorisierung und Generalisierung“ verschiedene Kriterien identifiziert. Demnach grenzen sich von den grundlegenden Funktionen (nachfolgend als **Basisfunktionen** bzw. im genauer ***Basisprüfprozesse*** und ***Basisreaktionsprozesse*** bezeichnet) Funktionen für Rückfallebenen, Übergangsbereiche zu anderen Technologien und Spezialfunktionen ab. Tab. 25 enthält eine Übersicht der daraus und aus den Ergänzungen in Kapitel 6.5.2 gefolgerten Kategorien sowie der Zuordnung der Prozessfunktionen zu den jeweiligen Kategorien, nachfolgend auch **Funktionsgruppen** genannt. Eine Prozessfunktion kann auch mehreren Kategorien zugeordnet sein, z. B. Rückfallebenen und Übergangsbereichen zu anderen Technologien. Die Zuordnung der einzelnen Funktionen zu den Kategorien kann in Anlage 2 nachvollzogen werden.

Aus Gründen der Übersichtlichkeit enthält die Tabelle auch eine Zuordnung der Prüfbedingung zu einer oder mehreren Kategorien. Ausschlaggebend ist, ob die Prüfbedingung immer relevant ist (dies stellt den Normalfall dar, die Prüfbedingung wird dann den Basisprozessen zugeordnet) oder mit hoher Wahrscheinlichkeit nur für die Prozesse und Subroutinen einer oder mehrerer bestimmter Kategorie(n) relevant ist. Es handelt sich an dieser Stelle allerdings um eine subjektive Einschätzung des Autors dieser Arbeit, um einen groben Eindruck von der Menge der jeweiligen Prüfbedingungen zu bekommen. Die Einteilung einer Prüfbedingung in eine der Kategorien enthält daher keine Aussage über die Relevanz der Prüfbedingung für Prozessfunktionen anderer Kategorien. Diese Relevanz muss jeweils getrennt untersucht werden, jeder Prozess muss also gegen alle Prüfbedingungen geprüft werden.

Eine Prüfbedingung kann ebenfalls zu mehreren Kategorien zugeordnet werden, sofern sie nicht ohnehin zu den Basisprüfprozessen zugeordnet wird und damit immer relevant ist. Bei den Prüfbedingungen, die anderen Kategorien zugeordnet sind, handelt es sich also um Prüfbedingungen, die für Prozesse aus dieser Kategorie zusätzlich zu den Basisprüfbedingungen relevant sind.

Tab. 25: Anzahl der Prozessfunktionen und Prüfbedingungen nach Kategorie

Kategorie (Funktionsgruppen)	Prozessfunktionen	Prüfbedingungen
GESAMT	62	175
Basisprüfprozesse	11	133
Basisreaktionsprozesse	28	

Rückfallebenen	4	16
Übergangsbereiche zu anderen Technologien	1	4
Spezialfunktionen (z. B. durch spezielle Fahrzeuge)	2	7
Spezialfunktionen Rangieren (nach bisheriger Definition)	5	9
Systemfunktionen	7	12
Bedienfunktionen	33	5

Zu den *Basisfunktionen* gehören die Funktionen, die für die Durchführung eines minimalen, sinnvollen Bahnbetriebs erforderlich sind und die notwendigen Prüfbedingungen, damit dieser sicher ist. Die Basisfunktionen wurden aufgeteilt in die *Basisprüfprozesse* und die *Basisreaktionsprozesse*. Der Unterschied wurde bereits in Kapitel 6.2.2 beschrieben: Prüfprozesse werden i. d. R. vom TMS aufgrund von betrieblichen Notwendigkeiten angestoßen, während Reaktionsprozesse auf unerwartet eintretende Ereignisse reagieren. Die Basisprüfprozesse umfassen nur einen kleinen Teil der gesamten Prozessfunktionen. Die meisten Prozessfunktionen sind für die Reaktion auf sicherheitskritische Ereignisse erforderlich. Bei den Prüfbedingungen ist hingegen ein großer Teil bereits für die Basisprüfprozesse relevant, während zusätzliche Prozessfunktionen häufig ähnliche Prüfbedingungen erfüllen müssen, wie die Basisprozessfunktionen. Deshalb kommen bei den anderen Kategorien nur wenige neue Prüfbedingungen hinzu. Bei den anderen Funktionsgruppen wurde aufgrund der deutlich geringeren Zahl von Prozessfunktionen in der jeweiligen Kategorie keine zusätzliche Unterscheidung zwischen Prüfprozess und Reaktionsprozess vorgenommen.

Spezialfunktionen sind Funktionen, die zur Erledigung besonderer betrieblicher Aufgaben erforderlich sind, wie z. B. wenn Spezialfahrzeuge verkehren sollen (vgl. die Überlegungen zur Kategorisierung und Priorisierung in Kapitel 6.2.2). Hierzu wurden jedoch keine gesonderten Prozessfunktionen identifiziert, da die Besonderheiten als Parameter in die bereits identifizierten Prozessfunktionen mit einfließen können (vgl. Kapitel 6.3.3). Zum Beispiel stellt die Fahrt eines Schneeräumfahrzeuges oder einer Fahrt mit Lademaßüberschreitung zwar eine besondere Fahrt da, aber es wird trotzdem eine Fahrerlaubnis benötigt, nur eben für ein Fahrzeug mit besonderen Eigenschaften. Es gibt allerdings einige Prüfbedingungen, die sich explizit auf solche besonderen Fahrten beziehen.

Aus den Spezialfunktionen wurde die Kategorie *Rangieren* ausgegliedert. Dieser Kategorie wurden Funktionen zugeordnet, welche nach der klassischen Einteilung in Zug- und Rangierfahrten nur für reine Rangierprozesse erforderlich sind, beispielsweise die Einfahrt in einen ortsgesteuerten Bereich (betriebliche Funktion). Diese Prozesse wurden sämtlich über den Einbezug des Stands der Technik identifiziert. Die klassische Unterscheidung zwischen Zug- und Rangierfahrten konnte allerdings in der heutigen Form nicht aus den globalen Anforderungen hergeleitet werden. Ob und wie der Einbezug verschiedener akzeptierter Sicherheitsniveaus für verschiedene Arten von Fahrten, wie er heute Zugfahrten und Rangierfahrten unterscheidet, bei der smartLogic erfolgt, bleibt eine im Kapitel der Logikentwicklung (vgl. Kapitel 8.3.5) zu beantwortende Frage. Da jedoch in den analysierten Dokumenten strikt zwischen Zug- und Rangierfahrten getrennt wurde, wurde hier zunächst eine eigene Kategorie erstellt. Dies erfolgt auch in Hinsicht auf eine aus Ressourcengründen erforderliche Priorisierung der betrieblichen Funktionen.

Die Kategorie der *Rückfallebenen* umfasst spezielle Funktionen mit denen der Betrieb trotz Betriebshindernissen weitergeführt werden kann. Zu beachten ist, dass nicht jede „Rückfallebene“ eine eigene Prozessfunktion benötigt. Es ist beispielsweise auch denkbar, dass das TMS einfach eine Fahrerlaubnis mit eingeschränkten Parametern wie einer reduzierten Geschwindigkeit im gestörten Bereich prüfen lässt, die dann von der smartLogic zugelassen werden kann. Eine globale Anforderung

zur Zieldimension Robustheit fordert, dass Rückfallebenen möglichst in die Logik integriert werden. Bei der Logik-Entwicklung ist daher zu prüfen, wie dies auf möglichst generischem Weg erfolgen kann.

Die Kategorie „*Übergangsbereiche zu anderen Technologien*“ bezieht sich auf Funktionen, die nur erforderlich sind, wenn Fahrzeugbewegungen den Bereich der Sicherungslogik verlassen und in einen „Alttechnikbereich“ einfahren. Diese Funktionen sind augrund der globalen Anforderung der *Migrationsfähigkeit* wichtig, da nicht davon ausgegangen werden kann, dass ein komplettes Eisenbahnnetz auf einmal von einem Netzwerk aus smartLogic-Sicherungslogiken überwacht wird. Zu dieser Kategorie gehören auch Funktionen, die Fahrzeugbewegungen betreffen, die zwar im Bereich der smartLogic stattfinden, aber nicht durch diese kontrolliert werden. Die Notwendigkeit für solche Funktionen ergibt sich z. B. ebenfalls aus der Anforderung der Migrationsfähigkeit, als auch aufgrund der globalen Anforderung der *modularen Außerbetriebnahme* oder aus der Möglichkeit, dass bei Fahrzeugen die Ausrüstung mit der notwendigen Sicherungstechnik (z. B. ETCS) fehlt oder die Sicherungstechnik nicht (vollständig) funktionstüchtig ist.

Die *Systemfunktionen* beziehen sich auf die interne Funktionsweise der Systemkomponente smartLogic, z. B. bei der Verknüpfung mit Umsystemen. Die *Bedienfunktionen* sind spezielle Funktionen für die Interaktion mit den menschlichen Bedienern des Systems. Vergleiche zu den beiden letztgenannten Gruppen die Definitionen in Kapitel 6.5.2.

6.6.2 Generalisierung

Durch die Kategorisierung können ähnliche Prüfbedingung nebeneinander dargestellt werden. Dies erleichtert die folgende Prüfung, ob Funktionen zur Reduzierung des Funktionskatalogs im Sinne einer Logik noch generischer formuliert und damit zusammengefasst werden können. Die generische Formulierung kann zudem zu einer größeren Flexibilität führen. Die Grenzen der generischen Formulierung werden jedoch durch die Eindeutigkeit der Formulierung vorgegeben (vgl. Kapitel 6.2.2, Abschnitt „Kategorisierung und Generalisierung“). Demnach muss insbesondere bei Prüfbedingungen darauf geachtet werden, dass durch eine generischere Formulierung keine Information verloren geht, die zu einer unvollständigen Prüfung der zugrundeliegenden funktionalen Sicherheitsanforderung führt.

Da bereits bei der initialen Formulierung der Prüfbedingungen auf eine generische Formulierung geachtet wurde, beschränken sich die Änderungen in diesem Arbeitsschritt auf wenige Fälle. Näherer Diskussion bedürfen insbesondere die auf die Rückfallebene bezogenen Prüfbedingungen. Die betroffenen Prüfbedingungen wurden daher zunächst als gesonderte Prüfbedingungen bestehen gelassen, so dass die Diskussion im Rahmen der Logikentwicklung zusammen mit dem Konzept für Rückfallebenen erfolgen kann (siehe Kapitel 8.3.6). Weitere Änderung am Funktionskatalog in Hinsicht auf die Generalisierung wurden nachträglich in Folge der Verhaltensmodellierung der Logik (Kapitel 8) in einem iterativen Prozess vorgenommen.

6.6.3 Priorisierung

Im letzten Arbeitsschritt erfolgt die Priorisierung, die aufgrund der äußeren Umstände dieser Arbeit und der damit verbundenen, begrenzten Zeitressourcen für deren Erstellung notwendig ist (vgl. Kapitel 3.3). Eine Priorisierung kann dabei, wie bereits in der Einleitung zu diesem Kapitel gefolgert, nur anhand der betrieblichen Funktionen erfolgen. Die Prüfbedingungen müssen dagegen prinzipiell immer erfüllt werden, auch wenn sie in Tab. 25 aus Übersichtsgründen ebenfalls den Kategorien

zugeordnet wurden. Zwar ist nicht jede Prüfbedingung für jede Prozessfunktion oder Subroutine relevant; ob eine Prüfbedingung relevant ist, muss jedoch für alle Prüfbedingungen geprüft werden.

Die Priorisierung ermöglicht es auch, die Sicherungslogik in einem agilen Prozess zu entwickeln. Es wird dabei nicht gleich zu Beginn ein maximaler Funktionsumfang in die smartLogic integriert, sondern zunächst eine Basislogik geschaffen, welche die Kernprozesse einer smarten Sicherungslogik abdeckt und somit einen grundlegenden Bahnbetrieb ermöglicht. Diese Basislogik kann dann anschließend mit weiteren identifizierten betrieblichen Funktionen schrittweise erweitertet werden, um auch speziellere sicherungstechnische Fälle abzudecken.

Am höchsten werden diejenigen Funktionen gewichtet, die zum Betrieb der smartLogic unbedingt erforderlich sind. Hierzu gehören die Basisfunktionen sowie die ebenfalls zum Betrieb der smartLogic erforderlichen Systemfunktionen. Weiterhin wird auch die durch eine eigene globale Anforderung geforderte und im digitalen Zeitalter leicht umsetzbare Protokollfunktion priorisiert. Die Protokollfunktion ist insbesondere auch für Diagnosezwecke und den weiteren Erkenntnisgewinn über den potenziellen Nutzen der smartLogic erforderlich. Die Funktionen dieser drei Gruppen stellen die **Kernprozessfunktionen** dar. Zur Erweiterung der Logik können dann schrittweise die Rückfallebenen, die Übergangsbereiche, die Rangierfunktionen und die allgemeinen Spezialfunktionen herangezogen werden. Die Bedienfunktionen rücken im Zuge der Betrachtung der Rückfallebenen mit in den Fokus.

Über die genaue Reihenfolge, in der die letztgenannten Gruppen zur Erweiterung der zu entwickelnden Sicherungslogik herangezogen werden, muss an dieser Stelle aus Sicht des Autors keine Entscheidung getroffen werden. Die Reihenfolge kann bei der Logikentwicklung auch im Einzelfall nach aktuellen Erfordernissen, zum Beispiel aus angedachten Praxisentwicklungen oder gewünschten weiterführenden Forschungsthemen in einem agilen Verfahren erfolgen.

6.7 finales Ergebnis

Der vollständige aus der Funktionsanalyse entstandene Funktionskatalog findet sich in Anlage 2.

Durch das beschriebene Verfahren konnten insgesamt 277 Funktionen für den Funktionskatalog der Sicherungslogik hergeleitet werden. Im Zuge der Klassifizierung und Priorisierung wurden daraus 11 Basisprüfprozesse und 28 Reaktionsprozesse zuzüglich 5 Systemfunktionen und der Protokollierungsfunktion identifiziert, die für eine erste grundlegende Sicherungslogik erforderlich sind. Diese bilden die Kernprozessfunktionen, die in Tab. 26 mit deutscher Funktionsbeschreibung aufgelistet sind. Die Prüfbedingungen wurden zunächst auf 106 eingegrenzt.

Die Anzahl der Einträge in Tab. 26 kann sich von der Anzahl der Prozessfunktionen, die in Tab. 25 der jeweiligen Kategorie zugeordnet sind, unterscheiden. Hintergrund ist, dass einige Funktionen aus Übersichtlichkeitsgründen in Tab. 26 textuell zusammengefasst wurden, die im Funktionskatalog einzeln erfasst sind (z. B. „Fahrzeug(e) auf- oder ausgleisen“).

Tab. 26: Übersicht der Kernprozessfunktionen

Typ	ID	Funktion	Gruppe
Basisprüfprozesse	F-E002	Registrierungsanfrage eines Fahrzeugs bearbeiten	Objekt-management
	F-E009	Stakeholder-Listen aktualisieren	

	F-E898, F-E899, F-E140	Infrastruktur-Einschränkung eingeben oder aktualisieren (z. B. Sperre eines Gleises, Eingabe oder Löschung einer LA), Veränderung globaler Parameter	
	F-E040, F-E257	Status eines Fahrwegelements oder externen Systems (Stakeholder-System) verändern (z. B. Stellanforderung)	Stell-anforderung
	F-E051	Fahrerlaubnis erteilen	Fahrerlaubnis (MA)
	F-E059	bereits ausgestellte Fahrerlaubnis aktualisieren	
	F-E091	Zug teilen (auch einzelne Fahrzeuge abkuppeln)	
	F-E092	Zug vereinigen (auch einzelne Fahrzeuge ankuppeln)	
Basis-reaktionsprozesse	F-E052	Nothalt wird von extern (außerhalb der Sicherungslogik) angeordnet	Nothalt
	F-E258, F-E741	angeschlossenes externes System (Stakeholder-System) sendet eine Information (z. B. Meldung eines Wetterwertes durch einen Wettersensor)	Stakeholder-Systeme
	F-E259	angeschlossenes externes System sendet einen neuen Zustand (z. B. Verlassen der Betriebsbereitschaft)	
	F-E745b	angeschlossenes externes System sendet Fehlermeldung	
	F-E107, F-E006	Status eines stellbaren Fahrwegelements ändert sich (z. B. Veränderung der Ist-Lage einer Weiche)	stellbare Fahrweg-elemente
	F-E108, F-E006	Zustand eines stellbaren Fahrwegelements ändert sich (z. B. Verlassen der Betriebsbereitschaft)	
	F-E745c	stellbares Fahrwegelement sendet Fehlermeldung	
	F-E003a, (F E074)	Registrierungsupdate von Fahrzeugen verarbeiten (An- und Abmeldung)	Fahrzeug
	F-E007, (F-E112a, F-E242)	Fahrzeugposition aktualisieren	
	F-E008	Fahrzeugdaten aktualisieren	
	F-E225	Fahrzeug überschreitet Fahrerlaubnis / verlässt zugewiesenen Infrastrukturbereich	
	F-E226	Schutzbereich eines Fahrzeugs wird verletzt	
	F-E132	Fahrzeug sendet Fehlermeldung	
	F-E700	Gleis besetzt / nicht befahrbar (auch z. B. am Bahnübergang)	spezifische Ereignis-

	F-E701	Fehler in Zusammenhang mit dem Bahnstrom (z. B. an Stromabnehmer, Oberleitung)	meldungen (können aus verschiedenen Quellen stammen)
	F-E702	Feuer	
	F-E709	unerwartete Zugtrennung	
	F-E715, F-E716	Zugspitzensignal unkorrekt	
	F-E717	Zugschlusssignal unkorrekt	
	F-E718	offene Tür	
	F-E719	ungesicherte Ladung	
	F-E132b, F-E720	Fahrzeugschaden (z. B. Heißläufer)	
	F-E727	Infrastrukturgefährdung (z. B. Erdbeben, Erdrutsch, Schienenbruch, ...)	
	F-E799	Ereignismeldung aufheben	
Systemfunktionen	F-E801, F-E802	Verbindung mit einem externen System herstellen oder trennen	
	F-E806a	Zuständigkeitsbereich der Logik verändern	
	F-E806b	Kontrollbereiche verändern	
	F-E807	hinterlegte Infrastruktur aktualisieren	
	F-E820, F-E821	Automatikbetrieb ein- oder ausschalten	
Protokollfunktion	F-E900	alle notwendigen Ereignisse protokollieren	

Für spätere Erweiterungen kann auf weitere Funktionen aus der Menge möglicher Funktionen und Funktionsbedingungen zurückgegriffen werden, die gemäß der Systematik in Kapitel 6.6 in andere Kategorien eingeteilt wurden.

6.8 Ergebnisdiskussion

Durch das mehrstufige, systematische Vorgehen wurde ein umfangreicher Funktionskatalog für die zu entwickelnde Sicherungslogik hergeleitet. Indem die abzuprüfenden Prüfbedingungen primär aus dem in der eigenständigen Gefährdungsanalyse neu bestimmten Gefährdungskatalog für den Bahnbetrieb hergeleitet wurden, bleibt der Funktionsumfang der Sicherungslogik nicht auf die sicherungstechnischen Funktionalitäten bisheriger Stellwerke begrenzt.

Der Rückgriff auf bestehende Dokumente im zweiten Schritt sichert zwar zum einen die Vollständigkeit des Funktionsumfangs auf geeignete Weise ab, birgt allerdings zum anderen auch die Gefahr einer zu umfangreichen Sicherungslogik. Hierbei sind aus Sicht des Autors zwei Sachverhalte diskussionswürdig.

- Zum einen besteht die Gefahr, dass durch eine zu umfangreiche Sicherungslogik deren Komplexität unüberschaubar zunimmt und somit zu komplexeren Genehmigungsverfahren führt (vgl. Kapitel 3.5). Hierzu wurde als Lösungsstrategie auf die Ausgliederung nicht sicherheitsrelevanter (Teile von) Prozessfunktionen und eine möglichst generische Formulierung der verbleibenden Funktionen gesetzt. Jedoch ist dies nur auf subjektiver Ebene erfolgt. Um die Kernanforderung der sicheren Logik

durch nicht eindeutig formulierte Funktionen nicht zu gefährden, wurde dabei eher konservativ vorgegangen und im Zweifelsfall lieber eine Funktion mehr als weniger belassen. Weiteres Potenzial zur generischeren Formulierung ist daher wahrscheinlich vorhanden, konnte aber durch die gewählte Vorgehensweise im Rahmen der verfügbaren Zeitressourcen nicht identifiziert werden.

- Zum anderen besteht die Möglichkeit, dass „Altlasten“, im Sinne von Regelungen zur Aufrechterhaltung der Sicherheit bei bestehenden sicherungstechnischen Anlagen, die unter den Bedingungen der smartLogic nicht mehr benötigt werden, unreflektiert in die neue Logik übernommen werden. Eine solche Übernahme von nicht mehr benötigten Regelungen könnte im schlimmsten Fall zu betrieblichen Einschränkungen führen, die nicht erforderlich wären und damit den Grundzielen der Neuentwicklung der Sicherungslogik widersprechen. Diese Gefahr kann auch durch die erfolgte generischere Formulierung der Prüfbedingungen nur bedingt gebannt werden, da die Umsetzungsquote der generischen Formulierung so gut wie nicht objektiv messbar ist. Zur Vermeidung des genannten Problems wurde eine qualitative Prüfung aller in den Funktionskatalog aufgenommener Funktionen auf ihre Sinnhaftigkeit im Kontext der Systemumgebung der neuen Sicherungslogik vorgenommen. Ohne die Sicherungslogik bereits fertig entwickelt zu haben, kann eine solche Prüfung jedoch nur eine erste Indikation für oder gegen eine Aufnahme in den Funktionskatalog geben. Eine endgültige Aussage ist in dieser frühen Entwicklungsphase nicht möglich. Um dem zuletzt geschilderten Problem zu begegnen, wurden aussortierte Funktionen in den Reservepool einsortiert. So kann die vorgenommene Hypothese, dass die aussortieren Funktionen für die neue Sicherungslogik nicht relevant sind, am Ende der Logikentwicklung noch einmal überprüft werden.

Insgesamt kann davon ausgegangen werden, dass durch die gewählte Vorgehensweise ein eher zu umfangreicher als zu knapper Funktionskatalog für die smartLogic bestimmt wurde. Durch die erfolgte Kategorisierung und anschließende Priorisierung kann die Entwicklung der Logik aber aus einer Basislogik heraus schrittweise nach aktuellen Prioritäten erfolgen. Hiermit ist eine agile Arbeitsweise bei der Logik-Entwicklung möglich.

Bei jeder Erweiterung des gewünschten betrieblichen Funktionsumfangs kann die jeweilige Prozessfunktion gegen alle identifizierten Prüfbedingungen geprüft werden. Der Vorteil gegenüber einem Ansatz, bei dem zunächst ein sehr enger Funktionsumfang als Ausgangsbasis der Entwicklung genutzt werden würde, besteht darin, dass mit dem umfangreichen Funktionskatalog mögliche zukünftige Anforderungen beim grundsätzlichen Design der smartLogic bereits mitbedacht werden können. Die Kombination aus agiler Entwicklungsmöglichkeit und ganzheitlich gedachtem Funktionskatalog macht eine spätere reale Einsetzbarkeit der Konzepte der smartLogic aus Sicht des Autors wahrscheinlicher.

6.9 Vergleich mit alternativen Ansätzen

Die Überlegungen zur RCA bzw. zu smartRail 4.0 sind gemäß Kapitel 2.3 von der Konzeption und Aktualität am nächsten an der smartLogic. Im Rahmen der RCA oder von smartRail 4.0 ist dem Autor zwar kein Dokument mit einer vollständig hergeleiteten Anforderungsdokumentation bekannt, in [SBB AG 2020] existiert jedoch ein Arbeitsstand einer Liste mit betrieblichen Funktionen, die

innerhalb des APS umgesetzt werden sollen (vgl. zu smartRail 4.0 Kapitel 2.3.1 und zur RCA Kapitel 2.4):

- „Monitor and Control Trafficability of Railway Network"
  - „Request Trafficability or Flank Protection for DPS [Drive Protection System]"
    - „Grant Trafficability Change"
    - „Distribute Trafficability Change"
  - „Provide Update of DPS"
    - „Propagate Trafficability"
- „Monitor and Control track-bound Movement"
  - „Provide Update of track-bound vehicle"
    - „Manage communication session"
    - „Translate TPR [Train Position Report]"
    - „Translate Movable Device Data"
    - „Aggregate track-bound MOB [Movable Object]"
    - „Propagate track-bound MOB"
    - „Translate state of occupancy section"
  - „Request Permission for track-bound Movement"
    - „Grant MP [Movement Permission] for track-bound MOB"
    - „Propagate track-bound MOB"
    - „Distribute MP for track-bound MOB"
    - „Translate MP"
- „Manage Usage Restriction of Railway Network"
  - „Request Creation of Usage Restriction Area [(URA)]"
    - „Grant URA"
    - „Propagate URA"
  - „View usage restriction"
    - „View usage restriction"

Die Liste besteht aus drei Gliederungsebenen:

- Erste Ebene: erforderliche Fähigkeiten („Capability Realizations")
- Zweite Ebene: Schnittstellenszenarien („Interface Scenarios")
- Dritte Ebene: logische Funktionen („Logical Function")

Dabei ähnelt die erste Ebene bzgl. der Gliederungstiefe der rechten Spalte in Tab. 26 und die zweite Gliederungstiefe den Prozessfunktionen. Auf Letzteres deutet auch die Bezeichnung als Schnittstellenszenarien hin, denn auch die Prozessfunktionen werden über Schnittstellen aufgerufen. Die dritte Ebene ähnelt den Subroutinen, da es sich um mehrere Funktionen handelt, die zur Umsetzung eines Schnittstellenszenarios benötigt werden.

Beim Vergleich mit den Ergebnissen der Funktionsanalyse für die smartLogic, die in Tab. 26 zusammengefasst sind, fällt zunächst auf, dass es keine Trennung zwischen Prüfprozessen und Reaktionsprozessen gibt. Dabei ist jedoch zu beachten, dass im Konzept von smartRail 4.0 bzw. der RCA einige Funktionen (z. B. Reaktionen auf unerwartete Ereignisse), die bei der smartLogic als Reaktionsprozesse geführt werden, nicht Teil der Safety Logic, sondern des Safety Managers sind. Aktualisierungen des Status von Fahrwegelementen und der Fahrzeugbewegungen finden sich jedoch in der Funktionsliste von smartRail 4.0.

Die Aufteilung der Funktionen auf der ersten Gliederungsebene weist Parallelen und Unterschiede im Vergleich zur Aufteilung der Prozessfunktionen in Tab. 26 auf. So wird ebenfalls zwischen Fahrwegelementen und Fahrzeugen getrennt. Das Objektmanagement wird auf die Verwaltung von Usage Restriction Areas begrenzt, während in Tab. 26 auch die Fahrzeugregistrierung dazu gezählt wird und mit den „Stakeholder-Listen“ ein eigenes Konzept berücksichtigt wird, welches bei smartRail 4.0 in dieser Form nicht existiert.

Für die Rahmenbedingungen, die für die Neuentwicklung der Sicherungslogik in dieser Arbeit festgelegt wurden, sind derzeit keine weiteren systematisch hergeleiteten Funktionskataloge bekannt, die den Anspruch auf eine weitgehende Vollständigkeit erheben (vgl. Kapitel 2.3). Es existieren zwar generische Funktionskataloge, z. B. bei BOSSE, diese basieren jedoch auf unterschiedlichen Rahmenbedingungen in Bezug auf die technologische Reife der Umsysteme (vgl. Kapitel 2.3.3). Von daher wird eine direkte Gegenüberstellung dieser Funktionskataloge mit dem in diesem Hauptkapitel erarbeiteten Funktionskatalog für die smartLogic als nicht sinnvoll eingeschätzt.

6.10 Zusammenfassung

Im vorliegenden Hauptkapitel wurde in mehreren Schritten ein umfangreicher Funktionskatalog für die in den folgenden Kapiteln zu entwickelnde Sicherungslogik smartLogic entworfen.

Der erste Schritt bestand aus einer systematischen Herleitung der notwendigen Funktionen im Sinne der funktionalen Anforderungen am die smartLogic. Als Ausgangsbasis dienten hierfür zum einen die aus der Zielsetzung hergeleiteten betrieblichen funktionalen Anforderungen (betriebliche Funktionen) und zum anderen die in der Gefährdungsanalyse identifizierten funktionalen Sicherheitsanforderungen (Schutzfunktionen) an die smartLogic. Dabei zeichnete sich ab, dass eine Unterteilung der Funktionen in Prozessfunktionen, Subroutinen und Prüfbedingungen sinnvoll ist. Die Prozessfunktionen lassen sich wiederum in Prüfprozesse und Reaktionsprozesse unterteilen (vgl. Kapitel 6.2.2).

Im zweiten Schritt wurde der Funktionskatalog durch den Einbezug der anerkannten Regeln der Technik vervollständigt. Außerdem erfolgte eine Betrachtung der Notwendigkeit von System- und Bedienfunktionen.

Um eine Priorisierung und eine agile Vorgehensweise bei der Entwicklung der neuen Sicherungslogik smartLogic zu ermöglichen, erfolgte anschließend eine Kategorisierung der identifizierten Funktionen nach verschiedenen Kriterien. Dabei standen die betrieblichen Funktionen in Form der Prozessfunktionen im Fokus, da sie je nach gewünschter Funktionalität der smartLogic im Umfang veränderbar sind. Als Kategorien stellten sich neben den Basisfunktionen, den Systemfunktionen und den Bedienfunktionen die Funktionen für die Rückfallebene, die Übergangsfunktionen und die Spezialfunktionen als zweckmäßig heraus. Aus den Spezialfunktionen wurden noch die Rangierfunktionen als gesonderte Gruppe ausgegliedert. Die Rangierfunktionen stehen als gesonderte Funktionen jedoch unter Vorbehalt, da die bisherige Arbeit eine Einteilung der Eisenbahnfahrzeugbewegungen gemäß der klassischen Zweiteilung zwischen Zug- und Rangierfahrten für die smartLogic nicht stützt (siehe auch Kapitel 8.3.5).

Von den identifizierten Funktionen wurden zunächst die in Tab. 26 aufgeführten Kernprozessfunktionen für die Erstellung der Basislogik priorisiert. Diese bestehen aus den Prozessfunktionen der Kategorien Basisfunktionen, Systemfunktionen und der gesondert identifizierten Protokollierungsfunktion, die sich aus der gesetzlichen Protokollierungspflicht herleitet. Die Basislogik stellt damit den minimalen Funktionsumfang einer Sicherungslogik für eine Durchführung von Bahnbetrieb zur Verfügung.

Der Funktionskatalog, der durch das oben beschriebene Verfahren erstellt wurde, bildet aus Sicht des Autors eine gute Grundlage für die weitere Entwicklung der Sicherungslogik, da er einen umfassenden Überblick über aktuelle und mögliche zukünftig gewünschte Funktionsanforderungen an die Sicherungslogik bietet. Zudem beinhalten die Prüfbedingungen auch Spezialfälle, die bei der Konzeption der Sicherungslogik bereits beachtet werden können. Damit ist eine spätere, weit verbreitete Einsetzbarkeit einer auf Basis dieser Arbeit entwickelten Logik wahrscheinlicher. Durch den umfassenden Blick auf den möglichen Funktionsumfang grenzt sich die Arbeit bewusst von vielen anderen Ansätzen ab, die sich derzeit auf dem Gebiet der Sicherungslogik in der Entwicklung befinden und zunächst nur den Kernbereich der Sicherungslogik betrachten.

7 Datenmodell

Damit die Beschreibung des Verhaltens der smartLogic eindeutig ist, werden für die Verhaltensmodellierung im 8. Hauptkapitel wohldefinierte Begriffe benötigt. Natürlichsprachliche Richtlinien enthalten deshalb üblicherweise ein Glossar, in dem wichtige oder mehrdeutige Begrifflichkeiten erläutert werden. Bei einer formalen Modellierung ist eine eindeutige Definition der Begriffe umso wichtiger. Diese Begriffe werden in der Softwareentwicklung üblicherweise im Rahmen der Strukturmodellierung in einem geeigneten Datenmodell (auch Domänen-Modell) beschrieben (vgl. [Gadatsch 2019, S. 4]). Ein solches Datenmodell soll gemäß der in Kapitel 3.6.6 beschriebenen Vorgehensweise im vorliegenden Hauptkapitel erarbeitet werden.

Wie in Kapitel 3.6.4 festgestellt, können Begriffe, wie z. B. „Belegung“ oder „Fahrweg“, abhängig vom Verhalten der Sicherungslogik unterschiedlich definiert werden. Zum Beispiel kann sich unterscheiden, von wo bis wo sich die Belegung des Gleises durch ein Fahrzeug bzw. einen Fahrzeugverbund genau erstreckt. Die Datenmodellierung ist daher mit der Verhaltensmodellierung eng verknüpft. Die Verhaltensmodellierung und die Strukturmodellierung sollten deshalb im gegenseitigen konzeptuellen Kontext erfolgen, in dem Sinne, dass bei der Verhaltensmodellierung zusätzlich benötigte Begriffe nachträglich ins Datenmodell ergänzt werden oder unklare Begriffe präzisiert werden (vgl. auch Kapitel 3.6.5). Daher sind Vorwärtsverweise auf Hauptkapitel 8 und zwischen den einzelnen Unterkapiteln zur Erläuterung der Notwendigkeit für bestimmte Begriffe in diesem Hauptkapitel nicht zu vermeiden.

Der Aufbau des Kapitels folgt der in Kapitel 1.3 beschriebenen Struktur. Demnach wird zunächst im folgenden Kapitel 7.1 die Zielsetzung des Hauptkapitels hergeleitet und der weitere Aufbau des Kapitels besprochen.

7.1 Ziel und Aufbau des Kapitels

In diesem Kapitel werden Ziel und Aufbau des Hauptkapitels zur Erarbeitung eines Datenmodells für die smartLogic genauer beschrieben.

In der Literatur sind unterschiedliche Verwendungen des Begriffs „Datenmodell“ zu finden. [Simsion 2007] enthält in Kapitel 2 eine Übersicht und Diskussion verschiedener Definitionen. Das Datenmodell für die smartLogic soll gemäß der in Kapitel 3.6.4 erarbeiteten Vorgehensweise die Begriffe für die Formulierung des Verhaltens der Logik definieren und deren Eigenschaften sowie Beziehungen untereinander beschreiben. In dieser Arbeit wird unter Datenmodell deshalb die Beschreibung der logischen (Informations-)Objekte mit ihren Beziehungen und Eigenschaften (Attribute und Funktionen) verstanden, die bei der Modellierung der Sicherungslogik eine Rolle spielen (vgl. [Gadatsch 2017, S. 7]). Dabei handelt es sich um eine vereinfachte Abbildung von realen Strukturen in konzeptuelle Strukturen [Simsion 2007, S. 48]. Das Hauptkapitel könnte daher auch mit der Überschrift „Strukturmodellierung“ versehen werden.

Abb. 45 stellt die gemäß der obigen Definition zum Datenmodell gehörenden Informationen am Beispiel einer Weiche dar und vergleicht sie zur Veranschaulichung mit den Komponenten einer natürlichsprachlichen Beschreibungssprache, wie sie z. B. in einem Glossar verwendet werden könnte. Die zu erläuternden Begriffe sind dabei die Subjekte eines natürlichsprachlichen Erläuterungssatzes. Attribute können durch Adjektive und Funktionen durch Verben ausgedrückt werden. Die Beziehungen entsprechen den Objekten des Satzes.

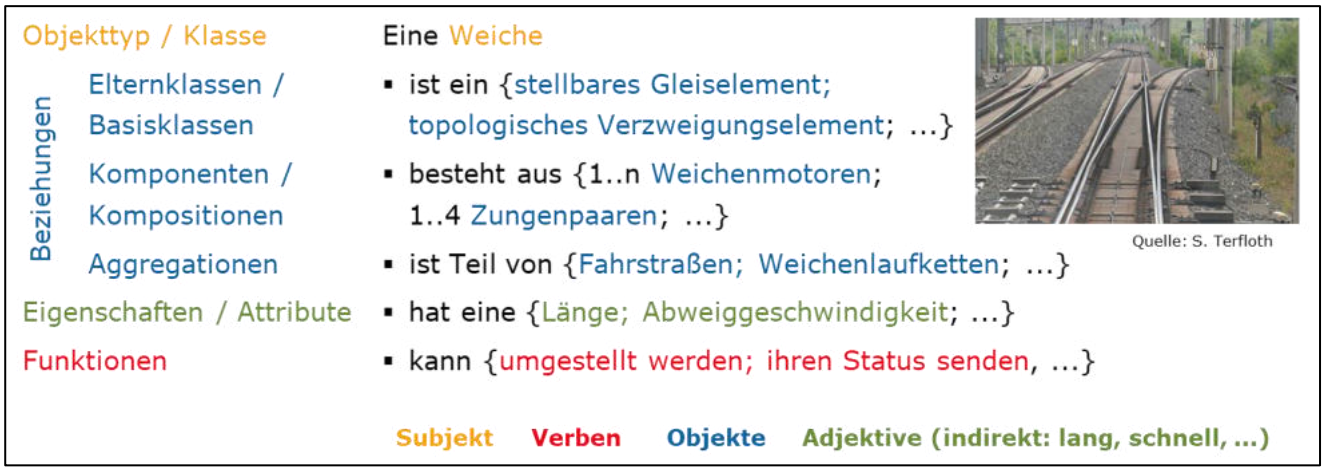


Abb. 45: verschiedene Arten von Information zu einem Objekttyp
[Eigene Darstellung; Bild S. Terfloth/Wikipedia.org]

In Kapitel 3.6.4 wurde unter Beachtung der Erkenntnisse aus Kapitel 2.5 bereits festgestellt, dass die bestehenden Datenmodelle aus dem Bereich der LST nicht alle Anforderungen der smartLogic erfüllen, da sie auf ihre konkreten Anwendungsfälle ausgerichtet sind oder nicht alle erforderlichen Begriffe enthalten. Somit ist ein Datenmodell für die smartLogic unter möglichst weitgehender Verwendung von Standards aus bestehenden Datenmodellen (vgl. globale Anforderungen der Unterstützung von Standardschnittstellen und der Migrationsfähigkeit in Kapitel 3.5) zu entwickeln, das die bei der Verhaltensmodellierung der Logik verwendeten Begriffe (Objekttypen im Modell) und die dahinterstehenden Datenkonstrukte bzw. inhaltlichen Konzepte erläutert. Dazu gehört die Beschreibung der Beziehungen, Eigenschaften (Attribute, Attributtypen zur Vorgabe der zulässigen Wertebereiche und Eigenschaften von Attributtypen (z. B. Anzahl, Verbindlichkeit etc.)) und Funktionen der Objekte (vgl. z. B. Inhalte von UML-Klassendiagrammen als ein Standard-beschreibungsmittel der Strukturmodellierung [OMG 2017]).

Für die Entwicklung des Datenmodells wird in Kapitel 7.2 zunächst eine geeignete Methode und Vorgehensweise erarbeitet. Aufgrund der Komplexität des erforderlichen Datenmodells wird dabei auch untersucht, in welche Teilmodelle das Datenmodell strukturiert werden kann. Anschließend werden die Inhalte der einzelnen Teilmodelle hergeleitet. Das Kapitel schließt wie die anderen inhaltlichen Hauptkapitel mit der Ergebnisdiskussion (Kapitel 7.8), dem am Ende des Hauptkapitels folgendem Vergleich mit anderen Datenmodellen im Bereich der Leit- und Sicherungstechnik bei der Eisenbahn (Kapitel 7.9) und einer Zusammenfassung (Kapitel 7.10).

7.2 Methode und Vorgehensweise

In diesem Kapitel werden aufbauend auf der Zielsetzung des Hauptkapitels, die in Kapitel 7.1 beschrieben wurde, Methode und Vorgehensweise für die Erarbeitung des Datenmodells diskutiert und festgelegt. Das Kapitel folgt dem üblichen wissenschaftlichen Aufbau, wonach zunächst aus den globalen Anforderungen aus Kapitel 3.5 spezifische Anforderungen an die Funktionsanalyse hergeleitet werden (Kapitel 7.2.1). Auf deren Grundlage werden anschließend Methode und Vorgehensweise erarbeitet (Kapitel 7.2.2). Kapitel 7.2.3 fasst die gewählte Methode und Vorgehensweise zusammen.

7.2.1 spezifische Anforderungen

Die spezifischen Anforderungen zur Bestimmung eines geeigneten Datenmodells leiten sich aus der oben beschriebenen Zielstellung für das Datenmodell und den globalen Anforderungen her, die

wiederum in Kapitel 3.5 hergeleitet wurden. Dazu wird für jede globale Anforderung überlegt, welchen Einfluss die Ergebnisse des Kapitels in Hinblick auf die Erfüllung der jeweiligen globalen Anforderung haben. Zusätzlich wurde zur Vervollständigung der spezifischen Anforderungen ein Brainstorming mit Fachkollegen durchgeführt.

Tab. 27 enthält eine Übersicht der globalen Anforderungen und der daraus folgenden spezifischen Anforderungen an die Erstellung des Datenmodells, die anschließend unterhalb der Tabelle näher erläutert werden. Bei nicht relevanten globalen Anforderungen ist dieser Umstand in kursiv vermerkt.

Tab. 27: spezifische Anforderungen an die Erstellung des Datenmodells

Zieldimension	**globale Anforderung**	**spezifische Anforderungen**
Kernanforderung sichere Logik		die Begrifflichkeiten sind eindeutig, (um Fehlinterpretation zu vermeiden, keine Redundanz) alle in der Logik verwendeten Begrifflichkeiten sind vollständig definiert
geringer Planungs- und Genehmigungsaufwand	schlanke Logik	das Datenmodell enthält nur Begriffe, die auch bei der Modellierung der Sicherungslogik benötigt werden
	Beschränkung auf sicherungskritischen Kern	
	generische Logik	Begriffe bezeichnen abstrakte Repräsentationen konkreter technischer Umsetzungen
	Topologieunabhängigkeit	
	flexible Infrastrukturzuordnung	das Datenmodell ermöglicht die Zuordnung von Infrastrukturelementen zur Sicherungslogik
Interoperabilität	Standardschnittstellen	das Datenmodell umfasst die für das Ansprechen der Standardschnittstellen notwendigen Begriffe
geringer Hardwareeinsatz	nur erforderliche Infrastrukturelemente	*keine Relevanz für die Erstellung des Datenmodells festgestellt*
geringer Arbeitskräfteeinsatz	hohe Automatisierung	
	flexible Kontrollbereiche	die Infrastrukturelemente müssen sich logisch zu Kontrollbereichen zusammenfassen lassen
Energieeffizienz	keine unnötigen Bremsvorgänge	diese Anforderungen stellen funktionale Anforderungen an die Logik; für die Realisierung der Funktionen müssen entsprechende Begriffe und Attribute im Datenmodell vorgesehen werden
	Freiraum für Fahrzeug	
hohe Kapazität	Ermöglichung maximaler Geschwindigkeit	
	geringe Latenz	die Datenstrukturen sind schnell durchsuchbar
	minimale Infrastrukturbeanspruchung	diese Anforderungen stellen funktionale Anforderungen an die Logik; für die Realisierung der Funktionen müssen entsprechende Begriffe und Attribute im Datenmodell vorgesehen werden
	frühestmögliche Infrastrukturfreigabe	
hohe Robustheit	Rückfallebenenintegration	

	Regelhandlungsgebot	Informationen und Beanspruchungen können so präzise wie möglich angegeben werden (auf beliebige Teile der Infrastruktur, nur bestimmte Fahrzeuge etc.)
	Freiraum für Fahrzeuge	
	Resilienz	
	modulare Außerbetriebnahme	die Infrastruktur sollte kleinteilig adressiert und mit Attributen versehen werden können
lange Nutzungszeiten	Migrationsfähigkeit	das verwendete Datenmodell sollte mit bestehenden Datenaustauschformaten (möglichst) kompatibel sein
	Zukunftsfähigkeit	das verwendete Datenmodell sollte auch möglicherweise zukünftig vorhandene Informationen abbilden können
[ohne]	Protokollierung	*keine Relevanz für die Erstellung des Datenmodells festgestellt*

Um die *Kernanforderung* der sicheren Logik zu erfüllen, ist es wichtig, dass das Datenmodell eindeutig und vollständig definiert ist. Es muss alle Begriffe umfassen, die in der späteren Modellierung vorkommen, da nicht definierte Begriffe ansonsten bei der Verhaltensmodellierung zu Mehrdeutigkeit führen könnten. Zudem sollten redundante Begriffe vermieden werden, um Widersprüchlichkeit zu vermeiden. Spätere Änderungen bereits definierter Begriffe im Datenmodell können durch ihre Verwendung im Verhaltensmodell zu einem abweichenden Verhalten der Sicherungslogik führen und daher schwerwiegender Konsequenzen haben. Aus diesem Grund sollte das Datenmodell sorgfältig definiert und nachträgliche Änderungen an bereits definierten Begriffen vermieden werden.

Das Datenmodell sollte sich an gängigen Definitionen orientieren (globale Anforderung der *Standardschnittstellen*), jedoch auch zweckmäßig für den Anwendungsfall der smartLogic sein und diese nicht einengen (*generische Logik* sowie die Anforderungen, die unter dem Stichpunkt *funktionale Anforderungen an die Logik* zusammengefasst wurden). Normierte Standards sollten allerdings nur in begründeten Ausnahmefällen verändert werden, um die Kompatibilität mit anderen Systemkomponenten und die Migrationsfähigkeit zu gewährleisten (*Migrationsfähigkeit*). Zukünftige Technologien sollten möglichst bereits berücksichtigt werden (*Zukunftsfähigkeit*).

Auch beim Datenmodell stehen sich wieder die globale Anforderung der *schlanken Logik* und die globalen Anforderungen zu den Zieldimensionen „*hohe Kapazität*“ und „*hohe Robustheit*“ entgegen. Letztere implizieren, dass das Datenmodell so umfangreich sein muss, dass es zum Beispiel möglichst detaillierte Fahrerlaubnisse zulässt und umfangreiche Möglichkeiten bietet, Bedingungen für Rückfallebenen zu definieren. Die Anforderung der schlanken Logik bedingt dagegen, dass das Datenmodell auch nicht unüberschaubar groß werden sollte und vor allem in Hinblick auf die Modellierung, die möglichst generisch erfolgen soll (*generische Logik*), hierfür auch generische Begriffe enthält. Ansonsten gilt aber analog zum Funktionsumfang (vgl. Kapitel 6.2.1), dass auf Vollständigkeit und auf die Erfüllung der funktionalen Anforderungen im Zweifel die Priorität gelegt wird (auf Kosten der Anforderung der schlanken Logik).

Die globalen Anforderungen „*flexible Infrastrukturzuordnung“* und „*flexible Kontrollbereiche*“ stellen spezifische Anforderungen an die Modellierung der Topologie. Demzufolge ist darauf zu achten, dass die Zuordnungen von Stellelementen und Überwachungsbereichen der Logik und der Bediener individuell anpassbar sind.

Weitere spezielle Anforderungen an die Modellierung der Topologie werden u. a. durch die globalen Anforderungen „*modulare Außerbetriebnahme*“, „*keine unnötigen Bremsvorgänge*“, „*Freiraum für Fahrzeuge*“ gestellt. Demnach sollen Infrastrukturattribute wie Beanspruchungen oder Langsamfahrstellen möglichst auf beliebige Teile der Infrastruktur angewendet werden können, d. h. es darf keine Beschränkung auf signifikant große diskrete Abschnitte der Gleise geben. Signifikant groß wäre der Abschnitt, wenn eine feinere Unterteilung desselben zu einer spürbaren Beeinflussung (außerhalb des Unsicherheitsfaktors) des Fahrverhaltens der Fahrzeugbewegungen führen würde. Weiterhin sollte der Wirkungsbereich möglicher Einschränkungen von Fahrerlaubnissen so präzise wie möglich angegeben werden können.

Als für das Datenmodell voraussichtlich nicht relevant wurden zum einen die globale Anforderung eingeordnet, die sich auf den Hardwareeinsatz bezieht (*nur erforderliche Infrastrukturelemente*), da dieser Umfang von der Funktionsweise der Logik (siehe Verhaltensmodellierung) und nicht vom Datenmodell abhängt. Dasselbe gilt auch für die Anforderung nach *hoher Automatisierung*. Die Anforderung der *Protokollierung* ist eine funktionale Anforderung an die Logik, die ebenfalls nicht das Datenmodell verändert. Sie wurde daher ebenfalls als nicht relevant eingestuft.

7.2.2 Erarbeitung der Methode und Vorgehensweise

In diesem Unterkapitel soll auf Basis der in Kapitel 7.2.1 identifizierten spezifischen Anforderungen eine geeignete Methode und Vorgehensweise für die Erstellung des Datenmodells erarbeitet werden. Zunächst soll eine geeignete Notationsform als Syntax des Modells ausgewählt werden. Neben einer Syntax wird auch eine Methode für die Bestimmung der Semantik des Modells benötigt. Dabei ist auf Basis der Anforderung zum einen die Vollständigkeit der Begriffe zu gewährleisten und zum anderen ein geeigneter Zuschnitt der einzelnen Begriffe zu wählen. Damit das Modell übersichtlich bleibt, wird abschließend diskutiert, wie sich das Modell sinnvoll gliedern lässt.

Notationsform

Um das zu erarbeitende Datenmodell eindeutig darstellen zu können, ist Klarheit über die Notationsform (Modellierungsarten) zu gewinnen. Die Vor- und Nachteile verschiedener Modellierungsarten wurden bereits in Kapitel 2.6.2 besprochen. Durch die spezifische Anforderung der eindeutigen Darstellung in Folge der *Kernanforderung der sicheren Logik* kommen nur formale Notationssprachen oder eine formale grafische Modellierungssprache in Frage.

Da smartLogic ein Forschungsprojekt ist, hat das verständliche Aufzeigen neuer Denkansätze einen hohen Stellenwert. Zudem ist es wichtig, dass neue Erkenntnisse auch nachträglich noch einfach in das Modell eingefügt werden können und Veränderungen an der Struktur unproblematisch möglich sind (vgl. Diskussion zur *Kernanforderung der sicheren Logik* in Kapitel 7.2.1). Diese Forderungen erfüllt die grafische Modellierung besser als eine formale Notationssprache. Zudem hat sie sich in der Softwareentwicklung als de facto Standard etabliert (vgl. Kapitel 3.4.3 in [Simsion 2007]). Die Verwendung eines Standards ist von Bedeutung, da die Ergebnisse aus der Arbeit später in Softwareprojekte zur Schaffung realer Sicherungslogiken einfließen sollen. Aus diesem Grund wird in der vorliegenden Arbeit eine grafische Modellierungssprache zur Beschreibung des Datenmodells genutzt.

In Kapitel 2.6.2 wurden verschiedene grafische Modellierunssprachen vorgestellt und die Vor- und Nachteile dieser Modellierungssprachen erläutert. Dabei zeigt sich, dass die UML gegenüber den anderen vorgestellten Modellierungssprachen eine umfassendere Modellierung ermöglicht, da u. a. die Strukturmodellierung mit der Verhaltensmodellierung verknüpft werden kann. Da die smartLogic als

Software modelliert werden soll, ist sie gemäß ihrem Fokus auf Softwaremodellierung außerdem passender als die SysML, die auf die Systementwicklung komplexer verteilter Systeme spezialisiert ist.

Aus diesen Gründen wird in der vorliegenden Arbeit die UML als Modellierungssprache für das Datenmodell der smartLogic verwendet. Von den in Kapitel 2.6.2 vorgestellten Diagrammarten ist das UML-Klassendiagramm für die Beschreibung der verschiedenen Objekttypen, die als Klassen bezeichnet werden, vorgesehen. Daher ist das UML-Klassendiagramm am besten für die Darstellung des zu erarbeitenden Datenmodells geeignet.

Sicherung der Vollständigkeit

Die Vollständigkeit des Datenmodells kann dadurch sichergestellt werden, dass für jeden bei der Verhaltensmodellierung verwendeten Begriff geprüft wird, ob er im Datenmodell enthalten ist. Ist kein geeigneter Begriff im Datenmodell enthalten, muss er ergänzt werden.

Eine nachträgliche Ergänzung eines Begriffs im Datenmodell ist im Gegensatz zur nachträglichen Anpassung von bereits im Datenmodell enthaltenen Begriffen kein Problem, denn der zu ergänzende Begriff kann ja zuvor noch nicht bei der Verhaltensmodellierung verwendet worden sein. Grund ist, dass alle bisher bei der Verhaltensmodellierung verwendeten Begriffe aufgrund der Regeln im vorigen Absatz bereits im Datenmodell enthalten sein müssen.

Zuschnitt der Begriffe

Für die Semantik des Modells wird von den spezifischen Anforderungen in Bezug auf den Zuschnitt der Begriffe eine möglichst generische Beschreibung der einzelnen Begriffe gefordert, die gleichzeitig präzise genug ist, um zum Beispiel auch Prüfbedingungen, deren Erfüllung räumlich begrenzte Einschränkung für einzelne Zugarten erforderlich macht, so abzubilden, dass kein Kapazitätsverlust eintritt. Ein Kapazitätsverlust würde zum Beispiel eintreten, wenn ein größerer Raum als benötigt mit einer Einschränkung versehen werden müsste oder eine solche Einschränkung länger als nötig oder für mehr Fahrzeugbewegungen als nötig gelten würde.

Um die geschilderte Anforderung zu erfüllen, bietet die UML verschiedene Möglichkeiten (vgl. Kapitel 2.6.2). So können Klassen von generischeren Klassen erben, z. B. die Klasse „einfache Weiche“ von der Klasse „Weiche“ und diese wiederum von der Klasse „Stellelement“. „Weiche“ wäre in dem Fall eine Unterklasse der Oberklasse „Stellelement“.

Prinzipiell gibt es auch die Möglichkeit von mehreren Oberklassen zu erben, z. B. wenn Weiche auch noch von „Fahrwegelement“ erben würde. Allerdings wird die Mehrfachvererbung nicht von allen Programmiersprachen unterstützt, z. B. Java, da es ein Mehrdeutigkeitsproblem geben kann, wenn mehrere Oberklassen die gleichen Attribute oder Funktionen enthalten und somit unklar ist, welche davon für die Unterklasse gelten [Ullenboom 2012, Kapitel 5.8.4]. Diese Priorisierung muss also in Konfliktfällen mitgedacht werden.

Für Java existiert ein Hilfskonstrukt über Interfaces, die zwar die Attribute und Funktionen, aber nicht deren Implementierung vorgeben. In verschiedenen Unterklassen könnte also eine in der Oberklasse definierte Funktion unterschiedlich ausgeführt werden [Ullenboom 2012, Kapitel 5.13.5]. Da das Datenmodell die Objekttypen für die smartLogic nur bis zur Ebene der Attribute und grundsätzlichen Funktionen definieren soll, kann das geschilderte Problem der Mehrfachvererbung nicht auftreten. Bei der Definition des Datenmodells muss also nicht auf das Konzept der Mehrfachvererbung verzichtet werden.

Durch generischere Oberklassen bestehen Vokabeln, die auch für generische Prozessschritte bei der Logikentwicklung in Kapitel 8 nutzbar sind. Gleichsam besteht über die konkreten Unterklassen die

Möglichkeit bei Bedarf eine genaue Beschreibung zu verwenden. Das Konstrukt der Vererbung ist auch wichtig, um redundante Informationen zu vermeiden. (Vergleiche auch zu diesem UML-Thema die einschlägige Fachliteratur, die in Kapitel 2.6.2 angegeben ist.)

Um eine möglichst generische Formulierung des Datenmodells sicherzustellen, macht es bei der Modellentwicklung Sinn, sich bei jeder Klasse, die mit einer anderen Klasse gleiche Attribute oder Funktionen hat, die Frage zu stellen, ob eine gemeinsame Oberklasse sinnvoll sein könnte.

Aufteilung in Teilmodelle

Da davon auszugehen ist, dass das Modell sehr umfangreich wird, bietet es sich aus Gründen der Übersichtlichkeit an, das gesamte Modell in mehrere Teilmodelle zu untergliedern. Eine Einteilung sollte dabei so erfolgen, dass auf der einen Seite das jeweilige Teilmodell vom Umfang her noch gut darstellbar ist, auf der anderen Seite aber möglichst wenige Verknüpfungen zu den anderen Teilmodellen enthält, um die Verständlichkeit nicht zu beeinträchtigen.

Mögliche Schnittgrenzen können sich zum Beispiel an den Grenzen orientieren, wie sie auch bei verschiedenen Teilmodellen von RailML (vgl. Kapitel 2.5.3) oder dem RTM (vgl. Kapitel 2.5.2) gezogen werden. Das Datenmodell muss zum einen die physischen Elemente umfassen. Hierbei kann nochmals zwischen den Infrastrukturelementen und Fahrzeugen unterschieden werden (vgl. Teilmodelle bei RailML), die sich über die Infrastruktur bewegen. Weiterhin ist die topologische Beziehung der Elemente zueinander abzubilden. Dieser Bereich hat naturgemäß Verknüpfungen zum physischen Bereich, es handelt sich dennoch um einen anderen Typus der Repräsentation der Infrastruktur als die Abbildung der physischen Infrastrukturelemente (vgl. hierzu den Aufbau des RTM).

Die Verknüpfung von Infrastrukturelementen und Fahrzeugen erfolgt über die Fahrzeugbewegungen, die ein weiteres Teilmodell bilden. Zum Teilmodell der Fahrzeugbewegungen gehören alle Klassen, die in Zusammenhang mit der Bewegung von Eisenbahnfahrzeugen auf der Eisenbahninfrastruktur temporär existieren, wie die Fahrzeugbewegung als solche, aber auch ihre zugehörige Fahrerlaubnis oder ein dazugehöriger Gefahrpunkt.

Auch im Bereich der Infrastruktur und der Topologie kann es temporäre Elemente geben, wie eine Langsamfahrstelle. Deren Anzahl ist allerdings gering und sie sind eng mit den physischen bzw. topologischen Elementen verknüpft, so dass es keinen Sinn macht, für sie eigene Teilmodelle zu erstellen.

Ein weiterer Typ sind Nachrichten, die zwischen den physischen Elementen ausgetauscht werden. Auch sie sollten im Datenmodell definiert werden. Hierbei handelt es sich um Unterschied zu den anderen Teilmodellen jedoch nicht um ein rein internes Teilmodell, sondern die Nachrichten bilden die Schnittstellen nach außen.

Eine alternative, sinnvolle grundsätzliche Möglichkeit die Teilmodelle zuzuschneiden, wurde nicht identifiziert. Deshalb wird das Datenmodell in die beschriebenen vier verknüpften internen Teilmodelle Infrastruktur, Fahrzeug, Fahrzeugbewegung und Topologie (vgl. Abb. 46), sowie das separate Teilmodell Nachrichten gegliedert. Während die vier erstgenannten Teilmodelle an einigen Stellen miteinander verknüpft sind, hat das Nachrichten-Teilmodell vielfältige Anknüpfungspunkte, die aufgrund der Standardschnittstellen teilweise auch von außen vorgegeben werden. Diese Anknüpfungspunkte sind deshalb aus Übersichtlichkeitsgründen nicht dargestellt.

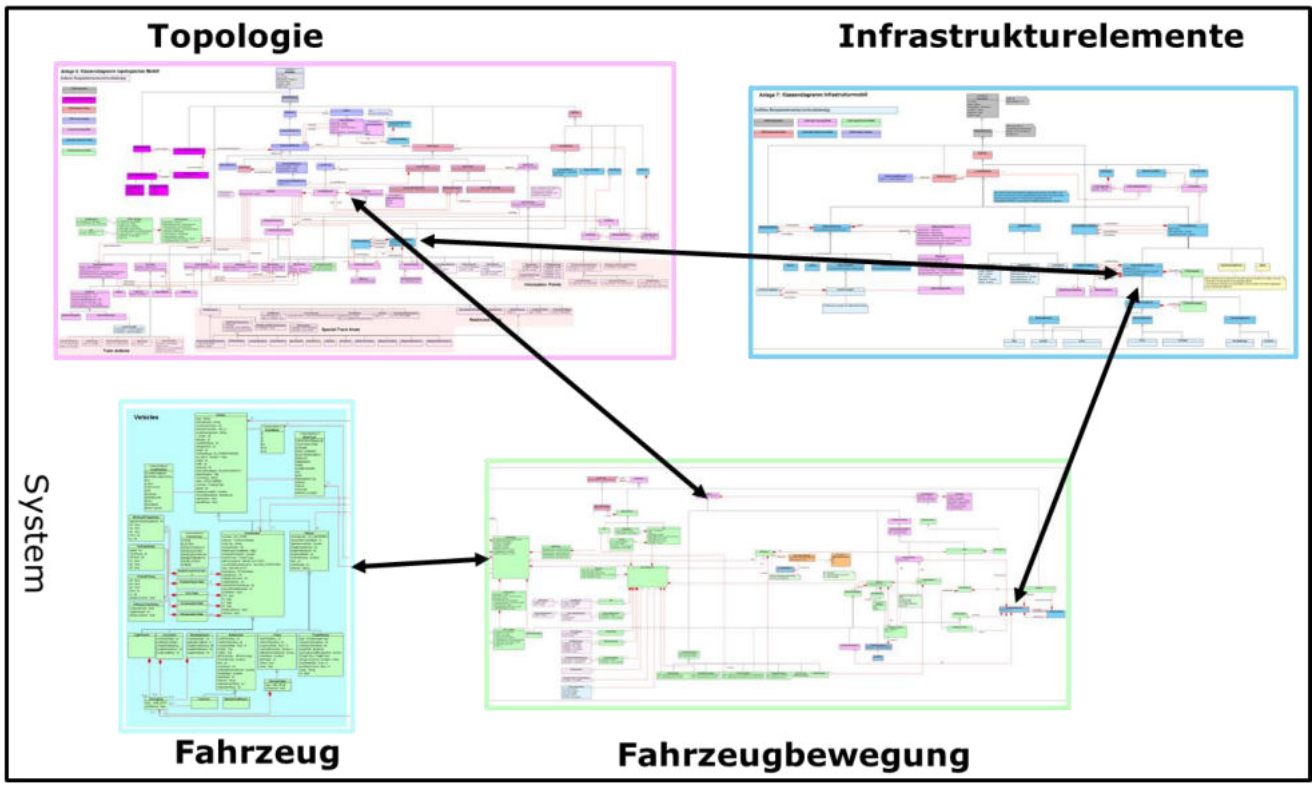


Abb. 46: interne Teilmodelle des Datenmodells
[Eigene Darstellung]

7.2.3 Zusammenfassung der gewählten Methode und Vorgehensweise

Als Datenmodell wird die Beschreibung der Begriffe zur Formulierung des Verhaltens der smartlLogic bezeichnet. Im Sinne der Softwareentwicklung enthält das Datenmodell hierfür die Beschreibung der logischen (Informations-)Objekte mit ihren Beziehungen und Eigenschaften, die bei der Modellierung der Sicherungslogik eine Rolle spielen. Die Beschreibung des Datenmodells erfolgt grafisch mit Hilfe der Unified Modelling Language (UML). Das Modell wird in die fünf Teilbereich Infrastruktur, Fahrzeug, Fahrzeugbewegung, Topologie und Nachrichten gegliedert, für die jeweils ein eigenes UML-Klassendiagramm erstellt wird.

Die Auswahl der benötigten Elemente der einzelnen Teilmodelle erfolgt in Hinblick auf ihre voraussichtliche Verwendung im Rahmen der Verhaltensmodellierung. Ausgangspunkt bilden bestehende Datenmodelle, die in Kapitel 2.5 beschrieben wurde. Existierende Standards werden beibehalten, sofern sie vorhanden sind und nicht zu einer Einschränkung der späteren Funktionalität der smartLogic führen. Es ist insbesondere darauf geachtet, dass beliebige topologische Bereiche festgelegt werden können, denen gemeinsame Eigenschaften zugewiesen werden können.

Sollten Änderungen erforderlich sein, werden – falls möglich – verschiedene denkbare Umsetzungsvarianten identifiziert und in Hinblick auf die in Kapitel 7.2.1 beschriebenen spezifischen Anforderungen und die Anwendung in Bezug auf die Logikentwicklung in Hauptkapitel 8 bewertet. Begriffe sind dabei möglichst generisch zu formulieren, jedoch so, dass es keine Einschränkungen der späteren Funktionalität der smartLogic in Hinblick auf die in Kapitel 3.2 beschriebenen Zieldimensionen, insbesondere Kapazität und Robustheit, gibt. Hierzu wird das Modellierungsprinzip der Vererbung benutzt.

Die Vollständigkeit des Datenmodells kann über die Verhaltensmodellierung sichergestellt werden, da für jeden dort verwendeten Begriff überprüft werden kann, ob er im Datenmodell enthalten ist.

7.3 topologisches Modell

Eine der wichtigsten Fragestellungen bei der Entwicklung des Datenmodells ist, wie die Gleistopologie modelliert wird und wie weitere Objekte daran verortet werden. Das topologische Modell bildet daher gemäß Kapitel 7.2 ein Teilmodell des Datenmodells und wird in diesem Kapitel erarbeitet. Gemäß den in Kapitel 7.2.1 bestimmten Anforderungen, soll dabei möglichst auf bestehende Modelle zurückgegriffen werden. Die in Kapitel 2.5 vorgestellten Infrastrukturdatenmodelle enthalten allesamt Modellierungen der Topologie, die sich jedoch in verschiedenen Punkten unterscheiden und insbesondere in Bezug auf die Verortung von Objekten nicht unter den Prämissen der smartLogic entstanden sind. Zwischen den in diesen Modellen enthaltenen Konzepten muss daher jeweils mit Blick auf die Anforderungen an die smartLogic abgewogen werden. Deswegen erfolgt in diesem Kapitel unter Berücksichtigung der bestehenden Modelle eine schrittweise Herleitung des topologischen Modells der smartLogic.

Ausgangspunkt ist naturgemäß die Modellierung der vorhandenen Gleise, welche die **Gleistopologie** bilden. Hierzu wurden in Kapitel 2.5 verschiedene Modellierungsansätze vorgestellt, von denen in Kapitel 7.3.1 auf Basis der spezifischen Anforderungen an dieses Kapitel eine grundlegende Modellierung ausgewählt werden soll. Die reine Gleistopologie enthält zunächst keine Informationen über die tatsächliche Gleisgeometrie. Ob eine Modellierung der Gleisgeometrie notwendig ist, wird deshalb in Kapitel 7.3.2 geklärt.

Neben den Gleisen existieren weitere Objekte, die topologisch verortet sein müssen. Es kann sich um rein informative, virtuelle Informationen, die sich durch die Eigenschaften der physischen Infrastruktur bedingen und für Zugfahrten beim Passieren des dazugehörigen Informationspunktes von Bedeutung sind, wie z. B. Geschwindigkeitswechsel handeln, aber auch um topologische Informationen zu physischen Objekten[27]. In beiden Fällen handelt es sich abstrakt gesagt um die vereinfachte informationstechnische Repräsentation von Informationen, die sich aus der physischen Realität ergeben. Diese topologischen Objekte können daher als **ortsgebundene Informationen** bezeichnet werden. Kapitel 7.3.3 beschäftigt sich mit der Verortung der ortsgebundenen Informationen.

Nachdem allgemeine Datenkonstrukte für die Abbildung von ortsgebundenen Informationen und deren Verortung an die Infrastruktur hergeleitet wurden, können mögliche Anwendungsgebiete und Eigenschaften der Informationsobjekte bestimmt werden (Kapitel 7.3.4). Dabei zeigt sich, dass bestimmte Abhängigkeiten zwischen verschiedenen Abschnitten der Gleistopologie existieren können (Kapitel 7.3.5). Als besonders relevante Typen von Informationsobjekten werden in Kapitel 7.3.4 Restricted Areas (Kapitel 7.3.6) und Danger Areas (Kapitel 7.3.7) identifiziert.

Im Sinne der Anforderungen, das Datenmodell möglichst generischen und redundanzfrei zu entwickeln, erweist es sich als sinnvoll, gewisse Informationen nicht im Einzelfall als Informationsobjekte direkt an der Gleistopologie zu verorten, sondern für größere Gleisbereiche pauschal vorzugeben (Kapitel 7.3.8).

Ein Gleis ist aus topologischer Sicht zunächst eindimensional. Für bestimmte in Kapitel 6 identifizierte Prüfbedingungen wird jedoch eine mehrdimensionale Betrachtung der Gleistopologie (Fahrzeugbegrenzungslinien/Lichtraumprofil) benötigt. Hiermit beschäftigt sich abschließend Kapitel 7.3.9.

[27] Sonstige Eigenschaften der pyhsischen Objekte sind Teil des Infrastrukturmodells (vgl. Abschnitt „Aufteilung in Teilmodelle“ in Kapitel 7.2.2), dessen Modellierung in Kapitel 7.4 näher erläutert wird.

7.3.1 Modellierung der Gleistopologie

Wie in der Einleitung zu diesem Kapitel festgestellt, bildet die Gleistopologie die Grundlage für das topologische Modell. Eine Modellierung der Gleistopologie erfolgt üblicherweise über ein Knoten-Kanten-Modell, da die Gleistopologie einem Netzwerk aus Knoten und sie verbindenden Kanten gleicht und für Knoten-Kanten-Modelle geeignete, effiziente Algorithmen bekannt sind, um eine Route für eine Fahrzeugbewegung über das Netzwerk zu generieren (vgl. Kapitel 2.5.1).

In Kapitel 2.5.1 wurden mehrere mögliche Arten der Modellierung der Topologie vorgestellt. Das Rail Topo Model wurde dabei von der UIC als Standard festgelegt und sollte deshalb gemäß der in Kapitel 7.2 beschriebenen Anforderung, wonach das Datenmodell möglichst Standards beibehalten soll, zuerst in Betracht gezogen werden. Vorteile der RTM-Modellierung gegenüber der klassischen topologischen Knoten-Kanten-Modellierung wurden in den Kapiteln 2.5.1 und 2.5.2 erläutert.

Insbesondere die Flexibilität durch die klare Trennung der topologischen und der physischen Sichtweise auf das Gleisnetz ist für die spezifische Anforderung, wonach Informationen auf beliebige Teile der Infrastruktur (bzw. Gleistopologie) angewendet werden können sollen, von Vorteil. Als zusätzlicher Nachteil kann jedoch gesehen werden, dass ggf. ein Kompatibilitätsproblem mit bestehenden Daten auftreten könnte. Dies ist vor allem ein Problem, da es momentan noch kaum RTM-kompatible Daten in Deutschland gibt. Da diese Arbeit jedoch zur Entwicklung einer zukünftigen Technologie beiträgt, erscheint es vertretbar das heutige Kompatibilitätsrisiko in Kauf zu nehmen, um dem geltenden Standard zu folgen und somit zukunftsfähig zu bleiben und die Vorteile der RTM-Modells nutzen zu können.

Die Knoten werden im Datenmodell der smartLogic gemäß der RTM-Systematik als „Positioning Net Element“ bezeichnet und stellen Teile des Gleises dar, die in dieser Arbeit als „**Gleissegmente**“[28] (im Datenmodell wurde von der RCA die engl. Bezeichnung Track Edge übernommen, vgl. [ERTMS Users Group & EULYNX 2020a]) bezeichnet werden. Die Befahrbarkeitskanten werden als „Positioned Relation“ bezeichnet. Abb. 47 zeigt die Klasse der Positioned Relation im Datenmodell der smartLogic.

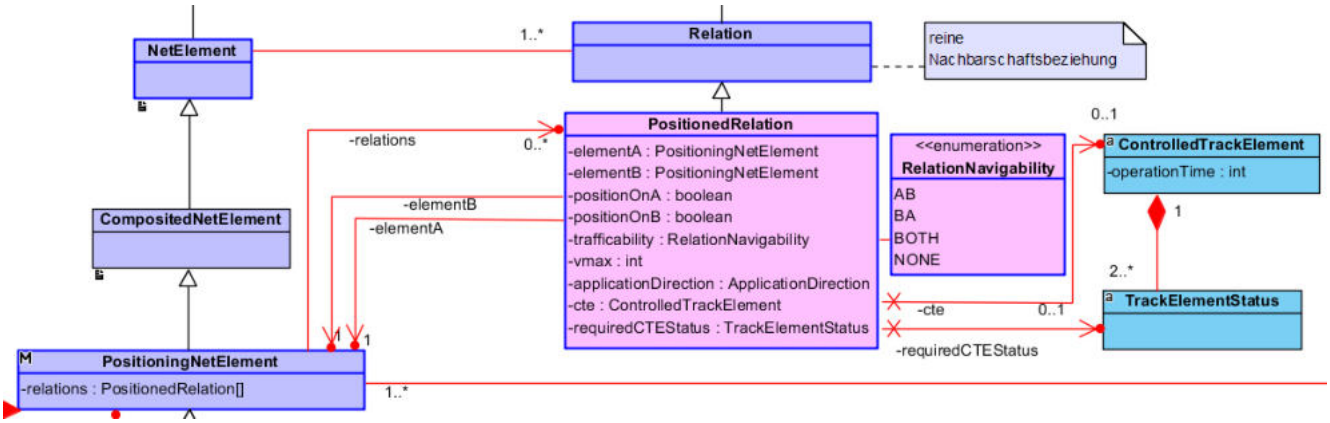


Abb. 47: Positioned Relation im Datenmodell
[Eigene Darstellung, erstellt mit Visual Paradigm]
(pink: topologisches Modell; blau: Infrastrukturdatenmodell; lila: aus dem RTM übernommen)

Ob die topologische Verbindung zweier Gleissegmente, welche mit der Befahrbarkeitskante angegeben wird, auch tatsächlich befahren werden kann, kann vom Status eines Infrastrukturelements abhängen.

[28] Der in der Bahnfachwelt weitverbreitete Begriff „Gleiskante“, der auch der wörtlichen Übersetzung von Track Edge entspricht, wurde hier bewusst vermieden, da es sich im Meta-Modell der RTM um einen Knoten handelt.

Werden die Gleissegmente zum Beispiel über eine Weiche verknüpft, kann die Befahrung nur erfolgen, wenn die Weiche die richtige Lage hat. Deshalb kann im Modell der smartLogic eine Befahrbarkeitskante mit einem stellbaren Fahrwegelement aus dem Infrastruktur-Teilmodell und einem bestimmten Status dieses stellbaren Fahrwegelements (siehe auch Kapitel 7.4.3) verknüpft sein.

Es wäre theoretisch auch möglich, dass dieselbe Verbindung zweier Gleissegmente über mehrere Befahrbarkeitskanten verfügt, die bei verschiedenen Status des verknüpften Infrastrukturelements befahrbar wären. Hierdurch könnten Befahrbarkeitsregeln abhängig vom Status des Infrastrukturelementes modelliert werden. Beispielsweise könnte eine topologische Verbindung mit 60 km/h befahren werden, wenn die zugehörige Weiche in verschlossener und überwachter Rechtslage ist und nur mit 5 km/h, wenn die Weiche in nicht überwachter Rechtslage ist.

7.3.2 Modellierung der Gleisgeometrie

Für die Erstellung des Datenmodells ist zu klären, ob es neben der Gleistopologie auch die Gleisgeometrie umfassen muss.

Gemäß den in Kapitel 6 identifizierten Funktionen, ist für die Zwecke der smartLogic hauptsächlich die Gleistopologie relevant. Die Gleisgeometrie ist vor allem für das Fahrzeug und dessen Berechnung der Bremskurven sowie für das TMS und dessen Berechnung der Fahrzeiten wichtig. Allerdings können z. B. bei ETCS Informationen über die Infrastruktur an das Fahrzeug übergeben werden (vgl. Kapitel 2.2.2). Da sich das Fahrzeug auf diese Daten verlassen können muss, müssen sie vor Weitergabe an das Fahrzeug von der smartLogic überprüft werden. Damit ist eine Modellierung der mit diesem Vorgang verbundenen Daten im Datenmodell erforderlich.

Bei den an das Fahrzeug in der MA übermittelten Daten geht es vor allem um die Neigungsdaten. Hierfür beinhaltet beispielsweise PlanPro eine mögliche Modellierung mittels Höhenpunkten.

Weiterhin ist die Lage von Elementen des konstruktiven Ingenieurbaus wie Tunnel, in denen beispielsweise ein Begegnungsverbot für bestimmte Fahrzeugkombinationen gelten kann, sowie Brücken, auf denen z. B. Einschränkungen bei Wind gelten können, für die Sicherungslogik von Bedeutung. Bei diesen Elementen handelt es sich um physische Objekte, die eine bestimmte Ausdehnung entlang der Gleise haben und – damit sie von Routensuchalgorithmen gefunden werden können – mit den Gleisen verknüpft werden sollten. Hierbei handelt es sich um eine Form von ortsgebundenen Informationen (vgl. die Einleitung zu Kapitel 7.3). Möglichkeiten zur Verortung von ortsgebundenen Informationen werden im nächsten Unterkapitel erläutert.

Die Radien sind dagegen für die Sicherungslogik nicht relevant, da sie sich weder negativ auf das Bremsvermögen auswirken, noch direkt einen Einfluss auf andere sicherheitsrelevante Eigenschaften des Fahrzeugs haben – zumindest sofern davon ausgegangen werden kann, dass ein Geschwindigkeitsprofil für das Gleis existiert, dass die Einschränkungen durch die Radien bereits berücksichtigt. Letzteres wird hier angenommen. Die Radien sind damit rein für Fahrzeitprognosezwecke für das TMS und das Fahrzeug relevant und müssen im Datenmodell der smartLogic nicht zwangsläufig vorhanden sein.

7.3.3 Verortung von ortsgebundenen Informationen

Wie in der Einleitung zu Kapitel 7.3 beschrieben, wird als **ortsgebundene Information** eine Information definiert, die beim Passieren eines Punktes auf der Gleistopologie durch eine Fahrzeugbewegung für diese Fahrzeugbewegung von Bedeutung ist. Das vorliegende Unterkapitel

beschäftigt sich daher mit verschiedenen Möglichkeiten der Modellierung solcher ortsgebundenen Informationen und ihrer genauen Verortung an die Gleistopologie.

Zunächst sollen hierfür einige grundsätzliche Eigenschaften von ortsgebundenen Informationen hergeleitet werden (erster Abschnitt). Anschließend werden verschiedene grundsätzliche Verortungsmöglichkeiten bzw. Koordinatensysteme vorgestellt und diskutiert (zweiter Abschnitt). Darauf aufbauend werden mögliche Ansätze zur Verbindung der ortsgebundenen Informationen mit der Gleistopologie analysiert und ein Ansatz für das topologische Modell der smartLogic ausgewählt (dritter Abschnitt).

Eigenschaften und Arten von ortsgebundenen Informationen

Jedes Gleis kann prinzipiell in beide Richtungen befahren werden.[29] Die ortsgebundene Information kann entweder für nur eine dieser Richtungen gelten oder für beide Richtungen (vgl. z. B. Definition der Wirkrichtung bei ETCS-Datenpunkten). Die Wirkrichtung bezieht sich auf die Richtung des verknüpften Infrastrukturelements (vgl. Kapitel 2.5.1, Abschnitt „Gély et al (2010)“).

Es erscheint weiterhin sinnvoll, zwei Arten von ortsgebundenen Informationen zu unterscheiden:

- ***Feste ortsgebundene Informationen*** wirken immer am gleichen Ort, beispielsweise feste Wechsel der zulässigen Geschwindigkeit aufgrund von Eigenschaften der Gleisgeometrie wie enger Radien.
- ***Dynamische ortsgebundene Informationen*** haben dagegen eine begrenzte Gültigkeit und können prinzipiell an nahezu beliebigen Orten auftreten, z. B. Langsamfahrstellen aufgrund von Baustellen.

Grundsätzliche Möglichkeiten der Verortung und Koordinatensysteme

Für die Verortung von ortsgebundenen Informationen sieht der RTM-Standard verschiedene Verortungsmethoden bzw. Koordinatensysteme vor (vgl. Kapitel 2.5.2).

- Die ***lineare Verortung*** *(„Linear referencing“)* verortet die Objekte entlang eindimensionaler Achsen. Diese Methode ist im Bereich der Eisenbahn weitverbreitet, da sich das Gleis in topologischer Hinsicht ebenfalls als eindimensionale Achse darstellen lässt, (wobei an den Verzweigungspunkten wie Weichen mehrere Achsen verknüpft werden).[30] Für die Verortung kommen verschiedene eindimensionale Achsen in Frage:
  - Verortung auf die ***Gleise***
  - Verortung auf parallel verlaufende Gleise, die zu Strecken zusammengefasst sind

    Die Strecke wird dann über eine separate ***Kilometrierungsachse*** repräsentiert, die normalerweise mittig zwischen den beiden (Haupt-)Gleisen verläuft (vgl.

[29] Die heute in Deutschland noch übliche Definition eines Richtungs- und eines Gegengleises auf zweigleisigen Strecken ist zunächst nicht intuitiv gegeben, sondern wird als Relikt der technischen und organisatorischen Begebenheiten der Vergangenheit betrachtet.

[30] In vielen Modellen, wie beispielsweise PlanPro, werden die einzelnen Gleissegmente daher auch abweichend zur Modellierung der Gleissegmente als *Knoten* des Knoten-Kanten-Modells im RTM als „topologische Kanten“ bezeichnet.

PlanPro). Bei eingleisigen Strecken verläuft die Kilometrierungsachse meist direkt auf der Gleisachse.[31]

- Die Verortung findet auf einem ***Geo-Koordinatensystem*** („Positioning“) statt.
- Es werden ***Bildkoordinaten*** genutzt.

Die Verortung über *Kilometrierungsachsen* hat gegenüber der Verortung über die *Gleise* den Vorteil, dass sie leichter nachvollziehbar ist, da es sehr viele verschiedene Gleissegmente geben kann. Dagegen steht der Nachteil, dass zur Unterscheidung bei mehreren Gleisen ohnehin noch das jeweilige Gleissegement mit verknüpft werden müsste. Entfernungsangaben lassen sich über die Verortung an der Kilometrierungsachse dagegen nicht einfach errechnen, da der parallele Abstand der Gleise nicht berücksichtigt wird und damit in Bögen oder bei Überleitungen zwischen den Gleisen Fehllängen entstehen können.

Im Falle einer Verortung über ein *GEO-Koordinatensystem* wäre der direkte Bezug zum jeweiligen Gleis und damit der Gleisinfrastruktur nur umständlich über Berechnungen zu bestimmen. Da sich aus der Verortung über ein Geo-Koordinatensystem auch kein erkennbarer Vorteil im Falle der smartLogic ergibt, wird von dieser Möglichkeit Abstand genommen.

Die Verortung über *Bildkoordinaten* ist für die Anzeige auf Plänen oder Anzeigegeräten gedacht. Es würde sich im Fall der smartLogic also um ein künstliches Koordinatensystem handeln, welches erst geschaffen und mit einem Referenzpunkt verknüpft werden müsste. Auch dieses Vorgehen hat bei deutlich erhöhtem Aufwand im Vergleich zur linear Verortung keinen erkennbaren Vorteil und scheidet im Falle der smartLogic daher ebenfalls aus.

Für die vorliegende Arbeit erscheint es daher am sinnvollsten, eine Verortung direkt über die Gleise zu realisieren. Die Zusammenfassung zu Strecken mit eigenen Kilometrierungsachsen wird nicht übernommen. Eine ausführlichere Diskussion der Thematik der Strecken und ihrer Bedeutung für die smartLogic findet sich in Kapitel 7.3.8 im Abschnitt „Umgang mit Strecken bzw. Streckenabschnitten und Betriebsstellen“.

Vorstellung verschiedener Ansätze der Verortung am Gleis

Bei der Verortung am Gleis sind ebenfalls verschiedene Ansätze denkbar, die nachfolgend erläutert und diskutiert werden sollen.

1. Bei festen ortsgebundenen Informationen wäre es denkbar, dass sie an ihrem Wirkpunkt als Unterteilung der Knoten des Knoten-Kanten-Modells mit aufgenommen werden und somit – sofern die Information nicht an einem bereits vorhandenen Knoten ergänzt werden kann (beispielsweise eine Geschwindigkeitseinschränkung, die über ein gesamtes Gleissegment gilt – das Gleissegment teilen kann. Abb. 48 verdeutlicht das Prinzip.

[31] Bei mehr als zwei parallelen Gleisen außerhalb von Bahnhöfen gibt es in der Regel mehrere Kilometrierungsachsen, da nach den aktuell geltenden deutschen Eisenbahnregelwerken eine Strecke außerhalb eines Bahnhofs nicht mehr als zwei Gleise haben kann. Diese Logik soll jedoch hier nicht übernommen werden, da sie sich nicht aus den Erkenntnissen der bisherigen Arbeit herleiten lässt.

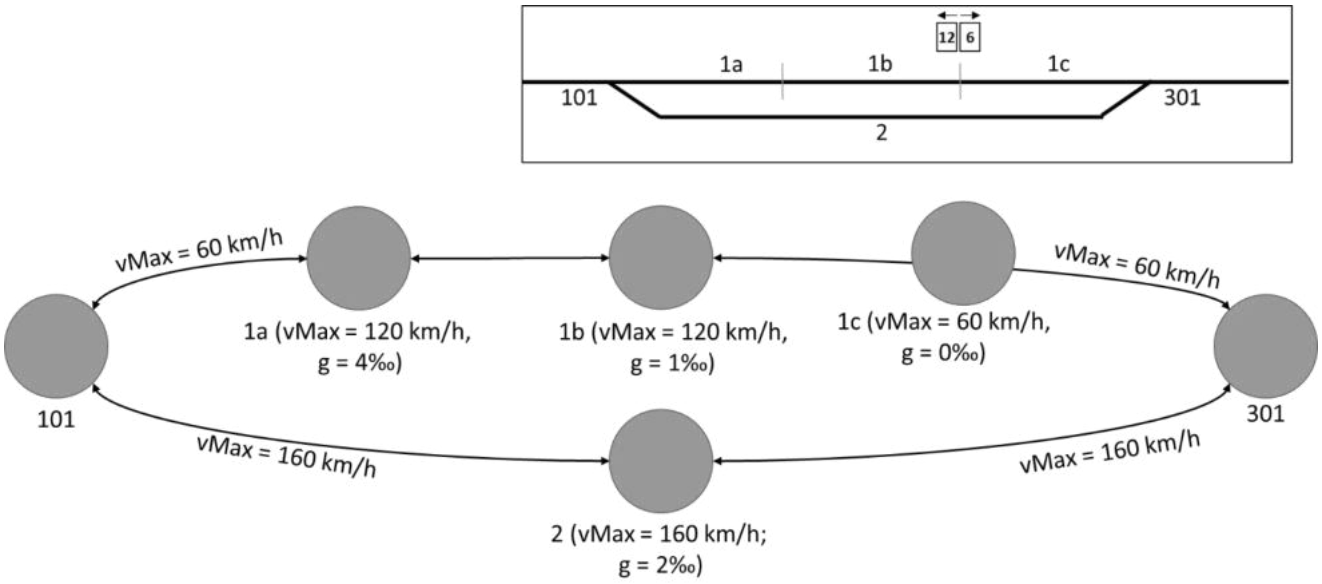


Abb. 48: Einfügen zusätzlicher topologischer Knoten zur Abbildung ortsgebundener Informationen [Eigene Darstellung]

Topologisch stellt das Netz zwei Gleise dar, die links und rechts miteinander verknüpft und in mehrere Segmente unterteilt sind. Es könnte sich z. B. um eine Überholmöglichkeit an einer eingleisigen Strecke handeln. Die Segmente sind jeweils durch einen Knoten abgebildet, der spezifische Eigenschaften des Segments enthält. (Nicht abgebildet ist, dass die Fahrkombination 1a –> 101 -> 2 zwar möglich ist, dazu aber in 101 die Fahrtrichtung gewechselt werden muss. Dies kann jedoch mittels Richtungsattribut an den gerichteten Gleiskanten modelliert werden (vgl. Kapitel 2.5.1, Abschnitt „Gély et al (2010)").

2. Alternativ wäre es auch möglich, die dynamischen ortsgebundenen Informationspunkte an feste ortsgebundene Informationspunkte zu knüpfen, die bereits vorhanden sind. Ebenso könnte durch eine Bündelung jeweils mehrerer ortsgebundener Informationen an einem festen Punkt die Anzahl der Punkte und damit Knotenobjekte reduziert werden. Sollte es in einem längeren Segment keine festen ortsgebundenen Informationspunkte geben, könnten zusätzliche Punkte vorgesehen werden. Theoretisch wäre es auch denkbar, die Information zwar an die ortsgebundene Information zu knüpfen, aber mit einer Zusatzinformation zu versehen, dass die Wirkung der eigentlichen Information erst nach einer bestimmten Distanz beginnt.
3. Informationspunkte müssen allerdings nicht direkt an der Topologie als Knoten im Knoten-Kanten-Modell verortet werden. Es kommen auch andere Möglichkeiten der Verknüpfung von Gleissegmenten und Informationen in Betracht. So wäre es möglich, dass zu jedem Gleissegment die aktuell relevanten ortsgebundenen Informationen verlinkt sind, die dieses Segment berühren (siehe Abb. 49). Anders als bei reinen Informationspunkten, können dann auch ein- oder theoretisch sogar mehrdimensionale ortsgebundene Informationen verknüpft werden. Eine Langsamfahrstelle, welche in beide Fahrrichtungen wirkt, wäre dann nur ein logisches Objekt, anstatt vier Objekte, die vier verschiedene Informationspunkte repräsentieren (aus jeder Fahrrichtung benötigt es am Anfang und am Ende der Langsamfahrstelle einen Wechsel der Geschwindigkeit). Eine ortsgebundene Information kann dann auch mehrere Elemente der Gleistopologie betreffen und entsprechend verlinkt sein.

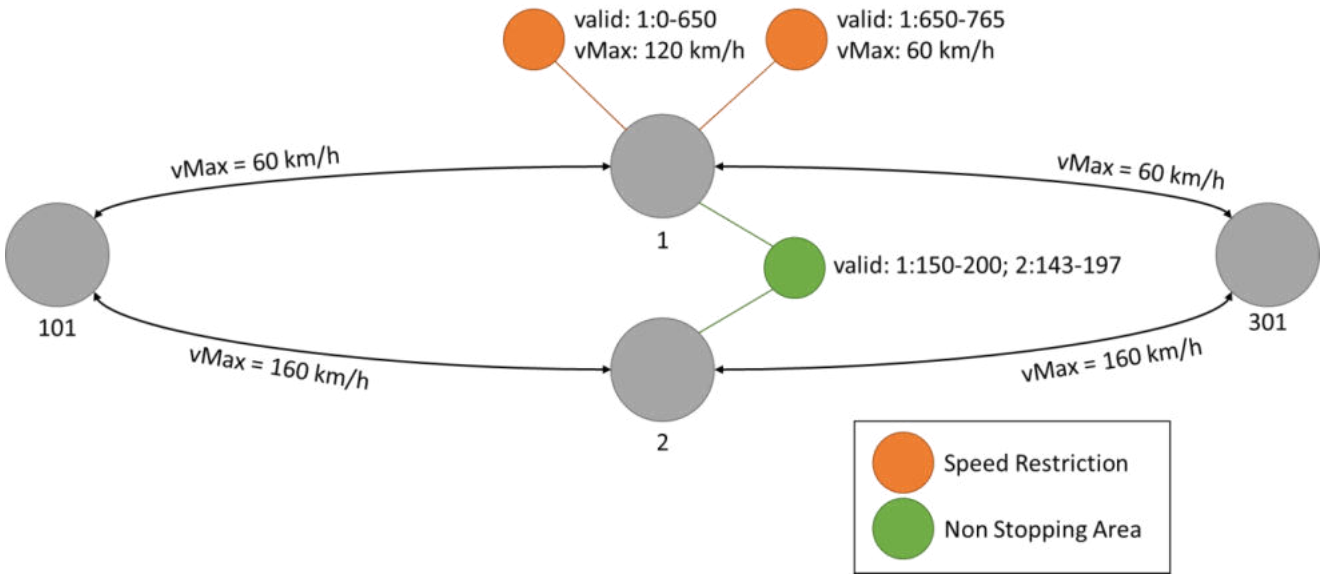


Abb. 49: Beispiel für eine Modellierung ortsgebundener Informationen als eigene Objekte [Eigene Darstellung]
Auf Gleissegment 1 existieren zwei Geschwindigkeitsbereiche mit 120 km/h und 60 km/h. Es wird angenommen, dass die auf Gleissegment 2 geltende Geschwindigkeit von 160 km/h über Standardwerte definiert ist (vgl. Kapitel 7.3.6). Auf beiden Gleissegmenten existiert eine zusammengehörende Non Stopping Area, z. B. aufgrund einer Brücke, die beide Gleise überqueren.

Der erste Ansatz mit einer Unterteilung der Gleissegmente an den Wirkpunkten der ortsgebundenen Informationen hat den Vorteil, dass die Aufnahme der Information bereits durch den zum Abprüfen der Zulässigkeit des beantragten Fahrwegs ohnehin erforderlichen Routenalgorithmus sichergestellt werden kann. Weiterhin lassen sich im Sinne der Anforderung der *schlanken Logik* Informationen, die das gesamte Gleissegment betreffen, direkt über den topologischen Knoten des Gleissegments abbilden.

Es gibt jedoch auch mehrere Nachteile des ersten Ansatzes. Gibt es viele ortsgebundene Informationen, die sich auch an verschiedenen Orten befinden, zerfällt das Netz in eine Vielzahl von einzelnen Gleissegmenten. Dieser Umstand könnte aus Performance-Gründen problematisch werden (Anforderung der *geringen Latenz*), da dann für jedes Gleissegment vielfältige Informationen gespeichert werden müssten, wie die aktuelle Geschwindigkeit oder Neigung. Die dadurch entstehende Redundanz kann zu Uneindeutigkeiten und damit einer Verletzung der *Kernanforderung der sicheren Logik* führen.

Weiterhin ergeben sich Probleme für dynamische ortsgebundene Informationen, da durch die Dynamik nicht klar ist, wo der Knoten angesiedelt sein müsste. Die Gleistopologie müsste also im betreffenden Segment bei einer Änderung des Ortes der dynamischen ortsgebundenen Information jedes Mal neu generiert werden. Dies könnte ebenfalls die Performance einschränken und zu Wartezeiten und damit einer Reduktion der Kapazität führen. Weiterhin könnte es sich negativ auf die parallele Prüfung von Anfragen auswirken, die insbesondere bei großen Zuständigkeitsbereichen der Sicherungslogik anzunehmen sind.

Beim zweiten Ansatz werden die geschilderten Probleme umgangen. Allerdings wäre es im Sinne der Anforderungen zur Zieldimension „*hohe Kapazität*“ von Nachteil, dass die Informationen nicht an ihrem optimalen Wirkpunkt verortet wären. Um auf der sicheren Seite zu sein, müsste die Information bereits in Fahrtrichtung des Zuges vor dem Punkt liegen, an dem die Information benötigt wird. Soll die ortsgebundene Information in beide Richtungen wirken, müsste sie an zwei feste ortsgebundene Informationspunkte geknüpft werden. Weiterhin müsste sichergestellt werden, dass die Punkte so

verteilt sind, dass beim Abprüfen der Route durch die smartLogic die Informationspunkt auch auf jeden Fall berücksichtigt werden. Insbesondere, wenn Fahrzeuge ihre Fahrt beginnen, kann dies zu Problemen führen, für die aber durchaus verschiedene Lösungsmöglichkeiten denkbar sind (z. B. könnte bei Beginn einer Fahrt der letzte zurückliegende Informationspunkt gesucht und dessen Informationen mit ausgewertet werden).

Der dritte Ansatz bietet sehr viel Flexibilität, da die eigentliche Gleistopologie nicht verändert werden müsste, wenn sich an den Informationspunkten etwas verändert. Zudem wird die Modellierung vereinfacht, da ein zusammenhängendes logisches Element (wie die Langsamfahrstelle) auch als ein Objekt modelliert werden kann und nicht in verschiedene einzelne ortsgebundene Informationspunkte aufgeteilt werden muss oder gar redundant in vielen verschiedenen topologischen Objekten wie Gleissegmenten gespeichert wird.

Es erscheint aus den geschilderten Gründen sinnvoll, ortsgebundene Informationen gemäß dem dritten Ansatz als eigene Objekttypen zu modellieren, die mit den Elementen der Gleistopologie verknüpft werden. Reine Punktobjekttypen (0-dimensional) können dabei als „**Spot Location**“ (0-dimensional) (bei der RCA als „***Track Edge Point***“[32] bezeichnet) modelliert werden. Eine Spot Location bezeichnet demnach einen beliebigen Punkt auf der Topologie. Mit der Modellierung linearen und flächigen Elementen, die sich auf einen Gleisabschnitt beziehen, befasst sich der nächste Abschnitt.

Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)

Wie im vorigen Abschnitt erläutert, können ortsgebundene Informationen nicht nur punktuell auftreten, sondern auch eine lineare oder flächige Ausdehnung haben, beispielsweise eine temporäre Langsamfahrstelle oder ein Gefälle. Sie beziehen sich dann auf einen Abschnitt des Gleises, der nachfolgend als **Gleisabschnitt** (bei der RCA engl. „Track Area“, siehe unten) bezeichnet wird. Der vorliegende Abschnitt beschäftigt sich daher mit der Modellierung von Gleisabschnitten.

Abb. 50 stellt verschiedene Arten von Gleisabschnitten angelehnt an die Einteilung der RCA dar.

Abb. 50: Verschiedene Arten von Gleisabschnitten aus der RCA
[Eigene Darstellung, angelehnt an [ERTMS Users Group & EULYNX 2020a]]

Der violette Abschnitt liegt völlig innerhalb eines topologischen Gleissegments zwischen zwei Verzweigungen (RCA: „***Track Edge Section***“). Der blaue Abschnitt erstreckt sich über Verzweigungen der Topologie hinweg, ist aber zusammenhängend und enthält nur eine mögliche Verbindung zwischen seinen Endpunkten (RCA: „***Linear Contiguous Track Area***“). Der grüne Abschnitt bildet einen größeren zusammenhängenden Gleisbereich mit Verzweigungen (RCA: „***Contiguous Track Area***“). Der rote Bereich beinhaltet Abschnitte von zwei Gleissegmenten, die nicht innerhalb des Abschnittsbereichs miteinander verbunden sind (RCA: „**Track Area**“). Beim gelben

[32] Die Bezeichnung wird hier nicht übernommen, da die wörtliche Übersetzung von „Track Edge“ „Gleiskante“ ist, die „Gleiskante“ aber gemäß der RTM-Logik ein Knoten ist und deshalb in dieser Arbeit als Gleissegment bezeichnet wird.

Abschnitt ist nur durch die Angabe der beiden ihn begrenzenden Punkte nicht klar, welche topologischen Elemente er alles beinhaltet. Er könnte sich entweder nur auf eine der beiden möglichen Verläufe beziehen oder sogar beide Verläufe miteinschließen.

Bezieht sich die räumliche Ausdehnung des Gleisabschnitts nur auf ein einzelnes Gleissegment, könnte der Geltungsbereich des Informationsobjektes mit Hilfe von zwei Spot Locations, die Beginn und Ende des Bereichs markieren, verortet werden. Erstreckt sich das Objekt jedoch auf mehrere Gleissegmente müssen weiterführendere Überlegungen angestellt werden, da es mehrere mögliche Fahrwege über die Gleistopologie zwischen den beiden begrenzenden Spot Locations geben könnte oder die beteiligten Gleissegmente möglicherweise gar nicht miteiander verbunden sind (vgl. roter Bereich in Abb. 50).

Die folgenden beiden Lösungsmöglichkeiten konnten identifiziert werden:

1. Eine Lösungsmöglichkeit, die alle oben angesprochenen Fälle abdeckt, wäre es, das Objekt der ortsgebundenen Information mit jedem topologischen Gleissegment zu verknüpfen und dabei jeweils den Bereich mit zwei Spot Locations anzugeben, in dem die ortsgebundene Information auf dem Gleissegment gilt (vgl. auch Abb. 49 im vorigen Abschnitt).
2. Alternativ könnte mit Hilfe der Angabe von Wegweisern (siehe auch Kapitel 7.6.3) eine Route zwischen den beiden Enden der Gültigkeit der ortsgebundenen Information festgelegt werden, so dass der Gültigkeitsbereich eindeutig ist.

Bei der zweiten Lösungsmöglichkeit könnten allerdings nur Gleissegmente miteinbezogen werden, wenn zwischen diesen eine topologische Verbindung besteht, die ununterbrochen zum Gültigkeitsbereich der ortsgebundenen Information gehört (*Linear Contiguous Track Area*). Wenn dies nicht der Fall ist, müssten mehrere Objekte zur Repräsentation der ortsgebundenen Information für jedes der betroffenen Gleissegmente angelegt werden.

Die erste geschilderte Lösungsstrategie erscheint daher einfacher umsetzbar zu sein, da sie das Problem der unverbundenen Gültigkeitsbereiche umgeht, und keine gravierenden Nachteile zu haben scheint. Sie wird daher bevorzugt und ist in Abb. 51 im Klassendiagramm dargestellt

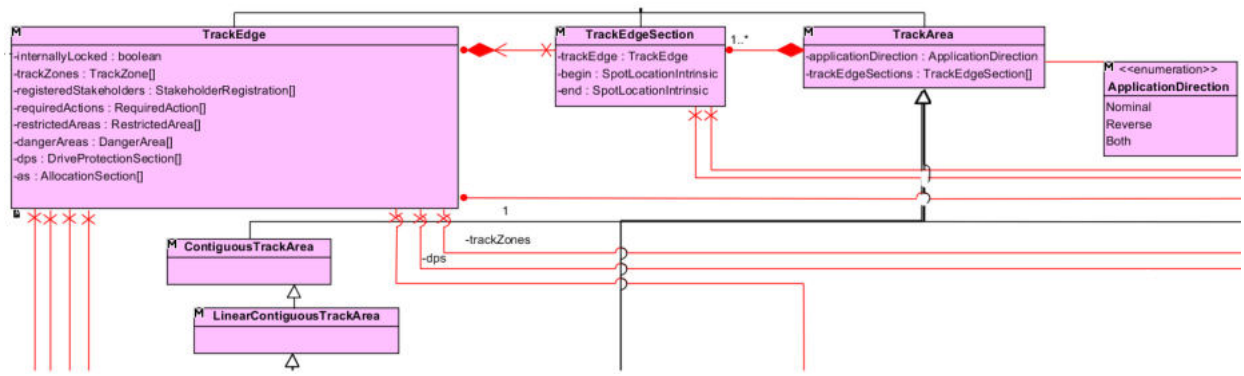


Abb. 51: Gleisabschnitte im Datenmodell
[Eigene Darstellung]

7.3.4 Anwendungsgebiete und Eigenschaften von punktförmigen ortsgebundenen Informationen und Gleisabschnitten

Gleisabschnitte stellen eine sehr generische Betrachtung von ortsgebundenen Informationen dar, die in Hinblick auf die Verhaltensmodellierung schnell unpräzise werden kann. Daher ist es sinnvoll, zu

untersuchen, in welche Typen sich Gleisabschnitte gliedern lassen. Ausgangspunkt für eine solche Untersuchung können potenzielle Anwendungsgebiete von punktförmigen ortsgebundenen Informationen sowie des Konstrukts der ein- oder mehrdimensional gültigen Informationsobjekte in Form von Gleisabschnitten sein. Zur Identifikation der Anwendungsgebiete können die verschiedenen Teilmodelle nacheinander betrachtet und jeweils ein Brainstorming durchgeführt werden. Die Vervollständigung kann dann im Rahmen der Verhaltensmodellierung erfolgen.

Dieses Unterkapitel soll einem Überblick über die verschiedenen Typen von Gleisabschnitten liefern und greift damit zum Teil Erkenntnissen nachfolgender Kapitel vor, auf die mit Vorwärtsverweisen verwiesen wird. Die Vorschau erfolgt an dieser Stelle, da sie sich hier thematisch am besten in die Arbeit einfügt.

Im topologischen Teilmodell können, wie bereits in Kapitel 7.3.2 angesprochen, Eigenschaften der mit der Topologie verwandten und daher in das topologische Teilmodell integrierten Gleisgeometrie als Gleisabschnitte oder punktförmige ortsgebundene Informationen abgebildet werden (z. B. Neigungsabschnitte). Weiterhin können auch Gleissegmente in ihrer Gänze als Gleisabschnitte betrachtet werden. In beiden Fällen handelt es sich um feste ortsgebundene Informationen. Bei Gleissegmenten geht deren Bedeutung als zentrale Elemente der Gleistopologie jedoch über das Bereitstellen von Informationen für sie passierende Fahrzeugbewegungen hinaus, weshalb sie einen Sondertyp bilden.

Auch der Bereich, in dem Fahrzeuge die Fahrzeugbegrenzungslinien auf einem anderen Gleis verletzen (Allocation Sections (AS)) können als Gleisabschnitte betrachtet werden (vgl. Kapitel 2.4.4 und 7.3.9). Sie können jedoch nicht vollständig den festen ortsgebundenen Informationen zugeordnet werden, da insbesondere Allocation Sections auch dynamisch, z. B. durch andere Fahrzeuge mit Lademaßüberschreitung, erzeugt werden können.

Im Infrastrukturmodell wird als weiterer Typus die vom Status eines Infrastrukturelements abhängige Unterbrechung der physischen Befahrbarkeit der Topologie identifiziert, die von der RCA als „Drive Protection Section (DPS)“ bezeichnet wird (vgl. Kapitel 2.4.4 und 7.4.3) und zum Beispiel bei Weichen und Sperrelementen vorkommt. Verallgemeinert können auch weitere Eigenschaften, wie die zulässige Geschwindigkeit, sowie Vorgaben für die Fahrzeugbewegung, wie das Betätigen der Pfeife, durch den Status von Infrastrukturelementen beeinflusst werden. Neben Stellelementen kommen als Quelle hierfür auch externe System in Betracht, welche über festgelegte Schnittstellen dynamische Gleisabschnitte definieren oder modifizieren können (vgl. hierzu das Stakeholder-Registrierungs-Konzept, welches in Kapitel 8.3.3 erläutert wird sowie Kapitel 7.4.7). Der verallgemeinerte Typ von Gleisabschnitten kann als „**Restricted Area**“ (RA) bezeichnet werden. Die RCA bezeichnet diesen Typ von Gleisabschnitten als Usage Restriction Area (URA) (vgl. Kapitel 2.4.4), wobei sie die DPS nicht zu den URA zählt. Mit diesem Typ beschäftigt sich Kapitel 7.3.6 näher.

Das Fahrzeug- und das Fahrzeugbewegungsteilmodell können aufgrund ihrer engen Verzahnung zusammen betrachtet werden. Sie enthalten verschiedene Typen von Gleisabschnitten, deren Position bzw. Ausmaße sich regelmäßig verändern und die somit als **dynamische Gleisabschnitte** bezeichnet werden können, zur Abbildung der Position und des Fahrwegs der Fahrzeugbewegung. Im Einzelnen sind diese Typen die tatsächliche Position des physischen Fahrzeugs (vgl. Kapitel 7.6.1) inkl. definierter Grade an Ortungsungenauigkeit und der für die Fahrzeugbewegung fest reservierte Bereich, in dem auch sein Bremsweg liegen muss (vgl. Kapitel 7.6.2).

Von diesen von der Fahrzeugbewegung bereits fest beanspruchten Raum kann die zukünftige Route abgegrenzt werden, die dem Fahrzeug über eine neue Fahrerlaubnis oder eine Verlängerung bzw. Modifikation der gegenwärtigen Fahrerlaubnis erst noch zugewiesen werden soll (vgl. Kapitel 7.6.3).

Ein weiterer auf die Fahrzeugbewegung bezogener Typ von Gleisabschnitten existiert auch in Zusammenhang mit dem Thema Flankenschutz, mit dem sich Kapitel 8.3.4 näher beschäftigt.

Diese Typen von Gleisabschnitten bilden Beanspruchungen der Infrastruktur ab. Es kann noch weitere Beanspruchungen der Infrastruktur geben, die nicht von Fahrzeugbewegungen ausgehen, sondern z. B. von Instandhaltungstrupps oder von unidentifizierten Objekten. Die beiden letzteren Gruppen werden von der RCA zu den URA gezählt, da sie unmittelbar Einschränkungen für die Nutzung der Gleistopologie definieren. Insbesondere unidentifizierte Objekte unterscheiden sich aber insofern von sonstigen URAs, dass sie sofortige Handlungen erforderlich machen, da nicht klar ist, ob sie kontrolliert werden können. Deshalb erscheint die Definition eines eigenen Typs für Gefahrenzonen („Danger Areas“ (DA)) als Sondertyps der RA / URA gerechtfertigt (siehe Kapitel 7.3.7).

7.3.5 Abhängigkeiten zwischen Gleisabschnitten

Zwischen Gleisabschnitten können Abhängigkeiten bestehen (vgl. z. B. Allocation Section Groups (ASG) zur Modellierung von voneinander abhängigen Lichtraumprofileinschränkungen in Kapitel 2.4.4), die näher betrachtet werden sollten. Hiermit beschäftigt sich dieses Unterkapitel.

Das Konstrukt des Gleisabschnittes kann demnach auf zwei verschiedene Arten genutzt werden, zum einen als **Wirkabschnitt**, der beschreibt, in welchem Bereich der Topologie eine Information wirkt, zum anderen als **Detektionsabschnitt**. Er beschreibt einen Abschnitt, dessen Beanspruchung oder tatsächliche Befahrung durch eine Fahrzeugbewegung eine Aktion auslöst. Z. B. kann die Wirksamkeit der Information eines Wirkabschnitts vom Status eines Detektionsabschnitts abhängen. Im Beispiel der ASG würde jeweils die eine AS Detektionsabschnitt für die andere AS sein, in der die Befahrbarkeitseinschränkung infolge der Lichtraumprofileinschränkung dann gelten würde.

Ein Abschnitt kann auch Wirk- und Detektionsabschnitt für sich selbst zugleich sein. Beide Objekte können auch punktförmig, also „Spot Locations“ sein. Prinzipiell können beliebige Gleisabschnitte als Wirk- und Detektionsabschnitte miteinander verknüpft sein. Ein Wirkabschnitt kann beispielsweise durch mehrere Detektionsabschnitte aktiviert bzw. deaktiviert werden. Ein Detektionsabschnitt kann wiederum auch mehrere Wirkabschnitte beeinflussen. Ein Wirkabschnitt ist nicht auf einen Detektionsabschnitt angewiesen, sondern kann auch immer gültig sein.

Ein Beispiel können Allocation Sections sein, die gegenseitige Abhängigkeiten zwischen Gleisbereichen herstellen, in denen es Fahrzeugbegrenzungslinien-Überlappungen gibt (vgl. Kapitel 7.3.9, 7.4.3 und 7.4.5).

7.3.6 Restricted Area / Usage Restriction Areas

In Kapitel 7.3.4 wurden Restricted Areas (RA) (oder gemäß RCA-Definition „Usage Restriction Areas“ (URA), vgl. Kapitel 2.4.4) als Typus von ortsgebundener Information identifiziert. Die Aufgabe von RAs ist die Bereitstellung von Informationen, die von Fahrzeugbewegungen, die sie passieren, beachtet werden müssen. In der Regel handelt es sich um Einschränkungen der Befahrbarkeit oder sonstige Vorgaben wie an einer definierten Stelle den Stromabnehmer zu senken oder zu heben. Eine RA kann eine Fahrt auch gänzlich unmöglich machen und somit als Sperrung des Gleises wirken.

RAs können sowohl als Gleisabschnitte (z. B. Gleisabschnitt mit temporärer Langsamfahrstelle (Temporary Speed Restriction (TSR))) als auch als Punktobjekte (z. B. Stelle an der ein Pfeiffsignal abgegeben werden muss) auftreten. Diese Unterscheidung ist jedoch für die Praxis von untergeordneter Rolle, da ein Punktobjekt ohnehin eine vereinfachte Form des Gleisabschnitts ist (Gleisabschnitt ohne Ausdehnung).

Im ersten Abschnitt werden mögliche Einschränkungen und Vorgaben für Züge, die über RAs modelliert werden können, hergeleitet. Darauf aufbauend wird im zweiten Abschnitt diskutiert, wie die Einschränkungen bzw. Vorgaben gemäß der Anforderung der präzisen Formulierung von Einschränkungen möglichst genau auf die notwendigen Adressaten zugeschnitten werden können. Im Sinne der gleichen Anforderung soll anschließend im dritten Abschnitt erarbeitet werden, wie die Gültigkeit von RAs von Voraussetzungen abhängig gemacht werden kann. Um zu Verhindern. dass RAs zur Unzeit unter Hervorrufen eines Sicherheitsrisikos gelöscht werden können, wird anschließend im vierten Abschnitt noch darauf eingegangen, wie Voraussetzungen für die Löschung oder Modifikation von RAs modelliert werden können, die nachfolgend als **Löschbedingungen** bezeichnet werden.

Mögliche Einschränkungen und Vorgaben

Als Quelle möglicher Einschränkungen und Vorgaben kann zum einen die durchgeführte Funktionsanalyse in Kapitel 6 dienen, zum anderen der Funktionsumfang von ETCS, mit dessen Nachrichten zahlreiche Einschränkungen und Vorgaben an das Fahrzeug übertragen werden können. Weiterhin enthält [Skowron 2020] eine Liste möglicher URA. Außerdem wurde ein Brainstorming mit Fachkollegen am Institut für Bahnsysteme und Bahntechnik der TU Darmstadt durchgeführt. (Letzteres gilt auch für die Inhalte von Tab. 29 und Tab. 30.)

Tab. 28 enthält die identifizierten, möglichen Einschränkungen bzw. Vorgaben für Fahrzeugbewegungen, die mit RAs abgebildet werden können.

Im Sinne der Zukunftsfestigkeit ist es sinnvoll, dass die Liste möglicher Einschränkungen und Vorgaben jedoch nicht abgeschlossen wird, sondern dynamisch bleibt, also zur Einsatzzeit der jeweiligen Sicherungslogik angepasst werden kann. Die Liste in der Tabelle erhebt daher bewusst nicht den Anspruch auf Vollständigkeit. Überlegungen zu einer möglichen Umsetzung der Anpassbarkeit dieser Liste zur Laufzeit enthält Kapitel 7.7.1 im Abschnitt „Erstellung, Anpassen oder Löschung eines (dynamischen) Gleisabschnitts (RA / URA) (RA Request)“.

Tab. 28: Mögliche über RAs definierte Einschränkungen bzw. Vorgaben

Einschränkung
physische Befahrbarkeitseinschränkung
logische Befahrbarkeitseinschränkung; kann ggf. in bestimmten Fälle dennoch befahren werden (heutige „Sperrfahrt“)
zulässige Geschwindigkeit
Überwachungsmodus (ETCS-Modus)
Level des automatisierten Fahrens
Vorgabe oder Beschränkung fahrzeugseitiger Funktionen wie Pfeifen, Läuten, Trittstufe ausfahren, Wirbelstrombremse nutzen, Schneepflug heben oder senken
Traktionshinweise / Fahrstromhinweise (z. B. Stromabnehmer heben oder senken)
Vorgabe von Informationen für den Tf (z. B. über ETCS-Textnachrichten)

Eingrenzung der Einschränkungen und Vorgaben auf bestimmte Fahrzeuge und Typen von Fahrzeugbewegungen

Die Einschränkungen bzw. Vorgaben können auf bestimmte Fahrzeuge bzw. Typen von Fahrzeugbewegungen eingegrenzt werden, um ihre Anwendung präziser zu machen und unnötige Einschränkungen für vom Sicherheitsproblem nicht betroffene Fahrzeugbewegungen zu vermeiden.

Als Quelle dienen hier die Eigenschaften der Fahrzeuge und Fahrzeugbewegungen aus den jeweiligen Teilmodellen des Datenmodells (Kapitel 7.5 und 7.6). Auch diese Liste kann theoretisch wie die Liste der möglichen Einschränkungen erweitert werden, allerdings nur sofern auch die Fahrzeugobjekte bzw. Fahrzeugbewegungsobjekte die neuen Attribute kennen.

Tab. 29: Mögliche Eingrenzungen der RAs auf bestimmte Fahrzeuge bzw. Arten von Fahrzeugbewegungen

Eingrenzung	**Beispiele / Kommentar**
Art der Fahrzeugbewegung	Güterzug, Personenzug (Kategorien aus dem SSP)
vorhandene Zugbeeinflussungssysteme	für Übergangsbereiche zu anderen Logiken
vorhandene Stromartausrüstungen	für Übergangsbereiche zu anderen Stromsystemen bzw. nicht elektrifizierten Bereichen
weitere Ausstattungsmerkmale	Wirbelstrombremse, Trittstufe ausfahrbar, Druckertüchtigung
erforderliche Bremskraft	
erforderliche Anfahrzugkraft relativ zur Zugmasse	um z. B. am Berg wieder anfahren zu können
Länge	z. B. um am Bahnsteig sicher halten zu können
Grenzlinien	
Achslast	
Lautstärke bzw. Vorhandensein von lautstärkeeinschränkenden Eigenschaften	*nicht unbedingt ein Sicherheitskriterium*
bestimmte Level (Grade of Automatisation (GoA)) automatisierten Fahrens	
spezielle Zulassungen	z. B. für BOStrab

Zu klären ist, wie damit umgegangen wird, wenn die Einschränkung auf bestimmte Fahrzeuge oder Typen von Fahrzeugbewegungen eingegrenzt ist, aber die Ausprägung eines dieser Attribute bei der betroffenen Fahrzeugbewegung nicht bekannt ist. Zum einen könnte die Einschränkung dann immer gelten oder sie würde in diesem Fall ignoriert werden. Die zweite Lösung scheint angesichts der Kernanforderung der sicheren Logik jedoch nicht vertretbar zu sein, da somit wichtige Einschränkungen wie eine verminderte Geschwindigkeit ignoriert werden könnten.

Dennoch sind Fälle vorstellbar, in denen eine Einfahrt in die RA möglich ist, ohne dass bekannt ist, ob das Fahrzeug die Einschränkung erfüllt. Deshalb könnte eine dritte Lösung sein, dass angegeben werden kann, wie im Falle des Nichtvorhandenseins eines Attributs zu verfahren ist. Dies macht die Logik komplexer und widerspricht damit der Anforderung der schlanken Logik, auf der anderen Seite macht es sie jedoch flexibler. Da die Fälle, in denen die Anforderung ignoriert werden kann, sehr rar sein dürften, tendiert der Autor dieser Arbeit in diesem Fall zur schlanken Logik und damit der Lösungsmöglichkeit 1.

Abhängigkeit von Detektionsabschnitten und Sensoren

Oftmals sind die der RA zugrundeliegenden Einschränkungen nicht zu jeder Zeit erforderlich, sondern nur unter bestimmten Voraussetzungen. Eine solche Voraussetzung könnte die Beanspruchung eines Detektionsabschnittes (vgl. zum Begriff „Detektionsabschnitt“ Kapitel 7.3.5) durch eine

Fahrzeugbewegung sein (z. B. im Fall eines Tunnelbegegnungsverbotes). Bei der Beanspruchung ist zwischen den verschiedenen Arten der Beanspruchung zu unterscheiden. Vor allem, ob es sich um die tatsächliche Befahrung, die Beanspruchung durch eine MA oder das Erreichen der Notbrems- oder der Betriebsbremskurve handelt.

Es sind auch Fälle denkbar, in denen nicht eine Beanspruchung des Detektionsabschnitts durch eine Fahrzeugbewegung entscheidend ist, sondern beispielsweise durch Gleisarbeitspersonal (z. B. im Falle einer TSR auf dem Nachbargleis zum Schutz des Gleisarbeitspersonals). Auch die Abhängigkeit von einem externen Sensor anstatt eines Detektionsabschnitts ist denkbar (z. B. im Falle eines Wettermessgeräts, welches eine Geschwindigkeitsbegrenzung aktivieren kann) (vgl. Kapitel 8.3.3).

Es ist auch denkbar, dass der Status eines Detektionsabschnitts oder der Wert eines externen Sensors nicht zum Aktivieren oder Deaktivieren einer RA führt, sondern deren Information beeinflusst. Beispielsweise gilt bei Überschreiten eines bestimmten Sensorwertes x1 die Einschränkung A und bei Überschreiten eines Sensorwertes x2 die Einschränkung B (z. B. könnte auf einer Brücke bei einer Windgeschwindigkeit ab 80 km/h eine Geschwindigkeitsbeschränkung für Güterzüge auf 90 km/h gelten und bei mehr als 100 km/h Windgeschwindigkeit eine Beschränkung für alle Fahrzeugbewegungen auf 80 km/h). Denkbar ist auch das Angeben einer Funktion, nach der abhängig vom gemessenen Wert auf dem Detektionsabschnitt bzw. dem gemessenen Sensorwert der eingeschränkte Wert auf dem Wirkabschnitt berechnet werden kann (z. B. beim Tunnelbegegnungsverbot, vgl. Kapitel 8.4.6).

Es erscheint sinnvoll, dass ein Wirkbereich auch verzögert aktiviert werden kann, indem eine Verzögerungszeit oder eine Verzögerungswegstrecke definiert wird. Die Verzögerungszeit beginnt abzulaufen, wenn der Detektionsabschnitt erreicht oder der Sensor aktiviert wird. Eine Verzögerungswegstrecke würde auf Basis der gemeldeten Geschwindigkeit konservativ berechnet, es würde also davon ausgegangen, dass die betreffende Fahrzeugbewegung mit maximal zulässiger Geschwindigkeit verkehrt.

Tab. 30 enthält eine Liste möglicher Detektionsabschnitte und externer Sensoren. Quelle sind die Ergebnisse der Funktionsanalyse aus Kapitel 6. Diese wird aus den gleichen Gründen wie die Liste in Tab. 28 nicht als abgeschlossen betrachtet, sondern soll nur einen Einblick in die Thematik liefern. Die Liste kann dynamisch während des Einsatzzeitraums der smartLogic ergänzt werden. Es ist jeweils eine weitere Einschränkung durch Attribute der genannten Elemente möglich (beispielsweise bei der Fahrzeugbewegung auf Fahrzeuge mit bestimmten Eigenschaften oder Fahrzeugbewegungen eines bestimmten Typs wie Güterzug.

Tab. 30: Mögliche Detektionsabschnitte und Sensoren zur Beeinflussung von RAs

Einfluss	Typ
Beanspruchung durch Fahrzeugbewegung durch Aufnahme in ihre MA	Detektionsabschnitt
Beanspruchung durch Fahrzeugbewegung durch tatsächliche Befahrung	Detektionsabschnitt
Beanspruchung durch Fahrzeugbewegung bei Erreichen der Notbremskurve	Detektionsabschnitt
Beanspruchung durch Fahrzeugbewegung bei Erreichen der Betriebsbremskurve	Detektionsabschnitt
Beanspruchung durch Gleisarbeitspersonal	Detektionsabschnitt
Beeinträchtigung des Lichtraumprofils, Verletzung der Grenzlinien	Sensor

Beeinträchtigung des Bahndamms	Sensor
Wettermessgeräte (Wind, Schnee, Eis, ...)	Sensor

Löschbedingungen

Wann RAs wieder gelöscht oder verkleinert werden können, kann sicherungstechnisch von verschiedenen Bedingungen abhängen. Nicht alle von diesen Bedingungen können von der Sicherungslogik kontrolliert werden (z. B. ob eine vom TMS beantragte Sperrung noch benötigt wird oder ob der Grund der Sperrung entfallen ist). Daher muss es Prozesse außerhalb der Sicherungslogik geben, die ein unzeitiges Löschen oder Modifizieren verhindern (z. B. durch betriebliche Regeln). Es kann aber die Sicherheit erhöhen, wenn von der Sicherungslogik zu kontrollierende Bedingungen formuliert werden können, die vor einer Löschung oder (verkleinernden) Modifizierung auf jeden Fall erfüllt sein müssten und die im Folgenden als **Löschbedingungen (Deletion Conditions)** bezeichnet werden.

Tab. 31 enthält Beispiele für Löschbedingungen, erhebt aber keinen Anspruch auf Vollständigkeit und kann jederzeit ergänzt werden. Die Bedingungen können dabei beliebig kombiniert und auch z. B. mit den Möglichkeiten aus dem Abschnitt „Eingrenzung der Einschränkungen und Vorgaben auf bestimmte Fahrzeuge und Typen von Fahrzeugbewegungen“ weiter eingegrenzt werden.

Tab. 31: Mögliche Löschbedingungen

Einfluss	ggf. Beispiele/Kommentar
Wirkabschnitt ist frei von Fahrzeugen	
Detektionsabschnitt ist frei von Fahrzeugen	
ein Sensorwert liegt vor oder nicht vor	zu beachten: das Vorliegen oder Nichtvorliegen führt nicht automatisch zur Löschung der RA, sondern stellt nur eine Voraussetzung dar
ein Stakeholder-System muss zuvor um Erlaubnis gefragt werden (vgl. Kapitel 8.3.2)	zum Beispiel darf eine Einschränkung, die zum Schutz einer Gleisbaustelle eingerichtet wurde, nur nach Zustimmung der betreffenden Rotte (Gleisarbeitertrupp) aufgelöst werden
eine bestimmte Zeit muss mindestens abgelaufen sein	hierdurch wird der frühestmögliche Zeitpunkt der Auflösung definiert

7.3.7 Danger Areas

Ziel dieses Kapitels ist die Besprechung von Gefahrenzonen (Danger Areas (DA)) in Hinblick auf ihre Repräsentation im Datenmodell. Die dazugehörigen Prozesse werden in Kapitel 8.6 thematisiert.

Zum besseren Verständnis der DAs sollen diese nachfolgend zunächst von den RAs abgegrenzt werden. Anschließend soll untersucht werden, welche Ausprägungen von DAs als Objekte im Datenmodell existieren müssen. Darauf aufbauend soll die optimale Ausdehnung der DAs hergeleitet werden, da eine zu kleine DA ein Sicherheitsproblem und eine zu große DA ein Kapazitätsproblem darstellen würde. Abschließend soll wie bei der RA auf Löschbedingungen eingegangen werden.

Abgrenzung der DAs von den RAs

In Kapitel 7.3.4 wurden DAs aufgrund ihrer Eigenschaft als Trigger sofortiger Handlungen als Spezialfall der RAs (URAs) definiert. Demnach handelt es sich also um ortsgebundene Informationen, deren Auftreten eine Sicherheitsreaktion auslösen kann (siehe Reaktionsprozesse, Kapitel 6.2.2). Ziel

der Sicherheitsreaktion ist es, die bereits verkehrenden Fahrzeugbewegungen sowie die Infrastruktur vor Schäden zu schützen.

Damit die Sicherheitsreaktion die richtigen Fahrzeuge erreicht, muss beim Anlegen der DA angegeben werden können, welche Fahrzeugbewegungen im räumlichen Sinne betroffen sind. Hierzu könnte ein entsprechender Wirkabschnitt (vgl. Kapitel 7.3.5) angelegt werden. Die angestoßene Sicherheitsreaktion würde allerdings mit ihrem Reaktionsprozess nur bereits bestehende und mit dem Detektionsabschnitt verbundene Fahrzeugbewegungen erreichen. Häufig besteht die Gefahr jedoch auch nach dem Ausführen der Sicherheitsreaktion fort, z.B. wenn eine nicht identifizierte Fahrzeugbewegung oder eine Verletzung des Lichtraumprofils von außen (z. B. durch einen Erdrutsch) detektiert wurde. Aus diesem Grunde muss die DA auch auf der Infrastruktur mittels einer geeigneten ortsgebundenen Information Einschränkungen definieren, die von der Sicherungslogik bei der Prüfung von zukünftigen Anfragen des TMS berücksichtigt werden. In diesem Sinne stellt die DA nach der Abarbeitung der Sicherheitsreaktion eine RA (URA) dar.

Während die RAs i. d. R. statisch an die Infrastruktur geknüpft sind und planmäßig eingerichtet werden, entstehen die DAs häufig unerwartet, z. B. durch die Bewegung eines nicht identifizierten Fahrzeugs oder durch die Detektion eines Gegenstandes auf dem Gleis.

Ausprägungen und Aufbau von DAs

Aufgrund der globalen Anforderung der *generischen Logik* wird eine Auflistung aller denkbaren Ausprägungen von DAs als nicht zielführend für die Erstellung der smartLogic angesehen und daher hier nicht weiterverfolgt. DAs werden in der Regel aufgrund der Detektion eines unerwarteten Ereignisses durch ein externes System (Sensor) angelegt. Die Sensoren könnten sich im Sinne des Stakeholder-Registrierungs-Konzepts (vgl. Kapitel 8.3.3) auf entsprechenden Schnittstellen registrieren und hierdurch die notwendigen Reaktionen einleiten.

Daher sollte zur Bestimmung der Ausprägungen der DAs von den Konsequenzen her gedacht werden, die das jeweilige Sensorereignis hat. Konsequenzen könnten das Beeinflussen der Fahrweise von Fahrzeugbewegungen in einem bestimmten räumlichen Bereich (Wirkabschnitt) sein (z. B. Anhalten oder Verlangsamen). Aber auch das Verändern des Status von Infrastrukturelementen erscheint denkbar (z. B. könnte theoretisch im Falle eines entlaufenden Wagens das Definieren einer Vorzugslage für eine Weiche und eine anschließende Entgleisungseinrichtung denkbar sein) (vgl. Kapitel 8.7.3).

Für das Datenmodell ist in Anbetracht dieser Konsequenzen relevant, dass für eine DA ein Reaktionsprozess festgelegt werden kann, dem verschiedene Parameter durch den aufrufenden Sensor mitgegeben werden können, wie der Wirkbereich und die Konsequenz für Fahrzeuge in diesem Bereich (vgl. Tab. 28 in Kapitel 7.3.6) sowie der Soll-Status von Infrastrukturelementen. Weiterhin muss definiert werden können, ob und wenn ja, welche RA durch die DA definiert werden soll.

Ausdehnung der DA (Wirkbereich)

Bei der Ausdehnung der DA erscheint es sinnvoll, zwei Bereiche zu unterscheiden: der tatsächlich oder vermutlich bereits betroffene Abschnitt, der durch den auslösenden Sensor abgedeckt wird, und der Abschnitt, der möglicherweise in Zukunft betroffen sein könnte. Letzterer tritt zum Beispiel bei einem entlaufenden Wagen auf, kann aber z. B. durch das Umstellen einer Weiche verändert werden.

Der tatsächlich oder vermutlich bereits betroffene Abschnitt sollte vom Sensor der DA mitgegeben werden. Der möglicherweise in Zukunft betroffene Abschnitt sollte von der Sicherungslogik anhand des aktuellen Betriebszustands (Position anderer Fahrzeuge, Bremsweg der verkehrenden

Fahrzeugbewegungen, Status der Infrastrukturelemente) bestimmt werden. Er kann nicht vom Sensor mitgegeben werden, da diesem in der Regel kein umfassender Betriebszustand vorliegt.

Es ist auch denkbar, dass sich eine DA im Laufe der Zeit weiter ausdehnt, z. B. wenn ein Fahrzeug zunächst nur detektiert wurde, aber im Nachhinein als rollend erkannt wurde oder wenn sich ein Erdrutsch weiterbewegt. Solche Ereignisse können in der Regel nicht von einem Sensor direkt erkannt werden. Allerdings könnte ein Nachbarsensor ebenfalls ein Ereignis detektieren, dass zum Anlegen einer DA führen müsste. Eine solche Detektion könnte entweder zur Ausweitung der bereits bestehenden DA führen oder es könnte eine neue DA angelegt werden. Die jeweils sinnvollere Vorgehensweise hängt von der Art des Sensors ab. Um die smartLogic generisch zu definieren, könnte bei der Registrierung eines Sensors als externes System (Stakeholdern, vgl. Kapitel 8.3.3), welches die Definition eines Gefahrenbereichs auslösen kann, eine Variable definiert werden, mit der festgelegt wird, welcher der beiden Fälle zum Tragen kommen soll.

Löschbedingungen für die DA

DAs können auf verschiedene Arten wieder gelöscht werden. Hierfür muss die der DA zugrundeliegende Gefahr gebannt sein. Diese Feststellung ist in jedem Fall ein sicherheitsrelevanter Prozess. Allerdings sind verschiedene solche Prozesse mit unterschiedlichen Parametern denkbar, die wie bei der Einrichtung auch für die Auflösung vom initiierenden System gesetzt werden können. Die Löschbedingungen müssen also ebenfalls im DA-Objekt gespeichert sein.

7.3.8 Definition von Gleisbereichen

Kapitel 7.3.3 hat sich im Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)“ mit der Definition verschiedener Ausprägungen von Gleisabschnitten beschäftigt, die ortsgebundene Informationen repräsentieren, die auf einem oder mehreren Gleissegmenten abschnittsweise wirken. Diese Gleisabschnitte könnten theoretisch beliebig große Bereiche der Gleistopologie umfassen, z. B. einen ganzen Kontrollbereich eines Mitarbeiters in der Leitzentrale. Aufgrund der unterschiedlichen Bedeutung solcher Bereiche als übergeordnete Gruppierung und Zuordnung von Infrastrukturelementen im Vergleich zu den für ortsgebundene Informationen konzipierten Gleisabschnitten erscheint eine begriffliche Unterscheidung sinnvoll. Hierzu soll der Begriff „**Gleisbereich**“ eingeführt werden.

Infrastrukturelemente können demnach zu Gleisbereichen zusammengefasst werden, wobei der Gleisbereich sich nicht nur auf einen Teil der Topologie bezieht, sondern auch die darin enthaltenen physischen Elemente bzw. deren Objektrepräsentationen im Datenmodell umfasst. Es handelt sich also um eine räumlich definierte Gruppe von Datenobjekten.

Nachfolgend soll der Nutzen und mögliche Anwendungsgebiete von Gleisbereichen näher untersucht werden. Dabei stellt sich auch die Frage, ob sich Gleisbereiche überlappen können. Mit dieser Fragestellung beschäftigt sich ein weiterer Abschnitt dieses Unterkapitels. Ein Spezialfall von Gleisbereichen kann die Definition von Strecken bzw. Streckenabschnitten darstellen. Die Notwendigkeit der Modellierung von Strecken wurde jedoch bisher noch nicht hergeleitet. Deshalb beschäftigt sich ein weiterer Abschnitt mit den Informationen, die bisher über Strecken und Streckenabschnitten festgelegt wurden und prüft somit die Notwendigkeit der Modellierung von Strecken.

Nutzen von Gleisbereichen

Um zu bestimmen, welche Gleisbereiche für die Modellierung der Sicherungslogik definiert werden sollten, ist ein Überblick über die Vorteile von Gleisbereichen erforderlich. Grob gesagt, macht die Definition eines Gleisbereiches für die Modellierung der Logik immer dann Sinn, wenn er als zusätzlicher Begriff in der Logik die redundante Angabe von Informationen vermeidet (vgl. *Kernanforderung der sicheren Logik*).

Ein Gleisbereich bietet beispielsweise die Möglichkeit für alle ihm zugewiesenen Infrastrukturelemente Standardwerte zu definieren. Beispielsweise könnten Eigenschaften wie Lichtraumprofil bzw. Grenzlinien und Höchstgeschwindigkeit sowie Befahrbarkeitsbedingungen wie z. B. die Spurweite über einen Gleisbereich definiert werden. Da häufig solche Standardwerte auch für den gesamten Wirkungsbereich der Sicherungslogik gelten, wird angenommen, dass auch die Definition eines globalen Gleisbereichs erfolgt, der als „smartLogic Area“ bezeichnet werden kann.

Ein weiterer sinnvoller Anwendungsfall von Gleisbereichen ist es, wenn über diese ein Zuständigkeitsbereich definiert wird, z. B. der Kontrollbereich der menschlichen Überwachung des Systems. Die Zuordnung der Elemente zum Gleisbereich muss dabei nicht fest sein, sondern kann auch durch einen entsprechenden Prozess verändert werden, welches auch durch eine entsprechende Anforderung gefordert wird (*flexible Kontrollbereiche*, vgl. Kapitel 7.2.1).

Eine dritte mögliche Anwendung eines Gleisbereiches wäre, mit diesem eine gemeinsame Funktion der zugeordneten Elemente zu definieren. Bei der Modellierung zeigte sich beispielsweise, dass die Einführung von „Interlocking Subareas“ sinnvoll ist, um sicherzustellen, dass die smartLogic bei der parallelen Bearbeitung mehrerer Anfragen durch das TMS nicht in einen Deadlock-Zustand gerät. Es handelt sich um eine Gruppe benachbarter Elemente der Gleistopologie, die während der Bearbeitung einer Anfrage kurzzeitig gesperrt werden, bis geprüft worden ist, welche dieser Elemente für die Anfrage wirklich benötigt werden und vorläufige Beanspruchungen eingetragen sind (siehe Kapitel 8.5.3).

Überlappung von Gleisbereichen

Aufgrund der verschiedenen Anwendungsfälle ist es sinnvoll, dass Elemente mehreren Gleisbereichen gleichzeitig zugewiesen sein können. Hierdurch kann jedoch ein Problem entstehen, wenn zwei sich überlappende Gleisbereiche für dasselbe Attribut einen widersprüchlichen Standardwert definieren, beispielsweise eine Maximalgeschwindigkeit.

Theoretisch gibt es für dieses Problem mehrere Lösungsmöglichkeiten. Drei denkbare Lösungsmöglichkeiten sind nachfolgend aufgeführt.

1. Der zuletzt definierte Wert überschreibt vorige Werte.
2. Es wird auf den restriktivsten Wert zurückgegriffen.
3. Es existiert eine Vorrangregelung für verschiedene Arten von Gleisbereichen.
4. Im Konflikt könnte manuell ein Vorrang der Werte definiert werden.

Bei der ersten Lösungsmöglichkeit müsste im Sinne der *Kernanforderung der sicheren Logik* sichergestellt werden, dass der vorige Wert auch wirklich keine Gültigkeit mehr hat. Dies erscheint aufwendig. Die dritte und die vierte Lösungsmöglichkeit widersprechen dem geforderten dynamischen Charakter der Logik, wonach diese weitgehend automatisiert arbeiten und generisch definiert sein soll (vgl. Anforderungen der *hohen Automatisierung* und *generischen Logik*. Daher scheint es am sinnvollsten, bei Konflikten den restriktivsten Wert zu verwenden. Die ist eine generische Priorisierungsregel, welche die Grundprämisse der sicheren Logik am ehesten erfüllt.

Umgang mit Strecken bzw. Streckenabschnitten und Betriebsstellen

Sowohl im XML-ISS als auch im PlanPro-Modell, ebenso wie in der Realität spielen Strecken für die Verortung der ortsgebundenen Informationen eine entscheidende Rolle. Jedes Gleissegment ist einer Strecke zugeordnet. XML ISS enthält weiterhin eine Zuordnung zu Betriebsstellen. Datenobjekte können allerdings auch alleine über eine eindeutige ID identifiziert werden, wie sie beispielsweise im PlanPro-Modell ebenfalls vergeben wird.

Strecken sind üblicherweise in den in Kapitel 2.5 beschriebenen Datenmodellen eine Reihe von Attributen zugeordnet, die sich neben deren Identifizierung auf die Vorgabe von Standards wie einer Höchstgeschwindigkeit für die Strecke beziehen. Die Standards können aber in der Regel durch zusätzliche ortsgebundene Informationen überschrieben werden. Da sich die Standards häufig nicht auf eine gesamte Strecke beziehen, werden Streckenabschnitte definiert. Ein Streckenabschnitt umfasst dabei einen definierten Bereich der Gleistopologie.

Die Definition von Strecken bzw. Streckenabschnitte entspricht damit neben ihrer Zuordnungseigenschaft, die für die smartLogic keine Rolle spielt, dem ersten beschriebenen Anwendungsfall (Definition von Standardeigenschaften). Sie können also auch als Gleisbereiche definiert werden. Für die Funktionsweise der smartLogic besteht damit keine Erfordernis Strecken oder Streckenabschnitte zu definieren, sondern es könnten auch für davon unabhängige Gleisbereiche oder theoretisch nur für die globale „smartLogic Area“ Standardwerte definiert werden.

7.3.9 Modellierung der Fahrzeugbegrenzungslinien / des Lichtraumprofils

Bisher wurde die Gleistopologie als Netz aus eindimensionalen Gleisen betrachtet, die an Verzeigungspunkten wie Weichen miteinander verknüpft sind. In der Realität verkehren jedoch Fahrzeuge mit dreidimensionaler räumlicher Ausdehnung auf den Gleisen, die weder miteinander noch mit Gegenständen an der Strecke kollidieren dürfen.

Da sich die Fahrzeuge jedoch nur in einer Dimension, nämlich entlang des Gleises bewegen können, werden die anderen beiden räumlichen Dimensionen in der Eisenbahnsicherungstechnik normalerweise aus Vereinfachungsgründen zu Klassen (im Sinne einer Einteilungsklasse, nicht eines Objekttyps des Datenmodells) zusammengefasst. Jede Klasse definiert eine zweidimensionale Fahrzeugbegrenzungslinie (Grenzlinie), welche ihre äußere Begrenzung definiert. Ein Fahrzeug kann zu einer Klasse gehören, wenn es gemessen von der Gleismittellinie an keiner Stelle die Grenzlinie überschreitet. Analog kann eine Fahrzeugbewegung zu einer Klasse gehören, wenn sie kein Fahrzeug enthält, dass an einer Stelle die Grenzlinie überschreitet. Die Grenzlinie ist vom Lichtraumprofil abzugrenzen, welches etwas großzügiger bemessen ist und die Grenzen für die Umbauung mit Gegenständen markiert, die nicht zur unmittelbar für den Eisenbahnbetrieb notwendigen Infrastruktur gehören.

Die Modellierung der räumlichen Ausmaße der Fahrzeuge mittels Klassen bietet den Vorteil, dass von der Sicherungslogik sehr einfach geprüft werden kann, ob ein Fahrzeug auf einem Gleis mit einer bestimmten Grenzlinie verkehren darf. Nachteile treten hingegen vor allem

- bei Fahrzeugen bzw. Zügen auf, die außergewöhnliche Fahrzeugbegrenzungslinien haben, welche zu keiner standardisierten Grenzlinie passen, oder
- Fahrzeuge auf Gleisen verkehren sollen, für die sie die vorgesehenen Grenzlinien überschreiten.

In diesen beiden Fällen kann vom automatisierten System weder entschieden werden, ob eine Kollision mit einem festen Gegenstand droht – das wäre ein absolutes Ausschlusskriterium für die

Fahrt (zumindest im automatischen Betrieb) –, noch, ob zwar theoretisch eine Befahrbarkeit möglich wäre, aber eine Beeinträchtigung eines benachbarten Gleises droht. Für diese beiden auszuschließenden Gefährdungen sind unterschiedliche Lösungsstrategien denkbar, die im Folgenden hergeleitet werden.

Lichtraumprofil für den Ausschluss der Kollision mit der Infrastruktur

Optimalerweise wäre für das erste Entscheidungskriterium für die Zulassung der Fahrt, der Kollisionsfreiheit mit festen Gegenständen an der Strecke, ein tatsächliches Lichtraumprofil an jeder Stelle des Gleises bekannt (gegenüber einem pauschalen Lichtraumprofil würde das z. B. einen Vorteil bringen, wenn das Gleis nur teilweise befahren wird, beispielsweise von einem Baustellenfahrzeug). Dies erscheint allerdings derzeit noch unrealistisch, denn dafür wäre ein sehr hoher Datenaufwand notwendig, zudem müsste eine regelmäßige Erfassung stattfinden, da das tatsächliche Lichtraumprofil durch Vegetationswachstum und anderen Begebenheiten regelmäßiger Veränderung unterliegt.[33]

Falls eine Fahrzeugbewegung einen Gleisabschnitt komplett befährt, hat die Angabe eines Lichtraumprofils, welches dem kleinsten freien lichten Raum auf dem entsprechenden Abschnitt entspricht, dagegen keinen Nachteil. Hierbei tritt jedoch das Problem auf, dass im Einzelfall festzulegen wäre, welche Ausdehnung ein solcher Gleisabschnitt hätte (vgl. hierzu Kapitel 7.4.2 und Kapitel 7.3.3, Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)“). Das Problem könnte jedoch umgangen werden, wenn ein großzügiges globales Lichtraumprofil (zumindest für einen größeren Gleisbereich) festgelegt würde und nur einschränkende Bereiche speziell als ortsgebundene Informationen mittels Gleisabschnitten markiert werden würden (vgl. auch hierzu Kapitel 7.3.3).

Für die Modellierung der smartLogic wird für den Ausschluss von Kollisionen mit der Infrastruktur demnach weiterhin mit dem Prinzip des Lichtraumprofils gearbeitet. Es wurden drei Möglichkeiten identifiziert, die Informationen zum Lichtraumprofil mit bestehenden Konzepten im Datenmodell zu hinterlegen, die alle genutzt werden können.

- Um Redundanzen zu vermeiden, können globale Lichtraumprofile definiert werden, die standardmäßig für eine gesamte smartLogic-Area (vgl. Kapitel 7.3.6) gelten.
- Weiterhin können die beiden Lichtraumprofile als Attribute der topologischen Gleisobjekte modelliert werden, die das globale Profil überschreiben.
- „Engstellen“ können als ortsgebundene Informationsobjekte in Form von topologischen Bereichen bzw. Gleisabschnitten mit eingeschränktem Lichtraumprofil angeben zu können (vgl. Kapitel 7.3.3), die dann im Vergleich zu den anderen beiden möglichen Angaben höchste Priorität haben.

Grenzlinien für den Ausschluss der Kollision mit einem anderen Eisenbahnfahrzeug

Klassischerweise definieren Fahrzeugbegrenzungslinien oder laut EBO „Grenzlinien“ die zulässigen Fahrzeugausmaße (unter ungünstigen Bedingungen wie beispielsweise in einer engen Bogenfahrt). Dabei ist sichergestellt, dass auf parallelen Gleisen bei Einhaltung der Grenzlinien keine Kollision mit anderen Fahrzeugen drohen, welche ebenfalls die Grenzlinien einhalten.

[33] Aufgrund der schnellen Weiterentwicklung der 3D-Erfassungstechnologien erscheint diese Möglichkeit jedoch für die Zukunft nicht ausgeschlossen. In diesem Fall, könnte aber auch mittels der Erfassung ein klassisches Lichtraumprofil aus den erfassten Daten heraus bestimmt werden.

Die tatsächlich möglichen Fahrzeugausmaße sind jedoch größer und hängen nicht nur wie oben beschrieben vom tatsächlichen Lichtraumprofil ab, sondern auch von der Beschaffenheit eines möglichen Fahrzeugs auf dem benachbarten Gleis. Heute unterscheidet die DB im betrieblichen Regelwerk daher verschiedene Arten von Lademaßüberschreitungen. Je nach Klasse sind Fahrten auf dem Nachbargleis unter unterschiedlichen Voraussetzungen möglich, beispielsweise, dass die benachbarte Fahrt nicht selbst eine Lademaßüberschreitung einer bestimmten Klasse hat.

An bestimmten Stellen der Topologie wird der Mindestabstand zum Nachbargleis sogar planmäßig unterschritten, wenn Gleise z. B. an Weichen zusammengeführt werden oder sich kreuzen. Um den Beginn der Unterschreitung der Grenzlinien zu markieren, dienen die Grenzzeichen. Die RCA definiert für solche Bereiche mit überlappenden Grenzlinien „**Allocation Sections**“ (AS) (vgl. Kapitel 2.4.4), deren Befahrbarkeit vom Freisein der jeweiligen verbundenen AS als Detektionsabschnitt abhängt.

Die erwähnten Klassen von Lademaßüberschreitungen stellen analog zur Klasseneinteilung der Grenzlinien eine einfache Möglichkeit dar, um Kollisionen mit anderen Fahrzeugen zu vermeiden. Theoretisch wäre es aus Kapazitätssicht jedoch optimal, immer die tatsächliche Breite der Fahrzeuge zu vergleichen und das Grenzzeichen quasi flexibel virtuell an die Position zu setzen, hinter der tatsächlich ein Konflikt zu erwarten ist. Damit würden auch Lademaßüberschreitungsklassen überflüssig werden.

Das Problem ist hierbei weniger, dass der Sicherungslogik die tatsächliche Breite der Züge nicht bekannt ist. Das ist zwar heute so, man könnte jedoch auf die fahrzeugseitigen Begrenzungslinien zurückgreifen oder eine zusätzliche Fahrzeugvariable einführen. Allerdings gibt es aktuell im reinen topologischen Modell auch keine Information darüber, wie weit die Gleise auseinanderliegen. Hierzu müsste auf ein geografisches Gleismodell zurückgegriffen werden.

Da in dieser Thematik nur wenig Optimierungspotential vermutet wird und es sich bei Fahrten mit Lademaßüberschreitung um Spezialfälle handelt, werden die Überlegungen zu diesem Thema hier zurückgestellt. Theoretisch ist eine nachträgliche Anpassung des Modells in diesem Bereich relativ einfach möglich, da hierdurch keine Änderung der grundsätzlichen Logik der smartLogic erwartet wird.

7.4 Infrastrukturmodell

In diesem Kapitel wird das Infrastrukturmodell für die smartLogic hergeleitet und beschrieben. Es umfasst gemäß der in Kapitel 7.2.2 beschriebenen Aufteilung in Teilmodelle die physischen Eigenschaften der Elemente der Infrastruktur, sofern diese für die Sicherungslogik von Relevanz sind. Dagegen beschreibt das in Kapitel 7.3 thematisierte topologische Modell, wie die physischen Elemente zueinander angeordnet sind und wie ortsgebundene Informationen auf der Topologie wirken.

Eine Eingrenzung der für die Sicherungslogik relevanten physischen Elemente erfolgt in Kapitel 7.4.1. In den weiteren Unterkapiteln dieses Kapitels wird jeweils die Modellierung einzelner Objekttypen des Infrastrukturmodells hergeleitet. Die Vollständigkeit wird wiederum darüber sichergestellt, dass bei der Verhaltensmodellierung für jeden dort vorkommenden Begriff geprüft wird, ob er im Datenmodell vorhanden ist (vgl. Kapitel 7.2.3).

7.4.1 Bestimmung und Zuschnitt der zu modellierenden Infrastrukturelemente

Zur Eisenbahn gehören heute umfangreiche und insbesondere sehr diverse Infrastrukturanlagen. Damit das Infrastrukturmodell im Sinne der spezifischen Anforderungen aus Kapitel 7.2.1 zwar

eindeutig und vollständig, aber gleichzeitig nicht zu umfangreich wird, muss zunächst der Betrachtungsraum eingegrenzt werden.

Jede Abbildung in einem Modell ist (aufgrund der Definition des Modellbegriffs) zwangsläufig eine Vereinfachung der Realität. Welche Aspekte in das Modell aufgenommen werden sollten, hängt vom Anwendungsfall des Modells ab. Daher sind in den in Kapitel 2.4.5 vorgestellten Datenmodelle physische Infrastrukturelemente in unterschiedlichem Maße repräsentiert, denn die Modelle sind auch für unterschiedliche Anwendungsfälle spezifiziert worden.

Gemäß den spezifischen Anforderungen sind für die smartLogic zwei Argumente für die Aufnahme und den Zuschnitt eines physischen Infrastrukturelements im Datenmodell entscheidend:

- Das Element muss eine Relevanz für die Logikentwicklung haben, also in der Logik als Begriff vorkommen, denn ansonsten sollte es aufgrund der Anforderung der *schlanken Logik* nicht im Datenmodell enthalten sein. Ein Begriff kommt dann in der Logik vor, wenn die smartLogic zur Erledigung ihrer Aufgaben in Form der Prüf- und Reaktionsprozesse bzw. der Subroutinen auf die spezifischen Eigenschaften der Infrastrukturelemente zurückgreifen wird.
- Aus Gründen der Kompatibilität und Zukunftssicherheit kann es sinnvoll sein, weitere Elemente bzw. vor allem Eigenschaften von Elementen mit in das Datenmodell aufzunehmen, die aufgrund von Standards bzw. Standardschnittstellen vorhanden sein sollten (vgl. Anforderung zu den *Standardschnittstellen*).

Ob ein Element als Begriff in der Verhaltensmodellierung der Logik vorkommen wird, kann zunächst aus den Funktionen und Prüfbedingungen der Sicherungslogik hergeleitet werden, die im 6. Hauptkapitel bestimmt wurden. Das Modell kann anschließend bei Bedarf parallel zur Logikentwicklung vervollständigt werden.

Bei der Durchsicht der funktionalen Anforderungen aus dem 6. Hauptkapitel zeigt sich, dass Infrastrukturelemente insbesondere dann in der Logik vorkommen, wenn sie

1. mit der Logik interagieren, indem sie Nachrichten mit ihr austauschen oder Funktionalitäten bereitstellen, die von der Sicherungslogik im Rahmen ihrer Aufgaben genutzt werden
2. für die Logik ortsgebundene Informationen enthalten (siehe auch Kapitel 7.3.3),
3. den Wirkbereich einer ortsgebundenen Information beeinflussen.

Treffen nur einer oder beide der letztgenannten Fälle (Fall 2 und 3) zu, kann eine Modellierung gegebenenfalls auch vollständig als ortsgebundene Information gemäß Kapitel 7.3.3 erfolgen, ohne, dass eine zusätzliche Repräsentation im Infrastrukturmodell notwendig erscheint. Ob diese Aussage generell gilt, soll jedoch nachfolgend noch untersucht werden.

7.4.2 Modellierung der Gleisinfrastruktur

Ein entscheidender Teil der Infrastruktur ist naturgemäß die Gleisinfrastruktur als Fahrweg für die Schienenfahrzeuge. Die physischen Bestandteile des Fahrwegs werden im Infrastruktur-Teilmodell als **Fahrwegelemente** („Track Elements“) bezeichnet, die von den topologischen Gleissegmenten (vgl. Kapitel 7.3.1) zu unterscheiden sind.

Die Gleisinfrastruktur bildet eine knappe Ressource, welche von den Schienenfahrzeugen abschnittsweise exklusiv genutzt werden muss. Das Vorhandensein und die Befahrbarkeit des Fahrwegs sowie die exklusive Nutzung durch ein einzelnes Schienenfahrzeug muss gemäß den im

6. Hauptkapitel bestimmten Prüfbedingungen von der Sicherungslogik sichergestellt werden. Für die Modellierung der möglichen Fahrwege ist jedoch nicht die physische Gleisinfrastruktur ausschlaggebend, sondern die Abbildung der Verknüpfung der einzelnen Elemente im topologischen Modell, welches bereits in Kapitel 7.3 beschrieben wurde.

Es stellt sich die Frage, ob dennoch eine Modellierung der Gleisinfrastruktur im Infrastrukturmodell sinnvoll ist oder ob die Abbildung der Gleistopologie im topologischen Modell ausreichend ist. Kapitel 7.4.1 enthält Bewertungskriterien für diese Frage, die in den beiden nachfolgenden Abschnitten überprüft werden sollen.

Prüfung der Relevanz in Bezug auf das Vorhandensein relevanter Informationen oder den Wirkbereich

Bewertungskriterium 2 und 3 beziehen sich auf das Vorhandensein von ortsgebundenen Informationen. Durch die physische Beschaffenheit des Gleiskörpers werden Eigenschaften vorgegeben, die für die darauf verkehrenden Fahrzeuge einzuhaltende Randbedingungen definieren, beispielsweise die Spurweite, das Lichtraumprofil (siehe hierzu Kapitel 7.3.9), die zulässige Achslast oder das erlaubte Geschwindigkeitsprofil betreffend. Diese Eigenschaften sind als auf unterschiedliche Elemente des Gleiskörpers zurückzuführen, wie beispielsweise die verwendeten Schienen mit ihrem Schienenprofil und ihrer Gleiskrümmung oder die Beschaffenheit des Oberbaus. Das topologische Modell enthält bereits mehrere Möglichkeiten, um Eigenschaften des Gleiskörpers zu abzubilden:

1. Die Eigenschaften könnten direkt den topologischen Gleissegment-Objekten als Attribute beigefügt werden.
2. Einzelne Eigenschaften könnten als ortsgebundene Informationen modelliert werden, die entweder einen Gültigkeitsbereich haben (Gleisabschnitt, vgl. Kapitel 7.3.4) und somit mit einem oder mehreren topologischen Objekten verknüpft werden müssten oder punktuell nur den Wechsel dieser Eigenschaft angeben (z. B. ein Wechsel der zulässigen Achslast oder der zulässigen Geschwindigkeit).
3. Die Informationen können für einen größeren Bereich als Standardwerte in Gleisbereich-Objekten gespeichert werden, so dass nur noch Abweichungen von diesen Standardwerten separat mit einer der anderen Möglichkeiten festgelegt werden müssen (vgl. Kapitel 7.3.8).

Ein Vorteil durch zusätzliche Objekte im Infrastrukturmodell zur Abbildung der phyischen Fahrwegelemente für die Speicherung von Informationen wird nicht gesehen.

Prüfung der Relevanz in Bezug auf das Vorhandensein von Interaktion mit der Sicherungslogik

Für die Prüfung des anderen Bewertungskriteriums (Kriterium 1) aus Kapitel 7.4.1 ist zu untersuchen, ob Interkation zwischen dem physischen Gleis und der Sicherungslogik stattfindet. Als potenzielle Interaktionsquellen wurden mittels Brainstorming folgende Elemente auf dem Gleis identifiziert

- verkehrende Fahrzeuge
- ansteuerbare Fahrwegelemente
- Überwachungssysteme des Gleises

Die *Fahrzeuge* verkehren zwar auf der Gleisinfrastruktur, dies ist jedoch eine Interaktion zwischen dem Fahrzeug und der Gleisinfrastruktur und die Sicherungslogik ist über die Fahrerlaubnis nur indirekt daran beteiligt (Wie bereits erwähnt findet die Prüfung des Fahrwegs auf Basis des

topologischen Modells statt). Eine direkte Kommunikation zwischen dem einfachen Gleis und der Sicherungslogik ist dagegen bisher nicht möglich.

Anders verhält es sich bei den *ansteuerbaren Fahrwegelementen*. Diese Fahrwegelemente werden im Folgenden als **stellbare Fahrwegelemente** („**Controlled Track Elements**“ **(CTE)**) bezeichnet.[34] Da es sich bei der Ansteuerung der stellbaren Fahrwegelemente um sicherheitskritische Operationen handelt, ist eine Interaktion mit der Sicherungslogik erforderlich. Weiterhin haben ihr Status und ihre Ausdehnung auch eine Auswirkung auf die Befahrbarkeit des Gleises. Daher sollten stellbare Fahrwegelemente im Infrastrukturmodell als Objekte abgebildet werden. Kapitel 7.4.3 beschäftigt sich näher mit ihrer Modellierung. Ein Bedarf für die Modellierung von nicht stellbaren Teilen des Gleises als Fahrwegelemente kann aus der Interkation mit den stellbaren Fahrwegelementen jedoch nicht hergeleitet werden.

Denkbar wäre auch, dass das Gleis zukünftig mit *Überwachungssystemen* ausgestattet wird, die dann mit der Sicherungslogik kommunizieren. Diese Überwachungssysteme können als externe Systeme betrachtet werden. Deshalb ergibt sich auch aus dieser Interaktionsart keine Indikation für eine separate Modellierung aller Bestandteile des physischen Gleises als Fahrwegelement-Objekte im Infrastrukturmodell.

Fazit

Insgesamt wird aus den im Unterkapitel beschriebenen Gründen geschlussfolgert, dass keine Modellierung aller Teile des physischen Gleises im Infrastrukturmodell notwendig ist, sondern nur der stellbaren Fahrwegelemente oder externer Systeme, die mit der Sicherungslogik kommunizieren. Mit der Modellierung der stellbaren Fahrwegelemente beschäftigt sich das nachfolgende Unterkapitel 7.4.3.

7.4.3 stellbare Fahrwegelemente

Mit dem Begriff „stellbare Fahrwegelemente“ wurden in Kapitel 7.4.2 die beweglichen und ansteuerbaren (und damit kontrollierbaren) Elemente der Gleisinfrastruktur bezeichnet. Im ersten Abschnitt soll darauf eingegangen werden, welche Elemente zu den stellbaren Fahrwegelementen gezählt werden können.

Für die Sicherungslogik sind die stellbaren Fahrwegelemente gemäß Kapitel 7.4.2 zum einen als Interaktionsobjekte von Bedeutung, da eine Veränderung ihres Status sicherheitsrelevant ist und daher jeder Stellauftrag vorher von der Sicherungslogik geprüft werden muss. Zum anderen ist die Abbildung ihrer topologischen Ausdehnungen im topologischen Teilmodell relevant, da sie die Befahrbarkeit des Gleises beeinflussen. Nachfolgend soll auf die Modellierung dieser beiden Eigenschaften im zweiten und dritten Abschnitt eingegangen werden.

Mögliche Untergliederung der stellbaren Fahrwegelemente

Bestehende Datenmodelle enthalten zahlreiche Elemente, die aufgrund ihrer Eigenschaften und zu den stellbaren Fahrwegelementen gezählt werden können. Diese Elemente können einer der folgenden Gruppen zugeordnet werden:

- An den **verzweigenden Fahrwegelementen** („branching elements“) verzweigt sich die Gleistopologie, so dass von mindestens einem Ende des Fahrwegelements aus

[34] Der häufig verwendete Begriff des „**Stellelements**“ wird nicht genutzt, da dieser auch Elemente umfasst, die nicht unmittelbar Teil des Gleises sind, wie z. B. Signale.

verschiedene Fahrbeziehungen möglich sind (eine reine Kreuzung ohne Weichenfunktion ist demnach kein verzweigendes Fahrwegelement). Hierzu gehören vor allem Weichen und Drehscheiben (Theoretisch sind noch weitere Elemente denkbar, die bisher jedoch hauptsächlich bei anderen spurgeführten Verkehrssystemen vorkommen.).

- Bei den **unterbrechenden Fahrwegelementen** („interrupting elements“) wird die Durchgängigkeit des Gleises unterbrochen, ohne dass sich das Gleis verzweigt, z. B. bei beweglichen Brücken oder Fähranlegern.
- **Sperrelemente** („blocking elements“) sind dagegen nicht direkt Teil des eigentlichen Gleises (beinhalten also keine Schienen), können jedoch dessen Befahrbarkeit unterbrechen. Klassische Beispiele sind Gleissperren und Tore, aber auch z. B. Schwenkkräne zur Entladung von Eisenbahnfahrzeugen, wenn diese ins Lichtraumprofil schwenken.

Modellierung der topologischen Ausdehnung

An verschiedenen Stellen in dieser Arbeit (u. a. in Kapitel 7.1) wurde eine Kompatibilität zu bestehenden Modellen und insbesondere der RCA als sinnvoll beurteilt. Die RCA definiert zwei verschiedene Arten von topologischer Ausdehnung von stellbaren Fahrwegelementen am Beispiel der Weichen (vgl. [SBB AG 2020], [ERTMS Users Group & EULYNX 2020a] und Kapitel 2.4.4):

Zum einen existiert der topologische Bereich, in dem Einschränkungen der Befahrbarkeit der Topologie vom Status des stellbaren Fahrwegelements abhängen. Der entsprechende topologische Bereich wird „**Drive Protection Section**“ (DPS) genannt. Die DPS könnten im Datenmodell der smartLogic als Gleisabschnitt modelliert werden (vgl. Kapitel 7.3.3, Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)“).

Zum anderen existiert bei verzweigenden Fahrwegelementen wie Weichen eine topologische Ausdehnung der Fahrwegelemente, die das Ausmaß der Überlappung der Grenzlinien bzw. des Lichtraumprofils und damit auch der gleichzeitigen Nutzung des stellbaren Fahrwegelements repräsentiert.[35] Die RCA-Gruppe nennt diese Gleisabschnitte „**Allocation Sections**“ (AS) (vgl. Kapitel 2.4.4, neuerdings existiert auch die Bezeichnung „**Allocation Area**“ (AA)). AS könnten im Datenmodell der smartLogic in Form mehrerer gekoppelter Gleisabschnitte gemäß der Definition in Kapitel 7.3.5 modelliert werden. Jeder dieser Gleisabschnitte würde dabei sowohl als Wirkbereich, als auch als Detektionsbereich dienen. Wird ein Abschnitt belegt, schließt er damit die Belegung der gekoppelten Abschnitte aus. Nähere Informationen zur Thematik der Grenzlinien und des Lichtraumprofils enthält Kapitel 7.3.9. Die AS eines stellbaren Fahrwegelements müssen nicht dieselbe topologische Ausdehnung wie die entsprechende DPS haben (siehe auch Kapitel 2.4.4)[36].

Abb. 52 wiederholt die Darstellung von Abb. 7 in Kapitel 2.4.4 und zeigt die beiden in Zusammenhang mit der Modellierung eines stellbaren Fahrwegelements auftretenden Arten von Gleisabschnitten am Beispiel einer einfachen Weiche. Die roten Linien stellen die AS dar, die grünen Linien die DPS.

[35] Bei Weichen wird die topologische Ausdehnung der AS üblicherweise durch den Weichenanfang und das Grenzzeichen markiert.

[36] Bei der Weiche wäre die DPS beispielsweise der Bereich zwischen dem Beginn der Zungen und dem Ende des Herzstücks oder bei der beweglichen Brücke der im geöffneten Zustand nicht befahrbare Teil.

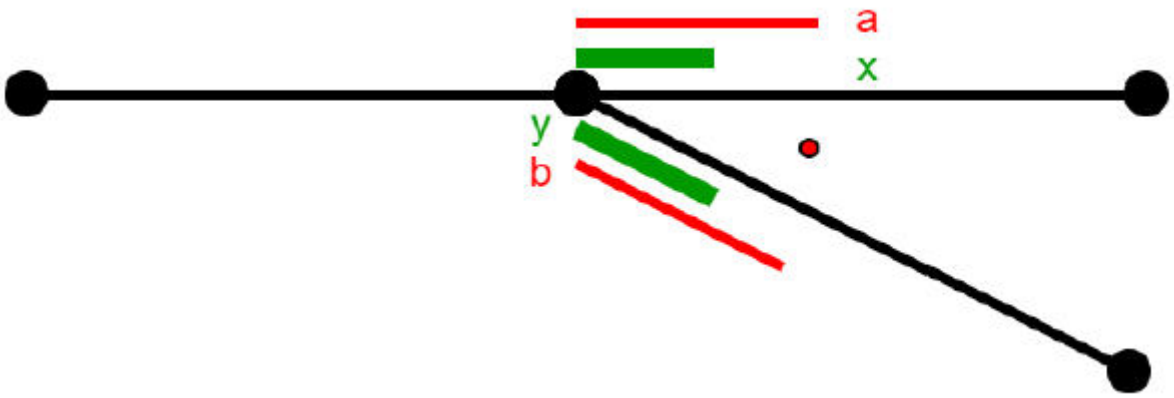


Abb. 52: Allocation Section und Drive Protection Section bei einer einfachen Weiche
Quelle: [ERTMS Users Group & EULYNX 2020a]
Die roten Linien zeigen die beiden gekoppelten AS, die sich vom Weichenanfang am Verzweigungspunkt der Topologie bis zum Grenzzeichen erstrecken. Die grünen Linien markieren die kürzeren DPS, die sich dort befinden, wo aufgrund der Lage der Weiche (also des Status des stellbaren Fahrwegelements) die Befahrbarkeit nicht gegeben ist. Die gezeigte Weiche hat derzeit in keiner Lage Endlage, da in beiden Strängen DPS existieren.

Alternativ zur Vorgehensweise der RCA könnten die beiden erwähnten Arten von Gleisabschnitten (DPS und AS) im Sinne der Anforderung der *schlanken Logik* auch zusammengefasst werden. Denkbar wäre ein Zusammenschluss, da sowohl eine DPS als auch eine AS die Befahrbarkeit des entsprechenden Gleisabschnitts ausschließen. Der kombinierte Abschnitt dürfte nicht befahren werden, wenn entweder einer der gekoppelten Abschnitte von einer Fahrzeugbewegung beansprucht wird (vgl. hierzu Kapitel 7.6) oder das stellbare Element nicht den erforderlichen Status hat, also z. B. bei einer Weiche nicht die entsprechende Endlage.

Die Modellierung in nur einem zusammengefassten Element hätte zwar zunächst weniger Komplexität, als die getrennte Modellierung mit DPS und AS, allerdings konnten auch zwei Nachteile erkannt werden.

1. Eine leicht negative Auswirkung auf die Kapazität bei verzweigenden Fahrwegelementen wäre möglich, da die kürzeren DPS in den längeren AS aufgehen müssten. Dieser Effekt ist jedoch vermutlich eher gering, da es sich in den meisten Fällen nur um wenige Meter Differenz handeln wird.
2. Der zweite Nachteil ist konzeptioneller Natur. Würden die Betrachtung von Verletzung der Fahrzeugbegrenzungslinien und der Einschränkung der Befahrbarkeit abhängig vom Status des stellbaren Fahrwegelements in einer Information zusammengefasst, könnte keine differenzierte Modellierung von reinen Grenzlinienverletzungen (z. B. bei Kreuzungen, vgl. auch Kapitel 7.3.9) oder reinen statusabhängigen Befahrbarkeitseinschränkungen wie bei Sperrelementen ohne das Vorsehen neuer Objekttypen erfolgen. Da die AS aufgrund ihrer Definition der natürliche Ausgangspunkt der Suche nach Flankenschutz sind (vgl. Kapitel 8.3.4), wären z. B. negative Auswirkungen auf die Bestimmung des Flankenschutzes möglich, wenn auch reine DPS durch das Zusammenfassen von AS und DPS unnötig miteinbezogen werden müssten.

Insbesondere aus dem ersten geschilderten Grund und entsprechend der Anforderung der *Migrationsfähigkeit*, wonach möglichst Standards übernommen werden sollen, wird im Folgenden auf die Modellierung der RCA mit getrennten DPS und AS zurückgegriffen.

Modellierung der Interaktion

In der Realität sind die Interaktionsobjekte nicht die stellbaren Fahrwegelemente selbst, sondern dazugehörige Object Controller, welche sie kontrollieren. Mit den Object Controllern kommuniziert die Sicherungslogik gemäß den Ausführungen in Kapitel 4.5.1 mittels geeigneter Nachrichten, die zu den EULYNX-Schnittstellen kompatibel sein sollten. Über diese Schnittstellen werden neben Aufrüstinformationen im Stadium der Initialisierung des stellbaren Fahrwegelements, im Wesentlichen Stellbefehle in Richtung der stellbaren Fahrwegelemente und Status-Updates aus Richtung der stellbaren Fahrwegelemente gesendet.

Alle stellbaren Fahrwegelemente haben gemeinsam, dass sie verschiedene Status haben. Da die Modellierung möglichst generisch erfolgen soll, erscheint es nicht sinnvoll, die jeweiligen Status für jedes Element einzeln zu modellieren. Eine generischere Herangehensweise wäre es, in der Topologie zu hinterlegen, mit welchem Status eine bestimmte topologische Verbindung befahrbar wird. Diese Verbindung wäre dann mit dem entsprechenden kontrollierbaren Fahrwegelement und dem dazugehörigen Status verknüpft. Für Rückfallebenen können weitere zulässige Status mit entsprechenden Einschränkungen definiert werden (vgl. Kapitel 8.3.6). Ein Status eines kontrollierbaren Infrastrukturelements bildet demnach ein eigenes Objekt, welches sowohl mit dem physischen Objekt als auch mit einem topologischen Verbindungsobjekt (Positioned Relation) aus dem topologischen Modell verknüpft ist. Abb. 53 zeigt das stellbare Fahrwegelement (Controlled Track Element) mit der generischen Status-Klasse.

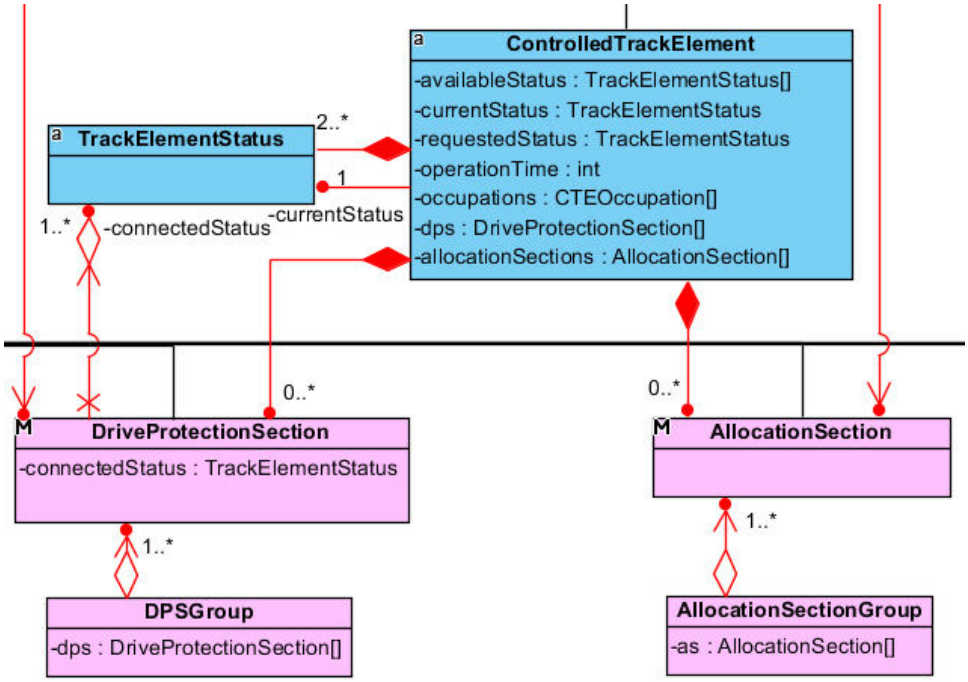


Abb. 53: Controlled Track Element und Track Element Status im Datenmodell (blau) mit Verknüpfung zur topologischen Repräsentation in Form der DPS und AS (rosa) [Eigene Darstellung]

7.4.4 mehrfachverzweigende Fahrwegelemente (einfache und doppelte Kreuzungsweichen)

Aufgrund ihrer Komplexität ist **mehrfachverzweigenden Fahrwegelementen** ein eigenes Unterkapitel gewidmet. Gemeint sind mit diesem generischen Begriff vor allem einfache und doppelte Kreuzungsweichen. Die Komplexität entsteht vor allem dadurch, dass aufgrund der existierenden

Technik im Feld ggf. mehrere Object Controller angesteuert werden müssen und es mehrere topologische Verzeigungspunkte gibt (bei der einfachen Weiche, gibt es nur eine topologische Verzweigung). Wie in den vorhergehenden Kapiteln erläutert, werden ausgehend vom RCA-Modell in Hinblick auf die Modellierung von stellbaren Fahrwegelementen (vgl. Kapitel 7.4.3) im Datenmodell für die smartLogic diese beiden Eigenschaften von mehrfachverzweigenden Fahrwegelementen getrennt betrachtet.

Modellierung der topologischen Ausdehnung

Topologisch gesehen werden die vier Enden der DKW als vier Verzweigungen der Topologie gesehen. Folglich existiert für den Schienenstrang zwischen den Enden jeweils ein topologisches Knotenobjekt (vgl. [Gély et al. 2010, S. 200]). Auf jedem dieser Schienenstränge existiert eine Verletzung der Grenzlinien, die von der Beanspruchung eines der drei anderen Schienenstränge abhängt. Demensprechend existieren vier AS, die miteinander verknüpft sind. Schließlich existiert für jede potenzielle Endlage eines Zungenpaares eine DPS, die dann deaktiviert wird, wenn das zugehörige Zungenpaar sich in dieser Endlage befindet.

Abb. 54 verdeutlicht die verschiedenen beschriebenen Objekte bei der doppelten Kreuzungsweiche. Das beschriebene Vorgehen kann auch analog bei weiteren mehrfachverzweigenden Fahrwegelementen angewandt werden.

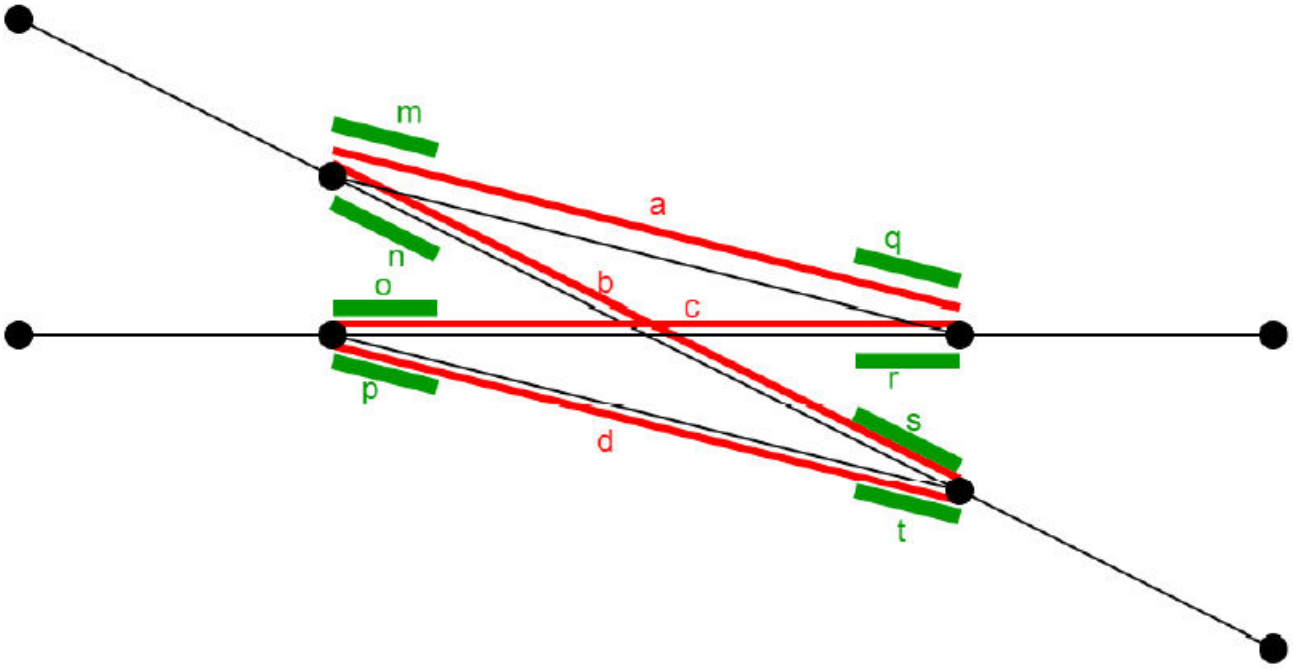


Abb. 54: Modellierung einer doppelten Kreuzungsweiche
Quelle: [ERTMS Users Group & EULYNX 2020a]

Modellierung der Interaktion

Für die Ansteuerung kann eine doppelte Kreuzungsweiche beispielsweise aus zwei „Object Controller"-Objekten bestehen oder aus einem einzigen. Hintergrund ist, dass heute zur Komplexitätsreduktion komplexe Elemente häufig in mehrere einfache Elemente aufgeteilt werden, da eine DKW z. B. nicht wie einfache Weichen nur eine Rechts- und Linkslage als Solllagen hat. Der RCA-Architektur folgend erfolgt die Ansprache allerdings über die „Object Transactors", wo eine Übersetzung auf die tatsächlichen Object Controller stattfinden kann.

Für die Sicherungslogik an sich wird eine Aufteilung auf mehrere Elemente jedoch nicht benötigt. Die Modellierung mit den verknüpften Status macht eine solche Aufteilung überflüssig, da beliebige Status definiert werden können (im Falle einer doppelten Kreuzungsweiche z. B. {links links; links rechts; rechts links; rechts rechts}). Hierfür ist es nur erforderlich, dass das TMS, die Infrastrukturmodellierung und der Object Controller die verfügbaren Status kennen. Die Logik selbst prüft dann einfach, ob der angeforderte Status dem tatsächlichen Status entspricht und ob es mit diesem Status eine gültige Route gibt, über welche eine Fahrt abgewickelt werden kann. Komplexere Elemente wie DKW können daher im Datenmodell der smartLogic als ein stellbares Fahrwegelement modelliert werden.

7.4.5 nicht kontrollierbare, Grenzlinien-verletzende Fahrwegelemente

Wie in den vorigen Kapiteln erläutert, überlappen sich bei verzweigende Elementen der Gleisinfrastruktur wie Weichen die Grenzlinien der Gleise kurz vor ihrer Vereinigung. Daraus ergibt sich eine Einschränkung für die Befahrbarkeit des einen Gleises, wenn das andere Gleis beansprucht ist. Dies trifft auch auf weitere Elemente der Gleisinfrastruktur zu, die jedoch nicht stellbar sind und damit für die Fahrzeuge keinen wählbaren Fahrweg bieten.

Hierzu gehören vor allem Kreuzungen. Bei diesen kann ebenfalls mittels des RCA-Prinzips der Allocation Sections ein gegenseitiger Ausschluss der gleichzeitigen Befahrbarkeit modelliert werden. Dasselbe kann theoretisch auch für einfache Gleise gelten, an denen das topologische Netz sich nicht verzweigt oder kreuzt, die aber dennoch einen gegenseitigen Ausschluss gleichzeitiger Fahrten bedingen, z. B. Gleisverschlingungen.

Diese Informationen können jedoch über das topologische Modell vollständig abgebildet werden, so dass kein Bedarf einer zusätzlichen Modellierung im Infrastrukturmodell gesehen wird.

7.4.6 statische Infrastrukturelemente am Gleis

Weitere Infrastrukturelemente finden sich am Gleis, sind aber nicht Teil des Gleises. Für das Datenmodell der smartLogic sind davon jedoch nur solche Elemente relevant, auf die die Kriterien aus Kapitel 7.4.1 zutreffen. Da die statischen Elemente nicht stellbar sind, ist das erste Kriterium nicht erfüllt. Einige Elemente können allerdings ortsgebundene Informationen definieren. Beispielsweise wäre es denkbar, dass zukünftig die Position der Bahnsteige übermittelt werden muss, damit ATO-geführte Fahrzeugbewegungen die Türen nur dort öffnen.

Die Eigenschaften solcher statischen Elemente können im Infrastrukturmodell beschrieben werden und über „Spot Locations“ (bei punktförmig wirkenden Informationen) oder Gleisabschnitten mit dem topologischen Modell verknüpft werden.

7.4.7 externe Systeme am Gleis

Eine weitere wichtige Gruppe bilden Elemente, die aus dem Blickwinkel der smartLogic externe Systeme sind, mit denen kommuniziert wird. Hierzu gehören z. B. Bahnübergänge, aber auch Messeinrichtungen und Rotten-Warngeräte. Sie können in mehrere Gruppen eingeordnet werden, die je nach Gruppe unterschiedliche Anforderungen an die Sicherungslogik stellen, zum Beispiel zustimmungspflichtige Elemente, die vor Erteilung der Zustimmung topologisch eine aktive DPS bilden. Weiterhin können sie mehrere Referenzen auf die Topologie haben. Zu unterscheiden sind insbesondere Detektionsabschnitt und Wirkabschnitt (vgl. Kapitel 7.3.5).

Nähere Informationen zur Thematik der „externen Systeme“, der Abgrenzung zu den Stellelementen und dem zugrundeliegenden Stakeholder-Registrierungs-Konzept sowie eine Herleitung dieses Konzepts enthält Kapitel 8.3.3.

7.5 Fahrzeugmodell

Das dritte Teilmodell des Datenmodells für die smartLogic ist das Fahrzeugmodell. Dafür sind die für die smartLogic relevanten Fahrzeugeigenschaften zu identifizieren, die im Teilmodell abgebildet werden müssen.

Der Inhalt des Teilmodells kann zunächst aus den Anforderungen hergeleitet werden (Kapitel 7.5.1). Eine Vervollständigung kann über die Schnittstelle zum Fahrzeug (in dieser Arbeit wird von der ETCS-Schnittstelle ausgegangen, vgl. Kapitel 4.5.2) erfolgen (Kapitel 7.5.2). Die Betrachtung weiterer Fahrzeugmodelle erscheint nicht sinnvoll, da ohnehin nur die in der Schnittstellenspezifikation übermittelten Daten zwischen Fahrzeug und Sicherungslogik übertragen werden können, es sei denn es würde ein aufwändiger Change Request für die Schnittstelle gestellt (vgl. Kapitel 2.2.2). Letzteres müsste allerdings durch die Anforderungen (siehe Kapitel 7.5.1) begründet werden.

7.5.1 Erforderliche Fahrzeugeigenschaften gemäß Anforderungen an die smartLogic

Mehrere globale Anforderungen beziehen sich auf die Fahrzeuge bzw. die Fahrzeugbewegungen. So sollen *unnötige Bremsvorgänge vermieden* und den Fahrzeugen *maximaler Freiraum* gewährt werden. Weiterhin sollen sie mit *maximal möglicher Geschwindigkeit* verkehren können sowie die Infrastruktur nur *minimal beanspruchen* und *frühestmöglich* [wieder] *freigeben* (vgl. Kapitel 3.5 und 7.2.1).

Die Arbeitsteilung zwischen Fahrzeugen und infrastrukturseitiger Sicherungstechnik wurde in Kapitel 4.3.2 ausführlich diskutiert. Demnach sind die Fahrzeuge für das Einhalten ihrer Fahrerlaubnis selbst verantwortlich. Genaueres Wissen über Beschleunigungs- und Bremseigenschaften der Fahrzeuge ist daher für die Sicherungslogik nicht erforderlich (anders als für das TMS, welches die Fahrzeugbewegung zur sinnvollen Disposition vorausprojizieren muss). Fahrzeuge können daher generisch mit einigen wenigen spezifischen Eigenschaften modelliert werden.

Um eine minimale Beanspruchung der Infrastruktur zu erreichen, ist eine möglichst genaue Information der Fahrzeug- bzw. Zuglänge erforderlich. Ebenfalls ist das Lademaßprofil relevant, um Profilüberschreitungen und damit Auswirkungen auf benachbarte Gleise erkennen zu können.

Hinter der Anforderung nach maximalen Freiraum für die Fahrzeuge verbirgt sich die Anforderung, dass die Fahrzeuge durch die Sicherungslogik nur möglichst wenig eingeschränkt werden sollten. Hierfür ist es sinnvoll, dass Beschränkungen aufgrund von Sicherheitsvorgaben nur für die Fahrzeuge gelten, für die oder durch die eine Gefährdung besteht. Um dies zu erreichen, ist es sinnvoll Fahrzeuge nach bestimmten Kategorien zu unterscheiden und im Falle von Gefährdungen für bestimmte Fahrzeugkategorien, Fahrerlaubnisse für Fahrzeuge anderer Kategorien dennoch zuzulassen.

7.5.2 übermittelbare Fahrzeugeigenschaften gemäß ETCS-Spezifikation

Die ETCS-Schnittstellenspezifikationen definieren verschiedene Pakete, mit denen Daten vom Fahrzeug an die Infrastruktur und damit die smartLogic übermittelt werden können (vgl. [ERA 2016]). Dabei ist insbesondere das fahrzeugseitige Paket 11 „Validated Train Data“ relevant. Tab. 32 enthält eine Übersicht der ETCS-Fahrzeugdaten mit einer Einordnung ihrer Bedeutung für die smartLogic. Als „nicht relevant“ bewertete Informationen sind kursiv dargestellt.

Tab. 32: Relevanz der ETCS-Fahrzeugdaten für smartLogic

„Validated Train Data"-Variable	Beschreibung	Relevanz für smartLogic
NC_CDTRAIN	Überhöhungsfehlbetrag	ggf. relevant für Unterscheidung der Zulässigkeit einer Fahrerlaubnis
NC_TRAIN	internationale Zugart	ggf. relevant für Unterscheidung der Zulässigkeit einer Fahrerlaubnis
L_TRAIN	Länge	relevant, wird jedoch später durch Ortungsinformationen ersetzt (siehe Kapitel 7.6.1)
V_MAXTRAIN	*Höchstgeschwindigkeit*	*nicht relevant, da das Fahrzeug selbst für deren Einhaltung verantwortlich ist*
M_LOADINGGAUGE	Lademaßprofil	relevant für Beanspruchung der Infrastruktur
M_AIRTIGHT	Ausstattung des Fahrzeuges mit drucksicheren Klimaklappen (kann bei Tunnelfahrten wichtig sein)	ggf. relevant für Unterscheidung der Zulässigkeit einer Fahrerlaubnis
N_AXLE	*Anzahl der Achsen des Triebfahrzeugs*	*nicht relevant (nur für Ortung)*
M_VOLTAGE (k) & NID_CTRACTION (k)	unterstützte Stromsysteme	ggf. relevant für Unterscheidung der Zulässigkeit einer Fahrerlaubnis
NID_NTC (k)	*unterstützte Zugbeeinflussungssysteme*	*nicht relevant auf Ebene der Sicherungslogik*

7.6 Modell der Fahrzeugbewegungen

Im Modell der Fahrzeugbewegungen werden gemäß Kapitel 7.2.2 die Teilmodelle Infrastruktur und Fahrzeug miteinander verbunden. Zum Teilmodell gehören auch alle mit der Fahrzeugbewegung verbundenen Eigenschaften, wie ihre aktuelle Fahrerlaubnis und die dazugehörigen Beanspruchungen der Infrastruktur (= dynamische Gleisabschnitte).

Zur Repräsentation der Fahrzeugbewegungen ist ein Objekttyp erforderlich, der eine Assoziation zu den entsprechenden Fahrzeugobjekten hat. U. a. zur Vermeidung von Kollisionen ist für die Sicherungslogik die Modellierung der aktuellen Position des Fahrzeuges von besonderer Relevanz. Hiermit beschäftigt sich Kapitel 7.6.1. Die aktuelle Position des Fahrzeuges ist jedoch nicht der einzige Bereich der Gleistopologie, der von der Fahrzeugbewegung beansprucht wird. Mit der Modellierung der notwendigen Beanspruchungen beschäftigt sich daher Kapitel 7.6.2. Während Position und Beanspruchung den Ist-Zustand abdecken, muss der im Rahmen einer Fahrerlaubnisanfrage zu prüfende zukünftige Soll-Fahrweg (Route) ebenfalls definiert werden. Dies erfolgt in Kapitel 7.6.3.

7.6.1 Modellierung der Position der Fahrzeugbewegung

Um die Fahrzeugposition zu beschreiben, ist zunächst zu klären, in welchem Koordinatensystem die Position verortet wird (erster Abschnitt). Da die Fahrzeuge und damit die Fahrzeugbewegungen nicht punktförmig sind, muss anschließend hergeleitet werden, durch welche Punkte die Ausdehnung der

Position begrenzt wird (zweiter Abschnitt). Bei der Ortung kann die Position des Fahrzeugs jedoch nur mit einer gewissen Ungenauigkeit ermittelt werden. Daher ist zu klären, wie mit der Ortungsungenauigkeit umgegangen wird (dritter Abschnitt). In der Praxis ist die Ausdehnung der Fahrzeugbewegung sogar dreidimensional. Dabei werden jedoch üblicherweise zwei Dimensionen über die statischen Fahrzeugbegrenzungslinien abgedeckt (vgl. Kapitel 7.3.9). Ob eine Berücksichtigung dieser beiden Dimensionen im Rahmen der Positionsbestimmung der Fahrzeuge sinnvoll ist, wird im vierten Abschnitt betrachtet. Die Vollständigkeit der analysierten Fragestellungen zeigt sich wiederum bei der Verhaltensmodellierung.

Koordinatensystem für die Positionsangabe

Die Position der Fahrzeuge bzw. der Fahrzeugbewegung kann theoretisch auf mehrere Arten angegeben werden. Zu unterscheiden sind

- die ***absolute Position*** und
- die ***relative Position***.

Die *absolute Position* gibt einen eindeutigen Standort in einem Koordinatensystem an (z. B. als Koordinaten in einem GEO-Koordinatensystem oder als absoluten Punkt auf einer Topologie).

Die *relative Position* ist nicht eindeutig, sondern bezieht sich auf einen Referenzpunkt, der eine absolute Position hat. Beispielsweise kennen Fahrzeuge bei ETCS nur relative Positionen (bisher mit Referenzpunkt zu einer Balisengruppe). Auf diesen Referenzpunkt werden alle übermittelten Positionen bezogen, z. B. die Länge einer Fahrerlaubnis. Um daraus die absolute Position zu ermitteln, muss beispielsweise der eingestellte Fahrweg bekannt sein.

Die relative Position hat damit den Vorteil, dass sie wesentlich einfacher zu bestimmen ist (beispielsweise mittels Odometrie). Sie kann immer dort eingesetzt werden, wo keine weiteren Positionsangaben zu verarbeiten sind, die nicht auf den relativen Bezugspunkt bezogen werden können. Für die Übersicht über die Beanspruchung muss die Sicherungslogik jedoch die absolute Position der Züge kennen. Es wird daher davon ausgegangen, dass die Position als absolute Position vom Ortungsinformationsaggregator übertragen wird.

Bestimmung der Ausdehnung der Position

Da das Fahrzeug bzw. die Fahrzeugbewegung keine Punktobjekte sind, ist zu klären, wie dessen volle Ausmaße definiert werden. Dabei konnten mehrere Möglichkeiten identifiziert werden:

1. Die Ausmaße können anhand der Fahrzeugdaten (Länge, Begrenzungslinien) mittels eines Referenzpunktes berechnet werden. Als Referenzpunkt hat sich die Zugspitze etabliert (vgl. z. B. ETCS und RCA), also der Punkt, der in Fahrtrichtung den vordersten Punkt der Fahrzeugbewegung markiert.
2. Die Ausmaße werden durch die Angabe mehrerer Positionen bestimmt. Dafür bietet sich neben der Zugspitze auch das Zugende an.

Ein Problem bei der ersten Möglichkeit ergibt sich, wenn die Fahrzeugbewegung bzw. das Fahrzeug steht und damit keine aktuelle Fahrtrichtung hat. Dieses Problem wird in bestehenden Modellen, z. B. bei ETCS, damit gelöst, dass die letzte bekannte Fahrtrichtung übernommen wird, falls diese Richtung bekannt ist. Falls diese Richtung nicht bekannt ist, kann die Position der Zugspitze nicht eindeutig zugeordnet werden.

Um mit dem Referenzpunkt die Ausmaße bestimmen zu können, müssen die Fahrzeugdaten bekannt sein und im Falle der Sicherungslogik als sicherungskritisches System aus einer sicheren Quelle

vorliegen. Bei der Länge stellt sich zudem das bereits beschriebene Problem, dass sie bei Zügen je nach Streckung schwanken kann. Um in Hinblick auf eine mit der Fahrzeugposition verbundene Beanspruchung der Infrastruktur die Sicherheit zu gewährleisten, müsste im Schwankungsbereich eine hohe Länge angenommen werden. Ein weiteres Problem in Bezug auf die Länge ist eine mögliche Zugtrennung, die sich ebenfalls auf die Länge des Zuges auswirkt. Eine solche Zugtrennung müsste erkannt und berücksichtigt werden. In ETCS ist daher vorgesehen, dass vom Fahrzeug übermittelt werden kann, ob die Zugintegrität sicher vorhanden ist.

Die zweite Möglichkeit hat dann Vorteile gegenüber der einfachen Berechnung aus der Zuglänge, wenn die Position des Zugendes aus einer sicheren Quelle vorliegt. Ist das nicht der Fall, hat die Modellierung über die Angabe des Zugendes allerdings auch keinen Nachteil gegenüber der Ermittlung über die Länge, denn die Zugende-Position kann auch aus der Angabe der Länge jederzeit mit den genannten Unsicherheitsfaktoren ermittelt werden.

Für die Anwendung in der smartLogic stellt daher die Modellierung der Ausmaße des Zuges in der Längsrichtung über die Angabe der Zugspitze und des Zugendes die vielfältiger einsetzbare Möglichkeit dar und wird deshalb bevorzugt.

Sind die absoluten Positionen von Zugende oder Zugspitze bekannt, ist die Gesamtposition der Fahrzeugbewegung jedoch noch nicht eindeutig beschrieben, da es mehrere mögliche topologische Verbindungen zwischen diesen beiden Positionen geben kann (vgl. Abb. 55) (dieses Problem würde auch bei Berechnung über die Länge auftreten). Handelt es sich bei der Fahrzeugbewegung um eine bekannte Fahrzeugbewegung, kann der genaue Laufweg mittels des eingestellten Fahrweges bestimmt werden.

Abb. 55: Unklarheit über Ausdehnung der Fahrzeugbewegung bei unklarem Laufweg
[Eigene Darstellung]

Entsteht ein neues Fahrzeugbewegungsobjekt und die Fahrzeugbewegung fährt nicht von einer Grenze des Betrachtungsraums in den smartLogic-kontrollierten Bereich über einen eingestellten Fahrweg hinein, muss zur Feststellung der Eindeutigkeit des Fahrweges geprüft werden, ob es mehrere befahrbare Verbindungen zwischen den beiden Positionspunkten gibt. Ist Letzteres der Fall kann die Position nicht eindeutig bestimmt werden. Für eine weitere Betrachtung dieser Problematik wird auf Kapitel 8.4.2 verwiesen.

Umgang mit der Ortungsungenauigkeit

Die Position der Fahrzeuge bzw. der Fahrzeugbewegung kann über die Angabe als Gleisabschnitt (vgl. Kapitel 7.3.3) präzise verortet werden. In der Realität liegen aufgrund von Ortungsungenauigkeiten die Informationen über die Positionen der Zugspitze und des Zugendes jedoch nicht so präzise vor. Für die Bestimmung der Ausdehnung des entsprechenden Gleisabschnitts muss die Position der Fahrzeugbewegung zur sicheren Seite abgeschätzt werden.

In Kapitel 2.2.2 wurde der Umgang mit der Ortungsungenauigkeit bei ETCS besprochen. Die ETCS-Spezifikation spricht in diesem Zusammenhang vom „Max Safe Front End“ und „Min Safe Rear End“, also dem Punkt, an dem die Zugspitze mit hinreichender Wahrscheinlichkeit maximal bereits sein kann, und dem Punkt, den das Zugende mindestens bereits passiert haben muss. Diese Definitionen beziehen sich zwar auf eine fahrende Fahrzeugbewegung, können aber analog auch auf stehende

Fahrzeuge angewandt werden, falls zumindest eine Richtung bekannt ist (siehe oben). In anderen Fällen muss der Gleisabschnitt zwischen den initial als Position übermittelten Punkten festgelegt werden.

Es muss davon ausgegangen werden, dass auch ein Ortungsinformationsaggregator die Zugposition in einem Intervall angeben wird, wenn auch möglicherweise mit höherer Genauigkeit als bei rein fahrzeugseitiger Ortung. Aus Sicherheitsgründen muss die smartLogic für die Begrenzung der Ausdehnung der Fahrzeugbewegung, wie bei ETCS, auf die sicheren Angaben „Min Safe Rear End“ und „Max Safe Front End“ zurückgreifen.

Fahrzeugbegrenzungslinien

Da Eisenbahnfahrzeuge dreidimensionale Objekte sind, wäre es denkbar, auch die theoretisch veränderlichen Fahrzeugbegrenzungslinien (Grenzlinien) zur Position zu zählen. Da sich bei den Grenzlinien die Ausmaße nicht kontinuierlich, sondern nur im Ausnahmefall (z. B. verrutschte Ladung) ändern, werden die Grenzlinien an dieser Stelle als während der Fahrt unveränderliche Eigenschaft der Fahrzeugbewegung und damit für die Position irrelevant angenommen. Die Detektion einer Änderung der angegebenen Grenzlinien wird als außergewöhnliches Ereignis angenommen, welches von einem externen System gemeldet wird und eine Reaktion der Sicherungslogik auslöst (vgl. hierzu Kapitel 8.7 und zur Modellierung der Grenzlinien allgemein Kapitel 7.3.9.). An dieser Stelle wird daher auf die Grenzlinien nicht weiter eingegangen.

7.6.2 Modellierung von Beanspruchungen der Infrastruktur

Fahrzeugbewegungen beanspruchen die Infrastruktur. Man könnte auch von Belegungen sprechen, jedoch verbindet sich mit diesem Begriff klassischerweise ein exklusiver Anspruch auf das mit der Belegung verknüpfte Infrastrukturelement bzw. auf den Freimeldeabschnitt, der nicht unreflektiert für die Modellierung der smartLogic übernommen werden soll. Daher wird für die smartLogic die etwas generischere Formulierung bevorzugt, wonach Infrastrukturressourcen Fahrzeugen zur exklusiven Nutzung oder mit entsprechenden Auflagen bzw. Einschränkungen zur teilweisen Nutzung überlassen werden können und damit von diesen beansprucht werden. Der Begriff „Beanspruchung“ ist nicht neu. Auch Maschek spricht z.B. davon, dass Infrastrukturelemente „beansprucht“ werden können [Maschek 2018].

Das vorliegende Kapitel beschäftigt sich mit der Modellierung der fahrzeugbewegungsspezifischen **Beanspruchungen** der Infrastruktur. Dazu soll im ersten Abschnitt geklärt werden, welche fahrzeugbewegungsspezifischen Beanspruchungen notwendig sind. Anschließend kann im zweiten Abschnitt festgelegt werden, wie diese Beanspruchungen im Datenmodell abgebildet werden können.

Notwendige fahrzeugspezifische Beanspruchungen der Infrastruktur

In den nachfolgenden Unterabschnitten sollen die einzelnen notwendigen fahrzeugspezifischen Beanspruchungen schrittweise hergeleitet werden.

Beanspruchung der Fahrzeugbelegung (Vehicle Occupation, Clearance Gauge Violation Occupation)

Der Begriff „Infrastrukturressource“ ist im obigen Kontext abstrakt zu verstehen und kann sich auf verschiedene Elemente der Infrastruktur beziehen, vor allem gehört dazu die Gleisinfrastruktur. Zunächst existiert die tatsächliche physische Belegung durch das Fahrzeug an seiner aktuellen Position (vgl. Kapitel 7.6.1, im Datenmodell als „Vehicle Occupation“ bezeichnet). Erstreckt sich die Belegung

zusätzlich auf ein Nachbargleis (bei Fahrten mit Lademaßüberschreitung), ist auf diesem Gleis ebenfalls eine Beanspruchung (Clearance Gauge Violation Occupation) einzurichten.

Wie in Kapitel 7.6.1 erläutert, existieren immer Ortungsungenauigkeiten, aufgrund deren die exakte Position von Zugspitze und Zugende sich nicht bestimmen lassen und diese Ortungsungenauigkeiten führen zu einer Vergrößerung der notwendigen Ausdehnung der Beaspruchung zur Abbildung der physischen Belegung, die für die Fahrzeugbewegung zur exklusiven Nutzung freigehalten werden muss. Für eine effiziente Ausnutzung der Infrastruktur ist daher eine solide Ortungstechnologie erforderlich.

Beanspruchung der Fahrerlaubnis (MA Occupation)

Außer der tatsächlichen Belegung durch das Fahrzeug inkl. Ortungsungenauigkeit muss zur sicheren Abwicklung der Fahrzeugbewegung auch der Bremsweg exklusiv beansprucht werden. Gemäß der in Kapitel 4.3.2 hergeleiteten Arbeitsteilung zwischen Fahrzeug bzw. Fahrzeugbewegung und smartLogic ist die Fahrzeugbewegung für die Einhaltung ihres Bremsweges innerhalb der Fahrerlaubnis verantwortlich. Daher muss der Bremsweg immer in der Fahrerlaubnis enthalten sein.

Damit nicht permanent eine neue Fahrerlaubnis beantragt werden muss, kann die Fahrerlaubnis über den erforderlichen Bremsweg inkl. Systemreaktions- und Übertragungszeit hinausgehen. Der Fahrzeugbewegung wird dadurch erlaubt, den entsprechenden Teil des Gleises zu nutzen, und es muss davon ausgegangen werden, dass die Fahrzeugbewegung das auch tut[37], z. B. im Falle eines Kommunikationsabbruchs. Daher muss der gesamte in der Fahrerlaubnis freigegebene Teil des Gleises vom der Fahrzeugbewegung exklusiv beansprucht werden. Hierfür wird im Datenmodell eine entsprechende „MA Occupation“ vorgesehen.

Die MA Occupation benötigt auch einen Startpunkt. Dieser muss vor der Zugspitze liegen, damit kein Bereich ohne Fahrerlaubnis vor der Zugspitze liegt. Da sich Estimated Front End und Max Safe Front End bei Aktualisierungen der Ortungsinformation auch entgegen der Fahrtrichtung bewegen könnten, könnte bei Wahl dieser Punkte als Startpunkt der MA eine solche Lücke zwischen aktueller Fahrzeugposition und MA entstehen. Es erscheint daher sinnvoll, die MA am Min Safe Front End beginnen zu lassen.

Beanspruchung des Sicherheitsabstands (Safety Buffer Occupation)

Das Ende der Fahrerlaubnis wird innerhalb der Fahrerlaubnis relativ zum letzten bekannten Referenzpunkt als erlaubte Fahrstrecke bis zu einem Zielpunkt angegeben. Allerdings kann die ETCS-Fahrerlaubnis unterschiedliche solcher Zielpunkte enthalten (vgl. Abschnitt „Fahrerlaubnis (MA)“ in Kapitel 2.2.2). Hintergrund ist, dass der Bremsweg je nach Fahrzeugzusammensetzung, Bremskurvenmodell und Umgebungsbedingungen wie Witterungsverhältnissen sehr unterschiedlich sein kann und einen großen Einfluss auf die Kapazität hat (vgl. z. B. [Fehlauer & Kahl 2019; Feltz et al. 2017]). Um nicht unnötig früh mit der Bremsung beginnen zu müssen, kennt die klassische Eisenbahnsicherungstechnik das Prinzip des Durchrutschweges bzw. Gefahrpunktabstandes (vgl. Kapitel 2.1.1) hinter dem eigentlichen (als Ziel der Bremsung angesteuerten) Zielpunkt (bei ETCS die End of Authority (EoA)) als Sicherheitsabstand, das in ETCS über die Supervised Location (SvL) umgesetzt ist.

[37] Außer die Fahrzeugbewegung verzichtet auf dieses Nutzungrecht (siehe „MP Change Request“ in Kapitel 8.5.4).

Der Sicherheitsabstand zwischen EoA und SvL muss zwar ebenfalls für die Zugfahrt freigehalten werden, darf sich aber unter bestimmten Umständen mit dem Durchrutschweg einer anderen Fahrzeugbewegung überlappen. Hintergrund ist die Überlegung, dass es unwahrscheinlich ist, dass zwei Fahrzeuge zum gleichen Zeitpunkt einen außergewöhnlich verlängerten Bremsweg benötigen. Mit dieser Thematik beschäftigt sich das Kapitel 8.3.2 näher. Um die Zulässigkeit einer möglichen Überlappung schnell prüfen zu können, erscheint die Abgrenzung einer Beanspruchung für den Sicherheitsabstand sinnvoll. Für den Bereich bis zur EoA wird deshalb im Datenmodell eine „MA Occupation“ und für den Bereich zwischen EoA und SvL eine „Safety Buffer Occupation“ vorgesehen.

Beanspruchungen der stellbaren Fahrweglemente (CTE Occupation)

Für das Zustandekommen einer Fahrerlaubnis werden auch stellbare Fahrwegelemente mit einem bestimmten Status benötigt (z. B. Weichen in einer bestimmten Lage). Dabei stellt sich die Frage, ob für die stellbaren Fahrwegelemente ebenfalls Beanspruchungen im Datenmodell hinterlegt werden müssen oder ob sie über die Beanspruchungen der Gleisinfrastruktur bereits abgedeckt sind. Da es denkbar ist, dass es auch Beanspruchungen gibt, die nicht mit einer Beanspruchung eines mit dem Fahrwegelement verbundenen Gleiselements in Zusammenhang stehen (z. B. durch Bauarbeiten), erscheint es sinnvoll, auch bei den stellbaren Fahrwegelementen die Beanspruchung zu hinterlegen.

Flankenschutzbeanspruchungen (Flank Occupation, CTE Flank Occupation)

Auch für die Abbildung von Flankenschutz-Funktionen werden sowohl Gleissegmente (Flank Occupation) als auch stellbare Fahrwegelemente (CTE Flank Occupation) beansprucht (siehe Kapitel 8.3.4).

Beanspruchung während eines Prüfprozesses (Request Occupation)

Weiterhin können Infrastrukturelemente für interne Vorgänge, wie die Vorabreservierung bei Prüfung einer Prüfanfrage zur Gewährleistung der Transaktionssicherheit, beansprucht werden (Request Occupation, siehe Kapitel 8.5.3).

Abbildung von Beanspruchungen im Datenmodell

Die im vorigen Abschnitt beschriebenen Beanspruchungen müssen im Datenmodell mit den entsprechenden Elementen verknüpft werden. Dabei fordert eine spezielle Anforderung, dass *Beanspruchungen so präzise wie möglich angegeben werden können* (vgl. Kapitel 7.2.1).

Bezogen auf die Beanspruchungen der Gleisinfrastruktur sollten sich die Beanspruchungen daher nicht immer auf ein ganzes topologisches Element (Gleissegment) beziehen, sondern auch Teile davon umfassen können. Eine Beanspruchung der Gleisinfrastruktur kann daher als Gleisabschnitt im Sinne der Definition in Kapitel 7.3.3, Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)“ modelliert werden. Die Grenzen dieses Typs von Gleisabschnitt können mit der Nachricht über das Fortschreiten der Fahrzeugbewegung (neuer Position Report vom Fahrzeug bzw. gemäß der Architektur aus Kapitel 4.4.4 Ortungsinformations-aggregator) angepasst werden.

Wenn die Zulässigkeit einer neuen Beanspruchung (z. B. durch Ausstellen einer Fahrerlaubnis) geprüft werden soll, muss jedoch die Auffindbarkeit der Beanspruchungen ermöglicht werden. Hierzu bieten sich die Gleissegmente als grundlegendes Element der Gleistopologie an. Jedes Gleissegement muss

daher eine Liste aller mit ihm verknüpften Beanspruchungen mit dem jeweiligen Typ der Beanspruchung enthalten.

Bei den stellbaren Fahrwegelementen kann ebenfalls eine solche Liste mit den Beanspruchungen und dem jeweiligen Typ hinterlegt sein.

7.6.3 Modellierung des Fahrwegs des Zuges (Route)

Die Beanspruchung der Infrastrukturelemente durch Fahrzeugbewegungen kann, wie im vorigen Kapitel angesprochen, intern über verschiedene dynamische Abschnitte abgebildet werden. Bei einer Neubeantragung bzw. Verlängerung oder sonstigen Modifikation einer Fahrerlaubnis durch das TMS muss ebenfalls der geplante räumliche Verlauf über die Topologie festgelegt sein. Dieser zukünftige Fahrweg (hier inkl. Sicherheitsabstand hinter dem anzusteuernden Zielpunkt, siehe Kapitel 8.3.2) einer Fahrzeugbewegung wird im Folgenden zur Abgrenzung von anderen Bedeutungen des Begriffs „Fahrweg“ als „**Route**“ bezeichnet. Der Begriff „Route“ ist auch vom Begriff der „Fahrstraße“ aus der klassischen Stellwerkstechnik zu unterscheiden, da der Begriff der Fahrstraße beispielsweise auch Flankenschutzelemente umfasst (vgl. Kapitel 2.1.1).

Nachfolgend soll zunächst ein grundlegendes Modellierungskonzept für die Modellierung der Route festgelegt werden (erster Abschnitt). Anschließend muss für das gewählte Konzept geklärt werden, welche Daten vom TMS in welcher Güte übermittelt werden müssen (zweiter und dritter Abschnitt). Zudem ist festzulegen, wie diese Daten (also die Route) im Datenmodell gespeichert werden kann (vierter Abschnitt). Abschließend soll noch auf die Notwendigkeit eindeutiger Bezeichner für die Elemente der Route eingegangen werden, damit es beim Datenaustausch nicht zu Missverständnissen kommt (fünfter Abschnitt).

Modellierungskonzept

Für die Modellierung einer Route wurden aus den Konzepten der bisherigen Modellierung des Datenmodells sowie der Literatur zwei mögliche Methoden identifiziert, die nachfolgend näher betrachtet werden sollen:

1. Bei einer Route handelt es sich gemäß der Begrifflichkeiten der RCA immer um eine „Linear Contiguous Track Area“ (vgl. Kapitel 7.3.3, Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)“). Die Route könnte daher als Gleisabschnitts modelliert werden (ebd.). Das bedeutet, die Route würde aus einer Liste aus Gleissegmenten sowie zwei Spot Locations (intrinsische Koordinaten auf dem ersten und letzten Gleissegment) bestehen, die den Beginn und das Ende der Route markieren, die an beliebiger Stelle auf dem jeweiligen Gleissegment liegen können.
2. Alternativ könnte die Route mit der Hilfe von sogenannten Wegweisern festgelegt werden, wie es bei der XML_ISS geschieht (vgl. Kapitel 2.5.5). Ein **Wegweiser (Waypoint)** der Route stellt dabei ein stellbares Fahrwegelement mit seinem für die Route erforderlichen Status dar.

Da zum TMS noch keine festgelegte Schnittstelle existiert (vgl. Kapitel 4.5.3) (die Anforderungen einer solchen Schnittstelle wäre wegen der Anforderung der Nutzung von Standardschnittstellen relevant gewesen), kann die Entscheidung auf Basis einer Abwägung der Vor- und Nachteile erfolgen.

Um zu überprüfen, ob die stellbaren Fahrwegelemente den richtigen Status haben, benötigt die smartLogic die Wegweiser. Im Sinne der Anforderungen der schlanken Logik könnte daher

angenommen werden, dass es von Vorteil ist, wenn das TMS die Wegweiser bereits mit der Route übermittelt (Lösungsmöglichkeit 2), insbesondere da das TMS die Wegweiser ohnehin bereits ermittelt haben wird, um beispielsweise die Weichen vorher in die korrekte Lage bringen zu können (durch beantragen entsprechender Lageänderungen bei der smartLogic). Allerdings kann sich die Sicherungslogik auf sicherheitskritische Information von außerhalb des „SIL 4“-Bereichs (wo sich das TMS befindet) nicht verlassen und müsste für die Prüfung der beantragten Route die Wegweiser ohnehin neu bestimmen. Daher kann ebenfalls im Sinne der Anforderung der schlanken Logik auch das bereits bestehende Datenkonstrukt des Gleisabschnitts genutzt werden. Demnach wird Lösungmöglichkeit 1 weiterverfolgt.

Reihenfolge der Gleissegemente

Lösungsmöglichkeit 1 sieht vor, einen Gleisabschnitt bestehend aus einer Liste von Gleissegmenten zu übermitteln. Dabei ist zu klären, ob die Liste der Gleissegmente der Route

1. vom TMS geordnet vorgegeben werden muss oder
2. auch ungeordnet sein kann.

Für die erste Möglichkeit spricht die Anforderung der schlanken Logik, da bei dieser Möglichkeit die Überprüfung der korrekten Verknüpfung der Gleissegmente wesentlich einfacher als bei der zweiten Möglichkeit wird, weil nicht erst die korrekte Reihenfolge ermittelt werden muss. Für die zweite Möglichkeit spricht die Anforderung, wonach Prüfanfragen nur abgelehnt werden sollen, wenn die Kernanforderung der sicheren Logik nicht erfüllt ist. In diesem Fall scheint allerdings die Anforderung der schlanken Logik schwerer zu wiegen, da davon ausgegangen werden kann, dass das TMS die Liste ohne Probleme geordnet erzeugen kann. Es wird also im Folgenden davon ausgegangen, dass die Liste geordnet übergeben wird.

Beginn und Ende der Route

Neben den Gleissegmenten muss das TMS gemäß dem gewählten Modellierungskonzept Angaben zum Beginn und Ende der Route übermitteln, da diese beiden Punkte sich an jeder Stelle auf dem ersten bzw. letzten Gleissegement befinden können.

Der Beginn der Route muss sich an der aktuellen Position der betrachteten Fahrzeugbewegung befinden, damit für das gesamte von der Fahrzeugbewegung zu befahrende Gleis eine Fahrerlaubnis vorliegt. Durch Ortungsungenauigkeiten können sich bei der Aktualisierung der Ortungsinformationen Ortungspunkte der Fahrzeugbewegungsspitze entgegen der Fahrtrichtung zurückbewegen, wodurch auch das Belegungsobjekt der Fahrzeugbewegung kleiner werden würde (vgl. Kapitel 7.6.1). Daher erscheint es sinnvoll als Beginn der Route nicht das Max Safe Front End, sondern das Min Safe Front End zu verwenden, das den Ortungspunkt markiert, den das Fahrzeug mit sehr großer Sicherheit bereits passiert hat. Das Min Safe Front End sollte sich daher auch bei Aktualisierungen der Ortungsinformation nur in Fahrtrichtung des Zuges bewegen.

Das Ende der Route ergibt sich aus dem Zielpunkt mit der größten Distanz zur betrachteten Fahrzeugbewegung.

Speichern der beantragen Route im Datenmodell

Damit nicht mehrere Prüfprozesse Infrastrukturelemente während der Prüfung gegensätzlich beeinflussen (bspw. könnte sonst ein Prüfprozess zum Umstellen einer Weiche gleichzeitig geprüft werden, wie ein Prüfprozess, der dieselbe Weiche in einer bestimmten Lage benötigt), ist es naheliegend, die beantragte Route ebenfalls über Beanspruchungsobjekte zu speichern, Die

entsprechenden Beanspruchungsobjekte werden nachfolgend als „Request Occupation“ bezeichnet. Nach Bewilligung der beantragten MA durch die smartLogic wird die Request Occupation dann zu einer „MA Occupation“ und einer „Safety Buffer Occupation“ (vgl. Kapitel 7.6.2).

Notwendigkeit eindeutiger Bezeichner

Damit es nicht zu Missverständnissen zwischen TMS und smartLogic kommt, benötigen die einzelnen Gleissegmente des Gleisabschnitts eine einheitliche Bezeichnung, welche sowohl das TMS als auch die smartLogic aus der sicheren Datenquelle für die Topologiedaten (vgl. Kapitel 4.4.3) laden müssen.

7.7 Modellierung der Nachrichten

Mittels Nachrichten werden Informationen zwischen Systemkomponenten und zu den Umsystemen ausgetauscht. Um eine eindeutige Modellierung zu erreichen, ist es wichtig, dass für sie ebenfalls genau definierte Datenklassen existieren.

Eine globale Anforderung fordert, in der Kommunikation zu den Umsystemen möglichst eine Kompatibilität zu heutigen Systemen durch die Verwendung von Standardschnittstellen zu gewährleisten. Kapitel 4.5 beschäftigte sich bereits ausführlich mit den Schnittstellen zu den Umsystemen. Die Strukturen der dort beschriebenen Schnittstellenformate müssen nicht 1:1 in das Datenmodell der smartLogic übernommen werden, sondern es kann durchaus begründete Abweichungen geben. Wenn möglich, sollte jedoch zumindest der in der Standardschnittstelle geforderte Informationsumfang abgedeckt werden, um eine Kompatibilität zur Standardschnittstelle über einen Adapter herstellen zu können.

Aus Vereinfachungsgründen werden im Folgenden nur diejenigen Nachrichten näher beschrieben, die nicht identisch aus einer der Standardschnittstellen-Beschreibungen übernommen werden. Da noch keine Standardschnittstelle zwischen Sicherungslogik und TMS existiert, müssen die entsprechenden Nachrichten neu definiert werden (Kapitel 7.7.1). Weiterhin benötigt die Sicherungslogik Status Updates von Fahrzeugen und Infrastrukturelementen, um ihren Zustand zu aktualisieren (Kapitel 7.7.2). Auch die Kommunikation mit externen „Stakeholder-“Systemen ist zu definieren (Kapitel 7.7.3).

Zu jeder im Kapitel vorgestellten Nachricht existiert zunächst eine tabellarische Übersicht, die Informationen zum vorgesehenen Sender und Empfänger der Nachricht sowie den übermittelten Daten veranschaulicht. Weiterhin wird angegeben, welcher Prozess der Sicherungslogik durch die Nachricht ausgelöst wird (falls die smartLogic der Empfänger ist und es sich nicht um eine Antwortnachricht auf eine Nachricht der smartLogic handelt) bzw. welche(r) Prozess(e) die Nachricht auslösen können (falls die smartLogic der Sender ist). Der Umfang dieses Kapitels beschränkt sich auf die für die in Kapitel 8 beschriebenen Basis-Funktionen benötigten Nachrichten.

7.7.1 Kommunikation zwischen TMS und Sicherungslogik

Movement Permission Request (MP Request)

Tab. 33: Aufbau Movement Permission Request

Sender	TMS
Empfänger	smartLogic
spezielle Attribute	Fahrzeugbewegung; (beantragte) MA;

	Route
ausgelöster/auslösender Prozess	MP Request

Mit dem ***MP Request*** beantragt das TMS die Prüfung einer Fahrerlaubnis für ein Fahrzeug. Wie bereits in Kapitel 4.3.1 beschrieben wurde, ist die Sicherungslogik eine reine Prüfinstanz, d. h. alle Entscheidungen, wie über den einzustellenden Fahrweg und das Geschwindigkeitsprofil wurden bereits im nicht sicherheitskritischen TMS getroffen. Die Nachricht muss deshalb die komplette zu prüfende Fahrerlaubnis enthalten, die später an das Fahrzeug geschickt wird. Weiterhin die Referenz auf das Fahrzeug, für das die Fahrerlaubnis gedacht ist, und zusätzlich die Route, auf der das Fahrzeug verkehren soll, da letzterer aufgrund der Anforderungen von ETCS nicht Bestandteil der Fahrerlaubnis ist. Vergleiche zum Aufbau auch die Ausführungen in Kapitel 5 der Masterarbeit von GRAU [Grau 2018].

Der MP Request löst in der smartLogic einen MP-Prüfprozess aus, der in Kapitel 8.5.1 näher beschrieben wird.

MP Change Request

Tab. 34: Aufbau MP Change Request

Sender	TMS
Empfänger	smartLogic
spezielle Attribute	Fahrzeugbewegung; (neue) MA
ausgelöster/auslösender Prozess	MP Change Request

Der ***MP Change Request*** ähnelt dem MP Request. Da er immer eine Einschränkung der aktuellen MA eines Zuges vorsieht, muss nur die neue MA übertragen werden, aber nicht noch zusätzlich eine Route, da bereits eine Route besteht, die ggf. anhand der neuen Zielpunkte aus der neuen MA gekürzt werden kann.

Der MP Change Request löst in der smartLogic einen entsprechenden Prüfprozess gleichen Namens aus, der in Kapitel 8.5.4 näher beschrieben wird.

Track Element Status Change Request (TESC Request)

Tab. 35: Aufbau TESC Request

Sender	TMS
Empfänger	smartLogic
spezielle Attribute	stellbares Fahrwegelement neuer Soll-Status
ausgelöster/auslösender Prozess	TESC Request

Der ***TESC Request*** ist neben dem MP Request die zweite grundlegende Prüfanfrage, mit der das TMS Stellaufträge, also Statusänderungen von Infrastrukturelementen beantragt (z. B. Weiche umstellen). Im Vergleich zum MP Request ist er deutlich einfacher aufgebaut und enthält als spezielle Attribute nur die Referenz auf das betroffene Infrastrukturelement und den gewünschten Status.

Der TESC Request löst in der smartLogic einen TESC-Prüfprozess aus, der in Kapitel 8.5.5 näher beschrieben wird.

Erstellung, Anpassen oder Löschung eines (dynamischen) Gleisabschnitts (RA / URA) (RA Request)

Tab. 36: Aufbau RA Request

Sender	TMS
Empfänger	smartLogic
spezielle Attribute	RA
ausgelöster/auslösender Prozess	RA Request

Neben dem Senden von Fahrerlaubnisanfragen und Stellaufträgen kann das TMS auch die Voraussetzungen für die Genehmigung dieser Anfragen verändern, indem es (dynamische) Abschnitte auf der Topologie erstellt, anpasst oder löscht. Hierfür ist der ***RA Request*** vorgesehen. Das TMS kann dabei im Regelbetrieb nur Änderungen bei RAs (bzw. URAs) beeinflussen (vgl. dazu Kapitel 7.3.6). Als letzte manuelle Rückfallebene ist jedoch auch das Entfernen von DAs möglich. Hierfür ist es jedoch sinnvoll, eine gesonderte Nachricht zu definieren, die im Abschnitt „Manuelles Overwrite“ besprochen wird.

Die Nachricht muss die neue oder geänderte RA enthalten. Das RA-Objekt enthält ggf. die ID der bestehenden RA, die geändert oder gelöscht werden soll. Das Löschen der RA kann z. B. als einfachste Variante dadurch angezeigt werden, dass das RA-Objekt außer der ID der zu löschenden RA leer ist. Soll die RA neu angelegt oder geändert werden, sind alle dafür erforderlichen Angaben (vgl. Kapitel 7.3.6) im RA-Objekt enthalten. Weitere Informationen müssen der smartLogic nicht übermittelt zu werden.

Sollte aus Gründen fehlender Synchronisierung keine ID einer zu löschenden oder zu ändernden RA bekannt sein, kann das TMS die ID erfragen. Hierfür ist es wichtig, dass die smartLogic eine Liste mit existierenden RAs / URAs in einem bestimmten topologischen Bereich zusammenstellen und versenden kann. Eine solche Liste abzurufen stellt einen separaten Prozess dar, der über eine separate Nachricht ausgelöst werden muss. Da es sich eher um einen Spezialfall handelt, wird diese separate Nachricht hier nicht modelliert.

Wie in Kapitel 7.3.6 erwähnt, ist die Liste der möglichen Attribute der RA nicht als abgeschlossen zu betrachten, um für neue, zukünftige Technologien vorbereitet zu sein und den Charakter der generischen Logik zu erhalten. In diesem Sinne ist es möglich, die zur Verfügung stehenden Attribute über einen separaten Prozess zu verändern, der über eine separate Nachricht ausgelöst werden müsste. Auf diesen separaten Prozess wird hier aus Zeitgründen ebenfalls nicht näher eingegangen.

Der RA Request löst in der smartLogic einen RA-Prüfprozess aus, der in Kapitel 8.5.1 näher beschrieben wird.

Manuelles Overwrite

Das ***manuelle Overwrite*** dient bei schwerwiegenden Störfällen dazu, eine Blockade der smartLogic aufzulösen. Mit ihm können Aktionen ausgeführt werden, die in der Funktionsanalyse in Kapitel 6.6 als „Bedienfunktionen“ klassifiziert wurden. Trotz aller Automatisierung wird davon ausgegangen, dass es solch einen manuellen Mechanismus auch in Zukunft noch braucht. Ein Ziel der smartLogic ist aber, solche Bedienhandlungen möglichst zu vermeiden und im Vergleich zu heute noch deutlich zu reduzieren (vgl. globale Anforderungen der Automatisierung und Rückfallebenenintegration in Kapitel 3.5).

Die Nachricht muss das auszuführende Kommando mit entsprechender ID-Referenz auf die betroffenen Objekte enthalten. Sie löst jeweils einen entsprechenden Prüfprozess aus. Aufgrund der geringen Bedeutung für die eigentliche Logik, wird das Thema der manuellen Bedienung in dieser Arbeit jedoch nur kurz angerissen, so dass keine Modellierung der jeweiligen manuellen Bedienprozesse erfolgt.

Request Return Message (RRM)

Tab. 37: Aufbau Request Return Message (RRM)

Sender	smartLogic
Empfänger	TMS und „Hörer“ *(siehe Kapitel 8.3.3)*
spezielle Attribute	Ergebnis; (optional) Fehlercodes
ausgelöster/auslösender Prozess	alle Prüfprozesse

Die ***Request Return Message*** **(RRM)** ist die Antwortnachricht, welche die smartLogic nach einer vom TMS beauftragten Prüfung an dieses schickt. Sie hat ihren Ursprung in der Überlegung, dass die smartLogic im Falle einer erforderlichen Ablehnung einer Anfrage aus Gründen der schlanken Logik nicht selbst eine alternative mögliche Fahrmöglichkeit festlegen sollte, sondern dies durch das TMS vorgenommen werden sollte (vgl. Kapitel 4.3.1 und siehe Kapitel 8.3.1). Hierfür benötigt das TMS jedoch eine möglichst genaue, maschinell verarbeitbare und dadurch standardisierte Information, worin der Grund der Ablehnung bestand.

Hierfür hat sich in der Informatik die Methode der *Ausnahmebehandlung* (engl. „*Exception Handling*“) etabliert (vgl. z. B. [Abts 2013]). Dabei werden vom aufgerufenen System, hier die Sicherungslogik, Fehlermeldungen generiert, die später vom übergeordneten System, welches die Anfrage geschickt hat, hier das TMS abgefangen werden müssen. Das TMS kann dann entsprechend mittels eines eigenen Algorithmus darauf reagieren.

Eine bereits ältere, ähnliche Alternative ist das Senden von *Fehlercodes* („*Failure Codes*“, *FC*). Die beiden Methoden haben einige Unterschiede, die sich allerdings eher in der Informatik-Praxis bemerkbar machen und an dieser Stelle nicht weiter diskutiert werden sollen, da sie auf die Konzeption der smartLogic keinen Einfluss haben. In beiden Fällen werden in die RRM die entsprechenden Hindernisse codiert und können dann – falls gewünscht – vom TMS ausgewertet werden.

Anders als im normalen Exception Handling führt ein Hindernis nicht gleich zum Senden der RRM, sondern diese wird erst am Ende des jeweiligen Prüfprozesses generiert und kann auch mehrere Hindernisse eincodiert haben. Außerdem wird auch im Fall der positiven Prüfung eine RRM generiert, damit das TMS über den Erfolg der Anfrage informiert wird.

Eine Übersicht über die verwendeten Fehlercodes findet sich in Anlage 3.

7.7.2 Update des aktuellen Zustands in der smartLogic

Update der Fahrzeugposition

Tab. 38: Aufbau Train Position Report

Sender	Ortungsinformationsaggregator
Empfänger	smartLogic
spezielle Attribute	Fahrzeugbewegung; Max Safe Front End; Min Safe Rear End
ausgelöster/auslösender Prozess	Train Position Report (Reaktionsprozess)

Die aktuelle Fahrzeugposition wird gemäß der in Kapitel 4 entwickelten Architektur aus verschiedenen Quellen vom Ortungsinformationsaggregator (OIA) berechnet, der für die smartLogic ein externes System darstellt. Auf dieser Basis kann die smartLogic Beanspruchungen anpassen.

Prinzipiell erscheinen drei Kommunikationsmodi denkbar:

1. Die smartLogic könnte bei Bedarf Ortungsinformationen beim OIA abfragen.
2. Der OIA sendet die Ortungsinformationen von sich aus an die smartLogic, sobald neue Informationen vorliegen.
3. Der OIA sendet in einem festen oder von der Sicherungslogik einstellbaren Sendeintervall Positionsupdates.

Der dritte Kommunikationsmodus hat den Vorteil, dass er zum aktuell in ETCS vorgesehenen Übertragungsmodus für die Position Reports passt. Hier kann das RBC dem Fahrzeug ein Intervall mitgeben, in dem das Fahrzeug Position Reports senden soll. Der Nachteil ist, dass bei feinerem Intervall viele unnötige Nachrichten generiert werden könnten, da sich die Position entweder nicht verändert hat und/oder die Sicherungslogik keinen neuen Prüfauftrag hat, für den sie eine aktualisierte Position benötigt. Bei kurzem Intervall kann die veraltete Information zu unnötigen Kapazitätseinschränkungen führen. Stellt die Sicherungslogik das Intervall ein, benötigt sie zusätzliche Intelligenz, die aufgrund der Forderung der schlanken Logik vermieden werden soll. Zudem könnte die Sicherungslogik dann auch direkt nach der benötigten Information (Positionsupdate eines bestimmten Fahrzeugs) fragen (siehe erster Kommunikationsmodus).

Fragt die smartLogic bei Bedarf neue Ortungsinformationen ab (Kommunikationsmodus 1), wird sichergestellt, dass sie immer auf dem aktuellsten Stand über Prüfaufträge entscheidet. Zudem wird die Anzahl an Nachrichten reduziert. Ein Nachteil ist allerdings, dass eine Verzögerung bei der Bearbeitung des Prüfprozesses auftritt, da zunächst die Positionsanfrage gestellt und auf deren Beantwortung bearbeitet werden kann. Die Wartezeit kann jedoch reduziert werden, wenn der Prüfprozess asynchron aufgebaut ist, so dass während der Wartezeit auf die Antwort des OIA weitere Prüfbedingungen geprüft werden können.

Die Abfrage-Nachricht von der Sicherungslogik an den OIA kann vermieden werden, wenn der OIA von sich aus jede Positionsänderung eines bekannten Fahrzeuges direkt an die Sicherungslogik weiterleitet (Kommunikationsmodus 2), sobald eine neue Position gesichert vorliegt. Dieses Vorgehen sichert ab, dass die smartLogic zu jedem Zeitpunkt den bestmöglichen Informationsstand über alle Fahrzeugpositionen hat, allerdings kann es auch zu vielen unnötigen Updates kommen, wenn die Sicherungslogik die Information gerade nicht benötigt. Für diesen Übertragungsmodus ist außerdem zu klären, was eine gesicherte neue Position ist. Bezieht sich „gesichert“ auf die für die Angabe der

Max Safe Front End und Min Safe Rear End erforderliche Sicherheit, ist die Definition klar vorgegeben. Wie in Kapitel 7.6 diskutiert wurde, kann es jedoch auch sinnvoll sein, zusätzlich „Graustufen“ zu übermitteln, bei der eine neue Position mit geringerer Wahrscheinlichkeit, als für die Aktualisierung von Max Safe Front End und Min Safe Rear End erforderlich, vorliegt. Wird jede neue Grauschattierung, also immer wenn ein einzelner Sensor ein Update meldet, berücksichtigt, könnte es zu noch mehr Nachrichten kommen.

Der dritte Kommunikationsmodus erscheint auf Basis der obigen Diskussion am wenigsten sinnvoll zu sein. Für die Kommunikation vom OIA Richtung Sicherungslogik wird in jedem Fall zur Aktualisierung einer Fahrzeugposition eine Nachricht benötigt, die im Folgenden „Train Position Report“ genannt wird. Hiermit der zweite Kommunikationsmodus, bei der der OIA das aktive System ist, bereits umgesetzt werden. Da der erste Kommunikationsmodus, in der die Sicherungslogik Positionsänderungen abfragt, ebenfalls sinnvoll erscheint, wird mit dem „Train Status Request“ auch eine Abfrage-Nachricht definiert, die außer der Fahrzeugidentifikation der abzufragenden Fahrzeuge keine Attribute enthält. Es können also sowohl der erste als auch der zweite Kommunikationsmodus genutzt werden.

Wie bereits in Kapitel 7.6 beschrieben, besteht die Position mindestens aus Max Safe Front End und Min Safe Rear End. Optional können für die angesprochenen „Graustufen“ im Train Position Report weitere Punkte für Zugspitze und Zugende mit einer dazugehörigen Sicherheit definiert werden, mit der das Fahrzeug diesen Punkt noch nicht passiert bzw. bereits vollständig passiert hat, um der smartLogic flexiblere Entscheidungen zur Zulassung von Fahrten zu überlassen. Die letztgenannte Möglichkeit wurde aber in Folgenden aus Zeitgründen nicht weiterbetrachtet.

Die Nachricht löst einen ***Train Position Report***-Reaktionsprozess aus (der als Reaktionsprozess in der vorliegenden Arbeit allerdings nicht detailliert modelliert wird, siehe zur Begründung die Einleitung zu Kapitel 8.7).

Update eines Infrastrukturelement-Status und Zustands

Tab. 39: Aufbau Element Status Message

Sender	Object Controller eines stellbaren Fahrwegelements
Empfänger	smartLogic
spezielle Attribute	stellbares Fahrwegelement; neuer Ist-Status; neuer Ist-Zustand
ausgelöster/auslösender Prozess	Element Status Message (Reaktionsprozess)

Mit dem ***Track Element Status Update*** informiert der Object Controller eines stellbaren Fahrwegelements die smartLogic über eine neue Lage des entsprechenden stellbaren Fahrwegelements. Eine analoge Nachricht existiert auch für einen neuen Zustand des Elements. Der Object Controller sendet die Nachricht nach jeder Veränderung des aktuellen Status/Lage oder Zustands am Element, damit die smartLogic möglichst immer über den aktuellen Zustand informiert ist. Die smartLogic kann eine Element Status Message mittels eines Element Status Requests auch anfordern. Diese Nachricht verläuft in umgekehrter Richtung und enthält als Attribut nur den Zeiger auf das stellbare Fahrwegelement, für den die Element Status Message angefordert wird.

Die Element Status Message löst einen gleichnamigen Reaktionsprozess aus (der als Reaktionsprozess in der vorliegenden Arbeit allerdings nicht detailliert modelliert wird, siehe zur Begründung die Einleitung zu Kapitel 8.7).

Updates weiterer Daten der smartLogic

Fahrzeugposition und Status/Lage sowie Zustand der stellbaren Fahrwegelemente werden im Laufenden Betrieb regelmäßig aktualisiert. Das generische Konzept der Logik sieht jedoch auch vor, dass weitere Daten wie z. B. die Topologiedaten ebenfalls aktualisiert werden können. Aufgrund der begrenzten Bearbeitungszeit kann eine Modellierung der hierfür benötigten Nachrichten jedoch nicht im Detail erfolgen.

7.7.3 Kommunikation mit externen „Stakeholder"-Systemen

Ein zentrales in Kapitel 8.3 entwickeltes Funktionskonzept der smartLogic ist das Stakeholder-Registrierungs-Konzept (siehe Kapitel 8.3.3), mit dem die Sicherheitsanforderungen und –funktionen externer Systeme auf generische Weise in die Logik eingebunden werden können. Hierzu gehört zum einen, dass neue Stakeholder registriert und alte Stakeholder deregistriert werden können. Zum anderen muss mit den vorhandenen Stakeholdern kommuniziert werden. So muss beispielsweise bei zustimmungspflichten Stakeholdern die Zustimmung zur Befahrung des zustimmungspflichtigen Gleisabschnitts (Wirkabschnitt der Stakeholder-Registrierung) eingeholt werden.

Registrieren und Deregistrieren von Systemen

Stakeholder-Systeme sollen sich jederzeit auf einer der Registrierungsschnittstellen registrieren können. Aus den in Kapitel 8.5.2 geschilderten Gründen wird jedoch in dieser Arbeit auf eine Modellierung des Stakeholder-Registrierungsprozesses verzichtet. Unter dieser Voraussetzung ist es auch nicht sinnvoll, an dieser Stelle näher auf die für den Registrierungsprozess benötigten Nachrichten einzugehen.

Empfang einer Stakeholderinformation

Die Bedingungen für die auszutauschenden Nachrichten zwischen Stakeholder-Systemen und smartLogic sind sehr individuell und hängen vom Typ des Stakeholder-Systems ab. Das Stakeholder-Registrierungs-Konzept sieht deshalb vor, dass die Bedingungen der Kommunikation mit den Stakeholdern bei der Registrierung spezifiziert werden können. Diese spezifische Kommunikation wird dann in generische Nachrichten integriert (siehe Kapitel 8.3.3). Aufgrund des Fokus auf die Basislogik in diesem Kapitel zu den Nachrichten wird im Folgenden nur auf die Nachrichten eingegangen, die im Zusammenhang mit den in Kapitel 8.5 modellierten Basis-Prüfprozessen relevant sind.

Wesentliche Nachrichten sind dabei das Nachrichten-Paar ***Stakeholder Status Request*** und ***Stakeholder Status Message***, die den aktuellen Zustand des Stakeholders anfragen bzw. übermitteln. Die übermittelbaren Status sind dabei völlig offen und können bei der Registrierung mit den zugehörigen Implikationen der smartLogic mitgeteilt werden.

Neben dem Status Update ist für zustimmungspflichtige Stakeholder die Zustimmung wichtig. Diese wird mit einem ***Stakeholder Approval Request*** angefragt, auf dem der Stakeholder im Falle der Zustimmung mit einer ***Stakholder Approval Message*** und im Falle der Ablehnung mit einer Stakeholder Failure Message antwortet. Im Falle von benachrichtigungspflichten Stakeholdern erfolgt die Benachrichtigung über eine ***Stakeholder Notification Message***, die mit einer ***Stakeholder Notification Acceptance Message*** beantwortet wird. Sowohl im Fall der zustimmungspflichtigen als auch der benachrichtigungspflichtigen Stakeholder kann der

Gleisabschnitt, auf den sich die Nachricht bezieht, angegeben werden, da es theoretisch denkbar ist, dass ein Stakeholder für Zustimmungen bzw. Benachrichtigungen für verschiedenen Gleisabschnitte zuständig ist. Bei den Antwortnachrichten auf die beiden Requests ist die Request ID als Attribut beizufügen, damit die Zustimmung bzw. Bestätigung der Benachrichtigung an die entsprechende Anfrage geknüpft ist.

Tab. 40 enthält die Zusammenfassung der genannten Nachrichten. Bei allen genannten Nachrichten ist die ID des Stakeholders als Empfänger oder Sender der Nachricht zu übertragen, die in der Tabelle aus Vereinfachungsgründen nicht aufgeführt wurde.

Tab. 40: Aufbau der für den MP Request relevanten Nachrichten zum Austausch mit den Stakeholder-Systemen

Nachricht	Sender	Empfänger	spez. Attribute	Prozess
Stakeholder Status Request	smartLogic	Stakeholder		diverse
Stakeholder Status Message	Stakeholder	smartLogic	Status	diverse
Stakeholder Approval Request	smartLogic	Stakeholder	Gleisabschnitt	MP Request
Stakeholder Approval Message	Stakeholder	smartLogic	Request ID	MP Request
Stakeholder Approval Failure Message	Stakeholder	smartLogic	Request ID	MP Request
Stakeholder Notification Message	smartLogic	Stakeholder	Gleisabschnitt	MP Request
Stakeholder Notification Acceptance Message	Stakeholder	smartLogic	Request ID	MP Request

7.7.4 Kommunikation mit dem Fahrzeug

Die Kommunikation mit dem Fahrzeug erfolgt auf der Basis von ETCS (vgl. Kapitel 2.2.2 und 4.5.2). Die ETCS-Nachrichten sind in den System Requirements Specification [ERA 2016] sehr genau beschrieben, so dass an dieser Stelle keine weitere Auseinandersetzung zu diesem Thema mehr erfolgen muss.

7.8 Ergebnisdiskussion

Im siebten Hauptkapitel wurde das Datenmodell für die smartLogic entworfen. Am einfachsten wäre es gewesen ein bestehendes Datenmodell zu übernehmen, allerdings konnte kein Datenmodell gefunden werden, welches alle Anforderungen der smartLogic erfüllt. Deshalb wurde stattdessen die Strategie verfolgt, bestehende Datenmodelle soweit wie möglich in das Datenmodell der smartLogic zu integrieren.

Die Modellierung der Topologie baut dabei auf dem Standard des Rail Topo Model (RTM) der UIC auf. Diese Entscheidung wurde aufgrund von funktionalen Vorteilen, aber auch zur Sicherung der Zukunftsfestigkeit getroffen (vgl. Kapitel 7.3.1). Nachteilig ist allerdings, dass momentan existierende Realdaten zumindest in Deutschland in der Regel noch nicht kompatibel mit dem RTM sind. Dies liegt auch daran, dass der RTM-Standard erst 2016 verabschiedet wurde und damit noch recht neu ist. Allerdings ist es problemlos möglich, bestehende Daten beispielsweise aus dem PlanPro- oder XML-ISS-Format in das Datenmodell der smartLogic zu konvertieren. Eine solche Konvertierung wurde im Rahmen des Demonstrators der smartLogic im EBD bereits durchgeführt (siehe Kapitel 9).

Es wurde gemäß dem RTM entschieden, eine klare Trennung zwischen topologischem Modell und Infrastrukturmodell vorzunehmen. Das topologische Modell besteht nur aus Gleisen und daran verordneten Informationen. Das Gleis wird nicht in Elemente wie Weichen und einfache Gleise

unterteilt. Weichen und andere Infrastrukturelemente sind im Infrastrukturmodell enthalten. Ihre Verortung erfolgt nicht gemäß der baulichen, sondern gemäß der betrieblichen Bedeutung. Gemäß der RCA-Logik wird hier der Bereich, der nicht befahren werden kann, wenn die Weiche in Umstellung ist, von dem Bereich unterschieden, der aufgrund fehlender Profilfreiheit nicht berührt werden darf, wenn der andere Strang von einem anderen Fahrzeug beansprucht wird. Hierdurch ist das Datenmodell zwar weniger intuitiv und etwas komplexer als andere Modelle, aber flexibler nutzbar.

Das Konzept der Verortung ortsgebundener Informationen in Form von Restricted Areas (RAs) (vgl. Kapitel 7.3.6) stellt eine Erweiterung der URAs der RCA dar. Die RAs erlauben die generische Integration zahlreicher Informationen in die Prüflogik der smartLogic, wobei die Liste an Informationen und auch an Informationstypen nicht abgeschlossen ist. Beispielsweise können heute noch nicht vorgesehene Informationen über das Konzept der RAs an der Infrastruktur verortet werden und beim Passieren einer Fahrzeugbewegung an diese Fahrzeugbewegung übertragen werden. Die smartLogic muss die Bedeutung dieser Information nicht zwangsläufig verstehen, solange das Fahrzeug die Bedeutung versteht. (Die Sicherheitsprüfung findet bei Eintrag der Information in die externe sichere Datenquelle der Topologiedaten und auf dem Fahrzeug statt.)

Von den RAs wurden in Kapitel 7.3.7 Danger Areas (DAs) abgegrenzt. Der Unterschied zu den dauerhaft gültigen RAs ist, dass diese ad hoc durch das Auftreten eines Ereignisses entstehen und in der Regel einen Reaktionsprozess aufrufen. Die Unterscheidung wurde vorgenommen, um die unterschiedlichen Funktionen zu verdeutlichen. Theoretisch wäre aber auch eine Umsetzung über RAs denkbar gewesen. Es ist schwer zu sagen, welche Variante „schlanker“ ist, da auf der einen Seite die Definition der RAs umfangreicher geworden wäre, auf der anderen Seite aber auf das zusätzliche Konstrukt der DAs hätte verzichtet werden können.

Als zusätzliches Datenkonstrukt wurden Gleisbereiche definiert, welche die Verortung von Informationen an größere Teile der Topologie ermöglichen. Eine schlankere Lösung im Sinne von weniger Regeln für die Logik wäre es gewesen, auf das zusätzliche Konstrukt des Gleisbereiches zu verzichten und alle damit verorteten Informationen einzeln an den Gleisen als ortsgebundene Informationen über Gleisabschnitte zu verorten. Dies hätte jedoch auf der anderen Seite zur Folge, dass es deutlich mehr Gleisabschnitte bedürfte. Eine Entscheidung für oder gegen Gleisbereiche hängt daher von der Gewichtung der verschiedenen Anforderungen an die Logik ab und wurde in dieser Arbeit zugunsten der Gleisbereiche entschieden.

Um die Ansprüche der Fahrzeugbewegungen auf der Topologie verorten zu können, wurde das Konzept der Beanspruchung entworfen. Zu den Beanspruchungen gehören sowohl die tatsächliche Belegung der Infrastruktur durch ein Fahrzeug als auch der für das Fahrzeug reservierte Raum. Es gibt aber auch andere Arten von Beanspruchungen, die nicht direkt im Fahrweg der betrachteten Fahrzeugbewegung liegen wie Flankenschutzbeanspruchungen. Ein Punkt der Infrastruktur kann daher Teil mehrerer aktiver Beanspruchungen sein. Auch Infrastrukturelemente wie Weichen können über ihre Verortung mit Beanspruchungen verknüpft werden. Mit dem Konzept der Beanspruchung können flexible Ausschlussregeln formuliert werden, wie dass sich zwei überlappende Vehicle Occupations ausschließen, die Überlappung bestimmter Teile der Fahrerlaubnis aber unter bestimmten Voraussetzungen zulässig ist.

7.9 Vergleich mit alternativen Ansätzen

Zunächst unterscheidet sich der in dieser Arbeit für das Datenmodell verfolgte Ansatz mindestens teilweise aufgrund seiner Fokussierung auf die Belange der Sicherungslogik von den Datenmodellen,

die in Kapitel 2.4.5 vorgestellt wurden. So werden beispielsweise für die Fahrplanerstellung und für die Infrastrukturplanung andere Daten benötigt.

U. a. von der UIC wurde erkannt, dass es sehr schwierig ist, ein einziges umfassendes Datenmodell für alle Anwendungszwecke zu erstellen. Die Gründe hierfür decken sich mit den Anforderungen an die Entwicklung des Datenmodells der smartLogic. Ein zu umfangreiches Datenmodell birgt die Gefahr, dass es häufig aufgrund von neueren Erkenntnissen angepasst werden muss, auch wenn diese Anpassungen für den jeweiligen Anwendungszweck (hier für die smartLogic) nicht von Bedeutung wären. Ein zu umfangreiches Datenmodell widerspricht daher den Anforderungen der *schlanken Logik* und der *Beschränkung auf den sicherungskritischen Kern*. Ein zu unspezifisches Datenmodell würde dagegen die funktionalen Anforderungen nicht hinreichend erfüllen oder es würde zu unnötigen Einschränkungen der Nutzbarkeit der Infrastruktur führen und damit die Anforderungen zu den Zieldimensionen der *hohen Kapazität* und *hohen Robustheit* verletzen.

Aus diesen Gründen wurde der Ansatz verfolgt, möglichst aufbauend auf den bestehenden Modellen ein eigenes Datenmodell zu entwickeln. Dabei sollte das Datenmodell der smartLogic zu den bestehenden Modellen möglichst kompatibel sein, so dass beispielsweise Infrastrukturdaten aus bestehenden Datenaustauschformaten einfach übertragen werden können.

Das RTM wurde bereits mit dem Gedanken erstellt, ein Metamodell für topologische Modelle zu schaffen, zu dem neu entstehende Datenmodelle für bestimmte Anwendungszwecke kompatibel sein sollen und das deshalb von der UIC als Standard herausgegeben wurde (vgl. Kapitel 2.5.2). Die topologische Modellierung des Datenmodells der smartLogic baut dieser Philosophie folgend auf dem RTM auf und grenzt sich damit zum Teil von anderen Datenmodellen bzgl. der topologischen Modellierung ab. Einzig RailML ist von den in Kapitel 2.4.5 vorgestellten Datenmodellen in den neueren Versionen ab Version 3 bereits kompatibel zum RTM. Allerdings zeigte sich bei der Demonstrator-Entwicklung, dass eine Übernahme von topologischen PlanPro-Daten über einen Adapter trotzdem möglich ist.

XML-ISS ist das am weitesten verbreitete Datenmodell mit topologischen Daten (vgl. Kapitel 2.5.5). Da es für die Fahrplanerstellung und Disposition genutzt wird, sind Datensätze für fast das gesamte Netz enthalten. Aufgrund der Ausrichtung des Modells auf Fahrplanerstellung Disposition sind viele mikroskopische Informationen zur Topologie bzw. Infrastruktur nicht im Modell enthalten. Aufgrund der großen Datenverfügbarkeit schien es dennoch sinnvoll, die Möglichkeit der Programmierung eines Adapters zu prüfen., mit dem sich grundlegende Informationen zur Infrastruktur und Topologie aus XML-ISS-Daten in das Datenmodell der smartLogic einlesen lassen, die anschließend weiter vervollständigt werden können. Im Rahmen der Demonstrator-Entwicklung im Eisenbahnbetriebsfeld Darmtadt zeigte sich, dass ein solcher Adapter umsetzbar ist und damit eine begrenzte Kompatibiltät zu den topologischen XML-ISS-Daten besteht.

Für die Infrastrukturdaten und die Modellierung ortsgebundener Informationen wurde vor allem auf Konzepte der RCA zurückgegriffen, da diese im Vergleich zu den Datenmodellen aus Kapitel 2.5 bereits auf die angenommene zukünftige Systemumgebund der smartLogic ausgerichtet ist (vgl. Kapitel 2.2 und 2.4). Dabei sind entsprechende Verweise in den einzelnen Kapiteln enthalten. Insbesondere die Konzepte der Drive Protection Section und der Allocation Section bzw. Allocation Area wurden übernommen (vgl. vor allem Kapitel 7.4.3 und 7.4.4). Weiterhin wurde das Konzept der Usage Restriction Areas im Konzept der Restricted Areas weiterentwickelt (vgl. Kapitel 7.3.6).

Die anderen in Kapitel 2.5 vorgestellten Infrastrukturdatenmodelle konnten als Referenz für die Modellierung einzelner Begriffe und insbesondere Attribute herangezogen werden. Sie enthalten

jedoch aufgrund der unterschiedlichen Intentionen (PlanPro für Planung, XML-ISS für Fahrplanerstellung und Disposition) viele Begriffe und Attribute, die für das Datenmodell der smartLogic im Sinne der Anforderung der *schlanken Logik* bzw. der *Beschränkung auf den sicherungskritischen Kern* nicht relevant sind. Weiterhin wurde das Infrastruktur-Datenmodell der smartLogic im Sinne der Anforderung der *generischen Logik* weniger detailliert und deutlich generischer gestaltet, zum Beispiel durch generische Objekttypen, wie die stellbaren Fahrwegelemente, die mit beliebigen generischen Status verknüpft sind.

Zum Fahrzeugmodell in Kapitel 7.5 wurde keine ausführliche Literaturrecherche durchgeführt, sondern sich weitestgehend auf die Vorgaben der ETCS-Schnittstelle beschränkt. Hintergrund ist, dass das Fahrzeugmodell nur einen geringen Einfluss auf die Funktionsweise der smartLogic hat und dass die Fahrzeugdaten im Wesentliche über die genannte Schnittstelle ausgetauscht werden müssen.

Die Modellierung der Fahrzeugbewegung in Kapitel 7.6 hat eine große Bedeutung für die Funktionsweise der smartLogic. In klassischen Modellen belegt eine Fahrzeugbewegung in der Regel feste Abschnitte der Infrastruktur. Dieses Prinzip wurde für die smartLogic aufgebrochen, so dass eine dynamische Beaspruchung von Infrastrukturelemten erfolgt. Dabei geben die Anforderungen genau vor, dass die Beanspruchungen sowohl räumlich als auch zeitlich kleinstmöglich sein sollen. Daher wurden die notwendigen Beanspruchungen im Sinne des „Grüne Wiese“-Ansatzes bereits unter Einbezug der Konzepte aus Kapitel 8.3 schrittweise hergeleitet. Auch bei der RCA existiert das dynamische Konzept der Movable Objects zur Abbildung der Fahrzeugbewegungen. Ein genauer Vergleich kann jedoch an dieser Stelle aufgrund des noch geringeren veröffentlichten Detaillierungsgrades nicht gezogen werden.

Kapitel 7.7 beschränkt sich auf die Modellierung von Nachrichten, die nicht bereits über Standardschnittstellen vorgegeben werden. Da diese Nachrichten sehr spezifisch für die smartLogic sind, ist ein Vergleich mit alternativen Datenmodellen für dieses Teilmodell nicht sinnvoll.

7.10 Zusammenfassung

Das in diesem Hauptkapitel beschriebene Datenmodell (oder Domänen-Modell) der smartLogic besteht aus den fünf Teilmodellen topologisches Modell, Infrastrukturmodell, Fahrzeugmodell, Modell der Fahrzeugbewegungen und Modellierung der Nachrichten, die mittels UML-Klassendiagrammen modelliert wurden. Das topologische Modell beruft auf den Grundsätzen des RTM. Weiterhin wurde auf Strukturen aus PlanPro und insbesondere aus der RCA-Modellierung zurückgegriffen. Das gilt insbesondere für die Restricted Areas (bei der RCA URA), mit deren Hilfe vielfältige ortsgebundenen Informationen generisch an der Topologie verortet werden können.

Aus Gründen der Kompatibilität dieser Forschungsarbeit zu den realen Entwicklungen in der RCA wurde möglichst auf eine begriffliche Angleichung der im Datenmodell modellierten Begriffe gesetzt, so dass einige Begriffe aus der RCA für diese Arbeit übernommen wurden. Das gilt besonders für die Begriffe der Drive Protection Sections (DPS) und der Allocation Sections (AS), mit denen die betrieblich bedeutsamen Ausdehnungen von Infrastrukturelementen in der Topologie abgebildet werden können. DPS stellen dabei Befahrbarkeitssperren bei bestimmten Zuständen des verknüpften Infrastrukturelements dar. AS markieren Gleisabschnitte in denen sich Fahrzeuggrenzlinien potenziell überschneiden können, wobei eine aktive AS eine Beanspruchung eines solchen Fahrwegabschnitts durch ein Fahrzeug darstellt, die eine Nutzung der verknüpften AS durch ein anderes Fahrzeug ausschließt.

Das Fahrzeugmodell orientiert sich an den Fahrzeugdaten, die in ETCS spezifiziert sind. Im Modell der Fahrzeugbewegungen wurde die Beschreibung der Zugposition ebenfalls an ETCS angelehnt, so dass

verschiedene Definitionen der Zugspitze und des Zugschlusses unterstützt werden. Der von der Fahrzeugbewegung direkt oder indirekt beanspruchte Raum auf der Topologie wurde durch das Konzept der Beanspruchung modelliert. Dabei können für verschiedene Typen von Beanspruchungen verschiedenen Ausschlussregeln festgelegt werden. Hierdurch wird auf generische Weise eine vielfältige Nutzung der Infrastrukturressourcen ermöglicht.

Das Nachrichtenmodell enthält die Nachrichten, die von der Sicherungslogik empfangen und gesendet werden. Eine vollständige Beschreibung aller Nachrichten war aufgrund des begrenzten Bearbeitungsumfangs dieser Arbeit nicht möglich, so dass nur die wesentlichen Nachrichten, die für die Umsetzung der Basisfunktionen erforderlich sind, modelliert wurden.

8 Verhaltensmodellierung der Logik

Das achte Hauptkapitel behandelt die Verhaltensmodellierung der smartLogic. Hierzu wird insbesondere der Ablauf der notwendigen Prozesse und Subroutinen hergeleitet und beschrieben, die im 6. Hauptkapitel identifiziert wurden. Die Modellierung greift dabei auf das Datenmodell aus dem 7. Hauptkapitel zurück. Das Hauptkapitel folgt dem grundsätzlichen Aufbau für Hauptkapitel wie in Kapitel 1.3 beschrieben.

8.1 Ziel und Aufbau des Kapitels

In diesem Kapitel werden Ziel und Aufbau des Hauptkapitels genauer beschrieben. Die Basis hierfür bilden die Erkenntnisse aus Kapitel 3.6 zur Vorgehensweise der Arbeit.

Ziel des vorliegenden Hauptkapitels ist es demnach, die Verhaltensmodellierung der wesentlichen Funktionen der Sicherungslogik herzuleiten und zu beschreiben. Von den in Kapitel 6.2.2 identifizierten Funktionsarten haben nur Prozessfunktionen (Prozesse) und Subroutinen ein dynamisches Verhalten, das mittels der Verhaltensmodellierung beschrieben werden könnte. Die einzelnen zu prüfenden Sachverhalte werden dabei durch die für den jeweiligen Prozess relevanten Prüfbedingungen aus dem in Kapitel 6 erstellten Katalog an Prüfbedingungen vorgegeben.

Gemäß der Zielsetzung der gesamten Arbeit als wissenschaftlicher Baustein zur Entwicklung einer neuen „digitalen“ Leit- und Sicherungstechnik (vgl. Kapitel 1 und 3) soll hinsichtlich zu treffender Entscheidungen bezüglich der Funktionsweise der smartLogic nicht nur eine einzige, beste Lösung beschrieben werden, sondern es sollen auch verschiedene, mögliche Lösungsansätze diskutiert werden. Diese Diskussionen sollen als Unterstützung der Entscheidungsfindung bei der späteren Ausgestaltung von Realsystemen dienen. Für die Modellierung der smartLogic in diesem Hauptkapitel und zur Erstellung des Demonstrators (siehe Kapitel 9) wird jedoch jeweils im Anschluss an die Diskussion eine der möglichen Lösungen zur Weiterverfolgung ausgewählt.

Wie in den anderen Hauptkapiteln werden nachfolgend zunächst Methode und Vorgehensweise für die Verhaltensmodellierung hergeleitet (Kapitel 8.2). Entsprechend der Aussage aus dem vorigen Absatz erfolgt anschließend als Grundlage für die darauf aufbauende Modellierung zunächst eine Diskussion und Erarbeitung grundsätzlicher Konzepte bzgl. der Funktionsweise der smartLogic. Aus Übersichtlichkeitsgründen werden hierbei Basis-Konzepte für den grundlegenden Betrieb in Kapitel 8.3 und Konzepte für betriebliche Spezialfälle in Kapitel 8.4 unterschieden. In Kapitel 8.5 folgt die Modellierung der Basis-Prüfprozesse, an die sich in Kapitel 8.6 die Modellierung der Funktionsweise der wichtigsten Subroutinen, die für die Basis-Prüfprozesse benötigt und von diesen aufgerufen werden (vgl. Kapitel 6.2.2), anschließt.

Innerhalb der Gruppe der Prozessfunktionen der smartLogic wurden in Kapitel 6.2.2 von den Prüfprozessen die Reaktionsprozesse unterschieden. Allerdings wurde in Kapitel 3.3 abgegrenzt, dass aus Ressourcengründen die Reaktionsprozesse in dieser Arbeit nicht im Detail behandelt werden können. Deshalb wird in Kapitel 8.7 nur ein kurzer Ausblick auf diese Thematik gegeben. Dasselbe gilt für erweiterte Anwendungsfälle wie Übergangsbedingungen, Rückfallebenen, Kommandoeingaben, Transaktionsbedingungen und die Protokollierung, die in Kapitel 8.8 der Vollständigkeit halber kurz angerissen werden. Anschließend erfolgt wie in den anderen inhaltlichen Hauptkapiteln die Ergebnisdiskussion (Kapitel 8.9), der Vergleich mit alternativen Ansätzen (Kapitel 8.10) und schließlich die Zusammenfassung (Kapitel 8.11).

8.2 Methode und Vorgehensweise

In diesem Kapitel werden Methode und Vorgehensweise zur Erstellung der Verhaltensmodellierung der smartLogic gemäß ihrer in Kapitel 8.1 beschriebenen Zielsetzung hergeleitet und beschrieben. Wie in den anderen Hauptkapiteln werden dazu zunächst die spezifischen Anforderungen an die Verhaltensmodellierung aus den globalen Anforderungen hergeleitet (Kapitel 8.2.1). Darauf aufbauend werden in Kapitel 8.2.2 zentrale Fragestellungen in Bezug auf die Auswahl der Methode und Vorgehensweise für die Verhaltensmodellierung diskutiert sowie die Entscheidungen für die in der weiteren Arbeit verwendete Methode und Vorgehensweise begründet. Kapitel 8.2.3 fasst anschließend die Erkenntnisse des Kapitels 8.2 zusammen.

8.2.1 spezifische Anforderungen

Die spezifischen Anforderungen an die Verhaltensmodellierung (Prozessmodellierung) der smartLogic leiten sich aus den globalen Anforderungen (vgl. Kapitel 3.5) und der in Kapitel 8.1 beschriebenen Zielsetzung des vorliegenden Hauptkapitels her. Dazu wird für jede globale Anforderung überlegt, welchen Einfluss die Ergebnisse des Kapitels in Hinblick auf die Erfüllung der jeweiligen globalen Anforderung haben. Zusätzlich wurde zur Vervollständigung der spezifischen Anforderungen ein Brainstorming mit Fachkollegen durchgeführt.

Bei den spezifischen Anforderungen handelt es sich um „Design-Prinzipien“ für die Verhaltensmodellierung der smartLogic. Tab. 41 enthält einen Überblick der globalen Anforderungen und ihrer Bedeutung für die Verhaltensmodellierung, die anschließend unterhalb der Tabelle näher erläutert werden. Bei nicht relevanten globalen Anforderungen ist dieser Umstand in kursiv vermerkt.

Tab. 41: spezifische Anforderungen/Design-Prinzipien für die Verhaltensmodellierung

Zieldimension	globale Anforderung	spezifische Anforderungen
Kernanforderung sichere Logik		Übergang in unsicheren Zustand verhindern; alle relevanten Prüfbedingungen erfüllen
geringer Planungs- und Genehmigungsaufwand	schlanke Logik	nur notwendige Prozessschritte durchführen
	Beschränkung auf sicherungskritischen Kern	keine zusätzlichen Prozessschritte, die nicht durch die Funktionsanalyse vorgegeben werden
	generische Logik	Prozessschritte möglichst generisch gestalten
	Topologieunabhängigkeit	Anwendung der Logik auf beliebige Topologie ermöglichen
	flexible Infrastrukturzuordnung	*bereits als funktionale Anforderungen über die Funktionsanalyse in den in diesem Hauptkapitel zu modellierenden Funktionsumfang eingeflossen*
Interoperabilität	Standardschnittstellen	*bereits als funktionale Anforderung in den Funktionsumfang eingeflossen*
geringer Hardwareeinsatz	nur erforderliche Infrastrukturelemente	*keine Relevanz für die Verhaltensmodellierung festgestellt*
geringer	hohe Automatisierung	Benutzerinteraktion vermeiden

Arbeitskräfteeinsatz	flexible Kontrollbereiche	*bereits als funktionale Anforderung in den Funktionsumfang eingeflossen*
Energieeffizienz	keine unnötigen Bremsvorgänge	Fahrerlaubnis gibt keine Einschränkungen für die Fahrweise der Züge vor, die nicht aus Sicherheitsgründen notwendig sind
	Freiraum für Fahrzeug	
hohe Kapazität	Ermöglichung maximaler Geschwindigkeit	
	geringe Latenz	möglichst wenige Nachrichten zwischen den Systemen austauschen; möglichst parallele Bearbeitung von Prozessschritten und Anfragen ermöglichen
	minimale Infrastrukturbeanspruchung	Beanspruchungen auf den Umfang der Gleisabschnitte und diejenigen Infrastrukturelemente beschränken, der bzw. die zur Aufrechterhaltung der Sicherheit erforderlich ist/sind
	frühestmögliche Infrastrukturfreigabe	Existenz von Beanspruchungen auf Zeitraum beschränken, der zur Aufrechterhaltung der Sicherheit erforderlich ist
hohe Robustheit	Rückfallebenenintegration	Abbruch des Prozesses nur, wenn Kernanforderung unter Berücksichtigung aller verfügbaren Informationen tatsächlich nicht erfüllt ist; (schafft für das TMS die Möglichkeit der Definition milderer Prüfkriterien in Verbindung mit Einschränkungen für die Fahrerlaubnis)
	Regelhandlungsgebot	*bereits als funktionale Anforderung in den Funktionsumfang eingeflossen*
	Freiraum für Fahrzeuge	Vorgaben so wenig restriktiv und passgenau wie möglich gestalten
	Resilienz	Abbruch des Prozesses nur, wenn Kernanforderung unter Berücksichtigung aller verfügbaren Informationen tatsächlich nicht erfüllt ist
	modulare Außerbetriebnahme	*keine Relevanz für die Verhaltensmodellierung festgestellt*
lange Nutzungszeiten	Migrationsfähigkeit	Regeln möglichst technologieunabhängig definieren
	Zukunftsfähigkeit	Prozessschritte möglichst generisch gestalten
[ohne]	Protokollierung	*bereits als funktionale Anforderung in den Funktionsumfang eingeflossen*

Die beiden spezifischen Anforderungen, die aus der *Kernanforderung* der smartLogic hergeleitet werden, stehen an erster Stelle und sind nicht verhandelbar. Die anderen Anforderungen sind, wie

bereits in Kapitel 3.5 festgestellt, zunächst gleichberechtigt, da keine eindeutige Rangfolge zwischen den Zieldimensionen festgestellt werden konnte, sondern eine Balance zwischen der Erfüllung der einzelnen Zieldimensionen erreicht werden muss. Daher ist bei in Konflikt stehenden Anforderungen für den Einzelfall eine Abwägungsentscheidung zu treffen und zu begründen, welche die Schwere der Verletzung der einzelnen Anforderungen berücksichtigt.

Die globale Anforderung der *schlanken Logik* bedeutet in Hinblick auf die Verhaltensmodellierung, dass nicht erforderliche Prozessschritte vermieden werden sollen. Die verbleibenden Prozessschritte sollen möglichst generisch und auch technologieunabhängig formuliert sein (globale Anforderung der *generischen Logik*).

Die globale Anforderung der *generischen Logik* steht im Widerspruch zu weiteren Anforderungen, die z. B. eine hohe Passgenauigkeit (*Freiraum für Fahrzeuge)* oder im Sinne der Robustheit das zusätzliche Abprüfen von Prüfbedingungen fordern, die für Rückfallebenen relevant sind (*Rückfallebenenintegration)*. Dieser Widerspruch zwischen einer schlanken und einer funktionalen Logik ist bereits aus den anderen Hauptkapiteln bekannt und wurde bisher zum bestmöglichen Heben von Kapazitätspotenzialen und zur Erhöhung der Robustheit in den meisten Fällen zugunsten einer maximal funktionalen Logik entschieden. Allerdings ist auch denkbar, dass es Fälle gibt, bei denen eine deutliche Verkomplizierung der Logik zur Hebung nur eines geringen Kapazitätspotenzials nicht gerechtfertigt wäre. Daher sollte auch bei diesem Zielkonflikt jeweils eine Abwägungsentscheidung getroffen werden.

Mehrere globale Anforderungen richten sich direkt an die Funktionsweise der einzelnen Prozesse. Demnach soll ein maximaler *Freiraum für Fahrzeuge* zur Optimierung ihrer Fahr- und Bremskurven durch eine Fahrerlaubnis geschaffen werden, die keine Einschränkungen (z. B. der erlaubten Geschwindigkeit, vgl. globale Anforderung der *Ernmöglichung maximaler Geschwindigkeit*) enthält, die für das entsprechende Fahrzeug nicht aus Sicherheitsgründen nötig sind. Weiterhin soll bei der Detailmodellierung der einzelnen Prozesse darauf geachtet werden, dass die Logik *topologieunabhängig* arbeitet und Benutzerinteraktionen vermieden werden (*hohe Automatisierung*).

Im Sinne der globalen Anforderung der *geringen Latenz* ist darauf zu achten, dass zeitaufwändige Prozessschritte wie die Kommunikation mit anderen Systemen auf das Notwendige begrenzt und möglichst parallel abgearbeitet werden. Weiterhin sollte die parallele Bearbeitung mehrerer Anfragen möglich sein (zum Beispiel könnte das Warten auf die Zustimmung eines Bahnübergangs zu einer Anfrage ansonsten zu einer relevanten Verzögerung für andere Anfragen führen).

Wie bereits erwähnt, sollte die Sicherungslogik auch das Fahren in Rückfallebenen ermöglichen (*Rückfallebenenintegration*), sofern ein ausreichendes Maß an Sicherheit erhalten bleibt. Ein ausreichendes Maß an Sicherheit kann trotz der für die Rückfallebene ursächlichen Einschränkung zum Beispiel erreicht werden, wenn grundsätzlich betrachtete Risiken in der spezifischen Betriebssituation nicht vorhanden sind (z. B. befindet sich mit hinreichender Sicherheit kein Fahrzeug im Flankenschutzraum) oder die Fahrerlaubnis soweit eingeschränkt ist, dass die durch eine Fehlfunktion entstehenden zusätzlichen Risiken als hinreichend gering angesehen werden können (z. B. Fahrerlaubnis mit niedriger Geschwindigkeit). Ein negativer Einfluss auf die Schutzrate durch eine nicht (vollständig) erfüllte Prüfbedingung sollte folglich auch im Sinne der globalen Anforderung der *Resilienz* nur dann zu einem negativen Ergebnis für die gesamte Anfrage führen, falls ein unsicherer Zustand des Gesamtsystems nicht ausgeschlossen werden kann.

Einige globale Anforderungen stellen Anforderungen an den Funktionsumfang der smartLogic, die deswegen (weil es Anforderungen an den Funktionsumfang sind) bereits in der Funktionsanalyse in Kapitel 6 in den Funktionskatalog eingeflossen sind. Der Funktionskatalog aus Kapitel 6 enthält gemäß

der Gesamt-Vorgehensweise für diese Arbeit (vgl. Kapitel 3.6.6) die im Rahmen der Verhaltensmodellierung zu modellierenden Funktionen der smartLogic. Es ist daher keine erneute Festlegung einer spezifischen Anforderung für diese globalen Anforderungen erforderlich.

Die globalen Anforderungen, wonach *nur erforderliche Infrastrukturelemente* berücksichtigt und eine *modulare Außerbetriebnahme* ermöglicht werden sollte, richten sich primär an die Systemdefinition und das Datenmodell. Ein Einfluss der Verhaltensmodellierung der smartLogic auf die Erfüllung dieser Anforderungen wurde nicht festgestellt.

8.2.2 Erarbeitung der Methode und Vorgehensweise

In diesem Unterkapitel soll auf Basis der in Kapitel 8.2.1 identifizierten spezifischen Anforderungen eine geeignete Methode und Vorgehensweise für die Verhaltensmodellierung erarbeitet werden. Hierfür ist zu klären, welche Arten von Informationen im Rahmen der Verhaltensmodellierung im Modell abgebildet sein müssen (erster Abschnitt). Darauf aufbauend kann die Art der Modellierung und damit verbunden die genaue Notationsform (Modellierungssprache) festgelegt werden (zweiter Abschnitt). Damit sichergestellt ist, dass alle relevanten Informationen auch in das Modell mitaufgenommen werden, ist eine strukturierte Vorgehensweise erforderlich, die herzuleiten ist (dritter Abschnitt).

Das Unterkapitel erhebt aus Gründen der Übersichtlichkeit nicht den Anspruch, neben den genannten Fragestellungen in Bezug auf die übergeordnete Methode, auch alle methodischen Fragestellungen zu thematisieren, die nur einzelne Design-Entscheidungen, zum Beispiel bei der Erarbeitung der Basis-Konzepte, betreffen. Diese werden in den jeweiligen Kapiteln des 8. Hauptkapitels besprochen.

Umfang (Bestandteile) der Verhaltensmodellierung

Wie in der Einleitung zu diesem Unterkapitel beschrieben, ist zunächst zu bestimmen, welche Arten von Informationen im Rahmen der Verhaltensmodellierung im Modell abgebildet sein müssen. Im Kapitel 7.2.2 wurde die Verhaltensmodellierung bereits von der Strukturmodellierung abgegrenzt, wobei dort das Datenmodell als Teil der Strukturmodellierung im Fokus stand. Die Verhaltensmodellierung beinhaltet dagegen je nach Bedarf (vgl. [Kahlbrandt 1998, S. 162] und die Liste der UML-Diagrammarten)

- eine Beschreibung von Interaktionen zwischen verschiedenen Teilsystemen oder dem betrachteten System und seinen Umsystemen (vgl. z. B. UML Sequenzdiagramm) bzw. des Zusammenspiels der verschiedenen Teilsysteme bei der Erfüllung einer Operation,
- eine Beschreibung der Zustandsübergänge von einzelnen Objekttypen (vgl. z. B. UML Zustandsdiagramm),
- eine Beschreibung des Ablaufs von Operationen bzw. Prozessen (vgl. z. B. UML Aktivitätsdiagramm).

Die Interaktion mit den Umsystemen wurde auf grundsätzlicher Ebene bereits im 4. Hauptkapitel besprochen. Demnach folgt der grundsätzliche Ablauf dem Aufbau, dass die smartLogic eine Anfrage empfängt oder über ein Ereignis benachrichtigt wird, dann in einer internen Logik die Auswirkungen der Anfrage bzw. des Ereignisses auf die Sicherheit anhand von Prüfbedingungen prüft und abschließend notwendige Maßnahmen an die Umsysteme kommuniziert. Da für das Verständnis der Funktionsweise der Sicherungslogik vor allem der mittlere interne Teil des Prozesses von Relevanz ist, steht die Interaktionsmodellierung nicht im Vordergrund.

Die Zustandsübergänge der einzelnen Objekttypen (wie z. B. bewegliche Fahrwegelemente oder externe Systeme wie Bahnübergänge) beeinflussen zwar die Funktionsweise der smartLogic, eine Zustandsmodellierung für alle Objekttypen wäre jedoch sehr umfangreich. Da viele Objekttypen nur wenige verschiedene Zustände kennen, erscheint es nicht notwendig, eine vollständige Zustandsmodellierung durchzuführen. Bei komplexeren Zustandsübergängen kann jedoch eine Zustandsmodellierung zur besseren Veranschaulichung durchgeführt werden, wenn dies erforderlich ist.

Zum Verständnis der internen Funktionsweise der Sicherungslogik ist vor allem ein Verständnis des Ablaufs der Prüfprozesse und Subroutinen nützlich, der unter den dritten Anstrich der obigen Auflistung fällt. Aus diesem Grunde liegt auf der Beschreibung des Ablaufs der Prozesse und Subroutinen der Hauptfokus dieses Kapitels. Je nach Bedarf können zusätzliche Beschreibungen der Interaktionen mit den Umsystemen sowie der Zustandsübergänge hinzukommen.

Modellierungssprache und Notationsform

Für die im vorigen Abschnitt bestimmten erforderlichen Bestandteile der Verhaltensmodellierung sind geeignete Notationsformen zu finden. Um eine eindeutige Verständlichkeit zu garantieren, erscheint es sinnvoll, auf eine bestehende Modellierungssprache zurückzugreifen. In den folgenden Unterabschnitten werden Kriterien für die Wahl einer geeigneten Modellierungssprache bestimmt und auf dieser Basis eine Modellierungssprache ausgewählt.

Kriterien für die Auswahl einer geeigneten Modellierungssprache

Da die smartLogic ein sicherheitskritisches Softwaresystem ist, müssen bei der Entwicklung die Voraussetzungen der EN 50126 [DIN EN 50126-1:2017] und EN 50128 [DIN EN 50128:2011] berücksichtigt werden. In den Normen wird zwischen Software-Entwurf und Implementierung unterschieden. Bestandteil des Forschungsprojekts smartLogic ist dabei nur die Entwurfsphase und nicht die Implementierung (vgl. Kapitel 3.6). Letztere wird in einem Demonstrator nur exemplarisch umgesetzt. EN 50128 schreibt unter anderem vor, dass die wesentlichen Algorithmen und Abläufe genau dargestellt werden müssen. Hierzu sind gemäß der Norm auch Diagramme zu verwenden [DIN EN 50128:2011]. Die Darstellung muss eindeutig sein und daher einer genau definierten Semantik und Syntax folgen. „Das gewählte Entwurfsverfahren muss Merkmale haben, die […] Folgendes unterstützen:

i) Abstraktion, Modularität und andere Eigenschaften, die die Komplexität kontrollieren;

ii) die klare und genaue Darstellung von

- Funktionalität;
- Informationsfluss zwischen den Komponenten;
- Reihenfolge und zeitbezogene Informationen;
- Parallelverarbeitung;
- Datenstrukturen und -eigenschaften;

iii) Verständlichkeit für den Menschen;

iv) Verifikation und Validierung.“ [DIN EN 50128:2011, S. 22–23]

Die Ziele der formalen Entwurfsmodellierung sind also vor allem das Herstellen von Eindeutigkeit der verwendeten Begriffe, Nachrichten und Abhängigkeiten sowie die Veranschaulichung und unmissverständliche Darstellung der Prozesse. Da aufgrund der Anzahl von Funktionen und vor allem Prüfbedingungen im Funktionskatalog damit zu rechnen ist, dass das gesamte Modell umfangreich

werden wird, kann angenommen werden, dass eine modulare Darstellungsweise hilfreich sein wird, die es ermöglicht, verschiedene Teilaspekte ein- oder auszublenden bzw. in feinerer oder gröberer Darstellung anzuzeigen.

Notationsform

Eine solche Entwurfsmodellierung, wie im vorigen Unterabschnitt beschrieben, kann, wie bereits in Kapitel 2.6.2 besprochen, mit formalen oder semiformalen Notations- bzw. Modellierungssprachen erfolgen oder mittels grafischer Notation. In Kapitel 2.6.2 wurden auch die Vor- und Nachteile dieser Modellierungsarten aufbauend auf der Literatur diskutiert.

Da smartLogic ein Forschungsprojekt ist, hat das verständliche Aufzeigen neuer Denkansätze einen hohen Stellenwert. Zudem ist es wichtig, dass neue Erkenntnisse auch nachträglich noch einfach in das Modell eingefügt werden können und Veränderungen an der Struktur unproblematisch möglich sind. Diese Anforderungen erfüllt die grafische Modellierung besser als formale und semiformale Notationssprachen. Aus diesen Gründen wird in der vorliegenden Arbeit die grafische Modellierung zur Beschreibung der Basislogik genutzt.

In Kapitel 2.6.2 wurde auch auf verschiedene grafische Modellierungssprachen für die Verhaltensmodellierung eingegangen, die weitverbreitet sind. [Höppner 2015] enthält auf Seite 120 beispielsweise einen Vergleich solcher Modellierungssprachen für einen ähnlichen wie den hier vorliegenden Anwendungsfall. Prinzipiell sind mehrere dieser Modellierungssprachen für den vorliegenden Anwendungsfall geeignet, zu denen auch die Unified Modelling Language (UML) gehört, die bereits für die Strukturmodellierung als Modellierungssprache ausgewählt wurde (vgl. Kapitel 7.2.2). Da Strukturmodellierung und die Verhaltensmodellierung bei UML verknüpft werden können (die verschiedenen Diagrammarten stellen nur eine Visualisierung des eigentlichen Modells dar), erscheint eine Nutzung der UML sowohl für die Struktur- als auch die Verhaltensmodellierung von Vorteil zu sein.

Die UML stellt den Standard für die grafische Modellierung im Bereich der Softwareentwicklung dar (vgl. Kapitel 2.6.2). Weiterhin ist die UML weltweit gebräuchlich, leicht verständlich und es existieren Werkzeuge, die es ermöglichen große Modelle übersichtlich und konsistent zu erstellen. Auch bei HÖPPNER schneidet die UML am besten ab und wurde deshalb von ihm verwendet.

Aufgrund der beschriebenen Vorteile der UML, der direkten Kompatibilität zur Strukturmodellierung des Datenmodells und da keine der anderen Modellierungssprachen einen eindeutigen Vorteil gegenüber der UML hat, wird die UML als Modellierungssprache für die Verhaltensmodellierung der smartLogic verwendet.

Diagrammarten

Wie in Kapitel 2.6.2 erläutert, beinhaltet die UML verschiedene Diagrammarten, von denen für die Verhaltensmodellierung in dieser Arbeit eine oder mehrere geeignete Diagrammarten auszuwählen sind.

Für die Beschreibung von Prozessen sind innerhalb der UML das Aktivitätsdiagramm und das Sequenzdiagramm vorgesehen. Beim Sequenzdiagramm liegt der Fokus auf der Interaktion verschiedener Systemkomponenten. Das Aktivitätsdiagramm eignet sich dagegen besser für die Beschreibung interner Prozessabläufe und ihrer Gliederung in einzelne Prozessschritte. Letzteres entspricht eher der Aufgabenstellung der Verhaltensmodellierung in dieser Arbeit (vgl. Abschnitt „Umfang (Bestandteile) der Verhaltensmodellierung“). Deshalb wird für die Verhaltensmodellierung der smartLogic primär das UML-Aktivitätsdiagramm verwendet.

Je nach Bedarf können allerdings weitere Verhaltensdiagramme wie das Sequenzdiagramm für sequentielle Abläufe mehrerer beteiligter Systeme oder das Zustandsdiagramm für die Modellierung des Verhaltens einer einzelnen Komponente zusätzlich zum besseren Verständnis des gewünschten Systemverhaltens beitragen und ergänzt werden.

Ablauf der Modellierung der Prozesse und Subroutinen

Nachdem im vorigen Abschnitt eine geeignete Notationsart bestimmt wurde, beschäftigt sich dieser Abschnitt damit, wie die Inhalte der Diagramme hergeleitet werden können. Wie bereits im Abschnitt „Umfang (Bestandteile) der Verhaltensmodellierung“ erwähnt, ist die Modellierung der Prüf- und Reaktionsprozesse der zentrale Bestandteil der Verhaltensmodellierung für die smartLogic. Gemäß Kapitel 6.2.2 gehört zu jedem dieser Prozesse eine Prozessfunktion, die sich wieder verschiedener Subroutinen bedienen kann. Für die Modellierung dieser Prozesse und Subroutinen ist eine geeignete Vorgehensweise zu finden.

Die Aufgabe der Prüfprozesse ist, zu bestimmen, ob die zugrundeliegende Anfrage zur Genehmigung einer Zustandsänderung an die Sicherungslogik mit hinreichender Wahrscheinlichkeit zu keinem unsicheren Zustand führen kann (vgl. Kapitel 4.3.1). Die Reaktionsprozesse stellen sicher, dass im Falle von auftretenden Ereignissen, welche die Sicherheit gefährden können, alle in der jeweiligen Betriebssituation erforderlichen Maßnahmen ergriffen werden, um eine größtmögliche Sicherheit zu gewährleisten bzw., falls ein Schaden nicht zu vermeiden ist, das Schadensausmaß bestmöglich zu begrenzen (vgl. Kapitel 6.2.2).

Für die Modellierung der Prozesse und Subroutinen ist Klarheit erforderlich, welche der in Kapitel 6 identifizierten Prüfbedingungen für die jeweilige Funktion relevant sind. Eine Prüfbedingung kann dann als relevant angesehen werden, wenn sie im Falle eines Prüfprozesses das Ergebnis der Prüfung (vgl. Kapitel 8.3.1 zur „Schutzrate“) signifikant beeinflusst bzw. sich im Falle eines Reaktionsprozesses aufgrund des zugrundeliegenden Ereignisses eine veränderte Bewertung des Erfüllungsgrads der Prüfbedingung und damit des Sicherheitsniveaus insgesamt ergeben kann.

Die Kriterien zur Bewertung, ob eine Prüfbedingung für die Prozessfunktion oder eine der Subroutinen von Relevanz ist, sind sehr vielfältig. Denkbare Beispiele sind, wenn

- die Prüfbedingung in ihrer Formulierung einen Objekttyp enthält, dessen Beanspruchung (vgl. Kapitel 7.6.2) sich durch die Umsetzung der Prozessfunktion ändern könnte oder dessen Eigenschaften in einer anderen Form verändert werden könnten,
- sich die Prüfbedingung auf einen Objekttyp innerhalb der Prozessfunktion bezieht (z. B. das Fahrzeug oder das Infrastrukturelement, dessen Status durch den Prozess verändert werden soll).

Eine vollständige Auflistung ist aufgrund der großen Vielfalt nicht möglich und die genannten Beispiele sind nur als Grundlage für die Bewertung zu verstehen. Die Bewertung kann demnach mangels eines vollständigen und durchgehend gewichteten Bewertungskataloges nicht quantitativ erfolgen, sondern muss stattdessen qualitativ getroffen werden. Im Rahmen dieser Arbeit erfolgt die Bewertung durch den Autor. Sie sollte bei Entwicklung eines Produktivsystems später von Fachexperten überprüft werden.

Um das Aktivitätsdiagramm vollständig und korrekt erstellen zu können, ist es in einem weiteren Schritt erforderlich, diejenigen externen Systeme zu identifizieren, mit denen im entsprechenden Prozess kommuniziert wird. Da in den Prozessen vielfach aktuelle Daten über die Infrastruktur und

die Fahrzeuge benötigt werden, würde eine Darstellung der Datenhaltungskomponenten (vgl. die Übersicht über die Systemumgebung der smartLogic in Kapitel 4.6) als externe Systeme die Komplexität der Diagramme deutlich erhöhen. Es wird an dieser Stelle angenommen, dass die sicheren Datenhaltungskomponenten physisch eng mit der Sicherungslogik verbunden sind, so dass Latenzzeiten an dieser Stelle keine relevante Größe darstellen. Mit dieser Annahme erscheint es vertretbar zu sein, die Datenhaltungskomponenten nicht gesondert als externe Systeme aufzuführen. Stattdessen wird angenommen, dass die Informationen aus den sicheren Datenhaltungskomponenten für die Sicherungslogik jederzeit zur Verfügung stehen.

Nach der Bestimmung der relevanten Prüfbedingungen und der beteiligten externen Systeme kann das Aktivitätsdiagramm erstellt werden. Es bietet sich an, die Prüfung der Prüfbedingungen mit dem Modellierungselement „Aktion“ darzustellen. Bei sehr einfach zu prüfenden Bedingungen, die auch in der späteren Implementierung mit einer einfachen if-Abfrage umgesetzt werden können, erscheint es sinnvoll, zur Vereinfachung der Darstellung auf das Einzeichnen einer Aktion zu verzichten und die Bedingung direkt an der Kontrollfluss-Verzweigung zu notieren.

Komplexere Prüfbedingungen, wie z. B. ob eine Gefährdung durch Flankenfahrt ausgeschlossen oder das vom TMS beantragte Geschwindigkeitsprofil (vgl. Inhalte der ETCS-MA in Kapitel 2.2.2) zulässig ist, sind mit einer einzelnen Aktion nicht hinreichend beschrieben. Hierfür bietet es sich an, die entsprechende Subroutine als eigene Aktivität zu modellieren, die wiederum ein Aktivitätsdiagramm und untergeordnete Aktionen (die wiederum weitere Aktivitäten sein können) besitzen. Die Subroutinen, die selbst wieder eine Aktivität bilden, werden im übergeordneten Aktivitätsdiagramm als sogenannte „Call Behavior Actions“ eingebunden (vgl. Kapitel 2.6.2). Subroutinen durchlaufen ebenfalls den gesamten hier geschilderten Modellierungsprozess.

Die Anordnung der Aktionen im Prozessablauf erfolgt gemäß den in Kapitel 8.2.1 beschriebenen Anforderungen. Demnach ist auf eine möglichst parallele Bearbeitung von einzelnen Aktionen und den Einbezug möglicher Latenzzeiten durch die Kommunikation mit Umsystemen zu achten. Werden Informationen von Umsystemen benötigt (z. B. vom Fahrzeug, von den Infrastrukturelementen oder über die Topologie), müssen die entsprechende Anfrage (Request) sowie die Antwort (Return Message) ebenfalls modelliert werden. Dabei muss überprüft werden, ob die Nachricht im Datenmodell aus Kapitel 7 bereits vorhanden ist. Falls dies nicht der Fall ist, muss sie zur Wahrung der Vollständigkeit ergänzt werden.

Um im Falle von Prüfprozessen entscheiden zu können, ob die dem Prozess zugrundeliegende Anfrage genehmigt oder abgelehnt wird, muss am Ende des Prüfprozesses die erreichbare Sicherheit durch die beantragte Zustandsänderung (Schutzrate, siehe Kapitel 8.3.1) ermittelt werden. Ist diese ausreichend hoch, kann die beantragte Zustandsänderung an den Empfänger (Fahrzeug, Infrastrukturelement) weitergeleitet werden. (Die Ermittlung von Werten für die Berechnung der vorhandenen Schutzrate ist jedoch nicht Teil des Projekts smartLogic, vgl. Kapitel 3.3). Im Falle von Reaktionsprozessen können ggf. notwendige Maßnahmen eingeleitet werden, sobald eine Verminderung der Sicherheit durch die Maßnahme an anderer Stelle (z. B. für eine andere als die ursprünglich betrachtete Fahrzeugbewegung) ausgeschlossen ist.

Da die Identifizierung aller relevanten Prüfbedingungen für das Erreichen der notwendigen Sicherheit kritisch ist und das zu Beginn dieses Abschnitts beschriebene Vorgehen zur Identifikation der relevanten Prüfbedingungen nicht garantieren kann, dass tatsächlich alle relevanten Prüfbedingungen berücksichtigt wurden, erscheint es sinnvoll, im Anschluss an die grafische Modellierung den modellierten Prozess nochmal in Hinblick auf die Erfüllung aller Prüfbedingungen – nicht nur die zuvor identifizierten – zu prüfen und ggf. Ergänzungen bzw. Modifikationen vorzunehmen.

Bei der Modellierung der ersten Prozesse stellte sich heraus, dass die grafisch zu modellierenden Prozesse schnell umfangreich werden. Deswegen erwies es sich als sinnvoll, vor die grafische Modellierung im Verfahren zur Modellierung des Ablaufs von Prozessen bzw. Subroutinen noch eine einfache textuelle Formulierung des grundsätzlichen Prozesses in natürlicher Sprache zu stellen, um in diesem Verfahrensschritt den Prozess besser zu strukturieren. Der Ablauf in natürlicher Sprache lässt sich unkomplizierter anpassen als die grafische Modellierung, wenn zum Beispiel die Reihenfolge der Prozessschritte nochmals verändert werden soll. Auch die Identifizierung der beteiligten externen Systeme wird durch diesen Schritt vereinfacht. Der gesamte Ablauf der Modellierung der Prozessfunktionen und Subroutinen besteht daher aus den in Abb. 56 dargestellten fünf Schritten:

Abb. 56: Verfahren zur Modellierung des Ablaufs der Prozesse und Subroutinen
[Eigene Darstellung]

Wie in den vorherigen Abschnitten dieses Unterkapitels beschrieben, können ggf. mit weiteren UML-Verhaltensdiagrammen weitere Details der Prozesse je nach Bedarf zusätzlich veranschaulicht werden.

8.2.3 Zusammenfassung der gewählten Methode und Vorgehensweise

Im vorliegenden Unterkapitel sollen die Erkenntnisse aus der Diskussion in Kapitel 8.2.2 nocheinmal zusammengefasst und damit die gewählte Methode und Vorgehensweise beschrieben werden.

Die Modellierung der Prozesse und Subroutinen erfolgt in fünf Schritten (vgl. Abb. 56 im Abschnitt „Ablauf der Modellierung der Prozesse und Subroutinen“ von Kapitel 8.2.2). Zunächst müssen die für die jeweilige Funktion relevanten Prüfbedingungen identifiziert werden. Auf dieser Basis wird der Prozess zunächst in natürlicher Sprache beschrieben, weil dieses nicht formale, dynamischere Beschreibungsmittel bei der Strukturierung des Prozessablaufes ein schnelleres Arbeiten als die nachfolgende grafische Modellierung erlaubt. Im dritten Schritt werden beteiligte externe Systeme identifiziert, bevor im vierten Schritt die grafische Modellierung des Prozesses mittels eines UML-Aktivitätsdiagramms erfolgt. Abschließend wird der Prozess erneut gegen alle in Kapitel 6 identifizierten Prüfbedingungen geprüft, um mit hoher Wahrscheinlichkeit ausschließen zu können, dass keine sicherheitskritischen Implikationen des Prozesses übersehen wurden.

Bevor die einzelnen Prozesse und Subroutinen mit der gewählten Methode und Vorgehensweise modelliert werden, sollen in den nächsten beiden Kapiteln jedoch einige Konzepte für die Funktionsweise der smartLogic hergeleitet werden.

8.3 Basis-Konzepte

In diesem Kapitel sollen grundlegende Konzepte bzgl. der Funktionsweise der smartLogic hergeleitet und ausführlich diskutiert werden, welche die weiteren Überlegungen zur Modellierung der einzelnen Prozesse maßgeblich beeinflussen (vgl. Kapitel 8.1). Grundlage der bei der Erarbeitung der Konzepte zu treffenden Abwägungen bilden die spezifischen Anforderungen für das vorliegende Hauptkapitel, die in Kapitel 8.2.1 beschrieben wurden.

Die Reihenfolge der behandelten Konzepte folgt nur teilweise einer bestimmten Logik, da die meisten Konzepte voneinander unabhängig sind. Das Konzept der Schutzrate bildet eine Ausnahme, da es sich um ein Konzept für den Bewertungsmaßstab zur Entscheidung über eine Prüfanfrage handelt und

damit eine Grundlage für die weiteren Konzepte bildet. Deshalb wird dieses Konzept zuerst thematisiert.

8.3.1 Kriterium für die Genehmigung von Prüfanfragen (Schutzrate)

Gemäß Kapitel 3.2 ist eine der beiden Hauptzuständigkeiten der Sicherungslogik als Komponente der infrastrukturseitigen Sicherungstechnik, „die Sicherheit von Zustandsänderungen im Bahnbetrieb wie Fahrerlaubnisse und geplante Statusänderungen von Infrastrukturelementen sicherzustellen“. Dazu prüft die Logik, ob an sie gestellte Prüfanfragen aus dem nicht sicherheitskritischen Bereich (in der Regel vom TMS) zu einem unsicheren Zustand des Systems Bahn führen können (vgl. Kapitel 4.6). Nur, wenn ein unsicherer Zustand mit hinreichender Sicherheit ausgeschlossen werden kann, darf die Prüfanfrage genehmigt werden.

Damit die Kapazität nicht unnötig eingeschränkt wird bzw. die smartLogic auch beim Vorliegen von Störungen noch Betrieb ermöglicht, sollen Prüfanfragen allerdings auch nur zurückgewiesen werden, wenn die „Kernanforderung [der Sicherheit] unter Berücksichtigung aller verfügbaren Informationen tatsächlich nicht erfüllt ist“ (vgl. Kapitel 8.2.1). In diesem Unterkapitel wird deshalb hergeleitet, nach welchen Kriterien entschieden werden kann, ob eine Prüfanfrage zurückgewiesen werden muss oder genehmigt werden kann.

Im ersten Abschnitt wird zunächst der klassische Ansatz (vgl. Kapitel 2.1) mit der Idee eines risikobasierten Ansatzes verglichen, der in den folgenden Abschnitten weiter untersetzt wird. Dazu geht der zweite Abschnitt auf die Bestimmung der Risikoakzeptanzkriterien für die Genehmigung von Prüfanfragen ein, während im dritten Abschnitt hergeleitet wird, wie nicht (vollständig) erfüllte Prüfbedingungen (z. B. eine falsch gestellte Weiche, ein nicht optimaler Flankenschutz, ein nicht vollständig gesicherter Bahnübergang) das tatsächliche Risiko zur Laufzeit der smartLogic beeinflussen. Das tatsächliche Risiko der gesamten Prüfanfrage setzt sich dann aus den verschiedenen Einflüssen zusammen, deren Verknüpfung im vierten Abschnitt untersucht wird. Der fünfte Abschnitt leitet schließlich her, wann ein Prüfprozess abbricht, für den Fall, dass die zugehörige Prüfanfrage nicht genehmigt werden kann. Abschließend erfolgt eine Zusammenfassung im sechsen Abschnitt.

Klassischer und risikobasierter Ansatz

Bei klassischen Stellwerken wurden vor der Inbetriebnahme klare Bedingungen für einzelne Prüfanfragen definiert, die erfüllt sein müssen, damit die entsprechende Prüfanfrage genehmigt werden kann. Bei Fahrstraßenstellwerken sind zum Beispiel für jede einstellbare Fahrstraße die entsprechenden Weichenlagen der beteiligten Elemente festelegt sowie weitere Kriterien, wie Blockbedingungen. Bei Spurplanstellwerken existiert ebenfalls ein festes Regelset an Bedingungen, allerdings werden die beteiligten Elemente, z. B. Weichen, mittels einer dynamischen Suche identifiziert. Vergleiche zu diesem Absatz Kapitel 2.1.2.

Die klassischen Regeln der Stellwerkslogik und damit verbunden auch die Zulassungskritieren für Fahrzeugbewegungen sind in einem evolutionären Prozess entstanden (vgl. Kapitel 2.1). Für eine Neuentwicklung auf der Grünen Wiese – wie für diese Arbeit gefordert – wird jedoch eine systematische Methode zur Bestimmung des Kriteriums für die Genehmigung von Prüfanfragen benötigt. Hierfür liegt es nahe, auf die Methode der Sicherheitsnachweisführung für sicherheitskritische Eisenbahnsysteme zurückzugreifen. Dabei wird im Rahmen einer Risikoanalyse eine ***tolerierbare Gefährdungsrate*** (***Tolerable Hazard Rate*** **THR**) als Risikoakzeptanzkriterium für die jeweilige Systemkomponente (hier die Sicherungslogik) bestimmt (vgl. die Erläuterungen zum V-

Modell in Kapitel 2.6.1). Die Systemkomponente muss dann ihrerseits garantieren, dass die THR eingehalten wird.

Normalerweise erfolgt diese Risikobetrachtung beim Entwurf der Systemkomponente, für die die Risikoanalyse durchgeführt wird. Dabei können jedoch nur pauschale Erfahrungswerte zur Einschätzung der jeweiligen Risiken berücksichtigt werden. Das tatsächliche Risiko der Gefährdung einer Fahrzeugbewegung zu einem bestimmten Zeitpunkt hängt jedoch von der betrieblichen Situation zu diesem Zeitpunkt ab. Beispielsweise hängt das tatsächliche Risiko einer Flankenfahrt nicht nur vom Status der stellbaren Fahrwegelemente, sondern auch von den Positionen der Fahrzeuge bzw. Fahrzeugbewegungen ab (bzw. davon, wie sicher diese Positionen bekannt sind), da Letzteres bestimmt, ob überhaupt andere Fahrzeuge bzw. Fahrzeugbewegungen als potenzielle Gefährder die Gefahrstelle erreichen können.

Um diese Einflüsse berücksichtigen zu können, sollte mindestens ein Teil der Risikoberechnung nicht beim Entwurf der Systemkomponente pauschal zur sicheren hin abgeschätzt, sondern zur Laufzeit dynamisch durchgeführt werden. In den folgenden Abschnitten dieses Kapitels soll ein Konzept für eine solche dynamische Risikobetrachtung zur Laufzeit der smartLogic hergeleitet werden.

Risikoakzeptanzkriterium für eine Prüfanfrage

Wie bereits im vorigen Abschnitt erwähnt, wird im Rahmen der Risikoanalyse für eine sicherheitskritische Systemkomponente eine tolerierbare Gefährdungsrate (THR) bestimmt, die als Risikoakzeptanzkriterium fungiert. Darüber wird also das akzeptable (Rest-)Risiko für den Betrieb dieser Systemkomponente bestimmt. Das akzeptable Risiko muss gemäß der Vorgehensweise in [DIN EN 50126-1:2017] aus dem erforderlichen Sicherheitsintegritätslevel (SIL) (in der Regel SIL 4) bestimmt werden (vgl. Kapitel 2.6.1 und 3.6 in dieser Arbeit). Die Einheit ist dabei in der Regel die Anzahl von kritischen Fehlern (z. B. Unfälle mit Todesfällen) pro Zeiteinheit (meist pro Stunde).

Da die THR für die gesamte Systemkomponente gilt, es innerhalb dieser Systemkomponente jedoch mehrere risikobehaftete Prozesse als unabhängige Funktionen der smartLogic gibt (vgl. Kapitel 6.3), muss das akzeptierte Risiko auf die einzelnen Arten von Prozessen aufgeteilt werden; das akzeptierte Risiko ist also für die einzelnen Prozesse geringer als die THR. In EN 50126 existiert hierfür der Begriff „***Tolerierbare funktionale Ausfallrate***“ (**TFFR**). Die THR muss dabei auf alle Prozesse aufgeteilt werden; da aber nur bei Prüfprozessen über deren Genehmigung oder Zurückweisung zu entscheiden ist, ist nur für diese Prozesse ein Risikoakzeptanzkriterium sinnvoll. Da die Prozesse auch mehrfach in der angegebenen Zeiteinheit durchgeführt werden können, muss das akzeptierte Risiko weiter auf die einzelnen Instanzen der Prozesse (hier z. B. einzelne vom TMS gestellte Prüfanfragen) aufgeteilt werden (z. B. anhand durchschnittlicher Zahlen von solchen Prozessinstanzen pro Zeiteinheit). Aus diesem letzten Schritt ergibt sich dann ein Risikoakzeptanzkriterium als **Schwellwert**, dessen Unterschreitung zur Genehmigung der Prüfanfrage garantiert werden muss.

Ein Ermitteln konkreter Werte für den Schwellwert für die einzelnen Arten von Prüfanfragen ist im Rahmen dieser Arbeit allerdings aufgrund des erforderlichen Zeitaufwands nicht möglich (vgl. Kapitel 3.3 und 3.6.4).

Bestimmung des tatsächlichen Risikos einer Prüfanfrage zur Laufzeit

Für die Entscheidung über die Genehmigung einer Prüfanfrage muss nun noch das tatsächliche Risiko einer Gefährdung einer Fahrzeugbewegung durch diese Prüfanfrage (auch **Gefährdungsrisiko**) im Kontext des aktuellen Betriebsgeschehens, also zur Laufzeit der smartLogic bestimmt werden. Das aktuelle Gefährdungsrisiko muss demnach von der smartLogic ermittelt und zur Bewertung der Sicherheit in Relation zum aus der TFFR ermittelten Schwellwert gesetzt werden.

Zur klaren Abgrenzung von den allgemeinen Begriffen aus dem vor der Zulassung eines Systems durchzuführenden Sicherheitsnachweis, wird im Folgenden ein neuer Begriff für das durch die Sicherungslogik zur Laufzeit zu ermittelnde Gefährdungsrisiko durch eine nicht (vollständig) erfüllte (= „**verletzte**“) **Prüfbedingung** eingeführt. Die Höhe dieses zu bestimmenden, aktuellen Risikos wird im Folgenden mit der **Schutzrate („Protection Rate“, PR)** ausgedrückt, wobei eine hohe Schutzrate ein niedriges Risiko bedeutet; damit ist die Schutzrate also eine inverse Abbildung des Risikos[38]. Die Höhe des Risikos für die gesamte Prüfanfrage wird mit der Gesamt-Schutzrate ausgedrückt (siehe Abschnitt „Verknüpfung der Schutzraten der Prüfbedingungen“).

Im ersten Unterabschnitt wird hergeleitet, welcher Wertebereich für die Angabe der Schutzrate sinnvoll ist und wie sie berechnet werden kann. Im zweiten Unterabschnitt wird dann im Sinne der gewählten Berechnungsmöglichkeit auf die einzelnen Bestandteile der Schutzrate näher eingegangen. Anschließend wird im dritten Unterabschnitt in Ergänzung zum zweiten Unterabschnitt im Sinne der Anforderung der Rückfallebenenintegration untersucht, wie risikomindernde Einflüsse bei der Berechnung der Schutzrate berücksichtigt werden können. Der vierte Unterabschnitt befasst sich mit einer möglichen Methode, wie die Werte der verschiedenen Einflussgrößen, die in die Berechnung der Schutzrate einfließen, bestimmt werden können. Ein Ermitteln konkreter Werte für die einzelnen Einflussgrößen ist im Rahmen dieser Arbeit allerdings nicht zu leisten (vgl. Kapitel 3.3 und 3.6.4).

Wertebereich und Berechnungsmöglichkeiten der Schutzrate

Gemäß ihrer Definition im vorigen Abschnitt spiegelt die Schutzrate das inverse Risiko und damit (vereinfacht ausgedrückt[39]) die Wahrscheinlichkeit wieder, mit der es zu keinem (schweren) Unfall kommt. Daher ist es sinnvoll, die Schutzrate als Wert zwischen 0 (völlig unsicher) und 1 (= 100 %) (sicher) anzugeben. Hierdurch kann auch eine Normierung der verschiedenen Einflüsse auf die Schutzrate erreicht werden. Es sind jedoch mehrere Methoden denkbar, wie die Werte interpretiert und errechnet werden können.

1. Es wird vom Stillstand als sicherem Zustand ausgegangen, bei dem die Schutzrate 100 % entspricht.
   - Eine Prüfanfrage des TMS wird zunächst als unsicher angenommen und eine entsprechend niedrige Gesamt-Schutzrate als Ausgangspunkt verwendet. Die genaue Höhe der Ausgangsschutzrate vor Prüfung der Prüfbedingungen wird durch die Parameter der Prüfanfrage bestimmt, wie beispielsweise das Geschwindigkeitsprofil. Eine (teilweise) erfüllte Prüfbedingung erhöht die Sicherheit der Anfrage und damit auch die Gesamt-Schutzrate. Wie stark die Gesamt-Schutzrate erhöht wird, hängt vom Erfüllungsgrad der Prüfbedingung und damit der Schutzrate der Prüfbedingung ab (zum Beispiel bietet physischer Flankenschutz eine höhere Sicherheit als Flankenschutz durch operative Maßnahmen). Insgesamt muss der Schwellwert für das Vorhandensein von Sicherheit überschritten werden, der vermutlich zwar nahe bei 100 %, aber immer unterhalb von 100 % liegt, denn wie oben gesagt, wird Stillstand

[38] Die Angabe eines inversen Risikos hat keinen grundlegenden Vorteil gegenüber der Angabe eines Risikos, da sich beides ohne Probleme ineinander umrechnen lässt; vereinfacht aber die Veranschaulichung der Verknüpfung der Einflüsse verschiedener Prüfbedingungen auf die Gesamtbewertung der Genehmigungsfähigkeit einer Prüfanfrage.

[39] Siehe in der folgenden Aufzählung bei 2.: Die Basis-Schutzrate von 1 für eine Prüfanfrage muss noch mit dem Grundrisiko für diese Prüfanfrage multipliziert werden, um die tatsächliche Wahrscheinlichkeit einer Gefährdung zu erhalten.

gemeinhin als sichererer Zustand betrachtet, als wenn Fahrzeuge in Bewegung sind.

2. Für die verschiedenen Prüfbedingungen wird jeweils eine Basis-Schutzrate (Schutzrate = 100 %) definiert, die dem höchsten erreichbaren Schutzniveau (ohne Berücksichtigung von nicht in jedem Fall notwendigen risikomindernden Einschränkung der Fahrweise der Fahrzeugbewegung (z. B. Vorgabe einer reduzierten Geschwindigkeit im Vergleich zur infrastrukturseitig vorgegebenen Geschwindigkeit)) entspricht (die Prüfbedingung kann dann als vollständig erfüllt betrachtet werden).
   - Dieser zweite Ansatz basiert auf der Annahme, dass im Regelfall die meisten Prüfbedingungen vollständig erfüllt sein werden und damit von einem akzeptablen, minimalen Risiko ausgegangen werden kann (z. B. Bahnübergang ist sicher vollständig geschlossen und freigemeldet). Gleichzeitig handelt es sich bei vollständig erfüllten Prüfbedingungen um die maximal erreichbare Schutzrate (bezogen auf die einzelne Prüfbedingung). Ist eine Prüfbedingung nicht vollständig erfüllt (also verletzt), würde sich eine niedrigere Schutzrate als 100 % für die Prüfbedingung ergeben (z. B. Bahnübergang ist zwar vollständig geschlossen, aber nicht freigemeldet). Eine Prüfanfrage könnte von der smartLogic genehmigt werden, falls die Gesamt-Schutzrate den Schwellwert für das Vorhandensein von Sicherheit nicht unterschreitet.
   - Gegebenenfalls könnte bei dieser Methode vor der Zulassung ein Grundrisiko für die jeweilige Prüfanfrage zur Abbildung des Risikos bei Vorliegen der Basis-Schutzrate bestimmt werden, welches vom aus der Risikoanalyse ermittelten Schwellwert für die Genehmigung dieser Prüfanfrage abgezogen wird. Die Schutzrate würde dann nur die weiteren Risiken abbilden, die über das Grundrisiko hinausgehen.

Bei der ersten Methode muss für jede Prüfbedingung und für jeden möglichen Grad der Erfüllung die resultierende Erhöhung der Schutzrate zur Laufzeit der smartLogic bestimmt werden. Bei der zweiten Methode muss dagegen nur für nicht erfüllte oder teilweise nicht erfüllte Prüfbedingungen der Einfluss auf die Schutzrate durch die smartLogic zur Laufzeit ermittelt werden, nicht aber der Beitrag einer vollständig erfüllten Prüfbedingung. Entsprechend sind für die erste Methode auch deutlich mehr Parameter im Vorfeld zu bestimmen, auf der die Berechnungen aufbauen können.

Die *Kernanforderung der sicheren Logik* wäre bei beiden Methoden erfüllt. Da davon ausgegangen werden kann, dass das TMS die Anfragen so stellt, dass die meisten Prüfbedingungen vollständig erfüllt sein werden, ist damit zu rechnen, dass die zweite Methode den Berechnungsaufwand signifikant reduziert und daher die Anforderung der *geringen Latenz* besser erfüllt. Weiterhin wird durch die geringere Anzahl an benötigten Parametern auch die Anforderung der *schlanken Logik* besser erfüllt. Aus diesem Grund wird im Folgenden die zweite Methode weiterverfolgt.

Bestandteile der Schutzrate

Da die Schutzrate das aktuelle Gefährdungsrisiko abbildet, kann die allgemeine Definition von Risiko als Ausgangspunkt genommen werden. Demnach berechnet sich das Risiko als Produkt des Schadensausmaßes (in der Beispielformel a_i) und der Eintrittswahrscheinlichkeit (in der

Beispielformel x_i) der Gefährdung, wobei beide Faktoren im Einzelfall auch als Funktion von weiteren Parametern angegeben werden können.

Falls verschiedene voneinander unabhängige Einflüsse existieren, die das Ergebnis der Prüfbedingung beeinflussen (z. B. der aktuelle Zustand von verschiedenen Weichen, die in der beantragten Route einer Fahrerlaubnis liegen oder mehrere Fahrzeuge, die potenziell eine Flankenschutzgefährdung verursachen könnten), müssen die einzelnen Einflüsse gemäß den Regeln der Statistik als Faktoren mit Werten zwischen 0 und 1 in die Berechnung der Schutzrate eingehen. (Abhängige Einflüsse müssen in einem gemeinsamen Term beschrieben werden, in dem die Abhängigkeit in den Parametern ausgedrückt wird. Die Abhängigkeit kann dabei individuell sehr verschieden sein, weshalb hier keine allgemeinen Regeln für diesen Fall angegeben werden können.) Die Schutzrate mit n unabhängigen Einflüssen setzt sich daher wie folgt zusammen:

$$Schutzrate\ f\ddot{u}r\ die\ Pr\ddot{u}fbedingung = \prod_{i=1}^{n}(1 - a_i x_i)\ mit\ a_i x_i \in [0,1] \quad [40]$$

Berücksichtigung risikomindernder Einflüsse auf die Schutzrate

Unter bestimmten Voraussetzungen ist es denkbar, dass eine Verringerung der Schutzrate für eine Prüfbedingung durch risikomindernde Eigenschaften der beantragten[41] Prüfanfrage wieder ausgeglichen werden kann. Zum Beispiel könnte eine niedrigere, beantragte Geschwindigkeit als die theoretisch mögliche, sichere Regelgeschwindigkeit das Risiko aus einer Achslastüberschreitung oder das Befahren eines nicht freigemeldeten Bahnübergangs bis zu einem gewissen Grad im Vergleich zur Situation mit Regelgeschwindigkeit reduzieren.

Es ist daher denkbar, dass solche Eigenschaften den negativen Einfluss auf die Schutzrate wieder teilweise ausgleichen. Eine Überkompensation ist jedoch nicht möglich, da die Schutzrate gemäß ihrem definierten Wertebereich nicht größer als ‚1' sein darf. Abb. 57 verdeutlicht das Prinzip. Mit diesem Ausgleichsmechanismus beschäftigt sich Kapitel 8.3.6 näher.

[40] Sind alle Einflüsse auf die Schutzrate optimal, wären alle Faktoren 1 und die Schutzrate damit ebenfalls 1. Liegt ein nicht kompensierbarer negativer Einfluss vor, z. B. eine falsch gestellte Weiche, würde der entsprechende Faktor 0 und damit die gesamte Schutzrate 0. Liegen zwei die Schutzrate reduzierende Einflüsse von 90 % vor, wäre die Schutzrate noch 81 Prozent.

[41] Das TMS muss den risikomindernden Einfluss also bereits in den Parametern der Prüfanfrage beantragt haben, als es die Prüfanfrage an die smartLogic übermittelt und damit den Prüfprozess gestartet hat. Die Einflüsse werden nicht nachträglich eingefügt. Vergleiche hierzu auch Kapitel 4.3.1.

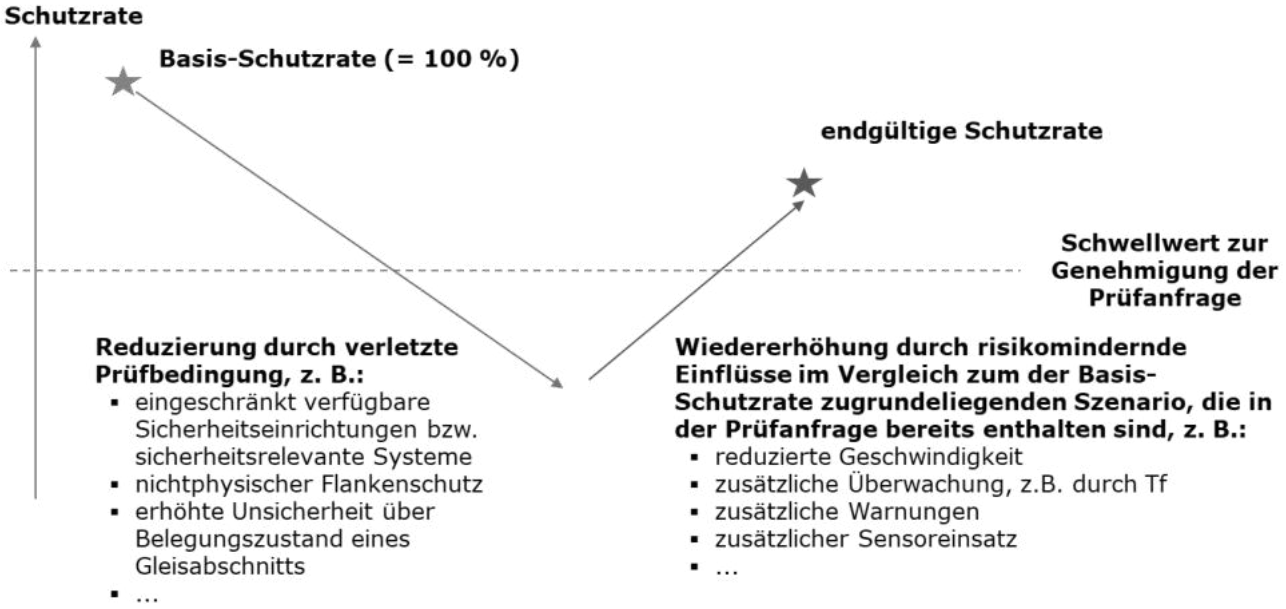


Abb. 57: Prinzip der Schutzrate
[Eigene Darstellung]

Exkurs: Mögliche Methode zur Ermittlung der Werte für die Berechnung der Schutzrate

Gemäß der Abgrenzungen des Bearbeitungsumfangs in dieser Arbeit in Kapitel 3.3 ist die Ermittlung von Zahlenwerten nicht Teil dieser Arbeit. Das gilt auch für die Ermittlung von Werten zur Quantifizierung der Schutzrate. Um eine bessere Nachvollziehbarkeit des Konzepts der Schutzrate zu erreichen, wird an dieser Stelle jedoch ein kurzer Ausblick auf eine mögliche Methode zur Ermittlung von Werten für Einflüsse auf die Berechnung der Schutzrate gegeben.

Eine solche mögliche Methode können z. B. Ereignisbäume sein, wie sie häufig in Risikoanalysen verwendet werden (vgl. z. B. [Wang & Roush 2000, 69ff]). Diesen liegt die Überlegung zugrunde, dass von jedem Ausgangsereignis ein Pfad über verschiedene weitere Ereignisse oder begünstigende Umstände bis zu einer Gefährdung existiert. Jedem dieser Ereignisse oder Umstände kann eine Wahrscheinlichkeit zugeordnet werden, mit der das Ereignis eintritt bzw. der Umstand vorliegt. Die Wahrscheinlichkeit für den Eintritt der Gefährdung auf Basis des betrachteten Ausgangsereignisses ist dann das Produkt der Einzel-Wahrscheinlichkeiten auf dem Pfad.

Abb. 58 zeigt ein Beispiel eines solchen Ereignisbaums. Zugrunde liegt das Ausgangsereignis, wonach sich Wagen eines sich von der zu schützenden Fahrzeugbewegung wegbewegenden Personenzuges lösen. Zu sehen sind mehrere Ereignisketten, von denen drei im Ergebnis zu einer Flankenfahrt mit der zu schützenden Zugfahrt führen. Die eingetragenen Wahrscheinlichkeiten dienen nur der Veranschaulichung und haben keinen realen Hintergrund.

Liegt nun eine Flankenschutz-Situation vor, welche den beschriebenen Fall nicht ausschließen kann, weil zwischen der zu schützenden Fahrzeugbewegung und dem sich von ihr wegbewegenden Personenzug kein phyisches Flankenschutzelement liegt, könnte die Schutzrate um die ermittelten Wahrscheinlichkeiten der potenziellen Kollisions-Ereignisketten reduziert werden.

An dieser Stelle sei noch darauf hingewiesen, dass es keine Voraussetzung für die smartLogic darstellt, alle potenziellen Einflüsse auf die Schutzrate vorher ermittelt zu haben. Da Einflüsse immer als normierter Faktor mit einem Wert zwischen 0 und 1 in die Berechnung der Schutzrate eingehen (siehe erster Unterabschnitt dieses Abschnitts), kann bei Unkenntnis eines genauen Risikos auch der Faktor zur sicheren Seite hin auf 0 gesetzt werden, wodurch, falls das Ereignis nicht mit hinreichender

Sicherheit ausgeschlossen werden kann, die Schutzrate auf 0 reduziert und die Anfrage immer abgelehnt werden würde.

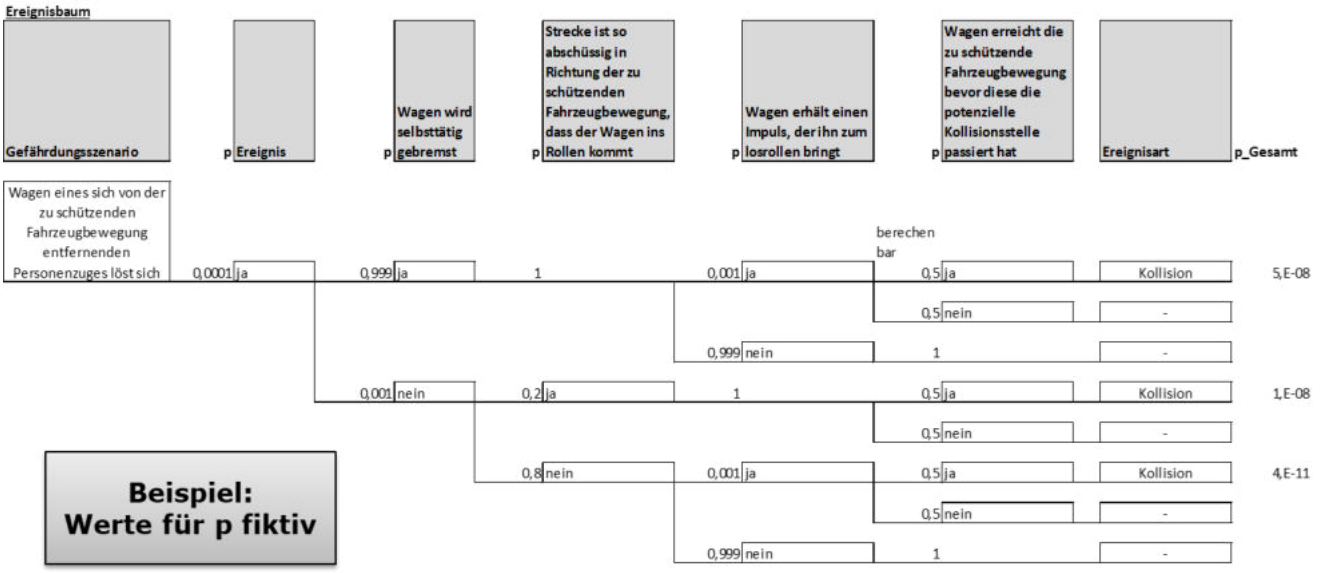


Abb. 58: Beispiel eines Ereignisbaums
[Eigene Grafik, angelehnt an die Darstellung in der ETCS-Risikoanalyse der DB Netz AG]

Verknüpfung der Schutzraten der Prüfbedingungen

Das akzeptable Risiko in Form des Schwellwertes bezieht sich auf die gesamte Prüfanfrage und nicht auf die Erfüllung einzelner Prüfbedingungen. Sollte daher als Ergebnis der Prüfung einer Prüfbedingung eine Senkung der Schutzrate ermittelt worden sein, die aber den Schwellwert für die Genehmigung von Prüfanfragen nicht unterschreitet und damit nicht sofort zur Zurückweisung der Prüfanfrage führt, muss die abgesenkte Schutzrate bei der weiteren Prüfung berücksichtigt werden. Diese Berücksichtigung ist erforderlich, denn weitere verletzte Prüfbedingungen, die ebenfalls für sich genommen den Schwellwert überschreiten würden, könnten in Kombination dazu führen, dass der Schwellwert unterschritten wird und daher die Prüfanfrage abgelehnt werden muss. Deshalb beschäftigt sich dieser Abschnitt damit, wie die bei der Prüfung von Prüfbedingungen errechneten eingeschränkten Schutzraten zur Berechnung der Gesamt-Schutzrate verknüft werden können.

Bei der Verknüpfung wird davon ausgegangen, dass das Risiko einer Gefährdung mit jeder zusätzlichen verletzten Prüfbedingung steigt, selbst wenn es sich nur um kleine Verletzungen handelt. Wie genau das Risiko steigt und damit die Schutzrate sinkt, hängt statistisch davon ab, ob die einzelnen Einflüsse (hier die Schutzraten der verletzten Prüfbedingungen) voneinander unabhängig sind. Mit dieser Frage beschäftigt sich der erste Unterabschnitt. Zudem ist zu klären, ob die Länge der Fahrerlaubnis bei der Berechnung der Gesamt-Schutzrate zu berücksichtigen ist, da eine lange Fahrerlaubnis potenziell mehr Gefährdungen ausgesetzt ist als eine kurze. Diese Klärung erfolgt im zweiten Unterabschnitt.

Annahme der Unabhängigkeit

Um den Einfluss der Schutzrate von verletzten Prüfbedingungen auf die Gesamt-Schutzrate zu bestimmen, ist wichtig, ob dieser Einfluss vom Erfüllungsgrad anderer Prüfbedingungen abhängt oder

als davon unabhängig betrachtet werden kann[42]. Eine eindeutige Antwort auf diese Frage ist schwierig zu finden, da hierfür die Abhängigkeiten zwischen allen Kombinationen von Prüfbedingungen betrachtet werden müssten.

Abhängigkeiten mit erhöhendem Einfluss auf die Schutzrate (wenn z. B. eine Überschreitung der maximalen Schließzeit eines BÜ eine Gefährdung durch einen fälschlich geöffneten BÜ weniger wahrscheinlich machen würde) dürften eher selten sein und würden sich nur zur sicheren Seite hin auswirken, also die Gesamt-Schutzrate würde bei Annahme der Unabhängigkeit unterschätzt werden. Sie können daher vernachlässigt werden.

Abhängigkeiten mit einem negativen Einfluss auf die Schutzrate (wenn z. B. ein eingeschränkter Flankenschutz einen Unfall durch Achslastüberschreitung wahrscheinlicher machen würde, als das Gefährdungsrisiko durch die Achslastüberschreitung ohnehin ist[43]), könnten dagegen bei Annahme der Unabhängigkeit zu einer Überschätzung der Schutzrate und daher zu einem Sicherheitsrisiko führen.

Da eine Untersuchung aller möglichen Abhängigkeiten in dieser Arbeit aufgrund der zeitlichen Rahmenbedingungen nicht möglich ist, muss zur Vereinfachung an dieser Stelle angenommen werden, dass der Einfluss der Schutzrate der einzelnen Prüfbedingungen auf die Gesamt-Schutzrate voneinander unabhängig ist. In diesem Fall könnte, analog zur Berechnung der Schutzrate für die einzelnen Prüfbedingungen aus den gewichteten Einflüssen einzelner Ereignisse, für jede Prüfbedingung die Schutzrate separat bestimmt werden und die Gesamt-Schutzrate als Produkt der Schutzraten für die einzelnen Prüfbedingungen errechnet werden.

Die Annahme der Unabhängigkeit kann dadurch gestützt werden, dass der Autor bei einer ersten Sichtung der Prüfbedingungen keine offensichtlichen Beispiele für Abhängigkeiten mit negativem Einfluss auf die Gesamt-Schutzrate finden konnte. Bei der Entwicklung eines Produktivsystems sollte jedoch dieser Punkt durch Fachexperten eingehender untersucht werden.

Einfluss der Länge der Fahrerlaubnis

Bei einigen Prüfbedingungen korrespondiert die Anzahl der Einflüsse und damit der möglichen Gefährdungen mit der Länge der Fahrerlaubnis. Eine lange Fahrerlaubnis hätte dann eine größere Wahrscheinlichkeit einer niedrigen Schutzrate als eine kurze. Bei kürzeren Fahrerlaubnissen würden allerdings insgesamt auch mehrere Fahrerlaubnisanfragen benötigt und das akzeptable Risiko müsste somit auf mehrere einzelne Prüfanfragen verteilt werden. Dadurch würde der Schwellwert für die Genehmigung einer einzelnen Prüfanfrage reduziert und es ergäbe sich kein Vorteil gegenüber längeren Fahrerlaubnissen.

Abbruch des Prüfprozesses

Sinkt die Schutzrate unter den Schwellwert, kann die Prüfanfrage nicht genehmigt werden. Dies kann entweder am Ende der Prüfung einer Prüfbedingung festgestellt werden oder – falls keine verletzte Prüfbedingung die Schutzrate unmittelbar unter den Schwellwert gedrückt hat – am Ende des Prüfprozesses bei der Berechnung der Gesamt-Schutzrate. Dabei stellt sich die Frage, ob der Prüfprozess unmittelbar abbrechen soll, sobald festgestellt wurde, dass die Schutzrate nicht ausreichend für die Genehmigung der Prüfanfrage ist (erster Unterabschnitt). Weiterhin stellt sich im

[42] Es geht an dieser Stelle nur um die Höhe des Einflusses des Erfüllungsgrades einer einzelnen Prüfbedingung auf die Schutzrate und nicht um die Gesamthöhe der Schutzrate. Die Gesamthöhe muss immer alle Einflüsse nicht erfüllter Prüfbedingungen berücksichtigen.

[43] Es handelt sich um ein fiktives Beispiel.

Sinne der Anforderung der *geringen Latenz* die Frage, ob die Schutzrate überhaupt immer berechnet werden muss. Hiermit beschäftigt sich der zweite Unterabschnitt.

Zeitpunkt des Beendens des Prüfprozesses

Nachdem sich herausgestellt hat, dass eine Prüfanfrage zurückgewiesen werden muss, stellt sich die Frage,

1. ob auch der Prüfprozess sofort beendet werden sollte oder
2. ob der Prüfprozess dennoch bis zum Ende durchlaufen sollte.

Bei der ersten Lösung würde im Vergleich zur zweiten Lösung im Sinne der Anforderung der *geringen Latenz* Berechnungsaufwand gespart. Gleichzeitig würden allerdings weitere nicht erfüllte Prüfbedingungen erst bei der Prüfung einer erneuten, vom TMS zur Behebung des ersten Abbruchgrundes modifizierten Anfrage auffallen. Damit würden weitere Ablehnungen der Anfrage und damit weitere Kommunikation zwischen TMS und smartLogic riskiert, wodurch wieder eine Erhöhung der Latenz auftreten könnte.

Allerdings kann angenommen werden, dass die meisten Anfragen vom TMS bereits so gestellt werden, dass sie von der smartLogic genehmigt werden würden. Daher erscheint der Mehraufwand der unnötig weiterzuführenden Prüfung der originalen Prüfanfrage bei der zweiten Lösung den dadurch entstehenden Nutzen durch möglicherweise zusätzlich zu findende nicht erfüllte Prüfbedingungen nicht zu überschreiten. Deshalb wird die erste Lösung bevorzugt.

Direkter Abbruch ohne Prüfung der Schutzrate

Einige Prüfbedingungen senken im Fall ihrer Verletzung die Schutzrate immer unter den Schwellwert. In diesem Fällen ist es unnötig, die Schutzrate erst noch auszurechnen; stattdessen kann ein Fehlercode (vgl. „Request Return Message (RRM)“ in Kapitel 7.7.1) an das den Prüfprozess aufrufende System (i. d. R. das TMS) übergegeben werden, damit dieses den Abbruchgrund einordnen kann. Daher wird bei der Modellierung eine Unterscheidung zwischen Prüfbedingungen, deren Verletzung zum sofortigen Abbruch des Prüfprozesses führen, und Prüfbedingungen, bei denen die Schutzrate ausgerechnet werden sollte, vorgenommen (vgl. Tab. 42). Die dargestellten Farben werden zur Veranschaulichung in der grafischen Modellierung in den Entscheidungsknoten (Rauten) der Aktivitätsdiagramme verwendet (siehe Kapitel 8.5 und 8.6).

Da es theoretisch auch möglich sein könnte, dass eine verletzte Prüfbedingungen durch zusätzliche interne Aktivitäten der smartLogic kompensiert werden kann, ohne dass durch die Verletzung eine unmittelbare Auswirkung auf die Schutzrate entsteht (z. B. ein ausgefallener Sensor, bei dem die fehlende Information ersatzweise durch einen zusätzlichen Prüfalgorithmus beschafft oder aus anderen verfügbaren Informationen hergeleitet werden kann), wird noch eine weitere Farbe (grün) eingefügt.

Tab. 42: Farbliche Zuordnung der Folgen einer verletzten Prüfbedingung

rot (Variante 1)	Die Prüfanfrage muss in jedem Fall zurückgewiesen werden. –> Schutzrate wird nicht berechnet, Prüfprozess bricht ab. Fehlercode wird an den Aufrufer der Prozessfunktion (i. d. R. das TMS) übergeben
gelb (Variante 2)	Die Verletzung der Prüfbedingung führt nicht in jedem Fall zur Ablehnung der Prüfanfrage bzw. eine Ablehnung kann ggf. durch risikomindernde Eigenschaften, die bereits in der Fahrerlaubnis enthalten sind, verhindert werden –> Schutzrate wird berechnet
grün	Die Verletzung der Prüfbedingung hat keine Auswirkung auf die Genehmigung der Prüfanfrage, sondern kann in jedem Fall innerhalb der Sicherungslogik kompensiert werden.

Zusammenfassung

Die smartLogic verwendet zur Bewertung der Zulässigkeit von Prüfanfragen einen risikobasierten Ansatz. Dabei wird für die einzelnen Prüfanfragen ein Risikoakzeptanzkriterium aus der Risikoanalyse hergeleitet, das das maximal akzeptable Risiko und damit einen Schwellwert für die Genehmigung der Prüfanfrage darstellt. Das tatsächliche Gefährdungsrisiko wird zum Zeitpunkt der Prüfanfrage, also zur Laufzeit der smartLogic, gemäß der Definition von Risiko als Produkt aus Schadensausmaß und Eintrittswahrscheinlichkeit berechnet. Dabei wurde der Begriff der Schutzrate eingeführt, wobei die Schutzrate dem inversen zur Laufzeit berechneten Risiko entspricht.

Die Schutzrate einer Prüfbedingung errechnet sich als Produkt der verschiedenen gewichteten Einflüsse auf den Grad der Erfüllung der Prüfbedingung, wobei als Ausgangswert eine Basis-Schutzrate von 1 angenommen wird. Die Basis-Schutzrate beschreibt den Fall, in dem die Prüfbedingung vollständig erfüllt ist und die Anfrage keine nicht erforderlichen Einschränkungen (z. B. eine niedrigere Geschwindigkeit als notwendig) enthält. Die Einflüsse können sich sowohl risikoerhöhend als auch risikomindernd auswirken. Allerdings kann die Schutzrate definitionsgemäß für eine einzelne Prüfbedingung nur Werte zwischen 0 und 1 annehmen, es kann also keine Überkompensation von (verletzten) Prüfbedingungen stattfinden.

Die Gesamt-Schutzrate der Prüfanfrage errechnet sich als Produkt der Schutzraten der einzelnen verletzten Prüfbedingungen, da die Einflüsse der verschiedenen Prüfbedingungen auf die Gesamt-Schutzrate als unabhängig voneinander angenommen wurden.

Die errechnete Schutzrate führt zur Ablehnung einer Prüfanfrage, wenn der Schwellwert für die Prüfanfrage unterschritten wird. Wird eine Prüfanfrage abgelehnt, bestimmt die smartLogic gemäß Kapitel 4.3.1 nicht selbstständig Kompensationsmaßnahmen für nicht erfüllte Prüfbedingungen, wie eine niedrigere Geschwindigkeit; Kompensationsmaßnahmen können als positive Einflüsse auf die Schutzrate nur berücksichtigt werden, wenn das TMS sie bereits als Parameter der Prüfanfrage beantragt hat. Sollte die Prüfanfrage nicht genehmigt werden können, erhält das TMS stattdessen einen detaillierten Fehlerbericht im Rahmen der Request Return Message (vgl. Kapitel 7.7.1), um selbst Kompensationsmaßnahmen für den oder die Ablehnungsgründe zu entwickeln und dann eine neue, angepasste Prüfanfrage stellen zu können.

Einige Prüfbedingungen führen bei Nichterfüllung immer zum Abbruch des Prüfprozesses (z. B. wenn die umzustellende Weiche nicht identifiziert wurde). Die Schutzrate braucht in diesen Fällen nicht berechnet zu werden. Ob die Schutzrate berechnet wird oder die Prüfanfrage sofort zurückgewiesen wird, wird zur besseren Veranschaulichung durch farbig gefüllte Entscheidungsknoten (Rauten) in den Aktivitätsdiagrammen in den Kapiteln 8.5 und 8.6 dargestellt (vgl. Tab. 42).

8.3.2 Räumliche Grenzen der MA (Zielpunkte und zugehörige Sicherheitsreserven, Durchrutschweg, Gefahrpunktabstand, EoA, SvL)

Mittels der Fahrerlaubnis (MA) wird einer Fahrzeugbewegung gestattet, einen darin festgelegten Gleisabschnitt zu nutzen. Die räumlichen Grenzen der MA werden vom TMS aufgrund von betrieblichen Überlegungen gewählt und von der Sicherungslogik dahingehend überprüft, ob die Wahrscheinlichkeit für eine Gefährdung der Fahrzeugbewegung im gewählten Gleisabschnitt hinreichend gering ist. Nach der erfolgreichen Prüfung und Übermittlung der MA an das Fahrzeug muss die Sicherungslogik dann den nun von der Fahrzeugbewegung beanspruchten (vgl. Konzept der Beanspruchung aus Kapitel 7.6.2) Gleisabschnitt auf unvorhergesehene Ereignisse wie eine eingehende Meldung einer Statusänderung einer darin enthaltenen Weiche überwachen.

In diesem Unterkapitel soll hergeleitet werden, nach welchen Regeln die Sicherungslogik über eine Zulassung der räumlichen Grenzen der Fahrerlaubnis entscheiden soll. Der Startpunkt liegt dabei natürlicherweise an der letzten bekannten Position der Fahrzeugbewegung (siehe erster Abschnitt). Deshalb beschäftigt sich das Kapitel insbesondere mit den Zielpunkten. Der Begriff „**Zielpunkt**“ dient in diesem Zusammenhang als generischer Oberbegriff für Punkte auf der Gleistopologie, die aus Sicherheitsgründen von der Fahrzeugbewegung bzw. dem Triebfahrzeugführer für die Berechnung von Bremskurven bzw. des Bremseinsatzpunktes verwendet werden.[44]

Einen solchen Zielpunkt bildet auch das Ende des Sicherheitsabstandes, hinter dem von der Fahrzeugbewegung als Ziel ihrer Bremsung anzusteuernden Zielpunkt der MA. Dieser Sicherheitsabstand wird in der klassischen Sicherungstechnik (in vielen Ländern) mit Durchrutschwegen bzw. Gefahrpunktabständen gesichert (vgl. Kapitel 2.1.1), da auch der für den Sicherheitsabstand benötigte Gleisabschnitt von der Sicherungslogik als von der Fahrzeugbewegung beansprucht angesehen und überwacht werden muss. Die genannten klassischen Konzepte des Durchrutschwegs und Gefahrpunktabstands sind auch in das europäische Zugsicherungssystem ETCS übernommen worden („Overlap“, „Dangerpoint“) (vgl. Kapitel 2.2.2), auf welches aufgrund der globalen Anforderung zur Verwendung von Standardschnittstellen für die Schnittstelle zum Fahrzeug zurückgegriffen werden soll (vgl. Kapitel 4.5.2).[45] ETCS enthält dementsprechend Variablen zur Übermittlung der entsprechenden Zielpunkte in der ETCS-MA.

Einer in der smartLogic optimierten Umsetzung des Themenkomplexes der Zielpunkte und insbesondere der Sicherheitsabstände hinter dem anzusteuernden Zielpunkt einer Fahrerlaubnis wurde bereits in der Nutzenanalyse eine hohe Hebelwirkung in Bezug auf die Zieldimensionen der Kapazität und der Robustheit vorhergesagt (vgl. Kapitel 3.4), so dass eine ausführliche Betrachtung dieses Themenkomplexes sinnvoll erscheint.

Im Sinne des „Grüne Wiese“-Ansatzes (vgl. Kapitel 3.6.2) basiert die Herleitung in diesem Kapitel mit erster Priorität auf den in Kapitel 3.5 identifizierten globalen Anforderungen sowie den in Kapitel 6 erfassten funktionalen Anforderungen (zweiter Abschnitt dieses Unterkapitels). Daneben gibt auch die bestehende ETCS-Schnittstelle Rahmenbedingungen vor, die in Kapitel 2.2.2 beschrieben wurden. Da Änderungen an der ETCS-Schnittstelle bei der Europäischen Eisenbahnagentur (ERA) beantragt werden können, müssen die Vorgaben der ETCS-Schnittstelle jedoch nicht vollständig eingehalten werden. Um (koordinativ anspruchsvolle) Änderungsbedarfe an der Standardschnittstelle möglichst zu vermeiden bzw. gering zu halten, sollten die Rahmenbedingungen der ETCS-Schnittstelle

[44] Gemäß der in Kapitel 4.3.2 festgelegten Abgrenzung zwischen der sicherungstechnischen Verantwortung der Fahrzeuge und der infrastrukturseitigen Sicherungstechnik sind die Fahrzeuge selbst dafür verantwortlich, mit hinreichender Sicherheit vor dem vorgegebenen Zielpunkt zum Stehen zu kommen.

[45] Für die Schnittstelle zum TMS existiert mit Stand Februar 2021 noch keine Standardschnittstelle (vgl. Kapitel 4.5.3).

allerdings beachtet werden, sofern keine anderen Anforderungen aus Kapitel 8.2.1 dadurch signifikant beeinträchtigt werden.

Auf Basis der Anforderungen kann die äußere Grenze (= der am weitesten von der aktuellen Position der zu schützenden Fahrzeugbewegung entfernte zulässige Ort) des zulässigen Bereichs für den Zielpunkt, der von der Fahrzeugbewegung mit hinreichender Sicherheit nicht überschritten werden darf, hergeleitet werden (dritter Abschnitt). Dieser Ort wird im Folgenden als **primärer sicherungstechnischer Zielpunkt** bezeichnet und entspricht bei ETCS der Supervised Location (SvL).

Neben der SvL wird dem Fahrzeug über die ETCS-Schnittstelle in der Fahrerlaubnis auch noch ein weiterer Zielpunkt übermittelt. Es handelt sich um die „End of Authority" (EoA), die für die Fahrzeugbewegung den Punkt darstellt, der nicht überschritten werden soll und deshalb von der Fahrzeugbewegung bzw. dem Tf als Ziel einer sicherungstechnisch gebotenen Bremsung anzusteuern ist[46]. Die EoA kann daher auch als (sicherungstechnisch) **anzusteuernder Zielpunkt** bezeichnet werden[47]. Für die smartLogic ist zu prüfen, ob das Vorhandensein bzw. die Positionierung der EoA ebenfalls sicherungstechnisch geprüft werden muss und welche Bedingungen dafür ggf. von der smartLogic sicherzustellen sind (vierter Abschnitt).

Neben den äußeren Grenzen des zulässigen Bereichs für die Zielpunkte, könnte es noch weitere Einschränkungen geben, die die Wahl der Zielpunkte durch das TMS einschränkt und von der smartLogic zu überprüfen sind. Mit solchen Einschränkungen beschäftigt sich der fünfte Abschnitt.

ETCS kennt neben den bereits genannten Arten von Zielpunkten noch die „Limit of Authority" (LoA) (vgl. Kapitel 2.2.2). Der vorletzte Abschnitt beschäftigt sich damit, ob die LoA einen relevanten Anwendungsfall für die smartLogic hat, bevor das Kapitel im letzten Abschnitt zusammengefasst wird.

Startpunkt

Oben wurde der räumliche Gültigkeitsbereich einer Fahrerlaubnis als Gleisabschnitt bezeichnet. Wenn davon ausgegangen werden kann, dass das TMS der Fahrzeugbewegung mit der MA einen eindeutigen Fahrweg zuweisen möchte, handelt es sich nach der RCA-Definition, die in Kapitel 7.3.3, im Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)" beschrieben ist, um eine „Linear Contiguous Track Area". Dieser Gleisabschnitt wird auch benötigt, um die Beanspruchung der Infrastruktur im internen Datenmodell zu speichern (vgl. Kapitel 7.6.2). Als eindimensionales Objekt benötigt die Linear Contiguous Track Area auch einen Startpunkt.

Da der Fahrzeugbewegung mit der Fahrerlaubnis die Weiterfahrt von ihrer aktuellen Position zum neuen anzusteuernden Zielpunkt genehmigt wird, muss die aktuell gültige Fahrerlaubnis an der aktuellen Position der Fahrzeugbewegung beginnen (vgl. Kapitel 7.6.2). In ETCS werden folglich auch nur die Zielpunkte übertragen, da die Fahrzeugbewegung ihre aktuelle Position kennt.

[46] Es sei darauf hingewiesen, dass ETCS ein sicherungstechnisches System ist. Es kann daher sein, dass der Fahrplan oder eine andere rein betriebliche Anforderung einen zusätzlichen Halt bzw. einen anzusteuernden Halteort vor der EoA fordert. Diese betriebliche Perspektive wird in dieser Arbeit aufgrund der Anforderung der schlanken Logik ausgeblendet.

[47] Anzusteuernder Zielpunkt heißt dabei allerdings nicht, dass die Fahrzeugbewegung diesen Punkt auch tatsächlich erreicht. Bei ungenauer Ortung kann sie ggf. nicht bis zum anzusteuernden Zielpunkt gelangen. Um unnötige Infrastrukturbeanspruchungen zu vermeiden, wäre es wünschenswert, wenn die Fahrzeuge immer möglichst nah an den anzusteuernden Zielpunkt heranfahren könnten. Allerdings wurde die Problematik der Ortungsungenauigkeit bewusst in einen vorgelagerten Ortungsinformationsaggregator ausgelagert (vgl. Kapitel 4.4.4). Es ist daher nicht Aufgabe der smartLogic, dafür zu sorgen, dass die Fahrzeugbewegung möglichst nahe an den vorgegebenen anzusteuernden Zielpunkt heranfahren kann. Die smartLogic garantiert nur, dass die Zielpunkte so gesetzt sind, dass wenn die Fahrzeugbewegung den Zielpunkt erreichen würde, sie nicht gefährdet werden würde.

Anforderungen an die Position der Zielpunkte der MA

Bei den Anforderungen an die Position der Zielpunkte der Fahrerlaubnis müssen die globalen Anforderungen sowie die daraus hergeleiteten betrieblichen funktionalen Anforderungen und die funktionalen Sicherheitsanforderungen beachtet werden (vgl. Einleitung zu diesem Hauptkapitel). Die beiden Arten der funktionalen Anforderungen können dabei im Gegensatz zueinander stehen.

Betrieblich muss die Sicherungslogik die Durchführung der Fahrzeugbewegungen ermöglichen – und zwar so, dass der Spielraum des TMS zur Optimierung des Eisenbahnverkehrs möglichst wenig eingeschränkt wird (vgl. globale Anforderungen zu den Zieldimensionen der Energieeffizienz, hohen Kapazität und hohen Robustheit in Kapitel 8.2.1). Diese Anforderung bedeutet insbesondere, dass die smartLogic vom TMS in der Fahrerlaubnisanfrage beantragte Zielpunkte genehmigen sollte, die so weit wie möglich von der aktuellen Position der Fahrzeugbewegung entfernt gesetzt sind und somit eine möglichst große Länge der Fahrerlaubnis ermöglichen.

Sicherungstechnisch gibt der im 6. Hauptkapitel zusammengestellte Funktionskatalog mit den dort enthaltenen Prüfbedingungen vor, dass eine Fahrerlaubnis nur für den Gleisabschnitt erteilt werden kann, der von der Sicherungslogik auf die Abwesenheit unvertretbarer Risiken für die Zugfahrt überprüft wurde und auf dem diese auch tatsächlich abwesend sind (vgl. Kernanforderung der sicheren Logik). Die betrieblich gewünschte flexible Länge der Fahrerlaubnis wird also durch das Auftreten von Gefährdungen im Fahrtverlauf begrenzt[48]. Die Gefährdungen können mit einem unterschiedlich hohen Risiko für die zu schützende Fahrzeugbewegung verbunden sein (z. B. stumpf und spitz befahrene Weiche mit falscher Lage), das als **Gefährdungsrisiko** dieser Gefährdung bezeichnet werden kann. Der Beginn eines Wirkbereichs einer Gefährdung, den die Fahrzeugbewegung im Fahrtverlauf erreichen könnte, stellt einen **Gefahrpunkt** für diese Fahrzeugbewegung dar. Zur Erfüllung der funktionalen Sicherheitsanforderungen ist zumindest die Vorgabe eines Zielpunkts in der MA vor dem nächsten Gefahrpunkt, der von der Fahrzeugbewegung erreicht würde und dessen Gefährdungsrisiko hoch genug ist, dass eine Absenkung der Gesamt-Schutzrate der Prüfanfrage unter den zulässigen Schwellwert für die Genehmigung der Prüfanfrage beim Passieren des Gefahrpunkts durch eine Fahrzeugbewegung zu erwarten wäre, von der smartLogic sicherzustellen.

Eine weitere, spezielle funktionale Sicherheitsanforderung fordert, dass der Zielpunkt nicht in einem Bereich liegen sollte, in dem ein Stopp vermieden werden soll (in einer sogenannten „Non Stopping Area“ (NSA)) (siehe auch Kapitel 8.6.7).

Prüfung der Positionierung des primären sicherungstechnischen Zielpunkts (SvL)

Aufgrund der zu beachtenden Sicherheitsanforderungen hängt der am weitesten entfernte, mögliche Ort des primären sicherungstechnischen Zielpunktes (bei ETCS ist das die Supervised Location (SvL), vgl. Kapitel 2.2.2) von den vorhandenen Gefährdungen zum Zeitpunkt der Prüfung der Fahrerlaubnisanfrage ab. Der Zielpunkt kann dabei maximal – in Fahrtrichtung der Fahrzeugbewegung betrachtet – vor den Beginn des Wirkbereichs der zuerst erreichbaren Gefährdung gesetzt werden, bei der der Schwellwert der Schutzrate für die Genehmigungsfähigkeit der Prüfanfrage (vgl. zum Begriff Kapitel 8.3.1) im Falle des Passierens des entsprechenden Ortes unterschritten werden würde. Dieser Ort kann auch als in der aktuellen Situation für das Setzen der Zielpunkte **maßgeblicher Gefahrpunkt** bezeichnet werden.

[48] Theoretisch könnte diese Anforderung zwar auch zu einer Fahrerlaubnis ohne Zielpunkt führen, beispielsweise auf einem Ring aus nur einem Gleis ohne Weichen, auf dem nur ein einzelnes Fahrzeug verkehrt und auf dem es auch sonst kein Risiko einer Gefährdung gibt, aber das dürfte ein irrelevanter Grenzfall sein.

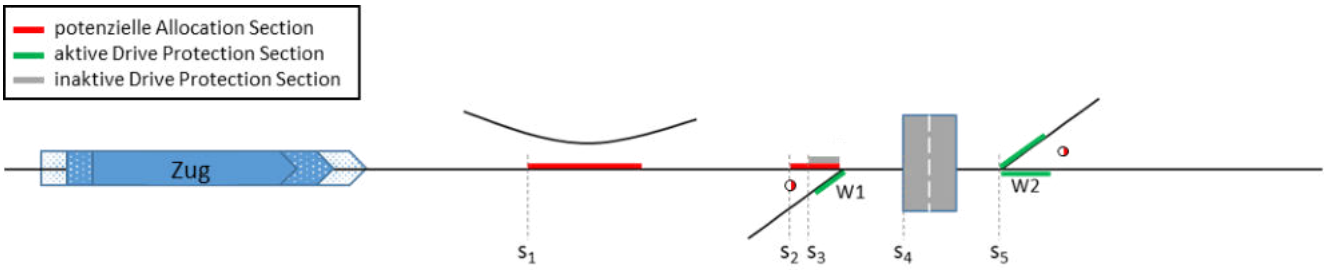


Abb. 59: Mögliche Wirkbereiche von Gefährdungen
[Eigene Darstellung]
Die roten Linien stellen potenzielle Allocation Sections und die grünen aktive Drive Protection Sections dar (vgl. zu den beiden Begriffen Kapitel 2.4.4, 7.3.9 und 7.4.3).

Abb. 59 zeigt verschiedene Beispiele für potenzielle Wirkbereiche von Gefährdungen. Für die Fahrzeugbewegung ist immer der ihr zugewandte Endpunkt des Wirkbereichs relevant. In der Grafik sind diese Punkte mit s_i gekennzeichnet. Der primäre sicherungstechnische Zielpunkt kann nach der oben beschriebenen Überlegung maximal an den Punkt s_x gesetzt werden, dessen zugehöriger Wirkbereich die Gesamt-Schutzrate der Prüfanfrage beim Passieren in den unzulässigen Bereich drücken würde und der damit gleichzeitig der maßgebliche Gefahrpunkt wäre. Dies könnte theoretisch je nach Betriebssituation jeder der aufgeführten Punkte sein. (In der Grafik wäre es spätestens der Punkt s_5, da die Weiche keine sichere Endlage hat, wie die beiden aktiven Drive Protection Sections in beiden Strängen zeigen, die jeweils das Befahren der Weiche im entsprechenden Strang verbieten, vgl. Kapitel 7.4.3.)

Bei der Bestimmung des maßgeblichen Gefahrpunkts ist zu beachten, dass bei einem später erreichten Gefahrpunkt (s_n im Falle des n-ten Gefahrpunkts) früher erreichte Gefahrpunkte (s_i) bereits passiert wurden und damit auch ihr Gefährdungsrisiko ($r(s_i)$) zum Gesamtrisiko ($r(s_n)_{ges}$) beiträgt. Das Gesamt-Gefährdungsrisiko des n-ten Gefahrpunkts ergibt sich daher als Multiplikation des inversen Gefährdungsrisikos des maßgeblichen Gefahrpunkts und der Gefährdungsrisiken der näher an der Fahrzeugbewegung liegenden Gefahrpunkte.

$$r(s_n)_{ges} = 1 - \prod_{i=1}^{n}\left(1 - r(s_i)\right)$$

Prüfung der Positionierung des anzusteuernden Zielpunkts (EoA) und weiterer Zielpunkte

In ETCS wird neben dem primären sicherungstechnischen Zielpunkt, der – wie im Abschnitt „Prüfung der Positionierung des primären sicherungstechnischen Zielpunkts“ beschrieben – bei ETCS der SvL entspricht, der von der Fahrzeugbewegung anzusteuernde Zielpunkt (EoA) an das Fahrzeug übergeben. Dabei stellt sich die Frage, ob das Vorhandensein bzw. die Positionierung der EoA von der smartLogic geprüft werden muss und falls ja, durch welche sicherheitskritischen Anforderungen die Positionierung der EoA durch das TMS eingeschränkt werden.

Im folgenden Unterabschnitt wird analysiert, wann eine Überprüfung des Vorhandenseins bzw. der Positionierung der EoA durch die smartLogic erfolgen sollte. In den nachfolgenden Unterabschnitten wird dann auf diese Anwendungsfälle näher eingegangen.

Wann muss die Positionierung der EoA von der smartLogic geprüft werden?

Aufgrund der Anforderung der schlanken Logik, sollte sich die smartLogic rein auf sicherheitskritische Aufgaben beschränken (vgl. Kapitel 4.3.1). Das Vorhandensein bzw. die Position der EoA müsste daher von der smartLogic nur überprüft werden, wenn die EoA eine Bedeutung für die Sicherheit hat.

Aus Sicht der Sicherheit gibt die EoA den Zielpunkt an, den die Fahrzeugbewegung zwar nicht überschreiten darf und damit ansteuert, aber für den die Überschreitung im Gegensatz zur SvL unter bestimmten Voraussetzungen in Kauf genommen werden kann (z. B. aufgrund eines verlängerten Bremsweges durch vorher nicht bekannte äußere Faktoren oder aufgrund einer ungenauen Fahrzeugortung) (vgl. Kapitel 2.2.2). Die EoA steht also für einen Zielpunkt, vor dem die betrachtete Fahrzeugbewegung nur mit einer geringeren Wahrscheinlichkeit zum Stehen kommt als vor der SvL.

Eine Bedeutung für die Sicherheit könnte daher zum einen vorliegen, wenn sich hinter der EoA zwar noch ein gesicherter Fahrweg befände – eine größere Gefährdung beim Passieren also vermieden würde –, die Fahrzeugbewegung aber dennoch einem kleineren Gefährdungsrisiko ausgesetzt wäre, wenn sie die EoA passierte. Dieses kleinere Risiko könnte durch die geringe Wahrscheinlichkeit, dass die Fahrzeugbewegung die EoA tatsächlich passiert, wieder ausgeglichen werden. Mit der Thematik solcher abgestuften Gefährdungsrisiken beschäftigt sich der nachfolgende Unterabschnitt „Zielpunkte mit abgestuftem Gefährdungsrisiko“.

Eine Bedeutung für die Sicherheit könnte zum anderen auch vorliegen, wenn durch die Prüfung der EoA die frühere Rücknahme von Beanspruchungen im Gleisabschnitt zwischen EoA und SvL, also dem Sicherheitsabstand hinter der EoA, ermöglicht werden würde, wie dies bei Durchrutschwegen heute der Fall ist. Hiermit beschäftigt sich der zweite nachfolgende Unterabschnitt „Vorzeitige Anpassung des Sicherheitsabstandes“.

Zielpunkte mit abgestuftem Gefährdungsrisiko

Wie im vorigen Unterabschnitt beschrieben, wäre ein Argument für eine Prüfung einer von der SvL getrennt positionierten EoA durch die smartLogic, wenn für die verschiedenen Zielpunkte jeweils ein anderes akzeptables Gefährdungsrisiko angenommen werden könnte. Dieses Vorgehen könnte dadurch begründet werden, dass die Wahrscheinlichkeit, mit der die Fahrzeugbewegung einen Punkt hinter dem anzusteuernden Zielpunkt (EoA) noch erreicht (im Folgenden als **Erreichens-wahrscheinlichkeit** $\phi(s_i)$ bezeichnet), mit zunehmender Distanz von der EoA sinkt. Die Erreichenswahrscheinlichkeit stellt damit die Eintrittswahrscheinlichkeit der Gefährdung dar.

Würde die EoA vom TMS (ggf. mit einem hinreichenden Abstand) vor einem bisher maßgeblichen Gefahrpunkt gesetzt werden, der jedoch nur mit einem geringen Gefährdungsrisiko für die Fahrzeugbewegung verbunden ist, könnte das Gefährdungsrisiko dieses Gefahrpunkts durch die niedrigere Erreichenswahrscheinlichkeit ausgeglichen werden. Dadurch könnte ein von der Fahrzeugbewegung weiter entfernt liegender Punkt zum maßgeblichen Gefahrpunkt für das Setzen der SvL werden und die Fahrzeugbewegung könnte sich aufgrund des größeren Sicherheitsabstandes mit einer höheren Geschwindigkeit an die EoA annähern.

Da die Schutzrate das Produkt der inversen Risiken darstellt (vgl. Kapitel 8.3.1), berechnet sich der Einfluss auf die Schutzrate als inverses Produkt aus Erreichenswahrscheinlichkeit und Gefährdungsrisiko.

$$Einfluss\ auf\ die\ Schutzrate = 1 - ((r(s_n)_{ges} * \phi(s_n))$$

Ein Beispiel ist die heute in Deutschland bereits erlaubte Überlappung von Durchrutschwegen. In diesen Fällen wird angenommen, dass die Wahrscheinlichkeit hinreichend klein ist, dass bei gleichzeitiger Anfahrt auf eine stumpf befahrene Weiche mit EoA vor und SvL hinter dieser Weiche mehr als eine Fahrzeugbewegung die EoA überschreitet und die stumpf befahrene Weiche überfährt (siehe Szenario II in Abb. 60).

Im Beispiel ergibt sich die Eintrittswahrscheinlichkeit der Gefährdung „Kollision der beiden Fahrzeugbewegungen“ aus dem Produkt der jeweiligen Erreichenswahrscheinlichkeit (und dem Gefährdungsrisiko für die Kollision, das hier als „1“ angenommen wird), sofern die letztgenannten Wahrscheinlichkeiten als voneinander unabhängig betrachtet werden können.[49]

Ist die Wahrscheinlichkeit der Kollision noch zu groß, wenn die beiden EoA direkt vor der Weiche liegen, könnte ein EoA oder beide EoAs entgegen der Fahrtrichtung näher an die aktuelle Position der Fahrzeugbewegungen verschoben werden. Hierdurch verringert sich die Erreichenswahrscheinlichkeit für den Wirkbereich der Gefährdung (im Beispiel die Weiche) weiter.

Zu beachten ist bei der Berechnung des Kollisionsrisikos, dass die Erreichenswahrscheinlichkeit eines bestimmten Ortes bei kurzen Distanzen zwischen EoA und SvL nicht nur von der Position der EoA abhängt, sondern auch von der Position der SvL, da die auf die SvL zulaufenden flacheren Bremskurven dann maßgeblich für die Fahrkurve der Fahrzeugbewegung sein können.

Abb. 60 stellt in Situation II eine mögliche Verschiebung der SvL vor einen von der Fahrzeugbewegung weiter entfernten Gefahrpunkt im Vergleich zur Referenz-Situation I durch das Trennen von EoA und SvL an einem Beispiel dar.

- In Situation I befinden sich EoA und SvL unmittelbar vor dem jeweiligen maßgeblichen Gefahrpunkt, bei dessen Überschreitung der erforderliche Schwellwert der Schutzrate unterschritten werden würde.
- In Situation II wurde die SvL der Fahrzeugbewegung MOB 2 vor den Gefahrpunkt durch die in Umstellung befindliche Weiche W2 verschoben, um MOB 2 eine schnellere Anfahrt auf ihre EoA und damit den Bahnsteig zu ermöglichen. Hierdurch kann die EoA von MOB 1 nicht mehr vor W2 liegen, da bereits vor W1 ein neuer Gefahrpunkt entsteht. Es dürfen auch nicht beide EoA unmittelbar vor dem Gefahrpunkt von W1 liegen, da dann die Wahrscheinlichkeit, dass beide Fahrzeugbewegungen die EoA überschreiten, z. B. in Folge von Ortungsungenauigkeit, zu hoch wäre. Deshalb wurde im Beispiel ein zusätzlicher Sicherheitsraum durch das Zurücksetzen der EoA von MOB 1 geschaffen.

Die untenstehende Grafik skizziert zu diesem Beispiel mögliche Erreichenswahrscheinlichkeiten der jeweiligen Punkte auf der x-Achse für die beiden Szenarien und die beiden beteiligten Fahrzeugbewegungen. Die durchgezogenen Linien beziehen sich auf Szenario I und die gestrichelten Linien auf Szenario II. Die Wahrscheinlichkeit einer Kollision ergibt sich aus dem Produkt der Erreichenswahrscheinlichkeiten für den Kollisionspunkt (Annahme: diese sind unabhängig voneinander).

Der Vorteil von Situation II gegenüber Situation I könnte darin liegen, dass die Fahrzeugbewegung MOB 2 schneller an ihre EoA und damit den Bahnsteig heranfahren könnte. Die Situation ist jedoch nicht pareto-optimal, da sich für MOB 1 durch die Verschiebung der EoA näher an ihre aktuelle Position ein Nachteil ergäbe. Ob Situation I oder II insgesamt vorteilhafter ist, muss nicht die smartLogic, sondern das TMS bewerten. Eine Trennung von EoA und SvL könnte aber einen Nutzen haben, so dass eine sicherungstechnische Prüfung der Position der EoA durch die smartLogic sinnvoll sein könnte.

[49] An der Unabhängigkeit der Erreichenswahrscheinlichkeit kann es Zweifel geben, da der Bremsweg z. B. durch eine verringerte Haftreibung verlängert werden könnte, die beide Fahrzeugbewegungen gleichermaßen beeinflusst. Allerdings ist die Berechnung der tatsächlichen Wahrscheinlichkeiten gemäß Kapitel 3.3 nicht Aufgabe dieser Arbeit.

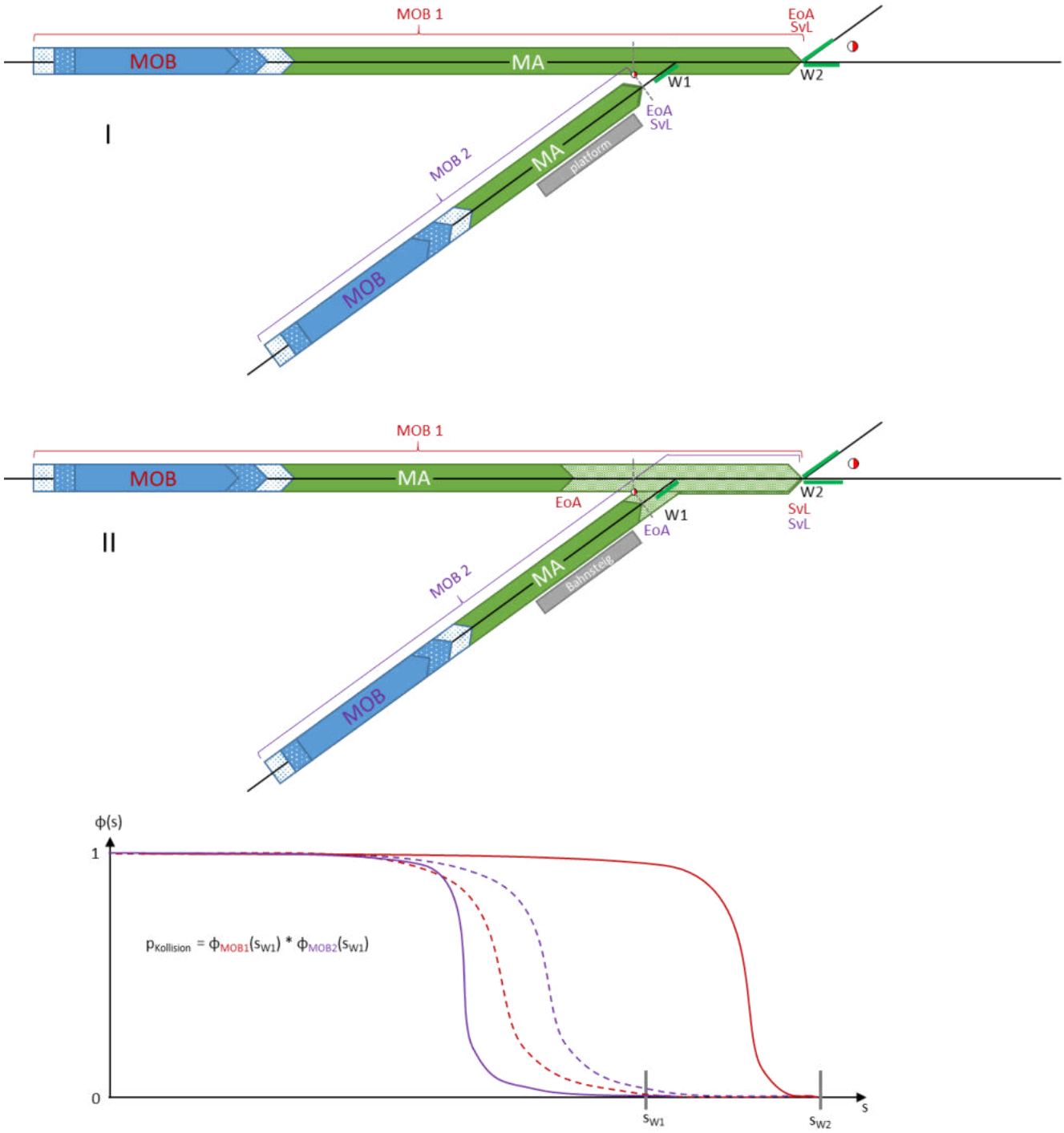


Abb. 60: Beispielsituation für verschobene SvL
s entspricht dem zurückgelegten Weg auf der darüber abgebildeten Infrastruktur
[Eigene Darstellung]

Es wäre prinzipiell denkbar, dass das TMS vor weitere Gefahrpunkte weitere Zielpunkte mit entsprechender zulässiger Erreichenswahrscheinlichkeit legt, so dass das Fahrzeug eine Optimierung der Bremskurven unter Berücksichtigung all dieser Zielpunkte, die als **sekundäre sicherungstechnische Zielpunkte** bezeichnet werden könnten, und der jeweils zulässigen Erreichenswahrscheinlichkeit vornehmen kann. Die smartLogic müsste dann für jede Gefährdung, die vor der SvL liegt, prüfen, ob das jeweilige Gefährdungsrisiko über einen entsprechenden sekundären sicherungstechnischen Zielpunkt mit einer geeigneten zulässigen Erreichenswahrscheinlichkeit korrekt in der MA enthalten wäre und damit korrekt an das Fahrzeug übermittelt würde. Die Logik würde

hierdurch allerdings nur geringfügig komplexer, da die zulässigen Erreichenswahrscheinlichkeiten der einzelnen Gefahrpunkte bei unterschiedlichen beantragten Positionen von EoA und SvL zur Ermittlung des maßgeblichen Gefahrpunkts ohnehin ermittelt werden muss. Es müsste dann nur zusätzlich geprüft werden, ob die zulässigen Erreichenswahrscheinlichkeiten in der MA korrekt hinterlegt sind (für Details hierzu siehe Kapitel 8.6.4). Eine Übermittlung solcher weiteren Zielpunkte wird jedoch derzeit von ETCS nicht unterstützt.

Vorzeitige Anpassung des Sicherheitsabstandes

Das zweite, identifizierte mögliche Argument für eine Prüfung einer von der SvL getrennt positionierten EoA durch die smartLogic basiert analog zur Funktionsweise des klassischen Durchrutschwegs (vgl. Kapitel 2.1.1) auf der Annahme, dass die Trennung eine vorzeitige Freigabe eines Teils oder des gesamten Sicherheitsabstandes zwischen EoA und SvL ermöglichen könnte. Durch die vorzeitige Freigabe könnte ein positiver Effekt auf die Kapazität entstehen, da der nicht mehr beanspruchte Gleisabschnitt von einer anderen Fahrzeugbewegung verwendet werden könnte.

Je geringer die Geschwindigkeit wird und je präziser die Ortung wird, desto weniger Sicherheitsabstand ist hinter dem anzusteuernden Zielpunkt (EoA) erforderlich (vgl. Bedeutung des Sicherheitsabstandes/Durchrutschweges in Kapitel 2.1.1 und 2.2.2). Der Gleisabschnitt, der für eine schnelle Annäherung an die EoA zusätzlich für die Fahrzeugbewegung beansprucht worden ist, könnte somit wieder freigegeben werden, sobald die Fahrzeugbewegung langsam genug ist bzw. ihre Ortungsungenauigkeit weit genug verringert hat, dass dieser Gleisabschnitt bzw. Teile davon nicht mehr benötigt werden. Zwei mögliche ETCS-Funktionen kommen zur Realisierung einer solchen vorzeitigen Freigabe in Betracht (vgl. Kapitel 2.2.2):

1. Die ETCS-MA enthält zur Ermöglichung des beschriebenen Vorgehens die optionale Angabe eines „Overlap“ genannten Gleisabschnitts hinter der EoA, der an einen Auflösetimer geknüpft sein kann, um dem Fahrzeug zu signalisieren, wie lange der Overlap zur Verfügung steht.
2. Das TMS kann auch beantragen die Fahrerlaubnis zu kürzen (mittels Funktion „Kürzen einer Fahrerlaubnis“). Hierfür existiert eine spezifizierte Nachricht an das Fahrzeug, die das Fahrzeug dazu veranlasst, zu prüfen, ob es vor den neuen Zielpunkten sicher bremsen kann.

Für die zweite Funktion würde keine vorgelagerte EoA benötigt, da der betrieblich gewünschte Zielpunkt auch über nicht sicherheitskritische Kommunikationswege (z. B. Fahrplan) übermittelt werden kann und die Kürzung vom Fahrzeug akzeptiert wird, sofern es eine Bremsung auf den neuen Zielpunkt sicherstellen kann. Die erste Funktion hat zudem beim derzeitigen Spezifikationsstand den Nachteil, dass der Freigabezeitpunkt durch den Auflösetimer nicht flexibel davon abhängt, wann das Fahrzeug den freizugebenden Gleisabschnitt nicht mehr benötigt, während es dies im zweiten Fall mitteilen kann (Anforderungen zur Zieldimension „hohe“ Kapazität). Dafür würden bei der ersten Lösung auszutauschende Nachrichten gespart, was der Anforderung der geringen Latenz zu Gute kommt. Dennoch scheint aus den genannten Gründen die zweite Funktion weiterverfolgenswert (siehe hierzu MP Change Request in Kapitel 8.5.4).

weitere Einschränkungen für die Positionierung der Zielpunkte

Durch die oben genannte Überlegung wird die maximale erlaubte Entfernung der sicherungstechnischen Zielpunkte von der aktuellen Position des Fahrzeugs bestimmt. In diesem

Abschnitt soll untersucht werden, ob es weitere von der smartLogic sicherzustellende Einschränkungen für die Positionierung der Zielpunkte gibt.

In Kapitel 6 wurde keine Sicherheitsanforderung identifiziert, die sich explizit auf die minimale Entfernung des Zielpunktes von der aktuellen Position der Fahrzeugbewegung bezieht. Theoretisch wäre es möglich, den Zielpunkt wenige Meter vor das Max Safe Front End (vgl. zum Begriff Kapitel 7.6.1) zu legen, z. B. um zum Kuppeln an ein anderes Fahrzeug beidrücken zu können.

Eine Ausnahme von der Aussage im vorigen Absatz existiert, wenn die neue Fahrerlaubnis eine aktuell gültige Fahrerlaubnis einschränken soll und damit möglicherweise ein in Bewegung befindliches Fahrzeug betrifft. In diesem Fall besteht die Gefahr, dass das betroffene Fahrzeug evtl. nicht mehr den notwendigen Bremswegabstand zum neuen Zielpunkt hat. Um das Problem zu lösen, kann auf die bereits im vorigen Abschnitt beschriebene ETCS-Funktion mit dem Titel „Kürzen einer Fahrerlaubnis“ zurückgegriffen werden. Zur Nutzung dieser Funktion ist auch in der smartLogic ein eigenständiger Prüfprozess erforderlich, der als „MP Change Request“ bezeichnet wird. Daher kann dieser Sonderfall hier ausgeklammert und im Rahmen von Kapitel 8.5.4 thematisiert werden.

Weiterhin ist, wie bereits im Abschnitt „Anforderungen an die Position der Zielpunkte der MA“ erwähnt, zu beachten, dass der Zielpunkt nicht in einer Non Stopping Area (NSA) liegen soll. Falls möglich sollte der Zielpunkt also hinter (oder vor) einer NSA liegen.

Aufgrund des Fahrplans kann es vorkommen, dass ggf. ein früherer Halt erwünscht ist (z. B. ein Fahrplanhalt), als der durch die Länge der MA vorgegebene Zielpunkt, der für das Fahrzeug die befahrbare Wegstrecke vorgibt. Dies ist jedoch aufgrund der Anforderung der schlanken Logik, wonach die Logik nur sicherheitsrelevante Bestandteile prüfen soll, keine Fragestellung der Sicherungslogik, sondern kann dem Fahrzeug über einen nicht sicherheitskritischen Weg mitgeteilt werden (z. B. über den gedruckten Fahrplan oder das ATO-Journey Profile). Oder es ist zumindest eine Entscheidung des nicht sicherheitskritischen TMS, bewusst einen kürzeren Zielpunkt zu beantragen als es theoretisch notwendig wäre. Fahrplanhalte haben daher keinen Einfluss auf die Überprüfung der Positionierung der in der Fahrerlaubnisanfrage enthaltenen Zielpunkte.

Einsatz der Limit of Authority (LoA)

Bei der Betrachtung der ETCS-Funktionalitäten stellt sich abschließend aus Gründen der Vollständigkeit noch die Frage, ob auch ein Verwendungszweck für die Funktionalität der LoA im Rahmen der smartLogic angezeigt ist (vgl. zum Begriff Abschnitt „Fahrerlaubnis (MA)“ in Kapitel 2.2.2). Ein solcher Verwendungszweck konnte jedoch aus der allgemeinen Betrachtung für vollständig von der smartLogic kontrollierte Bereiche und Fahrzeuge nicht festgestellt werden. Möglicherweise gibt es aber sinnvolle Anwendungsbereiche beim Übergang in Bereiche, die nicht von der smartLogic kontrolliert werden. Dies sollte bei einer späteren Betrachtung dieser Anwendungsbereiche, die aus Ressourcengründen nicht mehr in dieser Arbeit stattfindet, überprüft werden.

Zusammenfassung

Im vorliegenden Unterkapitel wurden die Regeln beschrieben, nach denen die smartLogic die vom TMS beantragtem räumlichen Grenzen der Fahrerlaubnis genehmigen kann. Dabei wurde festgestellt, dass der Startpunkt an der aktuellen Position der Fahrzeugbewegung liegen muss.

Für das Prüfen der beantragten Zielpunkte wurden zunächst relevante funktionale Sicherheits-anforderungen aus dem im 6. Hauptkapitel erarbeiteten Funktionskatalog hergeleitet. Aufgrund der globalen Anforderung der Nutzung von *Standardschnittstellen*, ergeben sich außerdem

Rahmenbedingungen durch die zu verwendende ETCS-Schnittstelle, die beachtet werden sollten, sofern keine globale Anforderung dadurch signifikant eingeschränkt wird. ETCS kennt zwei Zielpunkte, die EoA und die SvL. Die EoA ist der vom Fahrzeug für sicherheitstechnisch erforderliche Bremsungen anzusteuernde Zielpunkt und die SvL der primäre sicherungstechnische Zielpunkt, der mit hinreichender Sicherheit nicht passiert werden darf. Letzterer liegt gemäß der ETCS-Logik entweder am Ende des temporär zur Verfügung stehenden Overlaps oder am Danger Point. Die beiden Zielpunkte unterscheiden sich in der Wahrscheinlichkeit, mit dem das Fahrzeug vor ihnen zum Stehen kommt.

Die SvL darf sich maximal am Punkt des Beginns des Wirkbereichs der ersten Gefährdung befinden, deren Gefährdungsrisiko in Relation zur Erreichenswahrscheinlichkeit dieses Punktes nicht mehr hinreichend gering ist, da beim Passieren dieses Punktes die Gesamt-Schutzrate (vgl. Kapitel 8.3.1) in den unzulässigen Bereich absinken würde (= maßgeblicher Gefahrpunkt). Es wurde im Unterkapitel festgestellt, dass es nur in bestimmten Fällen einen Vorteil bringt, dass das TMS getrennte Orte für die EoA und die SvL beantragt, um eine höhere Kapazität zu erzielen. Befinden sich SvL und EoA an getrennten Orten, sinkt die Erreichenswahrscheinlichkeit der SvL und aller weiteren Punkte zwischen EoA und SvL. Hierdurch können beispielsweise überlappende Sicherheitsabstände zweier verschiedener Fahrzeugbewegungen ermöglicht werden. Da entsprechende Vorteile denkbar sind, muss die smartLogic die vom TMS beantragten Positionen beider Zielpunkte auf ihre Sicherheit hin überprüfen.

Theoretisch wäre es sogar möglich, beliebig viele Zielpunkte zwischen EoA und SvL zu konstruieren, für die aufgrund der unterschiedlichen Erreichenswahrscheinlichkeiten jeweils unterschiedliche Gefährdungsrisiken akzeptabel wären (sekundäre sicherungstechnische Zielpunkte). Der Fahrzeugbewegung könnten diese Zielpunkte mit der jeweils zulässigen Erreichenswahrscheinlichkeit mitgeteilt werden und es würde seine Bremskurven so berechnen, dass die Erreichenswahrscheinlichkeiten der jeweiligen Zielpunkte hinreichend gering wären.

Die Zielpunkte sollen sich nicht in ausgewiesenen Non Stopping Areas befinden. Weiterhin dürfen die Zielpunkte eine bestehende MA nicht einkürzen, es sei denn es wird hierfür die ETCS-Funktion „Kürzen einer Fahrerlaubnis“ genutzt (siehe MP Change Request in Kapitel 8.5.4). Nicht sicherungstechnisch-relevante Zielpunkte (z. B. Fahrplanhalte) wurden aufgrund der Anforderung der schlanken Logik nicht beachtet.

Für die ETCS-Funktion der Limit of Authority (LoA) wurde kein Anwendungsfall für den Fall der ausschließlichen Nutzung der smartLogic identifiziert. Möglicherweise gibt es allerdings Anwendungsfälle, wenn Übergangsbereiche zur Alttechnik betrachtet werden.

8.3.3 Einbezug sicherheitskritischer externer Systeme / Stakeholder-Registrierungs-Konzept

Die smartLogic soll gemäß ihren Anforderungen *schlank*, möglichst *generisch* und erweiterbar (vgl. globale Anforderung der *Zukunftsfähigkeit*) sein (vgl. Kapitel 8.2.1). Im Funktionskatalog, der im 6. Hauptkapitel erarbeitet wurde, finden sich jedoch zahlreiche funktionale Sicherheitsanforderungen, die sich auf spezielle Anwendungsfälle beziehen, z. B. Bauarbeiten auf der Strecke, wetterabhängige Einschränkungen (z. B. Maximalgeschwindigkeiten bei starkem Wind) oder die Sicherheits-anforderung, dass an bestimmten Bahnhöfen Reisende über Lautsprecher vor durchfahrenden Zügen gewarnt werden müssen.

Zur Erfüllung dieser speziellen Sicherheitsanforderungen in einem automatisierten System ist in der Regel die Hilfe externer Systeme, wie Kommunikationsgeräte, Wettersensoren oder Reisenden-

informationssysteme, notwendig. Diese Systeme sollen nachfolgend in Abgrenzung zu den anderen Umsystemen wie Stellelementen, den Fahrzeugsystemen oder dem TMS als „**Stakeholder-Systeme“** bezeichnet werden (feinere Abgrenzung siehe Abschnitt „Abgrenzung der Stakeholder-Systeme zu den anderen Umsystemen der smartLogic“ in diesem Unterkapitel).[50]

Da nicht angenommen werden kann, dass Sicherheitsanforderungen, wie die oben beschriebenen Sicherheitsanforderungen, in Zukunft entfallen und es auch möglich ist, dass zukünftig weitere Sicherheitsanforderungen von der smartLogic zu überwachen sind (z. B. die Automatisierung von bisher manuell erfüllten Sicherheitsanforderungen, vgl. beispielsweise das Tunnelbegegnungsverbot, siehe hierzu auch Kapitel 8.4.6), wird in diesem Unterkapitel ein Konzept erarbeitet, wie solche speziellen Sicherheitsanforderungen möglichst generisch in die smartLogic integriert werden können.

Zur Erarbeitung des Konzeptes ist es wie bei den anderen Konzepten in Kapitel 8.3 sinnvoll, zunächst die speziellen Anforderungen an das Konzept zu bestimmen. Um den benötigten Umfang der generischen Beschreibung (Welche Informationen müssen über welche Schnittstellen übermittelt werden können?) festlegen zu können, sollte weiterhin, wie im vorletzten Absatz bereits angekündigt, eine Abgrenzung der Stakeholder-Systeme von den anderen sicherheitskritischen Umsystemen der Sicherungslogik (vgl. Kapitel 4.6) erfolgen. In diesem Rahmen stellt sich auch die Frage, ob Menschen wie Posten an der Strecke ebenfalls als Stakeholder-„Systeme“ betrachtet werden können. Dieser Frage wird aufgrund der ausführlichen Diskussion ein eigener Abschnitt gewidmet.

Aufbauend auf der erfolgten Abgrenzung der Stakeholder-Systeme können die erforderlichen Arten von Schnittstellen zwischen smartLogic und Stakeholder-Systemen, deren Aufbau sowie die zu übermittelnden Parameter für Regelbetrieb und Rückfallebene aus den Funktionsanforderungen dieser Systeme hergeleitet werden. Darauf aufbauend können wiederum die Kernpunkte für den angestrebten, generischen Prozess zum Ansprechen der Schnittstellen (im Abschnitt „Art der Gliederung der generischen Schnittstellen“ werden für diesen Prozess die Begriffe „Registrierung“ und „Deregistrierung“ eingeführt) hergeleitet werden. Abschließend folgt eine Zusammenfassung des erarbeiteten Stakeholder-Registrierungs-Konzepts zum Einbezug externer Systeme.

Anforderungen an die Einbindung der Stakeholder-Systeme

Grundlage der speziellen Anforderungen an die Einbindung der Stakeholder-Systeme sind die globalen Anforderungen und die spezifischen Anforderungen für die Bearbeitung des 8. Hauptkapitels (vgl. hierzu die Kapitel 3.5 (globale Anforderungen) und 8.2.1 (spezifische Anforderungen für die Verhaltensmodellierung)).

Aus der Kernanforderung der sicheren Logik ergibt sich in Hinblick auf die Einbindung der Stakeholder-Systeme, dass die Kommunikation vollständig und korrekt sein muss bzw. eine unvollständige oder unkorrekte Kommunikation erkannt werden muss. Für die Sicherstellung einer diesen Anforderungen entsprechenden Kommunikation gibt es aus dem Bereich der Informatik bereits Lösungen, die hier nicht vertieft werden sollen, da sich die vorliegende Arbeit auf die funktionale Sicherheit beim Betrieb der Eisenbahnen beschränkt. Aus dem gleichen Grund wird auch der Bereich der IT-Sicherheit hier nicht weiter thematisiert (vgl. zu den inhaltlichen Abgrenzungen auch Kapitel 3.3).

Im Sinne der schlanken Logik soll eine großen Anzahl unterschiedlicher externer Schnittstellen vermieden werden und nur externe Systeme angebunden werden, die auch Sicherheitsverantwortung

[50] Für die smartLogic zählen aufgrund ihres sicherheitsbezogenen Auftrags (vgl. Kapitel 4.3) nur Systeme mit Sicherheitsverantwortung zu den Stakeholder-Systemen, da Systeme ohne Sicherheitsverantwortung im Sinne der Anforderung der schlanken Logik über das TMS mit der smartLogic kommunizieren können.

haben (vgl. auch die Abgrenzung zum Leitsystem in Kapitel 4.3.1). Die erforderlichen Schnittstellen sollen daher, wie oben bereits beschrieben, möglichst generisch gestaltet sein. Falls bereits vorhanden, sollen Standardschnittstellen genutzt werden (Anforderung möglichst Standardschnittstellen zu nutzen).

Eine weitere globale Anforderung fordert, dass die Infrastrukturzuordnung (bezogen auf Infrastrukturelemente, aber auch externe Systeme) flexibel sein soll. Dies ist auf die Laufzeit des Systems smartLogic bezogen (vgl. Kapitel 3.5). Demnach muss es möglich sein, dass während der Laufzeit der smartLogic externe Systeme Sicherheitsanforderungen zur Berücksichtigung in der smartLogic ergänzen, ändern oder löschen können.

Bei den Anforderungen, die den Zieldimensionen „Energieeffizienz“, „hohe Kapazität“ und „Robustheit“ zugeordnet sind, erscheint nur die geringe Latenz für die Fragestellung der Ausgestaltung der externen Systeme von Relevanz zu sein. Allerdings wirkt diese sich wiederum vor allem auf die Wahl der Kommunikationstechnik aus, die wie oben erwähnt nicht im Fokus dieser Arbeit steht.

Für die anderen in Kapitel 8.2.1 identifizierten Anforderungen konnte der Autor keine direkte Relevanz für eine Abwägungsentscheidung bei der Erarbeitung des Konzepts zur Einbindung der Stakeholder-Systeme feststellen.

Abgrenzung der Stakeholder-Systeme zu den anderen Umsystemen der smartLogic

Um den erforderlichen Umfang der Schnittstellen zur Einbindung der Stakeholder-Systeme modellieren zu können, müssen diese von anderen Umsystemen der smartLogic abgegrenzt werden. In Kapitel 4.6 wurde die Einbettung der smartLogic in ihre Umsysteme zusammengefasst. Da die Liste der Stakeholder-Systeme bewusst offen sein soll, damit das generische Konzept auch die Integration neuer Systeme in Folge neuer funktionaler Sicherheitsanforderungen ermöglicht, wird nach dem Ausschlussverfahren vorgegangen.

Gemäß der im vorigen Abschnitt beschriebenen Anforderung der schlanken Logik gehören die nicht sicherheitskritischen Umsysteme nicht zu den Stakeholder-Systemen.

Weiterhin ist die Intention des generischen Stakeholder-Konzepts, externe Systeme einzubinden, die nicht in jedem Anwendungsfall von Bahnbetrieb mit der smartLogic benötigt werden und somit nicht zu den grundlegenden Komponenten der infrastrukturseitigen Sicherungstechnik gehören.[51] Für das Funktionieren des Bahnbetriebs unerlässlich und somit zu den grundlegenden Systemkomponenten der infrastrukturseitigen Sicherungstechnik gehörend sind die Systeme der Datenhaltung, die Systeme zum Austausch von Informationen mit den Fahrzeugen und der Ortungsinformationsaggregator zur Bereitstellung bestmöglicher Ortungsinformationen der einzelnen Fahrzeuge auf der Infrastruktur sowie die Stellelemente bzw. deren Object Controller. Auch die Bereitstellung grundlegender Systemfunktionen wie die IT-Sicherheitsschicht oder die Übertragungssysteme gehören zu den grundlegenden Systemkomponenten (vgl. zur Architektur das 4. Hauptkapitel und insbesondere Kapitel 4.6).

Damit verbleiben als Stakeholder-Systeme gemäß der exemplarischen Aufzählung in der Einleitung zu diesem Unterkapitel zum Beispiel externe Systeme, die bestimmte Schutzfunktionen übernehmen (z. B. Kommunikationssysteme) oder Überwachungsfunktionen ausüben (z. B. Wettersensoren), um spezielle Sicherheitsanforderungen zu erfüllen. Zu den Stakeholder-Systemen können also

[51] Da die grundlegenden Komponenten immer berücksichtigt werden müssen, ist eine Integration in das generische Konzept zur Einbindung Stakeholder-Systeme schlichtweg nicht erforderlich und würde dieses nur komplexer als nötig machen.

beispielsweise Sensoren gezählt werden, die bestimmte Zustände detektieren und dabei Überwachungsfunktionen übernehmen, aber kein Stellelement sind.

In der Abgrenzung zu den Stellelementen sind auch Grenzfälle möglich. Bahnübergänge können zwar angewiesen werden, ihren Zustand zu ändern, aber im Gegensatz zu Stellelementen wie Weichen können sie weitgehend autonom agieren. So ist das Schließen des Bahnübergangs zunächst kein sicherheitskritischer Vorgang und erfordert daher auch keinen Prüfprozess. Erst das Öffnen des Bahnübergangs ist sicherheitskritisch, denn der Bahnübergang darf nur geöffnet werden, wenn seine Schutzfunktion von keinem Zug beansprucht wird. Im Sinne der schlanken Logik werden im Folgenden Bahnübergänge zu den Stakeholder-Systemen gezählt und nicht als eigener Typ von Umsystem betrachtet.

Einbindung von Personen und menschlichen Meldungen mit Sicherheitsbedeutung

Im Funktionskatalog befinden sich – identifiziert vor allem durch die Ergänzung der Funktionen mittels der Fahrdienstvorschrift (Ril 408)) – neben dem primären Bediener des Systems (Fahrdienstleiter) weitere Personen, die dezentral Informationen für den sicheren Bahnbetrieb bereitstellen oder sicherheitskritische Funktionen ausüben. Die meisten dieser Personen erfüllen Aufgaben, die nur in Rückfallebenensituationen auftreten können. Es gibt aber auch reguläre menschliche Funktionen, so sind Tf dazu verpflichtet, vorbeifahrende Fahrzeuge zu beobachten und Unregelmäßigkeiten zu melden. Auch die Gleisarbeiter geben sicherheitsrelevante Meldungen u. a. darüber ab, ob sie das Gleis geräumt haben. Daher ist neben der Abgrenzung zu den anderen technischen Umsystemen der smartLogic zu klären, inwieweit auch Personen zu den Stakeholder-Systemen gezählt werden sollten.

Eine automatische Sicherungslogik sollte gemäß der Kernanforderung der sicheren Logik Meldungen von Personen über standardisierte Schnittstellen verarbeiten können, um Verzögerungen zu vermeiden und das Verlust- oder Verfälschungsrisiko der Nachricht durch den Einbezug weiterer menschlicher Akteure als Übermittler zu reduzieren. Damit die automatisierte Logik mit den Informationen arbeiten kann, müssen sie über externe Systeme erfasst und digitalisiert sowie in standardisierte Formate übertragen werden. Aus diesem Grunde stehen hinter den menschlichen Meldungen auch technische Systeme. Die Meldungen erfüllen häufig auch die gleichen Aufgaben wie rein technische Sensoren bzw. Stakeholder-Systeme. Daher erscheint es sinnvoll, sie als Stakeholder-Systeme mitzudenken.

Beispiele für Personen mit Sicherheitsbedeutung bzw. dazugehörende Meldungen sind:

- arbeitende Personen im Gleis, die geschützt werden müssen,
- weitere baustellenbezogene Meldungen, z. B. zum Sperren und Aufheben der Sperrung von Gleisen oder zum Eingleisen von Fahrzeugen[52]
- manuelle Freimelder bestimmter Abschnitte, manuelle Räumungsprüfung,
- manuelle Lageüberwacher für ein Infrastrukturelement,
- Bahnübergangsposten oder sonstige Posten,
- Melder eines Notfalls und
- Melder von sicherheitskritischen Ereignissen bzw. Zustandsberichten wie Unbefahrbarkeit eines Gleisabschnitts.

[52] Der Autor empfiehlt allerdings, das Eingleisen nur in speziell dafür vorgesehenen Gleisen zu erlauben. Siehe u. a. Kapitel 8.3.4, Abschnitt „Schutzrate auf den Gleissegmenten des aktiven Flankenschutzraumes“.

Art der Gliederung der generischen Schnittstellen

Nachdem der Umfang der Stakeholder-Systeme abgegrenzt ist, können die Grundzüge der Interaktion mit diesen Systemen, also die Schnittstellen zwischen der smartLogic und diesen Systemen, hergeleitet werden. Die Anforderungen zu diesem Unterkapitel fordern, dass die Schnittstellen zur Interaktion mit den Stakeholder-Systemen möglichst generisch sein sollen. Daher stellt sich die Frage, wie diese optimal gestaltet werden können. Folgende Möglichkeiten konnten identifiziert werden:

1. Für die einzelnen Stakeholder-Systeme werden verschiedene Schnittstellen definiert, die passgenau auf diese Stakeholder-Systeme zugeschnitten sind.
2. Stakeholder-Systeme werden zu Gruppen von ähnlichen Systemen zusammengefasst, für die jeweils eine Gruppen-Schnittstelle existiert. z. B. verschiedene infrastruktur-seitige Überwachungssysteme oder verschiedene Wetter-Überwachungssysteme.
3. Es werden seitens der smartLogic generische Schnittstellen für verschiedene Funktionen definiert, die Stakeholder-Systeme bei der Logik ausüben, z. B. eine Schnittstelle für Stakeholder-Systeme, von denen vor der Genehmigung einer MA eine Rückmeldung erforderlich ist, oder eine Schnittstelle für Stakeholder-Systeme, die Befahrbarkeitseinschränkungen abhängig von ihrem Status vorgeben können. Die einzelnen Stakeholder-Systeme können sich dann mit ihrer jeweiligen Funktion bzw. Sicherheitsanforderung darauf **registrieren** und somit über die Schnittstelle kommunizieren.

   Die smartLogic würde während des Prüfprozesses für die einzelnen funktionalen Schnittstellen prüfen, welche Stakeholder-Systeme jeweils darauf registriert sind und diese Information im Prüfprozess verwerten. Beispielsweise wäre eine funktionale Schnittstelle für zustimmungspflichtige Systeme denkbar. Die smartLogic bittet demnach alle an dieser Schnittstelle registrierten Stakeholder-Systeme um Zustimmung zur Prüfanfrage, bevor diese genehmigt werden kann.

   Die Stakeholder-Systeme würden also je nach Funktion, die sie erfüllen, über die entsprechende Schnittstelle kommunizieren, indem sie sich auf dieser Schnittstelle mit bestimmten Parametern registrieren (siehe nächster Abschnitt). Sie könnten theoretisch auch über mehrere dieser funktionalen Schnittstellen kommunizieren, wenn sie mehrere Funktionen erfüllen.

Bei der ersten Möglichkeit handelt es sich nicht um generische Schnittstellen und die smartLogic wäre nicht zukunftsfest, wenn beispielsweise neue Systeme hinzukommen.

Die zweite Lösung verringert dagegen die Komplexität für die smartLogic. Nachteile ergeben sich allerdings daraus, dass durch die Zusammenfassung zu den Gruppen die einzelnen Schnittstellen komplexer werden würden, um alle Funktionalitäten abzudecken oder alternativ auf Funktionalitäten der Stakeholder-Systeme verzichtet werden müsste. Falls es Schnittmengen zwischen den Gruppen gibt, würde außerdem Redundanz entstehen.

Bei der dritten Lösung wären die Schnittstellen dagegen generisch und unabhängig von den sie nutzenden Stakeholder-Systemen. Die dritte Lösung erfüllt somit die Anforderungen der Zukunftsfestigkeit und der schlanken Logik sehr gut.

Für die smartLogic scheint daher die dritte Lösungsmöglichkeit am zielführendsten zu sein.

Registrierungsarten (Arten von Schnittstellen)

Da im Funktionskatalog aus dem 6. Hauptkapitel denkbare Sensoreinflüsse bereits enthalten sind, kann der Funktionskatalog als Quelle zur Bestimmung der verschiedenen Arten von funktionalen Schnittstellen, auf denen sich Stakeholder-Systeme registrieren können und die somit auch als „***Registrierungsarten***“ bezeichnet werden können, dienen. Registrierte Stakeholder-Systeme haben in der Regel einen Einfluss auf die Gestaltung oder Genehmigungsfähigkeit von Fahrerlaubnissen. Daher sind die Paramter, die mittels ETCS in einer Fahrerlaubnis an die Fahrzeugbewegung übertragen werden können, ebenfalls eine mögliche Quelle für Registrierungsarten. Tab. 43 enthält eine Übersicht, der so ermittelten funktionalen Schnittstellen, die beispielhaft auch in Abb. 61 dargestellt sind.

Tab. 43: Registrierungsarten für Stakeholder-Systeme

funktionale Schnittstelle (Registrierungsart)	**Funktion**	**Beispiele**
zustimmungspflichtige Stakeholder („approval“)	die Zustimmung von an dieser Schnittstelle registrierten Systemen ist zur Durchführung einer Fahrt über den definierten Wirkabschnitt erforderlich	z.B. Bahnübergänge, Rotte (Bautrupp), ...
benachrichtigungspflichtige Stakeholder („notification“)	Systeme an dieser Schnittstelle müssen zur Genehmigung einer MP Betriebsbereitschaft melden	z.B. Lautsprecheranlagen für betrieblich vorgeschriebene Ansagen, ...
einschränkende Stakeholder („restriction“)	Systeme an dieser Schnittstelle können beim Vorliegen bestimmter Bedingungen (z. B. Vorliegen eines Sensorwerts) Einschränkungen (im Sinne einer RA) vorschreiben, die entweder in einem Gleisbereich oder einem Wirkabschnitt gelten	z.B. ereignisabhängige Langsamfahrstellen oder Befahrbarkeitssperren (bspw. durch Windmesser), ...
kommandierende Stakeholder („required action“)	Systeme an dieser Schnittstelle können beim Vorliegen bestimmter Bedingungen Handlungen für Fahrzeugbewegungen vorschreiben (ähnlich zu einschränkenden Stakeholdern)	z. B. Achtungspfiff, Stromabnehmer senken, ...
überwachende Stakeholder („supervisor“ / „sensor“)	Systeme an dieser Schnittstelle können über Statusmeldungen Reaktionsprozesse auslösen, so dass bestehende Fahrerlaubnisse angepasst werden; die Konsequenzen der Statusmeldungen können über die Schnittstelle definiert werden oder vorgesehene Prozesse aktivieren (z. B. - bedingter oder unbedingter Nothalt - Geschwindigkeitsreduktion - Verkürzung der Zieldistanz - Reversing)	z. B. Zungenüberwachung, menschliche Meldung eines Notfalls, Brandmeldeanlage eines Tunnels, ...
Hörer („listener“)	reine Informationsschnittstelle ohne Einfluss auf die Entscheidungen der smartLogic	z.B. Informationssysteme, Aufzeichnungssysteme, ...

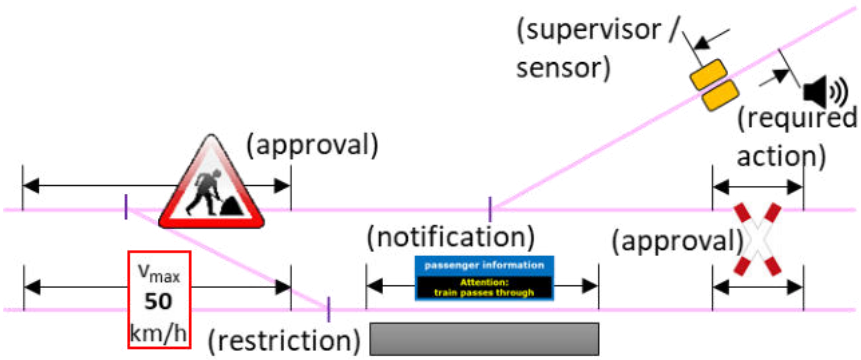


Abb. 61: Registrierung von Stakeholder-Systemen
[Eigene Darstellung]

Registrierungsparameter

Nachdem geklärt ist, welche generischen Schnittstellen zur Registrierung von Stakeholder-Systemen sinnvoll sind, stellt sich als nächstes die Frage, mit welchen Parametern sich die Stakeholder-Systeme registrieren können sollen. Die Parameter ergeben sich dabei zum einen aus der Prüfbedingung, die das Stakeholder-System erforderlich machen, und zum anderen aus möglichen Eingrenzungen, um mögliche Einschränkungen der Befahrbarkeit der Gleisinfrastruktur durch das Stakeholder-System so gering wie möglich zu halten (vgl. Kapitel 7.3.6).

Um den Einflussbereich der Registrierung des Stakeholder-Systems auf der Topologie zu verorten, ist ein Wirkabschnitt erforderlich, der angibt, wo sich die Registrierung auf die Zugfahrten auswirkt. Auch die Angabe eines Detektionsabschnitts kann erforderlich sein, wenn eine Abhängigkeit zwischen der Beanspruchung eines anderen Gleisabschnitts besteht, der nicht Teil des Wirkabschnitts ist (vgl. zu Wirk- und Detektionsabschnitt Kapitel 7.3.5).

Damit durch die Stakeholder-Registrierung verursachte Einschränkungen nicht länger bestehen, als erforderlich, sollte auch die zeitliche Gültigkeit angegeben werden können. Dabei kann die zeitliche Gültigkeit, ähnlich wie die räumliche Gültigkeit, nicht nur auf einen bestimmten Zeitraum beschränkt sein (z. B. die Sperrung gilt für fünf Stunden oder täglich von 15 – 17 Uhr), sondern auch von anderen zeitlichen Parametern abhängig sein. Beispielsweise ist es denkbar, dass eine Mindestzeit und/oder eine maximale Zeit für die Gültigkeit existiert (z. B. die maximale Schließzeit eines Bahnübergangs bevor ein Reaktionsprozess aktiv wird). Es ist auch denkbar, dass eine Mindest- oder maximale Zeit zwischen zwei Gültigkeiten existiert (z. B. eine minimale Zeit, die zwischen zwei Warnungen von Rotten (Gleisarbeitertrupps) vergangen sein muss, damit sie als getrennte Warnungen erkannt werden können).

Neben einer räumlichen und zeitlichen Gültigkeitsvorgabe und der Knüpfung an einen Detektionsabschnitt kann es sinnvoll sein, die Wirkung der Stakeholder-Registrierung auf bestimmte Fahrzeugbewegungen eingrenzen zu können. Ein Überblick über mögliche Eingrenzungen wird bei den RA in Tab. 29 gegeben. Zudem können Löschbedingungen definiert werden, mit denen festgelegt werden kann, unter welchen Voraussetzungen eine Einschränkung wieder zurückgenommen werden kann.

Wie in Tab. 43 geschildert, kann das Stakeholder-System je nach Registrierungsart eine RA vorgeben. Diese RAs könnten ebenfalls zu den Registrierungsparametern gehören oder sie müssten im Einzelfall – also wenn die Voraussetzungen für die Einschränkung oder Handlungsvorgabe für Fahrzeugbewegungen vorliegen – vom Stakeholder-System mit den entsprechenden Parametern an die smartLogic übermittelt werden. Die letztere Lösung ist flexibler, da das Stakeholder-System

beliebige Einschränkungen triggern kann, die nicht vorher festgelegt worden sein müssen. Bei den Einschränkungen ist noch festzulegen, ob sie

- auch für Fahrzeugbewegungen gelten, die sich aktuell im Wirkabschnitt befinden,
- nur für Fahrzeugbewegungen gelten, die bereits eine MA für den Wirkabschnitt haben, sich aber noch nicht im Wirkabschnitt befinden oder
- nur für zukünftige Fahrerlaubnisse gelten.

Mittels der Timeout-Parameter kann festgelegt werden, wie lange nach einer Kontaktaufnahme der smartLogic mit dem Stakeholder-System auf eine Reaktion des Stakeholder-Systems gewartet werden soll und wie oft angefragt werden soll, falls eine Kontaktaufnahme erfolglos war, bevor die entsprechende Prüfbedingung als fehlgeschlagen gewertet wird (vgl. „Timeout-Prozess“ in Kapitel 8.6.8).

Tab. 44 enthält einige mögliche Registrierungsparameter und für welche Registrierungsarten diese angegeben werden können. Die Tabelle enthält alle Parameter, die zur Beschreibung der in Kapitel 6 identifizierten Prüfbedingungen erforderlich sind. Zur Erhöhung der Vollständigkeit wurde die Tabelle durch Institutskollegen ergänzt. Als Anhaltspunkt dienten die bekannten W-Fragen, wobei die Frage „Wozu?“ (Erfüllung der Prüfbedingungen ohne unnötig große Einschränkung definieren zu müssen) bereits beantwortet ist. Damit ergeben sich auf den Gegenstand der Prüfbedingung bezogene (Was?), räumliche (Wo?), zeitliche (Wann?), auf Subjekte bezogene (Wer?), sowie auf die Umsetzungsart und -weise (Wie?) bezogene Registrierungsparameter. Die Liste kann bei Bedarf erweitert werden.

Tab. 44: Registrierungsparameter für Stakeholder-Systeme

Registrierungsparameter	**Registrierungsarten**
Registrierungsart	alle
Wirkabschnitt (vgl. Kapitel 7.3.5)	alle
Gültigkeitsbeschränkungen der Registrierung auf bestimmte Fahrzeugbewegungen (vgl. Kapitel 7.3.6) bezogen auf den Wirkabschnitt	alle
Detektionsabschnitt (vgl. Kapitel 7.3.5)	alle
Gültigkeitsbeschränkungen der Registrierung auf bestimmte Fahrzeugbewegungen (vgl. Kapitel 7.3.6) bezogen auf den Detektionsabschnitt	alle
Gültigkeitszeitraum der Registrierung	alle
maximale kontinuierliche Beanspruchungszeit	zustimmungspflichtige und benachrichtigungspflichtige
minimale kontinuierliche Beanspruchungszeit	zustimmungspflichtige und benachrichtigungspflichtige
maximale Zeit zwischen zwei Beanspruchungen	zustimmungspflichtige und benachrichtigungspflichtige
minimale Zeit zwischen zwei Beanspruchungen	zustimmungspflichtige und benachrichtigungspflichtige
zu definierende RAs bei Vorliegen eines bestimmten Status des Stakeholders-Systems (vgl. Kapitel 7.3.6)	einschränkende
Handlungsvorgaben für Fahrzeugbewegungen bei Vorliegen eines bestimmten Status des Stakeholders-Systems (vgl. Kapitel 7.3.6)	kommandierende

Parameter für Reaktionsprozesse bei Vorlage eines bestimmten Status des Stakeholder-Systems (siehe Kapitel 8.7)	überwachende
Timeout-Parameter	zustimmungspflichtige und benachrichtigungspflichtige
Funktion zur Bestimmung der Schutzrate im Abhängigkeit vom Status des Stakeholder-Systems (Rückfallebenenfunktion, siehe Kapitel 8.3.6)	zustimmungspflichtige und benachrichtigungspflichtige
Löschbedingungen	einschränkende und kommandierende
Auswirkungen bei Deregistrierung des Stakeholder-Systems auf aktive Fahrerlaubnisse (siehe Kapitel 8.5.2)	alle außer Hörer
bei Kommunikationsverlust auszulösende Aktivität	alle außer Hörer
bei Fehlermeldung auszulösende Aktivität	alle außer Hörer

Einfluss der Stakeholder-Registrierung auf die Schutzrate

Ein identifizierter Parameter in Tab. 44 bezieht sich auch auf den Einfluss der Stakeholder-Registrierung auf die Schutzrate. So kann der Status eines Stakeholder-Systems die Schutzrate über eine Funktion beeinflussen, um möglichst genau die aus diesem Status entstehenden Einschränkungen der Befahrbarkeit des entsprechenden Wirkabschnitts der Registrierung des Stakeholder-Systems in die Schutzrate übertragen zu können. In diesem Abschnitt soll der dahinterstehende Mechanismus erarbeitet werden.

Der Einfluss eines bestimmten Status eines Stakeholder-Systems kann je nach Zustand des Stakeholder-Systems unterschiedlich sein. Sowohl die Zustände der Stakeholder-Systeme als auch der Einfluss der jeweiligen Zustände auf die Schutzrate kann sich auch zwischen den verschiedenen Stakeholder-Systemen, die an einer Funktionsschnittstelle registriert sind, unterscheiden. Deshalb ist es sinnvoll, dass die Höhe des Einflusses auf die Schutzrate in Abhängigkeit des Systemzustands des Stakeholder-Systems bei der Registrierung als Registrierungsparameter angegeben werden kann.

In Kapitel 8.3.2 wurde beispielsweise festgestellt, dass mehrere Zielpunkte mit einem jeweils abgestuften Gefährdungsrisiko im Falle des Passierens durch eine Fahrzeugbewegung sinnvoll sein können. Die Zielpunkte sollten dabei jeweils unmittelbar vor den nächsten Gefahrpunkt gesetzt werden, durch dessen Passieren das dazugehörige Gefährdungsrisiko die Schutzrate unter den Schwellwert für die Genehmigung der Prüfanfrage drücken würde. Auch Stakeholder-Systeme können ein Gefährdungsrisiko repräsentieren und damit einen Zielpunkt bedingen. So wäre es beispielsweise prinzipiell denkbar, dass die EoA einer Fahrzeugbewegung vor einen teilweise gestörten Bahnübergang (Schranken schließen nicht, aber Lichtzeichenanlage funktioniert) gesetzt werden muss, die SvL allerdings dahinter gesetzt werden kann, weil die Wahrscheinlichkeit, dass die Fahrzeugbewegung den BÜ noch passiert und gleichzeitig ein Straßenverkehrsteilnehmer das Rotlicht des BÜs missachtet, entsprechend geringer ist, als wenn die Fahrzeugbewegung von vorneherein den BÜ passieren dürfte.

Weitere Möglichkeiten, abgestufte Schutzraten zu definieren, sind in Hinblick auf Rückfallebenen sinnvoll (siehe Kapitel 8.3.6). So könnte ein zustimmungspflichtiger Stakeholder seine Zustimmung mit verschiedenen Einschränkungen verbinden. Zum Beispiel könnte die Zustimmung bei einer Geschwindigkeit A mit Schutzrate x(A) erfolgen und bei Geschwindigkeit B mit Schutzrate x(B). Theoretisch wäre auch eine Angabe der Schutzrate als Funktion möglich. Auch weitere Bedingungen

für eine Erhöhung der Schutzrate, die in der MA für die Fahrzeugbewegung enthalten sein können, wie ein Kommando zum Pfeifen, könnten gegeben werden. Eine entsprechende Rückfallebene könnte für das Passieren eines Bahnübergangs beispielsweise ein Stopp vor dem Bahnübergang, Pfeifen und anschließend eine Befahrung auf Sicht mit 5 km/h sein. Diese Maßnahmenkombination könnte als Bedingung für eine hohe Schutzrate bei Vorliegen eines bestimmten Zustands registriert werden.

Überlegungen zum Registrierungs- bzw. Deregistrierungsprozess

Gemäß den Anforderungen muss es möglich sein, dass während der Laufzeit der smartLogic externe Systeme Sicherheitsanforderungen zur Berücksichtigung in der smartLogic ergänzen, ändern oder löschen können. Stakeholder-Systeme müssen sich also zur Laufzeit bei der smartLogic registrieren und deregistrieren können. Nachdem die Form der Registrierung von Stakeholder-Systemen bestimmt wurde, ist deshalb noch der Prozess zur Registrierung bzw. Deregistrierung zu erarbeiten.

Ein Beispiel für eine nachträgliche Registrierung könnten Gleisarbeiter sein, zu deren Schutz eine temporäre Befahrbarkeitssperre eingerichtet werden soll, die für einzelne Fahrzeugbewegungen nach Zustimmung der Rotte (Bautrupp) deaktiviert werden kann. Bei diesem Beispiel würde es sich um eine Registrierung auf der Schnittstelle für zustimmungspflichtige Stakeholder mit dem Baustellenbereich als entsprechendem Wirkabschnitt handeln. Der Wirkabschnitt muss folglich bei der Registrierung als Registrierungsparameter angegeben werden, damit die smartLogic bei einer Prüfanfrage für jedes in der Anfrage enthaltene Gleissegment prüfen kann, welche Stakeholder-Systeme auf diesem Gleissegment auf welcher Schnittstelle registriert sind, und die daraus resultierenden Einschränkungen und Vorgaben durch registrierte Stakeholder-Systeme beachten kann.

Um Missbrauch zu vermeiden, sollte ein Sicherheitsmechanismus vorhanden sein, der das unerlaubte Registrieren von Stakeholdern und, noch wichtiger, das unerlaubte Entfernen zuverlässig verhindert. Diese „Security“-Fragestellungen werden aber gemäß Kapitel 3.3 in dieser Arbeit nicht vertieft.

Bei der Registrierung ist zu klären, wie sich die Neuregistrierung auf bestehende Beanspruchungen im Bereich des Wirkabschnitts der Registrierung auswirkt:

1. Die Neuregistrierung wirkt sich erst auf die nächste zu prüfende Anfrage des TMS aus – bestehende Beanspruchungen von Fahrzeugbewegungen würden also nicht mehr beeinflusst werden.
2. Alle bestehenden Beanspruchungen werden im Wirkabschnitt auf eine mögliche, notwendige Aktualisierung hin überprüft.

Bei der zweiten Möglichkeit ist zu beachten, dass nicht garantiert werden kann, dass die Änderung von den Fahrzeugbewegungen mit bestehenden Beanspruchungen auch umgesetzt würde, da bei einer bestehenden MA und erst recht bei einer Fahrzeugbelegung bereits vollendete Tatsachen geschaffen wurden (die Fahrzeugbewegung darf ihre bereits übermittelte MA nutzen). Daher ist eine zuverlässige nachträgliche Beeinflussung nicht möglich. Sollte es unmittelbaren Interventionsbedarf in Bezug auf bereits genehmigte MA geben, sollte die Standardschnittstelle für das Einfordern eines Nothalts genutzt werden und nicht eine nachträgliche Stakeholder-Registrierung. Dennoch kann es Fälle geben, in denen eine unmittelbare Einschränkung möglichst auch auf bestehende Fahrten sinnvoll ist. Zum Beispiel bei einer Geschwindigkeitsreduzierung bei starkem Wind.

Um von beiden Möglichkeiten profitieren zu können, erscheint es sinnvoll, den Einfluss von Neuregistrierungen auf bestehende Beanspruchungen vom Stakeholder-System wählbar zu machen (vgl. Tab. 44). Allerdings darf das neu registrierte Stakeholder-System nicht davon ausgehen, dass die neue Einschränkung von Fahrzeugen mit bereits genehmigten MA bereits berücksichtigt wird.

Sinnvollerweise wird das System informiert, sobald keine bei der Registrierung bereits bestehende Beanspruchung mehr seine Nutzung verhindert.

Die Deregistrierung ist dagegen einfacher. In diesem Fall gilt die geänderte Betriebssituation ab der nächsten Anfrage vom TMS, die über den zugehörigen Wirkabschnitt verläuft. Dies wirkt sich zur sicheren Seite hin aus, denn die durch das Stakeholder-System definierten Voraussetzungen für die Genehmigung von Anfragen gelten ja für alle aktiven Anfragen noch. Möchte das TMS die Möglichkeit einer optimierten Anfrage aufgrund der weggefallenem Stakeholder-Bedingung nutzen, kann es einfach eine aktualisierte Fahrerlaubnis für das Fahrzeug beantragen. Für diese „neue“ Anfrage gilt dann die Bedingung durch das deregistrierte Stakeholder-System nicht mehr.

Zusammenfassung

Bei den Stakeholder-Systemen handelt es sich um externe Systeme, die bestimmte Schutzfunktionen übernehmen oder Überwachungsfunktionen ausüben, um spezielle Sicherheitsanforderungen zu erfüllen. Auch Personen (z. B. Posten) können für die smartLogic Stakeholder-Systeme sein, sofern eine standardisierte, digitale Kommunikationsmöglichkeit besteht. Gemäß den identifizierten Anforderungen wird eine generische Beschreibung der Stakeholder-Systeme benötigt. Zudem sollen Stakeholder-Systeme zur Laufzeit hinzugefügt („registriert“) und entfernt („deregistriert“) werden können.

Die Stakeholder-Systeme werden deshalb gemäß ihrer Funktion über generische, standardisierte Schnittstellen in die Prüfprozesse der smartLogic eingebunden. Die Stakeholder-Systeme können sich dazu auf diesen Schnittstellen registrieren. Zu jeder Registrierung gehören eine Reihe von Registrierungsparametern, welche die Registrierung und ihre Funktion näher beschreiben. Die Funktion der Registrierung kann sowohl für den Regelbetrieb als auch für die Rückfallebene angegeben werden. In letzterem Fall kann der Zustand eines Stakeholder-Systems zu einer eingeschränkten Schutzrate führen.

Über den Wirkabschnitt wird der Einflussbereich des Stakeholder-Systems beschrieben. Die Registrierung des Stakeholder-Systems erfolgt folglich auf den Gleissegmenten des Wirkbereichs. Im Rahmen von Prüfprozessen werden für jedes von der Prüfung betroffene Gleissegment die Registrierungen für die verschiedenen funktionalen Schnittstellen geprüft und die angeschlossenen Stakeholder-Systeme entsprechend ihrer Aufgaben im Prüfprozess berücksichtigt.

Die Möglichkeit zur Registrierung und Deregistrierung von Stakeholder-Systemen sollte über ein Security-Konzept begrenzt werden. Bei der Registrierung eines neuen Stakeholder-Systems ist zu klären, ob dessen Wirkung auch für bereits verkehrende Fahrzeugbewegungen oder nur für neue Anfragen an die Sicherungslogik gilt. Bei der Deregistrierung fällt die Wirkung des Stakeholder-Systems für alle anschließend beantragten Fahrzeugbewegung über den Wirkabschnitt weg.

8.3.4 Flankenschutz

Kollisionen verschiedener Eisenbahnfahrzeuge können als Frontalzusammenstoß, als Auffahrunfall oder als Flankenfahrt erfolgen (vgl. Kapitel 2.1.1). Der Schutz vor Flankenfahrten, für den sich im Eisenbahnwesen der Begriff „Flankenschutz“ etabliert hat, wurde in Kapitel 6 als Prüfbedingung in den Funktionskatalog aufgenommen und muss somit von der smartLogic sichergestellt werden. Daher soll im vorliegenden Unterkapitel ein grundsätzliches Konzept entwickelt werden, wie die smartLogic Flankenschutz sicherstellt. Die dazugehörige Subroutine (vgl. zum Begriff Kapitel 6.2.2) wird in Kapitel 8.6.1 beschrieben (vgl. zum Vorgehen die Einleitung zu Kapitel 8.3).

Flankenfahrten können häufig an verschiedenen Orten auf der Route einer beantragten Fahrerlaubnis auftreten, für die jeweils ein unterschiedlich hohes Risiko einer Flankenfahrt existieren kann. Das Gesamtrisiko des Eintritts einer Flankenfahrt für eine beantragte Fahrerlaubnis setzt sich daher aus den einzelnen Risiken für eine Flankenfahrt je potenziellem Kollisionsort zusammen. Um das Gesamtrisiko zu bestimmen, müssen daher die möglichen Kollisionsorte bestimmt werden (erster Abschnitt), für die dann jeweils das Risiko einer Flankenfahrt bestimmt werden muss. Würden mit hinreichender Sicherheit nur vollüberwachte Fahrzeuge verkehren, wäre die Berechnung einfach (zweiter Abschnitt). Jedoch kann eine solche Annahme in der Praxis derzeit nicht gerechtfertigt werden. Deswegen sind weitere Überlegungen notwendig (dritter bis achter Abschnitt).

Auch nach Genehmigung einer Fahrt, kann eine Flankenschutzgefährdung auftreten, wenn sich Rahmenbedingungen ändern, zum Beispiel, wenn ein flankenschutzbietendes Element wie eine Weiche unerwartet ihre Lage ändert. Aus diesem Grund sollten flankenschutzbietende Elemente auch nach Übermittlung einer Fahrerlaubnis an das Fahrzeug überwacht werden. Hierzu muss sich die smartLogic „merken“, welche Elemente Flankenschutz bieten, die Flankenschutzfunktion muss also im Datenmodell (vgl. zum Datenmodell Kapitel 7) abgebildet werden. Daher geht das Unterkapitel im neunten Abschnitt („Speichern von aktiven Flankenschutzbeanspruchungen“) darauf ein, wie die Flankenschutzfunktion im Datenmodell abgebildet werden kann.

Die Anforderung des Regelhandlungsgebots fordert zudem, dass bereits ausgestellte Fahrerlaubnisse nachträglich verändert werden können sollen, und die Anforderung der Resilienz, dass Fahrerlaubnisanfragen nicht abgelehnt werden sollen, wenn sie nicht zu einem unsicheren Zustand führen. Daher sollte geprüft werden, ob bei sich ändernden Anforderungen an flankenschutzgebende Elemente (z. B. andere Lage einer Weiche durch eine weitere beantragte Fahrerlaubnis) eine Neuberechnung der Flankenschutz-Schutzrate durchgeführt und somit das anderweitig benötigte flankenschutzgebende Element aus der Flankenschutzfunktion entlassen werden kann. Dem Thema der Neuberechnung widmet sich der vorletzte Abschnitt, bevor abschließend eine Zusammenfassung erfolgt. Im Abschnitt der Zusammenfassung findet sich auch eine Grafik zur Erläuterung der in diesem Kapitel eingeführten Begriffe.

Mögliche Orte, an denen Flankenfahrten auftreten können

Unter einer Flankenfahrt wird „die seitliche Verletzung eines für die Fahrt freigegebenen Lichtraums“ [Maschek 2018, S. 12] durch ein anderes Eisenbahnfahrzeug verstanden (vgl. auch Kapitel 2.1.1). Die Modellierung von Lichtraum und Fahrzeugbegrenzungslinien wurde bereits in Kapitel 7.3.9 diskutiert. Gemäß den Erkenntnissen aus Kapitel 7.3.9 kann eine Verletzung des Lichtraums zum einen an Verzweigungen des Gleises, wie z. B. Weichen, auftreten. Solche Verzweigungsstellen können demnach als **Flankenschutz-Gefahrstellen** bezeichnet werden (siehe auch Abb. 64 im Abschnitt „Zusammenfassung“). Zum anderen können Lichtraumverletzungen durch Flankenfahrten in Gleisabschnitten auftreten, die eng beieinanderliegen oder sich sogar überlappen oder kreuzen. Diese Gleisabschnitte, wie auch die einmündenden Gleisabschnitte vor Flankenschutz-Gefahrstellen bis zum Grenzzeichen, stellen demnach potenzielle **Flankenschutz-Gefahrabschnitte** dar.

Die für eine Fahrerlaubnisanfrage relevanten Flankenschutz-Gefahrabschnitte können mit Hilfe der topologischen Daten, die gemäß dem im 7. Hauptkapitel beschriebenen Datenmodell der smartLogic vorliegen, identifiziert werden. Zum besseren Verständnis der Zusammenhänge soll nachfolgend kurz darauf eingegangen werden, wie Flankenschutz-Gefahrabschnitte im Datenmodell abgebildet sind.

Zur Erfüllung der globalen Anforderung, wonach Standards möglichst übernommen werden sollen, wurde bereits in Kapitel 2.4 bzw. 2.7 festgestellt, dass eine Kompatibilität zur RCA sinnvoll ist, sofern dies nicht die smartLogic funktionell einschränkt. Die RCA verwendet dabei das Konzept der

Allocation Section Groups (ASG), um Überlappungen des Lichtraumprofils zweier Gleise und damit Flankenschutz-Gefahrabschnitte, wie sie im vorigen Absatz beschrieben wurden, zu beschreiben (vgl. Kapitel 7.3.9 und Kapitel 7.4.3 sowie zum Konzept der ASG Kapitel 2.4.4). Demnach wird der Teil des jeweiligen Gleissegments, in dem eine Lichtraumprofil-Überlappung mit dem Lichtraumprofil eines anderen Gleissegments vorliegt (also z. B. bei der Weiche jeweils der Teil des Gleissegments vom Weichenanfang bis zum Grenzzeichen), als Allocation Section (AS) oder in neueren Versionen der RCA-Dokumente auch als Allocation Area (AA) bezeichnet (im Folgenden wird AS als Bezeichnung verwendet). Die in Konflikt stehenden AS werden zu einer ASG zusammengefasst (vgl. Kapitel 2.4.4).

Gemäß Kapitel 7.4.3 sind die AS einer ASG im Datenmodell der smartLogic Gleisabschnitte (vgl. Kapitel 7.3.3, Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)“) und die gegenseitige Wechselwirkung der AS einer ASG wird über den Mechanismus von Detektions- und Wirkabschnitten beschrieben (vgl. zur Funktionsweise von Detektions- und Wirkabschnitt auch Kapitel 7.3.5). Demnach löst die Beanspruchung des Detektionsabschnitts durch eine Fahrzeugbewegung (z. B. Aufnahme in eine Fahrerlaubnis für diese Fahrzeugbewegung) eine vordefinierte Wirkung auf die verknüpften Wirkabschnitte aus. Der Detektionsabschnitt ist im Flankenschutz-Fall die AS, die von der zu schützenden Fahrt beansprucht wird. Die Wirkabschnitte sind die verknüpften AS und damit die zugehörigen Flankenschutz-Gefahrabschnitte. Allgemein kann daher ausgesagt werden, eine AS ist ein Flankenschutz-Gefahrabschnitt für eine Fahrzeugbewegung, wenn ihr Detektionsabschnitt von der Fahrzeugbewegung beansprucht wird.

Eine Auswahl verschiedener denkbarer statischer ASG und damit potenzieller Flankenschutz-Gefahrabschnitte enthält [Skowron 2020]. Nach der Logik aus Kapitel 7.3.9 kommen dynamische ASG hinzu, die in Folge von Fahrzeugen mit außergewöhnlichen Grenzlinien („Lademaßüberschreitungen“) entstehen. Diese können daher keine feste Ausdehnung haben. Diese letztgenannten ASG sollen jedoch hier aufgrund der in Kapitel 7.3.9 beschriebenen Gründe nicht tiefgehend betrachtet werden.

Sicherstellen des Ausschlusses von Flankenfahrten für den Fall, dass sich mit hinreichender Sicherheit ausschließlich vollüberwachte Fahrzeuge auf der Infrastruktur befinden

Bei vollüberwachten Fahrzeugen garantiert das Zugsicherungssystem, dass das Fahrzeug mit hinreichender Sicherheit innerhalb der Parameter seiner Fahrerlaubnis bleibt (vgl. Modus „Full Supervision“ im Kapitel 2.2.2 im Abschnitt „Betriebsmodi“). Im (Ideal-)Fall wären aus Flankenschutz-Sicht alle Fahrzeuge auf der von der smartLogic überwachten Infrastruktur jederzeit vollüberwacht. In diesem Fall würde es ausreichen sicherzustellen, dass eine zu genehmigende Fahrerlaubnis keinen Flankenschutz-Gefahrabschnitt beinhaltet, der zu einer anderen gültigen Fahrerlaubnis gehört bzw. dass eine solche Fahrerlaubnis nur in ganz speziellen Sonderfällen (wie Fahren auf Sicht und mit sehr niedriger Geschwindigkeit) genehmigt werden kann.

Allerdings ist davon auszugehen, dass die für den Idealfall beschriebene Bedingung (ausschließlich vollüberwachte Fahrzeuge) im Sinne der Anforderung der Migrationsfähigkeit nicht in allen Fällen erfüllbar sein wird, weil auf absehbare Zeit weiterhin nicht ortbare Züge bzw. zumindest einzelne Eisenbahnwagen existieren. Deshalb sind zusätzliche Überlegungen notwendig, um auszuschließen, dass nicht vollüberwachte Fahrzeuge existieren, die eine Flankenschutzgefährdung darstellen könnten.

Ausgangspunkte für die Berechnung der Schutzrate im komplexeren Fall

Für den Fall, dass die Anwesenheit von nicht vollüberwachten Fahrzeugen auf der betrachteten Infrastruktur nicht ausgeschlossen werden kann, beeinflusst die Wahrscheinlichkeit, mit der solche Fahrzeuge tatsächlich eine Flankenfahrt verursachen, die Schutzrate.[53] Daher ist diese Wahrscheinlichkeit zu bestimmen.

Zur Berechnung der Wahrscheinlichkeit, mit der eine Flankenfahrt tatsächlich stattfindet, sind verschiedene Einflussgrößen wie das Vorhandensein von Flankenschutzelementen oder die grundsätzliche Wahrscheinlichkeit des Vorhandenseins von potenziell gefährdenden Fahrzeugen denkbar. Um diese Einflussgrößen zu bestimmen, wurden zwei denkbare Ausgangspunkte identifiziert:

1. die möglichen Flankenschutz-Gefahrabschnitte
2. die potenziell gefährdenden Fahrzeuge

Für den zweiten Fall müsste allerdings festgestellt werden, welche Fahrzeuge potenziell eine Flankenfahrt verursachen könnten. Da jedoch im ersten Absatz dieses Abschnitts davon ausgegangen wurde, dass nicht zwangsläufig alle potenziell gefährdenden Fahrzeuge bekannt sind, wird diese Feststellung nicht immer möglich sein. Deshalb werden die Flankenschutz-Gefahrabschnitte als Ausgangspunkt gewählt.

Theoretisch könnte das Schadensereignis „Flankenfahrt“ an jedem Flankenschutz-Gefahrabschnitt getrennt voneinander von verschiedenen Fahrzeugen verursacht werden. Für die Berechnung erscheint daher die Annahme naheliegend, dass das Risiko einer Flankenfahrt für die einzelnen Gefahrabschnitte unabhängig voneinander ermittelt werden kann, wie es in Abb. 62 dargestellt ist.

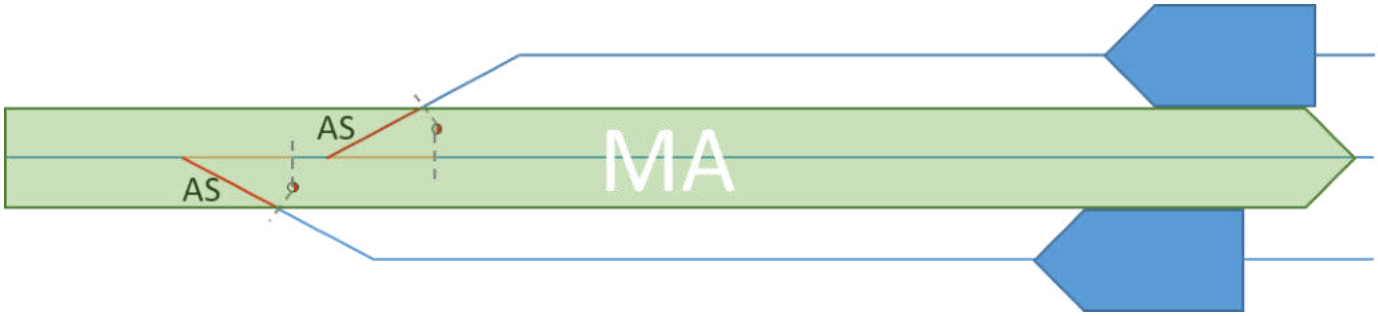


Abb. 62: zwei unabhängige Flankenschutz-Gefahrabschnitte (AS)
Quelle: [Eigene Darstellung]
in Rot sind die aktiven AS eingezeichnet und in Gelb die dazugehörigen Detektionsabschnitte, welche die AS bei Einbindung des Detektionsabschnitts in die MA aktiviert haben

Die Unabhängigkeit ist jedoch nicht immer gegeben. Zum Beispiel könnte theoretisch derselbe entlaufene Wagen eine Fahrt mit Lademaßüberschreitung auf parallelen Gleisen gefährden und dieselbe Fahrt auch an der nächsten Weiche gefährden, wie in Abb. 63 dargestellt. Diese Fälle werden allerdings als seltene Sonderfälle angesehen, die sich bei Annahme der Unabhängigkeit zur sicheren Seite hin auswirken, da dann dasselbe Risiko doppelt in die Berechnung der Schutzrate einfließt und

[53] Je nachdem, wie hoch die Schutzrate eingeschränkt wird, sind unterschiedliche Folgen denkbar. Eine potenzielle Flankenschutzgefährdung muss nicht direkt zur Ablehnung einer Anfrage führen, da es denkbar erscheint, dass z. B. ein fehlender physischer Schutz durch organisatorische Schutzmaßnahmen bis zu einem gewissen Maße kompensiert werden kann. Weiterhin kann auch durch eine Einschränkung der Fahrzeugbewegung, der die der Prüfung zugrundeliegende Anfrage gilt, die Schutzrate erhöht werden. Dies könnte z. B. durch eine niedrigere Geschwindigkeit geschehen, die ein rechtzeitiges Erkennen einer möglichen Flankenfahrt und eine entsprechende gefahrenmindernde Reaktion erlaubt. Es ist daher plausibel, dass eine Flankenschutzgefährdung vielfältige Einflüsse auf die Schutzrate haben kann.

die Schutzrate somit verschlechtert. Aus diesem Grund kann die Annahme der Unabhängigkeit als gerechtfertigt angenommen werden.

Abb. 63: Spezialfall Abhängigkeit zweier Flankenschutz-Gefahrabschnitte (AS) von derselben Fahrzeugbewegung
Quelle: [Eigene Darstellung]

Die Flankenschutz-Gefahrabschnitte bilden also die Quellen einer Risikobetrachtung, die für jeden Gefahrabschnitt unabhängig von den anderen Gefahrabschnitten durchgeführt werden kann. Die Ereignisketten, die zum Eintritt der Gefährdung führen könnten, werden dabei als unabhängig voneinander angenommen. Für jeden Flankenschutz-Gefahrabschnitt muss das Risiko einer Flankenfahrt ermittelt werden. In das jeweilige Gefährdungsrisiko für die betrachtete Zugfahrt fließt zudem noch die Erreichenswahrscheinlichkeit der zugehörigen Flankenschutz-Gefahrstelle als Faktor ein, die beispielsweise für Flankenschutz-Gefahrstellen hinter dem anzusteuernden Zielpunkt (EoA) einen Wert kleiner als 1 haben kann.

Die Flankenschutz-Schutzrate kann dann als Produkt der inversen Einzelrisiken bestimmt werden (vgl. auch Kapitel 8.3.1), wobei n die Anzahl der relevanten Flankenschutz-Gefahrabschnitte und r_i das Risiko einer Flankenfahrt bei Gefahrabschnitt i ist und $\phi(s_i)$ die Erreichenswahrscheinlichkeit der zum Gefahrabschnitt i gehörenden Flankenschutz-Gefahrstelle.

$$Flankenschutz\text{-}Schutzrate = \prod_i^n (1 - r_i * \phi(s_i))$$

Beispielsweise würde bei zwei Gefahrabschnitten mit jeweils einem Risiko einer Flankenfahrt von 10 Prozent und einer Erreichenswahrscheinlichkeit von 100 Prozent, weil die zugehörige Flankenschutz-Gefahrstelle von der betroffenen Fahrzeugbewegung vor der EoA erreicht wird, die flankenschutzbezogene Schutzrate 81 Prozent $((1 - 0{,}1) * (1 - 0{,}1) = 0{,}81)$ und damit das Gesamtrisiko einer Flankenfahrt im betrachteten Abschnitt 19 Prozent $(1 - 0{,}81 = 0{,}19)$ betragen.

Fälle, in denen eine Flankenschutzverletzung auftritt

Wie im vorigen Abschnitt festgestellt wurde, muss für jeden Flankenschutz-Gefahrabschnitt als Quelle der Risikobetrachtung nun das Risiko einer Flankenfahrt bestimmt werden. Um diese jeweiligen Risiken bestimmen zu können, ist es sinnvoll, zunächst zu fragen, in welchen Fällen bezogen auf den jeweiligen Gefahrabschnitt eine Flankenschutzverletzung auftritt.

Der naheliegendste Fall einer Flankenschutzverletzung ist, wenn ein Fahrzeug in einen Flankenschutz-Gefahrabschnitt einfährt, während der zugehörige Detektionsabschnitt von der zu schützenden Fahrzeugbewegung belegt ist (eine andere Fahrt würde der zu schützenden Fahrzeugbewegung in die Flanke fahren). Befindet sich bereits ein Fahrzeug in einem Gefahrabschnitt, der für die zu schützende Fahrzeugbewegung benötigt wird, und verletzt damit deren Lichtraumprofil, tritt ebenfalls eine Verletzung auf (die zu schützende Fahrt würde einer nicht profilfrei stehenden Fahrt in die Flanke fahren). Auch wenn es sich beim zweiten Fall strenggenommen um fehlende Profilfreiheit handelt, erscheint es sinnvoll, diese Fälle in die folgenden Überlegungen mit einzubeziehen, da in beiden Fällen eine Gefährdung der Fahrzeugbewegung von der Seite auftritt.

Bei fehlender Profilfreiheit ist die Flankenschutzverletzung zur Zeit der Prüfung der Prüfanfrage durch die smartLogic bereits eingetreten. Die beantragte Fahrt kann daher nicht stattfinden und die Anfrage

muss zurückgewiesen werden. Hierbei spielt auch die zeitliche Komponente keine Rolle, denn es kann nicht garantiert werden, dass ein Fahrzeug sich noch entfernt oder eine genehmigte MA nicht genutzt wird.

Bestimmen des potenziellen Flankenschutzraums

Befindet sich noch kein Fahrzeug im Flankenschutz-Gefahrabschnitt, ist also zunächst die Profilfreiheit gegeben, muss geklärt werden, wie hoch die Wahrscheinlichkeit ist, dass ein Fahrzeug aktiv in den Gefahrabschnitt einfährt bzw. passiv hineinrollt und damit eine Flankenfahrt verursacht. Hierfür muss ein Fahrzeug in relevanter Zeit über eine Gleisverbindung den Gefahrabschnitt erreichen können.

Dabei stellt sich die Frage, was eine relevante Zeit ist. Die Zeit beeinflusst die Größe des Suchraums für potenziell gefährdende Fahrzeuge, der auch Flankenschutz-Überwachungsraums oder kurz **Flankenschutzraum**, genannt werden kann.

Ein Extrem wäre, die Zeit auf unendlich zu setzen, um möglichst alle Fahrzeuge zu finden, die einen theoretisch möglichen Fahrweg zum betrachteten Flankenschutz-Gefahrabschnitt haben und somit theoretisch eine Flankenfahrt verursachen könnten. Alternativ kann geprüft werden, ob auch eine kürzere Zeit hinreichend sicher sein kann.

Bei unendlicher Zeit würde der Flankenschutzraum alle Gleise umfassen, von denen ein theoretisch möglicher Fahrweg zur AS existiert. Da die zu schützende Fahrzeugbewegung bei der Anfahrt auf den Flankenschutz-Gefahrabschnitt zum Stehen kommen könnte und in der Folge über den gesamten Standzeitraum, der theoretisch unendlich sein könnte, an dieser Stelle gefährdet werden könnte, ist die Wahl einer unendlich langen Zeit am sichersten. Allerdings könnte dieses Vorgehen zu sehr großen Flankenschutzräumen führen, wodurch eine effiziente Ausnutzung der Infrastruktur verhindert würde.

Bei einer kürzeren Zeit würde sich die Schutzrate mit der Länge dieser Zeit und damit mit der dann ebenfalls abnehmenden Größe des Flankenschutzraums verringern. Der Flankenschutzraum müsste daher, um unnötige Ablehnungen der Anfrage zu erreichen, so groß gewählt werden, dass die Schutzrate noch hinreichend groß ist, damit die Fahrerlaubnisanfrage genehmigt werden kann. Als Richtwert für eine akzeptable Zeit könnte die Zeit dienen, welche die zu schützende Fahrzeugbewegung erwartungsgemäß noch benötigt, um den Detektionsabschnitt des betrachteten Flankenschutz-Gefahrabschnitts mit hoher Wahrscheinlichkeit passiert zu haben. Der Flankenschutzraum würde sich dann soweit erstrecken, wie ein Fahrzeug, welches eine Flankenschutzgefährdung auslösen könnte, von den Grenzen des Flankenschutzraums mit maximaler Geschwindigkeit benötigen würde, um den Flankenschutz-Gefahrabschnitt innerhalb dieser Zeit erreichen zu können.

Kommt die zu schützende Fahrzeugbewegung unplanmäßig zum Halten bzw. verringert unerwartet ihre Geschwindigkeit und nähert sich zum gleichen Zeitpunkt tatsächlich unerwartet eine nicht vollüberwachte Fahrzeugbewegung, die zu einer Flankenfahrt führen könnte, müssten geeignete Schadensbegrenzungsmaßnahmen, wie das rechtzeitige Anhalten oder sogar ein mögliches „Reversing“ eingeleitet werden (siehe Kapitel 8.7). Trotzdem würde ein Restrisiko bestehen. Damit es in einem solchen Fall allerdings tatsächlich zu einer Flankenfahrt mit beträchtlichem Schadensausmaß kommt, müsste eine ganze Reihe von eher unwahrscheinlichen Fällen zusammenkommen. Es müsste ein Fahrzeug existieren, das

- nicht vollüberwacht ist,
- sich in Richtung der zu schützenden Fahrzeugbewegung bewegt,

- ohne Fahrerlaubnis verkehrt oder die Parameter der Fahrerlaubnis unerlaubt überschreitet oder dem unerlaubterweise das Überschreiten der Parameter der Fahrerlaubnis erlaubt wurde,
- trotz des langen Vorlaufs durch den großen Abstand nicht zum Stoppen bewegt werden kann oder dass trotz eines entsprechenden Reaktionsprozesses der smartLogic nicht gewarnt wird,
- ein Fahrzeug gefährdet, welches nicht rechtzeitig aus dem Gefahrenbereich gebracht werden kann UND
- an der Kollisionsstelle eine kinetische Energie freisetzt, die trotz Stopps des zu schützenden Fahrzeugs ausreichend groß ist, um einen fatalen Unfall zu erzeugen.

Eine solche Ereigniskette wird als hinreichend unwahrscheinlich angenommen, so dass eine entsprechend begrenzte Zeit und damit Ausdehnung des Flankenschutzraumes möglich erscheint. Auch heute wären Flankenfahrten in Folge einer solchen Ereigniskette beispielsweise an Abzweigstellen möglich, da hier teilweise kein physischer Flankenschutz existiert.

Aus der oben beschriebenen begrenzten Zeit kann entlang jedes möglichen Pfades auf der Topologie (möglicher Fahrweg einer feindlichen Fahrt) ein Punkt auf der Topologie hergeleitet werden, bis zu dem nach möglichen flankenschutzgefährdenden Fahrzeugen gesucht werden muss. Notwendige Sicherheitsreserven sind dabei zu berücksichtigen. Der Punkt markiert das Ende des **potenziellen Flankenschutz**(such)**raums**. Wenn innerhalb des potenziellen Flankenschutzraums keine potenzielle Flankenschutzgefährdung gefunden wurde, ist die Schutzrate hinreichend hoch, um nicht zu einer Ablehnung der Anfrage zu führen.

Abgrenzen des aktiven Flankenschutzraums

Der potenzielle Flankenschutzraum kann durch bestimmte Schranken, wie klassische physische Flankenschutzelemente (z. B. Schutzweichen oder Gleissperren), welche das Passieren von Eisenbahnfahrzeugen in Richtung des Flankenschutz-Gefahrabschnitts verhindern, weiter eingegrenzt werden. Da sich der Status dieser Elemente ändern kann, beschränken diese Elemente nicht den potenziellen Flankenschutzraum, sondern sie legen je nach Status einen **aktiven Flankenschutzraum** (**Active Flank Area (AFA)**) als Untermenge des potenziellen Flankenschutzraums fest. Als Begrenzungen des aktiven Flankenschutzraums kommen Elemente in Betracht, die das Passieren eines Fahrzeugs ausschließen oder unwahrscheinlich machen. Diese Flankenschutzelemente werden im Folgenden auch als **„Flank Protection Objects“ (FPO)** bezeichnet (siehe zu den Begriffen auch Abb. 64 im Abschnitt „Zusammenfassung“).

Mögliche FPOs wurden aus der Literatur und durch eigenes Brainstorming identifiziert und sind in Tab. 45 mit ihrer jeweiligen Quelle aufgelistet. Eine qualitative Angabe, wie sich die Existenz einer entsprechenden Begrenzung auf die Schutzrate auswirkt, ist ebenfalls angegeben. Wie bereits in Kapitel 8.3.1 erwähnt, ist es nicht Ziel dieser Arbeit, für die Einflussfaktoren auf die Schutzrate konkrete Werte zu ermitteln.

Tab. 45: Einflussgrößen auf die Wahrscheinlichkeit einer Flankenfahrt

Begrenzung (Flank Protection Object FPO)	Konsequenz	Schutzrate	Weiter-suchen	Quelle
DPS eines physischen Flankenschutzelements (FPD), welches nicht	Die DPS signalisiert, dass dieses Element in der Lage einer möglichen	sehr hoch	nein	RCA, klassische Logik

aufgefahren werden kann	Flankenschutzgefährdung nicht befahrbar ist; es kann daraus gefolgert werden, dass es von einer Eisenbahnfahrzeugbewegung nicht passiert werden kann			
DPS eines physischen Flankenschutzelements (FPD), welches aufgefahren werden kann (aber nicht dafür ausgelegt ist)	Eine solche DPS verhindert zwar die Aufnahme des Gleisabschnitts in eine MA, aber nicht, dass theoretisch ein Fahrzeug über diese Gleisverbindung zu einer Flankenschutzgefährdung werden könnte; dennoch besteht über die organisatorischen Maßnahmen ein gewisser Schutz (vergleichbar mit dem heutigen Flankenschutz durch Signale) –> siehe auch DPS einer organisatorisch nicht befahrbaren Stelle	mittel (aufgrund der organisatorischen Maßnahmen)	ja	klassische Logik
DPS einer physisch nicht befahrbaren Stelle	Ist ein Element physisch unbefahrbar, geht von dahinterliegenden Fahrzeugen auch keine Flankenschutzgefahr aus	sehr hoch	nein	eigene Überlegung
DPS einer organisatorisch nicht befahrbaren Stelle (z. B. ungesicherter Bahnübergang, manuelle Gleissperrung)	Hierbei handelt es sich um eine abgeschwächte Form der DPS einer physisch nicht befahrbaren Stelle, da zwar organisatorische Sicherheitsmaßnahmen existieren, dass sich durch diesen Abschnitt keine Fahrt bewegen soll, es aber theoretisch bei unüberwachten Fahrzeugen trotzdem möglich ist	mittel (aufgrund der organisatorischen Maßnahmen)	ja	eigene Überlegung
vollüberwachtes Fahrzeug	ein solches Fahrzeug kann (technisch) zum „Halten bleiben" aufgefordert werden. Es garantiert dann mit hinreichender Sicherheit, dass es sich nicht (nennenswert) bewegt	hoch (mit dem von ETCS garantierten Sicherheitsniveau)	nein	RBC-Lastenheft

Die physischen Flankenschutzelemente, die eine physische Begrenzung der Befahrbarkeit des Gleises herstellen können (dieser Zustand wird im Datenmodell als Drive Protection Section (DPS) abgebildet, vgl. Kapitel 7.4.3), bilden eine Untermenge der FPO. Sie können je nachdem, ob sie zum potenziellen oder aktiven Flankenschutzraum gehören, als **potenzielle** oder **aktive Flankenschutzelemente** (**potential / active Flank Protection Device (FPD)**) bezeichnet werden (siehe auch Abb. 64 im Abschnitt „Zusammenfassung").

Weitersuchen bei nicht optimaler Schutzrate

Wird bei der Suche nach einer Begrenzung des aktiven Flankenschutzraums ein FPO gefunden, das keine optimale Schutzrate bietet, entsteht die Frage, ob nach einem FPO mit besserem Einfluss auf die Schutzrate weitergesucht werden sollte. Prinzipiell wäre es denkbar,

1. nie weiterzusuchen,
2. immer weiterzusuchen,
3. nur weiterzusuchen, wenn eine höhere Schutzrate durch ein zusätzlich gefundenes, höherwertiges FPO auch einen Einfluss auf die Annahme oder Ablehnung der Prüfanfrage des TMS durch die smartLogic hat.

Zur Bewertung der drei Möglichkeiten ist eine Abwägung auf Basis der Anforderungen aus Kapitel 8.2.1 notwendig. Durch ein Weitersuchen würde der Flankenschutzraum größer und damit zum einen die Rechenzeit steigen (widerspricht Anforderung der geringen Latenz) und zum anderen das Risiko größer, dass sich innerhalb des aktiven Flankenschutzraums unbekannte Fahrzeuge befinden (wenn dieses Risiko zu groß wird, würde die Kernanforderung der sicheren Logik verletzt, siehe nachfolgender Abschnitt). Weiterhin würde die Komplexität des Algorithmus durch die Weitersuchen-Funktion möglicherweise etwas zunehmen (widerspricht Anforderung der schlanken Logik). Auf der anderen Seite, würde nicht weiterzusuchen zu mehr Ablehnungen von Anfragen führen, als möglicherweise notwendig (widerspricht der Anforderung, dass eine Anfrage nur bei Verletzung der Kernanforderung abgelehnt werden darf).

Eine Verletzung der Kernanforderung ist nicht zulässig, daher darf nur weitergesucht werden, wenn das Risiko eines unbekannten Fahrzeugs weiterhin[54] hinreichend gering ist. Von den anderen Anforderungen, wurde die letztgenannte Anforderung (Ablehnung einer Anfrage nur, wenn die Kernanforderung verletzt wird) in dieser Arbeit meistens höher gewichtet als andere Anforderungen (mit Ausnahme der Kernanforderung), um eine optimale Funktionsweise der smartLogic zu gewährleisten.

Die erste Möglichkeit (nie weitersuchen) würde die letztgenannte Anforderung auf jeden Fall verletzen. Zur Umsetzung der dritten Möglichkeit müsste zunächst festgestellt werden, ob ein signifikanter Einfluss auf die Schutzrate besteht. Hierfür müssten alle Einflussfaktoren auf die Schutzrate bereits bekannt sein. Dafür müsste die gesamte Prüfung der Prüfbedingung zunächst bis zum Ende durchgeführt werden und dann an die fragliche Stelle zurückgekehrt werden. Dieses Vorgehen erscheint im Vergleich zur zweiten Möglichkeit (pauschales Weitersuchen) auch aufgrund der höheren Komplexität des Vorgangs (vgl. globale Anforderung der schlanken Logik) ungünstiger zu sein. Dagegen wird davon ausgegangen, dass die zusätzlich benötigte Rechenzeit aufgrund der Begrenzung des potenziellen Flankenschutzraums noch akzeptabel bleiben würde.

Es erscheint also sinnvoll, bei einer gefundenen Begrenzung mit nicht optimaler Schutzrate zunächst weiterzusuchen (zweite Möglichkeit), sofern dadurch die Kernanforderung der sicheren Logik nicht verletzt wird (siehe vorletzter Absatz).

Für die Umsetzung dieser zweiten Möglichkeit ist noch zu klären, wann eine Schutzrate „nicht optimal“ ist – wann also weitergesucht werden soll. Die höchste Schutzrate bieten nach Tab. 45 FPDs, die eine nicht überwindbare, physische Unterbrechung der Befahrbarkeit des Gleises bewirken, also beispielsweise eine Weiche in abweisender Lage. Da es keine Begrenzungsarten mit höherer

[54] Wäre dieses Risiko bereits vorher im Flankenschutzraum bis zum ersten gefundenen FPO nicht hinreichend gering, müsste die Prüfanfrage ohnehin abgewiesen werden.

Schutzrate gibt, kann eine solche auch nicht beim Weitersuchen gefunden werden. Ein Weitersuchen macht also in diesem Fall keinen Sinn. Auch das Auffinden von vollüberwachten Fahrzeugen bietet eine hohe Schutzrate. Die verbleibende Gefährdung geht hier vom aufgefundenen Fahrzeug aus, da weitere Fahrzeuge an diesem nicht vorbeikommen. Ein Weitersuchen ergibt daher ebenfalls keinen Sinn. Bei den Begrenzungsarten aus Tab. 45, die nur eine mittlere Schutzrate bieten, besteht dagegen die Möglichkeit durch ein Weitersuchen noch ein FPO zu finden, dass eine höhere Schutzrate bietet. Daher macht Weitersuchen in diesen Fällen Sinn. Der aktive Flankenschutzraum wird deshalb durch diese Elemente nicht begrenzt, sie beeinflussen allerdings die Schutzrate positiv, wenn kein höherwertiger Schutz besteht.

Schutzrate auf den Gleissegmenten des aktiven Flankenschutzraumes

Zwar verhindern die in den beiden vorigen Abschnitten identifizierten Begrenzungen des aktiven Flankenschutzraumes, dass Fahrzeuge in diesen Raum eintreten und somit zu einer Flankenschutzgefährdung werden können, allerdings muss die Möglichkeit einer Gefährdung innerhalb des aktiven Flankenschutzraumes ebenfalls beachtet werden. Diese tritt dann auf, wenn sich innerhalb des aktiven Flankenschutzraums unerkannte Fahrzeuge befinden. Die Schutzrate setzt sich demnach nicht allein aus den verfügbaren Begrenzungen des Flankenschutzraums zusammen, sondern wird auch durch die verfügbaren Informationen über die im aktiven Flankenschutzraum liegenden Gleissegmente beeinflusst. Diese Gleissegmente werden im Folgenden auch als **Flankenschutzsegmente** (**Flank Area Sections (FAS)**) bezeichnet (siehe auch Abb. 64 im Abschnitt „Zusammenfassung“).

Für die einzelnen Flankenschutzsegmente ist also jeweils die Wahrscheinlichkeit zu bestimmen, mit der sich ein unentdecktes Fahrzeug im Segment befinden könnte sowie mit der ein unentdecktes oder bekanntes aber nicht vollüberwachtes Fahrzeug auch tatsächlich zu einer Flankenfahrt werden könnte. Hierzu ist es, wie oben bereits beschrieben, sinnvoll, nacheinander vom Flankenschutz-Gefahrabschnitt ausgehend die Flankenschutzsegmente zu betrachten. Für jedes Segment ist zu prüfen, ob sich auf dem Segment bekanntermaßen ein Fahrzeug befindet. Falls dies nicht der Fall ist, muss die Wahrscheinlichkeit berechnet werden, mit der ein Fahrzeug auf dem Segment übersehen wurde.

Die Wahrscheinlichkeit, dass ein Fahrzeug übersehen wurde, kann durch einige Maßnahmen gesenkt werden. So könnte das Eingleisen bis auf bestimmte Bereiche mit infrastrukturseitiger Ortung verboten werden. Weiterhin könnte der Zugang von diesen Bereichen ins restliche Netz begrenzt und mit Detektionsmöglichkeiten ausgestattet werden, so dass Fahrzeuge, die von einem Eingleisungsbereich ins restliche Netz übergehen, sicher erkannt werden. Ist bekannt, dass erst vor Kurzem eine Fahrzeugbewegung das betrachtete Flankenschutzsegment vollständig passiert hat, kann ebenfalls von einer hohen Schutzrate ausgegangen werden, sofern in der verbleibenden Zeit nach dem Passieren bis zur Durchfahrt der Fahrzeugbewegung, für die die MA beantragt wurde, das Erreichen des Flankenschutzsegments durch ein unentdecktes Fahrzeug hinreichend gering ist.

Wird ein Fahrzeug gefunden, welches sich im aktiven Flankenschutzraum befindet, kann die Schutzrate von einer Reihe von Einflussgrößen beeinflusst werden, z. B.:

- Handelt es sich um ein vollüberwachtes und damit kontrollierbares Fahrzeug?
  Falls ja, kann das Fahrzeug mittels ETCS-Funktionalität zum Halten bleiben verpflichtet werden und als Flankenschutzgeber zum Schutz von weiteren Flankenschutzgefährdungen über das von ihm belegte Gleis agieren.

- Bewegt sich das Fahrzeug in Richtung des Flankenschutz-Gefahrabschnitts oder von diesem weg?
  Es kann davon ausgegangen werden, dass von einem Fahrzeug, welches sich vom Flankenschutz-Gefahrabschnitt wegbewegt, nur ein geringes Gefährdungsrisiko ausgeht.
- Falls das Fahrzeug in Richtung des Flankenschutz-Gefahrabschnitts fährt: Handelt es sich um ein Fahrzeug, welches zwar nicht vollüberwacht ist, aber dennoch beeinflusst werden kann, wenn es seine MA überschreitet, z. B. falls ein Class B-Zugsicherungssystem wie die PZB vorhanden ist?
  Da eine Fahrerlaubnis über eine aktive AS mit wenigen Ausnahmen nicht möglich ist, würde das Fahrzeug bei funktionsfähiger Beeinflussungsanlage vor Beginn der AS und damit des Flankenschutz-Gefahrabschnitts zum Halten gebracht werden.
- Falls das Fahrzeug entgegen der Richtung der Gefahrstelle fährt: Wie wahrscheinlich ist es, dass sich ein Wagen losreißen kann?
  In diesem Fall könnte theoretisch der getrennte Wagen eine Flankenfahrt auslösen, wenn die folgenden Bedingungen zutreffen:
  - Der Wagen wird nicht (ausreichend) selbsttätig gebremst.
    Die Strecke ist abschüssig in Richtung des Flankenschutz-Gefahrabschnitts oder es besteht ein anderer Impuls, der einen losgerissenen Wagen ins Rollen bringen kann. Ansonsten würde der Wagen wegen der Impulserhaltung in seine ursprüngliche Fahrtrichtung weiterrollen.
  - Der Zeitraum, den der Wagen benötigen würde, um den Flankenschutz-Gefahrabschnitt zu erreichen, ist ausreichend kurz. Je länger der Zeitraum, desto unwahrscheinlicher ist es, dass das zu schützende Fahrzeug die Stelle nicht bereits passiert hat oder das geeignete Gegenmaßnahmen eingeleitet werden konnten, um die Gefahr abzuwenden.

Ist eine unbekannte DA in einem oder mehreren der Flankenschutzsegmente, senkt das die Schutzrate deutlich, denn die Wahrscheinlichkeit ist groß, dass es sich um ein „vergessenes“ bzw. nicht identifiziertes Fahrzeug handeln könnte.

Speichern von aktiven Flankenschutzbeanspruchungen

Mit dem in den vorigen Abschnitten geschilderten Vorgehen kann die aktuelle Schutzrate bezogen auf eine mögliche Flankenschutzgefährdung berechnet werden. Diese Schutzrate fließt – sofern der Schwellwert für die Genehmigung der Prüfanfrage nicht bereits unterschritten ist, gemäß dem Konzept der Schutzrate aus Kapitel 8.3.1 in die Gesamt-Schutzrate ein, auf deren Basis die smartLogic entscheidet, ob die zugrundeliegende Anfrage des TMS genehmigt oder zurückgewiesen wird.

Die Auswahl an möglichen Flankenschutzelementen (FPOs) enthält auch FPOs, deren Verfügbarkeit von der aktuellen Betriebssituation abhängig ist (vgl. Tab. 45). Die Betriebssituation kann sich jedoch während des Zeitraums, für die die Schutzfunktion durch den Flankenschutz benötigt wird, verändern. Aus diesem Grund muss die smartLogic für diesen Zeitraum speichern, dass bestimmte Objekte eine Flankenschutzfunktion erfüllen. Hierfür kann das Konzept der Beanspruchungen genutzt werden (vgl. Kapitel 7.6.2), womit die betroffenen Objekte mit entsprechenden Flankenschutzbeanspruchungen versehen werden können.

Dabei stellt sich die Frage, auf welchen Objekten Beanspruchungen registriert werden sollen und in welchem Bereich (potenzieller Flankenschutzraum oder aktiver Flankenschutzraum) eine Registrierung erfolgen soll. Bestandteile des Flankenschutzraums und damit potenzielle Objekte, für die Beanspruchungen registriert werden können, sind

- die FPDs,
- die Flankenschutzsegmente und
- die Fahrzeuge.

Der Vermerk, dass ein FPD als Flankenschutzelement beansprucht wird, erscheint auf jeden Fall sinnvoll, damit bei einer geplanten Statusänderung die Notwendigkeit einer Überprüfung der Flankenschutz-Schutzrate eingeleitet werden kann. Hierzu wird eine „CTE Flank Occupation“ (vgl. Kapitel 7.6.2) eingerichtet, die sowohl beim Objekt des Flankenschutzraums (Flank Area) als auch beim FPD eingetragen wird (CTE steht dabei für Controlled Track Element, vgl. Kapitel 7.4.3). Im Beanspruchungsobjekt kann auch der Status (aktiv oder potenziell) gespeichert werden.

Auch für die Flankenschutzsegmente erscheint das Eintragen von entsprechenden Flankenschutzbeanspruchungen (Flank Occupation) sinnvoll zu sein, damit bei unerwarteten Ereignissen die Auswirkungen auf die Schutzrate der zu schützenden Fahrzeugbewegung bestimmt werden können. Analog zur CTE Flank Occupation kann eine Beanspruchung für das entsprechende Gleissegment als „Flank Occupation“ eingetragen werden. Ebenso muss die Flankenschutzfunktion eines Fahrzeugs gespeichert werden.

Neuberechnen der Flankenschutz-Schutzrate

Die Anforderung des Regelhandlungsgebots fordert, dass Fahrerlaubnisse und Verschlüsse mit Regelhandlungen zurückgenommen und geändert werden können sollen. Dies kann auf den Flankenschutz insofern übertragen werden, dass eine Änderung des Flankenschutz-Status bei geänderten Rahmenbedingungen zulässig sein soll. Konkret könnte z. B. für eine weitere Fahrt ein aktives Flankenschutzelement in einer anderen Lage benötigt werden, ein vollüberwachtes Fahrzeug, welches Flankenschutz geboten hat, diese Funktion aufgeben, eine Gleissperrung aufgelöst werden oder einem weiteren Fahrzeug die Einfahrt in den aktiven Flankenschutzraum erlaubt werden.

Bei der Bearbeitung einer Prüfanfrage muss die smartLogic daher auch prüfen, ob die Anfrage Änderungen am Status von Elementen mit Flankenschutzbeanspruchung vorsieht und falls ja, ob die gewünschte Änderung zu einer Änderung der Schutzrate für die ursprüngliche, durch den Flankenschutz geschützte Fahrzeugbewegung führen würde.

Um diese Überprüfung zu vereinfachen, ist es sinnvoll, in der Flankenschutzbeanspruchung den zu schützenden Flankenschutz-Gefahrabschnitt mitzuspeichern. Somit kann dieser Flankenschutz-Gefahrabschnitt schnell identifiziert werden und die smartLogic kann für den entsprechenden Flankenschutz-Gefahrabschnitt eine Neuberechnung der Flankenschutz-Schutzrate unter Berücksichtigung der beantragten Änderung nach den gleichen Regeln wie für die ursprüngliche Berechnung der Schutzrate durchführen.

Ergibt diese Berechnung, dass ein Einfluss auf die Flankenschutz-Schutzrate besteht, ist zu überprüfen, ob durch die beantragte Änderung die Gesamt-Schutzrate der ursprünglich zu schützenden Fahrt soweit gesenkt würde, dass die ursprünglich zu schützende Fahrt nicht mehr hinreichend geschützt wäre. In diesem Fall wäre die aktuelle Anfrage abzulehnen. Ist dies nicht der Fall, kann für die neue Anfrage deren Schutzrate vollständig ermittelt werden. Wird die neue Anfrage genehmigt, sind zuvor die Flankenschutzbeanspruchungen für die ursprüngliche Fahrzeugbewegung zu aktualisieren.

Zusammenfassung

Da nicht von vorneherein angenommen werden kann, dass nur noch vollüberwachte Fahrzeuge im Bereich der smartLogic verkehren, ist eine Betrachtung des Risikos von Flankenfahrten auch im Falle der smartLogic sinnvoll. Das Risiko wird abhängig von der aktuellen Betriebssituation als Flankenschutz-Schutzrate bestimmt und wirkt sich auf die Gesamt-Schutzrate der dem Prüfprozess zugrundeliegenden Prüfanfrage aus.

Das Gesamtrisiko einer Flankenfahrt für eine betrachtete Fahrzeugbewegung im Gleisabschnitt einer zu prüfenden Fahrerlaubnis setzt sich aus den Risiken für eine Flankenfahrt für jeden Flankenschutz-Gefahrabschnitt unter Berücksichtigung der jeweiligen Erreichenswahrscheinlichkeit der Flankenschutz-Gefahrstellen zusammen, die innerhalb der Gültigkeit der Fahrerlaubnis von der Fahrzeugbewegung passiert werden könnten. Zur Bestimmung des Risikos einer Flankenfahrt für die einzelnen Flankenschutz-Gefahrabschnitte wird zunächst ein potenzieller Flankenschutzraum als Suchraum für mögliche Flankenschutzgefährdungen bestimmt. Innerhalb dieses potenziellen Flankenschutzraums kann anhand des Status möglicher begrenzender Flankenschutzobjekte (FPOs) ein aktiver Flankenschutzraum bestimmt werden. Das Risiko einer Flankenfahrt hängt dann von der Art der begrenzenden FPOs und der Wahrscheinlichkeit einer Flankenfahrt durch eine Gefährdung innerhalb des aktiven Flankenschutzraums ab.

Um den Flankenschutzraum überwachen zu können, werden Flankenschutzbeanspruchungen auf den aktiven Flankenschutzraum begrenzenden Elementen sowie den im Flankenschutzraum liegenden Gleissegmenten ergänzt. Bei jeder Statusänderung innerhalb des aktiven Flankenschutzraums wird die Flankenschutz-Schutzrate neu berechnet.

Abb. 64 dient zur Veranschaulichung der wichtigsten in diesem Kapitel eingeführten Begriffe zum Thema Flankenschutz.

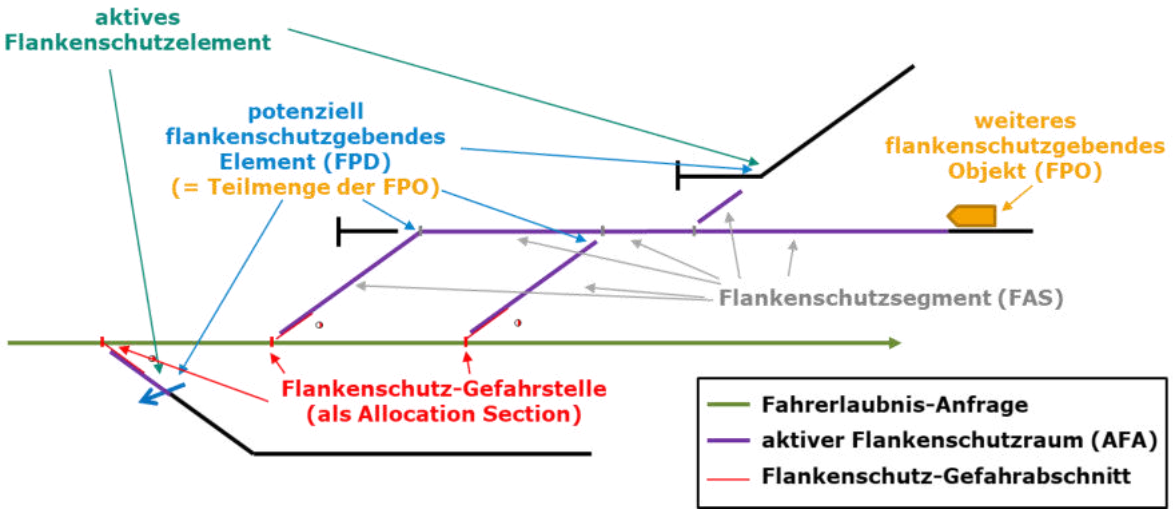


Abb. 64: Begriffe zum Thema Flankenschutz
[Eigene Darstellung]

8.3.5 Fahrzeugbewegungen mit unterschiedlichem Sicherheitsniveau / Unterscheidung zwischen Zug- und Rangierfahrten

In der klassischen Eisenbahnsicherungstechnik werden Fahrzeugbewegungen auf der Eisenbahninfrastruktur in Zug- und Rangierfahrten unterteilt, für die ein unterschiedliches Sicherheitsniveau gilt. Dieses Unterkapitel soll sich kurz mit der Notwendigkeit einer solchen Unterscheidung in Hinblick auf die Modellierung der smartLogic beschäftigen.

Die Unterscheidung von Zug- und Rangierfahrten wird vor allem dadurch begründet, dass bei Rangierfahrten das Gefährdungspotenzial niedriger ist, da in der Regel keine Passagiere befördert werden und verschiedene einschränkende Rahmenbedingungen wie eine niedrige Maximalgeschwindigkeit gelten. Aufgrund des Ansatzes der „Grünen Wiese“ in dieser Arbeit (vgl. Kapitel 3.6.2) soll die Unterteilung zwischen Zug- und Rangierfahrten nicht unreflektiert übernommen werden, sondern müsste sich aus den bereits gewonnen Erkenntnissen herleiten.

Eine Unterscheidung der generischen Prüfregeln der smartLogic für die Bewertung der Zulassung einer Fahrzeugbewegung für verschiedene notwendige Sicherheitsniveaus entspricht dem Sinne der Anforderung, wonach die Anfrage nur abgelehnt werden darf, wenn die *Kernanforderung der sicheren Logik unter Berücksichtigung aller verfügbaren Informationen tatsächlich nicht erfüllt ist* (vgl. Kapitel 8.2.1). Allerdings ist auch die globale Anforderung der *schlanken Logik* zu beachten. Deshalb sollte zunächst geprüft werden, ob es Ansätze gibt, mit denen die verschiedenen notwendigen Sicherheitsniveaus mit der bestehenden Logik abgebildet werden könnten. Dabei wurden folgende Ansätze identifiziert:

1. Im generischen Konzept der Schutzrate ist bereits abgebildet, wie hoch das Sicherheitsniveau der zu bewertenden Anfrage ist (vgl. Kapitel 8.3.1). Dabei können bei der Prüfung der einzelnen Prüfbedingungen auch risikoreduzierende Eigenschaften der Fahrzeugbewegung wie ein Geschwindigkeitsprofil mit niedrigen Geschwindigkeiten oder die Art der Fahrzeugbewegung (z. B. Fahrzeugbewegungen ohne Fahrgäste) als positiver Einfluss in die Berechnung der Schutzrate für die jeweilige Prüfbedingung eingehen und somit z. B. eine nicht optimale Flankenschutz-Schutzrate ausgleichen.
2. Es könnten unterschiedliche Schwellwerte, welche die Schutzrate zur Genehmigung der Anfrage überschreiten muss, für Fahrerlaubnisanfragen mit unterschiedlichem Sicherheitsniveau ermittelt werden.

Beide Ansätze wären mit der bestehenden Logik umsetzbar. Im Falle des zweiten Ansatzes müsste allerdings ein Mechanismus gefunden werden, der mit hinreichender Sicherheit die korrekte Zuordnung einer Fahrzeugbewegung zum erforderlichen Sicherheitsniveau gewährleistet. Ein solcher Mechanismus kann aus Gründen der verfügbaren Bearbeitungszeit nicht in dieser Arbeit erarbeitet werden.

Eine Notwendigkeit für über die in diesem Unterkapitel geschilderten Ansätze hinausgehende zusätzliche Regeln für Fahrten mit unterschiedlichem Sicherheitsniveau wurde nicht identifiziert.

8.3.6 Betrieb bei Abweichungen vom Regelbetrieb (Rückfallebenen)

In der Realität kommt es aufgrund verschiedenster Ursachen zu Einschränkungen der Verfügbarkeit von Hard- und Softwarekomponenten der Eisenbahn. Eine solche Einschränkung, z. B. der Ausfall eines Elements der Gleisfreimeldeanlage (wie ein Achszähler) oder eines Signals, führt in heutigen Stellwerken häufig zu einer manuellen Rückfallebene. Die **Rückfallebene** definiert Kompensationsmaßnahmen für die Schutzfunktion der Technik, die durch die Einschränkung beeinträchtigt wird. Da manuelle Kompensationsmaßnahmen aus vielfältigen, z. T. langwierigen Schritten bestehen, um ein akzeptables Maß an Sicherheit zu gewährleisten, bedingen sie oft eine starke Verringerung der Kapazität. Weiterhin bedeuten manuelle Rückfallebenen durch die höhere Fehlerwahrscheinlichkeit menschlicher Handlungen im Vergleich zur Technik auch ein geringeres Maß an Sicherheit.

Aus den oben genannten Gründen wurde eine höhere Robustheit im Sinne einer höheren Nutzbarkeit (auch) der Systemkomponente Sicherungslogik bei Abweichungen vom Regelbetrieb als eine der zentralen Zieldimensionen einer smarten Sicherungslogik definiert (vgl. Kapitel 3.2). Eine vollständige Betrachtung des Themenbereichs Umgang mit Abweichungen vom Regelbetrieb/Rückfallebenen ist wegen des begrenzten Bearbeitungsumfangs der Arbeit (vgl. Kapitel 3.3 und 3.6.1) hier allerdings nicht möglich und bleibt eine Aufgabe für zukünftige Forschungsarbeiten.

Aufgrund der oben erwähnten großen Bedeutung der Abweichungen vom Regelbetrieb für die Nutzenpotenziale der neuen Sicherungslogik, erscheint es dem Autor dieser Arbeit dennoch sinnvoll, mögliche Implikationen auf die Gestaltung des generischen Regelsets, welches die Grundlogik der smartLogic bildet, durch die spätere Erweiterung um Rückfallebenen bereits bei der Erstellung der Grundlogik mitzudenken. Deshalb wird in diesem Unterkapitel ein grundsätzliches Konzept für den Umgang mit Abweichungen vom Regelbetrieb hergeleitet.

Ausgangspunkt für die Erarbeitung sind spezielle Anforderungen an das Konzept, die sich aus den globalen Anforderungen sowie den spezifischen Anforderungen an dieses Hauptkapitel herleiten lassen (erster Abschnitt). Am einfachsten ist es, wenn Abweichungen vom Regelbetrieb mit dem regulären Regelset der Grundlogik kompensiert werden können (zweiter Abschnitt). Eine solche Kompensation ist jedoch nicht immer ohne den Verlust von Kapazität möglich. Deshalb wird anschließend gemäß den identifizierten Anforderungen schrittweise ein Konzept für die generische Integration von Rückfallebenen in die smartLogic entworfen (Abschnitte drei bis fünf) und an zwei unterschiedlichen Beispielen veranschaulicht (Abschnitt sechs und sieben). Im letzten Abschnitt folgt eine kurze Zusammenfassung.

Anforderungen

Um ein Konzept für die Berücksichtigung von Abweichungen vom Regelbetrieb in der smartLogic zu erarbeiten, muss zunächst Klarheit über die speziellen Anforderungen an ein solches Konzept geschaffen werden. Alle speziellen Anforderungen ergeben sich aus den globalen Anforderungen aus Kapitel 3.5, die in Kapitel 8.2.1 in Hinblick auf ihre Anwendung für die Verhaltensmodellierung in diesem Hauptkapitel detailliert wurden.

Wie oben erwähnt, ergibt sich die Notwendigkeit, ein Konzept für Abweichungen vom Regelbetrieb vorzusehen, aus den Zielen der smartLogic, die zur Zieldimension der „Robustheit“ zusammengefasst wurden (vgl. Kapitel 3.2). Hinter dem Begriff „Robustheit“ verbirgt sich das Ziel einer hohen Verfügbarkeit der Sicherungslogik, um die Belastung von Abweichungen vom Regelbetrieb auf die Kapazität und Pünktlichkeit zu minimieren. Daher sind insbesondere die Anforderungen zur Zieldimension der „Robustheit“ für das Konzept zu Abweichungen vom Regelbetrieb relevant.

Tab. 46 zeigt die in Kapitel 8.2.1 identifizierten Anforderungen zur Zieldimension „Robustheit“ und interpretiert die Bedeutung dieser Anforderungen für das Themengebiet des Umgangs mit Abweichungen vom Regelbetrieb. Die anderen in Kapitel 8.2.1 genannten Anforderungen sind in ihrer allgemeinen Form ebenfalls zu beachten (insbesondere die Kernanforderung der sicheren Logik und die Anforderung der schlanken Logik), bedingen jedoch keine speziellen Anforderungen für dieses Konzept und werden daher zur besseren Übersichtlichkeit in der Tabelle nicht erneut aufgeführt.

Tab. 46: Anforderungen an den Umgang mit Abweichungen vom Regelbetrieb (Modellierung der Rückfallebenen)

globale Anforderung	spezifische Anforderung für die Verhaltensmodellierung	Bedeutung für dieses Unterkapitel
Rückfallebenenintegration	Abbruch des Prozesses nur, wenn die Kernanforderung unter Berücksichtigung aller verfügbaren	in möglichst vielen Betriebssituationen soll die smartLogic

	Informationen tatsächlich nicht erfüllt ist; Möglichkeit der Definition milderer Prüfkriterien in Verbindung mit Einschränkungen für die Fahrerlaubnis	Fahrzeugbewegungen zulassen können; damit dies auch funktioniert, wenn einzelne Prüfbedingungen nicht voll erfüllt werden können, müssen Alternativbedingungen (Rückfallebenen) definiert werden können, unter denen dennoch eine ausreichende Schutzrate erreicht werden kann
Regelhandlungsgebot	Prozesse für reguläre Rücknahme von MAs und Verschlüssen vorsehen (bereits im Funktionsumfang berücksichtigt)	das TMS muss die Möglichkeit haben, die Anfragen an die smartLogic möglichst dynamisch zu stellen, damit die beim vorigen Punkt genannten Alternativbedingungen auch eingehalten werden können
Freiraum für Fahrzeuge	Vorgaben so wenig restriktiv und passgenau wie möglich gestalten	*siehe bei Regelhandlungsgebot*
Resilienz	Abbruch des Prozesses nur, wenn die Kernanforderung der sicheren Logik unter Berücksichtigung aller verfügbaren Informationen tatsächlich nicht erfüllt ist	*siehe vorherige Punkte*

Die Analyse in Tab. 46 zeigt, dass sich aus den globalen Anforderungen und den für die Verhaltensmodellierung spezifischen Anforderungen im Wesentlichen zwei spezielle Anforderungen an den Umgang mit Abweichungen vom Regelbetrieb herleiten lassen. Zum einen sollte die Sicherungslogik möglichst viele Abweichungen mit ihrem gewöhnlichen generischen Regelset abdecken können, z. B. geänderte Fahrerlaubnisse im Verspätungsfall (siehe „MP Change Request“ in Kapitel 8.5.4). Zum anderen sollte sie für den Fall, dass eine Abweichung mit dem gewöhnlichen Regelset nicht kompensiert werden kann, mit einer generischen Funktion die Integration von Rückfallebenen in die Logik ermöglichen. Die Rückfallebenen haben dabei zum Ziel, dass sie Regeln vorgeben, nach denen auch bei eingeschränkter Verfügbarkeit von Systemkomponenten eine ausreichende Schutzrate (vgl. Kapitel 8.3.1) wann immer möglich erreicht werden kann.

Anwendbarkeit und Grenzen des Regelhandlungsgebot

Wie im vorigen Abschnitt bereits erwähnt, ist es im Sinne der globalen Anforderung der schlanken Logik ideal, wenn für den Umgang mit Abweichungen vom Regelbetrieb keine speziellen Regelungen erforderlich sind, weil die Folgen der Abweichung durch das normale Regelset bewältigt werden können (Regelhandlungsgebot).

Das normale Regelset kann dann weitergenutzt werden, wenn trotz der Abweichung ohne die Definition zusätzlicher Regeln eine ausreichende Schutzrate für die betroffenen Prüfbedingungen und eine ausreichende Gesamt-Schutzrate erreicht werden können. Hierzu muss das TMS genügend Freiraum von der Sicherungslogik geboten bekommen, um präzise Anfragen stellen (z. B. durch die Möglichkeit, beliebige Punkte auf der Gleistopologie als Zielpunkte einer Fahrerlaubnisanfrage setzen zu können) und auf neue Betriebssituationen reagieren zu können (z. B. durch einen einfachen integrierten Kürzungsmechanismus für bereits ausgestellte Fahrerlaubnisse). Beides wurde bereits bei der Entwicklung der smartLogic beachtet.

Allerdings lässt sich nicht allen Abweichungen vom Regelbetrieb mit dieser Lösung ohne nennenswerte Kapazitätseinbußen und bedeutende Verspätungen begegnen. Beispielsweise müsste bei einer Bahnübergangsstörung eine Fahrerlaubnisanfrage über diesen BÜ abgelehnt werden, auch wenn er unter bestimmten Sicherheitsvorkehrungen noch befahrbar wäre. Das könnte zum Beispiel der Fall sein, wenn der BÜ zwar nicht freigemeldet werden kann, die Schranken aber dennoch geschlossen sind. Ein komplett manuelles Vorgehen könnte das Problem zwar lösen, wäre aber zeitaufwendig und fehleranfällig und entspricht daher nicht den definierten Anforderungen.

Aus diesem Grund ist ein Konzept für eine Integration von Rückfallebenen in die smartLogic zu finden, um mit Abweichungen, die nicht ohne nennenswerte Kapazitätseinbußen oder Verspätungen durch Regelhandlungen im Rahmen des normalen Regelsets abgebildet werden können, umgehen zu können. Ein solches Konzept wird in den folgenden Abschnitten beschrieben.

Definition von Sicherheitslevels und Rückfallebenen

Um Rückfallebenen in die Logik integrieren zu können, ist zunächst ein Überblick hilfreich, welche Rückfallebenen zu berücksichtigen sind, weil sie zu einer Erhöhung der Robustheit der Sicherungslogik beim Reagieren auf Abweichungen vom Regelbetrieb führen. Gemäß der in der Einleitung zu diesem Unterkapitel erwähnten Definition von Rückfallebenen und den Überlegungen aus den vorigen Abschnitten ist eine Rückfallebene dann sinnvoll, wenn sie die Behinderung des Betriebs durch die Abweichung vom Regelbetrieb im Vergleich zur Anwendung der Grundlogik verringert. Oder anders ausgedrückt, eine Rückfallebene ist sinnvoll, wenn Prüfanfragen, die in Folge der Grundlogik abgewiesen werden müssten, weil die Abweichung vom Regelbetrieb die Schutzrate unter den Schwellwert gesenkt hat (vgl. Kapitel 8.3.1), durch die Integration einer Rückfallebene doch genehmigt werden können.

Prinzipiell kann davon ausgegangen werden, dass der Ausfall einer Systemkomponente bzw. eine anderweitige Abweichung vom Regelbetrieb, wie ein blockiertes Fahrzeug auf dem Gleis (z. B. in Folge von Personen im Gleisbereich), in vielen Fällen verschiedene Schweregrade bezüglich der Auswirkungen auf die Schutzrate haben kann. Diese Schweregrade werden im Folgenden als **Sicherheitslevels** bezeichnet. Um den Betrieb geringstmöglichen zu beeinträchtigen, sollten für die verschiedenen Sicherheitslevels abgestufte Rückfallebenen existieren. Die Rückfallebene sollte also jeweils den Betrieb nur soweit einschränken, dass die erforderliche Schutzrate gerade wieder erreicht wird.

Die Anzahl der Sicherheitslevels ist dabei durch die zur Verfügung stehenden Informationen begrenzt, die häufig in diskreter Form vorliegen, beispielsweise als Systemzustände einer externen Systemkomponente. Bei einer Weiche könnten z. B. folgende Sicherheitslevels in Betracht kommen:

- die Weiche kann nicht umgestellt werden, hat aber eine überwachte Endlage
- die Weiche hat zwar eine gemeldete Endlage, diese ist aber nicht überwacht
- die Weiche hat keine gemeldete Endlage
- der Weichenstatus ist nicht bekannt / es kann kein Kontakt mit der Weiche aufgenommen werden

Für andere Prüfbedingungen, wie z. B. auf Vorlage der Zustimmung von zustimmungspflichten Stakeholdern wie Bahnübergängen (vgl. Kapitel 8.3.3), könnten die Sicherheitslevels der Weichen nicht übernommen werden. Stattdessen existieren komplett andere Sicherheitslevels (z. B. gesichert und freigemeldet; mit Schranke und Rotlicht gesichert, aber nicht freigemeldet; mit Rotlicht gesichert, aber nicht mit Schranke; ungesichert; etc.). Daher können die Sicherheitslevels und die dazugehörigen

Rückfallebenen nicht pauschal festgelegt werden, sondern es muss eine Möglichkeit geschaffen werden, sie für einzelne Anwendungsfälle festzulegen.

Möglichkeiten zur Festlegung und Übermittlung der Rückfallebenen

Wie im vorigen Abschnitt bereits festgestellt wurde, können Sicherheitslevels und dazugehörige Rückfallebenen nicht allgemeingültig festgelegt werden, sondern unterscheiden sich für verschiedene Prüfbedingungen. Eine der wichtigsten Anforderungen an die smartLogic ist jedoch, dass sie generisch formuliert und zukunftsfest sein soll (vgl. Kapitel 3.5 und 8.2.1) Es ist daher ein Weg zu finden, wie trotz dieser Unterschiedlichkeit der Prüfbedingungen eine generische Beschreibung der Sicherheitslevels und Rückfallebenen erfolgen kann. In den beiden folgenden Unterabschnitten sind zwei mögliche Umsetzungsideen beschrieben, die auf den bisherigen Konzepten der smartLogic aufbauen:

1. Definition zusätzlicher Prüfbedingungen für die Sicherheitslevels und Rückfallebenen (erster Unterabschnitt)
2. Berücksichtigung der Sicherheitslevels und Rückfallebenen über die Formel zur Berechnung der Schutzrate (zweiter Unterabschnitt)

Im dritten Unterabschnitt erfolgt eine Bewertung der beiden Varianten.

Definition zusätzlicher Prüfbedingungen für die Sicherheitslevels und Rückfallebenen

Für jedes Sicherheitslevel wird eine eigene Prüfbedingung ergänzt. Diese Prüfbedingung enthält die **Rückfallebenenbedingungen**, also die erforderlichen Parameter (i. d. R. von der Fahrzeugbewegung zu beachtende Einschränkungen, wie z. B. niedrigere Geschwindigkeit oder bestimmter ETCS-Modus), welche die beantragte MA zusätzlich enthalten muss, damit eine ausreichend hohe Schutzrate erreicht wird, verknüpft mit einer Abhängigkeit vom Umstand, der die Rückfallebene ausgelöst hat.

Es würden also im Fall des im vorigen Abschnitt beschriebenen Beispiels mit der Weiche vier zusätzliche Prüfbedingungen formuliert werden, da vier abgestufte Sicherheitslevels identifiziert wurden. Die Prüfbedingungen würden jeweils für eine Rückfallebene stehen und die zu überprüfenden Parameter, die in der Prüfanfrage enthalten sein müssen, als Rückfallebenenbedingungen festlegen, mit denen der Betrieb trotz des eingeschränkten Sicherheitslevels noch weitergeführt werden könnte. Es wäre dann ausreichend, wenn eine der neu entstandenen Prüfbedingungen oder die ursprüngliche Prüfbedingung (im Beispiel, ob die Weiche den richtigen Status hat) erfüllt ist. Um diesen Sachverhalt zu modellieren, könnten die neuen Prüfbedingungen, die aus derselben ursprünglichen Prüfbedingung entstanden sind, in einer Gruppe gruppiert werden und mit einer logischen „Oder“-Bedingung verknüpft werden, so dass es insgesamt für die Genehmigung der Prüfanfrage ausreichend wäre, wenn eine der Prüfbedingungen erfüllt ist.

Gemäß dem in Kapitel 8.3.1 eingeführten Konzept der Schutzrate wären bei der beschriebenen Vorgehensweise allerdings alle Rückfallebenen gleichwertig, denn jeder Prüfbedingung würde eine Basis-Schutzrate von ‚1‘ zugewiesen, wenn sie vollständig erfüllt ist, also im Falle der Rückfallebene, wenn alle Rückfallebenenbedingungen erfüllt sind. Es wäre dann aufgrund der globalen Anforderung der schlanken Logik Aufgabe des TMS, die Prüfanfrage so zu stellen, dass die Bedingungen von mindestens einer der Rückfallebenen erfüllt sind.

Da in diesem Modell alle Rückfallebenen prinzipiell als sicher angenommen werden, könnte das TMS aus betrieblichen Gründen eine Entscheidung für eine der Rückfallebenen treffen. Strenggenommen

würde es sich bei dieser Vorgehensweise allerdings nicht mehr um Rückfallebenen handeln, sondern um gleichberechtigte Entscheidungsvarianten mit gleicher Schutzrate.

Theoretisch könnten den einzelnen Rückfallebenen auch unterschiedlich hohe Schutzraten zugeordnet werden, indem innerhalb der Gruppe der Prüfbedingungen zusätzliche Gewichtungsfaktoren eingeführt werden würden. Dann könnte das TMS die Höhe der Schutzrate bei seiner Entscheidung mitberücksichtigen.

Berücksichtigung der Sicherheitslevels und Rückfallebenen über die Formel zur Berechnung der Schutzrate

Die Möglichkeit der Berücksichtigung negativer und positiver Einflüsse bei der Bestimmung der Schutzrate für die einzelnen Prüfbedingungen (vgl. Kapitel 8.3.1, Abschnitt „Bestimmung des tatsächlichen Risikos einer Prüfanfrage“) wird zur generischen Angabe von Sicherheitslevels und Rückfallebenen in der smartLogic genutzt. Der Einfluss eines Sicherheitslevels bzw. der Rückfallebenenparameter auf die Schutzrate einer Prüfbedingung könnte dabei als Funktion in Abhängigkeit bestimmter Parameter definiert werden. Das Ergebnis der Funktion würde dann einen Faktor bei der Berechnung der Schutzrate bilden.

Eine solche **Rückfallebenenfunktion (REF)** könnte je nach Einfluss entweder diskret (wie bei der Weiche oben geschildert) oder stetig sein (z. B. bei der Prüfbedingung zum Ausschluss einer Gefährdung starker Seitenwinde). Bei Vorliegen des höchsten Sicherheitslevels (Regelbetrieb) entspricht die Schutzrate für (den Einfluss auf) die Prüfbedingung gemäß Kapitel 8.3.1 der Basis-Schutzrate von 1 (100 %), womit kein Einfluss auf die Gesamt-Schutzrate besteht. Bei niedrigeren Sicherheitslevels könnte die Funktion für jedes Sicherheitslevel der jeweiligen Prüfbedingung eine entsprechend niedrigere Schutzrate für diese Prüfbedingung ergeben, die dann in die Berechnung der Gesamt-Schutzrate der Prüfanfrage einginge (vgl. Abschnitt „Verknüpfung der Schutzraten der Prüfbedingungen“ in Kapitel 8.3.1).

Die Funktion zur Abbildung der Rückfallebene könnte sowohl den negativen Sicherheitseinfluss berücksichtigen, der die Rückfallebene nötig macht, als auch den positiven Einfluss durch die Kompensationsmaßnahmen in Form der Rückfallebenenbedingungen. In der Funktion könnte der Beitrag der einzelnen Kompensationsmaßnahmen in Bezug auf die Berechnung der Schutzrate festgelegt werden, da dieser unterschiedlich hoch sein kann. Zum Beispiel kann eine Reduzierung der Geschwindigkeit je nach betrachteter Prüfbedingung unterschiedliche Einflüsse auf die Erhöhung der Schutzrate haben kann (z. B. für den Fall, dass eine nicht verschlossene Weiche befahren werden soll im Vergleich zum Fall, in dem starke Seitenwinde kompensiert werden sollen).

Neben dynamischen kompensierenden Einflüssen wie einer niedrigeren Geschwindigkeit, die einen negativen Einfluss auf die Schutzrate ausgleichen kann, könnten mittels Indikatorvariablen[55] bei Bedarf auch feste Rückfallebenen über die Rückfallebenenfunktion vorgegeben werden, die zum Beispiel von einem Zustand eines exterens Systems abhängig sind und abhängig von diesem Zustand eine feste eingeschränkte Schutzrate ergeben, wenn alle zur Rückfallebene gehörenden Bedingungen erfüllt sind.

[55] Indikatorvariablen sind Faktoren in der Funktion, die bei Vorliegen definierter Bedingungen (z. B. ein bestimmter Status eines externen Systems) den Wert 1 annehmen und sonst den Wert 0. Damit fungieren sie als Schalter, der bei Vorliegen der Bedingungen den nachfolgenden Funktionsteil aktiviert (multipliziert mit 1) oder deaktiviert (multipliziert mit 0).

Bewertung der Varianten

Der erste geschilderte Umsetzungsweg ermöglicht zwar über das Konzept der Prüfbedingungen eine generische Modellierung der jeweiligen für den sicheren Betrieb in Rückfallebenen erforderlichen Einschränkungen der Fahrerlaubnis (wie eine Geschwindigkeitsreduzierung), er birgt allerdings auch einige Probleme. So wurden die Prüfbedingungen ursprünglich durch die Funktionsanalyse bestimmt und hier mit den Überlegungen zur Rückfallebene vermischt. Dieses Vorgehen macht die Logik intransparenter. Weiterhin könnten die Rückfallebenen zwar mittels einer generischen Beschreibungssprache (Datenmodell) modelliert werden (vgl. Kapitel 7), diese Modellierung müsste aber dennoch für jede Rückfallebene einzeln bei der Logikentwicklung erfolgen. Dieser Umstand widerspricht wiederum der Anforderung der generischen Logik.

Mit der generisch aufgebauten, aber individuell parametrisierten Rückfallebenenfunktion können bei der zweiten Umsetzungsidee dagegen neben festen Rückfallebenen auch dynamische Rückfallebenen ermöglicht werden und dem TMS somit ein Spielraum gelassen werden, um die sinnvollsten Kompensationsmaßnahmen zu bestimmen und entsprechend in die MA aufzunehmen. Aus diesem Grund wird die zweite Lösung für das weitere Vorgehen bevorzugt und im nachfolgenden Abschnitt näher beschrieben.

Zusammensetzung der Rückfallebenenfunktion

In diesem Abschnitt soll die Zusammensetzung der Rückfallebenenfunktion hergeleitet werden. Als Ausgangsbasis können die Parameter dienen, die durch die Rückfallebenenfunktion beschrieben werden sollen. Hierfür werden zunächst die negativen Parameter der Rückfallebenenfunktion zur Beschreibung der Sicherheitslevels thematisiert (erster Unterabschnitt) und anschließend die positiven Parameter zur Beschreibung der Kompensationsmaßnahmen bzw. Rückfallebenenbedingungen identifiziert (vierter Unterabschnitt). Darauf aufbauend ist zu klären, woher die Parameter der Rückfallebenenfunktion und die Werte der Parameter kommen (dritter Unterabschnitt). Abschließend muss noch geklärt werden, ob die Rückfallebenenfunktion einer bestimmten Form folgen muss (vierter Unterabschnitt).

Funktionsparameter zur Abbildung der Sicherheitslevels (negativer Bestandteil der Rückfallebenenfunktion)

Gänge Beispiele für Parameter, die bei Abweichungen vom Regelbetrieb das Sicherheitslevel und damit die Schutzrate verringern, können einer der folgenden Gruppen zugeordnet werden:

- das Vorliegen eines bestimmten Systemzustands eines externen Systems (z. B. als Zeichen einer Funktionsstörung)
- das Vorliegen oder Fehlen eines definierten Sensorwertes
- die Beanspruchung eines Detektionsabschnitts (vgl. Kapitel 7.3.5)
- das Vorliegen eines bestimmten Fahrzeugmerkmals, z. B. das Fehlen eines Zugspitzen-signals
- das Vorliegen einer Danger Area (DA)
- das Überschreiten eines definierten Schwellwerts durch einen Sensor, das Fahrzeug oder eine interne Variable, wie z. B. die Außentemperatur

Die obige Auflistung stützt sich auf die bisherigen Erkenntnisse der Arbeit und hat nicht den Anspruch vollständig zu sein, da dieses Kapitel nicht den Anspruch erhebt, das Thema der Abweichungen vom Regelbetrieb vollständig zu bearbeiten. Stattdessen soll die Auflistung dazu beigetragen, dass

nachfolgend zielgerichtet verschiedene Möglichkeiten zur Formulierung von Rückfallebenenfunktion identifiziert werden können.

Die ersten fünf Fälle der Liste können z. B. über gewichtete Indikatorvariablen abgebildet werden (in der untenstehenden Beispielformel ‚x'), die jeweils den Wert ‚1' annehmen, wenn die zugeordnete Bedingung vorliegt (z. B. wenn das Zugspitzensignal fehlt). Die Gewichtung (in der Beispielformel ‚a') bestimmt, wie stark in diesem Fall die Schutzrate beeinträchtigt wird. Der Einfluss wird von der Basis-Schutzrate abgezogen.

$$Einfluss\ eines\ Parameters\ auf\ die\ Schutzrate = 1 - ax$$

Die einzelnen Parameter können analog zu Kapitel 8.3.1, Abschnitt „Bestimmung des tatsächlichen Risikos einer Prüfanfrage" als Produkt verknüpft werden, wenn sie voneinander unabhängig sind. Die Summe der Gewichte aller nicht erfüllten Prüfbedingungen ergibt dann die Verringerung der Schutzrate. Falls Parameter nicht unabhängig voneinander sind, kann der wechselseitige Einfluss ebenfalls in der Rückfallebenenfunktion abgebildet werden.

Beim letzten Punkt der obigen Liste handelt es sich um einen Parameter, der nicht nur wahr oder falsch sein kann. Er kann zum Beispiel als lineare Funktion angegeben werden, aber auch als Polynom höheren Grades oder als nicht differenzierbare Funktion mit Stützpunkten.

Funktionsparameter zur Abbildung der Kompensationsmaßnahmen (positiver Bestandteil der Rückfallebenenfunktion)

Gemäß dem im vorigen Abschnitt beschriebenen Konzept stehen den negativen Einflüssen auf die Schutzrate die positiven Einflüsse aufgrund von Kompensationsmaßnahmen für die negativen Einflüsse (verringerte Schutzlevels) als positiver Bestandteil der Rückfallebenenfunktion gegenüber.

Um mögliche Kompensationsmaßnahmen und damit Parameter für den positiven Bestandteil der Rückfallebenenfunktion zu identifizieren, gibt es viele Methoden aus dem Bereich der Problemlösungsfindung. Eine vertiefte Methodendiskussion soll an dieser Stelle nicht erfolgen, da, wie oben bereits geschildert, hier keine ausführliche Betrachtung des Rückfallebenen-Themengebiets erfolgen kann. Eine einfache und verbreitete Möglichkeit ist eine Analyse mittels der W-Fragen (vgl. Kapitel 3.4.3), die verschiedene Lösungsdimensionen für Kompensationsmaßnahmen aufzeigen, wie räumliche und zeitliche Kompensationsmaßnahmen. Die Frage lautet dabei immer (ggf. in leicht abgewandelter Form) „[Fragewort] wird die Stelle mit verminderter Schutzrate passiert?". Es sind allerdings nicht alle W-Fragen von Bedeutung.

Die Erkenntnisse aus der Analyse der W-Fragen sind in Tab. 47 dargestellt. Nicht alle so gefundenen Kompensationsmaßnahmen für eine Abweichung vom Regelbetrieb benötigen überhaupt eine Rückfallebene, da nicht alle Kompensationsmaßnahmen dazu führen, dass die Schutzrate überhaupt reduziert werden würde, z. B. wenn zur Vermeidung einer Störung vom TMS eine alternative Route beantragt wird. Es ist daher jeweils angegeben, ob die Kompensationsmöglichkeit überhaupt eine Rückfallebene benötigt oder bereits über das normale Regelset umgesetzt werden kann.

Tab. 47: Kompensationsmaßnahmen bei Abweichungen vom Regelbetrieb

Problemlösungsdimension	Kompensationsmaßnahmen für ausgefallene Systemkomponente	normales Regelset / Rückfallebene
räumlich (Wo?)	anderer Fahrweg (auch wenn Fahrerlaubnis bereits erfolgt ist)	normales Regelset

	Zurücksetzen, so dass ein neuer Fahrweg gewählt werden kann (kann mit MA erfolgen; von der ETCS-Funktion „Reversing“ zu unterscheiden, mit der Fahrzeugbewegungen im Notfall automatisch zurückgesetzt werden können)	normales Regelset
	automatisches Zurücksetzen (mittels der ETCS-Funktion „Reversing“	Rückfallebene
zeitlich (Wann?)	Warten (bis Verfügbarkeitseinschränkung behoben ist)	normales Regelset
Einschränkung der Fahrweise (Wie?)	Geschwindigkeit reduzieren	Rückfallebene
	zusätzliche Warnsignale (z. B. Pfeifen oder Läuten) vorschreiben	Rückfallebene
Verlagerung der Verantwortung (Wer/Von wem?)	Fahrmodus wechseln (z. B. auf Sicht)	Rückfallebene
	Auswertung zusätzlicher Sensoren	ggf. Rückfallebene
	Auswertungen von Meldungen vom Personal	Rückfallebene
	Bestätigung vom Fahrpersonal für Übernahme der Sicherheitsverantwortung anfordern	Rückfallebene
Ändern der Anfrage (Wozu?)	eine andere Anfrage stellen, die das gleiche Ziel erreicht	ggf. Rückfallebene

Die Frage „Was“ und „Warum“ scheinen für die obigen Überlegungen nicht relevant zu sein, da das Wesen der zu kompensierenden Anfrage (Was?) nicht verändert werden kann und sich „Warum“ in diesem Fall mit „Wozu“ doppelt.

Durch die festzulegenden positiven Einflüsse auf die Rückfallebenenfunktion wird beschrieben, in welchem Maße die einzelnen Kompensationsmaßnahmen zur Erhöhung der Schutzrate in Bezug auf die jeweilige der Rückfallebene zugrundeliegende Abweichung vom Regelbetrieb beitragen. Die entsprechenden Gewichtungsfaktoren sind im Vorfeld zu bestimmen und über die Funktion anzugeben. Für eine Rückfallebene können mehrere Kompensationsmaßnahmen kombiniert werden, z. B. eine langsamere Geschwindigkeit und ein zusätzliches Warnsignal. Dabei kann die Funktion theoretisch eine beliebige Form haben, sofern sie eine realistische Abbildung der Steigerung der Schutzrate durch die Kompensationsmaßnahmen darstellt.

Herkunft der Rückfallebenenfunktion und der Werte ihrer Parameter

Stakeholder-Systeme können sich mit dem die Schutzrate verringernden und dem erhöhenden Funktionsteil der Rückfallebenenfunktion auf einer der Registrierungsschnittstellen registrieren (vgl. Kapitel 8.3.3). Für andere Prüfbedingungen müssen die Parameter aus einer generischen und sicheren Quelle kommen, analog zu beispielsweise den Topologiedaten (vgl. Kapitel 4.4). Hiermit soll sichergestellt werden, dass die Form der Rückfallebenenfunktion oder deren Parameter angepasst werden können, ohne dass die gesamte Logik neu zugelassen werden muss (vgl. dazu die globale Anforderung der generischen Logik aus Kapitel 3.5).

Die Zusammenstellung der aktuellen Werte der einzelnen Parameter und die Berechnung des Ergebnisses müssen allerdings durch die smartLogic erfolgen. Die Rückfallebenenfunktion darf daher nur Parameter enthalten, deren Werte die smartLogic auch ermitteln kann. Allerdings kann z. B. ein Stakeholder-System Parameter in die Funktion integrieren, deren Werte es selbst an die smartLogic liefern kann, wie z. B. einen bestimmten Systemzustand oder einen Sensorwert.

Form der Funktion

Die Form der Funktion hängt, wie in den vorigen Unterabschnitten bereits geschildert, vom Zusammenhang der einzelnen Parameter ab. Es wurde kein Grund identifiziert, für die Form der Funktion bestimmte Grenzen zu setzen.

Beispiel zur Vorgabe von Rückfallebenen mit dynamischer Rückfallebenenfunktion

Als Beispiel für eine Rückfallebene mit einer dynamischer Rückfallebenenfunktion könnte die oben bereits erwähnte Weiche wieder aufgegriffen werden. Für diese wurden bereits verschiedene mögliche Sicherheitslevel aufgezeigt. Eines dieser Sicherheitslevel ist, dass die Weiche zwar Endlage hat, aber nicht überwacht ist. Es kann angenommen werden, dass hierdurch die Schutzrate beträchtlich sinkt. Das aktuelle betriebliche Regelwerk sieht für diesen Fall jedoch vor, dass die Weiche dennoch mit 5 km/h mit Befehl auf Sicht befahren werden kann [DB Netz AG 2017a]. Von daher wird an dieser Stelle angenommen, dass diese Kompensationsmaßnahmen die Schutzrate in ausreichendem Maß wieder steigern, um eine Anfrage genehmigen zu können. Es handelt sich hierbei um eine Annahme für das Beispiel, die nicht durch eine genaue Untersuchung gestützt ist.

Bei der Weiche handelt es sich gemäß dem Datenmodell aus Kapitel 7 aus Sicht des topologischen Modells um eine Verzweigung der Gleistopologie und aus Sicht des Infrastrukturmodells um ein stellbares Fahrwegelement. Im Infrastrukturmodell kann für Elemente des Objekttyps Weiche als Unterklasse der stellbaren Fahrwegelemente eine Rückfallebenenfunktion definiert werden.

In diesem Fall würde als negativer Bestandteil der Rückfallebenenfunktion für den Einfluss auf die Schutzrate mit dem Index 0 für das Sicherheitslevel „Endlage, aber nicht überwacht“ ein Term fungieren, der in etwa wie folgt aussehen könnte:

$$a_0 * x_0 \; mit \; x_0 = \begin{cases} x = 1, falls \; ElementStatus = "nicht \; überwacht" \\ x = 0, sonst \end{cases}$$

wobei a_0 der Gewichtungsfaktor ist, der beschreibt, wie stark die aus dem Sicherheitslevel resultierende Abweichung vom Regelbetrieb die Schutzrate drückt und x_0 die Indikatorvariable für Einfluss 0.

In den positiven Bestandteil könnten nun die genannte Geschwindigkeitsänderung und die ETCS-Modus-Änderung in „On Sight“ (OS) sowie eine weitere Erhöhung durch eine zu quittierende Nachricht integriert werden. Die Geschwindigkeitsänderung ist dabei unabhängig von den anderen Parametern, während der Modus OS und die zu quittierende Nachricht als voneinander abhängig angenommen werden. In diesem Beispiel wird zur Veranschaulichung angenommen, dass die Quittierung der Nachricht mit einem aussagekräftigen Grund für den Modus OS die Fehlerrate des Tf um den Faktor 4 drückt. Bei der Geschwindigkeitsänderung wird angenommen, dass sie die Schutzrate linear im Bereich zwischen 40 und 5 km/h beeinflusst. Die Funktion könnte dann die folgenden Terme enthalten:

$$a_1 y_1 (1 + 3y_2) * a_3 y_3 \; mit \; y_3 = \begin{cases} \frac{40 - v}{35}, falls \; 40 \geq v \geq 5 \\ 1, falls \; v < 5 \\ 0, sonst \end{cases}$$

In diesem Fall stehen die a-Variablen für die Gewichtungsfaktoren und die y-Werte für die Einflussfaktoren. Dabei geben y_1 und y_2 an, ob der Modus OS in der Fahrerlaubnis vorgegeben ist und ob die zu quittierende Nachricht in der Fahrerlaubnis enthalten ist. Es handelt sich demnach um Indikatorvariablen, die bei Vorliegen dieser Bedingung den Wert ‚1' annehmen und sonst den Wert ‚0'. y_3 nimmt dagegen einen Wert zwischen 0 und 1 an, wenn die Geschwindigkeit des Zuges zwischen 0 und 40 km/h liegt, wobei der Wert im Bereich zwischen 0 und 5 km/h immer 1 ist. Ab 40 km/h ist der Wert der Variable dagegen immer 0, es existiert also kein positiver Einfluss auf die Schutzrate mehr.

In der Gesamtrechnung würde dann zunächst der Wert aus dem negativen Teil der Rückfallebenenfunktion (negREF) für Einfluss i von der Basis-Schutzrate von 1 abgerechnet und anschließend der Wert aus dem positiven Teil der Rückfallebenenfunktion (posREF) wieder gegengerechnet, wobei der Wert von 1 nicht überschritten werden darf. Der resultierende Wert fließt als Faktor in die Berechnung der Schutzrate gemäß Kapitel 8.3.1 ein.

$$Anteil \; an \; Schutzrate \; durch \; dynamische \; REF = \prod_{i=1}^{n} \min(1; (1 - negREF_i + posREF_i))$$

Beispiel zur Vorgabe fester Rückfallebenen

Alternativ zu der dynamischen Bestimmung des Einflusses einer Rückfallebene auf die Schutzrate abhängig vom Betriebszustand, kann auch die Vorgabe fester Rückfallebenen sinnvoll sein, die beispielsweise von Stakeholder-Systemen abhängig von ihrem Zustand vorgegeben werden und spezifische Anforderungen des betrieblichen Regelwerkes abbilden. Beispielsweise könnte für einen Bahnübergang bei seiner Registrierung als Stakeholder-System festgelegt werden sollen, dass er auf eine der drei folgenden Weisen befahren werden kann:

- im Zustand Schranke geschlossen und Bahnübergang freigemeldet ohne Einschränkungen (Regelbetrieb)
- im Zustand Schranke geschlossen, aber nicht freigemeldet im Modus On Sight mit maximal 40 km/h
- im Zustand Schranke offen im Modus On Sight mit maximal 5 km/h nach vorherigem Achtungspfiff

Da sich die Kompensationsmaßnahmen immer nur auf den entsprechenden Zustand des Stakeholder-Systems beziehen sollen, kann für jeden Zustand einfach die damit verbundene Schutzrate in der Rückfallebenenfunktion vorgegeben werden. Das Vorliegen des entsprechenden Zustands dient dabei jeweils als Indikatorvariable (Faktor 1 für den Fall, dass der Zustand vorliegt und 0 sonst), so dass nur der Funktionsbestandteil gemäß dem aktuell vorliegenden Zustand tatsächlich in die Berechnung der Gesamt-Schutzrate eingeht:

$$Anteil \; an \; Schutzrate \; durch \; feste \; REF = \prod_{i=1}^{n} \min(1; \sum_{j=1}^{p} a_j \, z_j) \; mit \; z_j \in \{0; 1\}$$

Dabei ist a_j der Einfluss auf die Schutzrate bei Vorliegen des Zustands j (z_j=1) und p die Anzahl der definierten Rückfallebenen.

Zusammenfassung

Das vorliegende Unterkapitel befasste sich mit dem Umgang der smartLogic mit Abweichungen vom Regelbetrieb und dazugehörigen Rückfallebenen, da dieser Thematik eine hohe Relevanz für die Konzeption der smartLogic beigemessen wird. Aus Ressourcengründen wurde jedoch nur ein grundsätzliches Konzept zur Thematik entworfen.

Zu Beginn wurden aus den globalen und Hauptkapitel-spezifischen Anforderungen die speziellen Anforderungen hergeleitet, wonach zum einen „in möglichst vielen Betriebssituationen [– insbesondere auch bei Abweichungen vom Regelbetrieb –] die smartLogic Fahrzeugbewegungen zulassen können [soll]“, wozu die Bedingungen der Rückfallebenen in die Logik zu integrieren sind. Zum anderen soll „das TMS die Möglichkeit haben, die Anfragen an die smartLogic möglichst dynamisch zu stellen“.

Auf dieser Basis wurde ein Konzept entwickelt, welches die Möglichkeit bietet, Bedingungen von Rückfallebenen generisch zu beschreiben und als Funktionsbestandteile (Rückfallebenenfunktion) in die Funktion zur Berechnung der Schutzrate zur Bewertung von Anfragen an die smartLogic zu integrieren.

Ausgangspunkt für die Berechnung der Rückfallebenenfunktion sind unterschiedliche Sicherheitslevels, die verschiedene Systemkomponenten je nach aktuellem Status aufweisen können. Die verminderte Sicherheit der verschiedenen Sicherheitslevels fließt über einen negativen Bestandteil der Rückfallebenenfunktion in die Berechnung der Schutzrate ein. Auf der anderen Seite können Kompensationsmaßnahmen wie eine niedrigere Geschwindigkeit die Schutzrate wieder erhöhen. Der Einfluss dieser Kompensationsmaßnahmen wird im positiven Bestandteil der Rückfallebenenfunktion abgebildet.

Alternativ ist es auch möglich, dass der Wert der Rückfallebenenfunktion abhängig von einem Indikator (z. B. Status eines Stakeholder-Systems) fest vorgegeben wird. Das Ergebnis der Rückfallebenenfunktion fließt in beiden Fällen als Faktor in die Berechnung der Schutzrate für die jeweilige Prüfbedingung ein.

Die Rückfallebenenfunktionen können über die sichere Datenquelle an die smartLogic übermittelt werden. Alternativ können sie von externen Systemen bei deren Registrierung als Stakeholder-System festgelegt werden.

8.4 Konzepte für Spezialfälle

In Ergänzung zu den in Kapitel 8.3 diskutierten Basis-Konzepten, werden in diesem Kapitel für einige Spezialfälle Lösungsstrategien auf Basis der bisherigen Überlegungen zur smartLogic vorgeschlagen. Die Abgrenzung von „Spezialfällen“ zu den „Basis-Konzepten“ folgt keiner wissenschaftlich herleitbaren Unterscheidung, sondern dient zur besseren Orientierung des Lesers. Den Spezial-Konzepten wurden Themen zugeordnet, die im Vergleich zu den Basis-Konzepten seltener relevant sind und für einen vereinfachten Regelbetrieb auf einem beschränkten Netz zunächst nicht unbedingt geklärt sein müssen.

Aufgrund des für die Erstellung dieser Arbeit verfügbaren Zeitumfangs werden die Umsetzungskonzepte für Spezialfälle nicht so ausführlich hergeleitet wie die Basis-Konzepte. Für die einzelnen Themen könnten von ihrem Umfang her auch jeweils eigene wissenschaftliche Arbeiten verfasst werden. Erfahrungen aus der Praxis zeigen allerdings, dass häufig die Umsetzung neuer Ideen und Technologien daran scheitert, dass sie der Praxis nicht gerecht werden, da nicht alle erforderlichen Spezialfälle abgedeckt werden können. Um dieses Problem zu vermeiden, sollten die

Spezialfälle bei der Erarbeitung der smartLogic von Anfang an mitgedacht werden. Aus diesem Grund werden in diesem Kapitel zumindest grundlegende Überlegungen zu Konzepten für bekannte Spezialfälle angestellt. Eine ausführlichere Analyse der Spezialfälle kann in weiteren wissenschaftlichen Arbeiten erfolgen.

Die Themen der Spezialkonzepte stammen aus dem Funktionskatalog, insbesondere aus den dort identifizierten betrieblichen Funktionen (vgl. Kapitel 6.3). Gemäß Kapitel 6.3 gehört es zu den betrieblichen Funktionen der smartLogic, dass einer Fahrzeugbewegung der „gewünschte Fahrweg eingestellt werden kann“. Hierbei kann es vorkommen, dass ein Fahrtrichtungswechsel der Fahrzeugbewegung erforderlich ist. Dabei ist zu prüfen, ob zur sicheren Durchführung solcher Fahrtrichtungswechsel zusätzliche Regeln in der Sicherungslogik erforderlich sind (Kapitel 8.4.1). Da anzunehmen ist, dass es Situationen gibt, in denen neue Fahrzeuge im Bereich der smartLogic aufgerüstet werden (vgl. ebenfalls Kapitel 6.3), müssen diese auch der smartLogic bekannt werden (Kapitel 8.4.2). Als weitere betriebliche Funktion wird in Kapitel 6.3 das Verändern der Fahrzeugzusammensetzung für Eisenbahnfahrzeugbewegungen genannt (Kapitel 8.4.3). Fahrzeuge können dabei auch besondere Anforderungen wie außergewöhnliche Maße haben (Kapitel 8.4.4). Als weitere betriebliche Funktion soll die Zuordnung von Stellelementen zur smartLogic geändert werden können (Kapitel 8.4.5).

Unabhängig von den geforderten betrieblichen Funktionen wird in Kapitel 8.4.6 beispielhaft auf die sehr spezielle Sicherheitsanforderung des Tunnelbegegnungsverbots eingegangen, die in den letzten Jahren aufgekommen ist, um zu prüfen, ob auch eine solche spezielle Anforderung mit der bisherigen Logik abgedeckt werden kann.

8.4.1 Fahrtrichtungswechsel

Wechsel der Fahrtrichtung von Fahrzeugbewegungen (Fahrtrichtungswechsel) können sowohl fahrplanmäßig, z. B. in Kopfbahnhöfen, als auch außerplanmäßig in Folge außergewöhnlicher Ereignisse erfolgen. In diesem Unterkapitel soll hergeleitet werden, welche Implikationen durch planmäßige Fahrtrichtungswechsel für die smartLogic entstehen[56]. Dazu können die Geschehnisse bei einem Fahrtrichtungswechsel schrittweise betrachtet und mögliche Lösungen für auftretende Probleme skizziert werden.

Im Rahmen von smartRail 4.0 sind unabhängig von den Überlegungen in dieser Arbeit sehr ähnliche Konzepte entstanden, wie sie für dieses Kapitel erarbeitet wurden. Vergleiche dazu [SBB AG 2018] und siehe auch Kapitel 8.10.

Anfahrt auf den Ort des Fahrtrichtungswechsels

Bei der Anfahrt auf den Ort, an dem der Fahrtrichtungswechsel stattfinden soll, kann das Fahrzeug wie gewöhnlich eine Movement Authority bis zum gewünschten Zielpunkt nutzen.

Ist dieser Zielpunkt ein Prellbock (oder ein anderer Gefahrpunkt, der keinesfalls passiert werden darf), muss neben der EoA auch die SvL vor diesem Prellbock liegen (vgl. Kapitel 8.3.2). Dadurch ergibt sich eine langsame Einfahrgeschwindigkeit, die jedoch nicht fest vorgegeben werden muss, wie es heute in Deutschland mit i. d. R. 30 km/h der Fall ist (in Ostdeutschland z. T. 40 km/h). Stattdessen übernimmt ETCS die Überwachung der Anfahrt auf den Prellbock.

[56] Die Überlegungen lassen sich zum Teil auf außerplanmäßige Fahrtrichtungswechsel übertragen, z. B. könnte mittels einer neuen Fahrerlaubnis zurückgesetzt werden. Bei außerplanmäßigen Fahrtrichtungswechseln gibt es aber z. B. auch Funktionen wie „Reversing“ bei ETCS, die hier nicht thematisiert werden sollen.

Durch die Ortungsungenauigkeit kann es zu dem Problem kommen, dass bei rein fahrzeugseitiger Ortung der anzusteuernde Zielpunkt nicht annähernd erreicht werden kann. Für dieses Problem sieht ETCS das Konzept der Release Speed vor (vgl. Kapitel 2.2.2), welches jedoch bei ATO nicht genutzt werden kann, da es auf einem selbstständigen Annähern an den Zielpunkt durch den Tf basiert. Aufgrund dieser Tatsache und dem bei Kopfbahnhöfen systembedingten Problem der niedrigen Einfahrgeschwindigkeiten wird gefolgert, dass zusätzliche Fahrzeugortungsoptionen in entsprechenden Stumpfgleisen sinnvoll sind, die eine genauere Ortung ermöglichen. Je genauer die Ortung, desto schneller und präziser kann die Einfahrt erfolgen.

Ein Erweiterungsbedarf der Regeln der smartLogic für den Fall der Anfahrt auf den Ort eines Fahrtrichtungswechsels ergibt sich aus den obigen Überlegungen nicht.

Anlegen eines neuen Beanspruchungsobjektes und Bestimmung der neuen Position der Zugspitze

Nach dem Anhalten muss das Fahrzeug fahrzeugintern einen Fahrtrichtungswechsel vornehmen. Auf die Ab- und Aufrüstung der Führerstände und damit verbundene Ab- und Anmeldeprozesse soll hier jedoch nicht näher eingegangen werden, siehe dazu Kapitel 8.4.2. Damit die Beanspruchung der Infrastruktur durch die Fahrzeugbewegung innerhalb der smartLogic auch nach dem Richtungswechsel korrekt abgebildet werden kann, müssen die Beanspruchungsobjekte angepasst werden, bevor eine neue Fahrerlaubnis übermittelt werden kann.

Da beim Fahrtrichtungswechsel auch eine Änderung der Fahrzeugzusammensetzung erfolgt sein kann (siehe dazu auch Kapitel 8.4.3), kann das alte Fahrzeugbelegungsbeanspruchungsobjekt nicht ohne weitere Prüfung übernommen werden, sondern die Position und das Ausmaß der Fahrzeugbelegungs-beanspruchung sind neu zu bestimmen. Im Idealfall können dabei beide Enden der Fahrzeugbewegung automatisch vollständig geortet werden bzw. über eine Information zur sicheren Zuglänge hergeleitet werden. Auf Basis dieser Informationen kann ein neues Beanspruchungsobjekt mit den ermittelten Ausmaßen erzeugt werden. (Das alte Beanspruchungsobjekt wird noch benötigt, falls sich noch ein abgetrennter Zugteil auf dem Gleis befindet, siehe Abschnitt „Freigabe des Gleises, in dem der Fahrtrichtungswechsel stattfand“).)

Andernfalls muss zunächst das Beanspruchungsobjekt zur sicheren Seite hin großzügig ausgelegt werden und damit in den Grenzen des alten Beanspruchungsobjektes angelegt werden. Zusätzlich muss vor Genehmigung einer Fahrerlaubnis sichergestellt werden, dass sich kein Teil der ehemaligen Fahrzeugbewegung in Fahrtrichtung vor der neuen Zugspitze befindet (z. B. bei einer Zugteilung der ehemals hintere Zugteil). Hierfür kommen z. B. eine manuelle Bestätigung, eine Bestätigung über geeignete Sensoren oder eine Fahrt auf Sicht bis an das Ende der ursprünglichen Beanspruchung in Frage. Nach Fahrtbeginn können dann bei Vorliegen neuer Ortungsinformationen (z. B. beim Passieren eines Ortungspunktes wie einer Balisengruppe) die Ausmaße der Beanspruchung angepasst werden.

Bezugspunkt der neuen Fahrerlaubnis

Bei der Ausstellung der neuen Fahrerlaubnis entsteht ETCS-seitig das Problem, dass sich die Fahrerlaubnis immer auf eine dem Fahrzeug bekannte, rückwärtige Position auf dem Gleis beziehen muss und i. d. R. diese bereits bekannten Positionen sich nach dem Fahrtrichtungswechsel vor dem Fahrzeug statt hinter diesem befinden. Um das Problem zu lösen, sieht ETCS das Konzept der ***Shifted Location Reference*** vor. Dabei wird der Bezugspunkt in die ursprüngliche Fahrtrichtung (vor dem Fahrtrichtungswechsel) verschoben, bis er hinter der aktuellen Position des Fahrzeugs liegt. Dieser verschobene Bezugspunkt kann dem Fahrzeug über die ETCS-Nachricht 33 („MA with

Shifted Location Reference“) mitgeteilt werden. Das Konzept der Shifted Location Reference soll auch im Rahmen der RCA bzw. des APS verwendet werden [SBB AG 2020] und kann auch in Zusammenhang mit der smartLogic genutzt werden.

Freigabe des Gleises, in dem der Fahrtrichtungswechsel stattfand

Nachdem die Fahrzeugbewegung, welche zuvor die Fahrtrichtung gewechselt hat, ausgefahren ist, muss der Gleisabschnitt, in dem der Fahrtrichtungswechsel stattgefunden hat, wieder freigegeben werden. Hierzu muss sichergestellt werden, dass kein Teil der ursprünglichen Fahrzeugbewegung im Gleis verblieben ist. Deshalb ist die alte Fahrzeugbelegungsbeanspruchung noch vorhanden. Sendet die neue Fahrzeugbewegung ihre Zuglänge bzw. ist die Position des Zugendes bekannt (dann darf allerdings die Ortungsungenauigkeit keine Zweifel über die Länge des Zuges aufkommen lassen), kann diese Information mit der ursprünglichen Zuglänge bzw. dem Ende der alten Beanspruchung verglichen werden. Bei eindeutigem Befund kann die alte Beanspruchung durch die ursprüngliche Fahrzeugbewegung gelöscht werden.

Andernfalls wird eine Freimeldung über geeignete Sensoren oder manuell benötigt. Dieser Umstand ist ein weiteres Argument für die Beibehaltung einer infrastrukturseitigen Gleisfreimeldeanlage in Gleisen, in denen sich Fahrzeuge planmäßig auf- und abrüsten, die keine durchgängigen Daten zur Position von Zugspitze und Zugende senden.

8.4.2 Anmelden (Registrieren) von Fahrzeugen

In der Praxis sind nicht alle Fahrzeuge permanent vollüberwacht, sondern es ist davon auszugehen, dass es auch Fahrzeuge gibt, die kein aufgerüstetes Zugsicherungssystem haben. Dieses Unterkapitel beschäftigt sich daher mit dem Anmelden von neu aufgerüsteten Fahrzeugen.

Mit der Anmeldung muss gemäß dem Konzept der Beanspruchungen (vgl. Kapitel 7.6.2) eine Fahrzeugbelegungsbeanspruchung („Vehicle Occupation“) erzeugt werden. Es sind dabei verschiedene Vorgehensweisen bei unterschiedlichen Anwendungsfällen denkbar, mit denen sich der erste Abschnitt beschäftigt. Die Ausdehnung dieser Beanspruchung muss ebenfalls bestimmt werden. Hierzu dient der zweite Abschnitt.

Überlegungen zur Anpassung bzw. Generierung einer Fahrzeugbelegungsbeanspruchung

Normalerweise sollte bei Anmeldung eines Fahrzeugs bei der smartLogic bereits eine Beanspruchung auf der Infrastruktur existieren, in der sich das Fahrzeug befindet, da ansonsten der entsprechende Gleisabschnitt in eine MA für ein anderes Fahrzeug inkludiert werden und damit eine Kollision herbeigeführt werden könnte. Es sind verschiedene Typen von bereits existierenden Beanspruchungen denkbar, auf die unterschiedlich reagiert werden muss:

1. In vielen Fällen, z. B. bei Fahrtrichtungswechsel oder ggf. nach einer temporären Abstellung, wird bei Aufrüstung und Anmeldung eines Fahrzeugs an der gemeldeten Position bereits eine Fahrzeugbelegungsbeanspruchung vorhanden sein, die von der vorherigen Fahrzeugbewegung stammt. In diesem Fall sind die Überlegungen zu beachten, die bereits in Kapitel 8.4.1 beschrieben wurden, insbesondere muss zunächst geprüft werden, dass es keine Veränderung an der Fahrzeugzusammensetzung der Fahrzeugbewegung gab bzw. der Fahrwegabschnitt vor der neuen Zugspitze muss freigemeldet werden.
2. Statt einer (früheren) Fahrzeugbelegungsbeanspruchung könnte auch eine Danger Area (DA) vorhanden sein, z. B. weil der smartLogic ein Fahrzeug ohne

vorherige Identifizierung gemeldet wurde[57]. In diesem Fall ist eine neue Fahrzeugbelegungsbeanspruchung zu erzeugen und mit dem sich neu anmeldenden Fahrzeug zu verknüpfen. Es kann jedoch noch nicht mit Sicherheit gesagt werden, dass die bestehende DA gelöscht werden kann, da im Detektionsabschnitt der DA z. B. mehrere Fahrzeuge vorhanden sein könnten. Daher wird anschließend zusätzlich eine Freimeldung des Bereichs von der Zugspitze bis zum Ende des Detektionsabschnitts benötigt (z. B. durch Fahrt auf Sicht in diesem Abschnitt) sowie ggf. für den Bereich hinter der neuen Fahrzeugbewegung bis zum Ende des Detektionsabschnitts (siehe nächster Abschnitt).

3. Die Anmeldung des Fahrzeugs könnte auch in einem speziellen Gleisbereich stattfinden, dessen Belegungszustand (temporär) nicht von der smartLogic überwacht und damit für vollüberwachte Fahrzeugbewegungen gesperrt ist. Es besteht dann eine entsprechende Restricted Area (RA) oder Beanspruchung[58], welche diesen Sachverhalt abbilden. Dabei könnte es sich um Gleisbereiche handeln, die speziell für das Eingleisen von Fahrzeugen zugelassen sind und bei denen die Einfahrt mit entsprechend angepasster Geschwindigkeit ausschließlich auf Sicht oder mittels ähnlicher Sensorüberwachung stattfinden darf. In solchen Bereichen bietet es sich aus Sicht des Autors an, dass auch zukünftig infrastrukturseitige Gleisfreimeldesysteme wie Achszähler verwendet werden, um zu verhindern, dass Fahrzeuge aus dem unüberwachten Bereich unbemerkt in den überwachten Bereich gelangen können.
   Bei Anmeldung eines Fahrzeuges in einem speziellen Gleisbereich würde eine neue Fahrzeugbelegungsbeanspruchung innerhalb des speziellen Gleisbereiches erzeugt werden und dem Fahrzeug könnte regulär die Ausfahrt aus dem Bereich mit einer MA erlaubt werden. Für die Fahrtstrecke innerhalb des speziellen Bereichs gelten die gleichen Überlegungen wie beim Übergang aus der DA. Wenn der spezielle Gleisbereich gänzlich freigemeldet ist, könnte er auch aufgelöst werden, so dass in diesem Bereich vollüberwachte Fahrten stattfinden können. Wenn der spezielle Gleisbereich wieder für den Zweck des Eingleisens benötigt wird, könnte eine erneute RA oder Beanspruchung erzeugt werden.

Bestimmen der Ausdehnung der Beanspruchung und Löschung der vorherigen Beanspruchung

Für die neue Fahrzeugbelegungsbeanspruchung ist noch die Ausdehnung zu klären. Die Ausdehnung muss in Hinblick auf den Zweck der Fahrzeugbelegungsbeanspruchung mindestens das gesamte Fahrzeug umfassen, also von Zugspitze bis Zugende reichen. Sie sollte aufgrund der Anforderung zur Zieldimension „*hohe Kapazität*“ auch nicht größer als notwendig sein (vgl. Kapitel 8.2.1).

Die genaue Position der Zugspitze ist – abhängig von den zur Verfügung stehenden Ortungstechniken – möglicherweise unbekannt. Zum Beispiel kann bei einem Fahrtrichtungswechsel, wie bereits im vorigen Unterkapitel angedeutet, nicht automatisch davon ausgegangen werden, dass die neue Zugspitze an der Position des bisherigen Zugendes liegt, da eine Zugteilung stattgefunden haben

[57] In Folge der Einrichtung der DA erfolgt ein Reaktionsprozess, um zu ermitteln, ob durch das Ereignis schadensausmaßverringernde Maßnahmen erfolgen müssen (vgl. Kapitel 7.3.7). Hier geht es aber nur um den darauffolgenden Prozess, um das entdeckte Fahrzeug zu einer regulären Fahrzeugbewegung zu machen.

[58] Ob eine Abbildung über RAs oder Beanspruchungen sinnvoller ist, wird hier aufgrund der begrenzten Zeitressourcen für die Erstellung dieser Arbeit nicht diskutiert.

könnte. Ist das führende Fahrzeug nur mit relativer Ortung (z. B. Odometrie) ausgestattet, wird zunächst eine neue Ortungsinformation, zum Beispiel beim Passieren eines Ortungspunktes, zur Bestimmung der exakten Position benötigt.

Neben der Position der Zugspitze ist auch die Position des Zugendes nicht unbedingt bekannt. Wenn keine gesicherte Information über die Position des Zugendes vorliegt und auch keine gesicherte Information über dessen Länge, kann die Ausdehnung der Beanspruchung erst bestimmt werden, wenn sich die neue Fahrzeugbewegung in Bewegung gesetzt hat und über den Ortungsinformationsaggregator Informationen zur Position des Zugendes bestimmt wurden. Daher muss vorerst eine maximal mögliche Ausdehnung der Fahrzeugbelegungsbeanspruchung angenommen werden, die dann eingekürzt werden kann. Diese maximale Ausdehnung muss dann (mangels weiterer einschränkender Informationen) entweder vom Ende der kompletten früheren Fahrzeugbelegung oder Danger Area bestimmt werden, falls eine solche bestanden hat, oder (im dritten Fall des vorigen Abschnitts) vom Ende des Gleisbereiches, aus dem die Fahrzeugbewegung stammt.

8.4.3 Veränderungen an der Fahrzeugzusammensetzung der Fahrzeugbewegung

Auch wenn heute häufig aufgrund des hohen Aufwands versucht wird, Kupplungsvorgänge zu vermeiden, so gehört es doch zu den erforderlichen betrieblichen funktionalen Anforderungen, dass es möglich sein muss, Züge zu vereinigen oder zu teilen bzw. einzelne Wagen an- oder abzukuppeln (vgl. Kapitel 6.3). Ein solcher Vorgang ist deshalb besonders, weil er zum einen die Anzahl der Fahrzeugbewegungsobjekte und der zugehörigen Fahrzeugbewegungsbeanspruchungen verändert und zum anderen die Situation auftreten könnte, dass sich die beteiligten Fahrzeugbewegungsbeanspruchungen überlappen. Aus diesen Gründen wird eine genauere Untersuchung des Vorgangs als sinnvoll erachtet.

Hierzu erscheint es sinnvoll, die einzelnen Vorgänge (Vereinigung sowie Teilung von Fahrzeugbewegungen) zunächst getrennt voneinander zu betrachten, da angenommen werden kann, dass sie unterschiedliche Schritte und Problematiken enthalten. Im ersten Abschnitt werden Vereinigungen untersucht und im zweiten Abschnitt planmäßige Zugteilungen. Dabei wird im Sinne der Anforderung der *schlanken Logik* (vgl. Kapitel 8.2.1) auf die bestehenden Konzepte der smartLogic zurückgegriffen und von einer durchgängigen Überwachung der beteiligten Fahrzeugbewegungen ausgegangen. Abschließend soll im dritten Abschnitt noch auf den Fall von ungeplanten Zugtrennungen eingegangen werden.

Im Rahmen von smartRail 4.0 sind unabhängig von den Überlegungen in dieser Arbeit sehr ähnliche Überlegungen entstanden wie in diesem Kapitel. Vergleiche dazu [SBB AG 2018] und Kapitel 8.10.

Vereinigung von Fahrzeugbewegungen

Der grobe Ablauf einer Vereinigung mehrerer Fahrzeugbewegungen (bzw. Fahrzeuge) ergibt sich aus dem bekannten betrieblichen Prozess solcher Vereinigungen. Zunächst muss ermöglicht werden, dass sich beide Fahrzeugbewegungen nah genug aneinander befinden, dass sie gekuppelt werden können bzw. eine automatische Kupplung einrastet (erster Unterabschnitt). Der eigentliche physische Kupplungsvorgang liegt gemäß Kapitel 4.3.2 im Verantwortungsbereich der Fahrzeuge und nicht der infrastrukturseitigen Sicherungslogik. Anschließend müssen die Fahrzeugbewegungsobjekte und die zugehörigen Beanspruchungen angepasst und somit die Voraussetzungen für die Weiterfahrt geschaffen werden (zweiter Unterabschnitt). Schließlich muss der neu entstandenen Fahrzeugbewegung ermöglicht werden, mit einer neuen MA ihre Fahrt zu beginnen (dritter Unterabschnitt).

Erreichen des Kupplungspunktes

Um in die Kupplungsposition zu fahren, könnten in einer idealen Welt beide Fahrzeugbewegungen eine MA bekommen, mit der sie genau voreinander zum Halten kommen würden und dann ohne weitere Bewegung gekuppelt werden könnten bzw. die automatische Kupplung einrasten würde. Allerdings ist heute und in der näheren Zukunft noch damit zu rechnen, dass Ortungsungenauigkeiten ein solch präzises Halten am Zielpunkt verhindern. Daher ist zu prüfen, welche weiteren Möglichkeiten zum Heranfahren an den Kupplungspunkt existieren:

1. Klassischerweise finden Bereitstellungsfahrten zum Kuppeln als Rangierfahrt statt. Eine denkbare Lösung wäre daher ein Modus-Wechsel aus der Vollüberwachung (Modus „Full Supervision“) heraus in den Modus „Shunting“. Allerdings wurden bisher Fahrzeugbewegungen mit verschiedenem Sicherheitsniveaus und damit eine Einteilung von Fahrzeugbewegungen in Zug- und Rangierfahrten nicht für erforderlich gehalten (vgl. Kapitel 8.3.5). Die Entlassung eines Fahrzeugs aus der Vollüberwachung kann auch für andere Funktionen wie den Flankenschutz negative Auswirkungen haben (vgl. Kapitel 8.3.4).
2. Es könnte auch die ETCS-Funktion der „Release Speed“ genutzt werden (vgl. Kapitel 2.2.2), da diese Funktion das Passieren der vom Fahrzeug berechneten, aber durch die Ortungsungenauigkeit unpräzisen EoA erlaubt, um bis zur tatsächlichen Position der EoA vorzurücken. Dieses Vorgehen könnte auf den Kupplungspunkt übertragen werden, indem die EoA auf den geplanten Kupplungspunkt gesetzt wird. Allerdings darf die berechnete Position der SvL, die ebenfalls der Ortungsungenauigkeit unterliegt, nicht passiert werden. Damit die Release Speed ein exakteres Heranfahren an den Kupplungspunkt erlauben würde, müsste die SvL daher auf oder hinter dem anderen Fahrzeug liegen. Dies widerspricht jedoch der Intention der SvL, die immer vor dem maßgeblichen Gefahrpunkt für die betrachtete Fahrzeugbewegung liegen muss, da ansonsten bei einer theoretisch möglichen Fahrt bis zur SvL eine Kollision stattfinden würde.
3. Die Möglichkeit einer „Kollision“ könnte allerdings auch bewusst in Kauf genommen werden, denn strenggenommen ist für den Kupplungsvorgang mit einer modernen automatischen Kupplung ohnehin eine Berührung der beiden Fahrzeuge erforderlich. Dabei könnte ein Schaden verhindert werden, wenn eine ausreichend geringe Geschwindigkeit vorgegeben und überwacht werden würde. Dies wäre entweder über eine entsprechend geringe Release Speed oder einfach über ein passendes Geschwindigkeitsprofil möglich. Allerdings würde die Inkaufnahme einer „Kollision“ die Logik entgegen der Anforderung der schlanken Logik generell verkomplizieren, da die grundsätzliche Sicherheitsanforderung der Kollisionsfreiheit in Hinblick auf das Setzen der SvL in Frage gestellt würde.

Da die dritte Lösungsmöglichkeit im Sinne der Anforderungen der *schlanken Logik* und der *generischen Logik* mit einer einfachen generischen Regel unabhängig vom Zweck der Fahrzeugvereinigung umsetzbar ist, wird sie trotz der genannten Nachteile als am geeignetsten bewertet. Eine solche Regel könnte es generisch erlauben, bei Unterschreitung einer gewissen Geschwindigkeit die SvL so zu setzen, dass sich zwischen der EoA und der SvL eine andere Fahrzeugbewegung befinden darf. Die Ermittlung der Höhe dieser Geschwindigkeit als Wert ist nicht Teil dieser Arbeit (vgl. Kapitel 3.3).

Damit das eine Fahrzeug bei der Anfahrt zur Kupplung jedoch nicht das andere Fahrzeug vor sich herschiebt, sollte möglichst fahrzeugseitig ein Mechanismus vorhanden sein, der den Aufprall registriert und dann eine sofortige Bremsung einleitet. Die gewählte Lösung hat auch den Vorteil, dass sie bei ATO-Fahrten ebenfalls möglich ist.

Voraussetzungen für die Weiterfahrt und Anpassung der Objekte im Datenmodell

Nachdem die Fahrzeuge physisch gekuppelt sind, müssen auch die zu den Fahrzeugbewegungen gehörenden Objekte innerhalb des Datenmodells der Logik angepasst werden und die Voraussetzungen für die Weiterfahrt geschaffen werden. Die Schwierigkeit dabei ist, dass eine sichere Information benötigt wird, wie sich die Fahrzeugzusammensetzung verändert hat.

Wiederum im Idealfall würde die Fahrzeugbewegung ihre Fahrzeugzusammensetzung immer sicher kennen. In diesem Fall könnte sie einfach ihre neue Position und ihre neue Länge über einen Position Report und die aktualisierten Fahrzeugdaten (Validated Train Data) melden. Die smartLogic könnte dann aus diesen Angaben schlussfolgern, dass beide älteren Fahrzeugbewegungen vollständig in eine neue Fahrzeugbewegung aufgegangen sind oder umgekehrt, dass dies nicht der Fall ist, und die Objekte entsprechend anpassen.

Andernfalls müsste für die neu entstandene Fahrzeugbewegung trotzdem zunächst ein neues Objekt geschaffen werden und die zugehörige Fahrzeugbelegungsbeanspruchung vorsorglich auf den gesamten Gleisabschnitt der beiden ursprünglichen Fahrzeugbewegungsbeanspruchungen ausgedehnt werden. Damit die Infrastruktur nicht fälschlicherweise komplett freigegeben wird, müssen jedoch die alten Beanspruchungen vorsorglich bestehen bleiben, für den Fall, dass nicht alle Fahrzeuge in die neue Fahrzeugbewegung aufgegangen sind.

Falls keine sicheren Informationen zur Position der beiden Enden der neuen Fahrzeugbewegung vorliegen, muss davon ausgegangen werden, dass sich evtl. noch weitere separate Fahrzeuge im betrachteten Gleisabschnitt befinden. Der betrachtete Gleisabschnitt wird dabei durch die äußersten Positionspunkte der beteiligten Fahrzeuge vor der Vereinigung bestimmt. Für die Weiterfahrt der Fahrzeugbewegung können dabei die folgenden Fälle unterschieden werden:

- Ist zumindest die Position der Zugspitze bekannt und befindet diese sich an einem der äußeren Punkt des betrachteten Gleisabschnitts, kann eine Weiterfahrt vorwärts ohne weitere Maßnahmen erfolgen, denn der Fahrweg muss in diese Richtung frei sein.
- Ist die Position der Zugspitze nicht bekannt, muss das Fahrzeug ggf. durch Bewegung zunächst geortet werden. Hierzu kann eine Fahrerlaubnis mit einer entsprechend niedrigen Geschwindigkeit genehmigt werden, wie es auch bei ETCS für das Erfahren der Position vorgesehen ist (vgl. Kapitel 2.2.2).
- Befindet sich die Zugspitze nicht an einem äußeren Rand des betrachteten Gleisabschnitts gilt dasselbe wie bei unbekannter Position. Ein solcher Fall kann z.B. vorkommen, wenn sich das Fahrzeug durch den Kupplungsvorgang noch etwas bewegt hat. Es kann in diesem Fall nicht ausgeschlossen werden, dass vor der Zugspitze noch ein Zugteil oder ein einzelner Wagen abgekuppelt wurde.

Der Zugschluss kann erst über eine entsprechende Ortung erkannt werden. Erst dann können die alten Fahrzeugbewegungsbeanspruchungen gelöscht werden.

Um die Fehlerwahrscheinlichkeit zu senken, empfiehlt der Autor dieser Arbeit, Veränderung an der Fahrzeugzusammensetzung – wenn möglich – immer in dafür vorgesehenen Gleisabschnitten vorzunehmen und diese mit infrastrukturseitiger Sensorik wie Achszählern zu überwachen, auch wenn

dafür zusätzliche Infrastrukturelemente erforderlich sind. Durch die Sensorik kann die Länge der Fahrzeugbewegung und damit der Zugschluss mit hoher Zuverlässigkeit validiert werden.

Weiterfahrt

Für die Weiterfahrt benötigt die neu zusammengesetzte Fahrzeugbewegung eine neue MA. Ist die Fahrzeugposition vollständig bekannt und befindet sich nur noch eine Fahrzeugbewegung im betrachteten Gleisabschnitt, kann das TMS eine gewöhnliche Fahrerlaubnisanfrage an die smartLogic senden. Bei einem Fahrtrichtungswechsel gelten die Überlegungen aus Kapitel 8.4.1, wobei das Gleis nicht mehr freigeprüft werden muss.

Im Falle einer nicht vollständig bekannten Fahrzeugposition oder wenn sich mehrere separate Fahrzeugbewegungsobjekte im betrachteten Gleisabschnitt befinden, muss die Position, wie oben bereits erwähnt, zunächst „erfahren“ werden (vgl. die Überlegungen zur Registrierung von Fahrzeugbewegungen und dem Bestimmen der zugehörigen Ausdehnung in Kapitel 8.4.2).

(geplante) Teilung von Fahrzeugbewegungen

Im umgekehrten Fall einer Zugteilung (z. B. für eine Flügelung) werden aus einer Fahrzeugbewegung mehrere neue Fahrzeugbewegungen. Theoretisch könnten Fahrzeuge der ursprünglichen Fahrzeugbewegung auch erstmal abgestellt werden, sich also vorerst nicht bewegen. Die abgestellten Fahrzeuge würden in diesem Fall allerdings für die smartLogic dennoch als Fahrzeugbewegung mit entsprechenden Ausmaßen gespeichert werden, solange ETCS den Stillstand überwacht.

Im Fall der Zugteilung stellt die Fahrt zum Teilungsort kein Problem dar, da die zu teilende Fahrzeugbewegung als Ganzes zum Teilungsort fährt.

Nach der Teilung müssen die Objekte wiederum angepasst werden. Hierzu haben die Fahrzeugbewegungen die Pflicht, die Änderungen an der Fahrzeugzusammensetzung von sich aus mitzuteilen, da ansonsten die Sicherungslogik nicht wissen kann, dass überhaupt eine Teilung stattgefunden hat. Fehlt diese Meldung, muss wie bei einer ungeplanten Zugtrennung verfahren werden (siehe letzten Abschnitt dieses Unterkapitels).

Meldet sich eine Fahrzeugbewegung mit bekannter Position von Zugspitze und Zugende innerhalb der Fahrzeugbelegungsbeanspruchung einer bisherigen umfangreicheren Fahrzeugbewegung an, muss das bisherige Objekt der Fahrzeugbewegung im Datenmodell der smartLogic ersetzt werden. Anhand der gesendeten Daten kann ein passendes Fahrzeugbewegungsobjekt mit einer Beanspruchung zwischen Zugspitze und Zugende im von der Fahrzeugbewegung belegten Gleisabschnitt erstellt werden.

Damit die verbliebenen Fahrzeuge, die nicht in der sich zuerst wieder angemeldeten Fahrzeugbewegung enthalten sind, der smartLogic weiterhin bekannt sind, müssen um sie ebenfalls neue Fahrzeugbelegungsbeanspruchungen erstellt werden. Dabei sind bis zu zwei Beanspruchungen erforderlich: je eine vor und hinter der neuen Fahrzeugbewegung. Befindet sich die neue Fahrzeugbewegung bereits am Rand der Fahrzeugbelegungsbeanspruchung der vorherigen Fahrzeugbewegung, ist eine weitere Beanspruchung ausreichend. Bei Anmeldung einer weiteren Fahrzeugbewegung, die aus der ehemaligen Fahrzeugbewegung entstanden ist, wird der Vorgang wiederholt.

Im Fall, dass die Position des sich neu anmeldenden Fahrzeugs nicht eindeutig bekannt ist, muss dieses seine Position zunächst mit langsamer Geschwindigkeit und auf Sicht „erfahren“ (vgl. Kapitel 2.2.2). Auch bei Teilungen von Fahrzeugbewegungen würde eine infrastrukturseitige Ortungstechnologie wie Achszähler in den Bereichen, in denen normalerweise Teilungen stattfinden,

die Sicherheit erhöhen, beispielsweise um sicherzustellen, dass eine geplante Teilung einer Fahrzeugbewegung der smartLogic in jedem Fall bekannt wird.

(ungeplante) Zugtrennung

Neben geplanten Teilungen von Fahrzeugbewegungen können auch ungeplante Zugtrennungen nicht ausgeschlossen werden, z. B. falls eine Fahrzeugbewegung ein oder mehrere Fahrzeug(e) (Wagen) verliert. In diesem Falle sollte ebenfalls geklärt werden, wie verfahren werden kann.

Verlorene Fahrzeuge werden zunächst durch die Ortungstechnologie registriert. Die Registrierung kann entweder direkt im Fahrzeug mittels geeigneter Sensoren erfolgen oder im Ortungsinformationsaggregator wird festgestellt, dass die Position der Zugspitze und des Zugendes in unrealistischem Maße voneinander entfernt liegen. Da es sich um ein unvorhergesehenes Ereignis handelt, sollte ein entsprechender Reaktionsprozess gestartet werden, durch den der zu erwartende Schaden identifiziert und das Schadensausmaß begrenzt wird.

Ist bei der ursprünglichen Fahrzeugbewegung die neue Länge bekannt, kann das Objekt der Fahrzeugbewegung in seinen Ausmaßen an die neue Situation angepasst werden. Ansonsten muss die neue Länge erst durch die Fahrzeugbewegung, externe Sensoren oder den Menschen ermittelt werden.

Für den abgetrennten Teil der ursprünglichen Fahrzeugbewegung erscheint es aufgrund der Verknüpfung mit dem Reaktionsprozess sinnvoller, zunächst eine DA einzurichten (vgl. Kapitel 7.3.7), die später wieder in eine Fahrzeugbewegung umgewandelt werden kann. Kann der abgetrennte Zugteil sicher und vollständig geortet werden, können die Ausmaße der DA an diese Position angepasst werden.

Können die abgetrennten Fahrzeuge der ursprünglichen Fahrzeugbewegung nicht vollständig geortet werden, muss davon ausgegangen werden, dass sie sich an beliebiger Stelle im Gleisabschnitt zwischen der letzten bekannten Position des Zugendes der ursprünglichen Fahrzeugbewegung und der aktuellen Position der Fahrzeugbewegung befindet. Je nach Neigung des Gleises ist sogar denkbar, dass die abgetrennten Fahrzeuge aus diesem Gleisabschnitt herausrollen. Die erforderliche Ausdehnung der DA muss daher vom Reaktionsprozess auf Basis der möglichen erreichbaren Position der abgetrennten Fahrzeuge ermittelt werden. Mit einem Positionsupdate kann die DA entsprechend angepasst werden.

Sobald die abgetrennten Fahrzeuge wieder geortet wurden, können sie gemäß dem beschriebenen Verfahren zur Fahrzeugbewegungsvereinigung wieder mit einer anderen Fahrzeugbewegung vereinigt werden und die Fahrt der vereinten Fahrzeugbewegung kann fortgesetzt werden.

8.4.4 besondere Fahrzeuge / außergewöhnliche Sendungen

Einige der Prüfbedingungen aus dem im 6. Hauptkapitel ermittelten Funktionskatalog haben besondere Fahrzeuge und Sendungen zum Inhalt. Die Durchführung von Fahrzeugbewegungen mit solchen besonderen Fahrzeugen gehört zu den gewünschten, betrieblichen Funktionen (vgl. Kapitel 6.3). Die Prüfbedingungen beziehen sich zum Beispiel auf außergewöhnlich große Fahrzeugbegrenzungslinien der beteiligten Fahrzeuge (in der klassischen Eisenbahnsicherungstechnik wird der Begriff „Fahrzeuge mit Lademaßüberschreitung“ genutzt) oder besonders hohe Radsatzlasten/Achslasten bzw. spezielle Eigenschaften der Fahrzeuge.

Bei einer zu hohen Achslast kann der Fahrweg Schaden nehmen. Die Belastungen sind jedoch bei höheren Geschwindigkeiten größer, so dass ggf. in einem gewissen Bereich höhere Achslasten durch geringere Geschwindigkeiten kompensiert werden können. Theoretisch wäre es denkbar, die zulässige

Achslast nicht als einfachen Wert zu definieren, sondern in Abhängigkeit von der Geschwindigkeit eine Funktion anzugeben oder mehrere Klassen für verschiedene Geschwindigkeitsbereiche zu definieren. Dies könnte über die Gleisbereich-Objekte geschehen (vgl. Kapitel 7.3.8).

Lademaßüberschreitungen wirken sich, wie oben erwähnt, auf die Fahrzeugbegrenzungslinien (Grenzlinien) der Fahrzeugbewegung aus, mit dem sich bereits Kapitel 7.3.9 ausführlich beschäftigt. Die dortige Unterscheidung zwischen dem für den Ausschluss von Kollisionen mit der Infrastruktur relevanten Lichtraumprofil und den Grenzlinien für den Ausschluss von Kollisionen mit anderen Fahrzeugen ermöglicht bereits eine differenzierte Betrachtung verschiedener Fälle von Lademaßüberschreitungen. Werden dabei durch eine beantragte Fahrerlaubnis oder die tatsächliche Fahrzeugbelegung die Grenzlinien eines Nachbargleises verletzt, ist eine entsprechende Beanspruchung auf diesem Nachbargleis einzurichten (Clearance Gauge Violation Occupation). Soll eine Fahrt auf diesem Gleis stattfinden, müssen die tatsächlichen Fahrzeugausmaße mit der Grenzlinienverletzung abgeglichen werden. Damit kann die Befahrbarkeit flexibel an die tatsächliche Ausdehnung der Fahrt angepasst werden. Die Beachtung des Lichtraumprofils verhindert dabei eine Kollision mit der Infrastruktur.

Es ist allerdings davon auszugehen, dass die Zulässigkeit von Fahrzeugbewegungen mit besonderen Fahrzeugen oder Sendungen über die oben geschilderten Fälle hinaus auch zukünftig eine manuelle Prüfung benötigt, da in Hinblick auf die globale Anforderung der *schlanken Logik* nicht jeder erdenkliche Spezialfall in der Logik berücksichtigt werden kann.

Eine eingehendere Auseinandersetzung mit diesem Thema erfolgt aufgrund der in Kapitel 7.3.9 genannten Gründe in dieser Arbeit nicht.

8.4.5 Zuordnung eines Stellelements zur smartLogic ändern

Zwei eigenständige globale Anforderungen fordern die Möglichkeit der flexiblen Infrastrukturzuordnung zum Zuständigkeitsbereich der smartLogic ein (vgl. Kapitel 8.2.1), wofür im Funktionskatalog auch betriebliche Funktionen existieren (vgl. Kapitel 6.3); mit diesen Funktionen beschäftigt sich das vorliegende Unterkapitel. Demnach sollen als betriebliche Funktionen sowohl Infrastrukturelemente ohne Neuzulassung hinzugefügt oder entfernt werden können (erster Abschnitt), als auch zur Laufzeit eine flexible Zuordnung der Elemente zum Zuständigkeitsbereich der smartLogic möglich sein (zweiter Abschnitt). Dabei ist auch zu untersuchen, ob es Einschränkungen der möglichen Zeitpunkte für das Ausführen dieser betrieblichen Funktionen gibt (dritter Abschnitt).

Hinzufügen oder Entfernen von Infrastruktur- bzw. topologischen Elementen

Gemäß den im 6. Hauptkapitel identifizierten funktionalen Sicherheitsanforderungen sind bei den beiden genannten betrieblichen Funktionen verschiedene Sicherheitsanforderungen zu berücksichtigen. So muss sichergestellt sein, dass kein Element vorhanden ist, welches nicht erkannt wird. Insbesondere darf kein Element entfernt werden, welches noch benötigt wird. Die Sicherheit des der Logik zugrundeliegenden Gleisplans muss garantiert sein.

Da gemäß Kapitel 4.4.3 Gleistopologie und Infrastrukturdaten aus einer sicheren Datenquelle gelesen werden, muss untersucht werden, welche der oben identifizierten Sicherheitsanforderungen noch von der smartLogic geprüft werden müssen und welche bereits dadurch abgedeckt sind, dass geprüfte und damit sichere Daten über die Infrastruktur und die Gleistopologie vorliegen. Die primäre Prüfung der Korrektheit der Infrastrukturdaten ist aufgrund der Annahme der sicheren Datenquelle nicht Aufgabe der smartLogic. Dennoch wäre es möglich, bei einer Änderung der Infrastrukturdaten eine Plausibilitätsprüfung durchzuführen. Zum Beispiel könnte geprüft werden, ob Infrastrukturelemente

als Stakeholder oder stellbares Fahrwegelement registriert sind, die keine Entsprechung in der Topologie haben. Umgekehrt könnte geprüft werden, dass alle topologischen Elemente, die mit einem physischen stellbaren Fahrwegelement verknüpft sind, auch mit entsprechenden Infrastrukturelementen verknüpft sind. Inwieweit solche Überprüfungen Dopplungen zu den Tests wären, mit denen auf Seiten der sicheren Datenquelle die Sicherheit der Daten überprüft wird, kann in dieser Arbeit nicht beurteilt werden.

Bei einer Registrierung neuer Infrastrukturelemente in der smartLogic ist jedoch eine Prüfung, ob das zu registrierende Objekt eine korrekte Verortung auf der Topologie hat, auf jeden Fall sinnvoll. Bei einer Deregistrierung könnte geprüft werden, ob nach wie vor ein befahrbarer Gleisplan besteht.

Neuzuordnung von Infrastruktur- oder topologischen Elementen zu anderen Kontrollbereichen

Durch die Neuzuordnung eines Infrastruktur- oder topologischen Elements zu einem neuen Kontrollbereich ändern sich die physischen Gegebenheiten nicht. Die einzige notwendige Überprüfung ist daher, dass jedes Element einem aktiven Kontrollbereich zugeordnet ist.

Um Konsistenz zu erhalten und die Übersichtlichkeit für den Bediener zu gewährleisten, erscheint es nicht sinnvoll, nur einzelne Elemente neu zuzuordnen. Stattdessen wäre es praxisnäher, verschiedene Betriebszustände mit unterschiedlichen Zuordnungen zu definieren, zwischen denen umgeschaltet werden kann (ähnlich wie bei Bauzuständen).

Zulässige Zeitpunkte für Veränderungen

Zu diskutieren bleibt, ob es Einschränkungen für den Zeitpunkt von Veränderungen an der Infrastruktur bzw. der Neuzuordnung von Elementen zu Kontrollbereichen gibt. Ist eine Veränderung

- jederzeit möglich oder
- nur möglich, wenn ein Element derzeit nicht beansprucht wird?

Eine *Deregistrierung* von beanspruchten Elementen zum Zwecke einer der beiden in diesem Unterkapitel besprochenen betrieblichen Funktionen der smartLogic erscheint nicht sinnvoll zu sein, da bei diesem Prozess die Beanspruchung verloren gehen könnte und daraus ein Sicherheitsproblem entstehen würde (*Kernanforderung der sicheren Logik*). Bei einer *Neuregistrierung* eines Infrastrukturelementes oder topologischen Elements muss analog vorab geprüft werden, ob ein angrenzendes Gleissegment eine Beanspruchung hat, auf die sich das neue Element auswirken könnte.

Bei der *Neuzuordnung* sind die Sicherheitsrisiken geringer, da es keine physischen Änderungen gibt. Allerdings muss sichergestellt werden, dass der aktuelle Zustand in Form von sicherheitskritischen Beanspruchungen nicht verloren geht. Die einfachste Lösung wäre es jedoch auch im Fall von Neuzuordnungen, Infrastrukturelemente nur neu zuzuordnen, wenn keine Beanspruchungen für diese Elemente existieren. Diese Vorgehensweise könnte jedoch zu Problemen führen, wenn z. B. in großen Knoten von Tag- auf Nachtschicht umgestellt werden soll, da zu diesen Zeiten selten alle Elemente, die neu zugeordnet werden sollen, nicht beansprucht sein werden. Auch bei kleineren Anlagen existieren dauerhafte Beanspruchungen, wenn beispielsweise Fahrzeuge über einen längeren Zeitraum abgestellt sind. Aus diesen Gründen erscheint es sinnvoll, eine Möglichkeit zu schaffen, Elemente auch mit bestehenden Beanspruchungen neu zuzuordnen.

Eine solche Neuzuordnung von Elementen mit bestehenden Beanspruchungen kann mit einem generischen Datenmodell leicht erreicht werden, sofern auf eine zentrale Datenhaltung für alle Kontrollbereiche zurückgegriffen wird, in der die Objekte zentral hinterlegt sind. In diesem Fall muss nur die Zuordnung zum Kontrollbereich, die im Objekt in einer Variable gespeichert werden kann, geändert werden, das Originalobjekt bleibt aber bestehen.

8.4.6 Tunnelbegegnungsverbot

Ein in letzter Zeit in Deutschland diskutierter Spezialfall ist das Tunnelbegegnungsverbot. Hintergrund ist die Anordnung des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI), dass sich ab einer bestimmten Geschwindigkeit Güterzüge und Personenzüge wegen der Gefahr von sich lösender Ladung nicht mehr begegnen dürfen [BMVI 2017]. Das Tunnelbegegnungsverbot eignet sich gut zur Demonstration des generischen Ansatzes der Prüfprozesse der Sicherungslogik.

Die Anordnung des BMVI geht von absoluten Geschwindigkeitsgrenzwerten zur Auslösung des Begegnungsverbots aus. Denkbar wäre jedoch auch, dass zukünftig die Geschwindigkeitsdifferenz der sich begegnenden Fahrzeugbewegungen (= Relativgeschwindigkeit der Fahrzeugbewegungen zueinander) als maßgeblich betrachtet wird. Daher sollten beide Fälle betrachtet werden.

In beiden Fällen kann die funktionale Sicherheitsanforderung des Tunnelbegegnungsverbots über RAs generisch modelliert werden (vgl. Kapitel 7.3.6), bei der die beiden Gleise für sich gegenseitig Detektions- und Wirkabschnitt bilden. Dasselbe Vorgehen ist theoretisch auch für mehr als zwei Gleise möglich. Als durch die RAs implizierte Einschränkung könnte entweder eine Befahrbarkeitssperre (Fahrtausschluss) oder eine Einschränkung der zulässigen Geschwindigkeit wirkungsvoll sein.

Dabei werden für jedes Gleis zwei RAs mit verschiedenen Einschränkungen benötigt (vgl. auch Abb. 65):

1. Für den Fall, dass zunächst ein Personenzug mit einer Geschwindigkeit oberhalb des Wertes, ab dem das Tunnelbegegnungsverbot greift, ein Gleis im Tunnel und damit den Detektionsabschnitt des Nachbargleises beansprucht, würde sich im Nachbargleis – dem Wirkabschnitt dieser RA – die Einschränkung auf nachfolgende Güterzüge beziehen.
2. Im umgekehrten Fall würde zunächst ein Güterzug einfahren und damit eine Einschränkung der zulässigen Geschwindigkeit für einen nachfolgenden Personenzug im Nachbargleis hervorrufen.

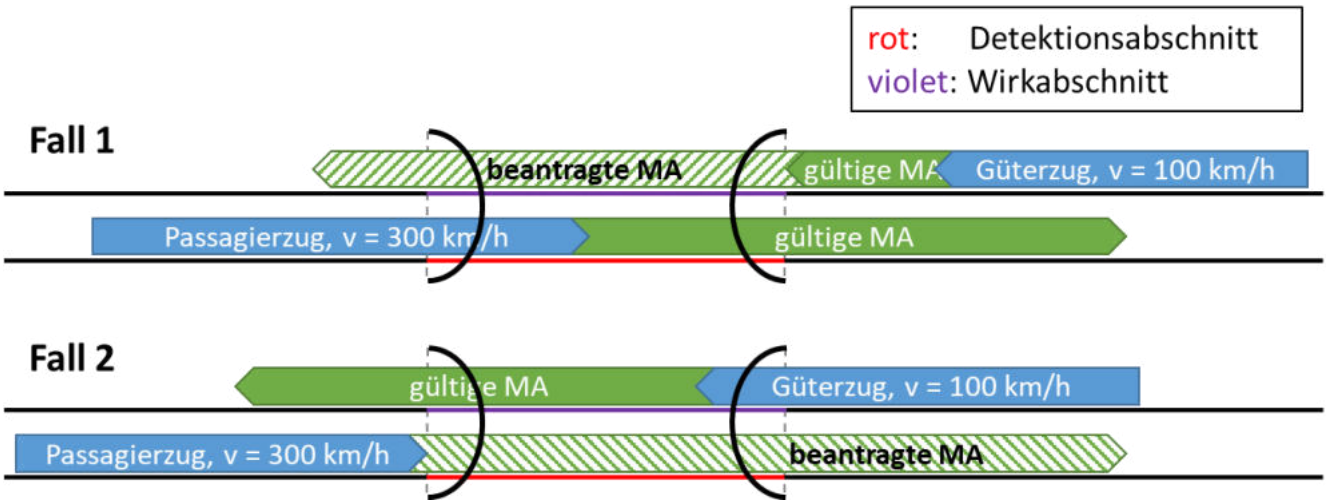


Abb. 65: Beispielfälle Tunnelbegegnungsverbot
[Eigene Darstellung]

Das TMS kann entscheiden, welcher der beiden Züge zuerst eine Fahrerlaubnis bis in den Tunnel bekommt, damit den Tunnel zuerst beansprucht und ihn ohne Einschränkung passieren kann.

Wenn angenommen wird, dass die dem Tunnelbegegnungsverbot zugrundeliegende Gefahr mit der Relativgeschwindigkeit der beteiligten Züge steigt, müsste die Schwere der Einschränkung im Idealfall

in einem bestimmten Intervall zwischen der Schwelle für die maximale Einschränkung (Fahrtausschluss) und der Grenze, ab der keine Einschränkung mehr gilt, relativ zur Geschwindigkeit verlaufen. In diesem Fall würde die erlaubte Geschwindigkeit für die eingeschränkte Fahrzeugbewegung relativ zur (Zunahme der) Geschwindigkeit der anderen Fahrzeugbewegung abnehmen.

Alternativ könnten Einschränkungsklassen definiert werden. Dies wären Geschwindigkeitsfenster der Fahrzeugbewegung auf dem Detektionsabschnitt, die jeweils eine maximale Geschwindigkeit für die Fahrzeugbewegung auf dem Wirkabschnitt definieren. Im vereinfachten Fall könnte die Anzahl der Klassen auf die beiden Extremfälle „volle Einschränkung“ und „keine Einschränkung“ reduziert werden.

Bei der räumlichen Geltung der Einschränkung ist zu beachten, ob es sich

1. um ein komplettes Fahrverbot oder
2. nur eine reduzierte Geschwindigkeit handelt.

Im ersten Fall eines kompletten Verbots, muss die Fahrzeugbewegung, der die Einfahrt in den Tunnel verwehrt ist, vor dem Tunnel zum Halten kommen, denn sonst würde ja eine Begegnung im Tunnel stattfinden[59]. Muss die Fahrt dagegen nur verlangsamt werden, ist es ausreichend, wenn die reduzierte Geschwindigkeit an dem Punkt erreicht ist, an dem die Begegnung beginnt. Dieser Punkt kann auch erst innerhalb des Tunnels liegen.

Um den zweiten Fall zu realisieren, müsste ein entsprechender Treffpunkt berechnet werden. Dabei müsste vom schlechtesten Fall ausgegangen werden, also davon, dass die Fahrzeugbewegungen jeweils ihre beantragte bzw. bereits genehmigte Fahrerlaubnis mit maximaler Geschwindigkeit ausfahren. Als Ausgangspunkt müssten die jeweiligen Max Safe Front End genommen werden, denn sie markieren bei Annahme, dass die beiden Fahrzeugbewegungen in entgegengesetzte Richtungen verkehren, den vom zu berechnenden Treffpunkt aus gesehen nächsten Punkt, an dem sich die Zugspitze zum letzten bekannten Ortungszeitpunkt befunden haben kann. Zur Realisierung des zweiten Falls müsste zudem das Konzept der RA erweitert werden, um als Einschränkung auch bedingte Geschwindigkeitsvorgaben zu erlauben, die sich nicht auf den kompletten Wirkabschnitt beziehen, sondern deren räumliche Geltung von einer Bedingung, wie dem Treffpunkt mit einer anderen Fahrzeugbewegung, abhängt.

Neben dem räumlichen Geltungsbereich der Einschränkung ist auch ihr zeitlicher Geltungsbereich zu analysieren. Beim Konzept der RA wird dieser zeitliche Geltungsbereich normalerweise durch den Zeitpunkt der Beanspruchung des entsprechenden Detektionsabschnitts vorgegeben. Eine solche Beanspruchung liegt bereits vor, wenn für die Befahrung des Tunnels eine Fahrerlaubnis vorliegt. Zwar kann die Gefährdung erst eintreten, wenn der Bremsweg der Fahrzeugbewegung in den Tunnel hineinragt, ein Kapazitätsproblem entsteht durch das Knüpfen der Einschränkung an die Beanspruchung einer Fahrerlaubnis jedoch nicht, da das TMS die Fahrerlaubnis so verlängern kann, dass keine andere Fahrzeugbewegung unnötig behindert wird.

In der Praxis stellt sich vor allem auch das Problem, dass sicher unterschieden werden muss, um welche Art von Fahrzeugbewegung (Personenzug oder Güterzug) es sich handelt. In der smartLogic wird allerdings vorausgesetzt, dass dieses Problem durch geeignete Sensortechnik oder organisatorische Maßnahmen gelöst werden kann. Ist bei Befahren eines der Detektionsabschnitte

[59] Es sei denn, beide Züge verkehren in dieselbe Richtung und der Personenzug holt den langsameren Güterzug im Tunnel ein. Dieser Fall wird jedoch hier nicht näher betrachtet.

keine Information über die Art der Fahrzeugbewegung vorhanden, ist dies für die Funktionsweise der Logik kein Problem. Die vorgesehene Einschränkung muss dann allerdings auf den verbundenen Wirkabschnitten aufgrund der Kernanforderung der sicheren Logik auf jeden Fall gelten (restriktivere Möglichkeit). Die Folge wäre also ggf. eine Einschränkung der Kapazität.

8.5 Basis-Prüfprozesse

In diesem Kapitel werden die Basisprüfprozesse der Logik erarbeitet, die den Kern der Funktionsweise der smartLogic beschreiben. Die Basisprüfprozesse wurden in Kapitel 6 im Rahmen der Funktionsanalyse identifiziert (vgl. Tab. 26 in Kapitel 6.7). Die einzelnen Prozesse werden nach der in Kapitel 8.2 entwickelten Methode und Vorgehensweise hergeleitet und modelliert. Die Modellierung baut zudem auf den Überlegungen zu den Basis-Konzepten sowie den Konzepten für Spezialfälle aus den Kapiteln 8.3 und 8.4 sowie auf dem Datenmodell aus Kapitel 7 auf.

Um die Lesbarkeit der einzelnen Unterkapitel zu erhöhen, kommt es an einigen Stellen in diesem Kapitel zu redundanten Formulierungen zu Kapitel 8.2.2 und zwischen den einzelnen Unterkapiteln dieses Kapitels. Die (fast) identischen Wortlaute sind explizit gewollt, um zu verdeutlichen, dass es sich jeweils um den gleichen Schritt des Ablaufs zur Modellierung der Prozesse der smartLogic handelt.

8.5.1 RA Change Request

Gemäß dem Konzept der Restricted Areas (RAs) muss das TMS das Anlegen, Löschen oder Verändern von bestehenden RAs bei der smartLogic beantragen können (vgl. Kapitel 7.3.6 und 8.3.3). Aus Gründen der Übersichtlichkeit wird angenommen, dass diese Funktionen mittels eines gemeinsamen Prüfprozesses von der smartLogic abgedeckt werden können. Dieser Prüfprozess wird im vorliegenden Unterkapitel erarbeitet.

Da es auch vorkommen kann, dass RAs innerhalb von anderen Prüf- oder Reaktionsprozessen angelegt oder verändert werden müssen, z. B. wenn in Folge einer Notfallmeldung mittels eines Reaktionsprozesses ein Gleisabschnitt gesperrt werden muss, wird ein Großteil des Prüfprozesses in eine Subroutine ausgelagert, die von der Prozessfunktion aufgerufen wird. Um das Verständnis des Prüfprozesses zu ermöglichen, wird diese Subroutine in diesem Kapitel zusammen mit der Prozessfunktion erarbeitet und vorgestellt.

Identifizieren der für den Prüfprozess und die zugehörigen Subroutine relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für den Prozess relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren. Wie in Kapitel 8.2.2 beschrieben, erfolgt die Einstufung als relevant auf Basis der persönlichen Erfahrung mit der Hilfe einiger allgemeingültiger, abstrakter[60] Kriterien. Bezogen auf den vorliegenden Prozess ist das Hauptkriterium, dass die Prüfbedingung als Subjekt oder Objekt eine RA oder eine Bedingung, die als RA im Datenmodell abgebildet werden kann, enthält.

Bei der Identifizierung der relevanten Prüfbedingungen stellte sich heraus, dass sich zwar viele Prüfbedingungen darauf beziehen, dass bestimmte RAs vorhanden sein müssen, aber nur wenige Prüfbedingungen beziehen sich konkret auf den Ablauf des betrachteten Prüfprozesses zur Einrichtung oder Anpassung von RAs. Der zu entwickelnde Prozess soll allerdings nicht sicherstellen, dass alle

[60] Spezifischere Kriterien konnten vom Autor aufgrund der in Kapitel 8.2.2 beschriebenen Gründe nicht identifiziert werden.

erforderlichen RAs in den topologischen Daten vorhanden sind (das würde das von der smartLogic Leistbare überschreiten, vgl. Annahme zur Verfügbarkeit einer sicheren Datenquelle für Topologiedaten in Kapitel 4.4.3), sondern nur, dass neue RAs sicher hinzugefügt und nicht mehr benötigte RAs sicher gelöscht oder modifiziert werden können. Deshalb sind nur die Prüfbedingungen relevant, die sich auf die Einrichtung und Anpassung der RAs beziehen.

Zu den relevanten Prüfbedingungen gehören allerdings solche, die bedingen, dass RAs nicht vorzeitig gelöscht oder modifiziert werden dürfen, solange sie noch gebraucht werden. Im Sinne der Anforderung der generischen Logik wurde hierfür das Konzept der Löschbedingungen entworfen, die im RA-Objekt hinterlegt werden können (siehe Kapitel 7.3.6, Abschnitt „Löschbedingungen“). Deshalb können die Prüfbedingungen zu diesem Themenbereich zu einer generischen Prüfbedingung zusammengefasst werden.

Tab. 48: Relevante Prüfbedingungen für den RA Change Request

ID	Beschreibung	ggf. Bemerkung
F-E000a	die smartLogic muss korrekt arbeiten	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.
F-E000b	die Nachricht muss bekannt und die Syntax korrekt sein	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.
F-E122	Einschränkungen, die eine RA vorgibt, müssen eingehalten werden	
diverse	bestehende RAs dürfen nicht gelöscht oder so modifziert werden, dass existierende Einschränkungen nicht mehr modelliert sind	generische Zusammenfassung einer Reihe von Prüfbedingungen, die Anforderungen an die vorhandenen RAs stellen, wird über die Löschbedingungen abgedeckt (vgl. Kapitel 7.3.6)

Ablauf des Prüfprozesses in natürlicher Sprache

Die Vorformulierung des Prüfprozesses (und der zugehörigen Subroutine) in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Prozessablauf zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf den betrachteten Prozess auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit des Prüfprozesses (und der Subroutine) ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt. Da nur wenige relevante Prüfbedingungen existieren, müssen keine ausführlichen Überlegungen zur Reihenfolge der Prozessschritte angestellt werden.

Bei der Erarbeitung des Ablaufs stellt sich die Frage, ob

1. eine neue RA nur Auswirkungen auf die Prüfung zukünftiger Prüfanfragen hat oder
2. auch Auswirkungen auf aktuelle Fahrzeugbewegungen, die bereits eine Fahrerlaubnis für den Wirkabschnitt haben, bestehen.

Im zweiten Fall müsste davon ausgegangen werden, dass nicht alle Fahrzeugbewegungen mit gültiger Fahrerlaubnis für den Wirkabschnitt der RA die durch die RA vorgegebenen, neuen Anforderungen erfüllen können. Beispielsweise kann nicht davon ausgegangen werden, dass bei einer plötzlich auftretenden neuen RA, die eine verminderte Geschwindigkeit vorschreibt, noch alle Fahrzeugbewegungen rechtzeitig bremsen können. Gegebenenfalls würde die neue RA dann eine Sicherheitsreaktion (Reaktionsprozess, vgl. Kapitel 8.7) hervorrufen. Aufgrund der negativen

Auswirkungen hierdurch sollte dieses Vorgehen nur im Gefahrfall verwendet werden. Zur Abgrenzung des Gefahrfalls vom Prozess der Etablierung zukünftig zu beachtender Einschränkung mittels RA wurde in Kapitel 7.3.7 das Konzept der Danger Area (DA) eingeführt. Daher wird an dieser Stelle angenommen, dass RAs nur Auswirkungen auf zukünftige Prüfanfragen haben.

1. Prüfe die Funktionsfähigkeit der smartLogic
2. Prüfe die Anfrage auf syntaktische Korrektheit
3. Falls eine RA aufgelöst werden soll, prüfe, ob die Löschbedingungen (Deletion Conditions) erfüllt sind (vgl. Kapitel 7.3.6, Abschnitt „Löschbedingungen“).
4. Bestimme die Gleissegmente, die zum Wirkabschnitt und ggf. Detektionsabschnitt der RA gehören[61] (bei einer beantragten Änderung kann sich die Ausdehnung der Abschnitte vor und nach der Änderung unterscheiden, in diesem Fall sind alle Segmente zu bestimmten)
5. Ändere die Eintragung der RA auf den betroffenen Gleissegmenten
6. Sende eine Rückmeldung über das Ergebnis des Prozesses (Request Return Message RRM) an das TMS

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Da RAs interne Informationsobjekte der smartLogic sind, sind beim RA Change Request außer dem TMS als aufrufende Instanz keine weiteren externen Systeme beteiligt.

Aktivitätsdiagramm

Zur Beschreibung des Prozesses „MP Change Request“ wurde das in Abb. 66 dargestellte Aktivitätsdiagramm erstellt. Der gestrichelte Teil grenzt die zugehörige Subroutine ab.

Folgende Abkürzungen werden im Diagramm verwendet:

- WFC: Write Failure Code (generiert einen entsprechenden Fehlercode)
- FC: Failure Code (Fehlercode)
- RA: Restricted Area
- RRM: Request Return Message

An den Verzweigungsknoten und den Ausgabe-Pins der Aktionen, die für Subroutinen stehen, ist dargestellt, welche Auswirkungen die Verletzung der jeweiligen Prüfbedingung hat. Die Einteilung erfolgt gemäß Tab. 42 in Kapitel 8.3.1. Im vorliegenden Beispiel sind die meisten Verzweigungsknoten rot eingefärbt. Das bedeutet, dass die Verletzung direkt zur Zurückweisung der Prüfanfrage führt. Grund hierfür ist, dass zu Beginn des Prüfprozesses die grundsätzliche Validität der Prüfanfrage geprüft werden muss. Ist die Validität nicht gegeben, muss das TMS eine erneute Anfrage stellen. Bei sofortiger Zurückweisung der Prüfanfrage wird ein Fehlercode generiert (vgl. Kapitel 7.7.1). Der Fehlercode wird am Ende des Prüfprozesses mit der Antwortnachricht an das TMS übermittelt, so dass das TMS den Fehler analysieren und eine erneute korrigierte Prüfanfrage stellen kann.

Falls kein Abbruchkritierium auftritt, kann am Ende des Prüfprozesses eine positive Antwortnachricht an das TMS generiert und an dieses versendet werden. Eine Gesamt-Schutzrate wird in diesem

[61] Wirkabschnitt und Detektionsabschnitt werden mit der angefragten RA vom aufrufenden Prozess übergeben (Neuanlegung, Änderung) bzw. können über das bestehende RA-Objekte hergeleitet werden (Löschung, Änderung) und bestehen als Gleisabschnitt jeweils aus einer Liste von Gleissegmenten.

Prozess nicht berechnet, da in diesem Prozess alle Verletzungen von Prüfbedingungen direkt zum Abbruch des Prozesses führen.

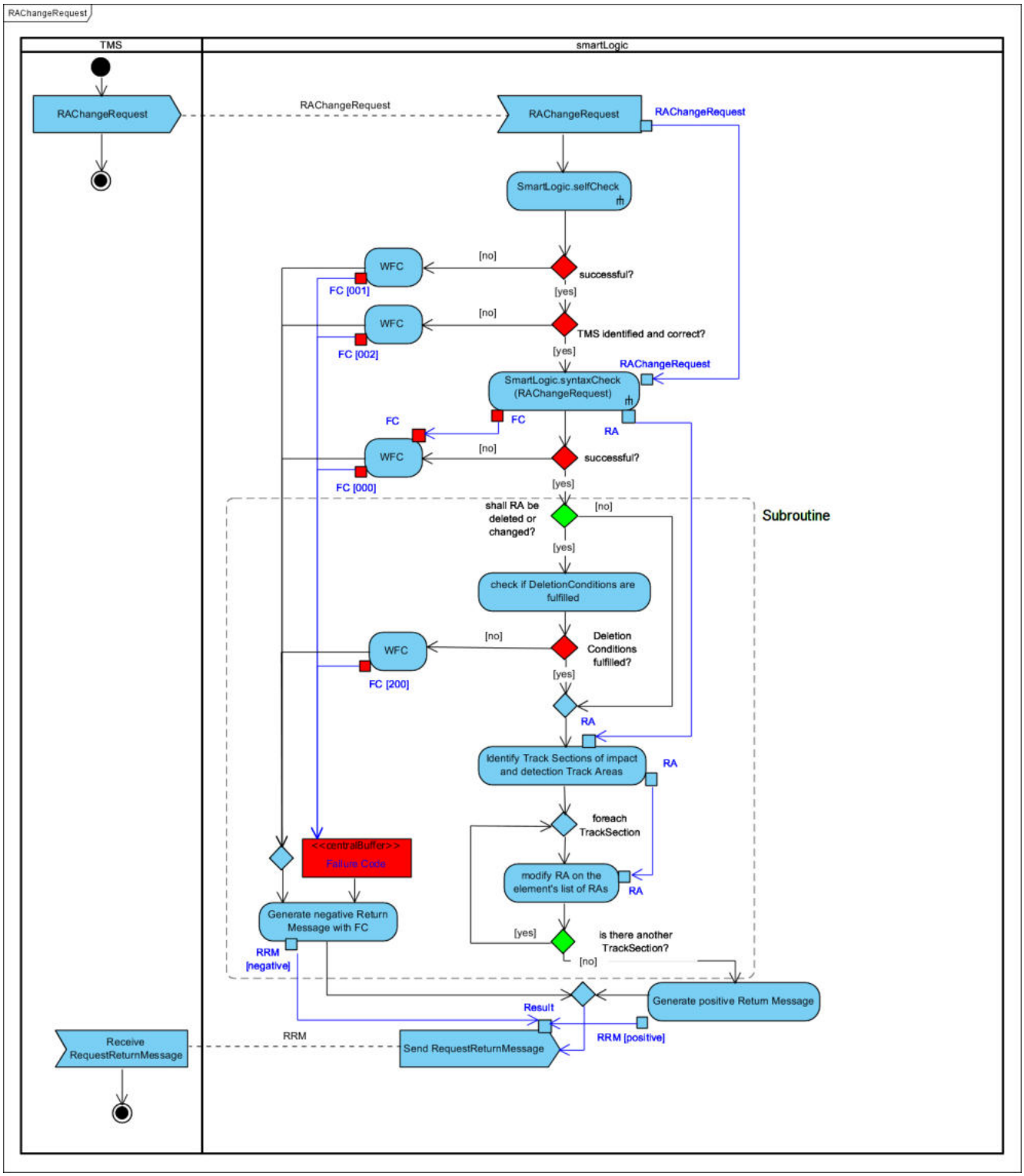


Abb. 66: Aktivitätsdiagramm für den Prozess „RA Change Request"
[Eigene Darstellung, erstellt mit Visual Paradigm]

Erneutes Überprüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von

Prüfbedingungen als nicht relevant zu überprüfen. Gegebenenfalls veränderte Einstufungen sind dabei iterativ in die bisher in diesem Unterkapitel vorgestellten Ergebnisse eingeflossen.

8.5.2 Verändern der Stakeholder-Listen

Gemäß dem Stakeholder-Registrierungs-Konzept ist ein Prozess zur Registrierung und Deregistrierung bzw. zur Veränderung bestehender Registrierungen von Stakeholder-Systemen auf Registrierungsschnittstellen erforderlich (vgl. Kapitel 8.3.3). Die Registrierung von Stakeholder-Systemen dient dabei dazu, zusätzliche Sicherheitsanforderungen generisch in der smartLogic abzubilden und zur Laufzeit verändern zu können.

Wenn ein Stakeholder-System eine zusätzliche Registrierung vornimmt, wird dadurch also eine zusätzliche Sicherheitsanforderung gestellt, die von der smartLogic unabhängig von anderen Sicherheitsanforderungen zu überwachen ist. Durch die Registierung sind damit keine direkten negativen Auswirkungen auf die Sicherheit zu erwarten. Allerdings besteht ein indirekter Einfluss auf die Sicherheit, wenn beispielsweise Stakeholder nicht oder fehlerhaft registriert sind. Dieses Problem kann jedoch nicht durch die Sicherungslogik behoben werden. Stattdessen ist ein Verfahren außerhalb des Funktionsumfangs der Sicherungslogik zu finden, mit dem die Vollständigkeit und Korrektheit der Stakeholder-Registrierungen sicherzustellen ist. An dieser Stelle muss daher angenommen werden, dass die Stakeholder-Systeme vollständig registriert sind.

Eine zusätzliche, fehlerhafte Registrierung würde gegebenenfalls zu einer nicht gerechtfertigten Einschränkung der Fahrmöglichkeiten, aber nicht zu einem Sicherheitsproblem führen. Bei einer Deregistrierung ist dagegen analog zum RA Change Request zu klären, ob sich die Deregistrierung nur auf neue Anfragen auswirkt oder auch auf bestehende Fahrerlaubnisse, die den zugehörigen Wirk- oder Detektionsabschnitt der Stakeholder-Registrierung beinhalten. Die flexibelste Lösung ist, wenn dies als Registrierungsparameter bei der Registrierung angegeben werden kann.

Aufgrund der großen Ähnlichkeit zum RAChangeRequest und weil, wie im vorletzten Absatz festgestellt, keine durch den Registrierungsvorgang verursachten Verletzungen von Prüfbedingungen zu erwarten sind, wurde an dieser Stelle auf eine komplette Modellierung des Prozesses verzichtet.

8.5.3 MP Request (Fahrerlaubnis)

Damit Fahrzeuge nicht gefährdet werden, dürfen sie nur mit einer Fahrerlaubnis auf der Eisenbahninfrastruktur verkehren. Die Kernaufgabe der smartLogic ist sicherzustellen, dass diese Fahrerlaubnisse sicher sind (vgl. Kapitel 6.3). Hierfür wird ein Prüfprozess zur Prüfung einer Fahrerlaubnisanfrage (Movement Permission Request), die gemäß der in Kapitel 4.3.1 hergeleiteteten Arbeitsaufteilung vom TMS beantragt wird, benötigt (vgl. zur Struktur des Requests Kapitel 7.7.1). Dieser Prüfprozess wird im vorliegenden Unterkapitel gemäß der in Kapitel 8.2.2 diskutierten Vorgehensweise entwickelt.

Identifizieren der für den Prüfprozess relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für den Prozess relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren. Wie in Kapitel 8.2.2 beschrieben, erfolgt die Einstufung als relevant auf Basis der persönlichen Erfahrung mit der Hilfe einiger allgemeingültiger, abstrakter[62] Kriterien. Bezogen auf den vorliegenden Prozess ist

[62] Spezifischere Kriterien konnten vom Autor aufgrund der in Kapitel 8.2.2 beschriebenen Gründe nicht identifiziert werden.

das Hauptkriterium, dass die Prüfbedingung eine Voraussetzung oder eine mögliche Einschränkung für das Befahren der Eisenbahninfrastruktur zum Inhalt hat.

Die Liste der für den MP Request relevanten Prüfbedingungen ist sehr umfangreich. Sie werden in Tab. 49 aufgeführt. Um die Übersichtlichkeit zu erhalten, sind in der Tabelle nur die Prüfbedingungen aufgeführt, die im Funktionskatalog gemäß der Systematik in Kapitel 6.6.1 den Basisprüfprozessen zugeordnet wurden.

In *kursiv* sind Prüfbedingungen gedruckt, die zunächst als relevant identifiziert, dann aber aufgrund einer eingehenderen Betrachtung wieder gestrichen wurden. Aus Gründen der besseren Übersichtlichkeit sind in der Spalte „Bemerkung“ zudem bereits Hinweise enthalten, wie die Prüfbedingung im Prüfprozess umgesetzt werden kann. Gibt es bezüglich der Umsetzung komplexere Fragen zu klären oder mehrere Lösungsmöglichkeiten, die eingehender diskutiert werden sollten, erfolgt diese Betrachtung im nächsten Abschnitt.

Zu beachten ist, dass die Formulierung „muss“ sich auf die Erfüllung der Prüfbedingung bezieht. Wenn die Prüfbedingung nicht vollständig erfüllt (und damit verletzt) ist, heißt das allerdings nicht automatisch, dass die Anfrage abgelehnt wird (vgl. Anforderung, dass der Prüfprozess nur abbrechen darf, wenn die Kernanforderung nicht erfüllt ist in Kapitel 8.2.1), jedoch wird zumindest die Schutzrate reduziert (vgl. hierzu Kapitel 8.3.1). Damit die Prüfanfrage dennoch genehmigt werden kann, müssten risikomindernde Einflüsse (wie z. B. eine niedrigere Geschwindigkeit als infrastrukturseitig erlaubt) in der Fahrerlaubnisanfrage bereits enthalten sein (vgl. Kapitel 8.3.1 und 8.3.6).

Tab. 49: Relevante Prüfbedingungen für den MP Request (Basisprüfbedingungen)

ID	Beschreibung	ggf. Bemerkung
F-E000a	die smartLogic muss korrekt arbeiten	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.
F-E000b	die Nachricht muss bekannt und die Syntax korrekt sein	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.
F-E034, F-E034a	Passagierzüge müssen für verkehrliche Halte an Bahnsteigen halten, die ausreichend lang sind	hat nach der Gefährdungsanalyse sicherheitskritische Implikationen in Hinblick auf den Schutz der Reisenden
F-E035a, F-E035b, F-E035c	Weichen, die keine Rückfallweichen sind, dürfen nicht aufgefahren werden, wenn sie - im Fahrweg liegen - im Gefahrpunktabstand bzw. Durchrutschweg liegen und über ein bewegliches Herzstück verfügen oder mit einem Riegel verschlossen sind	Forderung aus dem derzeitigen Lastenheft; dies kann generisch über die Prüfbedingung zum korrekten Elementstatus (F-E340) abgedeckt werden, über den Element-Status und damit verknüpfte Bedingungen sind auch besondere Bedingungen für Rückfallebenen möglich
F-E054	MAs dürfen nur an eindeutig identifizierbare Fahrzeuge herausgegeben werden	
F-E057	*das Fahrzeug darf keine MA bekommen, wenn es einen Trip mit ungeklärter Ursache gemacht hat*	*die Ursachen des Trips können im MP Request nicht geklärt werden; es sollte daher im entsprechenden Reaktionsprozess auf den ungeklärten Trip bzw. durch betriebliche Regeln sichergestellt werden, dass das Fahrzeug nicht vorzeitig in den Modus Post Trip wechselt und somit empfangsbereit für eine neue MA wird*

F-E121	die Streckengeschwindigkeit bzw. auf dem jeweiligen Gleis zulässige Geschwindigkeit darf nicht überschritten werden	ggf. differenziert nach Neigetechnik-Klassen (siehe auch F-E121b)
F-E121a	die Geschwindigkeit, die von Infrastrukturelementen vorgegeben wird, darf nicht überschritten werden	kann für verzweigende Fahrwegelemente über F-E121 abgedeckt werden; die Geschwindigkeiten werden über die Verknüpfungen der Gleissegmente angegeben; andere Elemente, die die Geschwindigkeit beeinflussen, müssen dies über die RA in ihrem Wirkabschnitt angeben, dann gilt F-E122
F-E121b	Geschwindigkeitsdifferenzierungen abhängig von vorhandener Neigetechnik müssen beachtet werden	Spezialfall von F-E121, muss bei F-E121 beachtet werden
F-E122	Einschränkungen, die eine RA vorgibt, müssen eingehalten werden	
F-E122a	Stopps in “Non Stopping Areas” (NAS) sind zu vermeiden	
F-E122b	die Geschwindigkeit, die eine zu passierende RA (z. B. TSR) vorgibt, darf nicht überschritten werden, (wenn die Fahrzeugbewegung die auf die Fahrzeugcharakteristik bezogenen Einschränkungen der RA erfüllt)	
F-E641	Geschwindigkeitsprofile in Ladeeinrichtungen und an Bahnsteigen müssen eingehalten werden	
F-E129	über Gleisbereiche angegebene, globale temporäre Geschwindigkeitsvorgaben müssen eingehalten werden	z. B. bei bestimmten Wetterereignissen mit großflächigem Einfluss (sonst ist die Angabe über eine RA sinnvoller, da Gleisbereiche für großräumige Einflüsse und RAs für kleinteilige Einflüsse konzipiert sind, vgl. Kapitel 7.3.8)
F-E141	Beschränkungen bei Sturm müssen beachtet werden	kann über RAs oder Gleisbereiche gelöst werden
F-E142, F-E143	Beschränkungen bei Eiszapfenbildungsgefahr müssen beachtet werden	kann über RAs gelöst werden
F-E144	Beschränkungen bei vereisten Schienen müssen beachtet werden	kann über RAs gelöst werden
F-E145	Beschränkungen bei Schnee auf den Schienen müssen beachtet werden	kann über RAs gelöst werden
F-E211	Beschränkungen durch DAs müssen beachtet werden	
F-E212a	*Fahrzeuge dürfen sich nicht in Gleisabschnitte strecken können, die von anderen Fahrzeugen beansprucht werden*	*entsprechende Sicherheitsreserven sind einzuplanen; es wird jedoch davon ausgegangen, dass dies bei der Ortungsinformationsaggregation geschieht*

F-E216	Fahrzeugbewegungen müssen an für sie vorgeschriebenen Betriebshalten halten	dies kann entweder durch das Setzen des Zielpunkts am Betriebshalt oder durch eine entsprechende Vorgabe im Geschwindigkeitsprofil erreicht werden
F-E217	alle erforderlichen Zustimmungen von externen Systemen müssen vorliegen	die externen Systeme registrieren entsprechende Wirkabschnitte (vgl. Kapitel 8.3.3)
F-E217a, F-E217b	alle erforderlichen Benachrichtigungen müssen gesendet und empfangen worden sein	die benachrichtigungspflichtigen Stakeholder-Systeme müssen dafür erreichbar und betriebsbereit sein
F-E252	die Route der MA darf keine mit Fahrzeugen beanspruchten Abschnitte enthalten	Ausnahmen gibt es in bestimmten Fällen für Veränderungen an der Fahrzeugzusammensetzung (vgl. Kapitel 8.4.3)
F-E227	die Route der MA darf keine Teile enthalten, die Teil einer anderen MA sind (Ausnahme: überlappende D-Wege)	Berücksichtigung gemäß dem Konzept zu den Zielpunkten in Kapitel 8.3.2
F-E230	es muss ausreichender Flankenschutz bestehen	Berücksichtigung gemäß dem Konzept zum Flankenschutz in Kapitel 8.3.4
F-E232a	*Schlüsselsperren im Flankenschutzraum müssen gesichert sein*	*vermutlich nicht relevant, da über allgemeine Regeln zum Flankenschutz abgedeckt*
F-E236	falls eingeschränkter Flankenschutz besteht, muss die Geschwindigkeit reduziert sein	funktionale Sicherheitsanforderung an die Rückfallebene; genaue Werte für die Reduktion hängen von der Schutzrate ab und werden in dieser Arbeit nicht ermittelt (vgl. Kapitel 3.3)
F-E239	die Einfahrt in Gleise, in denen sich Personen befinden, muss verhindert werden	kann über RAs oder DAs (je nachdem, ob der Aufenthalt geplant oder ungeplant ist) gelöst werden
F-E264	die maximale Schließzeit am Bahnübergang muss eingehalten werden	kann für das geplante Fahrprofil mit dem Registrierungsparameter „maximale kontinuierliche Beanspruchung“ über die BÜ-Stakeholder-Registrierung gelöst werden, siehe Kapitel 8.3.3 (bei ungeplant längeren Fahrzeiten muss ggf. eine Reaktion geplant werden, sofern die Fahrzeugbewegung nicht bereits auf dem BÜ steht; aufgrund der zeitlichen Rahmenbedingungen der Arbeit wird dies hier allerdings nicht weiter ausgeführt, siehe Einleitung zu Kapitel 8.7)
F-E265	Bahnübergänge müssen geschlossen und freigemeldet sein	kann gemäß Kapitel 8.3.3 über die Einbindung als zustimmungspflichtiges Stakeholder-System gelöst werden
F-E270, F-E270b, F-E631	Gleis-Arbeitsstellen müssen gesichert sein	kann über RAs gelöst werden
F-E275	es dürfen sich keine Arbeitsmaterialien innerhalb der Fahrzeugbegrenzungslinien befinden	bedeutet generischer, dass die Fahrzeugbegrenzungslinien auf der beantragten Route frei sein müssen; eine Verletzung muss detektiert werden und kann dann über eine DA gelöst werden

F-E276	Personen- und Güterzüge dürfen sich im Tunnel nicht begegnen, wenn eine bestimmte Relativgeschwindigkeit überschritten wurde	kann über RAs gelöst werden, siehe Kapitel 8.4.6
F-E282	es dürfen keine Hindernisse auf dem Gleis detektiert sein	kann jeweils nach Sensor-Meldung über DAs gelöst werden
F-E311	die Route der MA muss topologisch gültig sein	es muss eine durchgehende und befahrbare Verbindung vom Start- zum Zielpunkt über die im MP Request angegebenen Gleissegmente geben
F-E312	Fahrzeugbewegungen müssen sicher vor einem Gleisende zum Stehen kommen	der Zielpunkt muss also vor dem Gleisende auf einem Gleis liegen, siehe auch F-E311
F-E321	betrieblich gesperrte Gleise dürfen nicht befahren werden, außer mit spezieller Genehmigung	kann über RAs gelöst werden
F-E340	stellbare Fahrwegelemente auf der Route müssen den richtigen Status haben	
F-E350	Fahrzeuge dürfen nur auf für sie zugelassenen Gleisabschnitten verkehren	kann über Gleisbereiche oder RAs gelöst werden
F-E351	BoStrab-Gleise dürfen nur von dafür zugelassenen Fahrzeugen befahren werden	kann über Gleisbereiche oder RAs gelöst werden
F-E352	rein elektrisch angetriebene Fahrzeuge dürfen nur auf Gleisen verkehren, die mit einem auf dem Fahrzeug verfügbaren Stromsystem ausgerüstet sind	kann über Gleisbereiche oder RAs gelöst werden
F-E353	die Spurweite muss übereinstimmen	kann über Gleisbereiche oder RAs gelöst werden
F-E354	eines der erlaubten ATP (Zugbeeinflussungssysteme) muss auf dem Fahrzeug vorhanden sein	kann über Gleisbereiche oder RAs gelöst werden
F-E355	das Fahrzeug muss für den Fahrweg zugelassen sein	kann über Gleisbereiche oder RAs gelöst werden
F-E356	der Tf bzw. das ATO-System müssen für den Fahrweg zugelassen sein	kann über Gleisbereiche oder RAs gelöst werden
F-E357, F-E364	das Fahrzeug muss genügend Bremskraft für die Route haben	kann über Gleisbereiche oder RAs gelöst werden
F-E357a	Fahrzeugbewegungen mit geringem Zugkraftüberschuss dürfen beim Anfahren in steil geneigten Rampen nicht zum Stehen kommen	kann über Gleisbereiche oder RAs gelöst werden
F-E358	das Achslastprofil darf auf der Route nicht überschritten werden	kann über Gleisbereiche oder RAs gelöst werden
F-E359	das Lichtraumprofil bzw. die Fahrzeugbegrenzungslinien müssen eingehalten werden	siehe Kapitel 7.3.9

F-E361, F-E540	das Fahrzeug muss über eine betriebsbereite Magnetschienenbremse verfügen, wo dies gefordert ist	kann über Gleisbereiche oder RAs gelöst werden
F-E362, F-E540, F-E541	die Benutzung der Magnetschienenbremse muss verhindert werden, wo ihre Benutzung nicht erlaubt ist	die Information über entsprechende Abschnitte muss dem Fahrzeug vorgegeben werden
F-E363	weitere fahrzeugseitige Vorgaben müssen (je nach Bedarf) übermittelt und eingehalten werden	
F-E365	die Fahrerlaubnis darf nicht in einen nicht vollüberwachten Bereich führen, (wenn nicht entsprechende Sicherheitsregeln eingehalten werden)	
F-E411, F-E412	gefährliche Längs-Beschleunigungen bzw. seitliche Beschleunigungen müssen vermieden werden	tritt die Gefährdung ohne Befahrung einer Weiche auf, kann die Geschwindigkeits-einschränkung über dauerhaft bestehende RAs gelöst werden; tritt die Gefährdung nur in Zusammenhang mit einer Weiche auf, kann sie über eine RA gelöst werden, die einen Detektionsabschnitt unmittelbar hinter dem Verzweigungspunkt der Topologie auf dem Weichenstrang enthält, der vom Fahrzeug befahren wird
F-E431	Fahrzeugtüren dürfen nur geöffnet werden, wenn sich das Fahrzeug am Bahnsteig befindet	
F-E432	Trittstufen müssen zum richtigen Zeitpunkt ausgefahren werden	sie sollen weder, wo es nicht erlaubt ist, ausgefahren werden können, noch nicht ausgefahren werden, wo es geboten ist
F-E510, F-E512, F-E726, F-E726a	der Stromabnehmer muss an den richtigen Punkten gesenkt und gehoben werden	
F-E513	Fahrzeuge mit gehobenem Stromabnehmer dürfen nur Gleise mit Oberleitung benutzen	
F-E515	Fahrzeuge müssen mit der richtigen Geschwindigkeit Gleisabschnitte mit defekter oder nicht vorhandener Oberleitung befahren	
F-E611a, F-E613	Reisendenübergänge (RÜ) müssen geschlossen und freigemeldet sein und dies bleiben, solange die Fahrzeugbewegung den zugehörigen Gleisabschnitt beansprucht	
F-E632	Geschwindigkeitsbegrenzung in Baustellenbereichen müssen eingehalten werden	kann über RAs gelöst werden

F-E642	Fahrgäste müssen gewarnt werden, falls der Zug bei der Vorbeifahrt am Bahnhof eine festgelegte Geschwindigkeit überschreiten darf	kann über ein benachrichtigungspflichtiges Stakeholder-System erfolgen
F-E643	das Fahrzeug muss alle vorgeschriebenen Warnungen durchführen (z. B. Pfeifen, Läuten)	die Weitergabe der Warnungen und ihrer Zeitpunkte bzw. Standorte ans Fahrzeug muss sichergestellt werden
F-E704a	ein reduzierte Haftbeiwert muss dem Fahrzeug gemeldet werden	
F-E721	im Falle, dass technische Sicherheit an einem verzweigenden Fahrwegelement nicht gegeben ist, muss sichergestellt werden, dass das Element nur mit eingeschränkter Geschwindigkeit befahren werden darf	
F-E722	die Geschwindigkeit muss auf dem topologischen Abschnitt eines stellbaren Fahrwegelements stark reduziert werden, falls das Element manuell gesteuert wird	in Deutschland ist die noch zulässige Geschwindigkeit üblicherweise 5 km/h
F-E750	akute Gefahrenstellen dürfen nicht passiert werden	es wird davon ausgegangen, dass dies über die DAs abgebildet ist, die vom entsprechenden Reaktionsprozess direkt gebildet werden

Ablauf des Prüfprozesses in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Prozessablauf zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf den betrachteten Prozess auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden.

Die Vollständigkeit des Prozessablaufs ist dabei über das systematische Vorgehen zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt. Da im vorigen Abschnitt für den MP Request eine große Anzahl von Prüfbedingungen als relevant eingestuft wurden, sollen im Sinne der Anforderung der schlanken Logik im ersten Unterabschnitt dieses Abschnitts Möglichkeiten zur Verringerung der Anzahl der Prozessschritte untersucht werden.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen im Prüfprozesses bezogen auf die Kernanforderung der sicheren Logik mit Ausnahme der formalen Prüfungen der Funktionsfähigkeit der smartLogic und der Syntax der Prüfanfrage zu Beginn irrelevant. Die Reihenfolge wird daher nur durch nachgeordnete Anforderungen wie die Anforderung der geringen Latenz sowie praktische Abhängigkeiten (z. B. „Rufe Belegungen ab“ vor „Prüfe auf einen Konflikt“) bedingt. Auf Basis dieser Anforderungen wird im zweiten Unterabschnitt dieses Abschnitts eine Reihenfolge der Schritte des Prüfprozesses diskutiert und festgelegt.

Umfangreiche zu treffende Entscheidungen oder Erläuterungen zu einer speziellen Fragestellung in Bezug auf den Ablauf des MP Requests, die im Rahmen der Erarbeitung des Ablaufs aufgekommen sind, werden zur besseren Übersichtlichkeit in eigene Unterabschnitte dieses Abschnitts ausgelagert. Eine solche spezielle Fragestellung betrifft die im dritten Unterabschnitt thematisierte Rückabwicklung

des MP Requests, wenn es zum Abbruch des Prüfprozesses und damit zur Zurückweisung der zugrundeliegenden Prüfanfrage kommt. Weiterhin ist während der Erarbeitung des Ablaufs des MP Requests die spezielle Fragestellung aufgekommen, wann der richtige Zeitpunkt zum Überprüfen des Status der zustimmungspflichtigen Stakeholder-Systeme ist, die im vierten Unterabschnitt aufgenommen wird.

Der vollständige Ablauf des MP Requests in natürlicher Sprache findet sich im letzten Unterabschnitt.

Überlegungen zur Verringerung der Anzahl der Prozessschritte

Für die Formulierung des Prüfprozesses erscheint es sinnvoll, die große Anzahl der relevanten Prüfbedingungen in Tab. 49 zu verringern, indem die Prüfung von einigen Prüfbedingungen in Subroutinen ausgelagert wird. Eine weitere Möglichkeit bietet sich darin, mehrere Prüfbedingungen in einen generischeren Prüfschritt zusammenzufassen. Zur besseren Übersichtlichkeit wurden hierzu bereits in der Bemerkungsspalte von Tab. 49 Anmerkungen gemacht.

Eine gute Möglichkeit für eine generische Zusammenfassung von Prüfbedingungen bieten die generischen Konzepte der Restricted Areas (RA) bzw. der Danger Areas (DA), da mit den RAs bzw. DAs sicherheitsbedingte Einschränkungen flexibel definiert und dann in generischer Form abgeprüft werden können (siehe „RA/Track Restriction Check“).

Die Prüfbedingung F-E275 scheint bei erster Betrachtung für den „MP Request“-Prozess nicht relevant zu sein. Generisch kann die Anforderung jedoch auf die Überwachung des Lichtraumprofils bezogen werden. Demnach muss zumindest der Raum der Fahrzeugbegrenzungslinien frei bleiben. Eine Verletzung der Fahrzeugbegrenzungslinien muss detektiert werden. Es handelt sich also um einen Sensorinput, der eine DA und einen entsprechenden Reaktionsprozess zur Folge hat (siehe Kapitel 8.7). Im Prüfprozess „MP Request“ werden DAs ähnlich zu den RAs generisch abgeprüft.

Weiterhin bietet es sich an, die Prüfbedingungen F-E035a-c zum Auffahren von Weichen zum einen über den Element-Status abzudecken, da gemäß der EULYNX-Schnittstellen (vgl. Kapitel4.5.1 und 2.2.5) „aufgefahren“ ein Zustand der Weiche ist. Zum anderen definieren die Prüfbedingungen Fälle, in denen das Auffahren der Weichen mit einer höheren Sicherheit verhindert werden muss als in anderen Fällen (vgl. F-E035x). Dies ist für die Berechnung der Schutzrate in Bezug auf die Wahl der Zielpunkte relevant, da es nach den Überlegungen aus Kapitel 8.3.2 verschiedene Zielpunkte mit abgestufter Gefährdungsrisiko geben kann, da hinter dem ersten Zielpunkt (EoA) die Wahrscheinlichkeit abnimmt, mit der das Fahrzeug weitere Zielpunkte (SvL) noch erreicht (siehe „Target Point Check“).

Die Prüfbedingungen der Gruppe F-E35x sowie F-E361 bzw. F-E540 behandeln Eigenschaften des Fahrzeugs bzw. der Fahrzeugbewegung, die bei der Befahrung der beantragten Route erfüllt sein müssen bzw. bei Nichterfüllung einen signifikanten Einfluss auf die Schutzrate haben. Diese Prüfbedingungen können im Datenmodell über die generischen Konzepte der Gleisbereiche oder RAs abgebildet werden. Diese generische Formulierung ist im Sinne der Anforderung der Zukunftsfähigkeit auch erweiterbar, falls zukünftig weitere Anforderungen hinzukommen.

Die Prüfbedingungen F-E034, F-E034a, F-E363, F-E411, F-E412, F-E431, F-E432, F-E510, F-E512, F-E726, F-E515 definieren Einschränkungen, die in erster Linie das Fahrzeug sicherstellen muss. Zur Umsetzung gibt es prinzipiell zwei Möglichkeiten.

1. Die smartLogic kann bereits sehr genaue Vorgaben über generische Parameter wie das Geschwindigkeitsprofil oder die Wahl der Zielpunkte machen.

2. Die Aufgabe der smartLogic kann darauf beschränkt werden, sicherzustellen, dass das Fahrzeug alle benötigten Informationen erhält, z. B. wo sich ein Bahnsteig befindet, um selbstständig die Prüfbedingungen einzuhalten.

Für die erste Möglichkeit benötigt die smartLogic sehr detaillierte Informationen, beispielsweise über den Fahrplan. Fahrplaninformationen werden bisher jedoch als nicht sicherheitskritisch betrachtet. Gegen die erste Möglichkeit spricht also die globale Anforderung der schlanken Logik.

Bei der zweiten Möglichkeit müsste die Schnittstelle zum Fahrzeug die Übertragung aller relevanten Informationen erlauben. Gemäß Kapitel 4.5.2 wird in dieser Arbeit von ETCS als Schnittstelle zum Fahrzeug ausgegangen. Tatsächlich enthält ETCS eine Vielzahl von Möglichkeiten, um genaue Informationen zu übertragen. Falls benötigte Informationen dennoch nicht übertragen werden könnten, würde gegebenenfalls die Anforderung verletzt, bestehende Standardschnittstellen zu verwenden. Für diesen Fall bestünde notfalls jedoch noch die Möglichkeit einen (aufwändigen) Change Request bei der ERA zu stellen, um die ETCS-Spezifikationen und damit die bestehende ETCS-Schnittstelle zu erweitern. Aufgrund der bereits sehr umfangreichen ETCS-Schnittstelle ist eine Erweiterung der ETCS-Schnittstelle jedoch vorerst nicht erforderlich.

Unter Abwägung der Anforderungen wird die zweite Möglichkeit als zielführender bewertet und wird weiterverfolgt (siehe „Track Information Check“).

In eine ähnliche Kategorie wie die zuletzt genannten Prüfbedingungen fällt auch die Prüfbedingung F-E704a (Berücksichtigung eines reduzierten Haftbeiwerts). Allerdings handelt es sich um eine variable Information, die von Sensorwerten abhängig ist. Deshalb ist jedoch auch die Angabe über eine RA möglich (an dieser Stelle wird angenommen, dass sich der Haftbeiwert nicht so schnell verändert, dass eine DA und ein damit verbundener Reaktionsprozess notwendig wäre). Auf Basis der RA kann die Information über ETCS-Packet 71 an das Fahrzeug weitergegeben werden (siehe „RA/Track Restriction Check“).

Gemäß der Definition der Subroutinen (vgl. Kapitel 6.2) eignet sich die Auslagerung von Prozessschritten in Subroutinen besonders, wenn erstens davon auszugehen ist, dass diese auch für andere Prüfprozesse von Relevanz sind. Weiterhin bieten sich Subroutinen zur Komplexitätsvermeidung bei der Beschreibung der Prozessfunktionen an, wenn zweitens mehrere ähnlich gelagerte Prüfbedingungen überprüft werden müssen, die jedoch nicht in einer generischen Prüfbedingung zusammengefasst werden konnten, weil diese zusammengefasste Prüfbedingung zu unspezifisch wäre oder Teilaspekte der Prüfbedingungen darin nicht mehr enthalten wären. Es kann dann beispielsweise eine Subroutine zur Prüfung des Geschwindigkeitsbandes geben, in der die verschiedenen Prüfbedingungen, die sich auf Geschwindigkeiten beziehen, zusammengefasst werden. Nachfolgend sind die Subroutinen gelistet, die gemäß den beiden beschriebenen Kriterien aus dem MP Request ausgelagert wurden und in Kapitel 8.6 modelliert werden.

Vor allem durch das erste Kriterium motivierte Subroutinen, die in Kapitel 8.6 modelliert werden:

- das Berechnen der Flankenschutz-Schutzrate („Calculate Flank Protection Rate“)
- das Prüfen der Einschränkungen durch RAs („RA/Track Restriction Check“) (aufgrund der Ähnlichkeit zur Prüfung der Einschränkungen zu RAs wurde aus Ressourcengründen auf eine gesonderte Modellierung der Prüfung der Einschränkungen von Gleisbereichen und DAs verzichtet)

Vor allem durch das zweite Kriterium motivierte Subroutinen, die in Kapitel 8.6 modelliert werden:

- das Prüfen der beantragten Route auf Existenz und Befahrbarkeit („Route Existence and Trafficability Check“)
- das Prüfen der in der MA enthaltenen Zielpunkte (EoA, SvL) („Target Point Check“)
- das Prüfen der korrekten Weitergabe von Infrastruktureigenschaften („Track Information Check“)
- das Prüfen des Geschwindigkeitsprofils („SSP Check“)

Überlegungen zur Reihenfolge der Prozessschritte

Bei der Bestimmung der Reihenfolge der Prozessschritte stehen bedingt durch die spezifischen Anforderungen aus Kapitel 8.2.1, die aus der globalen Anforderung der geringen Latenz hergeleitet wurden, zwei Überlegungen im Vordergrund.

1. Langwierige Prozessschritte sollten möglichst früh begonnen werden. Hierzu zählt nach Einschätzung des Autors vor allem die Kommunikation mit externen Systemen, da keine langwierigen internen Berechnungen zu erwarten sind, die ein leistungsfähiges System nicht in kurzer Zeit bewältigen könnte (Komplexe (NP-schwere) Sachverhalten wie die optimale Route werden bereits vom TMS vorgegeben, da die Komplexität beim TMS liegen soll.). Hierzu zählen Stakeholder-Systeme, aber auch die Kommunikation mit beweglichen Objekten, z. B. wenn ein Fahrzeug Flankenschutzfunktionen erfüllen soll (vgl. Kapitel 8.3.4).
2. Unnötige Kommunikation oder gar unnötige Statusänderungen von externen Systemen sollten vermieden werden. Hierzu wäre es sinnvoll, zunächst möglichst viele interne Prüfprozesse durchzuführen, bevor externe Systeme kontaktiert werden. Hintergrund ist, dass möglicherweise eine Prüfbedingung fehlschlagen könnte, die zu einem sofortigen Abbruch des Prüfprozesses führen könnte, so dass die Kommunikation mit dem externen System gar nicht mehr erforderlich wäre.

Die beiden Anforderungen widersprechen sich und es muss daher eine Abwägung stattfinden. Für ein performantes Funktionieren des Bahnbetriebs muss das TMS im Regelfall bereits Prüfanfragen stellen, die auch von der Sicherungslogik genehmigt werden. Es kann daher davon ausgegangen werden, dass die Ablehnung von Prüfanfragen des TMS durch die Sicherungslogik Ausnahmefälle darstellen. Damit würde auch eine unnötige Kommunikation nur einen Ausnahmefall darstellen. Aus diesem Grund erscheint es sinnvoller, die Kommunikation mit externen Systemen möglichst frühzeitig als Prozessschritt auszuführen.

Die Nachrichten an die externen Systeme können asynchron verschickt werden. Dies hat gegenüber dem alternativen synchronen Versand (d. h. bei dem immer vor der nächsten Nachricht auf die Antwort der vorherigen Nachricht gewartet werden würde) den Vorteil, dass sie parallel von den externen Systemen bearbeitet werden können. Die zuerst eintreffende Antwort kann dann in der smartLogic als erstes verwertet werden.

Das Geschwindigkeitsprofil kann erst ganz am Schluss überprüft werden, da u. a. die Flankenschutz-Schutzrate oder Stakeholder-Vorgaben noch einen Einfluss auf die erlaubten Geschwindigkeiten haben können.

Rückabwicklung eines MP Requests

Im Prüfprozess müssen, wie auch bereits im Unterabschnitt „Überlegungen zur Reihenfolge der Prozessschritte“ angedeutet, in einigen Fällen bereits vor der vollständigen Prüfung Statusänderungen an Elementen oder bei externen Systemen vorgenommen werden. Ist das Prüfergebnis negativ, müssen diese zurückgenommen werden.

Sofern die Fahrerlaubnis noch nicht an das Fahrzeug gesendet wurde, sind keine Gründe erkennbar, warum eine Rücknahme nicht auf direktem Wege erfolgen kann. Externen Stakeholder-Systemen kann also zum Beispiel mitgeteilt werden, dass der Grund, für den ihre Zustimmung benötigt wurde, entfallen ist. Die externen Systeme können dann selbst entscheiden, ob sie ihren Status wieder ändern (d. h. z. B., ob sich der Bahnübergang wieder öffnet). Bei den stellbaren Fahrwegelementen kann die entsprechende Beanspruchung des Elements gelöscht werden (eine komplette Freigabe des Elements kann allerdings erst erfolgen, wenn auch keine andere dagegensprechende Beanspruchung für das Element mehr existiert).

Am Ende des Prüfprozesses wird im Falle eines positiven Prüfergebnises die Fahrerlaubnis an das Fahrzeug übermittelt. Das Fahrzeug kann bei ETCS dazu aufgefordert werden, den Empfang zu bestätigen. Zwar ist es zunächst nicht sicherheitskritisch, wenn das Fahrzeug die MA nicht erhält, aber auch aus Performance-Gründen ist es sinnvoll sicherzugehen, dass das Fahrzeug die Nachricht auch wirklich erhalten hat, da sie ggf. bei Kommunikationsproblemen erneut geschickt werden kann. Falls das Fahrzeug die MA allerdings nicht bestätigt, besteht für die Sicherungslogik ein Problem. Es ist in diesem Fall nicht klar, ob das Fahrzeug die MA bekommen hat und damit auch ausnutzt, denn es könnte z. B. nur die Antwort des Fahrzeugs verloren gegangen sein. Andernfalls könnte das Fahrzeug die MA auch gar nicht erhalten habe.

Aus dem im vorigen Absatz genannten Grund ist es erforderlich, für den Fall einer nicht empfangenen Empfangsbestätigung einen Rückabwicklungsprozess vorzusehen, bei dem sichergestellt wird, dass das Fahrzeug auch wirklich die MA nicht nutzen wird, bevor Beanspruchungen von Infrastruktur-ressourcen gelöscht werden können. Der Rückabwicklungsprozess stellt eine Subroutine dar, die in dieser Arbeit aufgrund der zeitlichen Rahmenbedingungen jedoch nicht näher ausgearbeitet wird (vgl. auch Kapitel 8.6.8 zu „Transaktionsbedingungen“).

Zeitpunkt der Zustimmung von zustimmungspflichtigen Stakeholder-Systemen

Bei zustimmungspflichtigen Systemen ist häufig das Geben der Zustimmung zu einer Fahrerlaubnisanfrage mit der Beibehaltung eines festgelegten Status verbunden, der negative Begleiterscheinungen haben kann. Zum Beispiel muss ein Bahnübergang geschlossen und freigemeldet sein, damit er einer ihn passierenden Fahrzeugbewegung mit regulärer Geschwindigkeit zustimmt. Je länger der Bahnübergang geschlossen ist, desto mehr werden andere Verkehrsteilnehmer beeinflusst. Ein weiteres Beispiel wäre eine Rotte (Arbeitstrupp), die die Arbeiten unterbrochen und das Gleis verlassen haben muss, bevor sie die Zustimmung geben kann. Daher ist der optimale Zeitpunkt zum Abfragen der Zustimmung zu bestimmen.

Grundsätzlich wurden die folgenden Lösungsmöglichkeiten für das Problem identifiziert:

1. Die Zustimmung könnte zum Zeitpunkt der Anfrage eingeholt und die Ineffizienz zugunsten der Sicherheit in Kauf genommen werden, sofern eine zu frühe Zustimmung nicht von sich aus eine Prüfbedingung verletzten würde (z. B. durch Überschreiten der maximalen Schließzeit beim Bahnübergang).

2. Es könnte ein Mechanismus geschaffen werden, der die Zustimmung erst zu einem späteren Zeitpunkt (spätestens bevor das Fahrzeug nicht mehr rechtzeitig bremsen könnte) vorschreibt und falls sie dann nicht vorliegt, einen Reaktionsprozess einleitet, um das Fahrzeug noch rechtzeitig zu bremsen.

Die zweite Lösung ist mit einer Einschränkung der Sicherheit verbunden, da das Fahrzeug eine gültige MA hätte, die ein nicht gesichertes Element enthält. Zudem sind Reaktionsprozesse nur für den Notfall konzipiert, da nicht sichergestellt werden kann, dass das Fahrzeug auch tatsächlich die Nachricht zum Stopp erhält. Außerdem ist die zweite Lösung auch aufgrund der Anforderung der schlanken Logik wegen der benötigten Zusatzregeln nicht optimal.

Bei der ersten Lösung muss das zustimmungspflichtige System zum Zeitpunkt der Prüfung des MP Requests durch die smartLogic bereits im für die Zustimmung erforderlichen Zustand sein. Kommt die Zustimmungsanforderung sehr früh, kann sich das jedoch zum einen negativ auf die Sicherheit auswirken (z. B. wenn die maximale Schließzeit des BÜ überschritten werden würde) sowie zum anderen betrieblich ineffizient sein und damit gegen die Anforderung verstoßen, dass Vorgaben so wenig restriktiv wie möglich sein sollen (vgl. Kapitel 8.2.1). Im Beispiel der Rotte würde eine zu frühe Zustimmungsanforderung bedeuten, dass die Rotte unnötig lange ihre Arbeit unterbrechen und außerhalb des Gleisbereichs warten müsste, wenn sie bereits sehr früh der Fahrt zustimmen müsste.

Aufgrund der Nachteile der zweiten Lösung wird dennoch die erste Lösung weiterverfolgt. Damit zu frühe Statusänderungen bei den zustimmungspflichtigen Systemen vermieden werden, kann das TMS die MA für eine Fahrzeugbewegung immer nur mit einer Ausdehnung bis vor den Beginn des Wirkbereichs des nächsten zustimmungspflichtigen Stakeholder-Systems beantragen. Dieser Umstand würde dem TMS wiederum ermöglichen, die Statusänderung des Stakeholder-Systems erst so spät zu beantragen, dass nach erfolgter Statusänderung gerade noch genug Zeit bleibt, um die Verlängerung der Fahrerlaubnis für die betrachtete Fahrzeugbewegung zu beantragen, bevor die Fahrzeugbewegung beginnen müsste zu bremsen. Beispielsweise würde das TMS zunächst eine Fahrerlaubnis bis vor den Bahnübergang beantragen. Das Schließen des Bahnübergangs würde das TMS zeitlich so anstoßen, dass es anschließend grade noch genug Zeit hat, um die Fahrerlaubnis bei der smartLogic zu beantragen und der Zugfahrt so die Weiterfahrt zu ermöglichen. Die Zustimmungsanfrage der smartLogic beim Bahnübergang würde dann zu keiner weiteren Verzögerung mehr führen.

Die Wahl des richtigen Zeitpunkts und der richtigen Ausdehnung des jeweiligen MP Requests ist allerdings in jedem Fall eine nicht sicherheitskritische Aufgabe, die aufgrund der Anforderung der schlanken Logik dem TMS zuzuordnen ist.

Ablauf

Für den restlichen Ablauf des Prüfprozesses erscheint kein weiterer Diskussionsbedarf zu bestehen und der Ablauf kann somit im Wesentlichen dem Ablauf der bereits modellierten und in den vorherigen Unterkapiteln des vorliegenden Kapitels zu den Basis-Prüfprozessen vorgestellten Prozessen folgen. Der grobe Ablauf des Prüfprozesses „MP Request“ stellt sich demnach wie folgt dar, wobei die einige der Schritte auch parallel ausgeführt werden (siehe Aktivitätsdiagramm):

1. Prüfe die Funktionsfähigkeit der smartLogic
2. Prüfe die Anfrage auf syntaktische Korrektheit
3. Prüfe, ob das adressierte Fahrzeug existiert
4. Prüfe, ob die beantragte MA die aktuelle MA der Fahrerlaubnis einschränkt (für diesen Fall ist der MP Change Request vorgesehen, siehe Kapitel 8.5.4)

5. Prüfe, ob die beantragte Route (vgl. Kapitel 7.6.3) existiert und befahrbar ist (siehe Kapitel 8.6.1)
6. Prüfe intern, ob die benötigten Infrastrukturressourcen (Gleissegmente, stellbare Fahrwegelemente) derzeit für einen anderen Prüfprozess (nicht für eine andere Fahrzeugbewegung benötigt werden
   Ist dies der Fall, probiere es über einen festgelegten Zeitraum periodisch neu; Ist dies nicht der Fall, versehe die Ressourcen intern mit einer vorrübergehenden Beanspruchung für den Prüfprozess („Request Occupation“)
7. Prüfe, ob die stellbaren Fahrwegelemente den richtigen Status haben (hiermit wird auch die Auffahr-Prüfbedingung abgedeckt) (siehe Kapitel 8.6.2)
8. Lade die Liste der Stakeholder-Systeme, die auf den Registrierungsschnittstellen registriert sind (siehe Kapitel 8.3.3) und prüfe deren Zustand („Betriebsbereitschaft“)
9. Parallel zu 8.: Rufe die Zugdaten und Position der Fahrzeugbewegung ab, für die die zu prüfende MA bestimmt ist.
10. Parallel zu 7. und 9.: Rufe Zustand („Betriebsbereitschaft“) der stellbaren Fahrwegelemente ab
11. Nach Erhalt der Antwort auf 10.: Prüfe, ob die stellbaren Fahrwegelemente in einem Zustand sind, der sicherstellt, dass sie nicht ohne Überwachung durch die smartLogic umgestellt werden können (i. d. R. Zustand „Betriebsbereit“)[63]
12. Nach Absenden der Nachrichten zu 8.-10.: Prüfe, ob die über Gleisbereiche (vgl. Kapitel 7.3.8) global definierten Einschränkungen eingehalten werden
13. Nach 12. und dem Erhalt der Antworten auf 9.: Prüfe, ob alle weiteren streckenseitig vorgegebenen Einschränkungen bzw. Ereignisse in der MA enthalten (vorgegeben) sind (siehe Kapitel 8.6.3)
14. Prüfe, ob RAs (vgl. Kapitel 7.3.6) auf der Route vorhanden sind und die Vorgaben der RAs eingehalten werden (siehe Kapitel 8.6.6)
15. Prüfe, ob DAs (vgl. Kapitel 7.3.7) auf der Route vorhanden sind und berechne deren Auswirkungen auf die Schutzrate
16. Prüfe, ob Beanspruchungen (vgl. Kapitel 7.6.2) auf der Route vorhanden sind und berechne deren Auswirkungen auf die Schutzrate (insbesondere Überschneidungen mit der Belegung (= Fahrzeugbelegungsbeanspruchung) oder der MA anderer Fahrzeuge)
17. Nach der Antwort auf 8.: Prüfe den Status der registrierten Stakeholder
18. Fordere die Zustimmung von zustimmungspflichtigen Stakeholder-Systemen an
19. Prüfe, ob alle erforderlichen Zustimmungen von Stakeholder-Systemen eingegangen sind
20. Parallel zu 19.: Prüfe, ob alle anderen Anforderungen der Stakeholder-Systeme umgesetzt sind
21. Berechne die Flankenschutz-Schutzrate (siehe Kapitel 8.6.5)
22. Prüfe die in der beantragten MA angegebenen Zielpunkte (siehe Kapitel 8.6.4)
23. Prüfe das Geschwindigkeitsprofil (siehe Kapitel 8.6.7)
24. Prüfe, ob alle benachrichtigungspflichtigen Stakeholder-Systeme empfangsbereit sind und verschicke die Benachrichtigungen
25. Berechne die Gesamt-Schutzrate des MP Requests
26. Falls die Schutzrate nicht ausreichend ist oder der Prozess aus einem anderen Grund abgebrochen werden muss, entferne die nicht mehr benötigten Beanspruchungen (insbesondere die Request Occupations)

[63] In bestimmten Zuständen (z. B. Bauzustand) können z. B. Weichen außerhalb der Überwachung umgestellt werden.

27. Falls die Schutzrate ausreichend ist, generiere die MA und sende diese an das Fahrzeug (die ETCS-MA muss nicht direkt durch die Sicherungslogik generiert werden, das kann auch ein Transactor-Modul, wie bei der RCA das APS-MT-Modul (vgl. Kapitel 2.4.3) übernehmen)
28. Warte auf die Empfangsbestätigung des Fahrzeugs („Acknowledgement“)
29. Falls (nach mehrfachen Versuchen) kein Acknowledgement eingeht, ist eine Rückabwicklungsprozedur einzuleiten
30. Setze neue Beanspruchungen durch die genehmigte MA in der Datenhaltung (MA Occupations) und entferne die vorübergehende Beanspruchung für den Prüfprozess (Request Occupations) (vgl. Punkt 6)
31. Sende eine Rückmeldung über das Ergebnis des Prozesses (Request Return Message RRM) an das TMS

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind. Da sich die Registrierungen der Stakeholder-Systeme regelmäßig ändern können, werden die aktuellen Registrierungen während des Prozesses nachgeladen. Um diesen Sachverhalt darzustellen wird eine generische sichere Datenquelle modelliert (Safe Data Lake).

Im vorigen Abschnitt bzw. in den zu den einzelnen Schritten des Ablaufs gehörenden Prüfbedingungen werden eine ganze Reihe von weiteren externen Systemen genannt. Diese können jedoch generisch zu Gruppen zusammengefasst werden. Als Auslöser des „MP Request“-Prozesses und Empfänger der RRM tritt das TMS auf. Die MA muss abschließend an das Fahrzeug gesandt werden, von dem auch der Status abgefragt wird. Weiterhin werden Status und Zustand der stellbaren Fahrwegelemente (vgl. Kapitel 7.4.3) und der Stakeholder-Systeme benötigt.

Aktivitätsdiagramm

Zur Beschreibung des Prozesses „MP Request“ wurde gemäß der in Kapitel 8.2 diskutierten Vorgehensweise ein UML-Aktivitätsdiagramm erstellt. Aufgrund der Größe des Aktivitätsdiagrams kann es an dieser Stelle nicht abgedruckt werden. Es findet sich stattdessen in Anlage 9.

Da Teile des Prozesses auch für den MPChangeRequest (siehe Kapitel 8.5.5) benötigt werden, wird dieser Teil des dargestellten Prozesses (der gestrichelte Bereich im Aktivitätsdiagramm) in eine Subroutine ausgegliedert, die von der Prozessfunktion aufgerufen wird. Um ein besseres Verständnis des MP Requests als zentralem Prozess der smartLogic zu ermöglichen, wurde jedoch entschieden, diese Subroutine nicht in ein eigenes Digramm auszulagern, sondern im Diagramm des MP Requests darzustellen.

Erneutes Überprüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von Prüfbedingungen als nicht relevant zu überprüfen. Gegebenenfalls veränderte Einstufungen sind dabei iterativ in die bisher in diesem Unterkapitel vorgestellten Ergebnisse eingeflossen.

8.5.4 MP Change Request (Anpassen einer Fahrerlaubnis)

In Folge der globalen Anforderung des Regelhandlungsgebotes fordert eine spezielle Anforderung an die Verhaltensmodellierung der Logik, dass Fahrerlaubnisse (MAs) nachträglich ohne großen Aufwand wieder geändert werden können sollen (vgl. Kapitel 8.2.1). Verlängerungen der MA ohne

Einschränkung der vorherigen MA[64] sind jederzeit über den regulären Weg eines MP Requests möglich (siehe auch nächster Abschnitt). Verkürzte MAs oder MAs, die auf andere Weise restriktiver als die bestehende, zu ersetzende MA sind, können dagegen nicht einfach über den regulären MP Request geprüft und anschließend an die Fahrzeugbewegung übertragen werden, da nicht garantiert werden kann, dass die Fahrzeugbewegung die restriktiveren Vorgaben auch umsetzen kann. Aus diesem Grund soll im Folgenden ein gesonderter Prozess zum Anpassen einer bereits erteilten Fahrerlaubnis modelliert werden, der nachfolgend als „***MP Change Request***“ bezeichnet wird.

Hintergrund und Vorüberlegungen

Hintergrund der zu Beginn dieses Unterkapitels genannten Anforderung aus Kapitel 8.2.1 ist, dass ein performantes Reagieren auf ein verändertes Betriebsgeschehen, wie zum Beispiel Verspätungen oder eine kurzfristig entstandene Verfügbarkeitsänderung des Netzes, eine Anpassung bestehender MAs erforderlich macht. Ansonsten würde durch die Vielzahl der blockierten Elemente kaum Reaktionsspielraum für eine Optimierung des veränderten Betriebsgeschehens durch das TMS zur Verfügung stehen. Eine schnelle und unkomplizierte Anpassungsmöglichkeit für bereits erteilte MAs hat daher positive Auswirkungen auf die Zieldimension der Kapazität, da das TMS durch eine optimale Disposition die bestmögliche Kapazität im Netz erzielen kann. Zudem werden (manuelle) Hilfsauflösungen vermieden und damit Verbesserungen in Hinblick auf die Zieldimension der Robustheit erzielt.

ETCS enthält bereits Funktionalitäten, die eine Anpassung bestehender MAs automatisiert ermöglichen. Es bietet sich aufgrund der Anforderung zur Nutzung von Standardschnittstellen an, diese Funktionalitäten zu nutzen. Die verschiedenen Funktionalitäten sind für verschiedene Arten der Anpassung der Fahrerlaubnis vorgesehen. Im nachfolgenden Unterabschnitt wird näher betrachtet, welche Funktionalität für welche Art der Anpassung einer bestehenden MA geeignet sind. Der Ablauf der für den MP Change Request geeigneten ETCS-Funktionalität wird im zweiten Unterabschnitt dieses Abschnitts näher erläutert.

Arten möglicher Anpassungen der Fahrerlaubnis

Wie in der Einleitung dieses Abschnitts bereits gesagt, enthält ETCS (vgl. zu ETCS Kapitel 2.2.2) unterschiedliche Funktionalitäten, mit denen bestehende MAs verändert bzw. angepasst werden können. Es handelt sich um Nachrichten, die für verschiedene Anwendungsfälle vorgesehen sind und es muss angenommen werden, dass für die verschiedenen Anwendungsfälle auch unterschiedliche Prüfbedingungen relevant sind.

Als einfachste Form der Anpassung kann eine Verlängerung der Fahrerlaubnis angenommen werden, die in jedem Detail weniger oder gleich restriktiv als die ursprüngliche Fahrerlaubnis ist. Dies ist typischerweise bei reinen Verlängerungen der Fahrerlaubnis der Fall. Wie bereits in der Einleitung zu diesem Unterkapitel angedeutet, entsteht kein zusätzlicher Prüfaufwand, da die bisherige Fahrerlaubnis bereits sicher ist und die Parameter der neuen Fahrerlaubnis durch einen MP Request-Prüfpozess geprüft werden können. Da alle Werte weniger oder gleich restriktiv als die der ursprünglichen Fahrerlaubnis sind, können deren Werte nach erfolgreicher Prüfung direkt aktualisiert werden

[64] Mit dem Zusatz „ohne Einschränkung der vorherigen MA“ wird ausgedrückt, dass die verlängerte MA nicht beispielsweise eine niedrigere Geschwindigkeit im Gleisabschnitt, der bereits von der bestehenden MA abgedeckt wird, vorschreibt.

Für den Fall, dass der Hintergrund der Anpassung der MA die Abwehr einer unmittelbar drohenden Gefahr ist, sieht ETCS zwei mögliche Nachrichten an das Fahrzeug vor, den „***Unconditional Emergency Stop***“ (ETCS-Message 15) und den „***Conditional emergency Stop***“ (ETCS-Message 16) [ERA 2016]), die außerdem im Kommunikationsverlauf Priorität haben. Beim conditional emergency stop kann das Fahrzeug den Nothaltauftrag ablehnen, wenn es der Auffassung ist, nicht mehr rechtzeitig vor dem neuen Zielpunkt zum Halten zu kommen. Beim unconditional emergency stop besteht diese Möglichkeit nicht. Beide Emergency Stops sollten mit einem Reaktionsprozess gekoppelt sein, da in der Regel durch das auslösende Ereignis auch weitere Maßnahmen zur Begrenzung des Schadensausmaßes erforderlich werden könnten.

Falls eine neue Fahrerlaubnis vorgegeben werden soll, die nicht auf einer unmittelbar drohenden Gefahr beruht, aber (in der Regel aus betrieblichen Gründen) restriktivere Werte für das Fahrzeug vorgibt, als sie in der aktuell gültigen MA enthalten sind, ist bei ETCS die Funktion „Kürzen einer Fahrerlaubnis“ vorgesehen. Diese Funktion wird im Folgenden kurz erläutert.

Wirkprinzip der ETCS-Funktion „Kürzen einer Fahrerlaubnis“

ETCS hält für das nachträgliche Verändern einer Fahrerlaubnis mit restriktiveren Vorgaben („***Kürzen einer Fahrerlaubnis***“) die Messages 9, 137 und 138 bereit [ERA 2016]. Das Kürzen einer Fahrerlaubnis ist vor allem sinnvoll, um die bestehenden Beanspruchungen (vgl. Kapitel 7.6.2) der Fahrzeugbewegung, zu der die MA gehört, zu reduzieren und die entsprechenden Infrastrukturelemente somit für die Nutzung durch andere Fahrten freizugeben.

Bei der Prüfung der ursprünglichen Fahrerlaubnis hat die smartLogic die Beanspruchungen der benötigten Infrastrukturelemente eingetragen und mit dem Übermitteln der Fahrerlaubnis an die Fahrzeugbewegung der Fahrzeugbewegung gestattet die Infrastrukturelemente zu nutzen. Um die Beanspruchungen entfernen und damit die Infrastrukturelemente anderweitig nutzen zu können, muss zuvor sichergestellt werden, dass die Fahrzeugbewegung die Beanspruchungen auch nicht mehr benötigt.

Ein Fahrzeug darf davon ausgehen, dass es eine bereits erteilte MA ausnutzen kann und berechnet seine Bremskurven entsprechend den Parametern der MA. Aufgrund von möglichen Verbindungsabbrüchen kann nicht sicher davon ausgegangen werden, dass eine später veränderte Fahrerlaubnis das Fahrzeug auch erreicht und von diesem befolgt wird. Um das Problem zu lösen, könnte bei Verbindungsabbruch bereits nach kurzer Zeit eine Schnellbremsung erfolgen. Tatsächlich ist eine solche Funktion auch vorgesehen, allerdings in Deutschland erst nach 40 s, um Betriebsstörungen bei kürzeren Verbindungsabbrüchen zu vermeiden (vgl. [Trinckauf et al. 2020, S. 204]). Diese Zeitspanne reicht jedoch nicht aus, um sicher davon ausgehen zu können, dass eine veränderte MA vom Fahrzeug auch befolgt wird. Weiterhin könnten die restriktiveren Vorgaben auch unvollständig oder aufgrund eines anderweitigen Übertragungsproblems nicht korrekt empfangen werden (Die grundlegenden Sicherheitsprinzipien „Fail Safe“ und „Fehleroffenbarung“ wären damit nicht umgesetzt.).

Um das Problem zu lösen, sieht ETCS vor, dass das Fahrzeug den Empfang der Nachricht mit der restriktiveren MA bestätigen muss. Weiterhin muss es auch bestätigen, dass es die neuen Vorgaben einhalten kann. Mit ETCS-Message 9 („***Request to shorten MA***“) beantragt die Infrastrukturseite (heute das RBC, hier die smartLogic) beim Fahrzeug die „Kürzung“ der Fahrerlaubnis, indem es eine neue Fahrerlaubnis mit restriktiveren Vorgaben übermittelt. Kann das Fahrzeug die neuen Vorgaben einhalten, antwortet es mit Message 137 („***Request to shorten MA granted***“), andernfalls mit Message 138 („***Request to shorten MA rejected***“). Anschließend können die in der neuen

Fahrerlaubnis nicht mehr enthaltenen Beanspruchungen der Infrastruktur gelöscht werden und diese Infrastrukturelemente anderweitig beansprucht werden. Der Ablauf eines solchen Prozesses zur Kürzung einer Fahrerlaubnis mittels ETCS ist im Sequenzdiagramm in Abb. 67 skizziert.

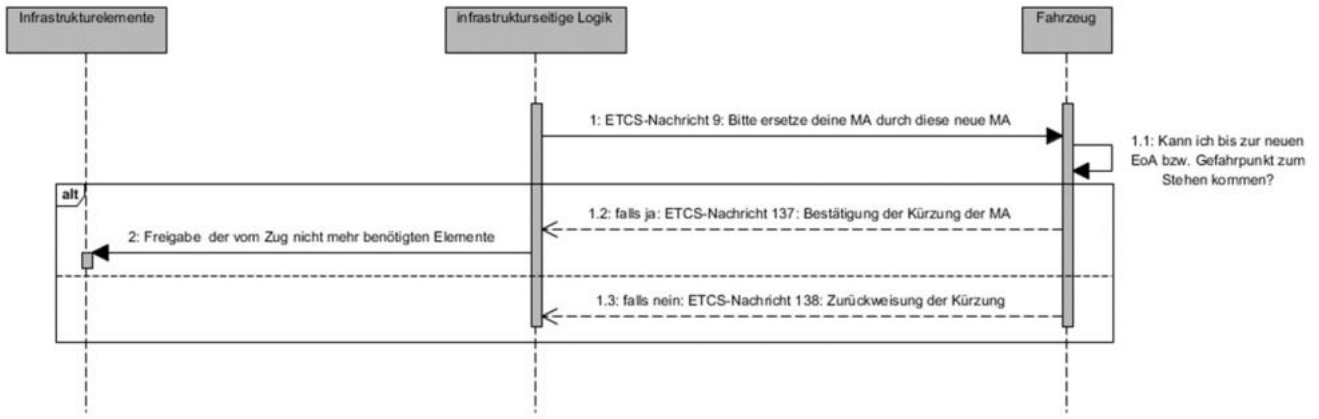


Abb. 67: Sequenzdiagramm eines Prozesses zum „Kürzen einer Fahrerlaubnis“ unter Verwendung der entsprechenden ETCS-Funktion
[Eigene Darstellung]

Bisher ist in ETCS-Message 9 nur vorgesehen, ein Paket 15 mit den Kerndaten der Fahrerlaubnis (Zielpunkte) zu übermitteln. Theoretisch wäre es jedoch auch möglich, weitere restriktive Parameter übermitteln zu wollen, wie eine zusätzliche für das Fahrzeug vorgegebene Handlung oder ein anderes Geschwindigkeits- oder Modusprofil. Die folgenden Ausführungen gehen erstmal davon aus, dass diese erweiterte Möglichkeit besteht. Soll sie bei einer Implementierung tatsächlich genutzt werden, müsste ggf. ein Change Request bei der ERA eingereicht werden.

Identifizieren der für den Prüfprozess relevanten Prüfbedingungen

Zunächst erscheint der Prozess „Kürzen einer Fahrerlaubnis“ für die Infrastrukturseite sicherungstechnisch unproblematisch zu sein, da das Fahrzeug für sich selbst prüft, ob es einen bestimmten Fahrweg noch benötigt oder nicht und mit der Freigabe auch garantiert, dass es den freigegebenen Fahrweg nicht mehr verwenden wird, sofern es keine neue Fahrerlaubnis dafür bekommt. Auf der Infrastrukturseite wurden dagegen die weniger restriktiven Parameter der ursprünglichen MA bereits geprüft, als die ursprüngliche MA genehmigt wurde.

Eine detailliertere Durchsicht der Prüfbedingungen aus dem Funktionskatalog in Anlage 2 ergibt dennoch Prüfbedingungen deren Verletzung zu einer Verringerung der Schutzrate führen könnte. Daher sollten diese Prüfbedingungen näher betrachtet werden. Ob eine Verletzung der einzelnen Prüfbedingungen auch wirklich eine signifikante Einschränkung der Schutzrate zur Folge hat, wird in diesem Verfahrensschritt jedoch noch nicht bewertet. In Tab. 50 sind die identifizierten Prüfbedingungen mit der Begründung, warum sie relevant sein könnten, aufgeführt. Die ID bezieht sich auf Anlage 2. Weiterer Diskussionsbedarf ist fett dargestellt und wird im nachfolgenden Abschnitt aufgegriffen.

Tab. 50: Relevante Prüfbedingungen für den MP Change Request

ID	Beschreibung	Bemerkung
F-E000a	die smartLogic muss korrekt arbeiten	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.
F-E000b	die Nachricht muss bekannt und die Syntax korrekt sein	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.

F-E054	die Ausgabe einer Fahrerlaubnis an eine nicht klar definierte Fahrzeugbewegung muss verhindert werden	Die Fahrzeugbewegung, für welche die Kürzung beantragt wurde, muss von der smartLogic eindeutig identifiziert werden.
F-E215b	es dürfen nur Elemente freigegeben werden, die die Fahrzeugbewegung nicht mehr nutzen kann	Es muss also sichergestellt werden, dass die Freigabe wirklich von der Fahrzeugbewegung erfolgt, für welche die Elemente, die freigegeben werden sollen, auch verschlossen waren und dass die Fahrzeugbewegung diese wieder freigegeben hat
F-E110	das Umstellen von Fahrwegelementen „unter dem Zug“ muss verhindert werden	Daraus folgt: Elemente dürfen erst freigegeben werden, wenn sie durch keine Zuweisung mehr beansprucht werden. Es muss verhindert werden, dass das Kürzen einer Fahrerlaubnis dazu führt, dass ein Element freigegeben wird, welches noch von anderen Fahrzeugen (z. B. überlappte Fahrerlaubnis im Bereich des Durchrutschwegs, Beanspruchung als Flankenschutzelement, Festlegung in der aktuellen Lage aufgrund eines Defekts...) in der aktuellen Lage benötigt wird.
F-E051	die neue Fahrerlaubnis muss zulässig sein	Es wird mit Message 9 eine komplett neue Fahrerlaubnis übermittelt, welche die vorgesehene Kürzung enthält und im Falle der Annahme durch das Fahrzeug die bestehende Fahrerlaubnis ersetzt. Diese könnte auch noch an anderen Stellen als den neuen Zielpunkten von der ursprünglichen Nachricht abweichen. Eine ganze Reihe von Prüfbedingungen ist für die Ausstellung neuer Fahrererlaubnisse von Relevanz. **Daher muss entweder festgestellt werden, dass die neue Fahrerlaubnis nicht weniger restriktiv ist als die alte oder die neue Fahrerlaubnis muss wie eine komplett neue Fahrerlaubnis den Prozess „Ausstellen einer Fahrerlaubnis“ durchlaufen.** Da es sich nicht um eine einzelne Prüfbedingung, sondern um ein ganzes Set an Prüfbedingungen handelt, ist dieser Punkt unterstrichen dargestellt.
F-E122a	Stopps in “Non Stopping Areas” (NAS) sind zu vermeiden	Bestimmte Zugtypen sollen in bestimmten Bereichen nicht zum Halten kommen, wenn dies vermeidbar ist. Ein vorzeitiger Stopp aus dispositiven Gründen darf daher nicht in einer NSA liegen.
F-E034	Passagierzüge müssen für verkehrliche Halte an Bahnsteigen halten, die ausreichend lang sind	Dies klingt erstmal nicht wie eine Aufgabe der Sicherungslogik. Eine Verletzung dieser Bedingung kann aber durchaus eine Verringerung der Schutzrate zur Folge haben, da Fahrgäste durch einen vorzeitigen Halt im Bahnhofsbereich dazu ermuntert werden können, die Türen unzeitig zu öffnen. Dies könnte bei gleichzeitig vorzeitig freigegebenen Türen zu einer erhöhten Wahrscheinlichkeit eines Unfalls führen.

F-E357a	Fahrzeugbewegungen mit zu geringem Zugkraftüberschuss dürfen beim Anfahren in steil geneigten Rampen nicht zum Stehen kommen	Für das Anfahren in Rampen ist mehr Energie nötig, als für das Durchrollen. Deshalb kann ein Stopp eines Zuges mit geringem Zugkraftüberschuss beim Anfahren in steil geneigten Rampen zum Problem werden. Zu prüfen ist hierbei, ob es sich nur um ein betriebshemmendes oder auch ein sicherheitsrelevantes Problem handelt. Eine abschließende Bewertung kann hier nicht vorgenommen werden, weswegen die Prüfbedingung hier aufgeführt wird.
F-E238	Flankenschutzgebende Elemente dürfen ihre schutzgebende Lage nicht verlassen, wenn dadurch kein ausreichender Flankenschutz für die zu schützende Fahrt mehr existiert	Bei vollüberwachten Fahrzeugen stellt ETCS sicher, dass diese definitiv bis zum Stillstand kommen und überwacht diesen Stillstand auch. Daher ist es unter bestimmten Voraussetzungen möglich, dass vollüberwachte ETCS-Fahrzeuge auch Flankenschutz bieten können.[65] Beim Kürzen einer Fahrerlaubnis ist daher darauf zu achten, ob dies Auswirkungen auf Schutzraten anderer Züge durch veränderte Flankenschutzbedingungen haben und falls ja, ob diese kompensiert werden können.
F-E264	die maximale Schließzeit eines Bahnübergangs ist sicherzustellen	Durch das Kürzen der Fahrerlaubnis und vorzeitige Bremsungen könnten Bahnübergänge später befahren werden, als ursprünglich vorgesehen. Dies könnte zur Überschreitung der maximal vorgesehenen Schließzeiten der BÜ führen, wodurch Auswirkungen auf die Schutzrate verbunden sind.
F-E276	die gleichzeitige Nutzung von Tunneln durch Reise- und Güterzüge muss ab einer Grenz-Relativgeschwindigkeit der beteiligten Züge verhindert werden	Das Tunnelbegegnungsverbot hat erst jüngst Einzug in die Eisenbahnsicherungstechnik gehalten. Derzeit ist noch nicht genau abzusehen, wie weitreichend das Tunnelbegegnungsverbot in Zukunft ausgelegt sein wird. Dennoch wird an dieser Stelle diese Prüfbedingung der Vollständigkeit halber mit aufgeführt, da eine vorzeitige Verlangsamung des Zuges auch zu geänderten Begegnungskonstellationen im Tunnel führen könnte.[66]

Wie bei der fünften identifizierten Prüfbedingung beschrieben, wird mit der ETCS-Message 9 eine neue Fahrerlaubnis übertragen. Für den Fall, dass diese den normalen Prüfprozesse für das „Ausstellen einer Fahrerlaubnis“ (vgl. Kapitel 8.5.2) durchläuft, brauchen einige der anderen Prüfbedingungen nicht mehr gesondert betrachtet zu werden, da deren Betrachtung bereits durch den Prüfprozess der neuen Fahrerlaubnis abgedeckt ist. Es verblieben dann neben der Prüfung der Grundvoraussetzung jeder Anfrage (F-E000) und der Prüfung der neuen Fahrerlaubnis (siehe

[65] Das Flankenschutzkonzept zur smartLogic ist noch nicht veröffentlicht. Der geschilderte Umstand ist hier dennoch der Vollständigkeit halber mitaufgeführt.

[66] Dies wird hier betrachtet, auch, wenn die Wahrscheinlichkeit für einen solchen Fall – ohne detaillierte Berechnung – gering erscheint, da nur hohe Geschwindigkeiten der beteiligten Züge für das Tunnelbegegnungsverbot eine Rolle spielen, diese aber durch den eingeleiteten Bremsvorgang des betrachteten Zuges bereits abgenommen haben muss.

„MP Request“-Prozess in Kapitel 8.5.2) noch die Prüfbedingungen F-E215b, F-E110 und F-E238 als zusätzlich zu prüfende Prüfbedingungen. Ob dies sinnvoll ist, soll im nächsten Arbeitsschritt, der im nächsten Abschnitt beschrieben ist, näher erläutert werden.

Ablauf des Prüfprozesses in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Prozessablauf zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf den betrachteten Prozess auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen im Prüfprozesses bezogen auf die Kernanforderung der sicheren Logik mit Ausnahme der formalen Prüfungen der Funktionsfähigkeit der smartLogic und der Syntax der Prüfanfrage zu Beginn irrelevant. Die Reihenfolge wird daher nur durch nachgeordnete Anforderungen wie die Anforderung der geringen Latenz sowie praktische Abhängigkeiten (z. B. „Rufe Belegungen ab“ vor „Prüfe auf einen Konflikt“) bedingt.

Bezüglich des Ablaufs des Prüfprozesses wurde bei der Identifizierung der relevanten Prüfbedingungen die Frage aufgeworfen, ob

1. die neue Fahrerlaubnis als verkürzte Variante der alten Fahrerlaubnis nur daraufhin überprüft wird, dass sie keine weniger restriktive Vorgabe enthält als die ursprüngliche Fahrerlaubnis (zum Beispiel eine höhere erlaubte Geschwindigkeit innerhalb des neuen Geschwindigkeitsprofils als an derselben Stelle im alten) oder ob
2. die neue Fahrerlaubnis in jedem Fall wie eine ganz neu beantragte Fahrerlaubnis den kompletten Prüfprozess für das „Ausstellen einer (neuen) Fahrerlaubnis“ durchläuft.

Bei der zweiten Lösungsmöglichkeit wäre der Prüfprozess sehr umfangreich und es bestünde daher die Gefahr, dass viele eigentlich nicht benötigte Abfragen durchgeführt würden (widersprüche der Latenz-Anforderung, vgl. Kapitel 8.2.1). Andererseits vereinfachte die zweite Möglichkeit im Vergleich zur ersten Möglichkeit die Modellierung der Prozessfunktion „MP Change Request“, da ein größerer Teil der identifizierten Prüfbedingungen im Prüfprozess „Ausstellen einer Fahrerlaubnis“ bereits abgeprüft würde. Dadurch würde der vorliegende Prozess übersichtlicher (vgl. Anforderung der schlanken Logik, ebd.). Zusätzlich böte die zweite Lösungsmöglichkeit die größtmögliche Flexibilität, da mit der gleichen Anfrage des TMS auch Abweichungen zur ursprünglichen MA möglich würden, die im Vergleich zu der ursprünglichen MA weniger restriktiv wären (vgl. Anforderung, Vorgaben so wenig restriktiv wie möglich zu gestalten). Die anderen in Kapitel 8.2.1 identifizierten Anforderungen haben keinen erkennbaren Einfluss auf die beiden hier diskutierten Lösungsmöglichkeiten.

Insgesamt kann davon ausgegangen werden, dass das Anpassen einer Fahrerlaubnis im Vergleich zum normalen Ausstellen von Fahrerlaubnissen seltener stattfindet, so dass die Latenz-Anforderung nicht als entscheidend angesehen wird. Deshalb erscheint in diesem Fall die zweite Lösungsmöglichkeit mit vollständiger Prüfung der neuen Fahrerlaubnis sinnvoller zu sein und wird im Folgenden weiterverfolgt.

Der restliche Ablauf des Prüfprozesses wird als nicht kontrovers eingeschätzt und kann im Wesentlichen dem Ablauf der bereits modellierten und in den vorherigen Unterkapiteln des

vorliegenden Kapitels zu den Basis-Prüfprozessen vorgestellten Prozessen folgen. Der grobe Ablauf des Prüfprozesses „MP Change Request“ stellt sich demnach wie folgt dar:

1. Prüfe die Funktionsfähigkeit der smartLogic
2. Prüfe die Anfrage auf syntaktische Korrektheit
3. Prüfe anhand der Elementzuweisungen, ob das richtige Fahrzeug adressiert wurde
4. Prüfe die neu beantragte Fahrerlaubnis auf Zulässigkeit
5. Prüfe, ob die Elementfreigabe Auswirkungen auf den Flankenschutz für andere Fahrzeugbewegungen hat und berechne die aktuelle Schutzrate für diese Fahrzeugbewegungen analog zum MP Request
6. Kalkuliere die Gesamt-Schutzrate für den Prozess
7. Falls hinreichender Schutz besteht, um den MP Change Request zu genehmigen, sende ETCS-Message 9 an das Fahrzeug
8. Prüfe die Antwort des Fahrzeugs auf Korrektheit
9. Falls die Antwort des Zuges positiv ist (ETCS-Message 137), lösche die Beanspruchungen für die nicht mehr benötigten Elemente
10. Lösche ggf. den Verschluss von Elementen am Element selbst, wenn dieses nicht mehr benötigt wird und damit keine weiteren Beanspruchungen mehr hat
11. Sende eine Rückmeldung über das Ergebnis des Prozesses (Request Return Message RRM) an das TMS

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Neben dem Traffic Management System, von welchem der Prüfprozess angestoßen wird, ist das Fahrzeug, dessen Fahrerlaubnis gekürzt werden soll, ein beteiligtes externes System.

Über den in den Ablauf integrierten Prozess der Prüfung „Ausstellen einer Fahrerlaubnis“ sind jedoch auch alle bei diesem Prozess beteiligten externen Systeme im Betrachtungsraum wie Infrastrukturelemente und Stakeholder-Systeme (z. B. Bahnübergänge) von Interesse (vgl. hierzu Kapitel 8.5.2). Auch andere Züge spielen dafür zum Beispiel bei den Themen Flankenschutz und Tunnelbegegnungsverbot eine Rolle. Im UML-Aktivitätsdiagramm des Prozesses „MP Change Request“ wird der Prüfprozess „Ausstellen einer Fahrerlaubnis“ jedoch als einfache Aktion beschrieben, welche auf die Modellierung des letztgenannten Prozesses verweist. Deshalb brauchen externe Systeme, die nur im Rahmen des letztgenannten Prozesses beschrieben werden, im Diagramm für den Prozess „Kürzen einer Fahrerlaubnis“ nicht aufgeführt werden.

Am Ende des Prozesses können ggf. Verschlüsse an den Feldelementen der stellbaren Fahrwegelemente aufgeboben werden, wenn keine weitere Beanspruchung mehr existiert, sofern solche Verschlüsse an den Feldelementen existieren. Hierfür ist eine Kommunikation mit den Feldelementen erforderlich. Auch dieser Kommunikationsprozess sollte als eigene Subroutine modelliert werden, da er von verschiedenen Prozessfunktionen angestoßen werden kann. Deshalb ist auch diese Kommunikation zur Vereinfachung der Darstellung im Aktivitätsdiagramm nicht dargestellt. Diese Subroutine wird allerdings aus Zeitgründen in Kapitel 8.6 nicht modelliert.

Demnach wird im Aktivitätsdiagramm neben dem den Prozess auslösenden TMS nur der beteiligte Zug als externes System berücksichtigt.

Aktivitätsdiagramm

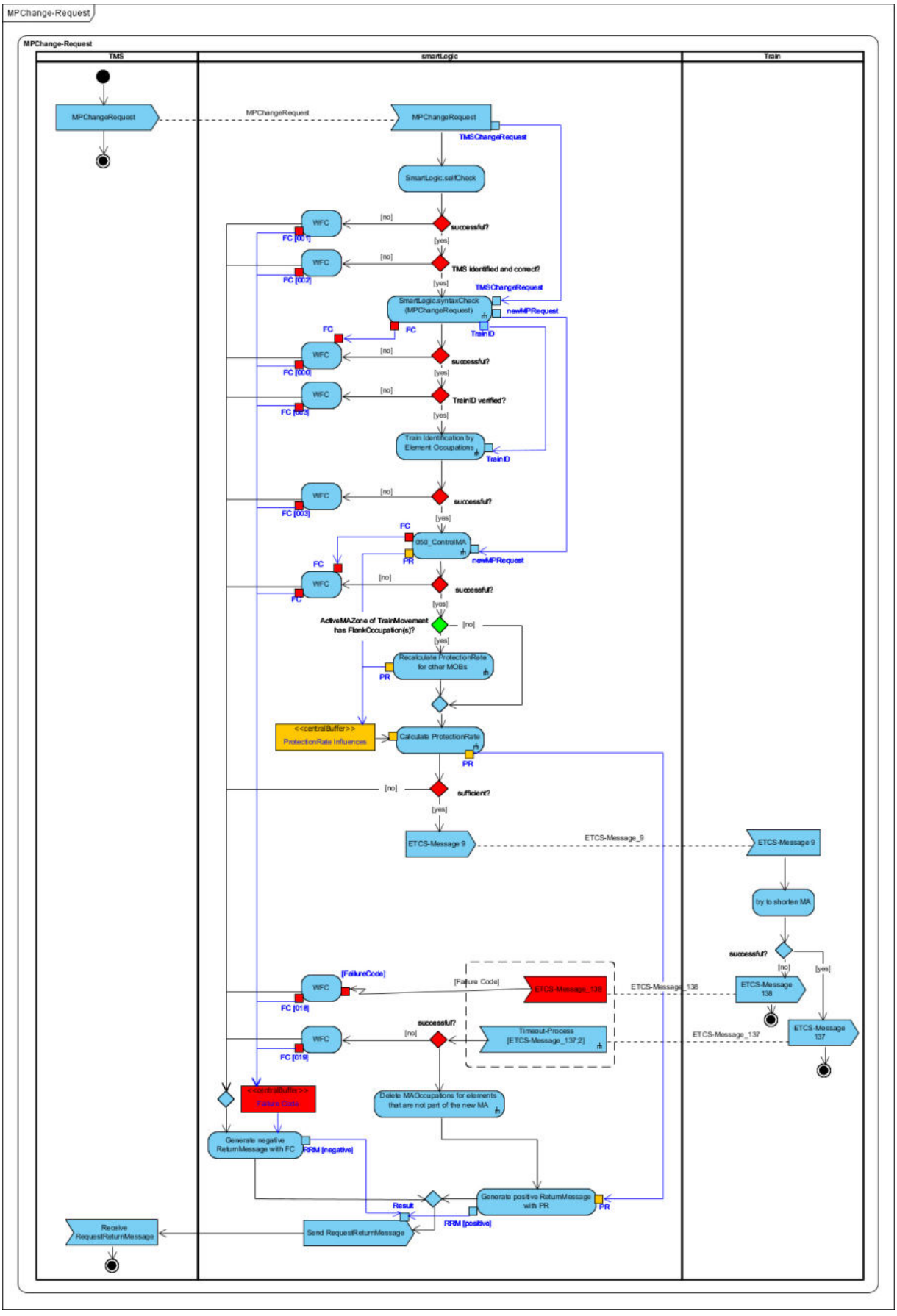


Abb. 68: Aktivitätsdiagramm für den Prozess „MP Change Request“

Zur Beschreibung des Prozesses „MP Change Request“ wurde das in Abb. 68 dargestellte Aktivitätsdiagramm erstellt, das im nachfolgenden Text zur Verdeutlichung der Lesart des Diagramms textuell beschrieben wird. Diese textuelle Beschreibung erfolgt jedoch aus Platzgründen in der Arbeit und aufgrund der Redundanz zum Ergebnis des Arbeitsschrittes „Ablauf des Prüfprozesses in natürlicher Sprache“ nicht nach jedem in Kapitel 8.5 und 8.6 enthaltenen UML-Aktivitätsdiagramm.

Erneutes Überprüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von Prüfbedingungen als nicht relevant zu überprüfen. Gegebenenfalls veränderte Einstufungen sind dabei iterativ in die bisher in diesem Unterkapitel vorgestellten Ergebnisse eingeflossen.

8.5.5 TESC Request (Stellanforderung)

Kapitel 6.3 benennt neben dem Ausstellen einer Fahrererlaubnis und dem Verändern der Fahrzeugzusammensetzung der Fahrzeugbewegungen das (gewünschte) Ändern des Status von stellbaren Fahrwegelementen als dritte primäre betriebliche funktionale Anforderung an die smartLogic. Mit Status ist die Soll- bzw. Ist-Lage des stellbaren Fahrwegelements gemeint, die im smartLogic-Datenmodell generisch über die Track Element Status-Objekte modelliert wird (vgl. Kapitel 7.4.3).[67] In diesem Kapitel wird also der Prüfprozess zur Prüfung von Stellanforderungen (= gewünschte Statusänderungen von stellbaren Fahrwegelementen) erarbeitet, der als **„Track Element Status Change Request“ (TESC Request)** bezeichnet wird. Gemäß der Aufgabenteilung der Systeme muss das TMS alle stellbaren Fahrwegelemente mit TESC-Requests richtig stellen, bevor es eine Fahrerlaubnisanfrage an die smartLogic stellen kann (vgl. Kapitel 4.3.1).

In der klassischen Stellwerkslogik werden zu den stellbaren Fahrwegelementen vor allem Weichen und Gleissperren gezählt (vgl. Kapitel 2.1.1)[68]. Aufgrund der Anforderung der generischen Logik (vgl. Kapitel 8.2.1) wird hier die allgemeinere Definition der stellbaren Fahrwegelemente verwendet, die in Kapitel 7.4.3 als „Controlled Track Elements“ modelliert wurden.

Identifizieren der für den Prozess relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind wiederum zunächst die für den Prozess relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren. Wie in Kapitel 8.2.2 beschrieben, erfolgt die Einstufung als relevant auf Basis der persönlichen Erfahrung mit der Hilfe einiger allgemeingültiger, abstrakter[69] Kriterien, wovon die Hauptkriterien sind, dass ein stellbares Fahrwegelement in der Prüfbedingung als Subjekt oder Objekt vorkommt und/oder dass die Prüfbedingung sich auf eine Beanspruchung bezieht, die in Zusammenhang mit einem stellbaren Fahrwegelement steht.

Das Ergebnis der Prüfung findet sich in Tab. 51. Prüfbedingungen, die als nicht relevant eingeschätzt werden, aber bei denen für diese Einschätzung eine Begründung sinnvoll erscheint, sind ebenfalls in der Tabelle enthalten und kursiv dargestellt. Die Begründung findet sich jeweils in der Spalte

[67] Der Status ist vom Zustand des Elements („element state“) abzugrenzen, der beschreibt, ob das Element beispielsweise „betriebsbereit“ ist.

[68] Bahnübergänge werden dagegen häufig als eigenständige Systeme betrachtet. Sie können zwar ebenfalls ins Stellwerk eingebunden werden, besitzen aber eine eigene Bedienungslogik und haben daher bspw. in Relaisstellwerken die Farbe gelb und nicht blau wie die Stellelemente. Für die smartLogic wurde in Kapitel 8.3.3 festgelegt, dass die Bahnübergänge als Stakeholder-Systeme eingebunden werden.

[69] Spezifischere Kriterien konnten vom Autor aufgrund der in Kapitel 8.2.2 beschriebenen Gründe nicht identifiziert werden.

„Bemerkung“. Weiterer Diskussionsbedarf ist fett dargestellt und wird im nachfolgenden Abschnitt aufgegriffen.

Tab. 51: Relevante Prüfbedingungen für den TESC Request

ID	Beschreibung	Bemerkung
F-E000a	die smartLogic muss korrekt arbeiten	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.
F-E000b	die Nachricht muss bekannt und die Syntax korrekt sein	Dies ist zu Beginn jedes Prüfprozesses sicherzustellen.
F-E101	das Element muss eindeutig identifizierbar sein	
F-E102	*das Element muss einen klar definierten aktuellen Status haben*	*ein unklarer Status könnte auf einen Fehler hindeuten[70]; allerdings erscheint die Annahme gerechtfertigt, dass dies kein Problem darstellt, solange nicht fälschlich ein falscher Status gemeldet wird und die Prüfbedingung somit nicht relevant ist*
F-E103	das zu stellende Element muss sich im Zustand „betriebsbereit“ befinden	
F-E104	Weichen mit beweglichem Herzstück dürfen nicht als aufgefahren gemeldet sein	könnte auch ein Spezialfall von F-E103 sein
F-E045	das zu stellende Elemente darf nicht verschlossen sein	könnte auch ein Spezialfall von F-E103 sein
F-E046	*das zu stellende Element darf nicht Teil einer gesperrten Weichenlaufkette sein*	*Relikt aus der bisherigen Stellwerkstechnik; da im Falle der smartLogic keine Weichen-laufketten eingeführt wurden, wird angenommen, dass die Prüfbedingung nicht relevant ist*
F-E084	das Element vor einer nicht vollüberwachten Fahrt darf erst umgestellt werden, wenn alle weiteren Elemente im geplanten Fahrweg bereits umgestellt sind	Relikt aus der Zeit, als das Umstellen der letzten Weiche vor einer Rangierfahrt die Zustimmung zur Fahrt darstellen konnte; befindet sich heute noch im betrieblichen Regelwerk, damit nicht aus früherer Gewohnheit das Umstellen fehlinterpretiert werden kann; Es sollte mit der Aufsichtsbehörde geklärt werden, ob auf die funktionale Sicherheitsanforderung verzichtet werden kann; *–> im Folgenden wird davon ausgegangen, dass dies der Fall ist*.
F-E110	das Element darf nicht von einer Fahrzeugbewegung oder einer MA beansprucht sein	ob ein Element räumlich beansprucht wird, hängt von den Ausmaßen seiner DPS ab (vgl. Kapitel 7.4.3)

[70] „Im Umlauf“ ist auch ein klar definierter Status.

F-E111	*ein nicht grenzzeichenfrei isoliertes Element darf nur umgestellt werden, wenn das verbundene Element auch nicht beansprucht ist, außer dieses bietet dem ersten Element Flankenschutz*	*Relikt aus dem derzeitigen ESTW-Lastenheft, das auf Basis der infrastrukturseitigen Ortung fungiert; aufgrund der Abbildung von Belegungen mittels der genauen Beanspruchungen der Gleistopologie nicht mehr relevant*
F-E112	*es darf sich keine Fahrzeugbewegung auf das zu stellende Element strecken können*	*es wird angenommen, dass mögliche Fahrzeugstreckungen in der Ausdehnung der Fahrzeugbewegung bereits vorhanden sind (vgl. Kapitel 7.6.1); daher nicht mehr relevant*
F-E238	flankenschutzgebende Elemente dürfen ihre schutzgebende Lage nicht verlassen, wenn dadurch kein ausreichender Flankenschutz für die zu schützende Fahrt mehr existiert	die flankenschutzgebende Funktion wird über entsprechende Beanspruchungen angezeigt; **Zu klären ist, ob auch die Möglichkeit einer Neuorganisation des Flankenschutzes (z. B. Neuberechnung der Flankenschutz-Schutzrate, ggf. Übertragung der Flankenschutzfunktion auf andere potenziell flankenschutzgebende Elemente) geprüft werden soll.**
F-E224, F-E324	Befahrbarkeitsverbote müssen durchgesetzt werden	nur relevant, falls nicht vollüberwachte Fahrzeuge den Verbotsbereich erreichen können; hierzu wird heutzutage häufig gefordert, entsprechende Zugangsweichen abweisend zu stellen; **Für den relevanten Anwendungsfall der Prüfbedingung sollte im Sinne der generischen Logik eine Verallgemeinerung geprüft werden (siehe unten „Schutz von Gleisabschnitten").**
F-E076	der Eintritt von Fahrzeugen mit elektrischer Traktion in Ladezonen mit abgeschalteter Oberleitung muss verhindert werden	Spezialfall von F-E224 bzw. F-E324
F-E239	Personen im Gleis müssen geschützt werden	auch hier geht es um die Schutzweichen-funktion; kann daher ebenfalls als Spezialfall von F-E224 bzw. F-E324 gesehen werden

Ablauf des Prüfprozesses in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Prozessablauf zu erhalten und erforderliche, grundsätzliche Design-Entscheidungen bezogen auf den betrachteten Prozess auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit des Prüfprozesses ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen im Prüfprozesses bezogen auf die Kernanforderung der sicheren Logik mit Ausnahme der formalen Prüfungen der Funktionsfähigkeit der smartLogic und der Syntax der Prüfanfrage zu Beginn irrelevant. Die Reihenfolge wird daher nur durch nachgeordnete Anforderungen wie die Anforderung der geringen

Latenz sowie praktische Abhängigkeiten (z. B. „Rufe Belegungen ab“ vor „Prüfe auf einen Konflikt“) bedingt.

Wie bereits in den Bemerkungen zu Tab. 51 beschrieben, ist nachfolgend zu klären,

- wie mit Flankenschutzbeanspruchungen zu verfahren ist (vgl. Bemerkung zu F-E238) und
- wie der Schutz von Gleisabschnitten, die nicht befahren werden sollen (vgl. Bemerkung zu F-E224 bzw. F-E324, Befahrbarkeitsverbote), vor nicht vollüberwachten Fahrzeugbewegungen erfolgen kann.

Umgang mit bestehenden Flankenschutzbeanspruchungen

Bei Vorhandensein einer Flankenschutzbeanspruchung auf einem stellbaren Fahrwegelement, dessen Status verändert werden soll, konnten zwei Optionen identifiziert werden, wie damit verfahren werden kann.

1. Die Flankenschutzbeanspruchung verändert direkt die Schutzrate der aktuellen zu prüfenden Prüfanfrage negativ, weil grundsätzlich davon ausgegangen wird, dass eine Flankenschutzverletzung vorliegen könnte.
2. Es wird zunächst geprüft, wie sich durch die zu prüfende Statusänderung die Schutzraten der Fahrzeugbewegungen verändern würden, die durch die Flankenschutzbeanspruchung geschützt werden, in der Hoffnung, dass die Änderung marginal und damit akzeptabel ist oder ein anderes Element existiert, welches die Flankenschutzfunktion übernehmen kann.

Der erste Fall ist im Sinne der Anforderung der schlanken Logik einfacher umzusetzen. Allerdings würde der Handlungsspielraum des TMS eingeschränkt und ggf. die Anforderung verletzt, wonach ein Prüfprozess nur abgebrochen werden sollte, wenn die Kernanforderung der sicheren Logik nicht erfüllt ist.

Für den zweiten Fall spricht weiterhin, dass die Neuberechnung der Flankenschutz-Schutzrate auch für andere Prozesse benötigt wird (vgl. Kapitel 8.5.4) und daher ohnehin eine entsprechende Subroutine benötigt wird, die vom „TESC Request“-Prozess genutzt werden kann (siehe „Calculate Flank Protection Rate“ in Kapitel 8.6.5). Da es sich nur um die Berechnung der aktuellen Schutzrate handelt – einen komplett sicherheitskritischen Vorgang –, wird auch nicht die Anforderung verletzt, wonach keine nicht sicherheitskritischen Bestandteile in die Logik aufgenommen werden sollen. Die zweite Lösung erscheint daher sinnvoller.

Schutz von Gleisabschnitten

In Bezug auf den Schutz von Gleisabschnitten, die nicht befahren werden sollen, handelt es sich um eine Schutzfunktion durch die stellbaren Fahrwegelemente ähnlich der Flankenschutz-Funktion. Der Unterschied ist, dass keine anderen Fahrzeugbewegungen, sondern andere Schutzgüter oder zu schützende Personen auf dem durch das Element gedeckten Gleis geschützt werden.

Im Sinne der schlanken Logik sollte geprüft werden, ob die Schutzfunktion durch bereits bestehende Konzepte abgedeckt werden kann. Aufgrund der Ähnlichkeit zum Flankenschutz liegt es nahe, auf das Konzept von (Flankenschutz-)Beanspruchungen zurückzugreifen (vgl. Kapitel 7.6.2). Der Objekttyp der Beanspruchungen ist bewusst generisch gehalten, um alle Arten von Beanspruchungen – und zu diesen zählt auch die Beanspruchung in der Schutzfunktion für das gedeckte Gleis – abbilden zu

können. Liegt eine solche Beanspruchung auf dem Fahrwegelement vor, dessen Status durch den „TESC Request“ verändert werden soll, verringert sich entsprechend die Schutzrate des „TESC Requests“, sodass die Prüfanfrage ggf. abgewiesen wird oder vom TMS in die Prüfanfrage zu integrierende Kompensationsmaßnahmen zur Übernahme der Schutzfunktion vom Fahrwegelement notwendig sind.

Ablauf des Prüfprozesses

Für den restlichen Ablauf des Prüfprozesses wurde kein weiterer Diskussionsbedarf identifiziert. Der Ablauf kann daher im Wesentlichen dem Ablauf der bereits modellierten und in den vorherigen Unterkapiteln des vorliegenden Kapitels zu den Basis-Prüfprozessen vorgestellten Prozessen folgen.

Der grobe Ablauf des Prüfprozesses „TESC Request“ stellt sich demnach wie folgt dar:

1. Prüfe die Funktionsfähigkeit der smartLogic
2. Prüfe die Anfrage auf syntaktische Korrektheit
3. Prüfe, ob das stellbare Fahrwegelement, für welches die Statusänderung beantragt wurde, eindeutig identifiziert wurde
4. Prüfe, ob das Element derzeit für einen anderen Prüfprozess benötigt wird (interner „lock“-Zustand)
   Ist dies der Fall, probiere es periodisch neu (solange bis ein Abbruchkriterium erreicht ist); Ist dies nicht der Fall, versetze es intern in den „lock“-Zustand
5. Prüfe, ob das Element innerhalb der smartLogic gegen Umstellen gesperrt ist bzw. ob sich eine (U)RA auf der Weiche befindet, die die gewünschte Statusänderung verhindert.
6. Prüfe den Zustand des stellbaren Fahrwegelements (inkl., dass es nicht (an der Außenanlage) verschlossen ist, und bei Elementen mit beweglicher Herzstückspitze, dass es nicht als aufgefahren gemeldet ist)
7. Prüfe, ob sich Danger Areas (DAs) über das Element erstrecken und berechne deren Einfluss auf die Schutzrate
8. Prüfe, ob Beanspruchungen für das Element vorliegen und berechne den Einfluss der Beanspruchung auf die Schutzrate
9. Prüfe, ob die Elementfreigabe Auswirkungen auf den Flankenschutz für andere Fahrzeugbewegungen hat und berechne die aktuelle Schutzrate für diese Fahrzeugbewegungen analog zum MP Request.
10. Kalkuliere die Gesamt-Schutzrate für den TESC Request
11. Falls hinreichender Schutz besteht, um den TESC Request zu genehmigen, sende den neuen Soll-Status an das Element
12. Falls das Element den neuen Status bestätigt, aktualisiere den Ist-Status in der smartLogic-Datenhaltung
13. Hebe den internen „lock“-Zustand auf
14. Sende eine Rückmeldung über das Ergebnis des Prozesses (Request Return Message RRM) an das TMS

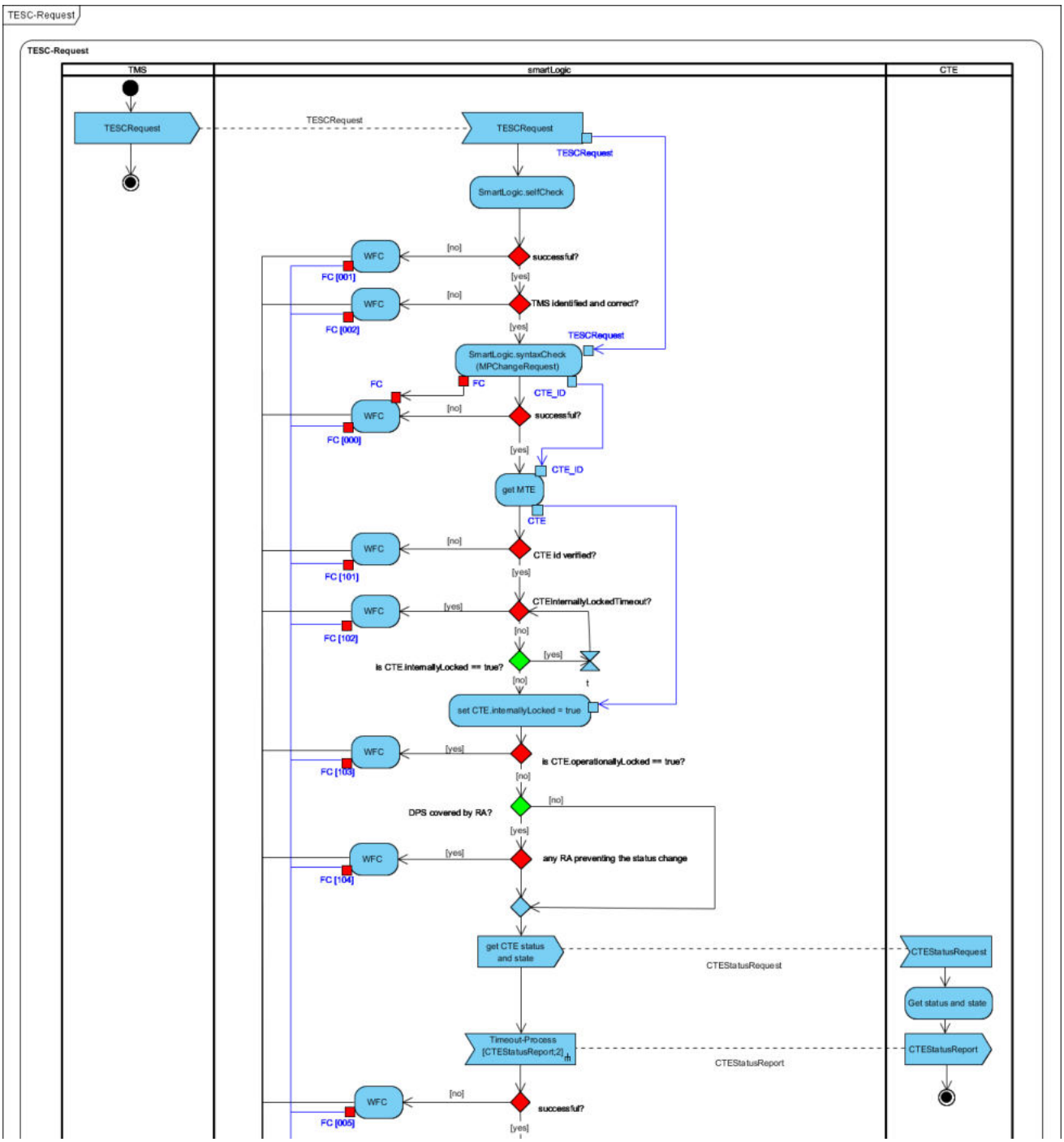
Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Dies sind neben dem TMS, das die Prüfanfrage stellt, die stellbaren Fahrwegelemente bzw. als deren Repräsentanz die zugehörigen Object Controller.

Für die Neuberechnung der Flankenschutz-Schutzrate sind keine zusätzlichen Systeme beteiligt, da die Berechnung rein intern erfolgen kann. Aufgrund der Überlegungen aus Kapitel 4.3.1 sind für evtl. zur Gewährung des Flankenschutzes erforderliche Statusänderungen von weiteren stellbaren Fahrwegelemente sowie für Flankenschutz-Anforderungen an die Fahrzeuge – wie bei allen anderen Stellanforderungen – auf jeden Fall gesonderte Anfragen durch das TMS erforderlich.

Aktivitätsdiagramm

Zur Beschreibung des Prozesses „TESC Request“ wurde das in Abb. 69 dargestellte Aktivitätsdiagramm erstellt.



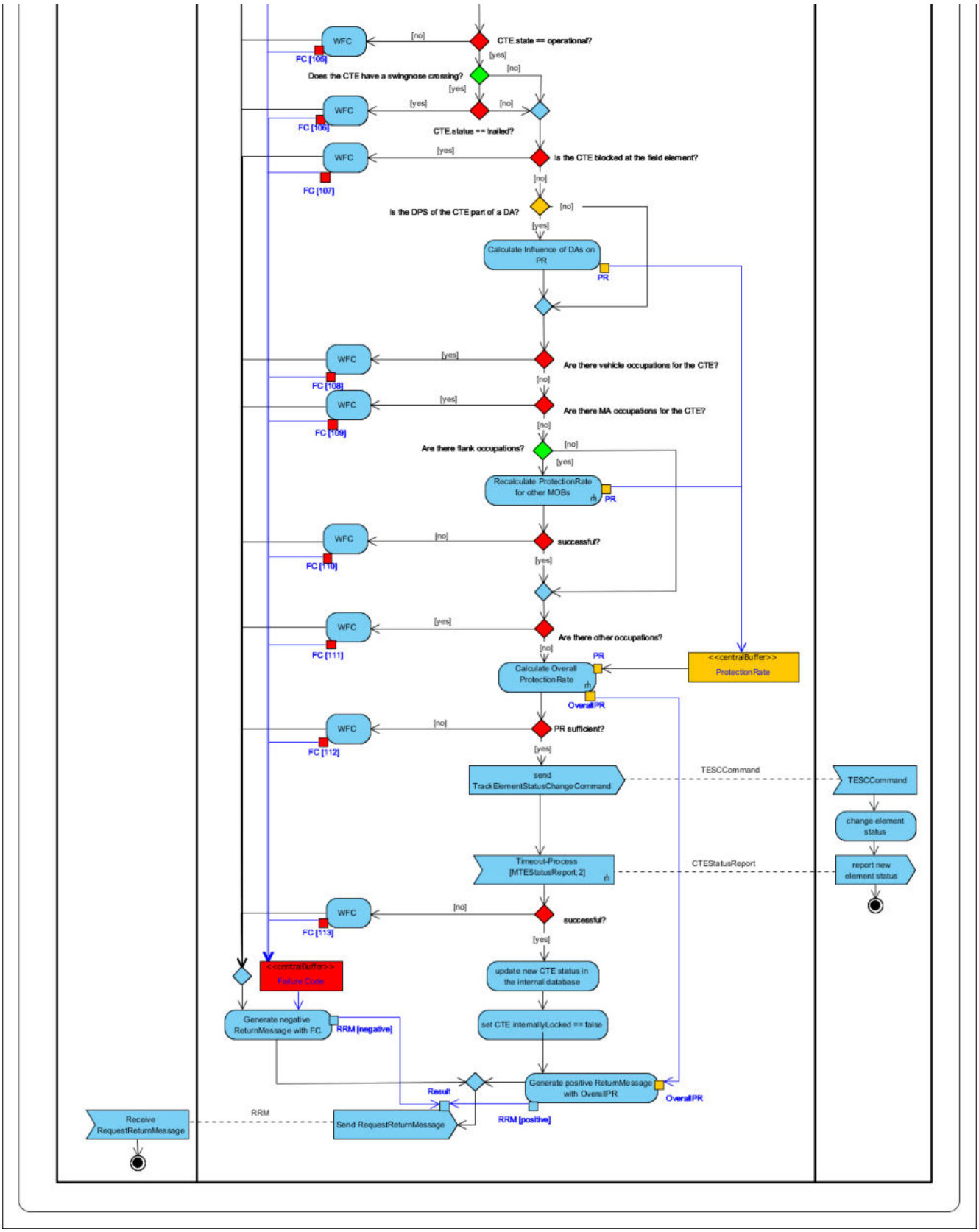


Abb. 69: Aktivitätsdiagramm für den Prozess „TESC Request“

Erneutes Prüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von

Prüfbedingungen als nicht relevant zu überprüfen. Gegebenenfalls veränderte Einstufungen sind dabei iterativ in die bisher in diesem Unterkapitel vorgestellten Ergebnisse eingeflossen.

8.6 wichtige Subroutinen

Gemäß Kapitel 6.2.2, Unterabschnitt „Abgrenzung von Prozessfunktionen und Subroutinen“ ist es sinnvoll, wiederkehrende Aufgaben aus den Prozessen in separate Subroutinen auszulagern. Die wichtigsten Subroutinen sind Bestandteil der in Kapitel 8.5 beschriebenen Basis-Prüfprozesse und sollen im vorliegenden Kapitel besprochen werden.

Die Notwendigkeit einer Subroutine wird bereits durch ihr Vorkommen in einer Prozessfunktion in Kapitel 8.5 hinreichend begründet. Aufgrund des begrenzten Umfangs dieser Arbeit kann hier jedoch nicht jede Subroutine ausführlich modelliert werden. Da jede Subroutine nur einen Prozessschritt (Aktion im UML-Aktivitätsdiagramm der Prozessfunktionen) in einer feineren Granularität beschreibt, wird durch diese Einschränkung die Vollständigkeit dieser Arbeit insofern nicht eingeschränkt, dass auf der übergeordneten Ebene der Prüfprozesse dennoch alle Prozessschritte in gröberer Granularität enthalten sind. In späteren Arbeiten kann die Modellierung je nach Bedarf mit der Modellierung zusätzlicher Subroutinen verfeinert werden.

Wie in Kapitel 8.2 beschrieben, können die Subroutinen nach dem gleichen Schema wie die Prozessfunktionen modelliert werden.

8.6.1 Route Existence and Trafficability Check

In dieser Subroutine wird überprüft, ob der in einer Fahrerlaubnisanfrage beantragte Fahrweg, der in dieser Arbeit in Abgrenzung zu anderen Bedeutungen des Begriffs „Fahrweg“ als Route bezeichnet wird (siehe Kapitel 7.6.3), als Liste von zusammenhängen Gleissegmenten existiert und in der beantragten Richtung für Eisenbahnfahrzeuge befahrbar ist (vgl. Kapitel 8.5.3). Hierzu wird die beantragte Route übergeben und mit der Topologie verglichen und gegebenenfalls ein Fehlercode oder die errechnete Schutzrate von der Subroutine zurückgegeben. Bei erfolgreicher Prüfung wird zudem die Liste der bestimmten Wegweiser an den aufrufenden Prozess übergeben.

Identifizieren der für die Subroutine relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für die Subroutine relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren. Als erstes Kriterium für eine Relevanz spricht, dass sich Prüfbedingungen auf die Gleisinfrastruktur bzw. die Befahrbarkeit und den Status der Gleisinfrastruktur beziehen. Von diesen Prüfbedingungen können wiederum einige ausgeschlossen werden, da sie sich speziell auf Prüfungen beziehen, die explizit in einer anderen Subroutine geprüft werden. Hierzu gehören Prüfbedingungen, die sich auf spezielle nicht physische Befahrbarkeitseinschränkungen beziehen, da diese Einschränkungen bei der Prüfung der Einschränkungen von Gleisbereichen und RAs geprüft werden. Weiterhin können Prüfbedingungen ausgeschlossen werden, die sich auf die zulässige Geschwindigkeit beziehen. Diese Prüfbedingungen werden im „SSP Check“ geprüft (Kapitel 8.6.7). Auch Prüfbedingungen, die sich auf die Weiterleitung von Informationen an das Fahrzeug beziehen, können ausgeschlossen werden (vgl. Track Information Check in Kapitel 8.6.3).

Tab. 52 listet die Prüfbedingungen, die für den „Route Existence and Trafficability Check“ als relevant eingestuft wurden. Prüfbedingungen, die als nicht relevant eingeschätzt werden, aber bei denen für diese Einschätzung eine Begründung sinnvoll erscheint, sind ebenfalls in der Tabelle enthalten und

kursiv dargestellt. Die Begründung findet sich jeweils in der Spalte „Bemerkung“. Weiterer Diskussionsbedarf ist fett dargestellt und wird im nachfolgenden Abschnitt aufgegriffen.

Tab. 52: Relevante Prüfbedingungen für den Route Existence and Trafficability Check

ID	Beschreibung	Bemerkung
F-E035a, F-E035b, F-E035c	Weichen, die keine Rückfallweichen sind, dürfen nicht aufgefahren werden, wenn sie - im Fahrweg liegen - im Gefahrpunktabstand bzw. Durchrutschweg liegen und über ein bewegliches Herzstück verfügen oder mit einem Riegel verschlossen sind	siehe Bemerkung zu F-E340
F-E311	die Route der MA muss topologisch gültig sein	dies bedeutet, dass die Route der Definition aus Kapitel 7.6.3 entsprechen müssen, also aus topologisch zusammenhängenden Gleissegmenten bestehen muss und die Verknüpfungen der Gleissegmente (Positioned Relations) topologisch befahrbar sein müssen (trafficability = true)
F-E340	stellbare Fahrwegelemente auf der Route müssen den richtigen Status haben	sie müssen also so gestellt sein, dass ein Passieren der Route möglich ist, dass ist der Fall, wenn es keine DPS auf der Route durch die Weiche gibt; **es ist zu klären, wie mit stumpf befahrenen Weichen ohne bewegliches Herzstück zu verfahren ist, die theoretisch physisch auch in der anderen Lage passierbar wären (aufgefahren werden könnten)**
F-E265	*Bahnübergänge müssen geschlossen und freigemeldet sein*	*da BÜ als zustimmungspflichtige Stakeholder-Systeme modelliert werden, werden sie nicht als Teil der Gleisinfrastruktur betrachtet und die Prüfbedingung muss hier nicht weiter berücksichtigt werden*
F-E611a, F-E613	*Reisendenübergänge (RÜ) müssen geschlossen und freigemeldet sein und dies bleiben, solange die Fahrzeugbewegung den zugehörigen Gleisabschnitt beansprucht*	*siehe Bemerkung zu F-E265 (BÜ)*
F-E232a	Schlüsselsperren im Flankenschutzraum müssen gesichert sein	sofern es sich um Stellelemente handelt, werden diese über F-E340 mit abgedeckt
F-E282	*es dürfen keine Hindernisse auf dem Gleis detektiert sein*	*kann über DAs abgedeckt werden (vgl. Kapitel 7.3.7)*
F-E275	*es dürfen sich keine Arbeitsmaterialien innerhalb der Fahrzeugbegrenzungslinien befinden*	*siehe Bemerkung zu F-E359*
F-E211	*Beschränkungen durch DAs müssen beachtet werden*	*vgl. Kapitel 7.3.7*
F-E750	*akute Gefahrenstellen dürfen nicht passiert werden*	*kann über DAs abgedeckt werden (vgl. Kapitel 7.3.7)*

F-E276	*Personen- und Güterzüge dürfen sich im Tunnel nicht begegnen, wenn eine bestimmte Relativgeschwindigkeit überschritten wurde*	*kann über RAs abgebildet werden und wird daher im „*RA/Track Restriction Check *“ abgedeckt*
F-E321	*betrieblich gesperrte Gleise dürfen nicht befahren werden, außer mit spezieller Genehmigung*	*kann über RAs abgebildet werden und wird daher im „RA/Track Restriction Check“ abgedeckt*
F-E351	*BoStrab-Gleise dürfen nur von dafür zugelassenen Fahrzeugen befahren werden*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E352	*rein elektrisch angetriebene Fahrzeuge dürfen nur auf Gleisen verkehren, die mit einem auf dem Fahrzeug verfügbaren Stromsystem ausgerüstet sind*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E353	*die Spurweite muss übereinstimmen*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E354	*eines der erlaubten ATP (Zugbeeinflussungssysteme) muss auf dem Fahrzeug vorhanden sein*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E355	*das Fahrzeug muss für den Fahrweg zugelassen sein*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E356	*der Tf bzw. das ATO-System müssen für den Fahrweg zugelassen sein*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E357, F-E364	*das Fahrzeug muss genügend Bremskraft für die Route haben*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E358	*das Achslastprofil darf auf der Route nicht überschritten werden*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E359	*das Lichtraumprofil bzw. die Fahrzeugbegrenzungslinien müssen eingehalten werden*	*kann über Gleisbereiche oder RAs abgebildet werden*
F-E361, F-E540	*das Fahrzeug muss über eine betriebsbereite Magnetschienenbremse verfügen, wo dies gefordert ist*	*kann über Gleisbereiche oder RAs abgebildet werden*

Ablauf der Subroutine in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Ablauf der Subroutine zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf die betrachtete Subroutine auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen in der Subroutine bezogen auf die Kernanforderung der sicheren Logik irrelevant. Die Reihenfolge wird daher nur durch nachgeordnete Anforderungen wie die Anforderung der geringen Latenz sowie praktische Abhängigkeiten (z. B. „Rufe Belegungen ab“ vor „Prüfe auf einen Konflikt“) bedingt.

Der Ablauf der Subroutine wird im nachfolgenden Unterabschnitt hergeleitet und im darauffolgenden Unterabschnitt zusammengefasst.

Herleitung des Ablaufs

Da eine smartLogic nicht für das gesamte Eisenbahnnetz zuständig sein kann, muss ihr Zuständigkeitsbereich räumlich begrenzt sein. Dieser Zuständigkeitsbereich wurde in Kapitel 7.3.8 als smartLogic Area eingeführt. Damit der Zuständigkeitsbereich nicht überschritten wird, sollte zu Beginn, vor Überprüfung der eigentlichen Prüfbedingungen, geprüft werden, ob die Sicherungslogik auch für die gesamte beantragte Route zuständig ist. Alle Elemente der Route bzw. ihr für die Route benötigter Teil müssen sich daher in der smartLogic Area befinden.

Gemäß F-E311 muss geprüft werden, ob die Route topologisch gültig ist. Die zu prüfende Route wird bei Aufruf der Subroutine in Folge eines „Route“-Objekts übergeben. Das Route-Objekt wurde in Kapitel 7.6.3 eingeführt. Die Route besteht demnach aus einer geordneten Liste an Gleissegmenten und zwei intrinsischen Koordinaten, die angeben, wo auf der ersten und letzten Kante sich der Beginn bzw. das Ende der Route befinden, da sich sowohl Beginn als auch Ende der Route an beliebiger Stelle auf dem ersten bzw. letzten Gleissegment der Route befinden können.

Demzufolge ist zur Berücksichtigung der Prüfbedingung F-E311 zunächst zu prüfen, ob jeweils das nachfolgende Element der Liste der Gleissegmente mit seinem Listenvorgänger topologisch verbunden ist, also eine „Positioned Relation“ zwischen den beiden Fahrwegelementen existiert, die befahrbar (trafficability = true) ist.

Zur Berücksichtigung der Prüfbedingung F-E340 muss der aktuelle Status der stellbaren Fahrwegelemente, die in der Route liegen, dem erforderlichen Status zur Befahrung der Route entsprechen. Ein stellbares Fahrwegelement, das in der Route liegt, kann mit seinem für die Befahrbarkeit der Route erforderlicher Status als **Wegweiser („Waypoint“)** der Route bezeichnet werden. Da die Wegweiser mit dem Route-Objekt nicht übergeben werden, müssen sie zunächst bestimmt werden. Die Bestimmung kann über die Positioned Relation, welche die Gleissegmente verbindet, erfolgen, da die Befahrbarkeit der Verbindung über das Positioned Relation-Objekt an einen bestimmten Status eines stellbaren Fahrwegelements gebunden sein kann.

Der so bestimmte erforderliche Status der Wegweiser muss anschließend noch mit dem aktuellen Status der jeweiligen stellbaren Fahrwegelemente abgeglichen werden. Da allerdings zuvor eine interne Vorreservierung (mittels Request Occupation, vgl. Kapitel 7.6.2) der Gleisabschnitte erfolgen sollte, damit sich der Status nicht während der Prüfung durch eine parallel laufende Prüfanfrage verändern kann, muss dieser Schritt in eine eigene Subroutine ausgegliedert werden (siehe Kapitel 7.6.3). Zur Überprüfung des Status gehört auch die spezielle Anforderung in Bezug auf den Status stumpf befahrener Weichen, die über kein bewegliches Herzstück verfügen.

Ablauf

1. Prüfe, ob alle Gleissegmente der Route zwischen Start- und Zielpunkt in der smartLogic Area liegen (übergehende Fahrten in andere Zuständigkeitsbereiche werden separat betrachet, siehe Kapitel 8.8.1)
2. Prüfe, ob die aufeinanderfolgenden Gleissegmente jeweils über eine Positioned Relation (ohne Fahrtrichtungswechsel) miteinander verbunden sind
3. Prüfe, ob die Befahrbarkeit der jeweiligen Positioned Relation ohne Fahrtrichtungswechsel gegeben ist (bei Fahrtrichtungswechsel muss eine neue MA beantragt werden, vgl. Kapitel 8.4.1)

4. Bestimme für jede Positioned Relation den jeweiligen Wegweiser (= CTE mit passendem Status) und füge diesen falls vorhanden zur Liste der Wegweiser hinzu. Andernfalls breche den Prüfprozess ab, da die Route nicht gültig ist.

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind. Die Subroutine wird von Prozessfunktionen aufgerufen. Wie in Kapitel 8.2.2 beschrieben, wird davon ausgegangen, dass die Topologiedaten innerhalb der smartLogic universell zur Verfügung stehen. Der Status der MTEs wird erst in der ausgegliederten Subroutine in Kapitel 8.6.2 abgerufen. Daher werden keine weiteren externen Systeme für den „Route Existence and Trafficability Check“ benötigt.

Aktivitätsdiagramm

Abb. 70 zeigt das Aktivitätsdiagramm zur Subroutine „Route Existence and Trafficability Check“.

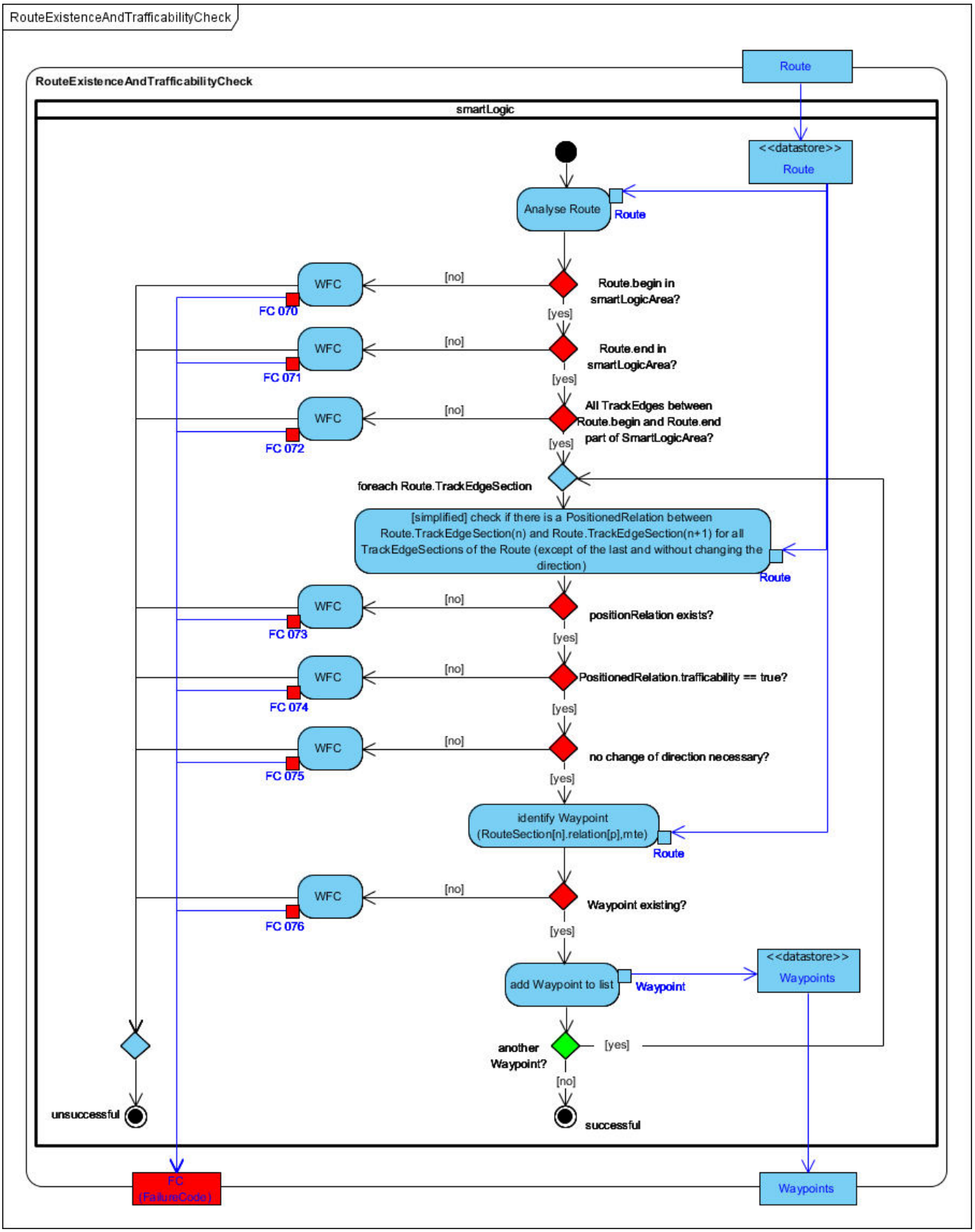


Abb. 70: Aktivitätsdiagramm der Subroutine „Route Existence and Trafficability Check“

Erneutes Prüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von

Prüfbedingungen als nicht relevant zu überprüfen. Aufgrund der Einfachheit des Prozesses ergeben sich durch diesen Arbeitsschritt bei der vorliegenden Subroutine keine Änderungen.

8.6.2 Route Status Check

In Kapitel 8.6.1 wurde begründet, warum der Route Status Check eine eigene Subroutine sein sollte. Aufgabe ist die Überprüfung des korrekten Status der stellbaren Fahrwegelemente in der Route (also z. B. die für die Route erforderliche Weichenlage). Als Eingangsdaten werden die identifizierten Wegweiser der Route benötigt sowie für die spezielle Regelung bei stumpf befahrenen Weichen ohne bewegliches Herzstück (siehe Tab. 53) die Position der EoA aus der beantragten MA. Die Funktion wird beispielsweise innerhalb des MP Requests aufgerufen (vgl. Kapitel 8.5.3) und übergibt nach ihrem Abschluss einen Fehlercode, falls ein Abbruchgrund aufgetreten ist oder die Schutzrate, die ggf. angepasst wurde.

Identifizierung der für die Subroutine relevanten Prüfbedingungen

Da sich die Subroutine wie der im vorigen Unterkapitel beschriebene Route Existence and Trafficability Check auf die Befahrbarkeit einer Route bezieht, können zunächst dieselben Kriterien für die Identifizierung der Prüfbedingungen angewendet werden. Als zusätzliches Kriterium kann herangezogen werden, dass sich die Prüfbedingung auf den Status der stellbaren Fahrwegelemente beziehen muss. Damit verbleiben die in Tab. 53 aufgeführten Prüfbedingungen.

Tab. 53: Relevante Prüfbedingungen für den Route Status Check

ID	Beschreibung	Bemerkung
F-E035a, F-E035b, F-E035c	Weichen, die keine Rückfallweichen sind, dürfen nicht aufgefahren werden, wenn sie - im Fahrweg liegen - im Gefahrpunktabstand bzw. Durchrutschweg liegen und über ein bewegliches Herzstück verfügen oder mit einem Riegel verschlossen sind	siehe Bemerkung zu F-E340
F-E340	stellbare Fahrwegelemente auf der Route müssen den richtigen Status haben	Sie müssen also so gestellt sein, dass ein Passieren der Route möglich ist. Das ist der Fall, wenn es keine DPS auf der Route durch die Weiche gibt. **Es ist zu klären, wie mit stumpf befahrenen Weichen ohne bewegliches Herzstück zu verfahren ist, die theoretisch physisch auch in der anderen Lage passierbar wären (aufgefahren werden könnten).**
F-E232a	Schlüsselsperren im Flankenschutzraum müssen gesichert sein	sofern es sich um Stellelemente handelt, werden diese über F-E340 mit abgedeckt

Ablauf der Subroutine in natürlicher Sprache

Da sich die Subroutine auf die Abprüfung einer speziellen Prüfbedingung konzentriert, ist der Ablauf relativ einfach. Zu klären ist nur, wie mit den stumpf befahrenen Weichen zu verfahren ist, für die eine Ausnahme von der allgemeinen Regel der Prüfbedingung gilt und wie sich diese Auswirkung auf die Schutzrate auswirkt.

Bei den stumpf befahrenen Weichen ohne bewegliches Herzstück kann das Unfallrisiko bei einer Befahrung mit niedriger Geschwindigkeit als gering angenommen werden. U. a. deshalb ist im heutigen Regelwerk eine Überlappung zweier Fahrwege im Durchrutschweg erlaubt. Da der Endpunkt der Route als beim letzten von der Fahrzeugbewegung erreichbaren in der MA enthaltenen Zielpunkt (vgl. zu Zielpunkten Kapitel 8.3.2) definiert wurde (vgl. Kapitel 7.6.3), müssten nach den bisher festgehaltenen Regeln diese Weichen jedoch auch den für die Route erforderlichen Status haben.

In Kapitel 8.3.2 wurde entschieden, dass die Möglichkeit überlappender Durchrutschwege bzw. Sicherheitsabstände hinter dem anzusteuernden Zielpunkt von der smartLogic bereitgestellt werden soll. Deshalb ist für den geschilderten Fall eine Sonderregel erforderlich, die in den Ablauf eingefügt wird. Im Sinne des Konzepts der Schutzrate sollte dabei bestimmt werden, wie groß das tatsächliche Risiko des Auffahrens der Weiche ist und entsprechend dieses Risikos die Schutzrate abgesenkt werden.

Damit ergibt sich der folgende Ablauf:

1. Rufe den aktuellen Status des zum Wegweiser gehörenden MTEs ab
2. Prüfe, ob der aktuelle Status des MTEs dem (erforderlichen) Status des Wegweisers entspricht
3. Falls ein Element nicht den erforderlichen Status hat, prüfe, ob es sich um eine stumpf befahrene Weiche ohne bewegliches Herzstück handelt und ob diese Weiche zwischen der EoA (erster Zielpunkt) und dem Ende der Route liegt.
4. Ermittle für eine stumpf befahrene Weiche mit abweichendem Status die Wahrscheinlichkeit, dass diese von der Fahrzeugbewegung erreicht wird in Bezug zur Geschwindigkeit, die die Fahrzeugbewegung beim Erreichen hätte und berechne daraus den Einfluss auf die Schutzrate für das Befahren dieses MTEs[71].
5. Berechne abschließend die Schutzrate für die Prüfbedingung auf Basis der gefundenen Einflüsse auf die Schutzrate.

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind. Die Subroutine wird von Prozessfunktionen aufgerufen. Im Rahmen der Prüfung muss der Status der zu den Wegweisern gehörenden MTEs abgerufen werden, so dass die MTEs als externe Systeme benötigt werden.

Aktivitätsdiagramm

Abb. 71 zeigt das Aktivitätsdiagramm zur Subroutine „Route Status Check“.

[71] Die genaue Berechnung der Schutzrate wird nach Kapitel 3.3 und 8.3.1 nicht in dieser Arbeit hergeleitet, da sie von vielen Einflussgrößen abhängt. Zum Beispiel müsste das Entgleisungsrisiko abhängig von der Geschwindigkeit ermittelt werden. Falls diese Werte nicht genau ermittelt werden können oder ermittelt wurden, kann für die smartLogic auch zunächst ein konservativer Wert verwendet werden, der auf jeden Fall zur sicheren Seite ausfällt (im Extremfall könnte z. B. eine stumpfe Weiche mit falscher Lage in der Route immer zur Ablehnung der Prüfanfrage führen.

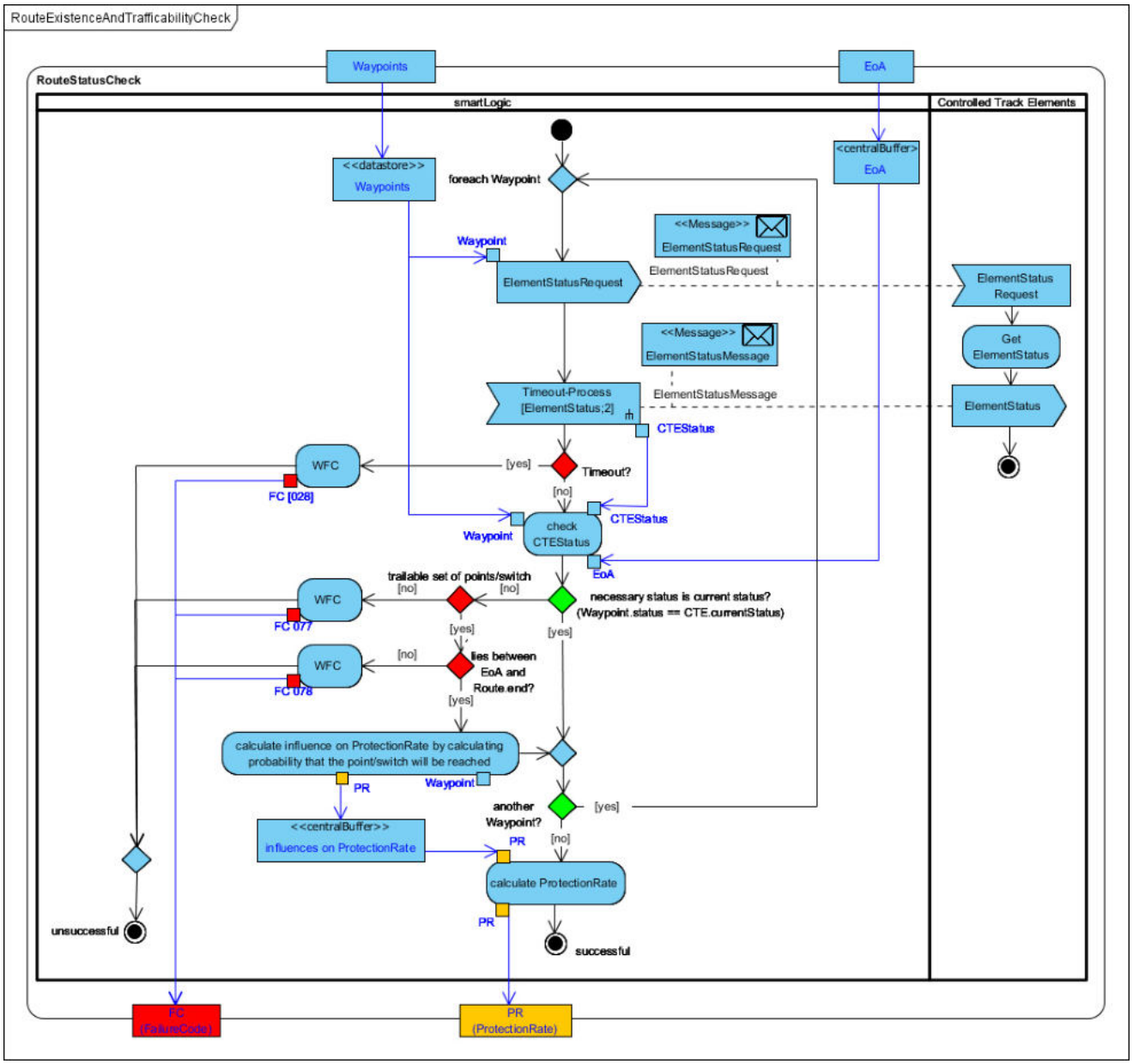


Abb. 71: Aktivitätsdiagramm der Subroutine „Route Status Check“

Erneutes Prüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von Prüfbedingungen als nicht relevant zu überprüfen. Aufgrund der Einfachheit des Prozesses ergeben sich durch diesen Arbeitsschritt bei der vorliegenden Subroutine keine Änderungen.

8.6.3 Track Information Check

Der Track Information Check dient dazu sicherzustellen, dass der Fahrzeugbewegung mit einer Fahrerlaubnis alle von ihr zu beachtenden Informationen über die Infrastruktur auf der Route mitgeteilt werden, damit die Fahrzeugbewegung daraus resultierende vorgeschriebene Handlungen auch durchführt. Hintergrund ist, dass mit ETCS eine Vielzahl von Parametern zur Fahrerlaubnis übermittelt werden können, mit denen die Fahrzeugbewegung ihre Bremskurven optimieren kann oder über vorgeschriebene Handlungen informiert wird (vgl. [ERA 2016]). Sie wird daher vor allem innerhalb des MP Requests aufgerufen (vgl. Kapitel 8.5.3), wodurch andere aufrufende Prozesse aber

nicht ausgeschlossen sind. Zur Prüfung müssen die beantragte Fahrerlaubnis sowie die beantragte Route übergeben werden. Bei fehlenden Informationen liefert die Subroutine einen Fehlercode zurück.

Identifizieren der für die Subroutine relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für die Subroutine relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren. Kriterien für die Relevanz sind daher vor allem, dass die Prüfbedingungen sich auf Fahrzeugfunktionen bezieht oder auf Informationen, die an das Fahrzeug weitergegeben werden sollen.

Tab. 54 listet die als relevant eingeschätzten Prüfbedingungen für den Track Information Check.

Tab. 54: Relevante Prüfbedingungen für den Track Information Check

ID	Beschreibung	Bemerkung
F-E034, F-E034a	Passagierzüge müssen für verkehrliche Halte an Bahnsteigen halten, die ausreichend lang sind	die Fahrzeugbewegung muss die Länge des Bahnsteigs kennen, um beispielsweise bestimmte Türen geschlossen zu halten
F-E641	*Geschwindigkeitsprofile in Ladeeinrichtungen und an Bahnsteigen müssen eingehalten werden*	*hierfür erscheint die sinnvollere Lösung zu sein, diese Prüfbedingung in die Prüfung des Geschwindigkeitsprofils (SSP Check) aufzunehmen*
F-E216	*Fahrzeugbewegungen müssen an für sie vorgeschriebenen Betriebshalten halten*	*dies kann entweder durch das Setzen des Zielpunkts vor den Betriebshalt oder durch eine entsprechende Vorgabe im Geschwindigkeitsprofil erreicht werden; deshalb muss es nicht als Information an das Fahrzeug weitergegeben werden*
F-E276	*Personen- und Güterzüge dürfen sich im Tunnel nicht begegnen, wenn eine bestimmte Relativgeschwindigkeit überschritten wurde*	*kann über RAs gelöst werden, siehe Kapitel 8.4.6, daher hier nicht relevant*
F-E357a	Fahrzeugbewegungen mit geringem Zugkraftüberschuss dürfen beim Anfahren in steil geneigten Rampen nicht zum Stehen kommen	
F-E362, F-E540, F-E541	die Benutzung der Magnetschienenbremse muss verhindert werden, wo ihre Benutzung nicht erlaubt ist	
F-E431	Fahrzeugtüren dürfen nur geöffnet werden, wenn sich das Fahrzeug am Bahnsteig befindet	siehe Bemerkung zu F-E034, F-E034a
F-E432	Trittstufen müssen zum richtigen Zeitpunkt ausgefahren werden	sie sollen weder, wo es nicht erlaubt ist, ausgefahren werden können, noch nicht ausgefahren werden, wo es geboten ist
F-E510, F-E512, F-E726, F-E726a	der Stromabnehmer muss an den richtigen Punkten gesenkt und gehoben werden	

F-E513	Fahrzeuge mit gehobenem Stromabnehmer dürfen nur Gleise mit Oberleitung benutzen	
F-E531	ein evtl. vorhandener Schneepflug muss an den richtigen Stellen gehoben (und gesenkt) werden	das Heben ist sicherheitskritisch
F-E643	das Fahrzeug muss alle vorgeschriebenen Warnungen durchführen (z. B. Pfeifen, Läuten)	
F-E704a	ein reduzierte Haftbeiwert muss dem Fahrzeug gemeldet werden	
F-E363	weitere fahrzeugseitige Vorgaben müssen (je nach Bedarf) übermittelt und eingehalten werden	Dies ist eine generische Prüfbedingung, die im Sinne der globalen Anforderung der Zukunftsfähigkeit hinzugefügt wurde; zusätzliche relevante Informationen können im Datenmodell in Gleisbereichen oder über RAs hinterlegt werden

Ablauf der Subroutine in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Ablauf der Subroutine zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf die betrachtete Subroutine auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt. Nachfolgend wird im ersten Unterabschnitt zunächst der Ablauf hergeleitet. Anschließend wird im zweiten Unterabschnitt darauf eingegangen, wie mit fehlenden Informationen umgegangen wird, da bei Verletzung der zugehörigen Prüfbedingungen mehrere Möglichkeiten plausibel erscheinen.

Ablauf

Der Ablauf der Subroutine kann einfach aus einer sequentiellen Abfrage der einzelnen Prüfbedingungen bestehen, da nur Inhalte der beantragten Fahrerlaubnis überprüft werden. Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen im Prüfprozesses bezogen auf die Kernanforderung der sicheren Logik irrelevant. Die folgende Liste kann bei Bedarf erweitert werden.

1. Prüfe, ob alle Informationen über Bahnsteige entlang der Route in der Fahrerlaubnis enthalten sind
2. Prüfe, ob die Neigungsinformationen enthalten sind
3. Prüfe, ob alle Ausschlusszonen für die Verwendung der Magnetschienenbremse enthalten sind
4. Prüfe, ob alle Punkte zum Heben und Senken des Stromabnehmers enthalten sind
5. Prüfe, ob bei Fahrzeugen mit Schneepflug Informationen zum Heben und Senken des Schneepflugs enthalten sind
6. Prüfe, ob Gleisbereiche mit vermindertem Haftbeiwert enthalten sind
7. Prüfe, ob Punkte, an denen Warnsignale abgegeben werden müssen, enthalten sind

8. Prüfe, ob weitere sicherheitskritische Informationspunkte an der Strecke vorhanden sind, die dem Fahrzeug Vorgaben zur Verwendung von Fahrzeugfunktionen machen

Umgang mit fehlenden Informationen

In Anbetracht der Überlegungen zur Schutzrate in Kapitel 8.3.1 (vgl. die verschiedenen Fälle in Tab. 42) ist zu analysieren, ob eine Verletzung der oben genannten Prüfbedingungen (also fehlenden Informationen in der beantragten Fahrerlaubnis)

1. direkt zur Zurückweisung der Prüfanfrage führt oder
2. nur eine negative Auswirkung auf die Schutzrate entsteht.

Auf der einen Seite ist im Sinne der zweiten Möglichkeit nicht davon auszugehen, dass eine fehlende Information immer gleich dazu führt, dass das Gefährdungsrisiko bei der Genehmigung der Prüfanfrage unzulässig hoch wäre. Eine direkte Zurückweisung der Prüfanfrage könnte daher der Anforderung der *Rückfallebenenintegration* widersprechen, wonach der Prozess nur abbrechen soll, wenn die Kernanforderung der sicheren Logik unter Berücksichtigung aller verfügbaren Informationen tatsächlich nicht erfüllt ist. Auf der anderen Seite kann bei der ersten Möglichkeit die smartLogic das TMS über die fehlenden Informationen informieren und das TMS kann diese Informationen in einer neuen Prüfanfrage ergänzen und die negativen Auswirkungen würden sich auf etwas zusätzlichen Zeitbedarf beschränken (Anforderung der *geringen Latenz*).

Da bei der zweiten Lösungsmöglichkeit – auch wenn das im Einzelfall zulässig sein kann – immer noch eine negative Auswirkung auf die Kernanforderung der sicheren Logik besteht und die negative Auswirkung bei der ersten Möglichkeit durch die geringfügig erhöhte Übertragungszeit als sehr gering eingeschätzt wird, wird die erste Möglichkeit für die in dieser Subroutine zu prüfenden Prüfbedingungen weiterverfolgt.

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Die Subroutine wird von Prozessfunktionen aufgerufen. Es wird davon ausgegangen, dass alle notwendigen Informationen über das Fahrzeug und die Infrastruktur bereits innerhalb der smartLogic vorliegen. Damit enthält die Subroutine ausschließlich interne Prüfungen und externe Systeme müssen bei der Modellierung nicht berücksichtigt werden.

Aktivitätsdiagramm

Abb. 72 zeigt das Aktivitätsdiagramm zur Subroutine „Track Information Check“.

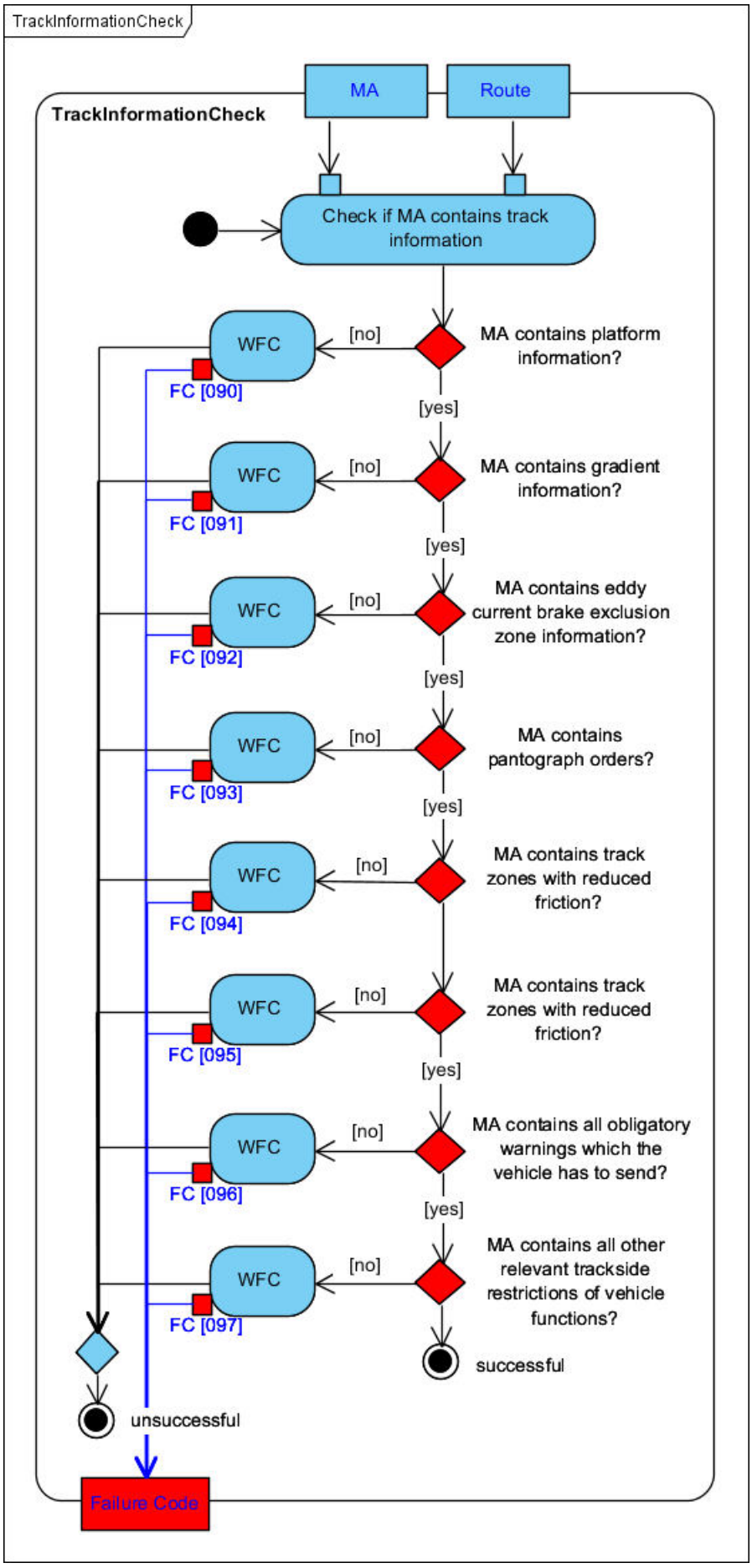


Abb. 72: Aktivitätsdiagramm der Subroutine „Track Information Check“

Erneutes Prüfen der Prüfbedingungen

Aufgrund der Einfachheit des Prozesses ergeben sich durch diesen Arbeitsschritt bei der vorliegenden Subroutine keine Änderungen.

8.6.4 Target Point Check

Dieses Unterkapitel beschreibt die Subroutine zur Überprüfung der korrekten Angabe der Zielpunkte in einer beantragten MA, die somit im MP Request benötigt wird (vgl. Kapitel 8.5.3). Die grundsätzlichen Überlegungen hierzu wurden bereits ausführlich in Kapitel 8.3.2 diskutiert. Für den Target Point Check sind zahlreiche Eingangsdaten erforderlich. Dazu gehören die Fahrzeugdaten, die beantragte MA, die beantragte Route, die registrierten Stakeholder-Systeme sowie die bis zum Zeitpunkt des Aufrufs des Target Point Checks zusammengerechnete Gesamt-Schutzrate, da sie zur Bestimmung des Gefährdungsrisikos an den einzelnen Zielpunkten benötigt wird. Die Subroutine gibt entweder einen Fehlercode oder eine neu kalkulierte Gesamt-Schutzrate zurück.

Identifizieren der für die Subroutine relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für die Subroutine relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren. Hierfür ist zu klären, wie diese Subroutine genau abzugrenzen ist.

In Kapitel 8.3.2 wurde festgestellt, dass der primäre sicherungstechnische Zielpunkt einer beantragten Fahrerlaubnis vom TMS maximal unmittelbar vor den nächsten Gefahrpunkt gesetzt werden darf, bei dessen Überquerung die (Gesamt-)Schutzrate der Prüfanfrage unter den zulässigen Schwellwert für die Genehmigung der Prüfanfrage sinken würde (maßgeblicher Gefahrpunkt). Um diesen Sachverhalt zu überprüfen, müssen daher potenzielle Gefahrpunkte identifiziert werden.[72]

Daher sind alle Prüfbedingungen relevant, die Gefahrpunkte benennen. Dazu zählt erstmal jeder Punkt, der unter bestimmten Voraussetzungen von der Fahrzeugbewegung nicht passiert werden darf.

Um doppelte Prüfungen zu vermeiden, sollte bewertet werden, ob alle diese Prüfbedingungen im Target Point Check abgeprüft werden müssen oder ob die Prüfbedingungen bereits durch andere Subroutinen abgeprüft werden, die im Rahmen des MP Requests aufgerufen werden. Beispielsweise könnte die Prüfbedingung F-E340 auf zwei verschiedene Weisen interpretiert werden: „Der primäre sicherungstechnische Zielpunkt (und damit das Ende der Route) darf nicht hinter einer falsch gestellten Weiche liegen[73]“ oder alternativ „Eine Weiche in der Route darf nicht falsch gestellt sein.“ Im ersten Fall wäre es eine Prüfbedingung, die für den Target Point Check relevant ist. Im zweiten Fall würde die Prüfbedingung bei der Überprüfung der Route greifen, während der primäre sicherungstechnische Zielpunkt als feste Vorgabe zu sehen ist.

Da die beantragten Zielpunkte (neben dem primären sicherungstechnischen Zielpunkt kann es weitere Zielpunkte in der Fahrerlaubnis geben, vgl. Kapitel 8.3.2) aufgrund der globalen Anforderung der schlanken Logik nicht selbst durch die smartLogic versetzt werden sollen (vgl. Kapitel 4.3.1), erscheint es sinnvoll, die Überprüfung der Route und der damit verbundenen Voraussetzungen zur Befahrung der Route bis zum gesetzten maßgeblichen Zielpunkt in den bereits beschriebenen Subroutinen durchzuführen und damit verbundene Prüfbedingungen im Rahmen dieser SharedFunction nicht erneut zu überprüfen.

[72] Falls es sekundäre sicherungstechnische Zielpunkte gäbe, müssten ebenfalls die potenziellen Gefahrpunkte bestimmt werden, um die zulässigen Erreichenswahrscheinlichkeiten, die an die Fahrzeugbewegung übermittelt werden müssten, zu überprüfen.

[73] zumindest, wenn sie spitz befahren wird

Für die vorliegende Subroutine bleibt dann zu prüfen, ob die in der beantragten Fahrerlaubnis enthaltenen Zielpunkte in Hinblick auf die vorhandenen Gefährdungen und die damit verbundenen Gefährdungsrisiken unter Berücksichtigung der Erreichenswahrscheinlichkeit der jeweiligen Wirkbereiche der Gefährdungen korrekt gesetzt sind und somit kein Sicherheitsrisiko darstellen (vgl. Kapitel 8.3.2). Hierfür spielen ggf. im Rahmen des MP Requests bereits identifizierte negative Einflüsse auf die Gesamt-Schutzrate an den oben genannten potenziellen Gefahrpunkten eine Rolle. Die bis zum Zeitpunkt des Aufrufs des Target Point Checks berechnete Gesamt-Schutzrate des MP-Requests wird deshalb als Eingangswert an den Target Point Check übergeben.

In Tab. 55 sind alle Prüfbedingungen aufgeführt, die einen Einfluss auf die Zielpunkte haben. Diejenigen Prüfbedingungen, die jedoch nach der oben vorgenommenen Abgrenzung nicht zum Aufgabenbereich der hier thematisierten Subroutine gehören, sind kursiv dargestellt und in der Spalte „Bemerkungen“ findet sich eine entsprechende Erläuterung.

Tab. 55: Relevante Prüfbedingungen für den Target Point Check

ID	Beschreibung	Bemerkung
F-E034, F-E034a	*Passagierzüge müssen für verkehrliche Halte an Bahnsteigen halten, die ausreichend lang sind*	*da die Fahrzeuge die Erfüllung dieser Prüfbedingung, zum Beispiel durch die Freigabe nur eines Teils der Türen, maßgeblich beeinflussen können, wurde entschieden diese Vorgabe in der Verantwortung der Fahrzeuge zu belassen und nur sicherzustellen, dass die Fahrzeuge korrekte Information über die Lage der Bahnsteige haben (vgl. Kapitel 8.6.3)*
F-E035a, F-E035b, F-E035c	Weichen, die keine Rückfallweichen sind, dürfen nicht aufgefahren werden, wenn sie - im Fahrweg liegen - im Gefahrpunktabstand bzw. Durchrutschweg liegen und über ein bewegliches Herzstück verfügen oder mit einem Riegel verschlossen sind	die Prüfbedingung stammt aus der heutigen Stellwerkstechnik und enthält eine Unterscheidung zwischen dem Fahrweg und dem Gefahrpunktabstand bzw. Durchrutschweg; demnach wird das Auffahren von Weichen (außer bei Rückfallweichen) im Fahrweg gar nicht und sonst nur, wenn das Herzstück nicht beweglich ist, erlaubt; übersetzt auf die smartLogic kann eine höhere Wahrscheinlichkeit für das Auffahren von Weichen ohne bewegliches Herzstück akzeptiert werden, als für Weichen mit; dies ist für Zielpunkte mit eingeschränkter Sicherheit relevant
F-E211	Beschränkungen durch DAs müssen beachtet werden	–> kann maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein
F-E001	alle DAs müssen identifiziert sein (bzw. das Restrisiko einer unerkannten DA muss bekannt sein)	Das Restrisiko einer unerkannten DA spielt bei einer möglichen Verschiebung der SvL eine Rolle
F-E122	Einschränkungen (z. B. Geschwindigkeit), die eine RA (z. B. TSR) vorgibt, müssen eingehalten werden	–> kann maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein
F-E122a	Stopps in “Non Stopping Areas” (NSA) sind zu vermeiden	die Zielpunkte sollten nicht in einer NSA liegen

F-E212a	*Fahrzeuge dürfen sich nicht in Gleisabschnitte strecken können, die von anderen Fahrzeugen beansprucht werden*	*entsprechende Sicherheitsreserven sind einzuplanen; es wird jedoch davon ausgegangen, dass dies bei der Ortungsinformationsaggregation geschieht; den Zielpunkt so zu wählen, dass trotz dieser Sicherheitsreserven keine andere Fahrzeugbewegungen am hinteren Ende der betrachteten Fahrzeugbewegung eingeschränkt werden, ist eine nicht sicherheitskritische Aufgabe des TMS*
F-E216	Fahrzeugbewegungen müssen an für sie vorgeschriebenen Betriebshalten halten	dies kann entweder durch das Setzen des Zielpunkts vor den Betriebshalt oder durch eine entsprechende Vorgabe im Geschwindigkeitsprofil erreicht werden; –> im ersten Fall kann der Betriebshalt als maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte betrachtet werden, der nur temporär gilt; dies kann z. B. über eine RA erfolgen, die mit einem umgekehrten Detektionsabschnitt arbeitet, der kurz vor dem Betriebshalt liegt und die standardmäßig aktive RA deaktiviert
F-E217	alle erforderlichen Zustimmungen von externen Systemen müssen vorliegen	liegt die Zustimmung nicht vor, kann die Fahrzeugbewegung den Abschnitt nicht passieren, der Zielpunkt muss also vor dem topologischen Wirkabschnitt des externen Systems liegen –> kann maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein
F-E252	die Route der MA darf keine mit Fahrzeugen beanspruchten Abschnitte enthalten	–> kann maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein
F-E227	die Route der MA darf keine Teile enthalten, die Teil einer anderen MA sind (Ausnahme: überlappende D-Wege)	–> kann bestimmender Gefahrpunkt für die Platzierung der EoA sein; eine SvL hinter einem solchen Punkt ist aber unter bestimmten Voraussetzungen möglich
F-E230	es muss ausreichender Flankenschutz bestehen	bei nicht ausreichendem Flankenschutz verringert sich die Schutzrate ab dem ungeschützten Punkt –> kann maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein Schutzrate wird mittels separater Subroutine ermittelt (vgl. Kapitel 8.6.5) Verschiebung der SvL über einen solchen Punkt kann möglich sein
F-E239	die Einfahrt in Gleise, in denen sich Personen befinden, muss verhindert werden	kann über RAs oder DAs (je nachdem, ob der Aufenthalt geplant oder ungeplant ist) abgebildet werden –> kann maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein die Schutzrate wird mittels separater Subroutine ermittelt (vgl. Kapitel 8.6.6)

F-E264	die maximale Schließzeit am Bahnübergang muss eingehalten werden	siehe Kommentar zur Prüfbedingung in Tab. 49 die Überschreitung der maximalen Schließzeit senkt die Schutzrate beim Überqueren des BÜ; der BÜ kann daher theoretisch ein maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein
F-E265	*Bahnübergänge müssen geschlossen und freigemeldet sein*	*über F-E217 abgedeckt*
F-E270, F-E270b, F-E631	*Gleis-Arbeitsstellen müssen gesichert sein*	*kann über RAs erfolgen, siehe Bemerkung zu F-E239*
F-E275	*es dürfen sich keine Arbeitsmaterialien innerhalb der Fahrzeugbegrenzungslinien befinden*	*siehe Beschreibung in Tab. 49; über F-E122 abgedeckt*
F-E276	*Personen- und Güterzüge dürfen sich im Tunnel nicht begegnen, wenn eine bestimmte Relativgeschwindigkeit überschritten wurde*	*kann über RAs gelöst werden (siehe Kapitel 8.4.6), über F-E122 abgedeckt*
F-E282	*es dürfen keine Hindernisse auf dem Gleis detektiert sein*	*kann jeweils nach Sensor-Meldung über DAs gelöst werden, über F-E211 abgedeckt*
F-E312	Fahrzeugbewegungen müssen sicher vor einem Gleisende zum Stehen kommen	der Zielpunkt muss auf einem Gleis sein
F-E321	*betrieblich gesperrte Gleise dürfen nicht befahren werden, außer mit spezieller Genehmigung*	*kann über RAs gelöst werden, über F-E122 abgedeckt*
F-E340	stellbare Fahrwegelemente auf der Route müssen den richtigen Status haben	–> ein falsch gestellten Fahrwegelement kann maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein
F-E350	*Fahrzeuge dürfen nur auf für sie zugelassenen Gleisabschnitten verkehren*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E351	*BoStrab-Gleise dürfen nur von dafür zugelassenen Fahrzeugen befahren werden*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E352	*rein elektrisch angetriebene Fahrzeuge dürfen nur auf Gleisen verkehren, die mit einem auf dem Fahrzeug verfügbaren Stromsystem ausgerüstet sind*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E353	*die Spurweite muss übereinstimmen*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E354	*eines der erlaubten ATP (Zugbeeinflussungssysteme) muss auf dem Fahrzeug vorhanden sein*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E355	*das Fahrzeug muss für den Fahrweg zugelassen sein*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E356	*der Tf bzw. das ATO-System müssen für den Fahrweg zugelassen sein*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E357, F-E364	*das Fahrzeug muss genügend Bremskraft für die Route haben*	*kann über Gleisbereiche oder RAs gelöst werden*

F-E357a	Fahrzeugbewegungen mit geringem Zugkraftüberschuss dürfen beim Anfahren in steil geneigten Rampen nicht zum Stehen kommen	die Zielpunkte dürfen bei entsprechenden Fahrzeugen nicht in einen entsprechenden Bereich liegen
F-E358	*das Achslastprofil darf auf der Route nicht überschritten werden*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E359	*das Lichtraumprofil bzw. die Fahrzeugbegrenzungslinien müssen eingehalten werden*	*kann über Gleisbereiche oder RAs gelöst werden, siehe auch Kapitel 7.3.9*
F-E361, F-E540	*das Fahrzeug muss über eine betriebsbereite Magnetschienenbremse verfügen, wo dies gefordert ist*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E363	*weitere fahrzeugseitige Vorgaben müssen (je nach Bedarf) übermittelt und eingehalten werden*	*kann über Gleisbereiche oder RAs gelöst werden*
F-E365	die Fahrerlaubnis darf nicht in einen nicht vollüberwachten Bereich führen, (wenn nicht entsprechende Sicherheitsregeln eingehalten werden)	die Zielpunkte dürfen nicht in einem solchen Bereich liegen, da ansonsten die Fahrerlaubnis nur bis zum Beginn des Bereiches erteilt werden dürfte, evtl. mit einer anschließenden Release-Geschwindigkeit
F-E513	*Fahrzeuge mit gehobenem Stromabnehmer dürfen nur Gleise mit Oberleitung benutzen*	*wird durch den Track Information Check abgedeckt (siehe Kapitel 8.6.3)*
F-E611a, F-E613	*Reisendenübergänge (RÜ) müssen geschlossen und freigemeldet sein und dies bleiben, solange die Fahrzeugbewegung den zugehörigen Gleisabschnitt beansprucht*	*Reisendenübergänge können analog zu BÜ als zustimmungspflichtige Stakeholder-Systeme betrachtet werden und als solche auch ein maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein –> wird über Stakeholder abgedeckt (F-E217)*
F-E642	Fahrgäste müssen gewarnt werden, falls der Zug bei der Vorbeifahrt am Bahnhof eine festgelegte Geschwindigkeit überschreiten darf	kann über ein benachrichtigungspflichtiges Stakeholder-System erfolgen; und als solches theoretisch auch ein maßgeblicher Gefahrpunkt für die Platzierung der Zielpunkte sein
F-E750	*akute Gefahrenstellen dürfen nicht passiert werden*	*es wird davon ausgegangen, dass dies über die DAs abgebildet ist, die vom entsprechenden Reaktionsprozess direkt gebildet wird*

Nicht jede Prüfbedingung, die theoretisch einen maßgeblichen Gefahrpunkt für die Platzierung der Zielpunkte bedingen könnte, muss auch tatsächlich maßgeblich für die Ablehnung einer Anfrage sein, falls der vom TMS beantragte primäre sicherungstechnische Zielpunkt hinter diesem Gefahrpunkt liegt. Ob die Prüfanfrage abgelehnt werden muss, hängt von der Erreichenswahrscheinlichkeit dieses Punkts und vom individuellen Einfluss auf die Schutzrate durch die Verletzung dieser Prüfbedingung abhängig von der aktuellen Betriebssituation ab. Den Einfluss auf die Schutzrate zu quantifizieren, ist wie bereits mehrfach erwähnt, nicht Aufgabe der vorliegenden Arbeit (vgl. Kapitel 3.3).

Ablauf der Subroutine in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Ablauf der Subroutine zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf die betrachtete Subroutine auf Basis der Anforderungen aus Kapitel 8.2.1

zu diskutieren und zu entscheiden. Die Vollständigkeit ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt. Der Ablauf der Subroutine ergibt sich zudem aus dem Konzept zu den Zielpunkten, das in Kapitel 8.3.2 erarbeitet wurde.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen in der Subroutine bezogen auf die Kernanforderung der sicheren Logik irrelevant. Die Reihenfolge wird daher nur durch nachgeordnete Anforderungen wie die Anforderung der geringen Latenz sowie praktische Abhängigkeiten (z. B. „Rufe Belegungen ab“ vor „Prüfe auf einen Konflikt“) bedingt. Demnach erscheint es sinnvoll, zunächst die allgemeinen Prüfungen zu den Zielpunkten durchzuführen, da sie zum Teil Ausschlusskriterien für eine erfolgreiche Prüfung der Fahrerlaubnis sind und somit der umfangreichere Berechnungsaufwand zur Ermittlung der Schutzrate für die einzelnen Gefahrpunkte nicht durchgeführt werden muss.

1. Prüfe, ob die in der beantragten Fahrerlaubnis enthaltenen Zielpunkte auf einem Gleis der Topologie innerhalb der beantragten Route liegen
2. Prüfe, ob einer der Zielpunkt in einem nicht vollüberwachten Gleisbereich liegt
3. Prüfe, ob der anzusteuernde Zielpunkt in einer NSA liegt
4. Prüfe, ob ein gesetzter Zielpunkt die Wahrscheinlichkeit für die betrachtete Fahrzeugbewegung erhöht, in einem Gleisabschnitt anzuhalten, in dem das Anfahren wegen eines fehlenden Zugkraftüberschusses dieser Fahrzeugbewegung erschwert sein könnte
5. Ermittele alle möglichen Gefahrpunkte auf der beantragten Route (inkl. Flankenschutz-Gefahrpunkte) und die zugehörigen Gefährdungsrisiken
6. Ermittele für jeden in der beantragten Fahrerlaubnis enthaltenen Zielpunkt das Gesamt-Gefährdungsrisiko des letzten Gefahrpunkts, der von der Fahrzeugbewegung vor dem Zielpunkt erreicht werden würde
7. Berechne unter Beachtung des Gesamt-Gefährdungsrisikos die maximal zulässige Erreichenswahrscheinlichkeit dieses Gefahrpunktes, damit die Gesamt-Schutzrate noch oberhalb des Schwellwerts für die Genehmigung der Prüfanfrage liegt
8. Berechne die tatsächlichen Erreichenswahrscheinlichkeiten und prüfe, ob sie geringer als die maximal zulässige Erreichenswahrscheinlichkeit ist[74] [75] [76]
9. Berechne die neue Gesamt-Schutzrate

Für Gefahrstellen mit flächiger Ausdehnung (Gleisabschnitte) ist der Gefahrpunkt der Beginn dieser Gefahrstelle aus Richtung der betrachteten Fahrzeugbewegung. Ein Gefahrpunkt kann im Sinne des obigen Ablaufs auch durch das Risiko einer unentdeckten DA entstehen.

[74] Die tatsächliche Erreichenswahrscheinlichkeit (aus sicherungstechnischer Sicht) des letzten Gefahrpunkts vor dem anzusteuernden Zielpunkt EoA ist naturgemäß ‚1‘, da dieser Punkt ja immer erreicht werden darf.

[75] Für den Fall, der in Kapitel 8.3.2 ebenfalls diskutiert wurde, dass es möglich wäre, dem Fahrzeug die zulässigen Erreichenswahrscheinlichkeiten zu übermitteln, so dass das Fahrzeug seine Bremskurven entsprechend berechnet, müsste stattdessen geprüft werden, ob die in der Fahrerlaubnis für die jeweiligen Zielpunkte enthaltenen Erreichenswahrscheinlichkeiten kleiner als oder gleich den maximal zulässigen Erreichenswahrscheinlichkeiten sind.

[76] Falls eine Berechnung von Erreichenswahrscheinlichkeiten nicht möglich ist, weil keine sicheren Annahmen zur Erreichenswahrscheinlichkeit validiert sind, kann die Formel zur Bestimmung der Erreichenswahrscheinlichkeit auch zu ‚1‘ gesetzt werden. Das bedeutet, dass kein Gefahrpunkt vor der SvL zulässig ist, bei dem das inverse Gesamt-Gefährdungsrisiko (also der Einfluss auf die Schutzrate) den Schwellwert für die Genehmigung der Prüfanfrage unterschreitet.

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Die Subroutine wird von Prozessfunktionen aufgerufen. Es wird davon ausgegangen, dass alle notwendigen Informationen über das Fahrzeug und die Infrastruktur bereits innerhalb der smartLogic vorliegen. Damit enthält die Subroutine ausschließlich interne Prüfungen und externe Systeme müssen bei der Modellierung nicht berücksichtigt werden.

Aktivitätsdiagramm

Abb. 73 zeigt das Aktivitätsdiagramm zur Subroutine „Target Point Check“.

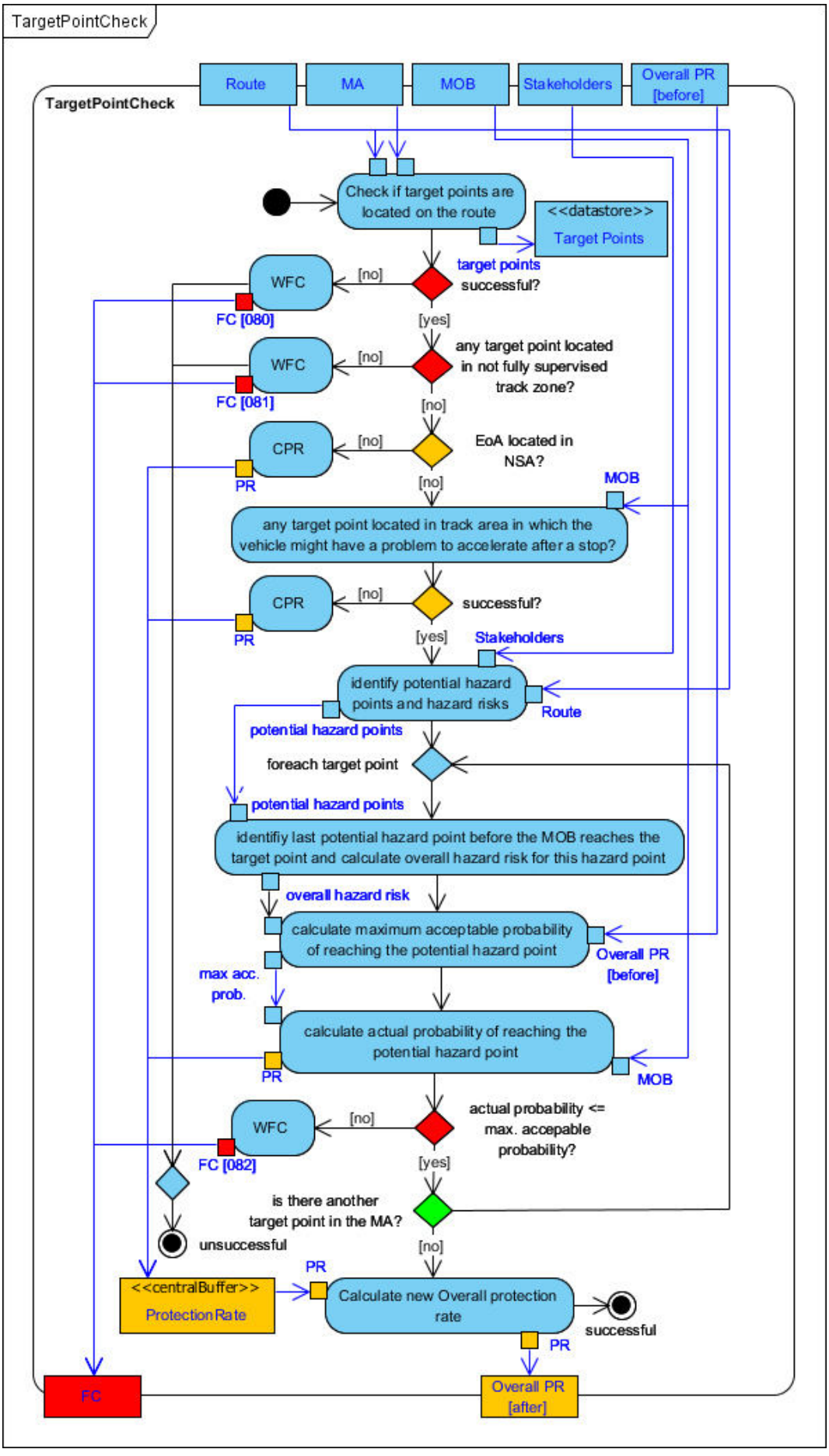


Abb. 73: Aktivitätsdiagramm der Subroutine „Target Point Check“

Erneutes Prüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von Prüfbedingungen als nicht relevant zu überprüfen. Bei der vorliegenden Subroutine ergaben sich keine Änderungen.

8.6.5 Calculate Flank Protection Rate

In diesem Unterkapitel soll die Subroutine zur Berechnung der Flankenschutz-Schutzrate beschrieben werden, die unter anderem im MP Request benötigt wird (vgl. Kapitel 8.5.2). Die Grundlagen dazu wurden bereits in Kapitel 8.3.4 hergeleitet. Der Subroutine muss die beantragte Route übergeben werden und sie gibt die berechnete Flankenschutz-Schutzrate zurück.

Identifizieren der für die Subroutine relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für die Subroutine relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren.

Die Anzahl der relevanten Prüfbedingungen für die Subroutine ist überschaubar, da die Subroutine im Wesentlichen auf die Prüfbedingung F-E230 zurückzuführen ist. Dennoch lassen sich einige weitere Prüfbedingungen mit Bezug zum Flankenschutz finden. Tab. 56 listet die als relevant eingestuften Prüfbedingungen. Wie bereits bei den Prozessfunktionen sind Prüfbedingungen kursiv gedruckt, die zwar als nicht relevant betrachtet werden, bei denen allerdings eine Erläuterung zu dieser Einschätzung sinnvoll erschien.

Tab. 56: Relevante Prüfbedingungen für die Berechnung der Flankenschutz-Schutzrate

ID	Beschreibung	Bemerkung
F-E230	es muss ausreichender Flankenschutz bestehen	
F-E001	alle DAs müssen identifiziert sein (bzw. das Restrisiko einer unerkannten DA muss bekannt sein)	Das Restrisiko einer unerkannten DA muss bei der Berechnung der Flankenschutz-Schutzrate berücksichtigt werden
F-E251	alle Fahrzeuge auf dem Gleis müssen identifiziert sein (bzw. das Restrisiko eines unerkannten Fahrzeugs muss bekannt sein)	Das Restrisiko eines unerkannten Fahrzeugs muss bei der Berechnung der Flankenschutz-Schutzrate berücksichtigt werden
F-E141	Beschränkungen bei Sturm müssen beachtet werden	ggf.: es muss verhindert werden, dass Fahrzeuge zur Erfüllung von Flankenschutzzwecken an gefährlichen Orten festgehalten werden
F-E215a, F-E238	Beanspruchungen dürfen nicht entfernt werden, solange sie benötigt werden	auf Flankenschutz bezogen, muss dies für das Entfernen von Flankenschutzbeanspruchungen gelten
F-E232a	*Schlüsselsperren im Flankenschutzraum müssen gesichert sein*	*vermutlich nicht relevant, da über allgemeine Regeln zum Flankenschutz abgedeckt*
F-E236	falls eingeschränkter Flankenschutz besteht, muss die Geschwindigkeit reduziert sein	funktionale Sicherheitsanforderung an die Rückfallebene; genaue Werte für die Reduktion hängen von der Schutzrate ab und werden in dieser Arbeit nicht ermittelt (vgl. Kapitel 3.3)

F-E264	*die maximale Schließzeit am Bahnübergang muss eingehalten werden*	*theoretisch könnte eine Flankenschutzanforderung dazu führen, dass ein Zug auf dem BÜ für längere Zeit stehen bleibt. In diesem Fall entstünde aber kein Sicherheitsrisiko, da der BÜ bereits besetzt wäre; daher ist die Verhinderung dieses Falls eine nicht sicherheitskritische Aufgabe des TMS*
F-E340	*Fahrwegelemente auf der Route müssen in der richtigen Lage sein*	*da durch die Subroutine Fahrwegelemente (genauer stellbare Fahrwegelemente) nicht umgestellt werden, ist diese Prüfbedingung hier nicht relevant; werden für den Flankenschutz stellbare Fahrwegelemente mit anderem Status benötigt, muss zuvor ein TESC-Request erfolgen*

Es wird angenommen, dass eine Überprüfung der Funktionsbereitschaft der smartLogic nicht erforderlich ist, da dies bereits im aufrufenden Prozess geprüft wurde.

Ablauf der Subroutine in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Ablauf der Subroutine zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf die betrachtete Subroutine auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt. Der Ablauf der Subroutine ergibt sich zudem aus dem Konzept zum Flankenschutz, das in Kapitel 8.3.4 erarbeitet wurde.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen in der Subroutine bezogen auf die Kernanforderung der sicheren Logik irrelevant. Die Reihenfolge wird daher nur durch nachgeordnete Anforderungen wie die Anforderung der geringen Latenz sowie praktische Abhängigkeiten (z. B. „Rufe Belegungen ab“ vor „Prüfe auf einen Konflikt“) bedingt. Insbesondere bei der Bestimmung der Flankenschutz-Schutzrate existieren zahlreiche praktische Abhängigkeiten. Die Reihenfolge der Schritte des Ablaufs der Subroutine orientiert sich daher am Vorgehen aus Kapitel 8.3.4.

Der Ablauf der Subroutine enthält demnach die folgenden Schritte:

1. Bestimme den potenziellen Flankenschutzraum
2. Identifiziere potenziell flankenschutzgebende Objekte (FPOs) für jede Allocation Section (AS) im Flankenschutzraum ausgehend von den AS
3. Frage den Status (die Lage) der potenziell flankenschutzgebenden Elemente (FPDs) ab, (falls dies innerhalb der aktuellen Prüfanfrage nicht bereits geschehen ist)
4. Definiere den aktiven Flankenschutzraum, in dem die maßgeblichen FPOs bestimmt werden (Grenze des potenziellen Flankenschutzraums oder ein FPO mit hoher Schutzrate (vgl. Spalte „Weitersuchen“ in Tab. 45 in Kapitel 8.3.4))
5. Fordere ggf. die Flankenschutz-Funktion bei den FPOs an
6. Identifiziere Gefahrenbereiche im aktiven Flankenschutzraum
7. Identifiziere Beanspruchungen im aktiven Flankenschutzraum
8. Berechne die Flankenschutz-Gefährdungsrate

9. Füge für die FPDs und die Gleissegmente des aktiven Flankenschutzraums Flankenschutzbeanspruchungen hinzu
10. Übergebe die berechnete Flankenschutz-Schutzrate an den auslösenden Prozess

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Da Subroutinen durch Prüfprozesse der smartLogic aufgerufen werden, ist das aufrufende System bei Subroutinen immer die smartLogic selbst. Als externe Systeme findet im Prozess eine Kommunikation mit stellbaren Fahrwegelementen (MTEs), Stakeholder-Systemen und Fahrzeugen statt, da diese Flankenschutz-Aufgaben wahrnehmen können.

Aktivitätsdiagramm

Um die Aktivitätsdiagramme besser verständlich zu machen, ist die Subroutine auf mehrere Diagramme aufgeteilt (einzelne Teile bilden quasi eine Subroutine für andere Teile). Abb. 74 zeigt den Hauptablauf, während Abb. 75, Abb. 76 und Abb. 77 die weiteren Subroutinen darstellt, die während des Ablaufs aufgerufen werden. Zur besseren Orientierung sind die jeweiligen „Call Behaviour Actions“ (vgl. Kapitel 2.6.2, Abschnitt „Ausführlicherer Hintergrund zur UML“) in der Farbe des jeweiligen Diagramms markiert.

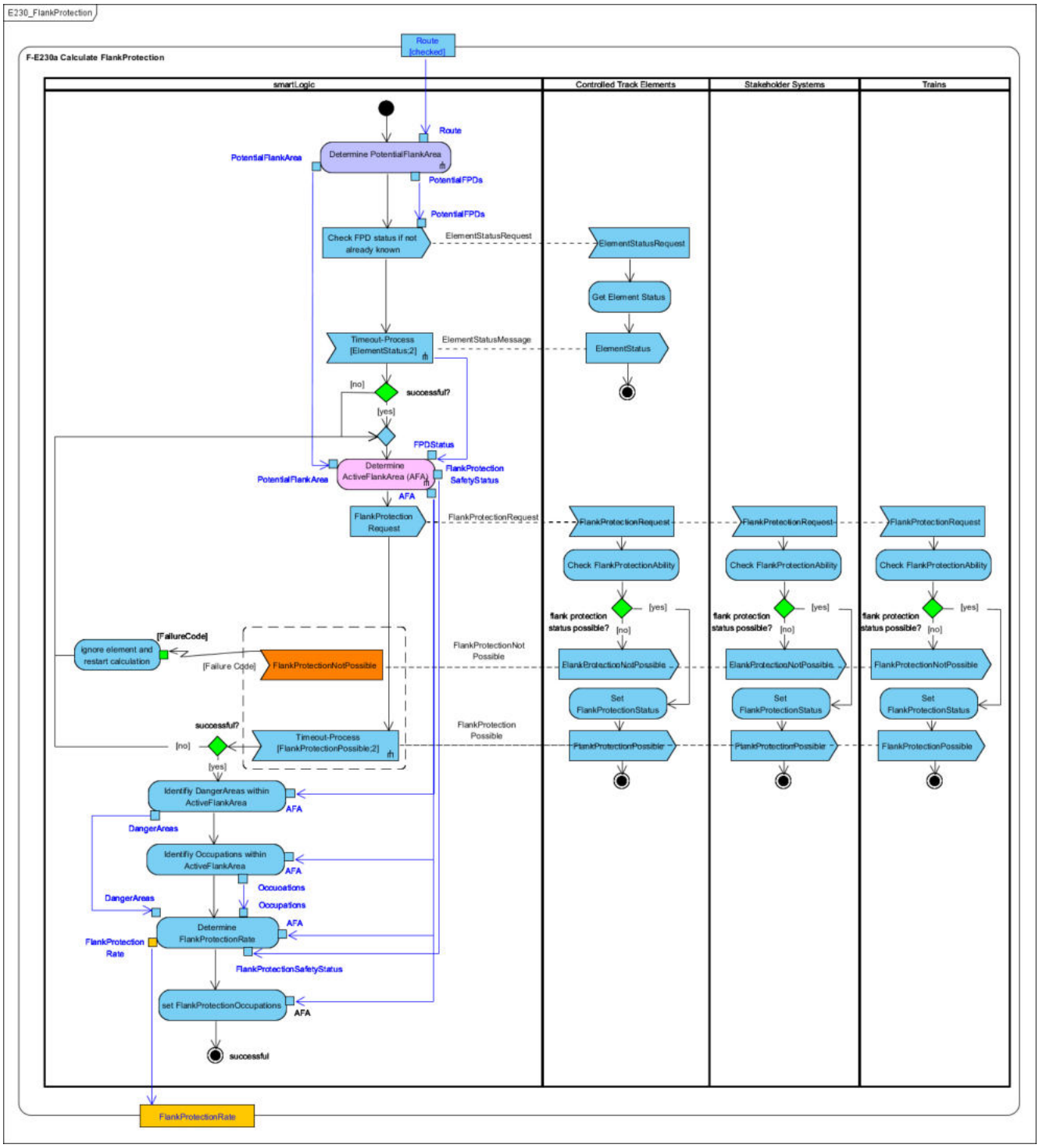


Abb. 74: Aktivitätsdiagramm der Subroutine „Calculate Flank Protection Rate“

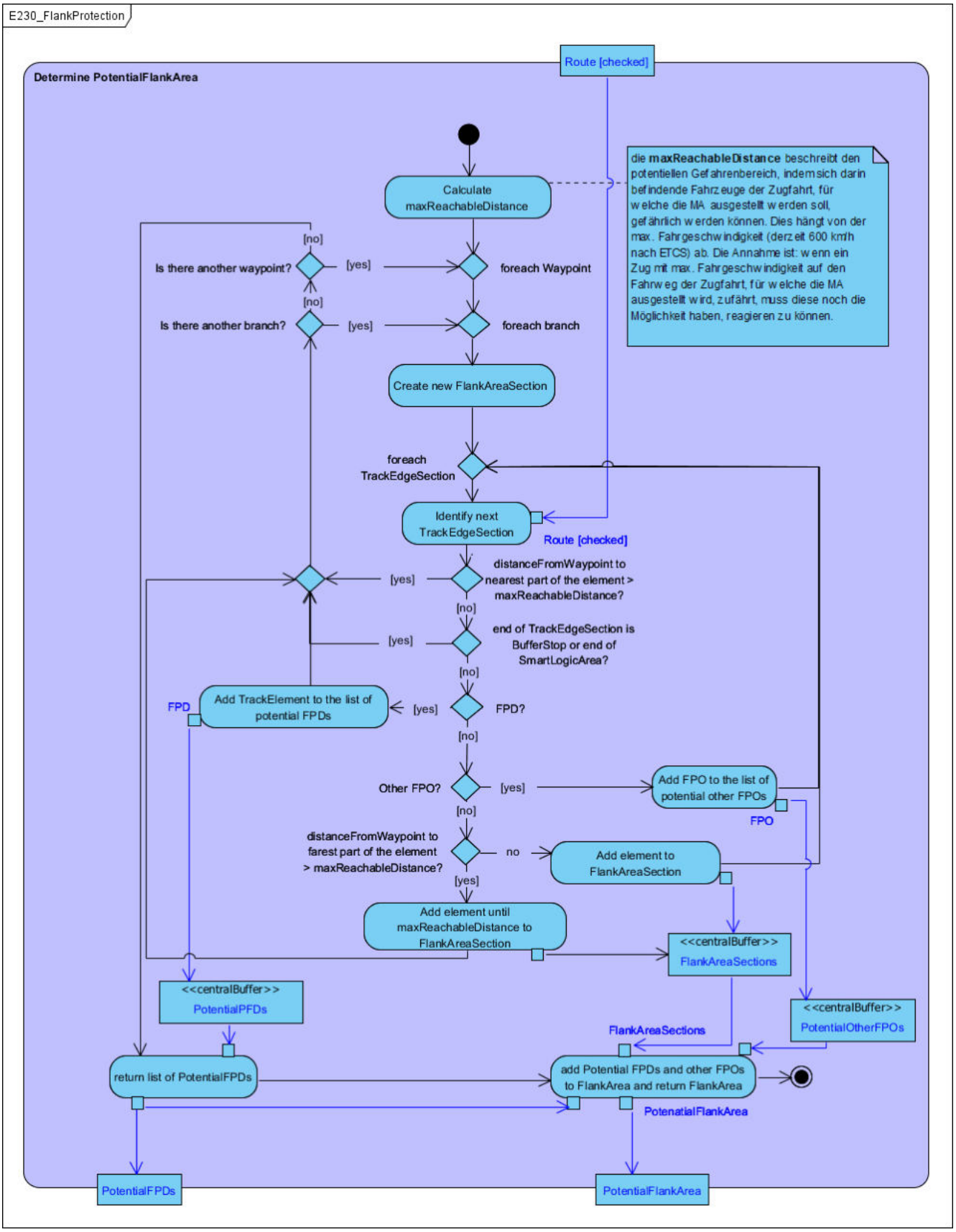


Abb. 75: Aktivitätsdiagramm der Subroutine zur Bestimmung des potenziellen Flankenschutzraums

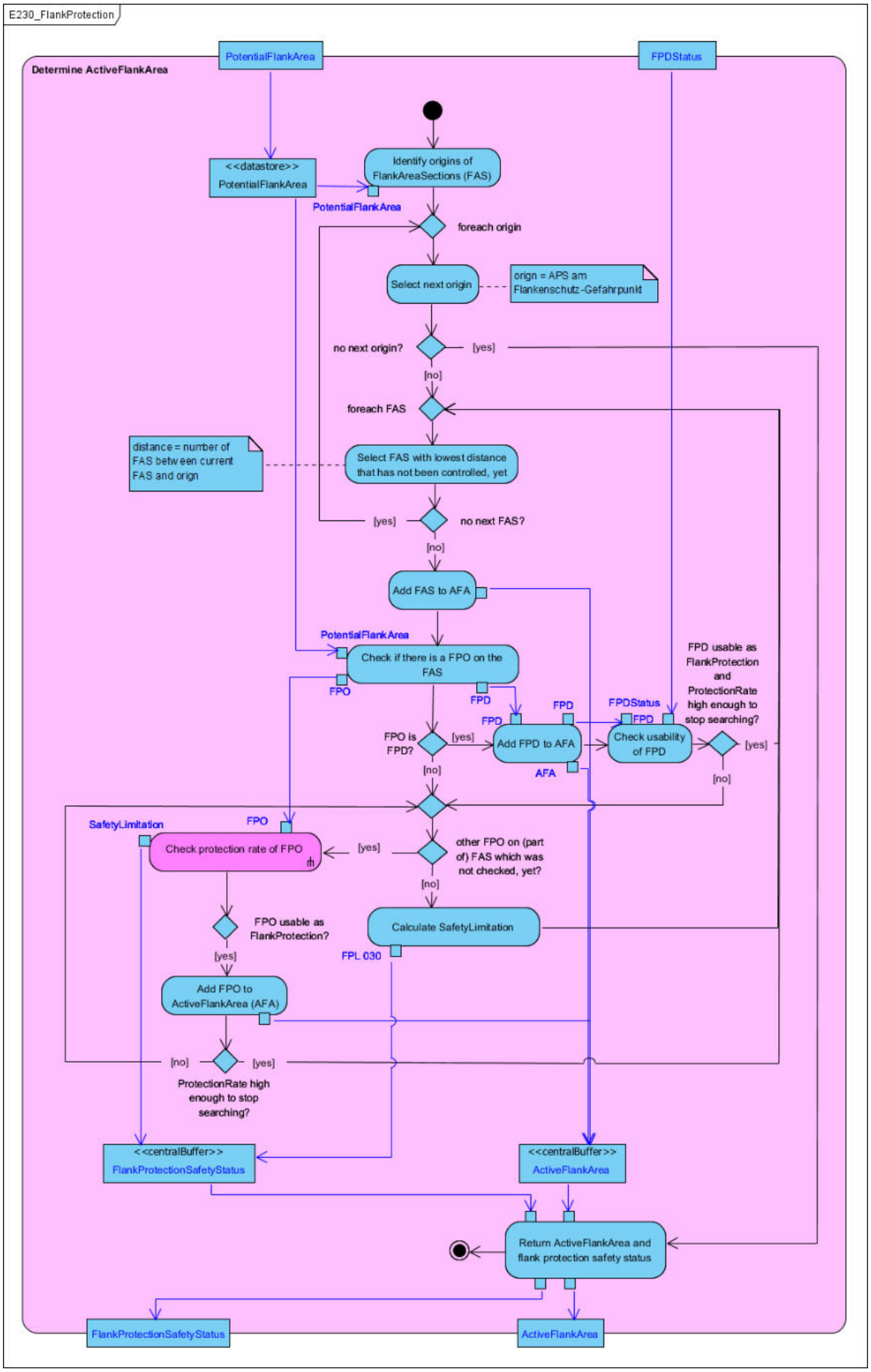


Abb. 76: Aktivitätsdiagramm der Subroutine zur Bestimmung des aktiven Flankenschutzraums

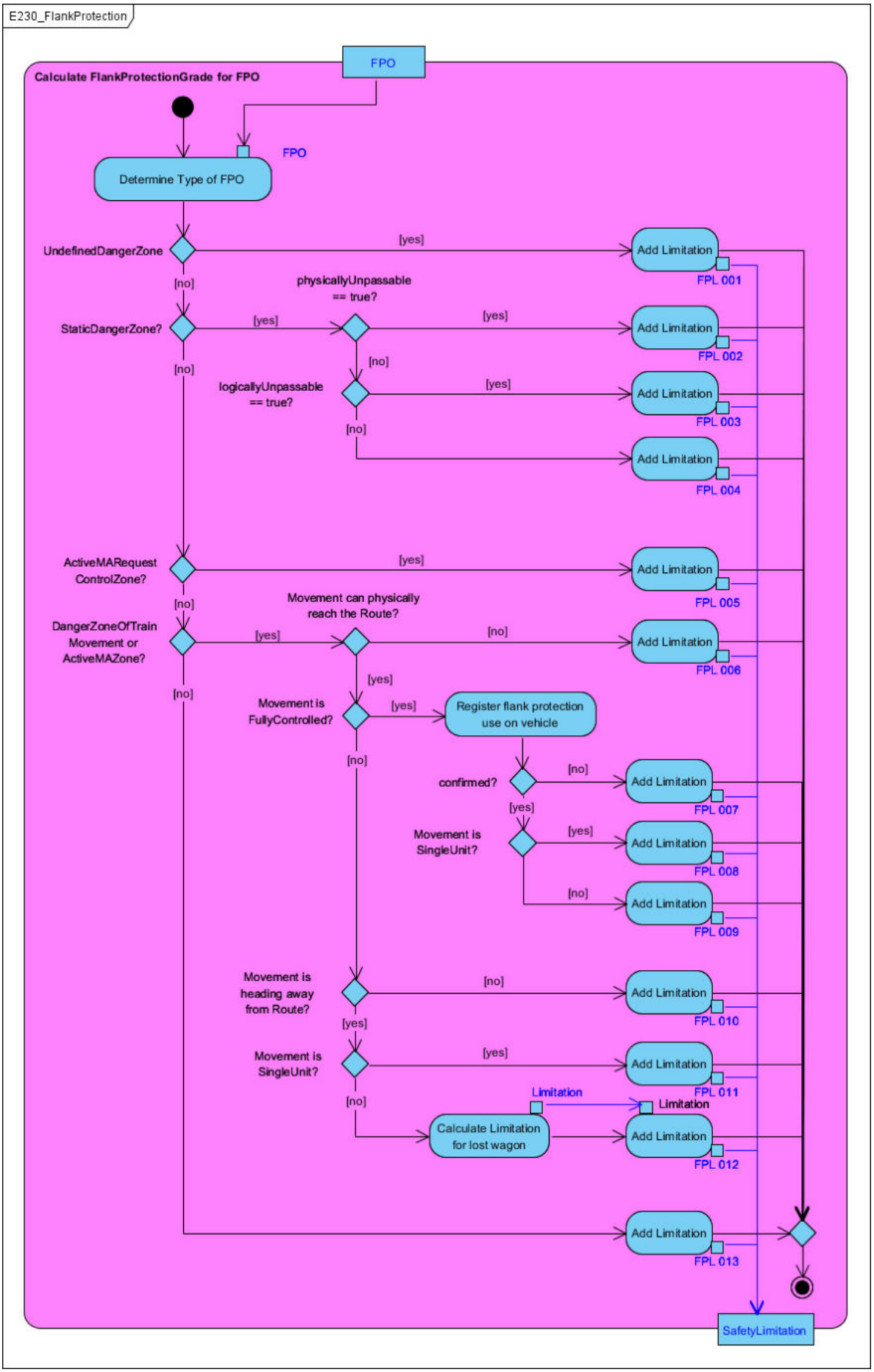


Abb. 77: Aktivitätsdiagramm der Subroutine zur Bestimmung der Flankenschutz-Schutzrate für ein FPO

Erneutes Prüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von Prüfbedingungen als nicht relevant zu überprüfen. Gegebenenfalls veränderte Einstufungen sind dabei iterativ in die bisher in diesem Unterkapitel vorgestellten Ergebnisse eingeflossen.

8.6.6 RA/Track Restriction Check

In der Subroutine „RA/Track Restriction Check“ wird überprüft, ob die Einschränkungen, die mittels RAs definiert sind, eingehalten werden. Vergleiche zum Konzept der RAs Kapitel 7.3.6. Die Subroutine benötigt die beantragte Route, die beantragte MA und die Fahrzeugdaten als Eingangsdaten und gibt eine Liste an aktiven RAs zurück, die für die Prüfanfrage relevant sind, sowie die berechnete Schutzrate.

Identifizieren der für die Subroutine relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für die Subroutine relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren.

Tab. 57 listet die relevanten Prüfbedingungen für den „RA/Track Restriction Check“. Kriterien für die Relevanz sind, ob die Prüfbedingung eine Einschränkung enthält, die sich auf einen bestimmten Gleisabschnitt (Wirkabschnitt oder Detektionsabschnitt, vgl. Kapitel 7.3.5) bezieht. Kontraindikation (kursiv) ist vor allem, wenn sich die Prüfbedingung auf eine Ursache der RA bezieht, da diese Prüfbedingungen damit für die Einrichtung der RA relevant sind. Dies gilt auch für Prüfbedingungen, die bereits Teil des „Track Information Check“ (vgl. Kapitel 8.6.3) sind.

Tab. 57: Relevante Prüfbedingungen für den RA/Track Restriction Check

ID	Beschreibung	Bemerkung
F-E122	Einschränkungen, die eine RA vorgibt, müssen eingehalten werden	
F-E122a	Stopps in “Non Stopping Areas” (NAS) sind zu vermeiden	konkrete Ausprägung einer RA
F-E122b	die Geschwindigkeit, die eine passierte RA (z. B. TSR) vorgibt, darf nicht überschritten werden, (wenn die Fahrzeugbewegung die auf die Fahrzeugcharakteristik bezogenen Einschränkungen der RA erfüllt)	passt inhaltlich auch zum „SSP Check“; Geschwindigkeitseinschränkungen durch RAs werden deshalb in der vorliegenden Subroutine identifiziert und an den auslösenden Prozess zurückgegeben, so dass sie vom auslösenden Prozess ggf. an den SSP Check zur Prüfung weitergegeben werden können
F-E641	*Geschwindigkeitsprofile in Ladeeinrichtungen und an Bahnsteigen müssen eingehalten werden*	*die Geschwindigkeitsbereiche können über Gleisbereiche oder als RAs modelliert werden, bei Letzterem siehe die Bemerkung zu F-E122b*
F-E141	*Beschränkungen bei Sturm müssen beachtet werden*	*konkrete Ausprägung einer RA; bezieht sich auf die Einrichtung von RAs; RA kann z. B. durch Sensor (Stakeholder-System) aktiviert werden; bewirkt Geschwindigkeitsänderung und Gleissperrungen*

F-E142, F-E143	*Beschränkungen bei Eiszapfenbildungsgefahr müssen beachtet werden*	*konkrete Ausprägung einer RA; bezieht sich auf die Einrichtung von RAs; RA kann z. B. durch Sensor (Stakeholder-System) aktiviert werden; bewirkt u. a. Geschwindigkeitsänderung und Gleissperrungen*
F-E144	*Beschränkungen bei vereisten Schienen müssen beachtet werden*	*konkrete Ausprägung einer RA; bezieht sich auf die Einrichtung von RAs; RA kann z. B. durch Sensor (Stakeholder-System) aktiviert werden; bewirkt Geschwindigkeitsänderung*
F-E145	*Beschränkungen bei Schnee auf den Schienen müssen beachtet werden*	*konkrete Ausprägung einer RA; bezieht sich auf die Einrichtung von RAs; RA kann z. B. durch Sensor (Stakeholder-System) aktiviert werden; bewirkt Geschwindigkeitsänderung*
F-E239	*die Einfahrt in Gleise, in denen sich Personen befinden, muss verhindert werden*	*konkrete Ausprägung einer RA; bezieht sich auf die Einrichtung von RAs; RA kann z. B. durch Stakeholder-System aktiviert werden; bewirkt Gleissperrung*
F-E270, F-E270b, F-E631	*Gleis-Arbeitsstellen müssen gesichert sein*	*siehe Bemerkung zu F-E239*
F-E632	*Geschwindigkeitsbegrenzung in Baustellenbereichen müssen eingehalten werden*	*siehe Bemerkung zu F-E122b*
F-E276	Personen- und Güterzüge dürfen sich im Tunnel nicht begegnen, wenn eine bestimmte Relativgeschwindigkeit überschritten wurde	konkrete Ausprägung einer RA, vgl. Kapitel 8.4.6
F-E321	betrieblich gesperrte Gleise dürfen nicht befahren werden, außer mit spezieller Genehmigung	die betriebliche Sperrung ist eine konkrete Ausprägung einer RA
F-E350	Fahrzeuge dürfen nur auf für sie zugelassenen Gleisabschnitten verkehren	kann als konkrete Ausprägung einer RA modelliert werden; kann auch als Gleisbereich modelliert werden, wenn in größerem Bereich gültig
F-E351	BoStrab-Gleise dürfen nur von dafür zugelassenen Fahrzeugen befahren werden	kann als konkrete Ausprägung einer RA modelliert werden; allerdings bietet sich die Modellierung über einen Gleisbereich aufgrund des großflächigen Geltungsgebiets eher an
F-E352	rein elektrisch angetriebene Fahrzeuge dürfen nur auf Gleisen verkehren, die mit einem auf dem Fahrzeug verfügbaren Stromsystem ausgerüstet sind	kann als konkrete Ausprägung einer RA modelliert werden; kann auch als Gleisbereich modelliert werden, wenn in größerem Bereich gültig
F-E353	die Spurweite muss übereinstimmen	die Modellierung über RAs erscheint eher nicht sinnvoll, da es sich immer um größere Bereiche handeln dürfte

F-E354	eines der erlaubten ATP (Zugbeeinflussungssysteme) muss auf dem Fahrzeug vorhanden sein	kann als konkrete Ausprägung einer RA modelliert werden; allerdings bietet sich die Modellierung über einen Gleisbereich aufgrund des großflächigen Geltungsgebiets eher an
F-E355	das Fahrzeug muss für den Fahrweg zugelassen sein	kann als konkrete Ausprägung einer RA modelliert werden; allerdings bietet sich die Modellierung über einen Gleisbereich aufgrund des großflächigen Geltungsgebiets eher an
F-E356	der Tf bzw. das ATO-System müssen für den Fahrweg zugelassen sein	kann als konkrete Ausprägung einer RA modelliert werden; allerdings bietet sich die Modellierung über einen Gleisbereich aufgrund des großflächigen Geltungsgebiets eher an
F-E357, F-E364	das Fahrzeug muss genügend Bremskraft für die Route haben	kann als konkrete Ausprägung einer RA modelliert werden; kann auch als Gleisbereich modelliert werden, wenn in größerem Bereich gültig
F-E357a	Fahrzeugbewegungen mit geringem Zugkraftüberschuss dürfen beim Anfahren in steil geneigten Rampen nicht zum Stehen kommen	konkrete Ausprägung einer RA
F-E358	das Achslastprofil darf auf der Route nicht überschritten werden	kann als konkrete Ausprägung einer RA modelliert werden; kann auch als Gleisbereich modelliert werden, wenn in größerem Bereich gültig
F-E359	das Lichtraumprofil bzw. die Fahrzeugbegrenzungslinien müssen eingehalten werden	kann als konkrete Ausprägung einer RA modelliert werden; kann auch als Gleisbereich modelliert werden, wenn in größerem Bereich gültig, siehe Kapitel 7.3.9
F-E361, F-E540	das Fahrzeug muss über eine betriebsbereite Magnetschienenbremse verfügen, wo dies gefordert ist	konkrete Ausprägung einer RA
F-E362, F-E540, F-E541	*die Benutzung der Magnetschienenbremse muss verhindert werden, wo ihre Benutzung nicht erlaubt ist*	*konkrete Ausprägung einer RA; wird über Track Information Check abgedeckt*
F-E363	*weitere fahrzeugseitige Vorgaben müssen (je nach Bedarf) übermittelt und eingehalten werden*	*mögliche konkrete Ausprägungen einer RA; wird über Track Information Check abgedeckt*
F-E411, F-E412	gefährliche Längs-Beschleunigungen bzw. seitliche Beschleunigungen müssen vermieden werden	konkrete Ausprägung einer RA
F-E431	*Fahrzeugtüren dürfen nur geöffnet werden, wenn sich das Fahrzeug am Bahnsteig befindet*	*der Bahnsteig kann als Gleisabschnitt modelliert werden, gibt aber keine Einschränkung vor und wird daher nicht als RA betrachtet*
F-E432	*Trittstufen müssen zum richtigen Zeitpunkt ausgefahren werden*	*konkrete Ausprägung einer RA wird über Track Information Check abgedeckt*

F-E510, F-E512, F-E726, F-E726a	*der Stromabnehmer muss an den richtigen Punkten gesenkt und gehoben werden*	*kann eine konkrete Ausprägung einer RA sein wird über Track Information Check abgedeckt*
F-E513	*Fahrzeuge mit gehobenem Stromabnehmer dürfen nur Gleise mit Oberleitung benutzen*	*Prüfbedingung für das Fahrzeug, siehe auch „Track Information Check", siehe F-E352*
F-E643	*das Fahrzeug muss alle vorgeschriebenen Warnungen durchführen (z. B. Pfeifen, Läuten)*	*der Standort kann als RA modelliert werden wird über Track Information Check abgedeckt*

Ablauf der Subroutine in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Ablauf der Subroutine zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf die betrachtete Subroutine auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt.

Auf Basis der Prüfbedingungen mit konkreten Ausprägungen der RAs ist die Liste der Arten der RAs in Kapitel 7.3.6 zu ergänzen. Da die dortige Liste nicht als vollständig betrachtet wird – wie im dortigen Kapitel beschrieben –, ist es sinnvoll, die Subroutine generisch zu formulieren und nur auf die genannte Liste zu verweisen.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen in der Subroutine bezogen auf die Kernanforderung der sicheren Logik irrelevant. Die Reihenfolge wird daher nur durch nachgeordnete Anforderungen wie die Anforderung der geringen Latenz sowie praktische Abhängigkeiten (z. B. „Rufe Belegungen ab" vor „Prüfe auf einen Konflikt") bedingt.

Zunächst müssen vorhandene RAs identifiziert werden, die einen Wirkabschnitt auf der beantragten Route haben. Solche RAs werden als für die Prüfanfrage aktive RAs bezeichnet. Die RAs werden als Gleisabschnitte nach Kapitel 7.3.3, Abschnitt „Modellierung von ein- oder mehrdimensional gültigen Informationsobjekten (Gleisabschnitte)" mit den Gleissegmenten verknüpft, d. h. jedes Gleissegment hat eine Liste mit verknüpften RAs. Die aktiven RAs können also identifiziert werden, indem die RAs aus den zur Route gehörenden Gleissegmente ausgelesen werden. Ist die RA von einem Detektionsabschnitt abhängig, ist der Status des Detektionsabschnitts zu prüfen. Weiterhin ist zu prüfen, ob die RA für die betrachtete Fahrzeugbewegung gültig ist (vgl. Tab. 29 in Kapitel 7.3.6). Die so identifizierten aktiven RA-Objekte können für eine mögliche weitere Verwendung, beispielsweise im Rahmen der Überprüfung des beantragten Geschwindigkeitsprofils, in einer Liste gespeichert werden, die bei Beendigung der Subroutine an den aufrufenden Prozess zurückgegeben werden.

Anschließend müssen die durch die MA definierten Vorgaben und Einschränkungen mit den Vorgaben in der MA abgeglichen werden. Für nicht erfüllte Einschränkungen oder Vorgaben muss die jeweilige Teil-Schutzrate berechnet werden. Nachdem alle RAs geprüft wurden, ist die Schutzrate für den „RA/Track Restriction Check" zu berechnen.

Der Ablauf der Subroutine kann daher wie folgt beschrieben werden:

1. Prüfe für jedes Gleissegment der Route, ob es einen oder mehrere Wirkabschnitte von RAs enthält

2. Prüfe für jede gefundene RA, ob diese von einem Detektionsabschnitt abhängt
3. Prüfe für jede gefundene RA, ob deren Gültigkeit auf bestimmte Fahrzeugbewegungen eingeschränkt ist und ob die betrachtete Fahrzeugbewegung dazu gehört
4. Füge RAs, die für die betrachtete Fahrzeugbewegung gültig sind und, falls sie einen Detektionsabschnitt haben, deren Detektionsabschnitt aktiv ist, zur Liste der aktiven RAs dem Request hinzu.
5. Prüfe, ob die Einschränkungen bzw. Vorgaben der aktiven RAs im Request enthalten sind.
6. Falls nicht, berechne den Einfluss auf die Schutzrate durch die verletzte RA
7. Wenn alle aktiven RA geprüft wurden, berechne die Schutzrate

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Die Subroutine wird von Prozessfunktionen aufgerufen. Es wird davon ausgegangen, dass alle notwendigen Informationen über das Fahrzeug und die Infrastruktur bereits innerhalb der smartLogic vorliegen. Damit enthält die Subroutine ausschließlich interne Prüfungen und externe Systeme müssen bei der Modellierung nicht berücksichtigt werden.

Aktivitätsdiagramm

Abb. 78 zeigt das Aktivitätsdiagramm zur Subroutine „RA/Track Restriction Check“.

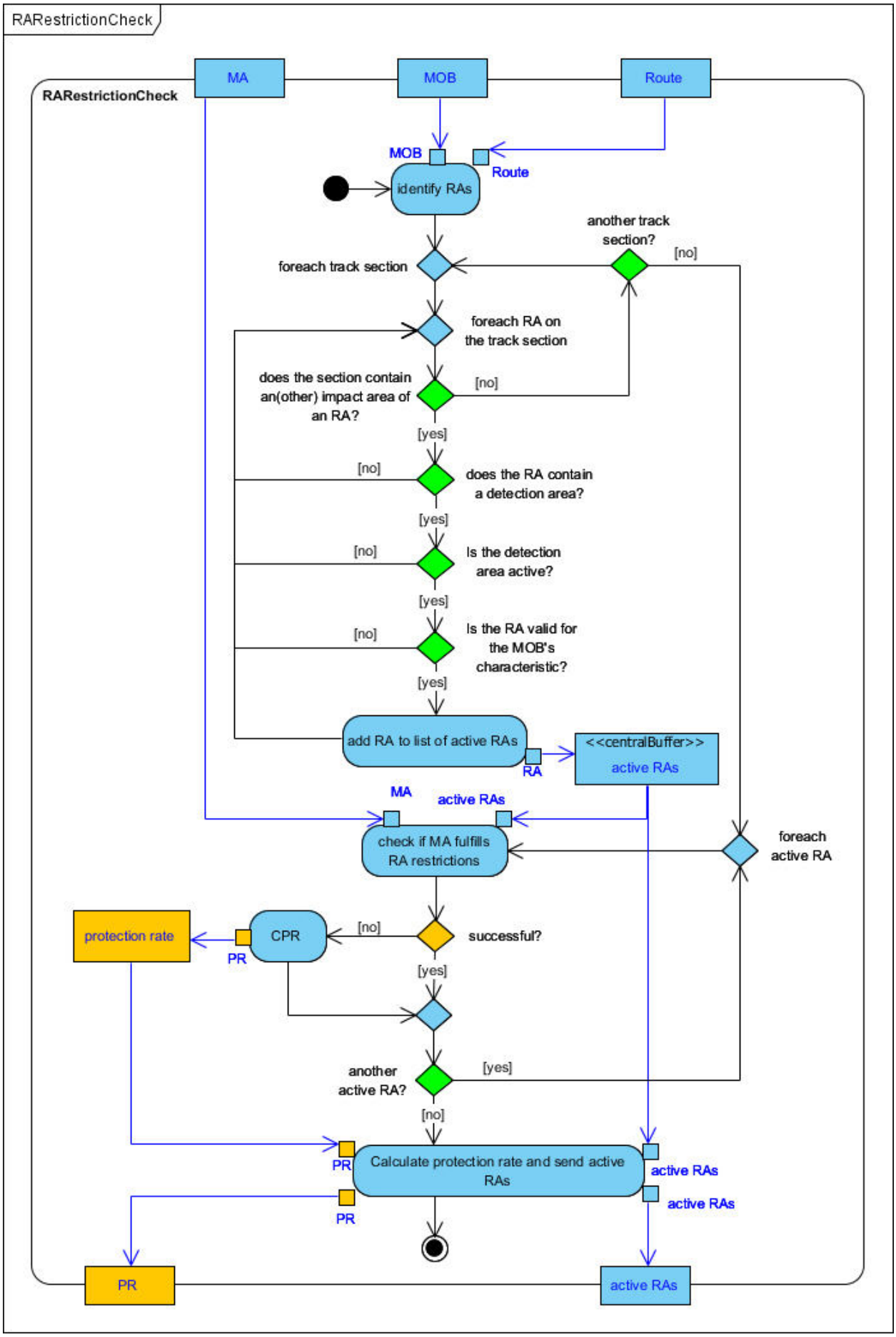


Abb. 78: Aktivitätsdiagramm der Subroutine „RA/Track Restriction Check“

Erneutes Prüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von Prüfbedingungen als nicht relevant zu überprüfen. Gegebenenfalls veränderte Einstufungen sind dabei iterativ in die bisher in diesem Unterkapitel vorgestellten Ergebnisse eingeflossen.

8.6.7 SSP Check

In dieser Subroutine soll das Geschwindigkeitsprofil einer beantragten MA auf Übereinstimmung mit den sicherheitskritischen Vorgaben geprüft werden. Die Subroutine benötigt die Route, die beantragte Fahrerlaubnis, in der das beantragte Geschwindigkeitsprofil enthalten ist und die Liste der aktiven RAs als Eingangsdaten und gibt bei negativem Prüfergebnis einen Fehlercode zurück. (Bei positivem Prüfergebnis muss nichts zurückgegeben werden.)

Identifizieren der für die Subroutine relevanten Prüfbedingungen

Gemäß der in Kapitel 8.2.2 hergeleiteten fünfstufigen Vorgehensweise sind zunächst die für die Subroutine relevanten Prüfbedingungen aus dem Funktionskatalog in Anlage 2 zu identifizieren.

Tab. 58 listet die Prüfbedingungen, die etwas mit der Geschwindigkeit zu tun haben, mit der die Infrastruktur durch die Fahrzeugbewegung befahren werden darf. Die Liste zeigt, dass es viele Einflüsse auf die Geschwindigkeit gibt. Jedoch können durch das generische Konzept der RAs viele der geschwindigkeitsbezogenen Prüfbedingungen in einer generischen Prüfbedingung (F-E122) abgedeckt werden. Diese fordert, dass Geschwindigkeitsbegrenzungen, die in RAs für Fahrzeugbewegungen mit bestimmten Charakteristika (vgl. Kapitel 7.3.6) festgelegt werden, von den Fahrzeugbewegungen einzuhalten sind und demnach im beantragten SSP berücksichtigt sein müssen.

Tab. 58: Relevante Prüfbedingungen für den SSP Check

ID	Beschreibung	Bemerkung
F-E121	die Streckengeschwindigkeit bzw. auf dem jeweiligen Gleis zulässige Geschwindigkeit darf nicht überschritten werden	ggf. differenziert nach Neigetechnik-Klassen (siehe auch F-E121b)
F-E121a	*die Geschwindigkeit, die von Infrastrukturelementen vorgegeben wird, darf nicht überschritten werden*	*kann für verzweigende Fahrwegelemente über F-E121 abgedeckt werden; die Geschwindigkeiten werden über die Verknüpfungen der Gleissegmente angegeben; andere Elemente, die die Geschwindigkeit beeinflussen, müssen dies über die RA in ihrem Wirkabschnitt angeben, dann gilt F-E122*
F-E121b	Geschwindigkeitsdifferenzierungen abhängig von vorhandener Neigetechnik müssen korrekt an den Zug übermittelt werden	Spezialfall von F-E121, muss bei F-E121 beachtet werden
F-E129	über Gleisbereiche angegebene, globale temporäre Geschwindigkeitsvorgaben müssen eingehalten werden	z. B. bei bestimmten Wetterereignissen mit großflächigem Einfluss (sonst ist die Angabe über eine RA sinnvoller)

F-E122, F-E122b	die Geschwindigkeit, die eine RA (z. B. TSR) vorgibt, darf nicht überschritten werden, (wenn die Fahrzeugbewegung die auf die Fahrzeugcharakteristik bezogenen Einschränkungen der RA erfüllt)	
F-E211	Beschränkungen durch DAs müssen beachtet werden	
F-E641	*Geschwindigkeitsprofile in Ladeeinrichtungen und an Bahnsteigen müssen eingehalten werden*	*kann über Gleisbereiche, die auf dem jeweiligen Gleis zulässige Geschwindigkeit oder von einem Sensorwert abhängige RAs modelliert werden (z. B. wenn die Einschränkung nur in bestimmten Fällen gilt)*
F-E141	*Beschränkungen bei Sturm müssen beachtet werden*	*kann über RAs oder Gleisbereiche modelliert werden*
F-E142, F-E143	*Beschränkungen bei Eiszapfenbildungsgefahr müssen beachtet werden*	*kann über RAs modelliert werden*
F-E144	*Beschränkungen bei vereisten Schienen müssen beachtet werden*	*kann über RAs modelliert werden*
F-E145	*Beschränkungen bei Schnee auf den Schienen müssen beachtet werden*	*kann über RAs modelliert werden*
F-E632	*Geschwindigkeitsbegrenzung in Baustellenbereichen müssen eingehalten werden*	*kann über RAs modelliert werden*
F-E276	*Personen- und Güterzüge dürfen sich im Tunnel nicht begegnen, wenn eine bestimmte Relativgeschwindigkeit überschritten wurde*	*kann über RAs gelöst werden, siehe Kapitel 8.4.6*
F-E411, F-E412	*gefährliche Längs-Beschleunigungen bzw. seitliche Beschleunigungen müssen vermieden werden*	*tritt die Gefährdung ohne Befahrung einer Weiche auf, kann die Geschwindigkeits-einschränkung über statische RA festgelegt werden; tritt die Gefährdung nur in Zusammenhang mit einer Weiche auf, kann sie über eine RA modelliert werden, die einen Detektionsabschnitt unmittelbar hinter dem Verzweigungspunkt der Topologie auf dem Weichenstrang enthält, der vom Fahrzeug befahren wird*
F-E515	*Fahrzeuge müssen mit der richtigen Geschwindigkeit Gleisabschnitte mit defekter oder nicht vorhandener Oberleitung befahren*	*kann über RAs oder DAs abgedeckt werden*
F-E642	*Fahrgäste müssen gewarnt werden, falls der Zug bei der Vorbeifahrt am Bahnhof eine festgelegte Geschwindigkeit überschreiten darf*	*diese Prüfbedingungen haben zwar etwas mit der Geschwindigkeit zu tun, allerdings wird hierdurch das Geschwindigkeitsprofil nur in der Rückfallebene eingeschränkt; die*

F-E721	*im Falle, dass technische Sicherheit an einem verzweigenden Fahrwegelement nicht gegeben ist, muss sichergestellt werden, dass das Element nur mit eingeschränkter Geschwindigkeit befahren werden darf*	*Prüfbedingung fließt daher gemäß dem Konzept zu Rückfallebenen in Kapitel 8.3.6 in die Berechnung der Schutzrate bei der entsprechenden Rückfallebene ein und muss hier nicht mehr geprüft werden*
F-E722	*die Geschwindigkeit muss auf dem topologischen Abschnitt eines stellbaren Fahrwegelements stark reduziert werden, falls das Element manuell gesteuert wird*	

Ablauf der Subroutine in natürlicher Sprache

Die Vorformulierung des Prüfprozesses in natürlicher Sprache dient gemäß Kapitel 8.2.2 dazu, einen Überblick über den Ablauf der Subroutine zu erhalten und erforderliche grundsätzliche Design-Entscheidungen bezogen auf die betrachtete Subroutine auf Basis der Anforderungen aus Kapitel 8.2.1 zu diskutieren und zu entscheiden. Die Vollständigkeit ist dabei über den systematischen Prozess zur Identifizierung der funktionalen Anforderungen in Kapitel 6 mit den in Kapitel 8.2.2 diskutierten Einschränkungen für die Auswahl der relevanten Prüfbedingungen sichergestellt.

Der Ablauf der Subroutine kann aus einer sequentiellen Abfrage der einzelnen Prüfbedingungen bestehen, bei der die einzelnen Geschwindigkeitsvorgaben abgeprüft werden. Wird eine Geschwindigkeit nicht eingehalten, bricht der die Subroutine auslösende Prozess immer ab, da das TMS sofort eine neue Anfrage mit verminderter Geschwindigkeit stellen kann. Es wird daher keine neue Schutzrate berechnet.

Da die Prüfbedingungen untereinander unverknüpft sind und ihre Erfüllung daher unabhängig voneinander erfolgen kann, ist die Reihenfolge der Abprüfung der Prüfbedingungen in der Subroutine bezogen auf die Kernanforderung der sicheren Logik irrelevant.

1. Prüfe, ob die Streckengeschwindigkeit eingehalten wird
2. Prüfe, ob die in der Topologie hinterlegten Geschwindigkeiten eingehalten werden
3. Prüfe, ob über Gleisbereiche festgelegte Geschwindigkeiten eingehalten werden
4. Prüfe, ob durch RAs bedingte Geschwindigkeiten eingehalten werden.
5. Prüfe, ob durch DAs bedingte Geschwindigkeiten eingehalten werden
6. Prüfe, ob weitere Geschwindigkeitsvorgaben zu beachten sind, z. B. aufgrund einer verminderten Flankenschutz-Schutzrate

Beteiligte externe Systeme

Als externe Systeme kommen die in Kapitel 4.6 benannten Umsysteme der smartLogic in Betracht, die am Ablauf des Prüfprozesses (vgl. voriger Abschnitt) beteiligt sind, wobei die Datenhaltungssysteme nicht betrachtet werden (vgl. Kapitel 8.2.2). Die Subroutine wird von Prozessfunktionen aufgerufen. Es wird davon ausgegangen, dass alle notwendigen Informationen über das Fahrzeug und die Infrastruktur bereits innerhalb der smartLogic vorliegen. Damit enthält die Subroutine ausschließlich interne Prüfungen und externe Systeme müssen bei der Modellierung nicht berücksichtigt werden.

Aktivitätsdiagramm

Abb. 79 zeigt das Aktivitätsdiagramm zur Subroutine „SSP Check“.

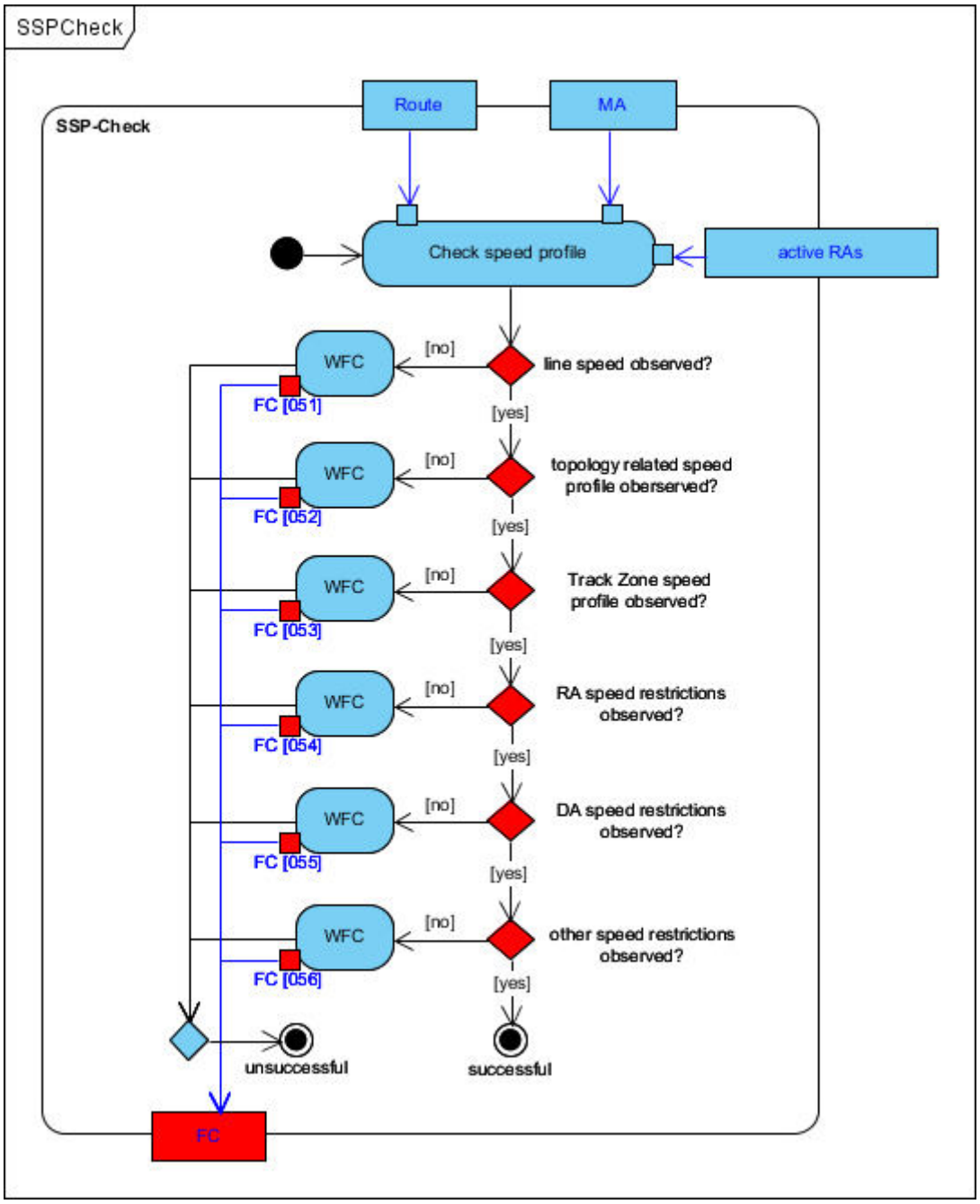


Abb. 79: Aktivitätsdiagramm der Subroutine „SSP Check“

Erneutes Prüfen der Prüfbedingungen

Der letzte Arbeitsschritt sieht vor, die Liste der Prüfbedingungen erneut durchzugehen, um auf Basis des nun modellierten Prozesses die im ersten Arbeitsschritt vorgenommene Einstufung von Prüfbedingungen als nicht relevant zu überprüfen. Aufgrund der Einfachheit des Prozesses ergeben sich durch diesen Arbeitsschritt bei der vorliegenden Subroutine keine Änderungen.

8.6.8 Hilfs-Subroutinen

Zum effizienteren Arbeiten sind einige Hilfs-Subroutinen sinnvoll. Ein Anwenden des in Kapitel 8.2.2 entwickelten Verfahrens wird für sie als nicht notwendig erachtet, da die Hilfs-Funktionen die Schutzrate nicht direkt beeinflussen.

Timeout-Prozess

Um einen Deadlock bei Anfragen an externe Systeme zu vermeiden und eine effiziente Bearbeitung der Prozesse zu ermöglichen, sollten Nachrichten an externen Systemen asynchron versandt werden können. Das heißt, dass der aufrufende Prozess in der smartLogic bereits die nächsten Prozessschritte ausführen kann, während auf die Antwort des externen Systems gewartet wird.

An der Stelle im Prozessablauf, an der die Antwort spätestens benötigt wird, wird das UML-Element „Accept Event Action“ modelliert. Geht die Nachricht ein, bis der Prozess an dieser Stelle angelangt ist, kann er fortgesetzt werden. Andernfalls kann eine gewisse Zeit gewartet werden. Diese festlegbare Zeit sollte jedoch nicht unendlich sein, da sonst ein Deadlock eintreten kann, wenn das angefragt System zum Beispiel nicht erreichbar ist.

Nach Ablauf der Zeit kann die Anfrage entweder erneut gesendet werden, wodurch wieder die festgelegte Zeit gewartet werden muss, oder das Warten wird mit negativem Ergebnis beendet. Abhängig von der Auswirkung der nicht erhaltenen Antwort auf die Schutzrate kann die Beendigung des Wartens entweder zu einem Abbruch des gesamten Prüfprozesses führen oder zu einer Reduzierung der Schutzrate. Im Falle eines Abbruchs des Prüfprozesses wird ein Fehlercode generiert. Die Anzahl, wie oft eine Anfrage erneut gesendet wird, sollte jeweils entsprechend der Wichtigkeit der Anfrage unter Berücksichtigung der globalen Anforderungen der *geringen Latenz* und der Zieldimension der *Robustheit* festlegbar sein.

Da Anfragen an externe Systeme und damit dieser Timeout-Prozess relativ häufig sind, ist eine entsprechende Hilfsfunktion sinnvoll. Diese ist im Ablaufdiagramm in Abb. 80 dargestellt.

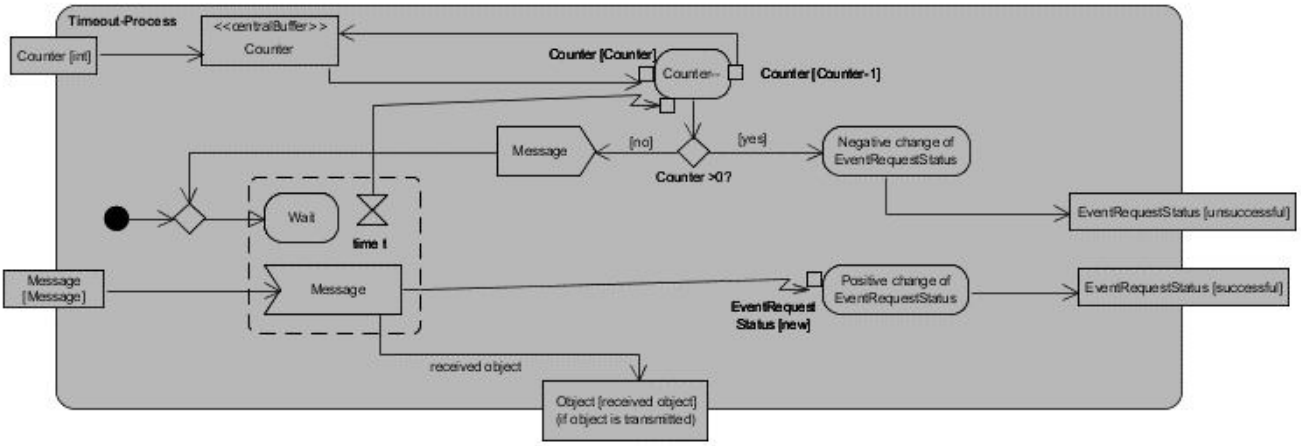


Abb. 80: Timeout-Prozess

Transaktionsbedingungen

Transaktionen sind in der Informatik Vorgänge, deren Ergebnis erst wirksam wird, wenn der gesamte Vorgang erfolgreich abgeschlossen werden konnte. Dies ist z. B. bei Online-Bankgeschäften von Bedeutung. Dort muss verhindert werden, dass, sollte die Verbindung abbrechen, während die Zahlung bereits in Auftrag gegeben, das Geld aber noch nicht auf dem Zielkonto gutgeschrieben wurde, die ganze Transaktion abgebrochen wird und nicht das Geld ohne Gegenbuchung verloren geht.

Auch bei der Prüfung von Anfragen an die smartLogic können Transaktionsprobleme auftreten. Denkbar wäre zum Beispiel, dass ein Element von zwei MP-Requests in kurzem zeitlichen Abstand auf Freisein geprüft wurde, aber, da die erste MA-Anfrage noch nicht vollständig geprüft wurde, noch nicht als Teil einer MA reserviert wurde. Dieser Umstand könnte dazu führen, dass im schlimmsten

Fall Fahrerlaubnisse ausgestellt werden, welche denselben Fahrwegabschnitt beinhalten. Eine solche Situation muss durch geeignete Transaktionsbedingungen ausgeschlossen werden.

Aus diesem Grund enthält die Logik eine entsprechende Subroutine zur Gewährleistung der Transaktionssicherheit, so dass zu Beginn einer Anfrage eine Vorabreservierung aller in der Prüfung beinhalteten Elemente durchgeführt. Während der Prüfung werden die Elemente entweder endgültig reserviert oder wieder freigegeben. Auch bei Abbruch des Prüfprozesses im Falle einer negativen Bewertung der Anfrage werden die Elemente wieder freigegeben, indem die Vorabreservierung gelöscht wird.

Die Subroutine wird am Beginn und Ende aller Prüfprozesse aufgerufen und funktioniert immer nach der oben beschriebenen Vorgehensweise. Aus Vereinfachungsgründen ist sie jedoch in den Diagrammen nicht dargestellt.

8.7 Reaktionsprozesse

Neben den Prüfprozessen bilden die Reaktionsprozesse die zweite Art der Prozessfunktionen in der smartLogic (vgl. Kapitel 6.2.2, Unterabschnitt „inhaltliche Aufteilung der Prozessfunktionen in Prüf- und Reaktionsprozesse“). Im Gegensatz zu den Prüfprozessen werden sie nicht vom TMS geplant aufgerufen, sondern durch den Eingang von z. B. bestimmten Sensorwerten ausgelöst.

Aufgrund der Rahmenbedingungen für diese Arbeit (vgl. Kapitel 3.6.1), insbesondere bezogen auf den begrenzten Umfang der Bearbeitungszeit, können die Reaktionsprozesse hier nicht gemäß der in Kapitel 8.2 beschriebenen Methode und Vorgehensweise ausführlich modelliert werden – das bleibt Aufgabe für zukünftige Arbeiten. Zur Vollständigkeit erfolgt in diesem Kapitel ein grundsätzlicher Überblick über die Funktionsweise und den Umfang der Reaktionsprozesse.

Als Ausgangspunkt für die Bestimmung der benötigten Reaktionsprozesse können die Auslöser der Reaktionsprozesse dienen, die in Kapitel 8.7.1 hergeleitet werden. Auf Basis der einzelnen Auslöser können anschließend in Kapitel 8.7.2 notwendige, generische Reaktionsprozesse identifiziert werden. Kapitel 8.7.3 leitet abschließend einen grundsätzlichen Aufbau dieser Reaktionsprozesse her, die wiederum als Ausgangspunkt für spätere, vertiefte Forschungsarbeiten zu den Reaktionsprozessen dienen können.

8.7.1 Auslösung von Reaktionsprozessen

Wie bereits in der Einleitung zu diesem Kapitel beschrieben, wurden in Kapitel 6.2.2 die Reaktionsprozesse von den Prüfprozessen abgegrenzt. Reaktionsprozesse werden demnach von externen Systemen über Nachrichten ausgelöst. Gemäß den Erkenntnissen aus Kapitel 4 kommen dafür prinzipiell die Fahrzeuge, die Stellelemente und Stakeholder-Systeme sowie die Datenhaltungssysteme in Frage (vgl. Kapitel 4.6). Außerdem können Reaktionsprozesse von Danger Areas (DAs) ausgehen (vgl. Kapitel 7.3.7).

Bei den Datenhaltungssystemen stellt sich die Frage, inwieweit diese als eigenständige Trigger (Auslöser) von Reaktionsprozessen fungieren können, da eine neue Information in der Datenhaltung immer aus einer anderen Quelle kommen muss und diese Quelle auch direkt die smartLogic triggern könnte. Allerdings sollen die Datenhaltungssysteme wie der Ortungsinformationsaggregator gerade verschiedene Eingangsdaten von verschiedenen Sensoren bündeln und zu einer konsistenten Information für die smartLogic aufbereiten. Deshalb erscheint es sinnvoll, die Datenhaltungssysteme auch als mögliche Trigger für Reaktionsprozesse zu betrachten und bestimmte Informationen, wie die Ortungsinformationen, zunächst über diese Systeme zu filtern.

Nachrichten, die Reaktionsprozesse auslösen können, können eine schnelle Handlung zum Abwenden von Schaden oder zur Verringerung des Schadensausmaßes erforderlich machen. Damit eine eintreffende Nachricht verarbeitet und bezüglich ihrer Relevanz bewertet werden kann, ist es deshalb sinnvoll, den entsprechenden Reaktionsprozesse unmittelbar durch das Eintreffen der Nachricht zu starten. Wie im vorigen Absatz bereits angeklungen, bilden Nachrichten, die von den Datenhaltungssystemen verarbeitet werden, eine Ausnahme, da in diesen Fällen das Datenhaltungssystem zunächst bewertet, ob ein Reaktionsprozess ausgelöst werden muss und anschließend selbst mit der Übermittlung einer Nachricht an die smartLogic einen Reaktionsprozess auslöst (vgl. Beispiel der Bündelung der verschiedenen Ortungsinformationen durch den Ortungs-informationsaggregator).

Bei den Datenhaltungssystemen muss entsprechend geklärt werden, wann sie neue Informationen mittels einer Nachricht an die Sicherungslogik übermitteln. Eine Übermittlung muss nicht zwangsläufig bei jedem neu verfügbaren Datensatz eines Sensors geschehen, z. B. könnten bei der Ortungsinformationsaggregation zunächst mehrere Sensordaten gebündelt werden, um das Konfidenzintervall um die bestimmte Ortungsposition zu verkleinern. Es muss nicht Aufgabe dieser Arbeit sein, Kriterien hierfür festzulegen. Dies kann auch im Einzelfall auf Seiten der Datenhaltungssysteme in Rücksprache mit dem TMS festgelegt werden, da es häufig nur betriebliche Auswirkungen hat, aber keine sicherheitskritischen (im Beispiel der Ortungsinformation bleiben so z. B. Infrastrukturbeanspruchungen länger als notwendig erhalten). Allerdings sollten sicherheits-kritische Status-Updates sofort weitergeleitet werden.

8.7.2 Identifizieren der notwendigen Reaktionsprozesse

Für die Identifizierung der notwendigen Reaktionsprozesse konnten mehrere Ausgangspunkte identifiziert werden, die zur Erhöhung der Vollständigkeit parallel weiterverfolgt werden können:

1. Im Rahmen der Funktionsanalyse in Kapitel 6 wurden bereits benötigte Reaktions-prozesse bestimmt.
2. Aus den Nachrichten, die in den Standardschnittstellen zu den auslösenden externen Systemen (vgl. Kapitel 8.7.1) vorgesehen sind, können Anhaltspunkt für die erforderlichen Reaktionsprozesse gesammelt werden.
3. Wie ebenfalls in Kapitel 8.7.1 beschrieben, lösen DAs Reaktionsprozesse aus, bei denen die Auswirkung der DA anhand der verfügbaren Informationen über ihre Ursache ermittelt werden und ggf. Maßnahmen zur Schadensabwehr bzw. zur Begrenzung des Schadensausmaßes ergriffen werden.

Reaktionsprozesse aus der Funktionsanalyse

Tab. 59 enthält die im Rahmen der Funktionsanalyse in Kapitel 6 identifizierten Reaktionsprozesse bzw. funktionale Anforderungen an dies Reaktionsprozesse.

Tab. 59: im Rahmen der Funktionsanalyse identifizierte Reaktionsprozesse

ID	Kategorie	Beschreibung	Bemerkung
F-E005	interner Prozess	überwache die Fahrzeugpositionen	
F-E230b	interner Prozess	überwache aktive Flankenschutzräume auf unerlaubte Verletzungen	

F-E255, F-E256, F-E745a	interner Prozess	überwache den Zustand von Stakeholdern mit aktiven Zustimmungen	z. B. dass der BÜ seinen geschlossenen Status beibehält
F-E005a, F-E706, F-E707	Prüfbedingung	falls der Zug nicht mehr geortet werden kann, leite Maßnahmen bei Gefahr ein, sperre die Gleise	falls ein Unfall stattgefunden hat
F-E052	Prozess	Verarbeite Notbremsaufträge	z. B. von Detektionssystemen an der Strecke
F-E107	Prozess	Verarbeite Status-Aktualisierungen von Infrastrukturelementen	z. B. falls eine Weiche ihre Endlage verliert
F-E108	Prozess	Verarbeite Zustandsänderungen von Infrastrukturelementen	z. B. falls eine Weiche nicht mehr betriebsbereit ist (jemand Unbefugtes könnte z. B. die Betriebsart geändert haben)
F-E132, F-E720	Prozess	Verarbeite Fehlermeldungen der Fahrzeuge	z. B. könnte ein Fahrzeug einen Bremskraftabfall melden
F-E132b	Prozess	Verarbeite Meldungen von Überwachungssensoren am Gleis	z. B. Heißläuferortungsanlage
F-E132a	Prüfbedingung	stelle sicher, dass das Fahrzeug anhält, falls ein Heißläufer geortet wurde	
F-E134	Prüfbedingung	stelle sicher, dass das Fahrzeug anhält, falls eine feste Bremse geortet wurde	
F-E140	Prozess	Verarbeite ein Status-Update eines Sensors, der globale Daten für einen oder mehrere Gleisbereiche ändert	z. B. Haftreibung, globale Wetterparameter
F-E146	Prüfbedingung	falls ein gravierender Gleisschaden festgestellt wurde, leite Maßnahmen bei Gefahr ein und sperre das Gleis	
F-E147	Prüfbedingung	falls ein gravierender Schaden am Bahndamm festgestellt wurde, leite Maßnahmen bei Gefahr ein und sperre das Gleis	
F-E148	Prüfbedingung	falls ein Oberleitungsschaden festgestellt wurde, leite Maßnahmen bei Gefahr ein und sperre das Gleis	
F-E225	Prüfbedingung	falls ein Fahrzeug seine Fahrerlaubnis überschreitet, leite Maßnahmen bei Gefahr ein und verhindere Gefährdungen im potenziellen Fahrweg	
F-E226	Prüfbedingung	falls der von der Fahrzeugbewegung unmittelbar beanspruchte Bereich anderweitig konfliktär belegt wird, leite Maßnahmen bei Gefahr ein	
F-E230d	Prüfbedingung	falls der aktive Flankenschutzraum verletzt wird, leite Maßnahmen ein, um eine Gefährdung der zu schützenden Fahrt zu vermeiden	

F-E258, F-E259, F-E262, F-E266, F-E724, F-E741, F-E745b	Prozess	Verarbeite Status- und Zustandsänderungen von Stakeholder-Systemen	
F-E700	Prozess	Verarbeite unidentifizierte Gleisbelegungsmeldungen	
F-E700a	Prüfbedingung	stelle sicher, dass Nothaltaufträge sofort umgesetzt werden	
F-E701	Prozess	Verarbeite Fehlermeldungen in Bezug auf den Stromabnehmer und die Oberleitung	
F-E701a	Prüfbedingung	im Falle von Oberleitungsstörungen ergreife Maßnahmen bei Gefahr, informiere die Schaltstelle für die Oberleitung und informiere das Fahrpersonal	
F-E702	Prozess	Verarbeite Feuermeldungen	
F-E702a	Prüfbedingung	im Falle von Feuer ergreife Maßnahmen bei Gefahr, halte betroffene Fahrzeuge außerhalb von NSAs und falls möglich in Bereichen ohne Oberleitung an; informiere das Fahrpersonal, falls im Tunnel sende Information zur Entfluchtung und aktiviere ggf. Belüftungs- und Fluchtwegweisersysteme; informiere weitere Betroffene; stelle sicher, dass alle potenziell betroffenen Gleise gesperrt werden	
F-E703	Prüfbedingung	im Falle einer Evakuierung eines Fahrzeugs, stelle sicher, dass die angrenzenden Gleise gesperrt sind	
F-E709	Prozess	Verarbeite Meldungen über Zugtrennungen	
F-E709a	Prüfbedingung	im Falle einer unerwarteten Zugtrennung stelle sicher, dass der hintere Zugteil von einer DA umgeben ist, ergreife Maßnahmen wie bei einem entrollten Fahrzeug (siehe F-E225)	
F-E711	Prüfbedingung	stelle sicher, dass Fahrzeuge aus Gefahrenbereichen herausgeholt werden können	

F-E712	Prüfbedingung	stelle bei der Erfordernis von Maßnahmen bei Gefahr sicher, dass alle betroffenen Fahrzeuge angehalten werden, alle betroffenen Nachbargleise gesperrt sind und sich nähernde Fahrzeuge informiert sind, alle Stakeholder informiert sind	z. B. bei entlaufenden Fahrzeugen BÜ auf dem potenziellen Weg des Fahrzeugs
F-E713	Prozess	ermögliche das Aufheben von Maßnahmen bei Gefahr	
F-E715, F-E716	Prozess	Verarbeite eine Nachricht über ein unvollständiges oder nicht vorhandenes Zugspitzensignal	
F-E717	Prozess	Verarbeite fehlendes Zugschlusssignal	
F-E718	Prozess	Verarbeite eine Nachricht über eine geöffnete Tür eines Fahrzeugs	
F-E719	Prozess	Verarbeite eine Nachricht über ungesicherte Ladung	
F-E727	Prozess	Verarbeite Nachrichten über Infrastrukturversagen	
F-E715a – F-E720a, F-E725a, F-E727a, F-E741a, F-E750	Prüfbedingung	siehe Anlage 2	
F-E799	Prozess	erlaube die Rücknahme von „emergency messages“	

Reaktionsprozesse in Folge von Nachrichten über Standardschnittstellen

Als Ergebnis der zweiten Methode enthält Tab. 60 eine Übersicht über die Reaktionsprozesse, die sich aus den Standardschnittstellen anhand der darin enthaltenen Nachrichten herleiten lassen (Quelle für ETCS: SRS Subset 026 [ERA 2016], Quelle für EULYNX: SCI Generic [EULYNX Initiative 2020a], SCI-P [EULYNX Initiative 2020b]). In kursiv sind Nachrichten aus den Schnittstellen aufgeführt, die nicht für relevant für den oben beschriebenen Anwendungszweck gehalten werden.

Tab. 60: Nachrichten-Indikatoren für Reaktionsprozesse aus den Standardschnittstellen

Nachrichten	Schnittstelle	Bemerkung
Msg 129: Validated Train Data	*ETCS*	*Änderung der Charakteristik der Fahrzeugbewegung; kann in der sicheren Datenquelle für die Fahrzeugdaten verarbeitet werden*
Msg 130: Request for Shunting	*ETCS*	*nicht sicherheitskritisch, sollte daher vom TMS verarbeitet werden*
Msg 132: MA Request	*ETCS*	*nicht sicherheitskritisch, sollte daher vom TMS verarbeitet werden*
Msg 136: Train Position Report	*ETCS*	*Update der fahrzeugseitig berechneten Fahrzeugposition; sollte im Ortungsinformationsaggregator verarbeitet werden*

Msg 137/138: Request to shorten MA is granted/rejected	*ETCS*	*Antwort auf den MP Change Request (vgl. Kapitel 8.5.4); die Antwort wird direkt im Prozess verarbeitet und braucht daher keinen Reaktionsprozess*
Msg 146/147: Acknowledgement; Msg 158: Text message acknowledged by driver	*ETCS*	*Empfangsbestätigung für Nachricht; wird direkt in dem Prozess verarbeitet, der die auslösende Nachricht ans Fahrzeug gesandt hat, und benötigt daher keinen Reaktionsprozess*
Msg 149: Track Ahead Free Message	*ETCS*	*manuelle Gleisfreimeldung für einen festgelegten Abschnitt vor der Fahrzeugspitze; ist immer eine Antwort auf einen entsprechenden Request und benötigt daher keinen Reaktionsprozess*
Msg 150: End of Mission	ETCS	der Abbau einer Kommunikationssession muss von der SL auf mögliche Komplikationen bewertet werden
Msg 154: No compatible version (supported)	*ETCS*	*gehört zum Prozess der Anmeldung eines Fahrzeugs, siehe Msg 155*
Msg 155: Initiation of a communication session	ETCS	mit dieser Nachricht meldet sich das Fahrzeug an, hierfür ist ein Reaktionsprozess erforderlich
Msg 156: Termination of a communication session	*ETCS*	*gehört zum Prozess der Abmeldung eines Fahrzeugs, siehe Msg 150*
Msg 157: SoM Position Report	*ETCS*	*erweiterter Position Report der zur Anmeldungsprozedur (Start of a mission (SoM)) gehört, siehe Msg 155*
Msg 159: Session Established	*ETCS*	*gehört zum Prozess der Anmeldung eines Fahrzeugs, siehe Msg 155*
EU.SCI-XX.PDI.77 PDI-Version check	*EULYNX*	*nur Antwortnachricht zum Kommunikationsaufbau*
EU.SCI-XX.PDI.102 Start Initialisation	EULYNX	repräsentiert Zustands-Änderung, Detaillierungen in EU.SCI-XX.SDI
EU.SDI-XX.10/12 pdiError / pdiStatus	EULYNX	Verbindung zum Element bricht ab
Eu.SCI-P.PDI.181: Point Position	EULYNX	repräsentiert aktuellen Status (im Sinne von “Lage”) eines stellbaren Fahrwegelements (CTE)
EU.SCI-XX.PDI.135 Status message transmission completed	*EULYNX*	*siehe EU.SCI-XX.PDI.102*

Wie aus Tab. 60 ersichtlich ist, beschränken sich die aus den ETCS-Nachrichten vom Zug an die Strecke ergebenden Reaktionsprozesse auf das Anmelden und Abmelden der Fahrzeuge, vor allem da weitere Zugdaten zunächst von den Systemen der sicheren Datenquelle verarbeitet werden.

Die stellbaren Fahrwegelemente können viele Diagnosedaten übertragen. Die wesentlichen Funktionen können jedoch mit der Übermittlung des Zustandes (operation state), der Übermittlung des Status bzw. der Lage des Elements (CTE Status, oben am Beispiel der Weiche „Point Position“) und dem Status der Kommunikationsverbindung abgedeckt werden. So können weitere Probleme aus dem Maintenance-Bereich darin zusammengefasst werden, dass sich bei einer Auswirkung auf die Sicherheit der „operation state“ nicht mehr im Modus „operational“ befindet. Weiterhin kann die Lage des Elements in „no end position“ oder „trailed“ wechseln. Falls die Verbindung abbricht, ist ebenfalls

ein Reaktionsprozess erforderlich, da sicherheitsrelevante Zustands- oder Statusänderungen des Elements nicht mehr übertragen werden können.

Reaktionsprozesse in Folge von Nachrichten aus Datenhaltungssystemen

Neben Nachrichten über Standardschnittstellen kommen auch Nachrichten von den Datenhaltungssystemen als Quelle von Reaktionsprozessen in Betracht. Es kann davon ausgegangen werden, dass jedes sicherheitsrelevante Datenhaltungssystem (vgl. Kapitel 4.4) ein Datenupdate durchführen möchte:

- Fahrzeugdatenupdate
- Update der Topologie
- Update einer (oder mehrerer) Fahrzeugpositionen

Es wird angenommen, dass die Fahrplandaten nicht sicherheitsrelevant sind und daher für ein Update der Fahrplandaten kein Reaktionsprozess benötigt wird.

Reaktionsprozesse in Folge von Stakeholder-Aktivitäten

Eine weitere wichtige Gruppe externer Systeme sind die Stakeholder-Systeme (vgl. Kapitel 8.3.3). Diese Gruppe kann sehr vielfältig sein und repräsentiert sowohl Sensoren als auch Systeme, die auf Anfrage der Sicherungslogik handeln. Aufgrund dieser Vielfältigkeit existieren bisher nur wenige Standardschnittstellen, die jedoch nicht auf das Stakeholder-Konzept der smartLogic zugeschnitten sind. So existiert eine EULYNX-Schnittstelle für Bahnübergangssicherungsanlagen, die anstatt einer Aufforderung zum Senden einer Zustimmung zur einer Fahrerlaubnis jedoch eine Reihe von Nachrichten mit detaillierten Kommandos für den BÜ enthält. Daher ist die existierende EULYNX-Schnittstelle nicht auf das in dieser Arbeit erarbeitete Konzept übertragbar und hier keine sinnvolle Quelle für die Identifizierung von benötigten Reaktionsprozessen.

Für die Stakeholder-Systeme können die notwendigen Reaktionsprozesse jedoch aus den Registrierungsschnittstellen (Registrierungsarten) hergeleitet werden. Die Ergebnisse davon sind in Tab. 61 zusammengefasst.

Tab. 61: durch Stakeholder-Systeme ausgelöste Reaktionsprozesse

Registrierungsart	benötigte Reaktionsprozesse
zustimmungspflichtige Stakeholder	eine Fehlermeldung oder ein Kommunikationsverlust können einen Reaktionsprozess auslösen, bei dem zu überprüfen ist, ob ggf. MAs zurückgenommen oder Fahrzeuge gestoppt werden müssen
einschränkende Stakeholder	Bei Veränderungen des Status ändern sich RAs; es ist zu klären, ob dies auch auf bereits bestehende Fahrerlaubnisse wirkt
benachrichtigungspflichtige Stakeholder	eine Fehlermeldung kann einen Reaktionsprozess auslösen, bei dem zu überprüfen ist, ob ggf. MAs zurückgenommen werden müssen
überwachende Stakeholder	der Eingang von Sensorwerten muss zu einem Reaktionsprozess führen, ebenfalls der Verlust der Kommunikation
Hörer	keine Implikationen, da Hörer passiv sind

Der Status von zustimmungspflichtigen und benachrichtigungspflichtigen Stakeholder-Systemen wird im Rahmen der Prozessfunktionen aktiv überprüft, bevor die smartLogic Entscheidungen über die Zulassung von Prüfanfragen des TMS trifft. Bei einer Fehlermeldung oder dem Kommunikationsverlust (weil dann eine Fehlermeldung nicht mehr übertragen werden kann) kann es jedoch erforderlich sein, anzunehmen, dass die Zustimmung bzw. der für die Benachrichtigungen erforderliche Zustand „operational“ nicht mehr vorliegt. Ist dies der Fall, sollten in manchen Situationen sich in der Anfahrt befindliche Fahrzeugbewegungen angehalten werden, bis der Sachverhalt geklärt ist. In anderen Fällen ist aber auch denkbar, dass weitergefahren werden kann. Deshalb wäre es sinnvoll, wenn die Stakeholder bei der Registrierung angeben könnten, ob ein Anhalten bei Fehlermeldungen oder Kommunikationsabbruch erforderlich ist (vgl. Tab. 44 in Kapitel 8.3.3). Dasselbe gilt insbesondere auch für einschränkende Stakeholder. Für sie sollte geklärt werden, ob immer die restriktivste Einschränkung gilt (und welche dies ist), falls sie nicht mehr erreichbar sind oder in einem Fehlerzustand sind.

Die Aufgabe von überwachenden Stakeholdern ist es gerade, Reaktionsprozesse auf Basis von Sensorwerten auszulösenden. Am einfachsten und im Sinne der globalen Anforderung der schlanken Logik (vgl. Kapitel 3.5 und 8.2.1) wäre es, einige generische Reaktionsprozesse zu definieren, die durch überwachende Stakeholder-Systeme ausgelöst werden könnten. Die Funktionsanalyse aus Kapitel 6 zeigt jedoch, dass es ganz verschiedene Anforderungen für solche Reaktionsprozesse gibt. Beispielsweise würde ein Brandsensor in einem Tunnel möglicherweise zu einem komplexen „Reversing“-Prozess führen. Auch aus Gründen der Zukunftsfestigkeit der Logik erscheint es daher wenig sinnvoll, die Reaktionsmaßnahmen auf einige feste Reaktionsprozesse zu begrenzen. Stattdessen sollten die überwachenden Stakeholder-Systeme ein möglichst umfangreiches Vokabular haben, um bei der Registrierung einen entsprechenden Reaktionsprozess definieren zu können. Dabei bleibt Aufgabe der Sicherungslogik zu überprüfen, ob jeder einzelne Schritt des Reaktionsprozesses auch sicher ist, also mit hinreichender Wahrscheinlichkeit nicht zu einem unsicheren Zustand führt.

Existieren überwachende Sensoren an zustimmungspflichtigen oder benachrichtigungspflichtigen Stakeholder-Systemen, sollten sich diese auch auf der Registrierungsschnittstelle für überwachende Stakeholder eintragen.

8.7.3 grundsätzlicher Aufbau der Reaktionsprozesse

Abschließend zur Betrachtung der Reaktionsprozesse soll auf deren grundsätzlichen Aufbau eingegangen werden. Primäres Ziel der Reaktionsprozesse ist gemäß Kapitel 6.2.2 die Verhinderung von Gefährdungen bei ungeplanten Ereignissen oder anderen Dateneingängen. Sekundäres Ziel ist auch die betriebliche Verarbeitung des Ereignisses. Hierzu zählt zum Beispiel die Anpassung von Beanspruchungen bei Aktualisierung von Fahrzeugpositionen, damit die entsprechenden Gleisabschnitte (z. B. von anderen Fahrzeugbewegungen) neu beansprucht werden können. Aus diesen Zielen und den Erkenntnissen aus Kapitel 8.7.2 kann der grundsätzliche Aufbau der Reaktionsprozesse hergeleitet werden. Die nachfolgend beschriebenen Schritte müssen je nach Bedarf auf den jeweiligen Reaktionsprozess angepasst werden.

Beim Auftreten eines Auslösungsereignisses (vgl. Kapitel 8.7.1) sollte zunächst festgestellt werden, welcher Reaktionsprozess (vgl. Kapitel 8.7.2) ausgelöst werden muss. Damit nicht zu viele Reaktionsprozesse beschrieben werden müssen, ist ein generischer Aufbau dieser Prozesse anzustreben (Anforderung der generischen Logik, vgl. Kapitel 8.2.1).

Um den vom Reaktionsprozess betroffenen Gleisabschnitt eingrenzen zu können, muss zunächst der Wirkabschnitt festgestellt werden bzw. bei großflächig wirkenden Ereignissen der Gleisbereich, auf den das Ereignis wirkt. Es kann sich auch nur um einen Punkt auf dem Gleis handeln.

Da der Reaktionsprozess Einschränkungen für die Befahrbarkeit des Wirkabschnitts nach sich ziehen kann, sollte im nächsten Schritt geprüft werden, ob eine RA für diesen Abschnitt angelegt werden sollte. Dies hängt davon ab, ob das auslösende Ereignis nur die aktuell im Wirkabschnitt verkehrenden Fahrzeugbewegungen bzw. stellbaren Fahrwegelemente betrifft oder dauerhaft als Einschränkung vorhanden sein soll.

Da der Reaktionsprozess auch bereits verkehrende Fahrzeuge betreffen kann, muss anschließend geprüft werden, welche aktuell verkehrenden Fahrzeugbewegungen von dem Ereignis betroffen sind. Dies kann über die Beanspruchungen der Gleissegmente und stellbaren Fahrwegelemente im Wirkabschnitt ermittelt werden. Für die Fahrzeugbewegungen ist zu klären, inwiefern sie betroffen sind. Hierzu kann eine eingerichtete RA ein Anhaltspunkt sein. Sie kann z. B. bei einer Sperrung einen Nothalt auslösen, zu einer Kürzung der Fahrerlaubnis führen oder eine niedrigere erlaubte Geschwindigkeit erforderlich machen.

Das auslösende Ereignis kann auch komplexere Prozesse erforderlich machen, bei denen z. B. verschiedene Anfragen, die normalerweise vom TMS kommen, intern getriggert werden und entsprechende Prüfprozesse auslösen. So könnten zum Beispiel bei einem Brand in einem Tunnel verschiedene Fahrerlaubnisse im ETCS-Modus „Reversing“ ausgegeben werden und zwischendurch Weichen gestellt werden müssen. Theoretisch könnten beliebige solcher Abläufe mittels eines Skripts vorprogrammiert werden, dass im Notfall durch einen entsprechenden Reaktionsprozess aufgerufen wird. Jede Anfrage müsste allerdings wie gewöhnlich durch die Sicherungslogik auf ihre Sicherheit hin geprüft werden, um eine Verschlechterung der Sicherheit durch den Reaktionsprozess zu verhindern.

Eine weitere wichtige Funktion des Reaktionsprozesses sind erforderliche Benachrichtigungen über das Ereignis zu verteilen. Die erforderlichen Benachrichtigungen können am besten durch das den Reaktionsprozess auslösende System vorgegeben werden, da davon ausgegangen werden muss, dass sie je nach Reaktionsprozess sehr unterschiedlich sein werden. Zu den erforderlichen Benachrichtigungen gehören beispielsweise die Benachrichtigungen der Notfallleitstelle und ggf. direkt auch von Einsatzkräften. Es ist auch denkbar, dass Stakeholder-Systeme benachrichtigt werden müssen, z. B. ein Rauchentlüftungssystem oder ein System zur Visualisierung von Fluchtwegen und -richtung. Um ein anderes Beispiel zu wählen, könnten z. B. Lautsprecher an einem defekten BÜ Passanten vor einem herannahenden Eisenbahnfahrzeug warnen.

8.8 Ausblick Verhaltensmodellierung

Es gibt einige weitere Funktionalitäten, die ebenfalls zu einer vollständigen Sicherungslogik gehören, aber in dieser Arbeit aufgrund der zeitlichen Rahmenbedingungen nicht untersucht werden konnten. In diesem Kapitel wird im Sinne der Vollständigkeit ein kurzer Überblick über diese Funktionalitäten gegeben.

8.8.1 Übergangsbedingungen

Aufgrund der Anforderung der Migrationsfähigkeit (vgl. Kapitel 3.5) muss die Logik auch mit Alttechnik kompatibel sein. Hierzu sind spezielle Übergangsbedingungen zur Alttechnik erforderlich. Zudem ist nicht davon auszugehen, dass das gesamte Netz auf einmal mit smartLogic ausgerüstet

würde. Daher ist zu definieren, wie der Übergang zwischen der smartLogic und anderen Stellwerkstechnologien oder auch zu einer anderen smartLogic funktionieren würde.

Weitere mögliche Übergangsbereiche betreffen Ortungsstellbereiche ohne Stellwerkstechnik sowie Nebenstrecken mit vereinfachter Sicherungstechnik.

8.8.2 Bedienfunktionen

Die smartLogic soll im Normalfall komplett automatisiert arbeiten. Dennoch ist davon auszugehen, dass auf absehbare Zeit bestimmte Handlungen wie das Löschen von Beanspruchungen nach schwerwiegenden Störungen noch manuell gemacht werden muss. Aus diesem Grund sind Bedienfunktionen für die smartLogic bereitzuhalten und Bedienkommandos zu verarbeiten. Auch in der Funktionsanalyse wurden Bedienfunktionen identifiziert (vgl. Kapitel 6.6.1).

8.8.3 Protokollierung

Eine globale Anforderung fordert explizit die Notwendigkeit einer genauen Protokollierung aller Prozesse der smartLogic, um bei einem Unfall Rückschlüsse auf die Ursache ziehen zu können. Mit diesem Themenkomplex beschäftigte sich die vorliegende Arbeit ebenfalls nicht.

8.9 Ergebnisdiskussion

Die in diesem Hauptkapitel vorgestellte Verhaltensmodellierung beschreibt die wichtigsten Prozessfunktionen und Subroutinen der smartLogic mit Hilfe von UML-Aktivitätsdiagrammen. Die funktionalen Grundlagen wurden in den Kapiteln 8.3 und 8.4 gelegt. Im vorliegende Kapitel sollen die wichtigsten Chancen und Herausforderungen durch die erarbeiteten Basis-Konzepte noch einmal zusammengefasst werden.

Schutzrate

Als Ergebnisgröße für die Entscheidung über eine Zulassung oder Ablehnung einer Prüfanfrage wurde das Konzept der Schutzrate eingeführt. Die Schutzrate ermöglicht, dass die Sicherheit der Prüfanfragen im Kontext des aktuellen Betriebsgeschehens bewertet werden kann. Zudem erlaubt sie bei Störungen durch die Berücksichtigung von Kompensationsmaßnahmen bei der Entscheidung über die Genehmigung einer Prüfanfrage möglichst lange den Betrieb ohne manuelle Rückfallebenen aufrechtzuerhalten.

Die Schutzrate wird zunächst für die einzelnen Prüfschritte des Prüfprozesses zum Prüfen der verschiedenen Prüfbedingungen berechnet. Ihre jeweilige Berechnungsfunktion setzt sich dabei aus Teilfunktionen zusammen, die den Einfluss einzelner potenzieller Gefährdungen auf die Sicherheit der Prüfanfrage repräsentieren. Dabei werden für jede Gefährdung die Eintrittswahrscheinlichkeit und die Schwere der Gefährdung als Gewichtungsfaktor berücksichtigt. Hierbei wurde die Annahme getroffen, dass bei vollständigem Regelbetrieb eines Elements dessen Einfluss auf die Schutzrate neutral ist. Der genaue Aufbau der Teilfunktionen ist nicht fest vorgegeben, sondern kann über eine sichere Topologie-Datenquelle auf die jeweilige Infrastruktur bzw. die vorhandenen Umsysteme angepasst werden. Über die Stakeholder-Registrierung können mit der Registrierung neuer externer (Stakeholder-)Systeme zusätzliche Teilfunktionen in die Berechnungsfunktion der Schutzrate integriert werden.

Falls negative Einflüsse auf die Schutzrate für einen Prüfschritt festgestellt wurden, wird bewertet, ob damit die Schutzrate unter den erforderlichen Schwellwert absinkt, um die Prüfanfrage genehmigen

zu können. Ist dies der Fall, bricht der Prüfprozess ab. Andernfalls wird der Prüfprozess fortgesetzt und die berechnete Schutzrate fließt am Ende des Prüfprozesses in die Berechnung einer Gesamt-Schutzrate ein, die ebenfalls oberhalb des Schwellwerts liegen muss, damit die Prüfanfrage genehmigt werden kann.

Das Konzept der Schutzrate (vgl. Kapitel 8.3.1) ermöglicht eine umfassende Bewertung der aktuellen Betriebssituation, um Prüfanfragen nicht unnötig zurückzuweisen. Es erscheint allerdings zunächst auch sehr komplex. Da es dennoch generisch sowie universal für alle Prüfbedingungen anwendbar ist, widerspricht es aus Sicht des Autors jedoch nicht der globalen Anforderung der *schlanken Logik*.

Ein Schwachpunkt des Konzepts der Schutzrate ist, dass die Gewichtungsfaktoren für die einzelnen Funktionsbestandteile zur Errechnung der Schutzrate erst noch bestimmt werden müssen und eine Bestimmung in vielen Fällen aufwendig sein dürfte. Allerdings kann die Schutzrate auch ohne Bestimmung aller Gewichtungsfaktoren angewendet werden, indem der fehlende Gewichtungsfaktor so gesetzt wird, dass ein Nichterfüllen der Prüfbedingung immer zur sicheren Seite ausgelegt wird.

Das Konzept der Schutzrate ist zudem noch nicht mit Zulassungsbehörden abgestimmt. Sollte die Zulassungsbehörde dem Konzept der Schutzrate generell kritisch gegenüberstehen, könnten theoretisch über die Gewichtungsfaktoren (Risiko durch Gefährdung = 100 %) ohne Änderung der Logik auch alle Prüfbedingungen zu Abbruchkriterien werden, bei deren Verletzung die Prüfanfrage abgelehnt wird. Allerdings ist ein risikobasierter Ansatz, wie er in dieser Arbeit vorgeschlagen wird, aus Sicht des Autors durchaus im Sinne der gültigen CENELEC-Normen für Systeme der Eisenbahnsicherungstechnik, da die Normen ebenfalls auf eine Beherrschung von Risiken ausgelegt sind. Dabei ist jederzeit sicherzustellen, dass das Risiko unterhalb der im Rahmen der Risikoanalyse bestimmten tolerierbaren Gefährdungsrate liegt (vgl. Kapitel 3.6.3).

Zielpunkte

Zur Übermittlung des Endes einer Fahrerlaubnis können in der smartLogic analog zur ETCS-Spezifikation verschiedene Zielpunkte dienen (vgl. Kapitel 8.3.2). Dabei kalkuliert die Fahrzeugbewegung ihre Bremsung so, dass sie im Normalfall vor dem anzusteuernden Zielpunkt (bei ETCS die End of Authority (EoA)) zum Halten kommt und mit hinreichender Sicherheit vor dem primären sicherungstechnischen Zielpunkt (bei ETCS die Supervised Location (SvL)). Zudem wurde noch die Möglichkeit weiterer sekundärer sicherungstechnischer Zielpunkte betrachtet, die jedoch derzeit bei ETCS nicht vorgesehen sind. Die Zielpunkte werden vom TMS in der Prüfanfage festgelegt und durch die smartLogic auf ihre Sicherheit hin überprüft.

Aus Sicht der smartLogic ist bei der Prüfung entscheidend, dass die SvL vor dem maßgeblichen Gefahrpunkt liegt, bei dessen Passieren die betrachtete Fahrzeugbewegung in unzulässigem Maße gefährdet werden würde. Bis zu diesem Punkt garantiert die smartLogic, dass mit hinreichender Wahrscheinlichkeit eine sichere Fahrt möglich ist. Die Position der EoA ist dagegen in Hinblick auf die Sicherheit weniger wichtig, stellt aber eine Möglichkeit dar, die Erreichenswahrscheinlichkeit eines Punktes zwischen EoA und SvL (und damit dem Sicherheitsabstand hinter der EoA) zu verringern und somit in diesem Bereich das Vorhandensein bestimmter Gefahrpunkt mit einem niedrigen (aber nicht gänzlich unbedeutenden) Gefährdungsrisiko zu akzeptieren. Ein gutes Beispiel sind überlappende Sicherheitsabstände verschiedener Fahrzeugbewegungen, die bei heutiger Stellwerkstechnik als überlappende Durchrutschwege unter bestimmten Voraussetzungen ebenfalls möglich sind (vgl. Abb. 60 in Kapitel 8.3.2).

Zu beachten ist, dass die Position der EoA nicht mit möglichen verkehrlich geplanten Halteplätzen zu verwechseln ist. Die Bremsung auf solche Halteplätze hat keine relevanten Auswirkungen auf die

Sicherheit und wird daher im Sinne der Anforderung der *schlanken Logik* bzw. der *Beschränkung auf den sicherungskritischen Kern* nicht von der Sicherungslogik überwacht. Die Rücknahme eines hinter dem verkehrlichen Zielpunkt liegenden Teils der ausgestellten Fahrerlaubnis, der zur Erhöhung der Einfahrgeschwindigkeit als zusätzlicher Sicherheitspuffer in die Fahrerlaubnis mitaufgenommen wurde und nach dem Halt am verkehrlichen Zielpunkt nicht mehr benötigt wird, kann dabei auch über einen MP Change Request in Verbindung mit der ETCS-Funktion zum Kürzen einer Fahrerlaubnis erfolgen. Letzteres bietet den Vorteil, dass der Zeitpunkt der Kürzung der Fahrerlaubnis und damit der Freigabe der nicht mehr benötigten Elemente flexibel ist und davon abhängig gemacht werden kann, ob die sich in Anfahrt befindliche Fahrzeugbewegung den zusätzlichen Raum hinter dem verkehrlich angestrebten Zielpunkt noch auf voller Länge benötigt.

Der entwickelte Mechanismus der Prüfung der Zielpunkte ermöglicht es dem TMS, die Zielpunkte betrieblich optimal zu platzieren. Dadurch können sowohl die SvL als auch die EoA unmittelbar vor den nächsten maßgeblichen Gefahrpunkt gesetzt werden, wodurch die Bremskurven weitestmöglich in Fahrtrichtung der Fahrzeugbewegung verschoben werden können und somit die Fahrzeugbewegung erst spätestmöglich mit einer Bremsung beginnen muss. Zudem wird durch den MP Change Request bei Bremsung auf einen verkehrlichen Zielpunkt auch ermöglicht, den Sicherheitspuffer hinter diesem Zielpunkt durch Rückverlegung der sicherungstechnischen Zielpunkte in einer aktualisierten MA in Richtung des verkehrlichen Zielpunktes zu kürzen, sobald die Erreichenswahrscheinlichkeit für den neuen sicherungstechnischen Zielpunkt hinreichend gering ist (vgl. die identifizierten Nutzenszenarien in Kapitel 3.4.4). Erste Analysen zur Kapazitätsauswirkung zeigen, dass durch diese Vorteile in Knoten im Vergleich zur Nutzung klassischer Durchrutschwege höhere Einfahrgeschwindigkeit und damit Zeitvorteile erreicht werden können [Merkel 2021].

Stakeholder-Registrierungs-Konzept

Mit dem Stakeholder-Registrierungs-Konzept (vgl. Kapitel 8.3.3) wurde eine flexible Möglichkeit geschaffen, um die Einbindung von vielfältigen externen sicherheitskritischen Systemen in die smartLogic auf generische Weise zu ermöglichen und auch zur Laufzeit der smartLogic zu verändern. Somit können teure Umplanungen im Falle von Anpassungsbedarf an der Infrastruktur bzw. bei den externen Systemen vermieden und auch mögliche zukünftige Sicherheitsanforderungen, wie die direkte Einbindung zusätzlicher Sensordaten, ohne Anpassungen an der Grundlogik ermöglicht werden. Hierzu greift das Stakeholder-Registrierungs-Konzept auf die generische Beschreibung von RAs, wie sie in Kapitel 7.3.6 beschrieben wurden, zurück.

Das Stakeholder-Registrierungs-Konzept bringt zwar auf den ersten Blick entgegen der globalen Anforderung der *schlanken Logik* zusätzliche Komplexität in das System, da nicht mehr auf eine abgeschlossene Liste möglicher Elemente gesetzt wird, die von der Sicherungslogik zu berücksichtigen sind. Das generische Konzept ermöglicht es jedoch im Sinne der globalen Anforderung der *generischen Logik* zahlreiche spezifische funktionale Anforderungen auf generische Weise in die Logik zu integrieren. Dabei muss nicht die Logik erneut zugelassen werden, sondern nur die Richtigkeit der hinzukommenden Stakeholder-Registrierung sichergestellt werden. Ein solches Vorgehen erscheint sinnvoll, da nicht davon ausgegangen werden kann, dass zukünftig keine neuen funktionalen Sicherheitsanforderungen mehr formuliert werden (vgl. globale Anforderungen der *Migrationsfähigkei*t und der *Zukunftsfähigkeit*).

Flankenschutz

Beim Flankenschutz setzt die smartLogic auf eine Bewertung der tatsächlichen Betriebssituation (vgl. Kapitel 8.3.4). Die ausführliche Flankenschutzbetrachtung ist dabei nur erforderlich, da davon

ausgegangen wurde, dass auf absehbare Zeit nicht alle Fahrzeuge zu jeder Zeit vollständig überwacht werden können.

Es wird zunächst ein Flankenschutzsuchraum (potenzieller Flankenschutzraum) bestimmt und anschließend werden alle potenziellen Flankenschutzgefährdungen darin ermittelt. Der potenzielle Flankenschutzraum wird dabei, wo dies möglich ist, durch verfügbare Flankenschutzelemente (FPO) zu einem aktiven Flankenschutzraum verkleinert. Schließlich wird anhand der vorhandenen Flankenschutzgefährdungen und dem Grad an Sicherheit, dass keine unerkannte Gefährdung existiert, die Flankenschutz-Schutzrate bestimmt, die in die Berechnung der Gesamt-Schutzrate für die jeweilige Prüfanfrage einfließt.

Bei den Flankenschutzelementen wird immer nach dem Element gesucht, dass den höchsten Grad an Sicherheit bietet. Diese Methode ist aufwändiger, als direkt nach Auffinden eines beliebigen Flankenschutzelementes die Suche zu stoppen (vgl. globale Anforderung der *geringen Latenz*). Dafür wird die tatsächliche Schutzrate ermittelt, die möglicherweise höher ist, als wenn nur das jeweils erste gefundene Flankenschutzelement betrachtet wird (vgl. Anforderungen zur Zieldimension der *Robustheit*).

Zudem wird eine schnelle Umplanung des Flankenschutzes ermöglicht. Die Flankenschutz-Schutzrate kann jederzeit neu bestimmt werden, wenn sich die Betriebssituation verändert, beispielsweise durch eine weitere von der smartLogic zu prüfende Prüfanfrage. Somit können Flankenschutzelemente analog zu heutigen Zwieschutzweichen flexibel wieder freigegeben werden, wenn sie von einer anderen Fahrzeugbewegung mit anderem erforderlichen Status beansprucht werden und ausreichender Flankenschutz für die ursprünglich zu schützende Fahrt anderweitig gewährleistet werden kann. Diese flexible Freigabemöglichkeit kann zum Beispiel sinnvoll sein, um Fahrzeugbewegung das weitestmögliche Vorrücken (bis zum Grenzzeichen vor der relevanten Flankenschutz-Gefahrstelle) zu ermöglichen und somit die Infrastruktur bestmöglich auszunutzen.

Durch das beschriebene Vorgehen, kann die Logik auch bei Ausfall einzelner Flankenschutzelemente (z. B. durch Störung) eine Flankenschutz-Schutzrate bestimmen, so dass in der Regel die Prüfanfrage genehmigt werden kann (vgl. Anforderung der *Rückfallebenenintegration*). Das gilt insbesondere für den Fall, dass sich mit hinreichender Sicherheit nur vollüberwachte Fahrzeuge im Flankenschutzraum befinden. Voraussetzung ist allerdings, dass eine solche Sicherungslogik genehmigungsfähig ist.

Rangierfahrten

In Kapitel 8.3.5 wurde festgestellt, dass eine Unterscheidung in Zug- und Rangierfahrten (= Fahrten mit eingeschränktem Sicherheitsniveau) für die smartLogic nicht unbedingt erforderlich ist. Das setzt allerdings voraus, dass auch die Rangierfahrzeuge mit ETCS-Bordgeräten ausgestattet sind. Hierfür ist ein entsprechender Finanzierungsaufwand für die Fahrzeugausstattung erforderlich. Dafür wird die Sicherheit erhöht (Rangierunfälle kommen heute noch regelmäßig vor, vgl. Kapitel 5.4). Weiterhin wird die notwendige Komplexität der Sicherungslogik im Sinne der globalen Anforderungen der *schlanken Logik* und der *generischen Logik* reduziert. Schließlich ist auch eine positive Wirkung auf die Kapazität zu erwarten, da vollüberwachte „Rangierfahrten“ in kurzen Abständen auf „Zugfahrten“ folgen können, da ihr Zielpunkt überwacht wird, und die „Rangierfahrten“ somit auch mit höheren Geschwindigkeiten verkehren können.

Betrieb bei Abweichungen vom Regelbetrieb

Bei Abweichungen vom Regelbetrieb sieht die smartLogic gemäß der globalen Anforderung der *Rückfallebenenintegration* vor, die „Rückfallebenen“ möglichst in die Logik zu integrieren (vgl.

Kapitel 8.3.6). Dafür wurde eine generische Definitionsmöglichkeit von Rückfallebenen über eine Rückfallebenenfunktion entworfen, die das Konzept der Schutzrate erweitert und in deren Berechnung einfließt. Die Rückfallebenenfunktion kann beispielsweise bei der Registrierung von Stakeholder-Systemen als Parameter übermittelt werden. Weiterhin kann sie mit den Topologiedaten aus einer sicheren Datenquelle übermittelt werden.

Die Integration von Rückfallebenen in die Logik verkompliziert die Logik zwar (vgl. Anforderung der *schlanken Logik*). Diese zusätzliche Komplexität ist jedoch beherrschbar, da die funktionalen Anforderungen der Rückfallebene auf generische Weise übermittelt werden und damit die Topologieunabhängigkeit und die Zukunftsfestigkeit der Logik gewahrt bleibt. Im Gegenzug zur erhöhten Komplexität steht ein Plus an *Kapazität* und *Robustheit*, weil zeitaufwendige manuelle Rückfallebene und Benutzerinteraktionen weitestgehend vermieden werden.

8.10 Vergleich mit alternativen Ansätzen

In diesem Kapitel soll gemäß der in Kapitel 1.3 beschriebenen Struktur der inhaltlichen Hauptkapitel auf wesentliche Unterschiede der Konzepte, die der Funktionsweise der smartLogic zugrundeliegen, im Vergleich mit Funktionsweisen anderer innovativer Sicherungslogik-Ansätze, die in den Kapiteln 2.3 und 2.4 vorgestellt wurden, eingegangen werden.

Insbesondere zur RCA bzw. dem damit verbundenen Schweizer Programm smartRail 4.0 bestehen durch die parallele Entstehung zahlreiche konzeptionelle Gemeinsamkeiten, die bereits an verschiedenen Stellen im Text angesprochen wurden. Hierzu zählen vor allem die Architektur des Gesamtsystems der infrastrukturseitigen Sicherungstechnik und damit verbunden die Aufgaben der Sicherungslogik sowie die Konzepte der Drive Proctection Section (DPS), Allocation Section (AS) bzw. Allocation Area (AA) und Usage Restriction Area (URA), die von der RCA als Grundlage für diese Arbeit trotz des „Grüne Wiese“-Ansatzes übernommen (und teilweise ausgebaut) wurden.

Die RCA-Dokumente enthalten allerdings noch keine sehr detaillierten Konzepte. Es gibt jedoch bereits Dokumente (Arbeitsversionen) mit detaillierteren Konzepten des eng mit der RCA verknüpften schweizer Programms smartRail 4.0, auf die sich deshalb zum Teil bezogen wird [SBB AG 2018] und [SBB AG 2020].

Nachfolgend wird zunächst auf einige generelle Unterschiede der smartLogic zu den genannten Referenzquellen und anschließend näher auf Unterschiede zu den einzelnen Basis-Konzepten, die in Kapitel 8.3 beschrieben wurden, eingegangen. Dabei ist zu beachten, dass es aufgrund des „Grüne Wiese“-Ansatzes nicht Ziel dieser Arbeit ist, eine ausführliche Literaturvergleichsarbeit anzufertigen, sondern ein eigenes Konzept von Grund auf zu entwickeln. Daher beschränkt sich der nachfolgende Vergleich auf wesentliche funktionale Aspekte der smartLogic und wesentliche im 2. Hauptkapitel vorgestellte Referenzquellen.

Generelle Unterschiede

Im Gegensatz zu den in Kapitel 2.3 vorgestellten Ansätzen, insbesondere den Forschungsansätzen (vgl. HÖPPNER, MENZEL, AUTHIER und ETIENNE), wurde bei der Erstellung der smartLogic nicht die Vorgehensweise gewählt, zunächst mit einem möglichst einfachen Problem (z. B. Fahrt im Kreis mit einem Zug) anzufangen und dann die Komplexität schrittweise zu erhöhen. Stattdessen wurde versucht, einen möglichst umfassenden Überblick über mögliche heutige und zukünftige funktionale Anforderungen an die Sicherungslogik zu gewinnen, diese funktionalen Anforderungen aber mit einer möglichst generischen Prüflogik abzudecken.

Die modellierten Prozesse sind durch diese Vorgehensweise umfangreicher als in vielen anderen in Kapitel 2.3.3 vorgestellten wissenschaftlichen Arbeiten. Allerdings ist aus Sicht des Autors auch die Wahrscheinlichkeit geringer, dass die Grundlogik der Sicherungslogik beim Aufkommen neuer funktionaler Anforderungen wieder angepasst werden muss.

Die smartLogic konzentriert sich weiterhin allein auf die Prüfung der Zulässigkeit von Prüfanfragen und verbindet diese Prüfung nicht mit weiteren aktiven Handlungen, wie dem Umstellen von Weichen im Rahmen einer Fahrerlaubnisprüfung oder der Festlegung des an die Fahrzeugbewegung übermittelten Geschwindigkeitsprofils. Hierin besteht ein Unterschied zu einigen der in Kapitel 2.3 vorgestellten Arbeiten (z. B. MEYER ZU HÖRSTE und HÖPPNER, wobei Letzterer einen stärkeren Fokus auf betriebliche Prozesse als auf sicherungstechnische Details gelegt hat). Bei AUTHIER und ETIENNE reservieren und stellen sich die Fahrzeugbewegungen die stellbaren Fahrwegelemente selbst.

Weiterhin unterscheidet sich die smartLogic durch den Ansatz, innerhalb der Ebene der Sicherungslogik konsequent auf das Konzept von Fahrstraßen und einer diskreten Unterteilung der Gleistopologie wie beispielsweise bei MEYER ZU HÖRSTE, HÖPPNER oder den sicherungstechnischen Tripolen bei MENZEL zu verzichten. Stattdessen kann eine Fahrerlaubnis von jedem beliebigen Punkt der Gleisinfrastruktur bis zu jedem anderen beliebigen Punkt der Gleisinfrastruktur führen. Dieses Konzept ist jedoch zur klassischen Fahrstraßenlogik abwärtskompatibel, denn der Ortungsinformationsaggregator (vgl. Kapitel 4.4.4) kann bei Bedarf weiterhin nur feste Blöcke freigeben, beispielsweise, wenn ortsfeste Gleisfreimeldeanlagen die einzigen zuverlässigen Informationsquellen für die Fahrzeugposition und -integrität sind.

Ein struktureller Unterschied zu den in Kapitel 2.3 vorgestellten Ansätzen und zur RCA ist – soweit dem Autor bekannt –, dass bereits die komplette Movement Authority inkl. der wählbaren Parameter vom TMS zusammengestellt wird, bevor sie an die smartLogic zur Prüfung geschickt wird. Die smartLogic ergänzt auch nicht die Parameter der Route. Die smartLogic prüft einzig, ob die Werte der beantragten MA zu keinem unsicheren Zustand führen. Durch diese Vorgehensweise entsteht zwar Redundanz, da das TMS alle Parameter vorab bestimmen muss und die smartLogic diese nochmal prüft. Dafür kann die Logik allerdings so schlank wie möglich gehalten werden und die Zulassung wird vereinfacht.

Schutzrate

Für das erarbeitete Konzept der Schutzrate wurden keine ähnlichen Konzepte in der Literatur identifiziert. Üblicherweise erfolgt die Entscheidung über die Zulassung einer Fahrt oder eines Stellbefehls auf Basis fester Kriterien.

Zielpunkte

Bei den Zielpunkten ist für die smartLogic das Ende des sicheren Fahrwegs der hauptsächlich zu überprüfende Punkt, an dem sich die SvL befinden muss. Die EoA wird nur zweitrangig in Verbindung mit der Überlegung der Erreichenswahrscheinlichkeit eines Punktes hinter der EoA geprüft. Hierin unterscheidet sich das Konzept der smartLogic von alternativen Ansätzen, die von der EoA als bestimmenden Punkt und Ende der Fahrerlaubnis ausgehen und daran anschließend einen separaten Sicherheitspuffer in Form eines Durchrutschweges, Gefahrpunktabstands oder bei der RCA „Risk Buffer“ vorsehen.

Die Rücknahme dieses Sicherheitspuffers nach Halt der Fahrzeugbewegung erfolgt klassischerweise über die Auflösung der Fahrstraße oder einen speziellen Mechanismus zum Auflösen des Durchrutchweges, z. B. nach Ablauf einer vorgesehenen Zeit. Bei der smartLogic wird dagegen vorgeschlagen, dass das TMS die Funktion zum Kürzen der Fahrerlaubnis nutzt, da dieser

Mechanismus zu jeder Zeit und für einen beliebigen Teil der Fahrerlaubnis verwendet werden kann. Dabei wird davon ausgegangen, dass der Halteplatz der Fahrzeugbewegung nicht am Ende der Fahrerlaubnis sein muss, sondern aus verkehrlichen Gründen festgelegt und über einen nichtsicherheitskritischen Kanal an die Fahrzeugbewegung übermittelt wird.

Ein alternatives Konzept verfolgen AUTHIER und ETIENNE. In diesem Konzept beanspruchen die Fahrzeugbewegungen ihre physische Belegung und ihren Bremsweg und verschieben diese Belegung solange mit ihrer Fahrt, bis der Beginn des sicheren Bremsweges, der als virtueller Stopp-Punkt bezeichnet wird, an ein Hindernis stößt. Dabei wird der Fahrzeugbewegung immer der Ort des nächsten Hindernisses mitgeteilt. Führere Halte aus dispositiven Gründen können der Fahrzeugbewegung über einen nichtsicherheitskritischen Kanal mitgeteilt werden. Auch bei der smartLogic ist es möglich, dass das TMS die Fahrerlaubnis immer bis zum nächsten Hindernis bzw. Gefahrpunkt beantragt. Anders als bei AUTHIER und ETIENNE wird jedoch der gesamte beantragte Fahrweg auch von der Fahrzeugbewegung beansprucht. Hierdurch entsteht der Nachteil, dass bei nachträglichen Änderungswünschen die Kürzung der Fahrerlaubnis erforderlich ist. Dafür besteht der Vorteil, dass durch die Unterscheidung verschiedener Zielpunkte beispielsweise „überlappende Durchrutschwege“ möglich sind.

Stakeholder-Registrierungskonzept

Die RCA enthält mit den URAs ein generisches Konzept um Einschränkungen der Befahrbarkeit der Gleistopologie abbilden zu können, dass als Vorlage für die Restricted Areas (RAs) in dieser Arbeit dient. Die grundsätzliche Wirkungsweise ist dabei ähnlich und die URAs können auch durch das TMS oder in Folge von äußeren Umständen, wie sie in der smartLogic über die Reaktionsprozesse abgedeckt werden, entstehen.

Das Konzept der URAs wurde für die smartLogic jedoch zum einen systematisch ausgebaut, indem zum Beispiel Einschränkungen auf bestimmte Arten von Fahrzeugbewegungen, Registrierungsparameter, Löschparameter und die Abhängigkeit von Detektionsabschnitten oder Sensorwerten hinzugefügt wurden. Zum anderen wurde die Möglichkeit geschaffen, generisch externe Systeme in die Logik einzubinden. Dabei können die externen Systeme nicht nur RAs auslösen, sondern beispielsweie auch als zustimmungspflichtiges System zur Laufzeit der smartLogic registriert werden, dessen Zustimmung fortan in den Prüfprozessen abgeprüft wird. Ein vergleichbares Konzept wurde vom Autor in der Literatur bisher nicht identifiziert.

Flankenschutz

Einige der Referenzquellen gehen davon aus, dass nur vollüberwachte Fahrzeuge auf der Infrastruktur existieren z. B. AUTHIER und ETIENNE, womit sich ein Flankenschutzkonzept erübrigt. Diese Annahme wurde aber für die Erstellung der smartLogic im Sinne der globalen Anforderung der *Migrationsfähigkeit* für die nächste Zeit als unrealistisch ausgeschlossen.

Bei der RCA existiert ebenfalls ein Flankenschutz-Konzept, bei welchem ausgehend von Allocation Areas Pfade bestimmt werden, über die Flankenfahrt stattfinden können, die als *Risk Paths* bezeichnet werden [ERTMS Users Group & EULYNX 2020a]. Das Ende der Risk Paths kann ein Prellbock, ein kontrollierbares („controlled“) Fahrzeug oder eine DPS sein, die den Fahrweg unterbricht. Die Möglichkeit einer Begrenzung des Flankenschutzraums wie bei der smartLogic ist zumindest in den Unterlagen nicht beschrieben. Auch enthält die smartLogic eine Gewichtung der Flankenschutzelemente, die sich in der RCA-Beschreibung (bisher) nicht findet. Eine detaillierte Beschreibung der Flankenschutzprüfung wurde jedoch von der RCA auch noch nicht veröffentlicht.

Weiterhin verknüpft die smartLogic das Flankenschutzkonzept mit dem Konzept der Schutzrate.

Rangierfahrten

Bei der RCA wird die Unterscheidung zwischen Zug- und Rangierfahrten wie bei der smartLogic als nicht mehr unbedingt notwendig angesehen und generisch von *Trackbound Movable Objects* gesprochen. Stattdessen wird zwischen vollständig ortbaren Fahrzeugbewegungen und nicht vollständig ortbaren Fahrzeugbewegungen unterschieden [ERTMS Users Group & EULYNX 2020a] (vgl. auch [SBB AG 2018, S. 44]). Andere in Kapitel 2.3 vorgestellte Arbeiten haben sich nicht näher mit der Fragestellung beschäftigt, ob auf die Unterscheidung von Zug- und Rangierfahrten verzichtet werden kann.

Betrieb bei Abweichungen vom Regelbetrieb

Betrieb bei Abweichungen vom Regelbetrieb ist ebenfalls ein Thema, das bei den in Kapitel 2.3 vorgestellten Konzepten bisher nicht vorrangig betrachtet wurde. Auch bei der Erarbeitung der smartLogic war es nur ein Randthema. Jedoch wurde von Beginn an die Anforderung mitgedacht, dass Rückfallebenen in die Logik integriert werden sollten, so dass die smartLogic möglichst lange ohne fehleranfällige manuelle Rückfallebenen arbeiten kann. Hierbei ist ein Grundkonzept in Verbindung mit dem Konzept Schutzrate entstanden, zu dem kein vergleichbares Konzept in der Literatur gefunden wurde.

Sonstiges

Die SBB erläutert im smartRail 4.0-Dokument [SBB AG 2018] ebenfalls ausführlich ein mögliches Verfahren für den planmäßigen Fahrtrichtungswechsel. Dabei wird die Möglichkeit des Vergleichs der vorherigen und aktuellen Länge der Fahrzeugbewegung im Falle einer sicheren Übermittlung dieser Daten durch die Fahrzeugbewegung nicht beachtet. Die Fahrzeugbewegung muss daher immer zunächst im ETCS-Modus „On Sight“ starten, aus dem sich der Tf mit einer Freimeldung („Track Ahead Free Message“) bei Erreichen eines bestimmten Punktes befreien kann [SBB AG 2018, 42f].

Weiterhin sind in [SBB AG 2018] auch detaillierte Verfahren für das Vereinigen und Trennen von Zugfahrten vorgestellt, die sehr ähnlich zu den Überlegungen aus Kapitel 8.4.3 sind:

- Bei Vereinigungen muss immer im ETCS-Modus On Sight an den Kupplungspunkt herangefahren werden. Dabei dürfen sich für den Vereinigungsfall die Fahrerlaubnisse überlappen, wobei zu beachten ist, dass sich im smartRail-Konzept auch um stehende Fahrzeuge eine Fahrerlaubnis befindet, die somit in etwa die Funktion des Beanspruchungsobjekts in der smartLogic übernimmt. Anschließend meldet eines der Fahrzeuge die Vereinigung und seine Fahrerlaubnis wird so ausgedehnt, dass sie auch die ehemals andere Fahrzeugbewegung umfasst. Die zweite Fahrerlaubnis kann analog zum Vorgehen bei der smartLogic erst aufgelöst werden, wenn das Freisein des Gleises bestätigt wurde.
- Der Prozess für Trennung ist dagegen fast gleich zur smartLogic, wobei nur von maximal zwei Fahrzeugbewegungen nach der Trennung ausgegangen wurde und kein Problem darin gesehen wurde, dass einer der neu entstandenen Fahrzeugbewegungen eine Fahrerlaubnis gegeben werden könnte, in der sich ein anderer Teil der ehemaligen Fahrzeugbewegung befinden könnte. In der Realität dürfte ein solcher Fehler auch vom Tf oder selbst der Hinderniserkennung eines ATO-Systems erkannt werden, so dass es sich vermutlich um kein tatsächliches Sicherheitsproblem handelt und die smartLogic an dieser Stelle übervorsichtig ausgelegt ist.

8.11 Zusammenfassung

Im achten Hauptkapitel wurde auf Grundlage des Datenmodells aus Kapitel 7 die Verhaltensmodellierung der neuen Sicherungslogik smartLogic entwickelt. Hierfür wurde ein Verfahren mit fünf Schritten entworfen. Demnach werden zunächst für jede zu modellierende Prozessfunktion bzw. Subroutine (vgl. zu den Begriffen den Abschnitt „Unterscheidung verschiedener Arten von Funktionen“ im Kapitel 6.2.2) die relevanten Prüfbedingungen identifiziert. Im zweiten Schritt folgt eine Beschreibung des Ablaufs der Prozesse bzw. Subroutinen in natürlicher Sprache, damit ein Überblick über den Ablauf gewonnen werden kann. Auf dieser Basis werden die beteiligten externen Systeme bestimmt und schließlich der Ablauf der Prozesse bzw. Subroutine grafisch mit einem UML-Aktivitätsdiagramm beschrieben. Anschließend folgt zur Vollständigkeitskontrolle als letzter Schritt eine erneute Prüfung gegen den Katalog der Prüfbedingungen aus Kapitel 6.

Bevor die Modellierung der einzelnen Prozesse und Subroutinen mit dem beschriebenen Verfahren durchgeführt wurde, mussten grundsätzliche konzeptionelle Fragestellungen zur Funktionsweise der smartLogic geklärt werden. Hierzu erfolgte eine ausführliche Erörterung der jeweiligen Thematik in den Konzept-Kapiteln 8.3 und 8.4. (Eine Zusammenfassung der Ergebnisse der Erörterung zu den Basis-Konzepten mit Abwägung der Vor- und Nachteile findet sich in Kapitel 8.9.)

Anschließend wurden in Kapitel 8.5 die Prüfprozesse und in Kapitel 8.6 Subroutinen nach dem beschriebenen fünfschritten Verfahren modelliert. Die beiden Kapitel enthalten aufgrund der begrenzten Bearbeitungszeit nur die wichtigsten Prüfprozesse, die in Kapitel 6.7 in die Kategorie der Basisfunktionen eingeordnet wurden, und für das Verständnis der Prozesse wesentliche Subroutinen.

Zu den Reaktionsprozessen konnten in Kapitel 8.7 – ebenfalls aus Zeitgründen – nur grundsätzliche Überlegungen angestellt werden. Insbesondere die Reaktionsprozesse, aber auch Übergangsbedingungen zu anderen Stellwerkssystemen, Bedienfunktionen und die Protokollierung sind daher noch zu erarbeiten (vgl. Kapitel 8.8).

Als Fazit der Ergebnisdiskussion zum vorliegenden Hauptkapitel (Kapitel 8.9) kann zusammengefasst werden, dass mit dem in diesem Hauptkapitel beschriebenen Verhalten der smartLogic eine zwar auf umfangreiche Anwendungsfälle und funktionale Anforderungen vorbereitete aber dennoch verhältnismäßig schlanke Sicherungslogik entstanden ist. Durch den generischen Aufbau, mit dem zusätzliche funktionale Anforderungen auch nachträglich ergänzt werden können, und der dynamischen Bewertung des Risikos von Prüfanfragen auf Basis der Schutzrate ist die Logik zukunftsfähig und ermöglicht eine gute Ausnutzung der Kapazität der Infrastruktur auf Basis der tatsächlichen aktuellen Betriebslage.

Im Vergleich zu alternativen Ansätzen (vgl. Kapitel 8.10) ist im Wesentlichen die Entwicklungsrichtung von einem umfangreichen Anforderungskatalog zu einer generischen Logik hervorzuheben, weiterhin der Verzicht auf eine Unterteilung der Infrastruktur in diskrete Fahrwegabschnitte und vorprojektierte Fahrstraßen. Zudem wird die Fahrerlaubnisanfrage vom TMS durch die Logik nicht mehr verändert, sondern als Ganzes vorgegeben.

9 Demonstrator und Anwendungsbeispiel

Zur Veranschaulichung und Evaluation der Erkenntnisse der vorherigen Kapitel, insbesondere in Hinblick auf Kapazitätseffekte durch die darin entwickelte smartLogic, ist im Eisenbahnbetriebsfeld Darmstadt (EBD) ein Software-Demonstrator (Pretotyp) der Sicherungslogik entstanden. In diesem Hauptkapitel soll der Demonstrator kurz vorgestellt werden (Kapitel 9.1). Weiterhin wird die Grundlogik der smartLogic an einem einfachen Beispiel verdeutlicht (Kapitel 9.2).

9.1 Demonstrator

In diesem Kapitel wird der im Rahmen des Projektes entstandene Software-Demonstrator kurz vorgestellt. Um den weiteren Entwicklungsprozess festlegen zu können, muss zunächst die Zielstellung für dessen Entwicklung hergeleitet werden (Kapitel 9.1.1). Aus der Zielstellung können die Anforderungen an den Demonstrator gefolgert werden (Kapitel 9.1.2). Auf dieser Basis kann schließlich hergeleitet werden, wie sich der Demonstrator in die Systemumgebung der Pretotypenlandschaft im EBD einfügt (Kapitel 9.1.3) und wie er technisch aufgebaut ist (Kapitel 9.1.4).

Zum Zeitplan der Erstellung dieser Dissertation sind die technischen Arbeiten am Demonstrator noch nicht ganz abgeschlossen und es wurden bisher nur einzelne Szenarien demonstriert, welche die Funktionsweise der smartLogic veranschaulichen. Eines dieser Szenarien ist in Kapitel 9.2 geschildert. Eine systematische Kapazitätsuntersuchung der neuen smartLogic wurde allerdings, wie in Kapitel 3.3 festgelegt, aus Ressourcengründen nicht durchgeführt. Hierzu laufen zum Zeitplan der Erstellung dieser Dissertation weitere wissenschaftliche Arbeiten, auf die Kapitel 9.1.5 einen Ausblick gibt.

Der Demonstrator wurde von einem aus technischen Mitarbeitern und studentischen Hilfskräften bestehenden Team auf Basis des in dieser Arbeit erstellten UML-Modells implementiert. Feedback des Entwicklerteams zur Logik wurde im Sinne eines iterativen Verfahren wieder in den Entwicklungsprozess der smartLogic integriert.

9.1.1 Ziele des Demonstrators

Primäres Ziel des Demonstrators ist es, die komplexen Sachverhalte und Nutzenpotenziale, wie sie in Kapitel 3.4 beschrieben wurden, zu verdeutlichen. Als Plattform bot sich die modular aufgebaute Eisenbahnsimulation am EBD an, in die der Demonstrator mit vertretbarem Aufwand integriert werden kann. Eine vertiefte Analyse möglicher weiterer Plattformen wurde daher nicht durchgeführt.

Damit der Demonstrator möglichst effektiv gestaltet ist, ist es sinnvoll, neben dem bereits genannten Ziel mögliche weitere Ziele bzw. Einsatzzwecke zu identifizieren. Die Ziele des Software-Demonstrators können nicht aus den inhaltlichen Zielen an die smartLogic hergeleitet werden, da der Demonstrator die erarbeitete Logik nur veranschaulichen, aber nicht inhaltlich verändern soll. Daher wurden mögliche Ziele am Institut für Bahnsysteme und Bahntechnik der TU Darmstadt sowie in Zusammenarbeit mit dem Fördermittelgeber, der DB Netz AG, erhoben. Dabei wurden die folgenden Ziele identifiziert:

- Der Demonstrator soll die Funktionsweise und insbesondere die Vorteile der smartLogic verdeutlichen, um das Konzept Entscheidungsträgern, Fachexperten und späteren Anwendern vermitteln zu können.
- Der Demonstrator soll die Evaluation der Nutzenpotenziale der smartLogic ermöglichen.

- Der Demonstrator soll die Wechselwirkungen der smartLogic mit den anderen Systemkomponenten des Produktionssystems Eisenbahn aufzeigen und eine Analyse der Wechselwirkungen ermöglichen.
- Der Demonstrator soll zur Evaluation des Konzepts der smartLogic dienen und helfen mögliche Logikfehler aufzudecken.

9.1.2 Anforderungen an den Demonstrator

Aus den in Kapitel 9.1.1 identifizierten Zielen konnten zusammen mit den Entwicklern die folgenden Anforderungen hergeleitet werden:

- Der Demonstrator darf bezüglich Aufbau und Funktionsweise nicht von der Beschreibung der smartLogic gemäß Hauptkapitel 7 und 8 dieser Arbeit abweichen. Nur so kann die smartLogic adäquat evaluiert werden.
- Die Umsysteme müssen den erwarteten Funktionsumfang für die Anwendungsszenarien über – soweit existent – standardisierte Schnittstellen bereitstellen, um die Wechselwirkungen mit den Umsystemen verdeutlichen.
- Es muss eine Benutzeroberfläche existieren, welche die demonstrierten Szenarien nachvollziehbar macht.
- Es muss eine geeignete Logging-Ausgabe existieren, welche die internen Prüfprozesse der smartLogic nachvollziehbar macht.
- Der Demonstrator muss in der Lage sein, komplexe betriebliche Situationen (Szenarien) oft hintereinander simulieren zu können, um Kapazitätsanalysen durchführen zu können.
- Die Simulation muss dabei zufällige Umwelteinflüsse, die einen relevanten Einfluss auf das Simulationsergebnis haben, berücksichtigen und bei jedem Simulationsdurchlauf leicht variieren können.
- Der Demonstrator muss ohne Anpassungsaufwand auf verschiedenen Gleistopologien und mit Fahrzeugen mit verschiedenen Eigenschaften arbeiten können.
- Es müssen auch Szenarien für die smartLogic generiert werden können, die Fehler enthalten, um zu untersuchen, ob fehlerhafte Prüfanfragen von der smartLogic abgelehnt werden.
- Perspektivisch sollen in die Szenarien auch außergewöhnliche Ereignisse eingepflegt werden können, um die Reaktionsprozesse der Logik zu testen. Diese Anforderung war jedoch vorerst nicht prioritär, da die Reaktionsprozesse in dieser Arbeit nur am Rand bearbeitet wurden.

Es wurden nur qualitative Anforderungen erfasst. Die technischen Anforderungen wurden dem Entwicklerteam nicht vorgegeben.

9.1.3 Einbettung in die Pretotypenlandschaft im EBD

Gemäß den Anforderungen in Kapitel 9.1.2 muss der Demonstrator der smartLogic sich in ein modulares Systemumfeld des EBD einfügen. Das EBD besteht aus einer Modelleisenbahnanlage, die mit einer umfangreichen, modularen Simulationssoftware für den Bahnbetrieb verknüpft ist und von dieser gesteuert wird. Die Modelleisenbahn kann dabei als Visualisierung der Berechnungen der Software, insbesondere der Fahrzeugsimulation gesehen werden

Auf Basis der genannten Anforderung sowie der in Kapitel 4 erarbeiteten Architektur wurde die bestehende EBD-Architektur erweitert. Die Architektur aus Kapitel 4 muss zwar vom Demonstrator eingehalten werden, kann jedoch nicht direkt übernommen werden, da es modellbahnspezifische Besonderheiten gibt. Abb. 81 zeigt die grundsätzliche Architektur, die mit dem Entwicklerteam gemeinsam erarbeitet wurde. Für eine nähere Erläuterung der einzelnen Komponenten vgl. auch Kapitel 4.

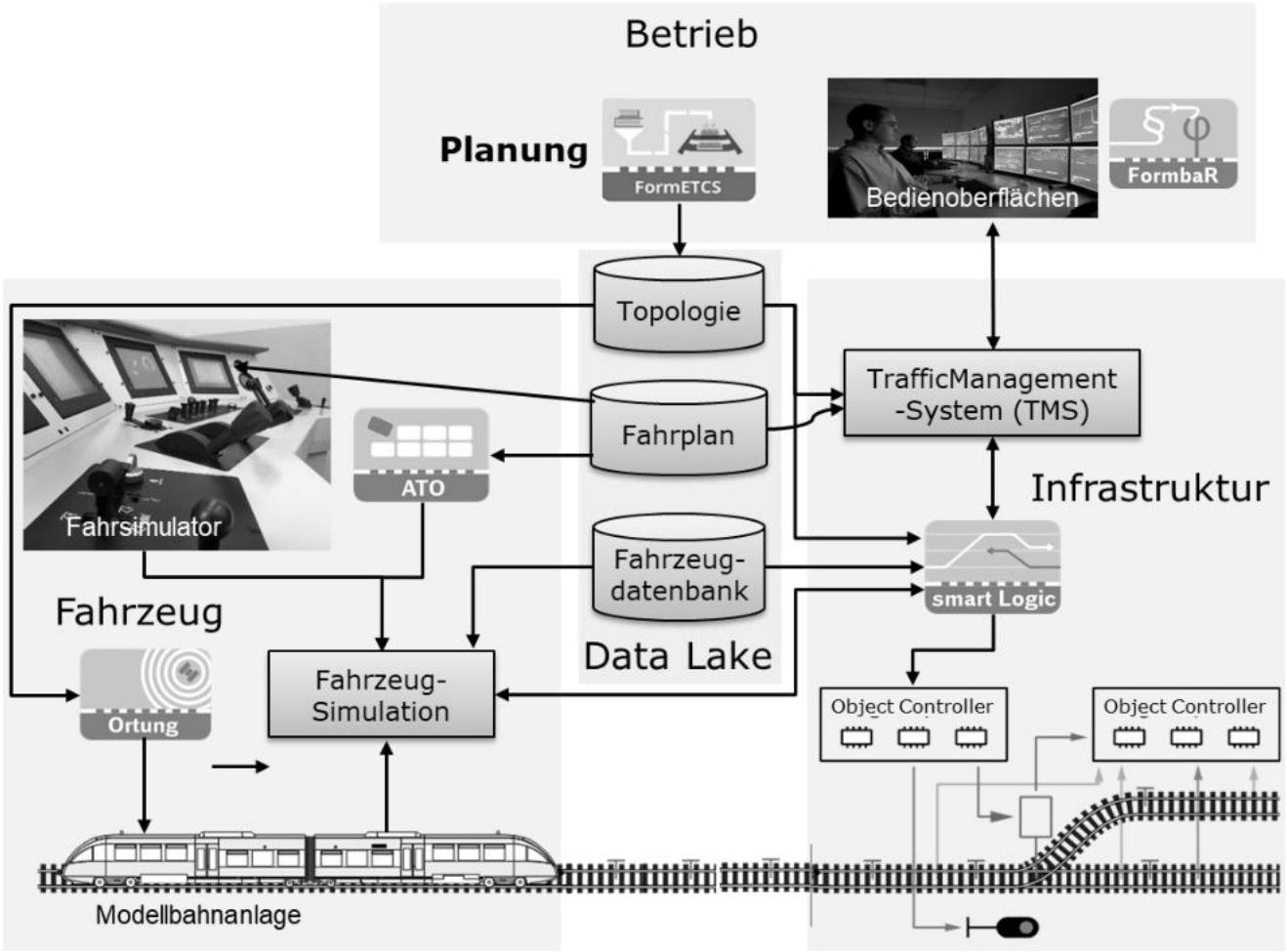


Abb. 81: Einbettung der smartLogic in die Pretotypenlandschaft im EBD (schematisch)
Quelle: Institut für Bahnsysteme und Bahntechnik, TU Darmstadt

Die smartLogic gehört zum Teil der Infrastruktur. Sie erhält Anfragen vom TMS. Die benötigten Daten für die Prüfung kommen aus dem Data Lake des EBD. Hier befinden sich unter anderem Topologie-Daten und Fahrzeugdaten in einer Fahrzeug-Datenbank. Die Topologie-Daten können derzeit aus dem PlanPro-Format eingelesen werden, in dem Daten über die Infrastruktur im Eisenbahnbetriebsfeld vorhanden sind und werden dann in das interne Datenmodell konvertiert. Über eine der ETCS-Schnittstelle nachgebildete Kommunikationsschnittstelle kommuniziert die smartLogic mit der Fahrzeugsimulation. Ein Ortungsinformationsaggregator kombiniert fahrzeugseitige und infrastrukturseitige Ortungsinformationen zu einem möglichst genauen Bild der tatsächlichen Fahrzeugpositionen. (Bei FormETCS und FormbaR handelt es sich um Forschungsdemonstratoren zur automatisierten Planung von ETCS-Ausrüstung bzw. digitalisierten Regelwerken.)

9.1.4 technischer Aufbau

Der Demonstrator der smartLogic ist in Java entwickelt und enthält eine Oberfläche in Form eines Webservices, die ein Test-TMS darstellt. Im Test-TMS kann der Benutzer manuell Fahrerlaubnisanfragen oder Stellanforderungen erstellen und an die smartLogic senden. Das Test-TMS lässt dabei bewusst auch fehlerhafte Anfragen zu, um die Funktionsweise der smartLogic zu testen. So können z. B. zu hohe Geschwindigkeiten, fehlerhafte (beispielsweise nicht zusammenhängende) Routen oder Kollisionen mit anderen Fahrzeugen angefragt werden.

Da das manuelle Erstellen einer MA im Test-TMS Zeit benötigt, existiert auch eine Szenarien-Datenbank, in der Anfragen an die Logik bereits vorausgefüllt integriert sind und mit einem Timecode gestartet werden können. Die Funktionsweise der smartLogic im Demonstrator entspricht der Modellierung in dieser Arbeit. Allerdings konnten bisher erst die grundlegenden Prüfprozesse umgesetzt werden.

9.1.5 Fazit und Ausblick

Mit dem Demonstrator der smartLogic lassen sich, eingebettet in die Systemlandschaft im EBD, vielfältige Szenarien demonstrieren. Dabei kann kurzfristig zwischen smartLogic und klassischer Stellwerkstechnik gewechselt werden. Somit können Unterschiede zwischen smartLogic und klassischen ESTW veranschaulicht werden. Durch die Szenarien-Datenbank können auch komplexere Simulationen mit genauen Zeitvorgaben für den Ablauf der einzelnen Simulationsschritte durchgeführt werden. Somit sind beispielsweise Kapazitätsuntersuchungen möglich und auch derzeit am Institut für Bahnsysteme und Bahntechnik der TU Darmstadt geplant.

Weiterhin konnte über kontinuierliches Feedback der Implementierer des Demonstrators ein Realitätscheck der Umsetzbarkeit der Logik durchgeführt und die Qualität der Darstellung der Modellierung verbessert werden.

9.2 Anwendungsbeispiel

Im Folgenden soll die Funktionsweise der smartLogic an einem einfachen Anwendungsbeispiel verdeutlicht werden.

9.2.1 Szenario

Die Infrastruktur für das Beispiel besteht aus einer zweigleisigen Abzweigstelle (vgl. Abb. 82). Die Weichengeschwindigkeiten der drei Weichen betragen 100 km/h im abzweigenden Strang. Zudem existiert über W1 sowie Teile der beiden angrenzenden Gleissegmente 101 und 102 eine vorübergehende Langsamfahrstelle (TSR) mit einer vorgegebenen Geschwindigkeit von 50 km/h. Über die Gleissegmente 101 und 111 sowie 102 und 114 existiert außerdem jeweils ein Bahnübergang.

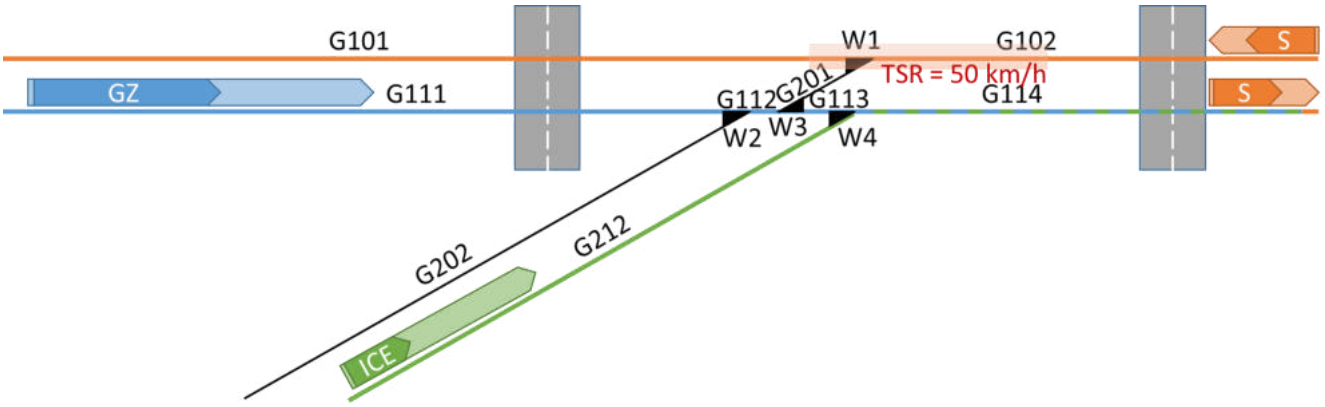


Abb. 82: Szenario für das Anwendungsbeispiel
Der geplante Fahrweg der Fahrzeugbewegungen ist jeweils mit der Farbe des Fahrzeuges eingezeichnet.
[Eigene Darstellung]

Im Szenario existieren vier Fahrzeugbewegungen, die alle vollüberwacht sind und eine gesicherte Länge und Zugvollständigkeit haben. Eine S-Bahn soll von Gleissegment 102 nach Gleissegment 101 verkehren. Zeitgleich soll ein Güterzug in die Gegenrichtung verkehren und dort einer weiteren S-Bahn folgen. Zusätzlich befindet sich ein ICE aus Richtung des Gleissegmentes 212 in der Anfahrt, der auf Gleissegment 114 weiterfahren soll. Für jeden Zug ist die tatsächliche physische Position (dunklerer Farbton) sowie der aktuelle Mindest-Bremsweg und die Ortungsungenauigkeit (hellerer Farbton) eingezeichnet. Um die Konzentration auf die verschiedenen Beanspruchungszustände der Gleisinfrastruktur zu lenken, wurden die Grafiken insofern vereinfacht, dass sich die verschiedenen Züge zwischen den dargestellten Schritten nicht gemäß ihrer Fahrtrichtung vorwärts bewegen. Ob nun zuerst der Güterzug oder der ICE auf die S-Bahn auf Gleis 114 folgen sollen, ist eine betriebliche Entscheidung, die vom TMS zu treffen ist. Im Beispiel entscheidet das TMS, dass der ICE Vorrang hat.

9.2.2 Ausgangslage

Abb. 83 zeigt die Ausgangslage für das Anwendungsbeispiel. Beide Bahnübergänge haben keine Zustimmung zur Befahrung gegeben, deshalb enden die aktuellen Fahrerlaubnisse der beteiligten Zugfahrten jeweils vor dem nächsten Bahnübergang. An diesem Punkt liegen sowohl EoA als auch SvL. Die Weichen befinden sich jeweils in der Lage, die nicht mit einem roten Balken markiert ist (der rote Balken steht für Nichtbefahrbarkeit in diesem Strang). Nur die Weiche 4 ist aktuell von einer Fahrzeugbewegung im Fahrweg beansprucht, da der ICE bereits eine Fahrerlaubnis bis vor den rechten Bahnübergang erhalten hat. Die Weiche 3 bietet derzeit dem ICE Flankenschutz und enthält daher eine Flankenschutzbeanspruchung.

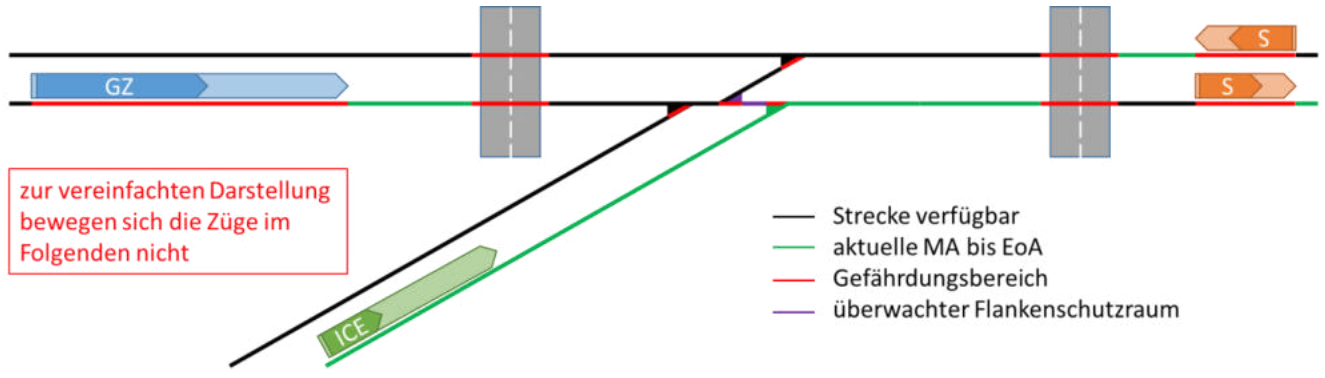


Abb. 83: Ausgangslage für das Anwendungsbeispiel
[Eigene Darstellung]

9.2.3 Schritt 1: Verlängern der Fahrerlaubnis von S-Bahn und ICE

Wenn nun der rechte Bahnübergang geschlossen ist (und sofern die maximale Schließzeit des BÜs voraussichtlich nicht überschritten wird), kann das TMS gemäß der in Kapitel 9.2.1 angenommenen Prioritäten die Verlängerung der Fahrerlaubnis für die S-Bahn und den ICE mit jeweils einem MP Request (unabhängig voneinander) beantragen. Die Aufforderung zum Schließen des Bahnübergangs kann durch das TMS oder auch durch einen Gleiskontakt erfolgen, da es sich nicht um einen sicherheitskritischen Vorgang handelt. Die smartLogic kontrolliert jedoch im Laufe des Prüfprozesses für die Fahrerlaubnis, ob der Bahnübergang geschlossen ist. Es ist auch möglich, dass sich der Bahnübergang erst zu diesem Zeitpunkt schließt, allerdings wird dann der Abschluss des Prüfprozesses für die Fahrerlaubnis entsprechend verzögert.

Beim Beantragen der Fahrerlaubnis macht es Sinn, dass das TMS jeweils den vom aktuellen Standort am weitesten entfernten Punkt auf der Route der Fahrzeugbewegung als Zielpunkt wählt, der von der smartLogic noch genehmigt werden kann (vgl. Kapitel 8.3.2). (Theoretisch könnte das TMS auch einen näheren Punkt am aktuellen Standort der Fahrzeugbewegung wählen.) Der Zielpunkt für die S-Bahn ist demnach der Beginn des zweiten Bahnübergangs. Der Zielpunkt für den ICE das Ende der Beanspruchung der Infrastruktur der zweiten S-Bahn auf Gleissegment 114. In beiden Fällen setzt das TMS sowohl EoA als auch SvL auf diese Punkte.

Die smartLogic prüft jetzt die beiden MP Requests gemäß der Vorgehensweise aus Kapitel 8.5.3. Zunächst wird die Betriebsbereitschaft der smartLogic mittels Selbsttest überprüft und die übermittelte Nachricht wird einem Syntax-Check unterzogen. Auf die übermittelten Elemente der jeweiligen Route wird vorübergehend während dem Zeitraum der Prüfung der Anfrage eine Request Occupation eingetragen. Anschließend wird der Status der beteiligten Elemente abgefragt, um sicherzugehen, dass die smartLogic das aktuellste Bild der Realität kennt.

Als nächstes wird die beantragte Route geprüft. Im Fall der in der Grafik im oberen Gleis abgebildeten S-Bahn führt diese Route über die Gleissegmente 102 und 101, wobei das Ende der Route sich in etwa mittig auf Gleissegment 101 befindet und deshalb mit einer intrinsischen Koordinate auf dem Gleissegment 101 angegeben wird. Danach wird auch geprüft, ob sich die Weichen in der richtigen Lage für diese Route befinden.

Für jedes Gleissegement der Route wird nun überprüft, welche Einschränkungen der Befahrbarkeit ggf. existieren und ob diese Vorgaben in der beantragten Fahrerlaubnis eingehalten wurden. Dies umfasst zunächst die Vorgaben für Gleisbereiche, durch welche die Route führt (vgl. Kapitel 7.3.8) sowie Restricted Areas (RAs) (vgl. Kapitel 7.3.6). Für alle existierenden RAs wird geprüft, ob die Vorgaben eingehalten werden. Im Beispiel ist die TSR von 50 km/h zu beachten, die sowohl über Gleissegment 102 als auch über Gleissegment 101 gefunden wird (vgl. Abb. 82). Informationen über die Strecke, die Vorgaben für die Fahrzeugbewegung enthalten, müssen in der beantragten Fahrerlaubnis korrekt enthalten sein (Track Information Check).

Anschließend wird auf der Route nach Gefahrenbereichen (DAs) (vgl. Kapitel 7.3.7) gesucht, mit denen sich die Route überschneidet. Für gefundene Gefahrenbereiche muss jeweils bewertet werden, wie diese sich auf die Schutzrate auswirken. Auch Konflikte mit den Beanspruchungen durch andere Fahrzeugbewegungen müssen gefunden und auf ihre Vereinbarkeit mit der Sicherheit geprüft werden.

In Bezug auf vorhandene Stakeholder-Systeme müssen die Registrierungen geprüft werden. Zustimmungspflichtige Stakeholder-Systeme müssen um Zustimmung zur beantragten Fahrerlaubnis gebeten werden, benachrichtigungspflichtige Systeme müssen betriebsbereit sein, um die Benachrichtigung empfangen zu können. Im Beispiel muss für beide Fahrerlaubnisse die Zustimmung des rechten Bahnübergangs eingeholt werden. Dieser Vorgang ist in jedem Fall erforderlich, auch

wenn das TMS bereits weiß, dass der Bahnübergang geschlossen ist und deshalb die beiden Prüfprozesse überhaupt erst in Gang gebracht hat.

Die Flankenschutzbetrachtung ist für den ICE wegen der physischen Flankenschutzweiche W3, welche die einzige Flankenschutz-Gefahrstelle nach einem kurzen zu prüfenden Gleissegment vollständig abdeckt, schnell abgeschlossen. Für die S-Bahn ist die Situation dagegen nicht so klar. Theoretisch könnte sowohl aus Gleissegment 111 als auch aus Gleissegment 202 ein Fahrzeug die Flankenschutz-Gefahrstelle an W1 erreichen. Bei der Prüfung von G111 ist die erste zu überprüfende Stelle (rote Linie in Abb. 83) am linken Bahnübergang. Auch wenn hier kein physischer Schutz besteht, kann die Information über den ungesicherten Bahnübergang dennoch indirekt betrieblichen Flankenschutz bieten, da der ungesicherte Bahnübergang bereits auf unzulässiges Befahren überwacht wird. Eine weitere Fahrt kann deshalb über den Bahnübergang nicht erlaubt werden und die Wahrscheinlichkeit für eine undetektierte Befahrung des Bahnübergangs muss zu dessen Schutz hinreichend klein und mit einem Reaktionsprozess abgesichert sein. Spätestens der Güterzug kann jedoch Flankenschutz bieten, solange er vollüberwacht ist, denn den Güterzug kann kein weiteres schienengebundenes Fahrzeug passieren und die Vollüberwachung impliziert, dass der Güterzug mit hinreichender Sicherheit vor der Gefahrstelle zum Stehen gebracht wird. Auf Gleissegment 202 gibt es keine Elemente, die Flankenschutz bieten können. Daher muss die Timeout-Regelung für die Bestimmung des potenziellen Flankenschutzraumes angewandt werden (vgl. Kapitel 8.3.4).

Anschließend werden die mit der MA übermittelten Parameter auf ihre Übereinstimmung mit den topologischen Daten geprüft, wie die darin übermittelten Zielpunkte und das Geschwindigkeitsprofil. Zudem werden die benachrichtigungspflichten Stakeholder-Systeme benachrichtigt. Wenn die jeweilige Prüfung abgeschlossen und die jeweilige Fahrerlaubnisanfrage genehmigt ist, können die Fahrerlaubnisse an die Züge übermittelt und die RRM an das TMS gesendet werden. Der gesamte Prüfprozess erfolgt für jede der Fahrerlaubnisse getrennt und verläuft in beiden Beispielfällen mit positivem Ergebnis.

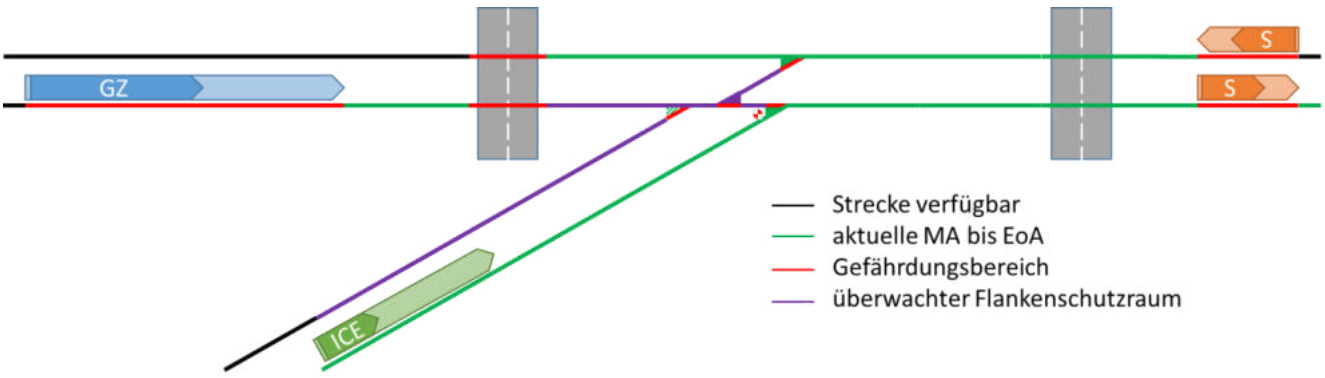


Abb. 84: Situation nach Schritt 1 im Anwendungsbeispiel

9.2.4 Schritt 2: Umstellen der Weiche W3

Um dem Güterzug möglichst wenig auszubremsen, soll dieser ebenfalls einen Zielpunkt bekommen, der so weit wie möglich von seiner aktuellen Position entfernt ist. Der theoretisch am weitesten entfernte noch sicher anzufahrende Zielpunkt ist das Grenzzeichen von Weiche 4. Um dieses zu erreichen, muss allerdings Weiche 3 umgestellt werden. Hierfür sendet das TMS einen TESC Request an die smartLogic. Die smartLogic prüft nach Selbsttest und Syntax-Check nur, ob weitere Beanspruchungen der Weiche vorhanden sind.

Es existiert zwar keine Fahrzeugbelegungsbeanspruchung, aber eine Flankenschutzbeanspruchung. Daher muss geprüft werden, ob der Flankenschutz anderweitig gewährleistet werden kann. Im Beispiel kann der Flankenschutz für den ICE auf die gleiche Weise gewährleistet werden, wie dies in Kapitel 9.2.3 für die S-Bahn beschrieben wurde. Deshalb ist ein Umstellen der Weiche möglich. Die Situation nach Schritt 2 ist in Abb. 85 dargestellt.

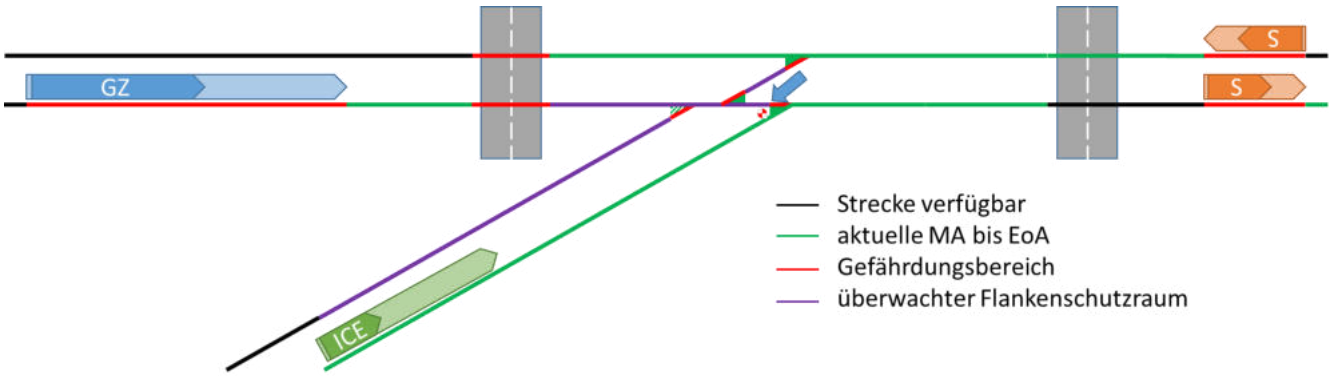


Abb. 85: Situation nach Schritt 2 im Anwendungsbeispiel

9.2.5 Schritt 3: Verlängern der Fahrerlaubnis des Güterzuges

Sobald auch der linke Bahnübergang (z. B. nach Aufforderung durch das TMS) geschlossen ist, kann nun auch die Fahrerlaubnis des Güterzuges bis vor das Grenzzeichen von W4 verlängert werden. Auch in diesem Fall wird das TMS vermutlich EoA und SvL an die gleiche Position, nämlich die des Grenzzeichens von W4 setzen. Ansonsten verläuft die Prüfung des MP Requests analog zur Prüfung der MP Requests für die S-Bahn und den ICE.

Der Flankenschutz für den Güterzug muss an W1 natürlich auch gewährleistet sein. Hierzu weitet sich der potenzielle Flankenschutzraum (violette Linie parallel zum ICE in der Grafik) im Vergleich zum bisherigen Flankenschutzraum für die S-Bahn (bzw. nach dem Umstellen von W2 dem Flankenschutzraum des ICEs) etwas aus, da die neue Flankenschutz-Gefahrstelle von einer potenziellen Flankenschutzgefährdung bereits etwas früher erreicht werden würde (vgl. Kapitel 8.3.4). Abb. 86 zeigt den Zustand nach Schritt 3.

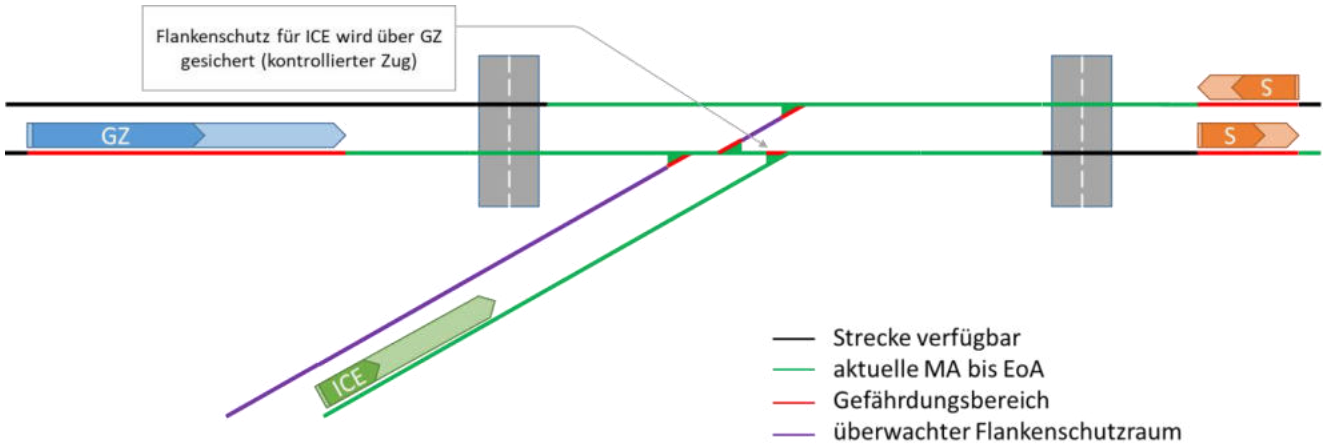


Abb. 86: Situation nach Schritt 3 im Anwendungsbeispiel

9.2.6 Fazit

Das Anwendungsbeispiel hat einige der Arbeitsprinzipien der smartLogic in einem Szenario auf einer einfachen Infrastruktur gezeigt. Bereits auf dieser einfachen Infrastruktur konnte deutlich werden, dass die smartLogic Wartezeiten reduzieren kann, indem die Infrastruktur durch Fahrerlaubnisse mit flexiblen Längen bestmöglich für die Fahrzeuge zur Verfügung gestellt werden kann. Weiterhin konnte das Prinzip der dynamischen Flankenschutzsuche verdeutlicht werden, so dass nicht zwingend nötige Fahrstraßenausschlüsse vermieden werden.

10 Fazit und Ausblick

In der vorliegenden Dissertation wurde unter der Bezeichnung smartLogic ein Ansatz für die Neugestaltung der Sicherungslogik als zentrale infrastrukturseitige Komponente der Eisenbahnsicherungstechnik entwickelt und evaluiert. Dabei wurden verschiedene Umsetzungsvarianten identifiziert und in Bezug auf die einzelnen Design-Entscheidungen gegeneinander abgewogen. Die Arbeit möchte damit einen Beitrag zur aktuellen Debatte der zukünftigen Ausrichtung der Eisenbahnsicherungstechnik im digitalen Informationszeitalter liefern.

Zusammenfassung der Vorgehensweise

Hierzu wurde zunächst der Aufbau der klassischen Sicherungslogik erläutert und verschiedene bisherige innovative Forschungs- und Praxisansätze für eine neue Sicherungslogik, insbesondere auf Basis eines generischen Ansatzes, vorgestellt. Diese Forschungsarbeiten beschreiben üblicherweise ein stark vereinfachtes System, das zunächst sowohl von der Infrastruktur als auch dem Funktionsumfang auf das Minimum beschränkt wurde und anschließend schrittweise erweitert wird. In dieser Arbeit wurde dagegen der umgekehrte Ansatz gewählt, wonach zunächst in einer breit angelegten Vorgehensweise mögliche Anforderungen an die Sicherungslogik erfasst wurden und anschließend ein generisches Konzept entwickelt wurde, um möglichst viele funktionale Anforderungen in einem schlanken generischen System abzubilden. Hierdurch wird das Risiko reduziert, dass das Grundkonzept später nicht mit allen Anforderungen kompatibel ist und deswegen abgelehnt wird.

Ausgehend von den Zieldimensionen Kapazitätssteigerung, Kosteneinsparung und Verbesserung der Robustheit des Bahnbetriebs sowie der angestrebten langen Nutzungszeit und der Notwendigkeit der schnellen Markteinführung mittels kurzer Projektierungs- und Zulassungszeiten wurden zunächst die Anforderungen für die neue Sicherungslogik „smartLogic“ hergeleitet. Neben diesen beeinflussbaren Anforderungen bestimmt die Aufrechterhaltung der erforderlichen Sicherheit als feste und grundlegende Kernanforderung an eine Sicherungslogik deren Funktionsweise.

Auf Basis der identifizierten Anforderungen wurde gemäß der Vorgehensweise im V-Modell zunächst das System sowie das Systemumfeld definiert und die Schnittstellen zu den Umsystemen festgelegt. Zur Herleitung der einzelnen betrieblich funktionalen Anforderungen und funktionalen Sicherheitsanforderungen im Arbeitsschritt der Funktionsanalyse wurde anschließend eine ausführliche Gefährdungsanalyse durchgeführt.

Daraus wurde ein ausführlicher Katalog mit betrieblichen Funktionen und Prüfbedingungen als funktionale Anforderungen an die smartLogic erstellt, der zur Erhöhung der Vollständigkeit um eine Auswertung aktueller Regelwerke und Lastenhefte der bisherigen technischen Umsetzungen von Sicherungslogiken in aktuellen Stellwerken ergänzt wurde. Der entstandene Funktionskatalog wurde anschließend kategorisiert und generalisiert. Zudem wurde für die Implementierung eine Priorisierung vorgenommen.

Die Funktionen des Funktionskatalogs wurden in Prozesse und untergeordnete Subroutinen unterteilt. Die Prozessfunktionen wurden wiederum in Prüfprozesse und Reaktionsprozesse unterteilt. Prüfprozesse prüfen Anfragen an die Logik, die in der Regel vom übergeordneten Traffic Management System an sie gestellt werden. Reaktionsprozesse beschreiben dagegen die durchzuführenden Aktionen nach Eintritt eines (unerwarteten) Ereignisses.

Im Hauptteil der Arbeit wurde zunächst ein Datenmodell für die Modellierung der smartLogic mittels UML-Klassendiagrammen modelliert, welches aus fünf Teilmodellen besteht. Dabei wurde auf eine

gute Kompatibilität zu bestehenden Modellen geachtet. Insbesondere basiert das topologische Modell auf dem Standard des Rail Topo Model der UIC.

Im achten Hauptkapitel wurde die Verhaltensmodellierung der smartLogic hergeleitet. Dabei wurden zunächst grundlegende konzeptionelle Fragestellungen des Designs der Logik diskutiert und jeweils anhand der Anforderungen an die Sicherungslogik eine geeignete Vorgehensweise ausgewählt und ausgearbeitet. Anschließend wurden die in der Funktionsanalyse im 6. Hauptkapitel identifizierten Basis-Prüfprozesse mit einem zu Beginn des 8. Hauptkapitels entwickelten Verfahrens mit fünf Schritten modelliert. Dabei erfolgte die Detailmodellierung mittels UML-Aktivitätsdiagrammen. Die Ergebnisse sind in die Implementierung eines Software-Demonstrators im Eisenbahnbetriebsfeld Darmstadt eingeflossen.

Zusammenfassung der Ergebnisse

Insgesamt wurden in der Arbeit neben einer ausführlichen Gefährdungsanalyse inkl. Auswertung von Unfallereignissen und einem umfangreichen und systematisch hergeleiteten Funktionskatalog mit funktionalen Anforderungen an eine moderne Sicherungslogik ein ausführliches Datenmodell für die smartLogic geschaffen. Im Rahmen der Verhaltensmodellierung wurden insgesamt vier Basis-Prüfprozesse und sieben grundlegende Subroutinen modelliert. Diese basieren auf ausführlichen Konzepten für die zentralen Design-Fragestellungen der Sicherungslogik wie Bewertungskriterium, Wahl der Zielpunkte für die Fahrerlaubnis, Flankenschutz und dem Umgang mit Rückfallebenen. Auch der Bereich der Rangierfahrten wurde insofern thematisiert, dass festgestellt wurde, dass eine gesonderte Berücksichtigung von Rangierfahrten mit einem eigenen Regelset nicht mehr gerechtfertigt erscheint.

Die detaillierte Modellierung der Reaktionsprozesse konnte aufgrund des zeitlichen Umfangs der Arbeit noch nicht durchgeführt werden. Sie bietet daher Potenzial für zukünftige Arbeiten. Dasselbe gilt für Übergangsbedingungen zu anderen Stellwerksbereichen, Bedienfunktionen und der Protokollierung.

Nutzen der Arbeit

Aufbau und qualitative Analyse der Funktionsweise der smartLogic lassen vermuten, dass durch die smartLogic deutliche Kapazitätsvorteile insbesondere bei Abweichungen vom Regelbetrieb oder sehr enger Zugfolge im Bereich von Knoten zu erwarten sind. Dadurch können auch die Pünktlichkeit erhöht bzw. Folgeverspätungen reduziert werden. Eine erste detaillierte eisenbahnbetriebswissenschaftliche Untersuchung wurde hierzu bereits in einer Masterarbeit am Institut für Bahnsysteme und Bahntechnik der TU Darmstadt anhand von Simulationen mit dem im Rahmen der Arbeit entstandenen Demonstrator durchgeführt [Merkel 2021].

Weiterhin bietet die smartLogic durch ihren generischen Aufbau deutliche Potenziale zur Einsparung von Planungs- und Zulassungsaufwand, wenn das Konzept einer sicheren Datenquelle realisiert werden kann. Hierdurch können ein beschleunigter Rollout sowie Kosteneinsparungen erreicht werden.

Um die Vorteile voll ausnutzen zu können müssen jedoch auch die Umsysteme weiterentwickelt werden. So ist eine Führerstandsignalisierung auf der überwiegenden Mehrheit der Fahrzeuge erforderlich, ebenso wie eine stabile und performante Kommunikationsverbindung zwischen den Fahrzeugbewegungen und der Infrastruktur. Auch ATO ab GoA 2 ist hilfreich, um vorgegebene Fahrkurven präzise abfahren zu können. Weiterhin wird eine hinreichend genaue Ortung benötigt, die jedoch nicht zwangsweise auf dem Fahrzeug angesiedelt sein muss, sondern aus verschiedenen Sensorsystemen bestehen kann. Aus diesem Grund wäre anzudenken, in ETCS eine Möglichkeit des

Positionsupdates von der Infrastrukturseite für den Zug vorzusehen, für den Fall, dass infrastrukturseitig die Fahrzeugposition genauer bestimmt wurde, als auf dem Fahrzeug, damit das Fahrzeug seine Bremskurven bestmöglich optimieren kann.

zentrale Erkenntnisse

Im Wesentlichen können aus der Arbeit die folgenden Erkenntnisse geschlussfolgert werden:

- Eine reine Implementierung von Technologien wie ETCS und digitale Stellwerke ohne die Anpassung der Sicherungslogik erzielt nicht die gewünschten Kapazitäts- und Kostensenkungseffekte.
- Im Bereich der Sicherungslogik besteht noch Optimierungspotenzial, insbesondere im Hinblick auf eine passgenauere Gestaltung und Auflösung von Durchrutschwegen. Dieses Optimierungspotenzial kann durch die smartLogic gehoben werden kann, wenn technologische Voraussetzungen in der Systemumgebung (wie geringe Latenzzeiten, eine präzise Ortung und möglichst genaues Abfahren von Fahr- und Bremskurven durch automatisiertes Fahren) realisiert sind.
- Fehleranfällige manuelle Rückfallebenen können stark reduziert werden, indem eine smarte Sicherungslogik eingeschränkte Fahrerlaubnisse mit einem hinreichenden Sicherheitslevel im regulären Betriebsmodus zulässt.
- Folgeverspätungen können reduziert werden, da die smartLogic eine flexiblere Zuweisung und Auflösung von Gleisressourcen als heutige Stellwerkslogiken zulässt.
- Eine generische Sicherungslogik wie die smartLogic kann den Zulassungs- und Projektierungsaufwand deutlich senken.
- Der bzgl. der Anforderungen breit beginnende und dann durch Integration der Anforderungen in generische Konzepte sich verschmälernde Ansatz aus dieser Dissertation bringt Vorteile bei der Migration in einer Landschaft bestehender Altsysteme mit sich.
- Die entwickelte Modellierungsmethode erlaubt eine schnelle Modellierung von Prüfprozessen für die Sicherungslogik.

Fazit und Ausblick

Aufgrund der geschilderten Ergebnisse darf gefolgert werden, dass für das Erreichen der eingangs geschilderten Ziele einer günstigeren Leit- und Sicherungstechnik im Rahmen des „digitalen Bahnbetriebs“ eine Überarbeitung der aktuellen Sicherungslogik in den Stellwerkskernen sinnvoll ist. Der Autor dieser Arbeit empfiehlt daher den zuständigen Stellen in die Entwicklung eines marktfähigen Produktes zügig einzusteigen. Hierfür kann die vorliegende Arbeit aus Sicht des Autors im Verbund mit bereits bekannten Ansätzen aus der Forschung und praktischen Entwicklung hilfreiche Impulse liefern.

Intentially blank

11 Literaturverzeichnis

Abrach et al. 2019 — Abrach, Ivo N.; Metz, Kurt; Schneider, Hans Jakob (2019): Smartrail 4.0: Sanft auf dem Weg zur Automation im Führerstand. In: *Signal+Draht* 111 (6/2019), S. 24–32.

Abts 2013 — Abts, Dietmar (2013): Grundkurs JAVA Von den Grundlagen bis zu Datenbank- und Netzanwendungen. 7., akt. Aufl. 2013. Wiesbaden: Springer. Online verfügbar unter http://gbv.eblib.com/patron/FullRecord.aspx?p=1156856.

AG CYSIS 2016 — Innovationsallianz zwischen TU Darmstadt und Deutsche Bahn, Arbeitsgruppe CYSIS (2016): Resiliente Architekturen in der Eisenbahn-Signaltechnik. Online verfügbar unter https://docplayer.org/47411253-Resiliente-architekturen-in-der-eisenbahn-signaltechnik-arbeitsgruppe-cysis.html, zuletzt geprüft am 26.06.2021.

AG CYSIS 2018 — Innovationsallianz zwischen TU Darmstadt und Deutsche Bahn, Arbeitsgruppe CYSIS (2018): Security for Safety –Anforderungen an eine digitalisierte Bahnwelt. Online verfügbar unter https://www.seceng.informatik.tu-darmstadt.de/media/seceng/ag_cysis/Whitepaper_Security_for_Safety.pdf, zuletzt geprüft am 26.06.2021.

Anzenhofer 2019 — Anzenhofer, Lena (2019): Schweizer Bahn wirbt deutsche Lokführer ab — und verärgert die Deutsche Bahn. In: *Business Insider*, 09.02.2019. Online verfügbar unter https://www.businessinsider.de/wirtschaft/schweizer-bahn-wirbt-deutsche-lokfuehrer-ab-und-veraergert-die-deutsche-bahn-2019-2/, zuletzt geprüft am 14.12.2019.

Authier & Etienne 2017 — Authier, Leonard; Etienne, David (2017): Safe Railway Operation With Minimal Requirements. Masterthesis an der ETH Zürich. Institut für Elektronik.

Bachurina 2018 — Bachurina, Daria (2018): Neue Generation der Bahnsicherungstechnik. Anforderungen und Technologie. Paper. In: Andreas Oetting (Hg.): Tagungsband des Scientific Railway Signalling Symposiums 2017. Die Steuerung des Eisenbahnbetriebs der Zukunft. Scientific Railway Signalling Symposium. Darmstadt, 19.04.2017. Technische Universität Darmstadt. Darmstadt: Universitäts- und Landesbibliothek Darmstadt.

Badke-Schaub et al. 2008 — Badke-Schaub, Petra; Hofinger, Gesine; Lauche, Kristina (2008): Human Factors Psychologie sicheren Handelns in Risikobranchen. Berlin, Heidelberg: Springer Medizin Verlag Heidelberg. Online verfügbar unter http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10245937.

Balzert & Liggesmeyer 2011 — Balzert, Helmut; Liggesmeyer, Peter (2011): Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb. 3. Aufl. Heidelberg: Spektrum Akademischer Verlag (Lehrbücher der

Informatik). Online verfügbar unter http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10494391.

Balzert 2009 — Balzert, Helmut (2009): Lehrbuch der Softwaretechnik Basiskonzepte und Requirements-Engineering. 3. Aufl. Heidelberg: Spektrum Akad. Verl. (Lehrbücher der Informatik).

Bertagnolli 2018 — Bertagnolli, Frank (2018): Lean Management Einführung und Vertiefung in die japanische Management-Philosophie. 1. Auflage. Wiesbaden: Springer Fachmedien.

BEU 2019 — Bundesstelle für Eisenbahnunfalluntersuchung (2019): Unfalluntersuchungsberichte. Auswertung zum Stichtag 23.10.2017. Online verfügbar unter https://www.eisenbahn-unfalluntersuchung.de/EUB/DE/Publikationen/publikationen_node.html , zuletzt geprüft am 30.12.2019.

Beyer et al. 2019 — Beyer, Martin; Jurtz, Steffen; Langhof, Michael; Reinhart, Peter; Vogel, Thomas (2019): ETCS als Trägersystem zur Leistungssteigerung bei der S-Bahn Stuttgart. In: *Signal+Draht* 111 (6/2019), S. 6–16.

BfGA 2020 — Beratungsgesellschaft für Arbeits- und Gesundheitsschutz mbH (BfGA): Definition Gefährdung. Online verfügbar unter https://www.bfga.de/arbeitsschutz-lexikon-von-a-bis-z/fachbegriffe-c-i/gefaehrdung-fachbegriff/, zuletzt geprüft am 03.06.2020.

BG RCI 2017 — Berufsgenossenschaft Rohstoffe und chemische Industrie (Hg.) (2017): Merkblatt A 017 "Gefährdungsbeurteilung -Gefährdungskatalog". Online verfügbar unter https://www.baua.de/SharedDocs/Handlungshilfen/DE/Gefaehrdungsbeurteilung/BG-RCI-Schaedel/Merkblatt-A-017-Gefaehrdungsbeurteilung-Gefaehrdungskatalog.html, zuletzt geprüft am 30.12.2019.

BMVI 2017 — Bundesministerium für Verkehr und digitale Infrastruktur (05.10.2017): Zulassung einer Ausnahme von §40 Abs. 2 Nr. 1 EBO für die Strecke 5919 im Abschnitt Ebensfeld - Erfurt.

BMVI 2017b — Bundesministerium für Verkehr und digitale Infrastruktur (2017): Nationaler Umsetzungsplan ETCS. Version 1.11.

Bosse 2010 — Bosse, Gunnar (2010): Grundlagen für ein generisches Referenzsystem für die Betriebsverfahren spurgeführter Verkehrssysteme. Dissertation an der Technischen Universität Braunschweig.

Braband 2013 — Braband, Jens (2013): Funktionale Sicherheit. In: Lothar Fendrich und Wolfgang Fengler (Hg.): Handbuch Eisenbahninfrastruktur. 2., neu bearbeitete Auflage. Berlin, Heidelberg: Springer Vieweg, S. 553–606.

Brand & Nänni 2019 — Brand, Alex E.; Nänni, Christian (2019): Bahn- und Fahrgastkommunikation: von 2G/GSM-R zu 5G/FRMCS aus SBB-Perspektive. In: *Signal+Draht* 111 (7+8/2019), S. 6–15.

Buder & Oelschläger 2014a — Buder, Jens; Oelschläger, Sven (2014): Veränderter ESTW-Planungsprozess mit "PlanPro" (Teil 2). In: *EI - Der Eisenbahningenieur* (12/2014), S. 36–39.

Buder & Oelschläger 2014b — Buder, Jens; Oelschläger, Sven (2014): Veränderter ESTW-Planungsprozess mit "PlanPro" (Teil 1). In: *EI - Der Eisenbahningenieur* (11/2014), S. 48–51.

Bührsch & Schlichting 2018 — Bührsch, Philipp; Schlichting, Jörn (2018) Zukunft Bahn: ETCS und digitale Stellwerke. In: *Eisenbahn Ingenieur Kompendium (EIK)*, S. 210–219.

Bührsch et al. 2022 — Bührsch, Philipp; Büker, Thorsten; Schotten, Simon; Hardel, Sascha (2022): Vorteile und Nutzen von ETCS L2oS und DSTW im Schienenverkehr. In: *Eisenbahn Ingenieur Kompendium (EIK)*, S. 223–238.

Büker 2017 — Büker, Thorsten (2017): ETCS Level 1 LS (ESG) unter dem Aspekt der Leistungsfähigkeit. In: *Eisenbahntechnische Rundschau ETR* (11/2017), S. 24–31.

Büker et al. 2019 — Büker, Thorsten; Graffagnino, Thomas; Hennig, Eike; Kuckelberg, Alexander (2019): Enhancement of Blocking-time Theory to Represent Future Interlocking Architectures. In: Proceedings of the 8th International Conference on Railway Operations Modelling and Analysis (RailNorrköping 2019). 8th International Conference on Railway Operations Modelling and Analysis (RailNorrköping 2019). Norrköping, Sweden. IAROR - International Association of Railway Operations Research.

Büker et al. 2020 — Büker, Thorsten; Hennig, Eike; Schotten, Simon (2020): Kapazitätsberechnung im Moving Block - die Tücke im Detail. In: *Eisenbahntechnische Rundschau ETR* (7+8), S. 32–37.

Buseyne 2017 — Buseyne, Emmanuel (2017): Final Report Summary - INESS (INtegrated EuropeanSignalling System) an der Europäische Kommission. Online verfügbar unter file:///C:/Users/DUEPME~1/AppData/Local/Temp/CORDIS_project_218575_en.pdf, zuletzt geprüft am 21.06.2021.

BVU 2014 — BVU Beratergruppe Verkehr+Umwelt GmbH; TNS Infratest (2014): Entwicklung eines Modells zur Berechnung von modalen Verlagerungen im Güterverkehr für die Ableitung konsistenter Bewertungsansätze für die Bundesverkehrswegeplanung. Vorläufiger Endbericht.

Cui et al. 2017 — Cui, Yong; Martin, Ullrich; Liang, Jiajian (2017): Decentralised, Autonomous Train Dispatching using Swarm Intelligence in Railway Operations and Control. In: RailLille-International Conference on Railway Operations Modelling and Analysis. RailLille-International Conference on Railway Operations Modelling and Analysis. Lille. International Association of Railway Operations Research.

DB AG 2018	Deutsche Bahn AG (25.01.2018a): „Digitale Schiene Deutschland“ bringt mehr Leistung und Qualität auf die Gleise. Berlin. Online verfügbar unter www.deutschebahn.com, zuletzt geprüft am 20.02.2018.
DB AG 2018b	Deutsche Bahn AG (2018): Themendienst Digitale Schiene Deutschland: Revolution für den Bahnbetrieb. Berlin. Online verfügbar unter https://www.deutschebahn.com/de/presse/suche_Medienpakete/medienpaket_digitale_schiene_deutschland-1177310, zuletzt geprüft am 26.03.2019.
DB Netz AG 2001	DB Netz AG (2001): Lastenheft für das Elektronische Stellwerk (ESTW) - Funktionsbedingungen der Stellwerkslogik und der in das ESTW integrierten Techniken - Teilheft F1 Grundausbau (GRU). München, Frankfurt am Main, zuletzt geprüft am 03.04.2017.
DB Netz AG 2013	DB Netz AG (2013): Geschäftliche Anwendungsfälle für die Leitung und Sicherung des Bahnbetriebs (Projekt NeuPro). Version 1.0.0. Unter Mitarbeit von Thomas Henning und Dietmar Homeyer. Frankfurt am Main, zuletzt geprüft am 08.04.2016.
DB Netz AG 2014	DB Netz AG (2014): Risikoanalyse zu ETCS, Gefährdungsidentifikation. v. 5.5. München.
DB Netz AG 2015	DB Netz AG (2015): PlanPro - Ein Werkzeug um die Datenprojektierung der LST zu rationalisieren. DB Netz AG, I. NPS 3. Zürich, 12.06.2015.
DB Netz AG 2016	DB Netz AG (2016): Lastenheft BTSF3 Betrieblich-technische Systemfunktionen für ETCS SRS Baseline 3. Version 2.1. Unter Mitarbeit von Jürgen Haas. München.
DB Netz AG 2017a	DB Netz AG (10.12.2017): Fahrdienstvorschrift Ril 408, vom 10.12.2017.
DB Netz AG 2017b	DB Netz AG (2017): Systemdefinition ESTW-NeuPro. Version 4.0. Unter Mitarbeit von Stephan Wallasch. Frankfurt am Main.
Deutsche Bahn AG 2019	Deutsche Bahn AG (10/2019): Themendienst: Vom Stellhebel zum Mausklick: Wie die Bahn in ihrem Schienennetz täglich 40.000 Züge lenkt. Berlin. Online verfügbar unter https://digitale-schiene-deutschland.de/Downloads/Themendienst-Warnemuende-Vom%20Stellhebel%20zum%20Mausklick.pdf, zuletzt geprüft am 18.06.2021.
DIN EN 50126-1:2017	DIN EN 50126-1:2017, Oktober 2018: Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS).
DIN EN 50128:2011	DIN EN 50128:2011, März 2012: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme.
DIN EN 50129:2018	DIN EN 50129:2018 + AC:2019, Juni 2019: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme.

Drescher et al. 2017	Drescher, Andreas; Koschmider, Agnes; Oberweis, Andreas (Hg.) (2017): Modellierung und Analyse von Geschäftsprozessen: De Gruyter Oldenbourg.
Düpmeier & Oetting 2018	Düpmeier, Frederik; Oetting, Andreas (2018): Funktionsumfang einer Sicherungslogik zur effizienten Ausnutzung der Möglichkeiten von ETCS. In: Jörn Schönberger und Susanne Nerlich (Hg.): Tagungsband der 26. Verkehrswissenschaftliche Tage der TU Dresden. Grenzenlos(er) Verkehr?! 26. Verkehrswissenschaftliche Tage. Dresden, 14.03.-15.03.2018, S. 123–128.
Düpmeier 2018	Düpmeier, Frederik (2018): Entwurf einer neuen, regelbasierten Sicherungslogik unter Annahme der vollständigen Ortung aller Schienenfahrzeuge. In: Andreas Oetting (Hg.): Tagungsband des Scientific Railway Signalling Symposiums 2017. Die Steuerung des Eisenbahnbetriebs der Zukunft. Scientific Railway Signalling Symposium. Darmstadt, 19.04.2017. Technische Universität Darmstadt. Darmstadt: Universitäts- und Landesbibliothek Darmstadt, S. 36–45. Online verfügbar unter https://tuprints.ulb.tu-darmstadt.de/7403/7/SRSS_2017_Tagungsband_final2_korrigiert.pdf, zuletzt geprüft am 16.10.2019.
Düpmeier 2020	Düpmeier, Frederik (2020): Modellierung generischer sicherungstechnischer Prüfprozesse unter Ausnutzung aktueller Informationen zum Betriebsgeschehen. In: Andreas Oetting (Hg.): Scientific Railway Signalling Symposium 2019: Mehr Verkehr auf die Schiene durch Digitalisierung?! – Was kann die Leit- und Sicherungstechnik dazu beitragen? Tagungsband. Unter Mitarbeit von Miroslav Pejic. Scientific Railway Signalling Symposium. Darmstadt, 26.06.2019. Technische Universität Darmstadt: UNSPECIFIED, S. 5–24.
Düpmeier 2021	Düpmeier, Frederik (2021): Capacity benefits of dynamic route assignment in nodes – a qualitative analysis. In: Proceedings of RailBeijing. International Conference on Railway Operations Modelling and Analysis (RailBeijing). Beijing. International Association of Railway Operations Research.
EBO:2019-04-05	Bundesminister für Verkehr: Eisenbahn-Bau- und Betriebsordnung EBO, vom 05.04.2019. Fundstelle: www.gesetze-im-internet.de.
Eigner et al. 2014	Eigner, Martin; Roubanov, Daniil; Zafirov, Radoslav (2014): Modellbasierte virtuelle Produktentwicklung. Berlin: Springer Vieweg.
ERA 2015	European Railway Agency (2015): ERTMS Longer Term Perspective. Final Report. Brüssel. Online verfügbar unter https://www.era.europa.eu/sites/default/files/library/docs/ex_post_evaluation/era_rep_150_ertms_longer_term_perspective_report_en.pdf, zuletzt geprüft am 16.12.2019.
ERA 2016	European Railway Agency (2016): ERTMS / ETCS Subset-026 System Requirement Specification v. 3.6.0 ETCS Subset-026 v. 3.6.0, vom 13.05.2016.

ERTMS Users Group & EULYNX 2020a ERTMS Users Group; EULYNX (2020): RCA Domain Knowledge. Version 0.2 (0.A).

ERTMS Users Group & EULYNX 2020b ERTMS Users Group; EULYNX (2020): RCA System Architecture. Version 0.2 (0.A).

ERTMS Users Group & EULYNX 2020c ERTMS Users Group; EULYNX (2020): RCA Logical Architecture Overview. RCA Baseline set 0 Release 1, Version 0.2 (0.A).

Eschbach et al. 2017 Eschbach, Robert; Freissler, Thomas; Hofbauer, Tobias; Laub, Harald (2017): Smart Engineering - Effiziente Softwareentwicklung in der Bahntechnik. In: *ZEVrail* 141 (12/2017), S. 444–451.

EUB 2009 Eisenbahn-Unfalluntersuchungsstelle des Bundes (EUB) (10.11.2009): Allgemeinverfügung zum Melden von gefährlichen Ereignissen im Eisenbahnbetrieb.

EUB 2011 Eisenbahn-Unfalluntersuchungsstelle des Bundes (EUB) (2011): Untersuchungsbericht Zugkollision Überleitstelle Hordorf / Strecke Magdeburg Hbf - Halberstadt am 29.01.2011. Bonn.

EUG & EULYNX 2018 ERTMS Users Group; EULYNX (2018): White Paper Reference CCS Architecture based on ERTMS. 18C044-0C. Brüssel. Online verfügbar unter https://eulynx.eu/index.php/documents2/press-releases/194-18c044-1-white-paper-reference-ccs-architecture-final, zuletzt geprüft am 12.09.2019.

EUG & EULYNX 2019 ERTMS Users Group; EULYNX (2019): RCA- Architecture Overview. v. Beta 1. Brüssel, zuletzt geprüft am 17.09.2019.

EULYNX Initiative 2020a EULYNX Initiative (2020): Interface specification SCI Generic. Document number: Eu.Doc.93, Baseline: 2.3 (1.A), EULYNX Baseline Set: 3.

EULYNX Initiative 2020b EULYNX Initiative (2020): Interface specification SCI-P. Document number: Eu.Doc.38, Baseline: 3.1 (1.A), EULYNX Baseline Set: 3.

Europäische Kommission 2016 Europäische Kommission (27.05.2016): Verordnung (EU) 2016/919 der Kommission vom 27. Mai 2016 über die technische Spezifikation für die Interoperabilität der Teilsysteme „Zugsteuerung, Zugsicherung und Signalgebung“ des Eisenbahnsystems in der Europäischen Union C/2016/3044. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0919, zuletzt geprüft am 08.06.2021.

Europäische Kommission 2021 Europäische Kommission (2021): Eurointerlocking. Online verfügbar unter https://trimis.ec.europa.eu/project/ertms-eurointerlocking, zuletzt aktualisiert am 20.06.2021, zuletzt geprüft am 21.06.2021.

Fantechi et al. 2016 Fantechi, A.; Gnesi, S.; Haxthausen, A.; van de Pol, J.; Roveri, M.; Treharne, H. (2016): SaRDIn - A Safe Reconfigurable Distributed Interlocking. Paper. In: World Congress on Railway Research 2016. WCRR World Congress on Railway Research. Mailand, 29.05.-02.06.2019. WCRR.

Fehlauer & Kahl 2019 — Fehlauer, Lars; Kahl, Richard (2019): Einfluss der ETCS-Bremskurven auf die Infrastrukturplanung. In: *EI - Der Eisenbahningenieur* (8), S. 34–37.

Feltz et al. 2017 — Feltz, André; Nießen, Nils; Walke, Tobias; Jacobs, Jürgen (2017): Analyse und Optimierung von ETCS-Parametern im Luxemburger Eisenbahnnetz. In: *Signal+Draht* 109 (3/2017), S. 6–17.

Flamm & Scheier 2019 — Flamm, Leander; Scheier, Benedikt (2019): Integrierte Bewertung von Steuerungssystemen auf dem Weg zum automatisierten Bahnbetrieb. In: *Signal+Draht* 111 (6/2019), S. 33–40.

Flamm et al. 2019 — Flamm, Leander; Meirich, Christian; Jäger, Bärbel (2019): Die Umsetzung des automatisierten Bahnbetriebs zwischen Technik, Regelwerken und Wirtschaftlichkeit. In: *Eisenbahntechnische Rundschau ETR* (03), S. 27–31.

Gadatsch 2017 — Gadatsch, Andreas (2017): Datenmodellierung für Einsteiger Einführung in die Entity-Relationship-Modellierung und das Relationenmodell. Wiesbaden: Springer Fachmedien Wiesbaden (essentials). Online verfügbar unter https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=4926940.

Gadatsch 2019 — Gadatsch, Andreas (2019): Datenmodellierung Einführung in die Entity-Relationship-Modellierung und das Relationenmodell. 2., aktualisierte Auflage (essentials).

Gély et al. 2010 — Gély, L.; Dessagne, G.; Pesneau, P.; Vanderbeck, F. (2010): A multi scalable model based on a connexity graph representation. In: WIT Transactions on The Built Environment, Bd. 114. Transactions on The Built Environment. WIT Press, S. 193–204. Online verfügbar unter http://www.witpress.com/elibrary/wit-transactions-on-the-built-environment/114/21421, zuletzt geprüft am 29.01.2016.

Goers et al. 2019 — Goers, Hannes; Reinhart, Peter; Weiß, Rüdiger (2019): Knoten Stuttgart - ETCS als Träger für Leistungs- und Qualitätssteierungen an der DB Netz AG, DB Projekt Stuttgart-Ulm GmbH. Berlin, Karlsruhe, Stuttgart.

Grau 2018 — Grau, Felix Johannes (2018): Entwicklung konkreter Testfälle auf einer geeigneten Eisenbahninfrastruktur für das Testen einer formalisierten Eisenbahnsicherungslogik. Masterarbeit an der Technischen Universität Darmstadt. Institut für Bahnsysteme und Bahntechnik.

Guss 2016 — Guss, Martin (2016): Das Verschwinden des Stellwerks. In: *Signal+Draht* 108 (9/2016), S. 59–66.

Hametner & Sünder 2017 — Hametner, Reinhard; Sünder, Christoph (2017): Der agile Wasserfall - ein Sturm im Wasserglas (EN 50128). In: *Signal+Draht* 109 (11/2017), S. 41–50.

Hennig et al. 2021 — Hennig, Eike; van Hövell, Madeleine; Büker, Kerstin (2021): Diskussion zu ausgewählten Aspekten von ETCS Hybrid Level 3. In: *Eisenbahntechnische Rundschau ETR* (6), S. 44–49.

Höppner 2015 — Höppner, Silko (2015): Generische Beschreibung von Eisenbahnbetriebsprozessen. Dissertation an der ETH Zürich.

IHK 2015 — Industrie- und Handelskammer Nürnberg für Mittelfranken: Umweltverschmutzung. In: Lexikon der Nachhaltigkeit. Online verfügbar unter https://www.nachhaltigkeit.info/artikel/umweltverschmutzung_1759.htm, zuletzt geprüft am 07.01.2020.

IRS 30100 — IRS 30100:2016, September 2016: IRS 30100 - RailTopoModel - Railway infrastructure topological model, zuletzt geprüft am 22.11.2016.

Kaffenberger 2013 — Kaffenberger, Rüdiger (2013): Prozesse und Methoden - von was reden wir denn gerade? Online verfügbar unter https://www.softwareinmotion.de/news/prozesse_und_methoden, zuletzt aktualisiert am 07.05.2013, zuletzt geprüft am 03.10.2021.

Kahlbrandt 1998 — Kahlbrandt, Bernd (1998): Verhaltensmodellierung. In: Bernd Kahlbrandt (Hg.): Software Engineering. Objektorientierte Software-Entwicklung mit der Unified Modeling Language. Berlin, Heidelberg, s.l.: Springer Berlin Heidelberg, S. 162–185.

Kamiske 2015a — Kamiske, Gerd F. (Hg.) (2015): Handbuch QM-Methoden. 3., aktualisierte und erweiterte Auflage. München: Carl Hanser Verlag GmbH & Co. KG.

Kamiske 2015b — Kamiske, Gerd F. (2015): Stakeholder-Analyse. In: Gerd F. Kamiske (Hg.): Handbuch QM-Methoden. 3., aktualisierte und erweiterte Auflage. München: Carl Hanser Verlag GmbH & Co. KG, S. 907–909.

Kleuker 2013 — Kleuker, Stephan (2013): Grundkurs Datenbankentwicklung. Wiesbaden: Springer Fachmedien Wiesbaden.

Kleuker 2018 — Kleuker, Stephan (2018): Grundkurs Software-Engineering mit UML Der pragmatische Weg zu erfolgreichen Softwareprojekten. 4. Auflage. Wiesbaden: Springer Fachmedien.

Klöters & Herten 2017 — Klöters, Georg; Herten, Ulrich (2017): Schnittstellen in der LST zur Abwehr negativer Auswirkungen von Obsoleszenz. In: *Signal+Draht* 109 (11/2017), S. 26–33.

Krauß et al. 2020 — Krauß, Christoph; Zhdanova, Mario; Eckel, Michael; Katzenbeisser, Stefan; Heinrich, Markus; Kuzhiyelil, Don; Cosic, Jasmin (2020): Projekt HASELNUSS - IT-Sicherheitsarchitektur für die nächste Generation der Leit- und Sicherheitstechnik. In: *Deine Bahn* (12), S. 57–61.

Kümmling & Wanstrath 2021 — Kümmling, Michael; Wanstrath, Sven (2021): Maximierung der Fahrwegkapazität mit Digitaler Leit- und Sicherungstechnik. In: *Eisenbahntechnische Rundschau ETR* (7+8), S. 16–21.

Kuster et al. 2019 — Kuster, Jürg; Bachmann, Christian; Huber, Eugen (2019): Handbuch Projektmanagement Agil - klassisch - hybrid. 4., vollständig überarbeitete und erweiterte Auflage. Berlin: Springer Gabler.

Kuttig-Trölenberg et al. 2021 Kuttig-Trölenberg, Markus; Schurig, Jörg; Koch, Raimo (2021): Die Zukunft mit ETCS Level 3 Hybrid. In: *Signal+Draht* 113 (7+8/2021), S. 39–45.

Leining & Elsweiler 2013 Leining, Michael; Elsweiler, Bernd (2013): Standardisierung in der Leit- und Sicherungstechnik. In: *Deine Bahn* (1/2013), S. 11–15.

Lindner & Becker 2015 Lindner, Alexandra; Becker, Peter (2015): Wertstromdesign. In: Gerd F. Kamiske (Hg.): Handbuch QM-Methoden. 3., aktualisierte und erweiterte Auflage. München: Carl Hanser Verlag GmbH & Co. KG, S. 293–340.

Maschek 2001 Maschek, Ulrich (2001): Datenmodell zur Planung von Stellwerken. Dissertation an der Technischen Universität Braunschweig.

Maschek 2009 Maschek, Ulrich (2009): Eine generische Sicht auf die Betriebssicherheit im spurgeführten Verkehr. In: *EI - Der Eisenbahningenieur* 60 (2/2009), S. 36–40.

Maschek 2013 Maschek, Ulrich (2013): Sicherung des Schienenverkehrs - Grundlagen und Planung der Leit- und Sicherungstechnik. 2. Aufl. Wiesbaden: Springer Vieweg.

Maschek 2017 Maschek, Ulrich (2017): Neue Ausgabeformate für LST-Planung. In: *EI - Der Eisenbahningenieur* (1/2017), S. 18–20.

Maschek 2018 Maschek, Ulrich (2018): Sicherung des Schienenverkehrs Grundlagen und Planung der Leit- und Sicherungstechnik. 4. überarbeitete und erweiterte Auflage. Wiesbaden: Springer Vieweg.

McKinsey & Company 2018 McKinsey & Company (2018): Machbarkeitsstudie zum Rollout von ETCS/DSTW Zusammenfassung der Ergebnisse. Online verfügbar unter https://www.bmvi.de/SharedDocs/DE/Anlage/E/machbarkeitsstudie-digitalisierung-schiene.pdf?__blob=publicationFile, zuletzt geprüft am 19.06.2021.

Menzel 2019 Menzel, Daria (2019): Generisches Konzept zur Fahrzeugbewegungssicherung. In: *Signal+Draht* 111 (10/2019), S. 6–15.

Menzel et al. 2020 Menzel, Daria; Sommer, Martin; Trinckauf, Jochen (2020): Neue Sekundärbahn - innovative Fahrzeugbewegungssicherung. In: *Signal+Draht* 112 (11/2020), S. 6–11.

Merkel 2021 Merkel, Diego (2021): Auswirkungen einer regelbasierten Sicherungslogik auf die Kapazität von ausgewählten Eisenbahnbetriebssituationen. Masterarbeit an der Technischen Universität Darmstadt.

Meyer zu Hörste 2003 Meyer zu Hörste, Michael (2003): Methodische Analyse und generische Modellierung von Eisenbahnleit- und -sicherungssystemen. Dissertation an der Technischen Universität Braunschweig.

Nüttgens & Rump 2002 Nüttgens, Markus; Rump, Frank J. (2002): Syntax und Semantik Ereignisgesteuerter Prozessketten (EPK). In: J. Desel und M. Weske (Hg.): Promise 2002 - Prozessorientierte Methoden und Werkzeuge für

die Entwicklung von Informationssystemen, Proceedings des GI-Workshops und Fachgruppentreffens. Potsdam. Bonn (LNI, P-21), S. 64–77.

Oetting & Keck 2015 — Oetting, Andreas; Keck, Anna-Katharina (2015): Monetarization of Delay Valuation for Freight. In: I. A. Hansen, N. Tomii und C. Hirai (Hg.): 6th International Conference on Railway Operations Modelling and Analysis. RailTokyo2015. Tsudanuma Campus, Chiba Institute of Technology, Narashino, Japan, 26.03.2015. International Association of Railway Operations Research, 92ff.

OMG 2017 — Object Management Group (OMG) (2017): OMG Unified Modeling Language (OMG UML). Version 2.5.1. Online verfügbar unter https://www.omg.org/spec/UML/2.5.1/PDF, zuletzt geprüft am 09.02.2021.

OMG 2019 — The Object Management Group (Hg.) (2019): What is SysML? Online verfügbar unter http://www.omgsysml.org/what-is-sysml.htm, zuletzt geprüft am 04.04.2019.

Pachl 2016 — Pachl, Jörn (2016): Besonderheiten ausländischer Eisenbahnbetriebsverfahren - Grundbegriffe, Stellwerksfunktionen, Signalbegriffe. Wiesbaden: Springer Vieweg (essentials).

Pachl 2020 — Pachl, Jörn (2020): Railway Signalling Principles. Unter Mitarbeit von Universitätsbibliothek Braunschweig: Universitätsbibliothek Braunschweig.

Pachl 2021 — Pachl, Jörn (2021): Glossar der Systemtechnik des Schienenverkehrs, zuletzt aktualisiert am 22.02.2021, zuletzt geprüft am 17.01.2022.

Papula — Papula, Lothar (1997): „Fehlerarten“ (systematische und zufällige Meßabweichungen). Aufgaben der Fehler- und Ausgleichsrechnung. In: Lothar Papula (Hg.): Mathematik für Ingenieure und Naturwissenschaftler. Vektoranalysis, Wahrscheinlichkeitsrechnung, Mathematische Statistik, Fehler- und Ausgleichsrechnung. 2., verbesserte Auflage. Wiesbaden, s.l.: Vieweg+Teubner Verlag (Viewegs Fachbücher der Technik), S. 645–648.

Pohl & Rupp 2015 — Pohl, Klaus; Rupp, Chris (2015): Basiswissen Requirements Engineering - Aus- und Weiterbildung nach IREB-Standard zum Certified Professional for Requirements Engineering: foundation level nach IREB-Standard. 4., überarbeitete Auflage. Heidelberg: dpunkt. Online verfügbar unter https://ebookcentral.proquest.com/lib/subhh/detail.action?docID=2029882.

Priese & Wimmel 2008 — Priese, Lutz; Wimmel, Harro (2008): Petri-Netze. 2. Auflage. Berlin, Heidelberg: Springer (eXamen.press). Online verfügbar unter http://digitale-objekte.hbz-nrw.de/webclient/DeliveryManager?pid=2346550&custom_att_2=simple_viewer.

Radtke 2014 — Radtke, Alfons (2014): Infrastructure Modelling. In: Ingo A. Hansen (Hg.): Railway timetabling & operations. Analysis, modelling, optimisation, simulation, performance evaluation. 2. rev. and extended ed. Hamburg: Eurailpress in DVV Media Group, S. 47–63.

Rau 2015 — Rau, Matthias (2015): 7 W-Fragen. In: Gerd F. Kamiske (Hg.): Handbuch QM-Methoden. 3., aktualisierte und erweiterte Auflage. München: Carl Hanser Verlag GmbH & Co. KG, S. 719–721.

Rupp 2007 — Rupp, Chris (2007): Requirements-Engineering und -Management Professionelle, iterative Anforderungsanalyse für die Praxis. 4., aktualisierte und erw. Aufl. München: Hanser. Online verfügbar unter http://deposit.d-nb.de/cgi-bin/dokserv?id=2850705&prov=M&dok_var=1&dok_ext=htm.

SBB AG 2018 — SBB AG (2018): General Concept ETCS Interlocking. rev. 141167. Bern, zuletzt geprüft am 20.09.2019.

SBB AG 2020 — SBB AG (2020): APS Core Functional Behaviour. erschienen im Rahmen von smartRail 4.0. Bern.

Schlick et al. 2018 — Schlick, Christopher; Bruder, Ralph; Luczak, Holger (2018): Arbeitswissenschaft. 4. Auflage. Berlin: Springer Vieweg. Online verfügbar unter http://dx.doi.org/10.1007/978-3-662-56037-2.

Schmidt & Grabowski 2018 — Schmidt, Steffen; Grabowski, David (2018): Das "ETCS-Stellwerk". In: *Signal+Draht* 110 (10/2018), S. 29–39.

Schmidt 2019 — Schmidt, Steffen (2019): APS - Advanced Protection System, die günstige Einführung von ETCS Level 2/3. In: *Signal+Draht* 111 (10/2019), S. 22–31.

Schnieder 2021 — Schnieder, Lars (2021): European Train Control System (ETCS) Einführung in das einheitliche europäische Zugbeeinflussungssystem. 2nd ed. 2021. Berlin, Heidelberg: Springer Vieweg.

Schubert et al. 2016 — Schubert, Andreas; Rahmig, Christian; Scholz, Michael; Böhm, Thomas (2016): Zentralisiertes Management von Geodaten im Schienenverkehr. In: *Signal+Draht* 108 (12/2016), S. 6–14.

Sezgün 2017 — Sezgün, Sedat (2017): Schlanke Sicherheitstechnik für dezentrale Stellwerks- und Signalanlagen. In: *ZEVrail* (141), S. 134–139.

Siebert et al. 2015 — Siebert, Gunnar; Kempf, Stefan; Maßalski, Oliver (2015): Benchmarking. In: Gerd F. Kamiske (Hg.): Handbuch QM-Methoden. 3., aktualisierte und erweiterte Auflage. München: Carl Hanser Verlag GmbH & Co. KG, S. 911–942.

Simsion 2007 — Simsion, Graeme C. (2007): Data modeling Theory and practice. Bradley Beach, NJ: Technics Publications. Online verfügbar unter http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1005029.

Skowron 2020 — Skowron, Frank (2020): Concept: APS and ATO topology. v. vom 03.06.2020. Unter Mitarbeit von Maria Bertram. Berlin.

smartRail 4.0 2018	smartRail 4.0 (2018): Background information on Automatic Train Operation (ATO)and Grades of Automation (GoA) for smartrail 4.0. Online verfügbar unter https://www.smartrail40.ch/download/ATOBasisEN.pdf, zuletzt geprüft am 18.06.2021.
Staffel 2020	Staffel, Alexander (2020): Ausweitung der Nutzung des Überhöhungsfehlbetrags von 150 mm. In: *EI - Der Eisenbahningenieur* (6), S. 55–59.
Stanley 2011	Stanley, Peter (Hg.) (2011): ETCS for engineers. 1. ed. Hamburg: Eurailpress.
Stoll et al. 2019	Stoll, Fabian; Nießen, Nils; Nelles, Jochen; Brandl, Christopher; Mertens. Alexander; Nitsch, Verena (2019): Auswirkungen der Digitalisierung auf den Eisenbahnbetrieb - Ableitung möglicher Veränderungen für den Triebfahrzeugführer. Unter Mitarbeit von Marcus Daniel und Meike Holtkämper. Hg. v. Eisenbahn-Bundesamt. Bonn.
Theeg et al. 2020	Theeg, Gregor; Vlasenko, Sergej; Anders, Enrico; Arndt, Jelena; Berndt, Thomas; Braband, Jens (2020): Railway signalling and interlocking International compendium. 3rd edition. Leverkusen: PMC Media House GmbH (Edition Eurail press).
Trinckauf 2013	Trinckauf, Jochen (2013): Visionen und Aussichten in der Bahnsicherungstechnik. In: *Deine Bahn* (1/2013), S. 7–10.
Trinckauf et al. 2020	Trinckauf, Jochen; Maschek, Ulrich; Kahl, Richard; Krahl, Claudia (2020): ETCS in Deutschland. 1. Auflage. Leverkusen: PMC (Edition Eurailpress).
UIC 2013	International Union of Railways (UIC) (2013): Ursachenbaum der UIC-Sicherheitsdatenbank. Paris.
UIC 2017	International Union of Railways (UIC) (2017): UIC Safety Report 2017 Significant Accidents occured in Europe during the year 2016. Public Report. Paris.
Ullenboom 2012	Ullenboom, Christian (2012): Java ist auch eine Insel. 10., aktualisierte und überarbeitete Auflage, 1. Nachdruck. Bonn: Galileo Press (Galileo computing). Online verfügbar unter http://www.tutego.de/javabuch/Java-ist-auch-eine-Insel/10/javainsel_05_013.html#dodtp1beab676-fa68-4036-9fa0-ac41e5fd5907, zuletzt geprüft am 29.09.2020.
Unife 2021	Unife (2021): www.ertms.net, zuletzt geprüft am 08.06.2021.
Üyümez 2019	Üyümez, Bilal (2019): Potenziale einer Mensch-Maschine Kooperation bei Störungen im automatisierten Betrieb. In: *Eisenbahntechnische Rundschau ETR* (10), S. 18–24.
VDV 2018	Verband Deutscher Verkehrsunternehmen e. V. (VDV) (2018): Modernisierung desdeutschenEisen-bahnnetzes durch Digitalisierung und ETCS-Ausrüstung. Positionspapier. Köln. Online verfügbar unter

https://www.vdv.de/vdv-positionspapier-etcs.pdfx, zuletzt geprüft am 14.12.2019.

Verkehrsrundschau 2019 — Verkehrsrundschau (2019): Der Bahn fehlen für Infrastrukturausbau die Ingenieure. In: *www.verkehrsrundschau.de*, 27.09.2019. Online verfügbar unter https://www.verkehrsrundschau.de/nachrichten/der-bahn-fehlen-fuer-infrastrukturausbau-die-ingenieure-2466670.html, zuletzt geprüft am 14.12.2019.

Wang & Roush 2000 — Wang, John X.; Roush, Marvin L. (2000): What every engineer should know about risk engineering and management. New York: Marcel Dekker Inc.

Wehr 2017 — Wehr, Hans (2017): Entwicklung der Sicherheitsaspekte bei der Planung von Hochleistungsstrecken. In: *Eisenbahntechnische Rundschau ETR* (3/2017), S. 60–63.

Widmann 2022 — Widmann, Reiner (2022): Wie funktioniert eigentlich…? Was ist der Unterschied zwischen Fahrweg und Fahrstraße? In: *EI - Der Eisenbahningenieur* (1), S. 78.

Winter et al. 2018 — Winter, Hanno; Willert, Volker; Adamy, Jürgen (2018): Localization Reference Train - Sichere Ortung für den Schienenverkehr. In: Andreas Oetting (Hg.): Tagungsband des Scientific Railway Signalling Symposiums 2017. Die Steuerung des Eisenbahnbetriebs der Zukunft. Scientific Railway Signalling Symposium. Darmstadt, 19.04.2017. Technische Universität Darmstadt. Darmstadt: Universitäts- und Landesbibliothek Darmstadt.

Wirth & Schöbel 2020 — Wirth, Maximilian; Schöbel, Andreas (2020): Mindestzugfolgezeiten bei ETCS Level 2 und Level 3 auf der Wiener S-Bahn-Stammstrecke. In: *Signal+Draht* 112 (4/2020), S. 21–26.

Wunsch & Jaekel 2017 — Wunsch, Susanne; Jaekel, Birgit (2017): Modellprinzipien des RailTopoModel - Einsatzmöglichkeiten in Planung, Simulation und Betrieb bei Eisenbahnen. In: *EI - Der Eisenbahningenieur* (3/2017).

Zeilinger 2019 — Zeilinger, Rene (2019): Faseroptische Sensoren für effizienteren Bahnbetrieb. In: *Signal+Draht* 111 (12/2019), S. 32–41.

Verzeichnisse

Abkürzungsverzeichnis

Hinweis zum Umgang mit Abkürzungen:

Abkürzungen werden beim ersten Vorkommen eingeführt und dann im zugehörigen Kapitel und Unterkapitel verwendet. Sollten sie in anderen Kapiteln erneut auftauchen, werden sie je nach Gebräuchlichkeit der Abkürzung zum besseren Verständnis der Arbeit ggf. neu eingeführt. Dies trägt dem Umstand Rechnung, dass umfangreiche wissenschaftliche Arbeiten in der Regel nicht am Stück gelesen werden.

AA	Allocation Area (--> *siehe AS*)
AFA	Active Flank Area (dt. aktiver Flankenschutzraum)
APS	Advanced Protection System
AS	Allocation Section [RCA Konzept], neuerdings auch AA (Allocation Area)
ASG	Allocation Section Group [RCA-Konzept]
ATC	Automatic Train Control (Zugüberwachungs- und Steuerungssystem)
ATO	Automatic Train Operation (automatisiertes Fahren)
ATP	Automatic Train Protection (Zugbeinflussungssystem)
BAuA	Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
BEU	Bundesstelle für Eisenbahnunfalluntersuchung (BEU)
BG RCI	Berufsgenossenschaft Rohstoffe und chemische Industrie
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BNetzA	Bundesnetzagentur
BÜ	Bahnübergang
BZ	Betriebszentrale
CCS	Command, Control, and Signalling (vgl. >*LST*)
CTE	Controlled Track Element (stellbares Fahrwegelement)
CTMS	Capacity and Traffic Management System (= erweitertes >*TMS*)
D-Weg	Durchrutschweg
DA	Danger Area
DB	Deutsche Bahn AG
DBB	Digitaler Bahnbetrieb
DKW	Doppelte Kreuzungsweiche
DP	Danger Point (bei ETCS)
DPS	Drive Protection Section [RCA-Konzept]
DSD	Digitale Schiene Deutschlands
DSTW	Digitales Stellwerk
EBA	Eisenbahnbundesamt

EBD	Eisenbahnbetriebsfeld Darmstadt
EBO	Eisenbahn-Bau- und Betriebsordnung
EIU	Eisenbahninfrastrukturunternehmen
EN	Europäische Norm
EoA	End of Authority (Endpunkt der ETCS-Fahrerlaubnis)
ERA	European Railway Agency
ERM	Entity-Relationship-Modell
ERTMS	European Railway Traffic Management System
ESTW	Elektronisches Stellwerk
ETCS	European Train Control System
EU	Europäische Union
EUG	ERTMS Users Group
EVU	Eisenbahnverkehrsunternehmen
FAS	Flank Area Section (dt. Flankenschutzsegment)
FC	Failure Code (dt. Fehlercode)
Fdl	Fahrdienstleiter
FMEA	Failure Mode and Effects Analysis (dt. Auswirkungsanalyse)
FRMCS	Future Railway Mobile Communication System
FPD	Flank Protection Device (dt. Flankenschutzelement)
FPO	Flank Protection Object (im Sinne von Flankenschutzbegrenzungsobjekt)
FTA	Fault Tree Analysis (dt. Fehlerbaumanalyse)
GoA	Grade of Automation (Level des automatisierten Fahrens (ATO))
IH	Instandhaltung
LEU	Lineside electronic unit (Kommunikationsweg von ETCS)
LoA	Limit of Authority (Endpunkt der ETCS-Fahrerlaubnis, wenn die Zielgeschwindigkeit größer 0 ist)
LST	Leit- und Sicherungstechnik
LZB	Linienzugbeeinflussung
MA	Movement Authority (dt. Fahrerlaubnis)
MP	Movement Permission (bei der RCA)
NSA	Non Stopping Area (bei ETCS)
OBU	On-Board Unit
OC	Object Controller
OL	Overlap (bei ETCS)
PR	Protection Rate (dt. Schutzrate)
PZB	Punktförmige Zugbeeinflussung
RA	Restricted Area

RailML	Railway Markup Language
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability, and Safety
RBC	Radio block center (dt. auch ETCS-Zentrale)
RCA	Reference CCS Architecture
REF	Rückfallebenenfunktion (posRef = positiver Bestandteil der R.; negRef = negativer Bestandteil der R.)
RRM	Request Return Message (RRM)
RSTW	Relaisstellwerk
RTM	Rail Topo Model
RÜ	Reisendenübergang
SL	Sicherungslogik / Safety logic
SRS	System Requirements Specification (ETCS-Spezifikation)
SSP	Static Speed Profile (ETCS-Geschwindigkeitsprofil)
SvL	Supervised Location (aktuell gültiger Gefahrpunkt der ETCS-Fahrerlaubnis)
SysML	Systems Modeling Language
TESC	Track Element Status Change (-Request)
Tf	Triebfahrzeugführer
TFFR	Tolerierbare funktionale Ausfallrate
THR	tolerierbare Gefährdungsrate / Tolerable Hazard Rate
TMS	Traffic Management System
TSR	Temporary Speed Restriction (vorübergehende Langsamfahrstelle)
UIC	Union internationale des chemins de fer (internationaler Eisenbahnverband)
UML	Unified Modeling Language
URA	Usage Restriction Area [RCA-Konzept]
WFC	Write Failure Code (Aktion in den smartLogic-Aktivitätsdiagrammen, die einen Fehlercode generiert)

Abbildungsverzeichnis

Tabellenverzeichnis

Anlagen

Anlagen außerhalb des eigentlichen Dokuments (daher ohne Seitenzahlen):

Anlage 1: Glossar

Allocation Area (AA)	siehe >*Allocation Section (AS)*
Advanced Protection System (APS)	Oberbegriff für die infrastrukturseitigen sicherungskritischen Komponenten innerhalb der >*RCA* (siehe Kapitel 2.4.3)
Aktion	stellt einen >*Prozessschritt* im UML-Aktivitätsdiagramm dar (siehe Kapitel 2.6.2)
aktives Flankenschutzelement	ein >*potenzielles Flankenschutzelement*, welches tatsächlich aktuell den für den Flankenschutz benötigten Status innehat und damit Flankenschutz bietet (vgl. Kapitel 8.3.4)
aktiver Flankenschutzraum (AFA)	der Teil des >*Flankenschutzraums*, aus dem aktuell eine >*Gefährdung* für die zu schützende >*Fahrzeugbewegung* kommen kann; wird z. B. durch eine flankenschutzgebende Weiche oder Gleissperre begrenzt (vgl. Kapitel 8.3.4)
Allocation Section (AS)	Begriff aus der RCA bzw. von smartRail 4.0; schränkt die Befahrbarkeit eines >*Gleissegments* aufgrund der gleichzeitigen Belegung eines benachbarten Gleissegments ein; in der neusten Version der RCA-Dokumente auch Allocation Area (AA) (vgl. Kapitel 2.4.4)
anzusteuernder Zielpunkt	>*Zielpunkt* in der >*MA*, vor dem die >*Fahrzeugbewegung* zu stoppen versucht, also ihre Betriebsbremskurve auf diesen Zielpunkt hin berechnet bzw. der Punkt, vor dem der Tf die Fahrzeugbewegung zum Stehen bringen möchte (vgl. Kapitel 8.3.2)
Arbeitsschritt	einzelner Schritt der Vorgehensweise in dieser Arbeit (vgl. Kapitel 3.6.4)
Automatic Train Operation (ATO)	Oberbegriff für verschiedenen Arten des automatisierten Fahrens von Eisenbahnfahrzeugen; Unterschieden wird in vier „Grades of Automation“ (GoA): GoA 1 – Fahren in menschlicher Verantwortung unter zu Hilfenahme von Fahrassistenzsystemen; GoA 2 – automatisches Fahren unter ständiger Überwachung eines Tf; GoA 3 – automatisches Fahren ohne ständige menschliche Überwachung im Triebfahrzeug, bei der allerdings einige Aufgaben (z. B. Überwachung der Türschließung) durch andere Mitglieder des >*Fahrpersonals* übernommen werden; GoA 4 – vollautomatisches Fahren, ohne Beteiligung von Fahrpersonal, welches in dieser Automatisierungsstufe nicht mehr erforderlich ist (aber, z. B. als Servicepersonal noch an Bord sein kann) (vgl. Kapitel 2.2.7)
Bahnbetrieb	Bewegen von Fahrzeugen (vgl. u. a. [DB Netz AG 2017a]) auf der Infrastruktur und alle unmittelbar dazu notwendigen Tätigkeiten (vgl. https://de.wikipedia.org/wiki/Bahnbetrieb, abgerufen am 06.01.2022, 15:21 Uhr); in dieser Arbeit werden rein vorbereitende, planerische Tätigkeiten wie die

	Fahrplanerstellung nicht zum Bahnbetrieb gezählt (die oben genannten Quellen ziehen keine genaue Grenze, welche Tätigkeiten noch unmittelbar zum Bahnbetrieb gehören)
Bahnproduktionsprozess	siehe >*Produktionsprozess*
Basisfunktionen	Kategorie im >*Funktionskatalog*, welche die grundlegenden Funktionen, die für einen zielführenden Betrieb der >*smartLogic* erforderlich sind, umfasst (vgl. Kapitel 6.6.1)
Beanspruchung	registrierte Nutzung einer Infrastrukturressource; kann vor allem mit >*Gleissegmenten* und >*stellbare Fahrwegelementen* verknüpft werden; schließt häufig (aber nicht immer) die Registrierung anderer Nutzungen aus (vgl. Kapitel 7.6.2)
betrieblich funktionale Anforderung	Anforderung an den >*Funktionsumfang* der >*smartLogic*, die sich aus den gewünschten, betrieblichen Aufgaben der >*Sicherungslogik* heraus ergibt (vgl. Kapitel 6.1)
Betriebspersonal	alle am unmittelbaren Betrieb beteiligten Personale; besteht aus >*Stellwerkspersonal*, >*Zugbildungspersonal*, >*Fahrpersonal*, Sicherungsposten (vgl. >*Bahnbetrieb*)
Branching Elements	siehe >*verzweigende Fahrwegelemente*
Controlled Track Element (CTE)	siehe >*stellbare Fahrwegelemente*
Danger Area (DA)	Typ von >*Gleisabschnitt* zur Definition von Gefahrenbereichen (vgl. Kapitel 7.3.7)
Danger Point (DP)	>*ETCS*-Begriff: bezeichnet den >*Gefahrpunkt*, der für eine zu schützende Fahrzeugbewegung maßgeblich ist, wenn kein Durchrutschweg zur Verfügung steht (vgl. Kapitel 8.3.2 und [Trinckauf et al. 2020, S. 115]); zu unterscheiden von anderen Verwendungen des deutschen Begriffs “Gefahrpunkt“
Deletion Conditions	siehe >*Löschbedingungen*
Detektionsabschnitt	Typ von >*Gleisabschnitt*, der bei definierten Arten von >*Beanspruchungen* durch eine >*Fahrzeugbewegung* eine Aktion auslöst; vor allem die Aktivierung bzw. Deaktivierung eines >*Wirkabschnitts* bzw. die Anpassung der dort übermittelten >*ortsgebundenen Information* (z. B. erlaubte Geschwindigkeit) (vgl. Kapitel 7.3.5)
Digitaler Bahnbetrieb (DBB)	umfangreiches Programm der Deutschen Bahn AG und ihrer Tochtergesellschaften zur „Digitalisierung“ verschiedener Bereiche des >*Bahnproduktionsprozesses* (vgl. Kapitel 2.2.1)
Digitale Schiene Deutschland (DSD)	Teilbereich des Programms >*„Digitaler Bahnbetrieb“*, der sich mit der strecken- und fahrzeugseitigen Leit- und Sicherungstechnik befasst (vgl. Kapitel 2.2.1)
Digitales Stellwerk (DSTW)	(neuer) Stellwerkstyp, bei dem die Informationen zwischen den Feldelementen und dem Stellwerkskern über die standardisierten, digitalen >*EULYNX*-Schnittstellen übertragen werden (vgl. Kapitel 2.2.5)

Drive Protection Section (DPS)	Begriff aus der RCA bzw. von smartRail 4.0; bezeichnet den Teil der Gleistopologie, dessen Befahrbarkeit vom Status eines kontrollierbaren Fahrwegelements (>*Controlled Track Element*) abhängt (vgl. Kapitel 2.4.4)
dynamischer Gleisabschnitt	Typ von >*Gleisabschnitt*, dessen Position bzw. Ausmaße sich regelmäßig verändern (vgl. Kapitel 7.3.4)
einfaches Fahrwegelement	>*Fahrwegelement*, ohne besondere Funktion (insbesondere kein >*stellbares Fahrwegelement* oder >*unterbrechendes Fahrwegelement*) (vgl. Kapitel 7.4.2)
Ereignismeldung	von einem Umsystem an die >*Sicherungslogik* über eine dafür vorgesehene Schnittstelle gemeldete Zustandsänderung im Gesamtsystem (vgl. Kapitel 6.2.2)
Erreichenswahrscheinlichkeit	Wahrscheinlichkeit, dass eine >*Fahrzeugbewegung* einen Ort auf der >*Gleistopologie* bei Anfahrt auf einen >*Zielpunkt* erreicht (vgl. Kapitel 8.3.2)
ETCS	europaweit standardisiertes Zugbeeinflussungssystem, welches schrittweise die nationalen Systeme („Class B"-Systeme) ablösen soll; Teil des europäischen Eisenbahnverkehrs-mangementsystems ERTMS (vgl. Kapitel 2.2.2)
EULYNX	europäische Initiative von Eisenbahninfrastrukturunter-nehmen, die gemeinsame, digitale Stellwerksschnittstellen erarbeitet (vgl. Kapitel 2.2.5)
Fahrerlaubnis	siehe >*Movement Authority* (vgl. Kapitel 2.1.1)
Fahrerlaubnisanfrage	>*Prüfanfrage* an die >*Sicherungslogik*, einen Fahrerlaubniswunsch dahingehend zu prüfen, ob er zu einem unsicheren Systemzustand führt; bei erfolgreicher Prüfung wird eine >*Fahrerlaubnis (MA)* generiert und an das betreffende Fahrzeug weitergeleitet (vgl. Kapitel 4.3.1)
Fahrpersonal	alle Mitarbeiter von Eisenbahnunternehmen und von ihnen beauftragten Subunternehmen, die in Eisenbahnfahrzeugen während der Fahrt beschäftigt sind (vgl. Kapitel 5.2.2)
Fahrstraße	Begriff aus der klassischen Eisenbahnsicherungstechnik für einen vordefinierten, gesicherten >*Fahrweg* von einem fest definierten Punkt zu einem anderen fest definierten Punkt inkl. dazugehöriger Schutzelemente (Flankenschutz) und Schutzweg hinter dem Zielpunkt (Durchrutschweg, Gefahrpunktabstand); ein klassisches Stellwerk hat eine definierte Anzahl Fahrstraßen; der Begriff wird bei der >*smartLogic* nicht mehr verwendet, da sie keine vordefinierten Fahrstraßen kennt, sondern flexible >*Fahrerlaubnisse* von und zu beliebigen Punkten auf der Topologie erlaubt (vgl. Kapitel 2.1.1)
Fahrweg	Allgemein: „Eine sich aus der Lage der Gleise und Weichen in der Gleistopologie ergebende Fahrmöglichkeit eines

	Schienenfahrzeugs“ [Pachl 2021]; Ebenfalls gebräuchliche Verwendung: tatsächlich von einer >*Fahrzeugbewegung* befahrener Teil einer >*Fahrstraße* (zur Fahrstraße gehören in diesem Zusammenhang weiterhin Flankenschutzelemente und der Durchrutschweg) (vgl. [Widmann 2022]); der in einer >*MA* oder >*MP* beantragte Fahrweg wird in dieser Arbeit zur besseren Abgrenzung des allgemeinen Fahrweg-Begriffs als >*Route* bezeichnet; Gröbere Definition: Oberbegriff für Ober- und Unterbau (vgl. [Maschek 2018, S. 2])
Fahrwegelement	Oberbegriff für >*Infrastrukturelemente*, aus denen sich der >*Fahrweg* bzw. >*Durchrutschweg* von >*Fahrzeugbewegungen* zusammensetzen kann (inkl. Sperrelemente), wie >*einfache Fahrwegelemente*, >*stellbare Fahrwegelemente* (z. B. Weichen), Kreuzungen etc. (vgl. Kapitel 7.4.2)
Fahrzeugbewegung	Sammelbegriff für alle Bewegungen von Eisenbahnfahrzeugen auf dem Schienennetz (Zug- und Rangierfahrten) (vgl. z. B. Verwendung des Begriffs in [DB Netz AG 2017a]: u. a. „Eine Rangierfahrt ist eine Fahrzeugbewegung […]“)
Feldelement(e)	>*Infrastrukturelemente*, die sich direkt an der Strecke befinden (in Abgrenzung zu den Infrastrukturelementen, die sich in den Zentralstellen (z. B. Stellwerken) befinden (vgl. Kapitel 2.2.5)
Flank Area Section (FAS)	siehe >*Flankenschutzsegment*
Flank Protection Device (FPD)	siehe >*Flankenschutzelement (FPD)* (vgl. Kapitel 8.3.4)
Flank Protection Object (FPO)	Begrenzung, welche den >*aktiven Flankenschutzraum* begrenzt und die Schutzrate in Bezug auf den Flankenschutz erhöht (Object bezieht sich auf ein Objekt des Datenmodells) (vgl. Kapitel 8.3.4)
Flankenschutzelement (FPD)	>*Stellelement*, welches bei entsprechendem Status das Risiko einer Flankenfahrt verringern kann; siehe auch >*potenzielles Flankenschutzelement* und >*aktives Flankenschutzelement* (vgl. Kapitel 8.3.4)
Flankenschutz-Gefahrabschnitt	>*Gleisabschnitt*, in dem ein Eisenbahnfahrzeug eine Flankenfahrt erzeugen kann (Abschnitt zwischen >*Flankenschutz-Gefahrstelle* und Grenzzeichen bzw. weitere Abschnitte, in denen ein Gleis das Lichtraumprofil eines anderen Gleises beeinträchtigt (vgl. Kapitel 8.3.4))
Flankenschutz-Gefahrstelle	>*Allocation Section*, an der potenziell eine Flankenschutz-gefährdung auftreten kann; Ausgangspunkt für die Bestimmung des >*Flankenschutzraums* (vgl. Kapitel 8.3.4)
Flankenschutzraum	Gleisbereich, aus dem eine zu schützende >*Fahrzeugbewegung* von einem durch sie zu passierenden >*Flankenschutz-Gefahrabschnitt* aus (z. B. Weiche, Kreuzung) theoretisch physisch (durch eine Flankenfahrt) gefährdet werden kann; zu unterscheiden vom >*aktiven Flankenschutzraum*, der einen

	Teilbereich des Flankenschutzraums darstellt (vgl. Kapitel 8.3.4)
Flankenschutzsegment	einzelnes >*Gleissegment* im >*Flankenschutzraum* (vgl. Kapitel 8.3.4)
FRMCS	in der Konzeptionsphase befindliches zukünftiges mobiles Kommunikationssystem, primär für die Luftschnittstelle Fahrzeug – Infrastruktur (vgl. Kapitel 2.2.4)
funktionale Sicherheit	Schutz gegen systematische und zufällige Fehler; in Abgrenzung zum Schutz gegen vorsätzliche Gefährdungen (vgl. engl. >*safety* versus security) (vgl. Kapitel 3.3)
funktionale Sicherheitsanforderung	Anforderung an den >*Funktionsumfang* der smartLogic, die sich aus der Gefährdungsanalyse heraus ergibt; hinter einer funktionalen Sicherheitsanforderung verbirgt sich der Ausschluss einer Gefährdung, die durch entsprechende >*Prüfbedingungen* von der >*Sicherungslogik* sichergestellt werden muss (vgl. Kapitel 6.1)
Funktionsgruppe	Kategorie im >*Funktionskatalog* (vgl. Kapitel 6.6.1)
Funktionskatalog	Gesamtheit aller in der Funktionsanalyse identifizierten möglichen Funktionen der >*smartLogic*; ist nicht identisch mit dem >*Funktionsumfang*, da nicht alle Funktionen aus dem Funktionskatalog tatsächlich umgesetzt wurden (aufgrund von Relevanzüberlegungen und Priorisierung) (vgl. Einleitung zum 6. Hauptkapitel)
Funktionsumfang	Gesamtheit aller Funktionen (Prozessfunktionen, Subroutinen und Prüfbedingungen), die in der >*smartLogic* umgesetzt wurden; nicht zu verwechseln mit dem >*Funktionskatalog*, der alle möglichen Funktionen enthält und daher umfangreicher als der umgesetzte Funktionsumfang ist (vgl. Kapitel 6.1)
Gefahrpunkt	klassisch angelehnt an [Pachl 2021], „die erste auf [das Ende der Fahrerlaubnis] folgende Stelle im Gleis, an der beim Durchrutschen eines Zuges eine >*Gefährdung* eintreten kann“ (vgl. Kapitel 2.1.1); bezogen auf diese Arbeit allgemeiner formuliert: von der zu schützenden >*Fahrzeugbewegung* in Fahrtrichtung zu erreichender Punkt auf der >*Gleistopologie*, an dem eine >*Gefährdung* der Fahrzeugbewegung auftreten kann, (vgl. Kapitel 8.3.2); zu unterscheiden vom >*ETCS*-Begriff >*Danger Point*
Gefahrstelle	der Begriff wird in Zusammenhang mit dem Flankenschutz im Begriff „>*Flankenschutz-Gefahrstelle“* verwendet, um eine Verwechslung mit dem >*Gefahrpunkt* zu vermeiden, der sich auf das Ende der >*Fahrstraße* bzw. >*Fahrerlaubnis* bezieht
Gefährdung	Zustand, der zu einem Unfall führen kann (gem. [DIN EN 50126-1:2017, S. 15])

Gefährdungsanalyse	mit dem Begriff wird in der Arbeit der Arbeitsschritt der Gefährdungsidentifikation als Voraussetzung für die Bestimmung der funktionalen Sicherheitsanforderungen bezeichnet; er wird demzufolge nicht im Sinne einer „betrieblichen Gefährdungsanalyse“ verwendet (vgl. Kapitel 3.6.4)
Gefährdungsrisiko	Risiko, mit dem eine beliebige >*Gefährdung* bei Passieren eines >*Wirkbereiches* der Gefährdung durch eine >*Fahrzeugbewegung* eintritt (vgl. Kapitel 8.3.1 und 8.3.2)
Gefährliches Ereignis	von der BEU (vormals EUB) klassifizierte Unfälle oder Ereignisse, die zu einem Unfall hätten führen können (vgl. [EUB 2009])
Gleisabschnitt	der Begriff bezeichnet einen beliebigen Abschnitt der >*Gleistopologie*, der ein oder mehrere >*Gleissegmente* umfassen kann; zu unterscheiden von >*Gleisbereich* (vgl. Kapitel 7.3.3)
Gleisbereich	größerer Bereich der >*Gleistopologie*, zu unterscheiden von >*Gleisabschnitt* und >*Gleissegment* (vgl. Kapitel 7.3.8)
Gleissegment	Teil der >*Gleistopologie*, der gemäß der RTM-Methodik durch einen topologischen Knoten modelliert wird; ein Gleissegment kann keine Verzweigung des Gleises enthalten; zu unterscheiden von >*Gleisabschnitt* und >*Gleisbereich* (vgl. Kapitel 7.3.1)
Gleistopologie	Gesamtheit der betrachteten Gleise (vgl. Einleitung zu Kapitel 7.3)
globale Anforderung	Anforderung, die sich auf die Durchführung der gesamten Arbeit auswirkt; zur Abgrenzung von >*funktionalen Sicherheitsanforderungen* oder >*betrieblichen funktionalen Anforderungen* an die Logik und von Anforderungen an die Vorgehensweise oder Methodik einzelner Teilschritte der Gesamt-Vorgehensweise (einzelner Kapitel) (vgl. Kapitel 3.5)
Infrastrukturelement	Oberbegriff für ortsgebundene und mobile Bestandteile der Eisenbahninfrastruktur
infrastrukturseitige Sicherungstechnik	Gesamtheit aller technischen Komponenten, die nicht zu den Fahrzeugen gehören und zur unmittelbaren >*funktionalen Sicherheit* des >*Bahnbetriebs* beitragen
Interrupting Element	siehe >*unterbrechende Fahrwegelemente*
Kernanforderung	die Kernanforderung in dieser Arbeit ist, dass die >*smartLogic* die Sicherheit innerhalb des ihr zugewiesenen Aufgaben¬bereiches gewährleisten muss (sichere Logik) (vgl. Kapitel 3.5)

Kernprozessfunktion	>*Prozessfunktionen*, die im Zug der in dieser Arbeit vorgenommenen Priorisierung zum initialen >*Funktionsumfang* der >*smartLogic* gehören (vgl. Kapitel 6.6.3)
Klasse	>*Objekttyp / Klasse* (vgl. Kapitel 2.6.2) oder Bezeichnung für eine Einteilungsklasse in der Mengenlehre/Statistik
Kompensationsmaßnahmen	risikomindernde in der >*Fahrerlaubnisanfrage* vorgegebene Eigenschaften der beantragten >*Fahrerlaubnis*, wie eine niedrigere Geschwindigkeit, als eigentlich erlaubt wäre (vgl. Kapitel 8.2.2 und 8.3.6)
Linienzugbeeinflussung (LZB)	seit den 1970er Jahren in Deutschland eingesetzte Technologie, mit der u. a. die zulässige Geschwindigkeit und die Bremsung auf einen vom Stellwerk vorgegebenen Zielpunkt eines Eisenbahnfahrzeugs überwacht werden kann; der Datenaustausch zwischen Zug und Infrastruktur ist dabei anders als bei der >*"Punktförmigen Zugbeeinflussung"* kontinuierlich möglich, so dass Veränderungen direkt vom Fahrzeug verarbeitet werden können; bis 2030 abgekündigt; soll durch >*ETCS* ab Level 2 ersetzt werden; ETCS-„Class B"-System (vgl. Kapitel 2.1.1)
Löschbedingungen	Bedingungen, die erfüllt sein müssen, bevor eine >*Restricted Area* gelöscht oder verkürzt werden darf (vgl. Kapitel 7.3.6)
(aktuell) maßgeblicher Gefahrpunkt	nächster von der zu schützenden >*Fahrzeugbewegung* erreichbarer >*Gefahrpunkt*, bei dessen Überquerung die >*Schutzrate* unzulässig sinken würde (vgl. Kapitel 8.3.2)
mehrfachverzw. Fahrwegelemente	doppelte Kreuzungsweichen etc. (vgl. Kapitel 7.4.4)
Movable Object (MOB)	siehe >*Fahrzeugbewegung;* siehe insbesondere bei der RCA (vgl. Kapitel 2.4.4)
Movement Authority (MA)	umfangreiche >*ETCS*-Nachricht, die (vereinfacht gesagt) einem Eisenbahnfahrzeug das Fahren mit einem definierten Geschwindigkeits- und Modusprofil bis zu einem definierten Zielpunkt unter Beachtung eines definierten Gefahrpunkts erlaubt; das ETCS-Bordgerät überwacht die Einhaltung dieser Parameter; bei der RCA existiert die Bezeichnung >*Movement Permission* für die Fahrerlaubnis, bevor diese endgültig als ETCS-Nachricht an das Fahrzeug übermittelt wird (vgl. Kapitel 2.2.2)
Movement Permission (MP)	spätere >*Movement Authority;* so wird die angefragte Fahrerlaubnis bei der RCA bezeichnet, bevor sie an das Fahrzeug als MA übermittelt wird (vgl. Kapitel 2.4.4)
Object Controller	Steuerungscomputer von >*Feldelementen*; befindet sich bei >*Digitalen Stellwerken* in unmittelbarer Nähe des Feldelements (vgl. Kapitel 2.2.5)

Objekt	informationstechnische Abbildung eines konkreten Systemelements zur Laufzeit des Systems; Instanz eines >*Objekttyps/Klasse* (vgl. Kapitel 2.6.2)
Objekttyp / Klasse	Abbildung eines Systemelements im Datenmodell, auch als „Klasse“ im UML-Klassendiagramm bezeichnet (vgl. Kapitel 2.6.2)
ortsgebundene Information	allgemeine Bezeichnung für Informationen, die entweder fest oder dynamisch an der Topologie verortet werden und für die Durchführung von >*Fahrzeugbewegungen* beim Passieren des Informationspunktes relevant sind (vgl. Kapitel 7.3)
Ortungsinformationsaggregator	Softwarekomponente innerhalb der >*infrastrukturseitigen Sicherungstechnik*, die aus verschiedenen Ortungsquellen die Zugposition so genau wie möglich bestimmt (vgl. Kapitel 4.4.4)
potenzielles Flankenschutzelement	>*stellbares Fahrwegelement*, welches einen Status besitzt, mit dem es theoretisch für den betrachteten >*Flankenschutz-Gefahrabschnitt* (>*Allocation Section*) eine Funktion als >*Flankenschutzelement* übernehmen könnte (aber nicht zwangsläufig aktuell auch tut, da es möglicherweise derzeit nicht den notwendigen Status hat) (vgl. Kapitel 8.3.4)
primärer sicherungstechn. Zielpunkt	>*Zielpunkt* der >*MA*, vor dem die betroffene >*Fahrzeugbewegung* mit hinreichender >*Sicherheit* zum Stehen kommen muss (vgl. Kapitel 8.3.2)
Produktionsprozess	der (Bahn-)Produktionsprozess umfasst alle Tätigkeiten bzw. Aktionen, die zur Durchführung von Fahrzeugbewegungen auf der Eisenbahninfrastruktur erforderlich sind (vgl. >*Produktionssystem Eisenbahn*)
Produktionssystem Eisenbahn	dieser Begriff wird in der Praxis mit unterschiedlichen Definitionen verwendet und bezeichnet in der vorliegenden Arbeit als Oberbegriff alle Systemkomponenten, die unmittelbar zum Produktionsprozess „Durchführen einer Zugfahrt“ beitragen; ausgeklammert sind vorgelagerte Planungsprozesse wie die Fahrplanerstellung
Prozess	in Bezug auf Software: Durchführung einer Reihe von >*Prozessschritten* in Folge eines Auslösers, die in einem Ergebnis münden; siehe auch >*Prozessfunktion* (vgl. Kapitel 6.2.2)
Prozessfunktion	Funktionalität der >*smartLogic*, die von einem berechtigten >*Umsystem* aus aufgerufen werden kann; startet in der Regel einen >*Prüf-* oder *Reaktionsprozess* innerhalb der smartLogic (vgl. Kapitel 6.2.2)
Prozessschritt	einzelner Schritt innerhalb eines >*Prüf-* oder >*Reaktionsprozesses* oder >*Subroutine*; im UML-Aktivitätsdiagramm als >*Aktion* dargestellt (vgl. Kapitel 6.2.2)

Prüfanfrage	Anfrage (in der Regel vom TMS) an die >*smartLogic*, eine gewünschte Zustandsänderung (z. B. Weiche stellen oder >*Fahrerlaubnis*) dahingehend zu überprüfen, ob sie zu einem unsicheren Zustand führt; löst in der Regel einen >*Prüfprozess* aus; die Prüfanfrage muss durch eine entsprechende >*Prozessfunktion* von der smartLogic abgedeckt sein (vgl. Kapitel 4.3.1)
Prüfbedingung	eine Bedingung, deren Einhaltung durch einen entsprechenden >*Prüfprozess* bei jeder >*Prüfanfrage* an die >*smartLogic* sichergestellt werden muss; leitet sich aus einer >*funktionalen Sicherheitsanforderung* ab (vgl. Kapitel 6.2.1 und 6.2.2)
Prüfprozess	Prozess zur Überprüfung der Einhaltung aller relevanten >*Prüfbedingungen* bei Aufruf einer >*Prozessfunktion* (vgl. Kapitel 6.2.2)
Punktförmige Zugbeeinflussung (PZB)	seit den 1930er Jahren in Deutschland bei zugelassenen Geschwindigkeiten bis 160 km/h eingesetzte Technologie, mit der die Bremsung von Eisenbahnfahrzeugen auf einen Zielpunkt mit reduzierter Geschwindigkeit fahrzeugseitig überwacht werden kann; die Datenübertragung findet dabei nur an bestimmten Punkten auf dem Gleis statt; >*ETCS*-„Class B“-System (vgl. Kapitel 2.1.1)
Reaktionsprozess	Prozess zur Prüfung einer geeigneten Reaktion auf eine >*Ereignismeldung* und Einleitung erforderlicher >*Sicherheitsreaktionen* (vgl. Kapitel 6.2.2)
Reference CCS Architecture (RCA)	europäische Initiative von Eisenbahninfrastrukturunternehmen, die eine gemeinsame Referenz-Architektur für die streckenseitige Eisenbahnleit- und -sicherungstechnik entwickelt (vgl. Kapitel 2.4)
Registrierung	bezogen auf die Einbindung von >*Stakeholder-Systemen* in die >*smartLogic*: Prozess, in dem ein Stakeholder-System eine bestimmte Funktion auf einer funktionalen Schnittstelle der smartLogic registriert (z. B. könnte ein Windmesssystem eine automatische Geschwindigkeitsbegrenzung auf einem bestimmten >*Gleisabschnitt* abhängig von seinem Systemstatus registrieren) (vgl. Kapitel 8.3.3)
Reservepool	Sammlung an Funktionen, die zunächst in der Funktionsanalyse identifiziert wurden, dann jedoch aufgrund angenommener fehlender Relevanz für die >*smartLogic* aussortieren wurden; die endgültige Aussortierung erfolgt jedoch erst, wenn im Rahmen der Modellanalyse die Irrelevanz der Funktion für die smartLogic tatsächlich erwiesen wurde (vgl. Kapitel 6.2.3)
Restricted Area (RA)	Typ von >*Gleisabschnitt*, der Einschränkungen oder Vorgaben für >*Fahrzeugbewegungen* definiert; ähnlich den

	>*Usage Restriction Areas* bei der RCA (vgl. Kapitel 7.3.4 und 7.3.6)
Route	beantragter >*Fahrweg* für eine Fahrzeugbewegung in einer >*Fahrerlaubnis* (>*MA* bzw. >*MP*) (vgl. Kapitel 7.6.3)
Rückfallebene	Systemzustand bei eingeschränkter Funktionsweise eines oder mehrerer Teilsysteme; Rückfallebenen werden aktiv, wenn Teilsysteme der >*infrastrukturseitigen Sicherungstechnik* nicht voll funktionsfähig sind, sich in einem eingeschränkten Systemzustand befinden oder benötigte Informationen nicht in ausreichender Güte vorliegen; es gibt keine begrenzte Anzahl von vordefinierten Rückfallebenen; für eindeutig identifizierbare Einschränkungen können spezielle Funktionsbedingungen für das Teilsystem festgelegt werden, die von der >*Sicherungslogik* berücksichtigt werden können (>*Rückfallebenenbedingungen*) (vgl. Kapitel 2.1.1 und 8.3.6)
Rückfallebenenbedingungen	erforderliche Parameter (i. d. R. von der Fahrzeugbewegung zu beachtende Einschränkungen, wie z. B. eine niedrigere Geschwindigkeit oder ein bestimmter ETCS-Modus), welche die beantragte MA zusätzlich enthalten muss, damit in einer >*Rückfallebene* (und damit bei einem eingeschränkten >*Sicherheitslevel*) eine ausreichend hohe >*Schutzrate* erreicht wird (vgl. Kapitel 8.3.6)
Rückfallebenenfunktion (REF)	Funktion zur Beschreibung des Einflusses von >*Rückfallebenen* auf die >*Schutzrate* (vgl. Kapitel 8.3.6)
Rückfallebenenbedingung	siehe >*Rückfallebene*
Schutzfunktionen	vom Stellwerk zu erfüllende funktionale Sicherheits-anforderungen (vgl. [Maschek 2009])
Schutzrate	Maß für das vorhandene Risiko einer Gefährdung des >*Bahnbetriebs* durch eine mittels >*Prüfanfrage* beantragte Zustandsänderung des Eisenbahnsystems (z. B. Zustimmung zu einer Fahrt) (vgl. Kapitel 8.3.1)
Schwellwert	Wert, den die >*Schutzrate* überschreiten muss, damit eine >*Prüfanfrage* genehmigt werden kann
Security	Schutz vor vorsätzlichen Angriffen, in Abgrenzung zur >*funktionalen Sicherheit* (vgl. Kapitel 3.3)
sekundärer sicherungstechn. Zielpunkt	>*Zielpunkt* der >*MA* mit abgestuftem >*Gefährdungsrisiko* (vgl. Kapitel 8.3.2)
Subroutine	Ein Prozess, der nicht von außen, sondern intern von einer oder mehreren >*Prozessfunktionen* aufgerufen wird; Teil-baustein einer Prozessfunktion (vgl. Kapitel 6.2.2)
Sicherheit / sicher	Sicherheit bedeutet die „Freiheit von inakzeptablem Risiko“ [DIN EN 50126-1:2017, S. 21]; was als vertretbares Risiko gilt,

	regeln die anerkannten Regeln der Technik bzw. gesetzliche oder normenbasierte Vorgaben
Sicherheitsanforderung	siehe >*funktionale Sicherungsanforderung*
Sicherheitslevel	abgestuftes Maß an >*Sicherheit*, das Systemkomponenten der >*infrastrukturseitigen Sicherungstechnik* bzw. >*Stakeholder-Systeme* abhängig von ihrem Status in Bezug auf die Berechnung der >*Schutzrate* liefern können; niedrigere Sicherheitslevels können ggf. mit >*Rückfallebenenbedingungen* kompensiert werden (vgl. Kapitel 8.3.6)
Sicherheitsreaktion	Maßnahmen, die nach der Meldung eines unerwarteten Ereignisses getroffen werden, um Schaden abzuwenden oder zu verringern (vgl. Kapitel 3.2)
Sicherungslogik / Safety Logic	Komponente der >*infrastrukturseitigen Sicherungstechnik*, deren Aufgabe es ist, betriebliche Anfragen (>*Prüfanfragen)* zur Nutzung der Infrastruktur oder zur Statusänderung von Infrastrukturelementen oder Fahrzeugen (z. B. >*Fahrerlaubnisanfrage* oder >*Stellanforderung*) daraufhin zu überprüfen, ob sie zu einem unsicheren Zustand führen (vgl. Kapitel 4.3.1)
Sicherungstechnischer Tripol	Konzept aus der Doktorarbeit von Daria Menzel (geb. Bachurina); beschreibt generisch die sicherungstechnischen Anforderungen an Abschnitte des Gleisnetzes (vgl. Kapitel 2.3.3 und [Menzel 2019])
smartLogic	einprägsame Bezeichnung für eine auf dieser Arbeit basierende neu zu entwickelnde >*Sicherungslogik* (vgl. Einleitung zu Kapitel 1)
smartRail 4.0	umfangreiches Eisenbahn-Branchenprogramm in der Schweiz zur Neudefinition des Eisenbahnproduktionsprozesses (vgl. Kapitel 2.3.1)
Sperrelement	>*Feldelement*, welches nicht Teil des Gleises ist, aber die Befahrbarkeit desselben einschränken kann (z. B. Gleissperren, Tore) (vgl. Kapitel 7.4.2)
Spot Location	beliebiger Punkt auf der >*Gleistopologie*
Stakeholder	a) am Bahnbetrieb beteiligte Person im Sinne der Stakeholder-Analyse (vgl. Kapitel 3.1.2) b) siehe >*Stakeholder-System*
Stakeholder-System	externes System, welches über bereitgestellte Daten-Schnittstellen mit der >*Sicherungslogik* in Kontakt tritt (vgl. Kapitel 8.3.3)
Stellanforderung	>*Prüfanfrage* an die >*smartLogic*, eine gewünschte Statusänderung eines >*stellbaren Fahrwegelements* daraufhin zu überprüfen, ob dadurch ein unsicherer Zustand eintreten könnte (vgl. Kapitel 4.3.1)

stellbare Fahrwegelemente	*Fahrwegelemente*, die planmäßig verschiedene Status annehmen können; zu den stellbaren Fahrwegelementen gehören die >*verzweigenden Fahrwegelemente*, die >*unterbrechenden Fahrwegelemente* sowie die Sperrelemente; Untermenge der >*Stellelemente* (vgl. Kapitel 7.4.3)
Stellbefehl	Anweisung an >*Stellelemente*, ihren Status zu verändern; wird von der smartLogic nach erfolgreicher Prüfung einer >*Stellanforderung* vom TMS mittels eines >*TESC-Requests* an das Stellelement gesendet (vgl. Kapitel 4.3.1)
Stellelemente	>*Feldelemente*, deren Status durch die >*Sicherungslogik* verändert werden kann (vgl. [Maschek 2001, S. 5]); häufig (im eher betriebswirtschaftlichen Kontext) auch „Stelleinheit“
Stellwerkslogik	anderer Begriff für >*Sicherungslogik*, der vorwiegend im Zusammenhang mit bestehender Stellwerkstechnik verwendet wird; der Begriff „Sicherungslogik“ wird dagegen vorwiegend bei zukünftigen Systemen der infrastrukturseitigen Sicherungstechnik verwendet, bei denen es keine klassischen Stellwerke als technische Einheiten mehr gibt (vgl. Kapitel 2.1.1)
Stellwerkspersonal	umfasst in dieser Arbeit Fahrdienstleiter inkl. örtlich zuständiger Fahrdienstleiter, Weichenwärter, Schrankenwärter und von diesen beauftragte Mitarbeiter (z. B. Posten, Boten, Melder) (vgl. Kapitel 5.2.2) (eine allgemeingültige Definition wurde nicht gefunden)
System Requirements Specific. (SRS)	bezeichnet in Bezug auf ETCS das standardisierte ETCS-Regelwerk (vgl. Kapitel 2.2.2)
Track Area	siehe >*Gleisabschnitt*; vgl. insbesondere bei der RCA (vgl. Kapitel 2.4.4 und 7.3.3)
Track Edge	siehe >*Gleissegment*; vgl. insbesondere bei der RCA (vgl. Kapitel 2.4.4)
Track Edge Section	beliebiger Teil eines >*Gleissegments*; vgl. insbesondere bei der RCA (vgl. Kapitel 2.4.4)
Track Element	>*Fahrwegelement*
TESC-Request	steht für Track Element Status Change-Request; bezeichnet den >*Prüfprozess* zur Prüfung einer >*Stellanforderung* (vgl. Kapitel 8.5.5)
Umsysteme	externe Systeme, die mit der Sicherungslogik über Nachrichten kommunizieren (vgl. Einleitung zu Kapitel 4)
Unfall	„unerwünschtes oder unbeabsichtigtes plötzliches Ereignis im Eisenbahnbetrieb oder eine Verkettung derartiger Ereignisse mit Personen-, Sach- oder Umweltschäden“ [EUB 2009]

unterbrechende Fahrwegelemente	>*stellbare Fahrwegelemente*, welche die physische Befahrbarkeit des Gleises vorrübergehend unterbrechen können (vgl. Kapitel 7.4.3)
Usage Restriction Area (URA)	Begriff aus der RCA bzw. von smartRail 4.0; bezeichnet einen Typ von >*Gleisabschnitten*, durch den Einschränkungen für auf der Topologie verkehrende Fahrzeugbewegungen definiert werden können (z. B. Befahrbarkeitseinschränkungen für bestimmte oder alle Fahrzeugtypen, Definition erforderlicher Fahrzeugausstattung) bzw. Vorgaben für das vorbeifahrende Fahrzeug gemacht werden können (Geschwindigkeits-einschränkungen, vorgeschriebene fahrzeugseitige Aktionen wie Pfeifen) (vgl. Kapitel 2.4.4)
verletzte Prüfbedingung	>*Prüfbedingung*, deren zugrundeliegende >*funktionale Sicherheitsanforderung* nicht vollständig erfüllt ist
verzweigende Fahrwegelemente	Oberbegriff für >*Fahrwegelemente*, an denen sich das Gleis verzweigt (Weichen, Drehscheiben), so dass von mindestens einem Ende des Fahrwegelements aus verschiedene Fahrbeziehungen möglich sind (eine reine Kreuzung ohne Weichenfunktion ist demnach kein verzweigendes Fahrwegelement) (vgl. Kapitel 7.4.3)
Waypoint	siehe >*Wegweiser*
Wegweiser	>*stellbares Fahrwegelement* mit definiertem Status als Teil einer >*Route* (vgl. Kapitel 7.6.3 und 8.6.1)
Wirkabschnitt	Typ von >*Gleisabschnitt*, der definiert, in welchem Bereich eine >*ortsgebundene Information* Gültigkeit hat (vgl. Kapitel 7.3.5)
Zielpunkt	in der >*MA* vorgegebener Schnittpunkt von fahrzeugseitigen Bremskurven mit einer definierten Abfanggeschwindigkeit (vgl. Kapitel 8.3.2)
Zugbildungspersonal	umfasst alle an der Zugbildung und sonstigen Rangierprozessen beteiligte Mitarbeiter, die nicht zum Stellwerkspersonal gehören (z. B. Rangierer, Rangierbegleiter, Wagenmeister, Rangiertriebfahrzeugführer) (es kann Überschneidungen zum >*Fahrpersonal* geben) (vgl. Kapitel 5.2.2)

Anlage 2: Funktionskatalog

Legende

Funktionsart (P / R / SF / I):

- P = Prozessfunktion
- SF = Subroutine
- R = Prüfbedingung
- I = Information

Bei Prozessfunktionen nähere Unterteilung in C/R/U:

- C: Prüfprozess
- R: Reaktionsprozess
- U: Bedienprozess

Herkunft:

- Systematic Approach: Wurde durch das systematische Verfahren gemäß Kapitel 6.3 und Kapitel 6.4 identifiziert
- Ril 408: Wurde bei der Literaturergänzung aus [DB Netz AG 2017a] identifiziert
- Lastenheft F1: Wurde bei der Literaturergänzung aus [DB Netz AG 2001] identifiziert

Kategorie:

- B: Basisfunktion
- M: Überwachungsfunktion
- C: Bedienfunktion
- O: Out of Scope (zur Verdeutlichung in den Katalog aufgenommen)
- P: Protokollierung
- F: Rückfallebenenfunktion
- S: Systemfunktion
- Sh: Rangierfunktion (bei Funktionen, die aus der klassischen Stellwerkstechnik übernommen wurden)
- T: Übergangsfunktion (Übergang in anderen Stellbereich)
- Z: Spezialfunktion

Katalog

ID	P / R / SF / I	C/R/U	Origin	Category	Description
F-E000a	R		systematic approach	B	ensure that the safety logic is functioning
F-E000b	R		systematic approach	B	ensure that the SL knows the request message type and that the message has a correct syntax
F-E001	R		systematic approach	B	ensure that all danger areas are identified (ensure that the risk of an undetected danger area is knsystematic approach)
F-E002	P	C	systematic approach	B	process train registration request

F-E002a	SF		ril 408	B	allocate vehicle identification numbers and change status of associated danger zones
F-E003	SF		systematic approach	T	unregister vehicle after leaving the controlled area
F-E003a	P	R	systematic approach	B	process "end of mission" notification
F-E004	P	U	systematic approach	C	process user input to ignore danger zones
F-E005	SF		systematic approach	M	monitor train position
F-E005a	R		systematic approach	M	in case of sudden disappearance / unreachability of a vehicle / train: ensure that - emergency measures are taken - both tracks are blocked
F-E006	P	R	systematic approach	B	process externally triggered status update of infrastructure attributes
F-E007	P	R	systematic approach	B	process train position report
F-E008	P	R	systematic approach	B	process train information updates
F-E009	P	C	systematic approach	B	process stakeholder list update
F-E034	R		systematic approach	B	ensure that passenger trains stop at a platform for timetable stops
F-E034a	R		ril 408	B	ensure that the platform is sufficiently long, otherwise F-E372
F-E035a	R		Lastenheft F1	B	ensure that switches (points) (or crossings) in the train route are not trailed
F-E035b	R		Lastenheft F1	B	ensure that switches (points) (or crossings) with swingnose crossing (moveable point frog) are not trailed
F-E035c	R		Lastenheft F1	B	ensure that switches (points) (or crossings) without swingnose crossing (moveable point frog) which are part of the overlap are not trailed if they are locked in the other direction than needed for the overlap
F-E035d	R		systematic approach	B	ensure that switches (points) (or crossings) with a closed point lock are not trailed if they are locked in the other direction than needed
F-E040	P	C	systematic approach	B	process status change requests for controlled track element
F-E040b	SF		systematic approach	B	register route or overlap occupancies
F-E042	SF		Lastenheft F1	B	set track element status to reset position

F-E045	R		Lastenheft F1	C	prevent status changes of locked track elements
F-E046	R		Lastenheft F1	C	prevent status changes if the element is part of a locked points operation sequence
F-E051	P	C	systematic approach	B	process movement authority request
F-E052	P	R	systematic approach	B	process ermergency stop request
F-E052a-new	R		Lastenheft F1	S, C	in case of human interaction: prevent message sequences that might be misinterpreted due to human perception.
F-E053	P	U	systematic approach	C	process manual movement authority withdrawal request
F-E054	R		ril 408	B	ensure that MAs are only issued to clearly identified vehicles
F-E055	SF		systematic approach	B	calculate speed profile (in 5 km/h steps according to ETCS)
F-E057	R		ril 408	B	ensure that a vehicle does not continue after a trip before the reason of the trip is knsystematic approach and it has a new (safe) MA
F-E059	P	C	systematic approach	B	process movement authority change request
F-E059a	R		systematic approach	B	ensure that vehicle confirms the new MA, is able to stop before the new EoA, and is able to follow all parameters of the new MA (e.g., speed profile)
F-E063	R		ril 408	Sh	ensure banking restrictions
F-E064	P	R	ril 408	Sh	process confirmation that train has been stabled at a defined position
F-E065	R		ril 408	Sh	ensure that vehicles are only been stabled in (suitable) areas with inclination <10 parts per thousand
F-E071	SF		ril 408	Sh	allow entering and leaving of locally controlled areas
F-E072	R		ril 408	Sh	ensure that vehicles that get a permission to enter a locally controlled area will follow all relevant information on F-B332
F-E073	R		systematic approach	Sh	ensure that all vehicles leaving a locally controlled area are detected
F-E074	P	R	systematic approach	Sh	process vehicle registration after leaving a locally controlled area
F-E075	R		ril 408	Sh	ensure that overhead line / catenary in loading zones is turned on only if - all personnell is informed and left dangerous areas - a vehicle needs it

F-E076	R		ril 408	Sh	prevent electric vehicles from entering a loading zone as long as the catenary is switched off
F-E077	SF		ril 408	Sh	swing the entrance switch to a loading zones with overhead line, after a vehicle left the loading track or a vehicle lowered its pantograph in the loading track so that it gives the loading track flank protection; switch off the overhead line (F-B632); wait for confirmation of the switch off process (F-B622)
F-E078	R		ril 408	Sh	ensure that loading work will only be approved in a track with overhead lines when it is switched off
F-E080	P	C	ril 408	Sh	process mode change requests (e.g. shunting)
F-E081	P	C	ril 408	Sh	process MA request for manual shunting (not ETCS-controlled vehicle)
F-E082	P	R	ril 408	Sh	process termination of manual shunting after receiving a hold message (F-B243) and a position report (F-B246) together with train complete message (F-B241) for the shunting unit
F-E084	R		ril 408	Sh	ensure the correct order of switch / point state changes for non supervised movements (the switch closest to the movement has to be the last switch to be swinged, the farest one the first)
F-E091	P	C	systematic approach	B	process train dividing request
F-E092	P	C	systematic approach	B	process train joining request
F-E093	P	C/R	systematic approach	Z	process vehicle transfer on track
F-E094	P	R	systematic approach	Z	process vehicle transfer from track
F-E101	R		ril 408	B	prevent the output of control commands to not clearly identified controlled track elements
F-E102	R		systematic approach	B	prevent the output of status change commands to controlled track elements whose status or state is unknsystematic approach
F-E103	R		systematic approach	B	prevent the output of control commands to controlled track elements whose status is not "ready for operation"
F-E104	R		Lastenheft F1	B	ensure that a point/switch with movable tip of point frog is not swinged after it has been trailed

F-E105	SF		systematic approach	B	send state requests to controlled track elements
F-E106	SF		systematic approach	B	send status requests to controlled track elements
F-E107	P	R	systematic approach	B	process status updates of controlled track elements
F-E108	P	R	systematic approach	B	process state reports of controlled track elements
F-E110	R		systematic approach	B	prevent controlled track elements from swinging while they are allocated to vehicles or vehicle movements
F-E111	R		Lastenheft F1	B	ensure that a non-clearance-mark-free insulated track element status (ie the areas of the clearance mark overlap) may only be changed if the other track element is free except the latter track element is a flank protection element for the element whose state is to be changed
F-E112	R		Lastenheft F1	B	ensure that a controlled track element may only change its state if no vehicle group can stretch itself in the clearance area around a switch
F-E112a	P	R	ril 408	F	process a clearance area free message
F-E115	R			F	ensure plausibility of clearance area free message
F-E121	R		systematic approach	B	prevent exceedings of the trackside/lineside speed limit
F-E121a	R		systematic approach	B	prevent exceedings of track element speed restrictions (e.g. by a switch)
F-E121b	R		systematic approach	B	ensure that differentiations of tilting train speed profile classes are communicated to the train
F-E122	R		systematic approach	B	ensure restrictions of restricted areas are observed (e.g. speed restrictions)
F-E122a	R		systematic approach	B	prevent vehicles from stopping in non stopping areas (NSA)
F-E122b	R		systematic approach	B	prevent vehicles from exceeding temporary speed limits
F-E129	R		systematic approach	B	ensure that implications on braking behavior due to snow and ice are included in braking calculations
F-E132	P	R	systematic approach	B	process vehicle failure reports
F-E132a	R		systematic approach	M	in case a hot box is detected: ensure that - the vehicle / train stops

F-E132b	P	R	systematic approach	B	process trackside monitoring system reports
F-E134	R		systematic approach	M	in case a sticking brake is detected: ensure that - the vehicle / train stops timely
F-E140	P	C	systematic approach	B	process change of global paramter request (e.g. friction, breaking distance, weather indicator)
F-E141	R		systematic approach	B	ensure that speed is reduced in exposed areas (W_STORM_IDENT = true) if allowable crosswind strength W_STORM_VMAX is exceeded
F-E142	R		ril 408	B	prevent chunks of ice on the rails by ice shedding, ensure restrictions of the MA when W_ICICLES_IDENT = true
F-E143	R		ril 408	B	ensure that speed in ice sheeding risk areas is restricted to W_ICESHEDDING_VMAX if ice shedding (F-B524) happens (W_ICESHEDDING_IDENT=true)
F-E144	R		ril 408	B	ensure that measures to handle flangeways are taken (first stop everything, after the OP_FLANGEWAY_ICY_TIME OP_FLANGEWAY_ICY_VMAX may be driven when the train is heavier than OP_FLANGEWAY_ICY_WEIGHT)
F-E145	R		ril 408	B	ensure that speed is limited to W_SNOW_VMAX if the operations center commands it (W_SNOW_IDENT = true)
F-E146	R		systematic approach	M	in case a broken rail is detected: ensure that - all vehicles / trains which are approaching the site stop
F-E147	R		systematic approach	M	in case of damage of the railroad embankment: ensure that - all vehicles / trains which are approaching the site stop
F-E148	R		ril 408	M	in case of a catenary damage report: ensure that - emergency measures are taken - a route reconnaissance and driving on sight is commanded
F-E201	SF		systematic approach	B	send position request to vehicle
F-E202	R		systematic approach	B	ensure that vehicle position reports are plausible (before relying on the information)
F-E203	R		systematic approach	B	ensure that vehicle locations are knsystematic approach and correct
F-E211	R		systematic approach	B	prevent vehicles from entering a danger zone unless it is explicitly intended

F-E212a	R		systematic approach	B	ensure vehicles cannot be stretched into track areas which are allocated by a train
F-E213	R		systematic approach	B	ensure that all potential obstacles are covered by a danger area
F-E214	R		ril 408	B	ensure that train detection system reports are plausible
F-E215a	R		Lastenheft F1	B	ensure that track element allocations/occupations are not removed as long as they are in use
F-E215b	R		systematic approach	B	in case of a MP Change Request: ensure that only vehicle occupations are deleted if the vehicle has confirmed that it will not use them
F-E216	R		systematic approach	B	ensure that vehicles stop at predefined stops which are marked as mandatory
F-E217	R		ril 408	B	ensure that all necessary approvals of external systems are valid before a MA is issued
F-E217a	R		ril 408	B	ensure that all necessary notifications (in accordance with rules in module 408.0421) are send before a MA is issued
F-E217b	R		ril 408	B	ensure that all necessary stakeholder notifications are sent
F-E218	R		Lastenheft F1	T	ensure that neighbouring control areas do not issue overlapping MAs
F-E219	R		Lastenheft F1	F	ensure that for MAs in modes of degraded operation (e.g. OS) all preconditions are true (see. Chapter Lastenheft F1), in particular that point operation sequences are disabled and level crossings are secured
F-E223	R		systematic approach	Z	prevent the meeting of two out-of-gauge loads which are not compatible to each other
F-E223a	R		ril 408	Z	ensure that no obstacle violate the clearance gauge (especially for vehicles with out-of-gauge loads
F-E223c	R		ril 408	Z	ensure for out-of-gauge loads that there are no special restrictions for them
F-E223d	R		ril 408	Z	ensure identication of out-of-gauge loads
F-E225	P	R	systematic approach	B	process danger prevention routine if driving bans are violated or unexpected vehicle movements are detected
F-E226	P	R	systematic approach	B	process danger prevention routine if the occupation of a (moving) vehicle is violated
F-E227	R		Lastenheft F1	B	ensure for any part of a MA's route that it is not part of the route of another active MA or part of an active overlap

F-E230	R		systematic approach	B	ensure flank protection
F-E230a	SF		ril 408	B	determine the flank protection area
F-E230b	SF		systematic approach	M	monitor the flank protection area
F-E230c	SF		systematic approach	B	registrate (flank protection) occupations
F-E230d	R		systematic approach	M	in case flank protection areas are violated: ensure measures are taken to avoid a possible collision
F-E230e	R		systematic approach	M	ensure flank protection areas are not vialated
F-E232a	R		Lastenheft F1	B	ensure that key locks in the flank protection area are locked and monitored
F-E236	R		systematic approach	B	ensure that the maximum permitted driving speed is reduced if flank protection cannot be guaranteed physically
F-E237	R		ril 408	Sh	ensure that shunting restrictions are not violated
F-E238	R		Lastenheft F1	B	ensure that a flank protection device which provides flank protection for several vehicle movements is not unlocked prematurely
F-E238a	SF		Lastenheft F1	B	remove occupations
F-E239	R		ril 408	B	ensure that no vehicles are able to reach tracks on which the presence of humans is (currently) allowed (e.g., construction works, lx or passenger lx)
F-E242	P	R	ril 408	F	process a track clearance message
F-E242a	R		ril 408	F	ensure that a track validation message is plausible
F-E246	P	U	systematic approach	C, F	process manual occupation deletion request
F-E251	R		systematic approach	B	ensure that all vehicles on the track are detected (ensure that the risk of an undetected vehicle is knsystematic approach)
F-E252	R		systematic approach	B	ensure that MAs do not contain any segments of its route that are occupied by anything else than a located vehicle
F-E252a	R		systematic approach	B	ensure that an undefined danger zone is defined around all unlocalized objects
F-E253	R		systematic approach	B	prevent violations of the clearance gauge by neighbouring vehicles (especially small vehicles, construction work vehicles)

F-E254	R		systematic approach	B	ensure that an undefined danger zone with unknsystematic approach occupancy status is defined if it is unclear whether the zone is occupied
F-E255	SF		systematic approach	M	monitor approval of mandatory approvals (of external systems)
F-E256	SF		systematic approach	M	monitor state ("ready") of external systems with mandatory approvals
F-E257	P	C	systematic approach	B	process stakeholder status change request for external systems such as LX (if safety relevant)
F-E258	P	R	systematic approach	B	process status reports of stakeholders
F-E259	P	R	systematic approach	B	process state reports of stakeholders
F-E260	SF		systematic approach	B	open and close railway level crossings
F-E262	SF		systematic approach	M	monitor the safety status of level crossings
F-E264	R		systematic approach	B	prevent the level crossings from exceeding the maximum closure time (LX_MAX-CLOSURE_TIME)
F-E265	R		systematic approach	B	prevent a MA to be issued across the level crossing if it has not been closed and marked free of objects
F-E266	SF		systematic approach	M	monitor status and state of a level crossing
F-E270	R		systematic approach	B	ensure that construction sites and construction material are adequately secured
F-E270a	SF		ril 408	B	process approval message by registered stakeholders (such as construction workers)
F-E270b	R		ril 408	B	ensure that construction works cannot interfere with active MAs
F-E275	R		systematic approach	B	ensure that no hazard exists due to lost load/cargo
F-E276	R		systematic approach	B	ensure that passenger and freight trains do not pass itself in tunnels if their relative speed difference exceeds P_TUNNEL_MAXDIFFSPEED
F-E281	SF		systematic approach	B	open and close tunnel entrance doors
F-E282	R		systematic approach	B	ensure animals are detected when entering closed areas (e.g. tunnels)
F-E311	R		systematic approach	B	ensure that all parts of the MA are navigable parts of the track topology and that the whole route is connected to each other

F-E312	R		systematic approach	B	ensure that vehicles are able to stop safely before end of tracks
F-E321	R		systematic approach	B	prevent trips to prohibited zones except if the train has a special permit
F-E321a	R		Lastenheft F1	F	ensure that a prohibited zone (closed track) is only be declared if there is no vehicle or MA active in the zone except for emergency reasons –> ensure that trains stop in the latter case except the danger is enlarged by stopping
F-E323	R		systematic approach	F	prevent vehicles from exceeding the maximum speed while entering prohibited zones (P_TC _ * _ VMAX)
F-E324	R		systematic approach	F	ensure flank protection for prohibited zones (closed tracks)
F-E330	R		systematic approach	B	ensure that impassable tracks are marked as prohibited zones (closed tracks)
F-E340	R		systematic approach	B	ensure that no MA includes controlled track elements with unsafe status
F-E350	R		systematic approach	B	prevent vehicles from entering tracks which are not made for them or in which they are not permitted
F-E351	R		systematic approach	B	prevent a vehicle from entering a BOStrab track if it is not allowed to use BOStrab tracks
F-E352	R		systematic approach	B	prevent a vehicle from entering a track which is equipped with a power system that is not available on the vehicle
F-E353	R		systematic approach	B	prevent a vehicle from entering a track with a wrong gauge
F-E354	R		ril 408	B	prevent a train from entering a track which is equipped with an ATP which is not available in the vehicle or limit its maximum speed on P_ATP-NA_VMAX (National Value) for driving without a train control system
F-E355	R		systematic approach	B	prevent a vehicle from entering a section of track for which it has no permission
F-E356	R		systematic approach	B	prevent a vehicle from entering a track for which the driver or ATO system has no permission
F-E357	R		systematic approach	B	prevent a vehicle from entering a track with a slope that exceeds the vehicles capability to brake timely
F-E357a	R		systematic approach	B	ensure vehicles have no planned stop in areas where they have little braking capability
F-E358	R		systematic approach	B	prevent a vehicle from entering a track for which it exceeds the maximum permissible axle load for its allowed speed

F-E359	R		systematic approach	B	prevent a vehicle from entering a track if its clearing gauge does not fit to the narrowest clearange gauge of that track
F-E361	R		systematic approach	B	prevent a vehicle without eddy current brake from moving on a track for which eddy current brake is mandatory
F-E362	R		systematic approach	B	prevent that a vehicle turns on eddy current brake, where this is not allowed
F-E363	R		systematic approach	B	prevent that further vehicle-side constraints are violated
F-E364	R		systematic approach	B	prevent a vehicle from entering a track where its breaking capability is not sufficient
F-E365	R		Lastenheft F1	B	ensure that no MA includes (parts of) active short range control areas
F-E366	R		ril 408	F	ensure that vmax is limited to P_PAX-TRAIN_NOT-ALLOWED_VMAX when a passenger train enters a track in which it is not authorized
F-E371	R		systematic approach	F	ensure that vmax is limited to P_TRACK-NOT-ALLOWED_VMAX when a vehicle is moving on a track on which it is not licenced, but it can use it physically
F-E372	R		ril 408	F	ensure there is a confirmation of the train driver if a passenger train should stop at a platform that is too short for it
F-E411	R		systematic approach	B	prevent dangerous lateral acceleration in point zones
F-E412	R		systematic approach	B	ensure adequat speeds while passing S curves
F-E422	R		systematic approach	O	ensure that the operating acceleration and braking curves are adjusted
F-E431	R		systematic approach	B	prevent doors from opening while the train does not stand at the platform
F-E432	R		systematic approach	B	ensure that additional footsteps are (only) moved out when they are necessary and not forbidden (task safety logic: provide information)
F-E510	R		systematic approach	B	prevent to raise the pantograph untimely
F-E511	SF		systematic approach	B	send information where to lift or lower the pantograph
F-E512	R		Lastenheft F1	B	ensure that hybrid trains have lowered their pantograph when they drive into an area without catenary
F-E513	R		ril 408	B	ensure that vehicles with raised pantograph only enter tracks in which catenary does exist, is switched on and is not out of order

F-E515	R		ril 408	B, F	ensure that the pantograph is lowered while the vehicle passes a track area in which the catenary is out of order, monitor maximum speed (P_PANTOGRAPH-Dsystematic approach_VMAX)
F-E531	R		systematic approach	Z	ensure that the snow plow is lifted where this is mandatory
F-E532	SF		systematic approach	Z	send information where to lift or lower the snow plow
F-E533	R		systematic approach	Z	Ensure that snow plows do not enter areas where they are not allowed
F-E534	R		systematic approach	Z	ensure that there are no MAs on neighbouring tracks when a snow plow is passing
F-E540	R		systematic approach	B	prevent unsafe operation of the eddy current brake
F-E541	R		systematic approach	B	ensure that information about route sections on which the eddy current brake must not be used is submitted to the vehicle
F-E542	R		systematic approach	B	ensure that information on existing eddy current brakes are included in the speed profile calculation of MA requests
F-E611	SF		systematic approach	B	open and close passenger level crossings (between platforms)
F-E611a	R		systematic approach	B	ensure that passenger level crossings are closed as long as the corresponding track is allocated by a train
F-E613	R		systematic approach	B	prevent MAs which include route elements with a passenger level crossing between platforms which is not closed and cleared
F-E631	R		systematic approach	B	prevent MAs with a route through a construction zone if the construction zone is not cleared
F-E632	R		systematic approach	B	ensure that the MA does not exceed speed limits in construction areas
F-E641	R		systematic approach	B	ensure that the MA does not exceed speed limits in platform areas or loading docks
F-E642	R		systematic approach	B	ensure that people at a platform are warned if a MA is issued to a train which is allowed to pass a platform with more than {TRAINTYPE|OP_CAUTION_VMAX}, otherwise ensure that the speed is reduced to {TRAINTYPE|OP_CAUTION-INACTIVE_VMAX}
F-E644	R		ril 408	B	ensure that the vehicle sends all obligatory warnings (e.g. whistling, ringing the bell)
F-E700	P	R	systematic approach	B	process emergency track occupation report

F-E700a	R		systematic approach	M	in case of an emergency stop request: ensure that - all vehicles / trains in the relevant area stop immediately
F-E701	P	R	ril 408	B	process pantograph / catenary failure report
F-E701a	R		ril 408	M	in case of a pantograph problem (e.g., damaged upscale pantograph, restless pantograph skiing, dining car with an upscale pantograph) (via interface F-B255): ensure that - measures in case of danger are taken - the electricity control center is informed (F-B612) - the train driver is informed
F-E702	P	R	ril 408	B	process fire detection report
F-E702a	R		ril 408	M	in case a fire is reported (F-B721): ensure that - measures in case of danger are taken - the vehicle / train stops as soon as possible; if possible not in tunnels or other non stopping areas or in places where the assistance is difficult; if possible, stop on a track without catenary, not in close proximity to catenary masts or landscape structures; In the tunnel: specify the direction of alignment (F-B322) and ensure feedback to the system (F-B321) - all vehicles / trains which are approaching the site are stopped if this does not enlarge the danger - no vehicles pass the site until the problem is solved
F-E703	R		ril 408	M	in case of a train evacuation is reported: ensure that - adjacent tracks are blocked
F-E704a	R		ril 408	B	ensure in case of reduced coefficient of friction (F-B248): - extend the danger zone to train - communicate fact to train driver of the following train
F-E704b	R		ril 408	B	ensure in case of prolonged braking distance (F-B248): - increase risk area - communicate fact to driver driver of the following train

F-E706	R		ril 408	M	in case a vehicle / train has not been tracked for more than T_LOST_TIME and no position report of train driver / ATO system has been received (F-B245): ensure that - the operator is notified that inquiries are necessary - all trains which are approaching the site are stopped - all necessary stakeholders are informed
F-E707	R		ril 408	M, T	in case a vehicle / train that was considered lost (expired T_LOST_TIME) shows up again: ensure that - it proceeds onsight if it is travelling to an area outside the smart logic area - the issue is reported to the interface for line messages (F-B110)
F-E709	P	R	systematic approach	B	process train separation report
F-E709a	R		ril 408	M	in case a train was separated unexpectedly: ensure that - a new danger zone is defined around the second part of a train that is separated unexpectedly (F-B249) and treat it as special (moving) danger zone; - all necessary stakeholders are informed
F-E710	SF		ril 408	F	send new MAs to both parts after a train was separated (train separation message F-B249) if both parts are still mobile; inform stakeholders
F-E711	R		ril 408	M	in case of emergency in which a stop would enlarge the danger: ensure that - a MA in mode "REVERSING" is processed
F-E712	R		ril 408	M	ensure for measures in case of danger: - stop all vehicles / trains that are endangered if this does not increase the risk (this needs to be tested, e.g. in case of a burning train in a tunnel, stopping would increase the risk) - check if another (neighboring) track is affected: If yes, extend the danger zone of the train on the other track and stop approaching trains; - inform registered stakeholders
F-E713	SF		ril 408	M	process an end routine for measures in case of danger (at F-B713)
F-E715	P	R	ril 408	B	process dead head signal report

F-E715a	R		ril 408	M	in case a dead head signal is reported: ensure that - the vehicle / train stops at the nearest station; - the vehicle / train stops immediately in case – the vehicle / train has to cross not technically-secured level crossings, – of darkness – limited visibility (e.g. due to bad weather) - the train driver is informed or in case of ATO goa 3 the service staff - all registered stakeholders are informed
F-E716	P	R	ril 408	B	process uncomplete head signal report
F-E716a	R		ril 408	M	in case an uncomplete head signal is reported (message via interface F-B212): ensure that - the vehicle stops at the nearest station (where the problem can be solved); in case - the vehicle / train has to pass not technically-secured level crossings - darkness - poor visibility (e.g. due to bad weather): ensure that - the vehicle / train stops at next station - all registered stakeholders are informed on interface F-B214 (e.g., neighbouring stations and stops, guards, etc.)
F-E717	P	R	ril 408	B, T	process missing end of train marker report
F-E717a	R		ril 408	M, T	in case of the absence of an end of train marker (message via interface F-B213): ensure that - the vehicle / train stops at the next suitable point; - a report is sent on F-B214; - if the vehicle / train enters a track section without trackside detection system, it is stopped before it leaves the smartLogic area - the train driver and maintenance personnel is informed - if the train is manually declared complete (which is assumend in automaticly controlled areas): the end of train marker was added and afterwards a "ready message" or "train complete message" was sent
F-E718	P	R	ril 408	B	process open door report
F-E718a	R		ril 408	M	in case an open door of a passenger train is reported: ensure that - the issue is reported to train driver or ATO system - the train stops if communication is impossible

F-E719	P	R	ril 408	B	process unsecured load report
F-E719a	R		ril 408	M	in case an open door of a freight train or unsecured load is reported: ensure that - the issue is reported to the train driver or ATO system - the train stops
F-E720	P	R	ril 408	B	process vehicle abnormality report
F-E720a	R		ril 408	M	in case an abnormality was detected that endangers a vehicle / train: ensure that - the vehicle stops
F-E721	R		ril 408	B, F	ensure speed is limited to P_POINTS-SIGNAL-INTERLOCKING_NA_VMAX if technical saftey is not ensured
F-E722	R		ril 408	B, F	ensure speed is limited to 5 km / h if the vehicle passes a point/switch which is just manually locked EXCEPTION: The point is monitored via F-B344
F-E723	R		ril 408	F	prevent (as far as possible) that points/switches which are trailed will be yielded against the direction in which they were trailed
F-E724	SF		ril 408	M	process measures in case of danger if a sudden failure occurs at a level crossing (indicates an accident at the level crossing)
F-E725a	R		ril 408	M	ensure opening of level crossing if F-B731 reports people detected within a closed lx and trains that were heading to the lx confirm that they have stopped or are able to stop before they reach the lx
F-E726	R		ril 408	B	ensure pantograph is lowered where it is necessary
F-E726a	R		ril 408	B, F	ensure the panthograph is lowered if the vehicle drives through a (short) non-electrified section, resp. a section in which the catenary does not work normal
F-E727	P	R	systematic approach	B	process infrastructure failure report
F-E727a	R		systematic approach	M	in case of an infrastructure failure ensure that - measures for infrastructure failure are taken
F-E741	P	R	ril 408	B	process weather detection system failure report

F-E741a	R		ril 408	M	in case of a weather system failure report: ensure that - the speed is limited to V_[WEATHERSYSTEM]_SYSTEMTIMEOUT after a time T_[WEATHERSYSTEM]_SYSTEMTIMEOUT if the weather informationen has not been updated via (F-B511)
F-E742	SF		systematic approach	F	identify train radio timeout and process defined measures for that case
F-E742a	R		systematic approach	F	ensure sufficient measures for trains without functional train radio or in case of a disturbed train radio
F-E743	SF		ril 408	F	process alternative measures if a necessary notification failed
F-E744	SF		ril 408	F	process alternative measures in case of not fully operating ETCS
F-E745	SF		ril 408	F	process alternative measures if a controlled track element does not work probably
F-E745a	SF		systematic approach	M	monitor stakeholder availability
F-E745b	P	R	systematic approach	B	process stakeholder failure report
F-E745c	P	R	systematic approach	B	process controlled element failure report
F-E746	P	R	ril 408	F	process "train complete" message
F-E747	SF		ril 408	F	process alternative measures if a level crossing must be passed which is not correctly secured
F-E750	R		systematic approach	B, M	in case a dangerous event occurs: ensure that - no vehicle / train passes the site of the dangerous event - no MA is issued through those sites
F-E751	SF		ril 408	F	generate written instructions
F-E752	SF		ril 408	F	retract a written instruction
F-E781	SF		ril 408	F, T	coordinate with neighboring control areas in case of vehicles enter closed sections of a line which are partly controlled by a neighboring control area
F-E782	SF		ril 408	F	allow to send a MA to a vehicle without radio to enter a closed section of a line
F-E785	R		ril 408	F, T	ensure a vehicle gets written instruction 14 (signals do not apply) if it gets a MA for sections of a line that are uncontrolled
F-E787	SF		ril 408	T	inform neighboring operating points about changes of the traction of a vehicle

F-E788	SF		ril 408	O	Inform neighboring operating points about changes of the order of vehicles
F-E799	P	R	systematic approach	B	process emergency message revocation
F-E801	P	U	systematic approach, ril 408	S	connect stakeholder
F-E802	P	U	systematic approach, ril 408	S	disconnect stakeholder
F-E803	R		systematic approach, ril 408	S	prevent sending messages to unauthorized stakeholders
F-E804	R		systematic approach, ril 408	S	prevent processing of messages from unauthorized stakeholders
F-E805	R		systematic approach	S	prevent processing of ambigous or unplausible messages
F-E806a	P	C	systematic approach	S	process area of responsibility change request
F-E806b	P	C	systematic approach	S	process control area change request
F-E807	P	C	systematic approach	S	process infrastructure update
F-E810	R		systematic approach	S	ensure that the system is working properly during all safety critical actions
F-E810a	SF		systematic approach	S	process self test
F-E812	R		systematic approach	S	ensure consistent operating status (e.g. after blackout)
F-E820	P	C	systematic approach	S, C	process turning on the automatic operation
F-E821	P	C	systematic approach	S, C	process turning off the automatic operation
F-E830	R		systematic approach	S	ensure that all external systems have subscribed to all necessary interfaces
F-E840	R		systematic approach	S	prevent to communicate an uncorrect system status
F-E840a	R		systematic approach	S	prevent to communicate an ambigous system status
F-E840b	R		systematic approach	S	ensure to communicate all safety relevant information to all registered stakeholders
F-E842	R		systematic approach	S, C	ensure that critical command inputs originate from the operator
F-E843	R		systematic approach	S, C	ensure that the operator has reflected critical command inputs probably

F-E896	P	U	systematic approach	C	insert special information for locally controlled area
F-E897	P	U	systematic approach	C	delete special information for locally controlled area
F-E898	P	C	systematic approach	B, C	insert restriction
F-E899	P	C	systematic approach	B, C	update restriction
F-E900	P	Internal	ril 408	P	log all necessary events

Anlage 3: Fehlercodes

Das Zeichen ‚#' fungiert als Platzhalter für einen Bezeichner.

- 000 - Message-Syntax incorrect
- 001 - smartLogic SelfCheck unsuccessful
- 002 - TMS not identified
- 003 - Train ID not identified
- 004 - Route element(s) # has/have incorrect status and is/are already prereserved
- 005 - CTEStatusRequest timed out for element(s) #
- 006 - Element status of element(s) # unequal requested status ""
- 007 - Element(s) # could not be locked
- 008 - TopologyRequest timed out
- 009 - Not all necessary route elements are part of the MPRequest
- 010 - There is no route that corresponds with the MPRequest
- 011 - RegisteredDangerZonesRequest timed out
- 012 - A registered danger zone blocks the requested route
- 013 - TrainStatusRequest timed out
- 014 - Train characteristics does unequal expected characteristics
- 015 - Train does not fulfil route criteria
- 016 - StakeholderListRequest timed out
- 017 - StakeholderStatusRequest timed out for stakeholder #
- 018 - Stakeholder # cannot approve MPRequest
- 019 - StakeholderApprovalRequest timed out for stakeholder #
- 021 - StakeholderNotificationMessage timed out
- 022 - RegisteredDangerZonesRequest timed out while trying to set up flank protection
- 023 - ElementStatusRequest timed out for element # while trying to set up flank protection
- 024 - Element # was requested but cannot give flank protection
- 025 - Acknowlegement of MA failed
- 026 - FlankProtectioRequest timed out for element #
- 027 - ElementStateRequest timed out for element #
- 028 - ElementStatusRequest timed out for element #
- 029 - Requested MA for MOB # restricts active MA of this MOB --> Use MPChangeRequest instead

- 030 - RouteExistenceAndTrafficabilityCheck failed - Route does not exist
- 031 - Start point not on route
- 032 - end point (last target point) not on route
- 033 - track edge # not connected with track edge #
- 034 - connection between track edge # and track edge # is not trafficable
- 035 - route element # has not the required status

- 040 - The train does not support required atp(s) #
- 041 - The train does not support the required gauge
- 042 - The train has no supported traction system

- 043 - The train does not support the required communication system #
- 044 - The train's breaking capability is insufficient
- 045 - The train does not suit the clearance gauge of the track at section of line #
- 046 - The train's axle load is to heavy for the requested track at section of line #
- 047 - Vehicle # is not allowed at track zone #
- 048 - The train category # is not allowed on the whole or a part of the requested track
- 049 - The train does not fulfil one or several special track requirements such as eddy current brake, etc.

- 050 - StaticSpeedProfile incorrect
- 051 - line speed at location # exceeded
- 052 - topology related maximum speed at location # exceeded
- 053 - track zone speed of zone # exceeded
- 054 - RA speed restriction # exceeded
- 055 - DA speed restriction at location # exceeded

- 060 - The MP-Request contains an unpassable zone (#.begin to #.end) that was requested by stakeholder #
- 061 - The MP-Request contains a construction area (#.begin to #.end) that cannot be passed
- 062 - The MP-Request contains an area (#.begin to #.end) which was automatically blocked by #
- 063 - The MP-Request contains an area (#.begin to #.end) which was manually blocked by #
- 064 - At least a part of the MP-Request is blocked by an undefined danger zone (#.begin to #.end) with id #.id
- 065 - At least a part of the MP-Request (#.begin to #.end) is occupied by vehicle #
- 066 - At least a part of the MP-Request (#.begin to #.end) is occupied by the MA of train movement #
- 067 - At least a part of the MP-Request (#.begin to #.end) is blocked by another MPRequest (id = #.id) and the waiting process timed out after # ms

- 070 - The begin of the requested route is not part of the specified smartLogicArea
- 071 - The end of the requested route is not part of the specified smartLogicArea
- 072 - At least one TrackEdgeSection of the Route (nr #) is not part of the specified smartLogicArea
- 073 - There is no connection from TrackEdge # to TrackEdge #
- 074 - The connection between TrackEdge # and TrackEdge # is not navigable
- 075 - The MovableObject would have to change its direction to use the connection between TrackEdge # and TrackEdge #
- 076 - There is no waypoint connected to the connection between TrackEdge # and TrackEdge #
- 077 - Set of points / Switch # has not the right status and is not trailable

- 078 - Set of points / Switch # has not the right status and does not lie between the EoA and SvL

- 080 - target point # is not located on the route
- 081 - target point # is located in a not fully supervised track zone
- 082 - probability to reach potential hazard point # in front of target point # is too high

- 090 - MA does not contain all relevant platform information
- 091 - MA does not contain all relevant gradient information
- 092 - MA does not contain all relevant eddy current brake exclusion zone information
- 093 - MA does not contain all relevant pantograph orders
- 094 - MA does not contain all relevant snow plow orders
- 095 - MA does not contain all relevant track zones with reduced friction
- 096 - Obligatory vehicle warning # is missing in MA
- 097 - MA does not contain all relevant trackside restrictions of vehicle functions

- 099 - Overall protection rate for MP-Request # is too low due to # {an unknown problem}. The request has been rejected.

- 101 - CTE # is unknown
- 102 - CTE # is internally locked and could not be unlocked
- 103 - CTE # is operationally locked
- 104 - CTE # is blocked by RA #
- 105 - CTE # not in state "operational"
- 106 - CTE # has status "trailed"
- 107 - CTE # is blocked at the field element
- 108 - DPS of CTE # is covered by vehicle #
- 109 - DPS of CTE # is covered by a MA for MOB #
- 110 - CTE # gives flank protection for vehicle #. The requested status change would lower the protection rate below a critical level.
- 111 - CTE # is occupied by occupation #
- 112 - Overall protection rate for TESC-Request # is too low due to # {an unknown problem}. The request has been rejected.
- 113 - TESC-Command for CTE # timed out
- 114 - CTE # has not DPS
- 115 - CTE # has no AS
- 116 - DBD-Server cannot change status of CTE #

- 200 - RA could not be deleted or modified because the Deletion Conditions are not fulfilled

Anlage 4: Auswertung Unfalluntersuchungen

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer	
1	09.06.2013	Güterzug	Zugentgleisung wegen Gleislagefehler	mehrere kurz hintereinander liegende Gleislagefehler in der Längshöhe. Nicht bzw. ein-geschränkt funktionierende Entwässerung des Gleiskörpers; fehlerhaftes Detektieren der Gleislagefehler, falsche Gefahreneinschätzung der Gleislagefehler	nicht definiert	EIU - IH	Versagen des Bahnkörpers	keine	
2	18.06.2015	Rangiertriebfahr	Auffahrunfall	zu spät eingeleiteter Bremsvorgang der Rangierfahrt	Triebfahrzeugführer der Rangierlok	EVU - RTf	Fahrfehler	keine	
3	20.11.2015	Güterzug, abgest	Auffahrunfall	mangelhafte Vorbereitung des Fahrwegs. Freisein des Fahrgleises wurde nicht geprüft	Fahrdienstleiter des Stellwerks	EIU - Fdl	fehlerhafte Fahrwegprüfung	keine	1 Wiederholung
4	09.10.2015	Personenzug	Zugentgleisung wegen Überpufferung	Überpufferung durch mangelde Signalbeobachtung durch den Tf. Zs 6 wurde übersehen und mit überhöhter Geschwindigkeit in die Weichenverbindung gefahren. Nach Halt Hp1 statt Hp2 erkannt und zu sehr beschleunigt. Entgleisung in der anschließenden Weichenverbindung	Triebfahrzeugführer der Rangierlok	EVU - Tf	Fahrfehler, Lücke in der PZB	keine	
5	13.12.2012	Güterzug	Zugentgleisung wegen Gleislagefehler	Schwingungen durch Längshöhenfehler bis zum Verlust des Rad-Schiene-Kontaktes und somit zur Entgleisung. Ursache vermutlich Unterbau, jedoch noch nicht sicher festgestellt	nicht definiert	EIU - IH	Versagen des Bahnkörpers	keine	1 Wiederholung
6	19.04.2015	Personenzug	Zugentgleisung wegen unzeitiger Weichenbedienung	spitz befahrene Weiche wurde umgestellt, obwohl diese noch besetzt war; Zs1 bedient; fehlende Räumungsprüfung; Fahrweg vor Ersatzsignalbedienung nicht richtig eingestellt und gesichert	Fahrdienstleiter des Stellwerks	EVU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	7 Wiederholungen
7	07.05.2014	S-Bahn, Zweiweg	Auffahrunfall	Auslegearm des Zweiwegebaggers in nicht gesperrtem Gleisbereich geschwenkt. Nicht gesperrtes Gleis trotz Baustelle. Einer von mehren Mängeln auf der Baustelle. Betra und Sicherungsplan waren nicht aufeinander abgestimmt	nicht definiert/unklar	EIU - Bauplaner / Baufirma	Fehlerhafte Bauplanung, Fehlerhafte Baudurchführung	keine	
8	28.06.2014	Güterzüge	Auffahrunfall	Zurückrollen auf freier Strecke und Kollision mit Zug vor Halt zeigendem Signal . Zurückrollen ermöglicht durch unter Alkoholeinfluss stehenden Tf	Triebfahrzeugführer des zurückrollenden Güterzuges	EVU - Tf	Fahrfehler, Alkohol	keine	
9	31.01.2015	S-Bahn	Personenschaden	Person wurde in sich schließender Tür mit der Hand festgeklemmt. Wurde im Dunkeln von Tf nicht bemerkt, da Türen per Leuchtsignal ordnungsgemäße Schließung vermittelten. Einklemmen kleiner Gegenstände kann von Tür nicht detektiert werden. SAT wurde (fehlerhaft) durchgeführt. Fahrt mit einkeklemmter Person wurde trotzdem eingeleitet	nicht definiert	EVU - Tf	Fehlerhafte Zugabfertigung	1	
10	10.06.2015	Personenzug	BÜ-Unfall	Fahrer des Kleintransports hat Vorrang des Schienenverkehrs missachtet und fuhr in BÜ (ohne technische Sicherung) ein. Eventuell verursacht durch fehlende Haltelinien und Geschwindigkeitsmessanlagen.	Fahrer des Kleintransporters	Individualverkehr	BÜ missachtet	keine	
11	05.09.2013	IC, Rangierfahrt	Frontalzusammenstoß	IC hatte Einfahrt, die über bestimmte Weiche führte, Rangierfahrt fuhr am haltzeigenden Sperrsignal vorbei bis zur besagten Weiche, was zur Kollision führte.	Triebfahrzeugführer der Rangierlok	EVU - RTf	Sperrsignal missachtet; fehlender physischer Flankenschutz	keine	
12	19.01.2014	Güterzug	Zugentgleisung wegen mechanischer Störung	Heißläufer am Wagen, was zum Bruch des Wellenschenkels am (rechten hinteren) Radsatz führte. HOA sind nicht angesprungen	nicht definiert	keiner	Heißläufer, undetektiert	keine	7 Wiederholungen
13	10.07.2014	Güterzug	Zugentgleisung wegen Gleislagefehler	Fahrstraße wurde trotz bekannter Weichenstörung zugelassen. Weiche kam nicht in Endlage und führte zu Entgleisung	Fahrdienstleiter des Stellwerks	EIU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	1 Wiederholung
14	29.10.2014	Güterwagen	Wagenentgleisung	Wagen wurde bei Zugbildung durch automatisierte Zugbildungsanlage trotz Verbot abgedrückt und entgleiste bei Aufprall auf vorigen Wagen im Richtungsgleis; Entgleisung wurde von Kuppler und Wagenmeister übersehen.	Rangierpersonal	Rangierpersonal	Fehlerhafte Bremsprobe / Zugbildung	keine	
15	02.12.2014	S-Bahn, PKW	BÜ-Unfall	Technische Sicherung des BÜ war außer Betrieb und wurde durch Bahnübergangsposten und zwei Hilfeposten ersetzt. Doch zum Unfallzeitpunkt war eine Seite des BÜ ungesichert. Das Geben von Zeichen durch die Posten zum Anhalten der Straßenbenutzer wurde vernachlässigt	nicht definiert	EIU - BÜP	BÜP-Fehler	keine	

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer	
16	01.08.2014	Güterzug, EC	Flankenfahrt	Tf des Güterzuges fährt an Halt zeigendem Zwischensignal vorbei, da er sich fälschlicherweise an links stehenden statt an rechts stehenden Signalen orientiert. Zug erfährt deshalb eine 2000 Hz-Beeinflussung. Tf löst Zwangsbremsung jedoch ohne vorgeschriebene Verbindungsaufnahme mit Fdl auf und setzt Fahrt fort. Fährt an weiteren Halt zeigenden Lichtsperrsignalen vorbei, bis er dem EC in die Flanke fährt.	Tf des Güterzugs	EVU - Tf	Fehlerhaftes Verhalten nach Zwangsbremsung	keine	
17	15.05.2014	Personenzug	BÜ-Unfall	Nichtbeachtung der StVO. An einem nicht-technisch gesicherten BÜ wurde nicht vor dem Andreaskreuz gehalten und trotz Vorrang des Zuges der BÜ befahren, was zur Kollision führte	Fahrer des PKW	Individualverkehr	BÜ missachtet	keine	
18	28.02.2014	Personenzug	BÜ-Unfall	aus ungeklärten Gründen missachtete ein PKW Fahrer das rote Blinklicht der technischen BÜ-Sicherung	Fahrer des PKW	Individualverkehr	BÜ missachtet		1 2 Wiederholung
19	14.02.2013	Güterzug	Zugentgleisung wegen mechanischer Störung	angelegte Feststellbremse an hinterer Wageneinheit, was zu starkem Materialabtrieb und -auftragung führte. Radsatz konnte sich nicht mehr in der Spur halten und entgleiste. Warum Feststellbremse angezogen war, ist nicht bekannt.	unklar	unklar	Fehlerhafte Bremsprobe	keine	
20	12.09.2015	Personenzug	BÜ-Unfall	geschlossene Halbschranken wurden von PKW Fahrer umfahren und der PKW anschließend erfasst	Fahrer des PKW	Individualverkehr	BÜ missachtet		5
21	13.11.2014	Personenzug, Ba	Auffahrunfall	Der Wagen der Rangierabteilung stand bei der signalmäßig durchgeführten Einfahrt der Regionalbahn nach Gleis 1 nicht grenzeichenfrei auf der Weiche. Das Entfernen der Sh 2 Scheibe wurde ohne Zustimmung des Technischen Berechtigten vorgenommen. Außerdem wurden die Vorgaben des Arbeitens mit Fahrzeugen im Bereich zwischen Fahrwegweiche und Wärterhaltscheibe nicht eingehalten.	nicht definiert	EVU - RTf	Fahrfehler	keine	
22	25.07.2015	Personenzug	Zugkollision	Bei einem Sturm prallte der Zug gegen einen an der Oberleitung hängenden Ast	nicht definiert	keiner	Kollision mit Gegenstand	keine	
23	26.10.2013	Güterzüge	Flankenfahrt	Durch ungenügende Bremswirkung wegen geschlossenem Luftabsperrhahn in der Hauptluftleitung kam der Güterzug weder am haltzeigenden Ausfahrvor- noch -hauptsignal zum stehen. Zug kollidiert mittig mit dem in Gegenrichtung einfahrenden Güterzug. Ausführung der Bremsprobe war mangelhaft.	Tf des Güterzugs	EVU - Tf	Fehlerhafte Bremsprobe	keine	1 Wiederholung
24	20.03.2014	Güterzug	Zugentgleisung	In einem Rechtsbogen entgleiste der Zug durch eine einseitige Belastung der Fahrzeuge auf der rechten Seite; Der Zugverband bestand aus einer unzulässigen Konfiguration und die Hauptluftleitung war nicht durchgängig; Die PZB war unzulässigerweise abgeschaltet	Tf des Güterzugs	EVU - Tf	Fehlerhafte Beladung	keine	
25	13.04.2012	Personenzug, Zw	Auffahrunfall	Aufgrund einer Gleisverwechslung wurde das Zweiwegefahrzeug in das nicht gesperrte Streckengleis eingegleist. Auf diesem verkehrte ein Personenzug, der mit dem Bagger kollidierte. Beide Besatzungsmitglieder des Zweiwegefahrzeugs waren nicht ortskundig und mglw. nicht eingewiesen, allerdings ist strittig, dass dies notwendig gewesen wäre. In der Betra fehlt ein drittes Gleis einer benachbarten Strecke in der maßgeblichen Zeichnung	EF, AZF	EVU - Kleinwagenbesatzung	Fehlerhafte Bauplanung, Fehlerhafte Baudurchführung		3
26	02.07.2013	Güterzug	Zugentgleisung	Durch unzulässige Spurerweiterung wegen biologischem Zerfall der Holzschwellen, entgleisten vier Wagen des Güterzuges.	nicht definiert	EIU - IH	Versagen des Bahnkörpers	keine	
27	24.07.2012 29.09.2012	IC	Zugentgleisung wegen Überpufferung	Versagen von Puffern an dem im Zugverband laufenden WRmz-Wagen. Federkennlinien der Puffer lagen außerhalb der festgelegten Bereiche und zugelassene Anfahrdruckkräfte waren zu hoch, weshalb der Zug entgleiste	nicht definiert	EVU - IH	Fahrzeugmangel, Fehlerhafte Fahrzeugwartung	keine	1 Wiederholung

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer	
28	19.12.2012	Güterzug, Linienl	BÜ-Unfall + anschließende Kollision	Fahrer des Busses hat BÜ bei ausgeschalteter BÜSA befahren und konnte den Kreuzungsbereich wegen technischem Defekt am Fahrzeug nicht rechtzeitug räumen. BÜSA wurde bei Annäherung der Züge eingeschaltet, jedoch war Bus bereits auf der Strecke. Systembedingt konnten Tfs nicht mehr anhalten und es kam zum Aufprall. Zweite Kollision kam zu Stande, da sich der erste Güterzug nach Aufprall und auch der Bus im Gegengleis befanden.	Linienbus	Vorgaben	Keine BÜ-Freimeldung	keine	
29	04.07.2010	Güterzug (Kessel	Zuentgleisung wegen Überladung	Das sich im Kesselwagen befindliche Marmormehl schaukelte sich beim Befahren mehrerer Weichen auf und führte zu kritischer Radentlastung. Zusätzlich begünstigten Schädigungen im Drehgestell aufgrund fehlerhafter Schweißnähte die Entgleisung. Hauptursache war jedoch die zu hohe Beladung des Kesselwagens. Notwendige Beschränkungen für Kesselwagen und das bestimmt Ladegut gab es bis dato jedoch nicht.	unklar	Vorgaben, EVU - IH	Fehlerhafte Beladung	keine	
30	26.07.2010	Güterzug	Zugentgleisung durch losen Radreifen	Durch losen Radreifen am linken Rad entgleiste der Wagen und stürzte um. Vermessen hat ergeben, dass das Schrumpfmaß zwischen Radreifen und Radkörper zu klein bemessen war. Zusätzlich hat die Formschlüssigkeit der Schrumpfverbindung nur an den Außenkanten der Radfelge gewirkt.	nicht definiert	EVU	Fahrzeugmangel	keine	1 Wiederholung
31	08.04.2011	Güterzug	Zugentgleisung wegen Gleislagefehler	Die Gleislagefehler waren Mängel bei der Längshöhe, der gegenseitigen Höhenlagen (Querhöhe) und der daraus resultierenden Gleisverwindung. Genauer: Aufgrund der Gleislagefehler in der Schlammstelle kam es in der Linkskrümmung zur Entlastung des rechten vorderen Rades des Triebfahrzeuges, weshalb eine Entgleisung folgte. Erforderliche Inspektionen wurden mindestens 6 Tage zu spät durchgeführt, weshalb Gleislagefehler mit hoher Wahrscheinlihkeit gefunden worden wäre.	unklar	EIU - IH	Versagen des Bahnkörpers	keine	
32	13.01.2012	Personenzug	Zugkollision	Trotz eingeleiteter Schnellbremsung kollidierte der DPN mit einer entlaufenen Rinderherde. Dunkelheit erschwerte eine frühzeitige Erkennung der Herde.	nicht der Eisenbahnbetrieb	keiner	Kollision mit Gegenstand	1+14 Tiere (Rinder)	
33	11.09.2011	IC	Zugkollision	IC kollidierte bei unwetterartigen Regenfällen mit einem Murgang, der durch Schlamm- und Geröllmassen eines im Hang befindlichen Gerinnes ausgelöst wurde. Murgangbarrieren wurden erst nach dem Unfall aufgestellt.	nicht definiert	keiner	Erdrutsch	keine	
34	20.05.2011	Güterzug (TEC)	Zugentgleisung wegen mechanischer Störung	Entgleisung durch Radschienenbruch am Radsatz (des Wagen 17). Rissentstehung vermutlich durch thermische Überanspruchung (durch überschleifende Bremsklotzsohle)	nicht definiert	EVU - IH	Heißläufer, undetektiert	keine	
35	12.11.2007	ICE	Personenschaden	Wegen mangelhafter Fahrwegsicherung und Fehlverhalten der Mitarbeiter, die Schweißarbeiten in planmäßigen Pausen im Gleis durchführten, wurde ein Mitarbeiter vom ICE erfasst. Fdl erteilte Zustimmung zur Fahrt, obwohl die Weiche noch gesperrt war. Fahrweg war nicht gesichert.	Fahrdienstleiter des Stellwerks	EIU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb		1
36	20.09.2011	Personenzug	BÜ-Unfall	Ein, durch Zusammenstoß mit einem Transporter, im Gleisbereich stehender Pkw kollidierte mit der RE. Ursache war der Auffahrunfall durch den Transporter. Nach Aufprall schlossen sich die Schranken für die Zugfahrt und die Kollision war unausweichlich.	Fahrer des Transporters	Vorgaben	Keine BÜ-Freimeldung	keine	
37	01.11.2006	Güterzug	Zugkollision	Aufgrund mangelnder Kommunikation zwischen Betriebsstelle und Rangierpersonal verließ die Rangierabteilung das Baugleis ohne Zustimmung des Fdl und prallte im Bereich der Kreuzung mit einem Güterzug zusammen.	Rangierabteilung	EVU - RTf	Sperrsignal missachtet; fehlender physischer Flankenschutz	keine	
38	17.08.2010	ICE	Zugkollision	Ein von der Straße abgekommenes Müllentsorgungsfahrzeug stürzte eine Böschung hinuter auf die Gleise. Daraufhin kollidierte der ICE und entgleiste teilweise. Eine Schutzeinrichtung war nicht vorhanden, hätte jedoch sehr wahrscheinlich zur Verhinderung des Unfalls beigetragen.	Müllentsorgungsfahrzeugfahrer	Individualverkehr	Kollision mit Gegenstand	keine	

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer	
39	08.04.2011	Güterzug (TEC)	Zugentgleisung wegen mechanischer Störung	Lagerschaden am Radsatz führte zu dessen Versagen. Gelöste Nutmutter könnte Ursache sein, wodurch es zur Überhitzung des Lagers und anschließendem Lagerversagen kam.	unklar	EVU - IH	Heißläufer, undetektiert	keine	
40	01.09.2010	Güterzug	Zugentgleisung wegen mechanischer Störung	Das in Fahrtrichtung links abgescherte Radsatzlager führte zum Bruch eines Stehbolzens der Radsatzpumpe und damit zum Wellenshenkelbruch	unklar	EVU - IH	Fahrzeugmangel	keine	
41	07.08.2010	Bauzug, Triebwa	Auffahrunfall	Unzulässige Einfahrt des Bauzuges in besetztes Gleis. Mitarbeiter beider Stellwerke beachteten die Bestimmung der gültigen Betra nicht. Die Hilfsperre zur Kennzeichnung des besetzten Einfahrgleises wurde entfernt, ohne Prüfung des freien Fahrwegs festzustellen; Der Abstellbereich der Fahrzeuge war von keinem Stellwerk einsehbar; Betriebliche Eintragungen wurden nicht gemacht und die Arbeit wurde nicht ordentlich übergeben. Eine zweite Hilfssperre beom Ww wurde nicht angebracht	Fahrdienstleiter des Stellwerks	EIU - Fdl	fehlerhafte Fahrwegprüfung	keine	
42	26.07.2007	Güterzug	Auffahrunfall	Durch mangelnde Kommunikation zwischen Fdl und TB. TB meldete sich ohne Funktion oder Ortsangabe, die vom Fdl jedoch auch nicht nachgefragt wurde. Anschließende Identifikation des TB war nicht möglich. Meldung des TB wurde fehlerhaft als Meldung der Befahrbarkeit der besetzten Strecke aufgefasst und führte zur Aufhebung der Gleissperrung. Fehlerhafte Fahrstraße wurde eingestellt. Anschließend prallte der Zug in ein stehendes Baugerüst.	Fahrdienstleiter des Stellwerks, TB	EIU - Fdl / Technisch Berechtigter der Baufirma	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	
43	28.11.2010	Güterzüge	Auffahrunfall	Fahrende Rangierfahrt fuhr auf stehende Rangierfahrt auf, da der Fahrweg nur unzureichend beobachtet wurde und mit etwa um 25 km/h überhöhter Geschwindigkeit im Baugleis gefahren wurde.	Triebfahzeugführer der Rangierfahrt	EVU - RTf	Fahrfehler	keine	
44	25.11.2008	Güzerzug, Triebf	Auffahrunfall	Trotz des durch die Lokomotive besetzten Gleises, konnte durch Regelbedienung eine Fahrstraße für den Güterzug eingestellt werden. Die Gleisfreimeldeanlage konnte wegen isolierenden Emissionen bestehend aus Feuchtigkeit, Sand und Schmierfett die stehendene Lokomotive nicht erkennen.	unklar	keiner	konstruktionsbedingter Fehler der Gleisfreimeldeanlage	keine	
45	13.04.2010	Personenzug, Lk	BÜ-Unfall	Unzeitiges Räumen des Bahnübergangs durch den Straßenverkehrsteilnehmer. Dieser hatte am BÜ einen Auffahrunfall verursacht und konnte die Unfallstelle nicht schnell genug räumen. Schließen der Schranken erfolgte unmittelbar nach Unfall. Begünstigend wirkten geringe Bemessung der Fahrbahnbreite und schlechte Sichtverhältnisse durch Nebel.	Fahrer des Transporters	Vorgaben	Keine BÜ-Freimeldung	keine	2 Wiederholung
46	20.01.2010	Personenzug, Lk	Zugkollision	Fahrer eines Lkws fuhr mit dem Fahrzeug vom Bahnübergang innerhalb des Gleises, bis der Lkw im Gleis stecken blieb. Der Tf kollidierte wenige Minuten später mit dem Lkw, der nicht rechtzeitig erkannt werden konnte.	Fahrer des Lkw	Individualverkeh r	Kollision mit Gegenstand	keine	
47	29.01.2011	Güterzug, Perso	Frontalzusammenstoß	Der Güterzug passierte an der Überleitstelle das haltzeigende Vor- und Blocksignal und fuhr somit in einen besetzten Gleisabschnitt. Es kam zur Kollision mit dem aus der Gegenrichtung kommenden Personenzug (eingleisge Strecke). Es war kein technisch wirkendes Zugbeeinflussungssystem vorhanden, da dort nicht mehr als 100 km/h zugelassen sind.	Triebfahrzuegführer Güterzug	Vorgaben	Hauptsignal missachtet, keine Zwangsbremsung		10
48	15.03.2010	Güterzug	Zugentgleisung nach Bauarbeiten	Durch fehlerhafte Stopf-Richtarbeiten wurde im Gleisbogen zwischen zwei Weichen eine Überhöhung von 40 mm hergestellt. Es entstand eine Steilrampe mit zu hoher Verwindung, wodurch der Zug entgleiste.	eingesetzte GSM	Baufirma	Fehlerhafte Bauausführung	keine	
49	19.12.2007	Güterzug	Zugentgleisung wegen mechanischer Störung	Entgleisung durch Schienenbruch	nicht definiert	keiner	Versagen des Bahnkörpers	keine	
50	24.07.2007	IC	Zugkollision	Nichtbeachtung der Vermeidung von Unfällen auf Bahngebiet. Beim Kranen von Altschienenteilen hatte sich ein Schienenteil aus dem Greifer gelöst und gelangte dadurch in das Profil des durch IC befahrenen Gleises. IC kollidierte mit der Altschiene	Auftragnehmer der Baustelle	Baufirma	Fehlerhafte Bauausführung	keine	

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer
51	07.08.2009	Güterzug	Zugentgleisung durch Spurerweiterung	Entgleisung aufgrund einer Spurerweiterung unter dem rollenden Rad. Grund war eine nicht ausreichende Spurhaltefähigkeit durch fehlende und ungenügend vorgespannte Schwellenschrauben.	nicht definiert	EIU - IH	Versagen des Bahnkörpers	keine
52	16.04.2009	Güterzug, Persor	Auffahrunfall	Zusammenstoß zwischen durchfahrendem Personenzug und ausfahrendem Güterzug wegen Nichtbeachtung der gültigen Fahrplanordnung. Güterzug erkannte den falsch eingestellten Fahrweg und hielt denoch nicht sofort an. Fahrwegprüfung wurde vom Fdl nicht ordnungsgemäß durchgeführt. Fahrdienstleiter hatte den falschen Fahrweg aufgelöst, jedoch ohne dass der Zug zum halten gekommen ist. (Der Signalhaltfall wurde anschließend nach vorne verlegt.). Hauptproblem: Durch den Signalhaltfall wegen der Fehlleitung wurde zurückgeblockt, so dass eine erneute Einfahrt möglich ist. Ich kapiere den Unfall nicht wirklich.	Fahrdienstleiter, Triebfahrzeugführer Güterzug	EVU - Tf, EIU - Fdl, EIU Planer	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine
53	23.01.2007	Güterzug (TEC)	Zugentgleisung wegen mechanischer Störung	Beim Güterzug durchbrach der hintere der beiden Stahlcoils den Container-Holzfußboden einschließlich der Bodenquerträger und fiel durch den Containertragwagen hindurch ins Gleisbett, was zur Entgleisung führte. Ursache war mangelhafte Verladung ohne Bettungsträger und ohnehin nicht ausreichende Belastbarkeit der Containerquerträger	Verlader	EVU - Verlader	Fehlerhafte Beladung	keine
54	26.04.2008	ICE	Zugkollision	ICE prallte auf eine im Gleisbereich stehende Schafherde und entgleiste daraufhin wegen der direkten Einwirkung auf den Triebkopf. Eine Einfriedung zum zurückhalten der Schafe war nicht vorhanden	nicht der Eisenbahnbetrieb	keiner	Kollision mit Gegenstand	ca. 10 Tiere (Schafe)
55	20.11.2006	S-Bahn, Ultrasch	Auffahrunfall	Trotz halt zeigendem Zwischensignal und eingeleiteter Betriebs- und Schnellbremsung fuhr die S-Bahn auf den stehenden Ultraschallschienenprüfzug auf. Ursache war die ungenügende Bremswirkung des Zuges durch stark verringerten Reibwert zeischen Rad und Schiene durch Feuchtigkeit und Schmutz. Verminderte Reibwerte als Folge des vorausfahrenden Ultraschallschienenprüfzuges, ein für diesen Schie-nenzustand nicht optimierter Gleitschutz der Bremse und die ungenügende Wirkung der Sandstreueinrichtungen des Triebzuges haben maßgeblich zu der unzureichenden Bremswirkung beigetragen.	S-Bahn Berlin GmbH	EVU - IH	Fahrzeugmangel	keine
56	15.03.2006	Güterzüge	Auffahrunfall	Aufprallursache war ein Zusammenwirken mit einer nicht ordnungsgemäßen Bedienung der Stellwerksanlage zu einer nicht zulässigen Fahrtstellung des Hauptsignals. Voraussetzung war die nicht erfolgte Vorblockung. Es kam zur fehlerhaften Weiterschaltung der Zugnummer über die Zugnummermeldeanlage zu einem falschen Ziel. (Manipulation nicht ausgeschlossen, jedoch nicht nachwisbar)	unklar	EIU - Fdl	Stellwerksfehlfunktion	keine
57	17.03.2004	Güterzug	Zugentgleisung wegen fehlerhafter Bremsen	Bei Einfahrt in den Vorbahnhof leitete Tf Bremsung ein, die jedoch keine nennenswerte Wirkung hatte. Nötige Langsamfahrt wurde deshalb nicht erreicht. Die Weichen im Durchrutschweg waren aufgrund ihrer Radien nur für Geschwindigkeiten von 40 km/h geeignet. Entgleisung erfolgte wegen zu hoher Geschwindigkeit. Vermutliche Ursache sind geschlossene Luftabsperrhähne zwischen Triebfahrzeug und erstem Wagen.	nicht definiert	EVU - Tf	Fehlerhafte Bremsprobe	keine 1 Wiederholung
58	28.09.2003	Personenzüge	Frontalzusammenstoß	Verstoß gegen Kornzernrichtlinie 436. Tf fuhr in Holzdorf ab ohne entsprechende Fahrerlaubnis durch den Zugbegleiter (eingleisige Strecke). Erlaubnis lag nur bis Holzdorf vor. Kreuzung hätte abgewartet werden müssen.	Triebfahrzeugführer aus Holzdorf	EVU - Tf	Zugleitbetrieb	1

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer
59	11.06.2003	Personenzüge	Frontalzusammenstoß	Durch Ausfall des Vorsignalwiederholers löste die Fahrstraße nicht selbstätig aus (?), was vom Fdl trotz älteren Vermerken nicht erkannt wurde. Die Streckenblockfelder blieben in Grundstellung und Strecke wurde als technisch frei angezeigt. Fdl ließ Fahrstraße mit Ersatzsignal zu, obwohl Strecke nicht frei war. Es folgte die Kollision. (Ursache fehlerhafte Diagnose der technischen Störung) - Schrozdorf --> Räumungsprüfung fehlerhaft ausgeführt		EIU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	6
60	29.06.2000	Personenzüge	Frontalzusammenstoß	Obwohl der Triebfahrzeugführer auf eine verspätete Einfahrt hätte warten sollen, fährt er unerlaubt über ein Halt zeigendes Signal, wodurch der Zug zwangsgebremst wird. Nach kurzem Halt fährt derZug erneut unerlaubt weiter und fährt dem einfahrenden Zug entgegen. Es kommt zur Kollision.	Triebfahrzeugführer	EVU - Tf	Fehlerhaftes Verhalten nach Zwangsbremsung	keine
61	06.02.2000	Personenzug	Zugentgleisung wegen überhöhter Geschwindigkeit	Die zulässige Geschwindigkeit von 40 km/h wurde nicht eingehalten, was im Gleisbogen zur Entgleisung führte. Eine technische Sicherung zur Geschwindigkeitsüberwachung der Züge war nicht vorhanden. --> Brühl (Widersprüchliche Angaben in der Betra, Gleisabschnitt wurde verwechselt, keine Geschwindigkeitsprüfung, etc.)	Triebfahrzeugführer	EVU - Tf, EIU - Betra-Bearbeiter, Vorgaben	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	9
62	22.06.2001	Personenzug, Lk	Frontalzusammenstoß	Zusammenprall zwischen Lkw und Triebzug, kein technisches Versagen der Bahnübergangssicherungsanlage	Fahrer des Lkw	Individualverkehr	BÜ missachtet	3
63	09.09.2002	Güterzüge	Frontalzusammenstoß	Der Gz kam nicht vor dem Halt anzeigenden Esig A zum Stehen, sondern fuhr ohne fahrdienstliche Zustimmung in das Gleis ein, welches zeitgleich vom entgegenkommenden Gz beansprucht wurde. Ursache: Gz hat nicht über ausreichendes Bremsvermögen verfügt, da Absperrhahn hinter 4/18 Wagen geschlossen war, kein Nachweis für ein etwaiges Fehlverhalten der am Prozess der Zugbildung und Bremsprobe beteiligten Personale, aber fehlerhaftes Bremsvermögen hätte bei vorheriger Bremsung erkannt werden müssen, Bremsart war falsch eingestellt, ...	Zugbildungspersonal, Tf	EVU	Fehlerhafte Bremsprobe / Zugbildung	keine
64	30.09.2005	Personenzug, Lk	Frontalzusammenstoß	Lkw hat beim Befahren des Bahnübergangs die Bestimmungen der EBO bzw. Straßenverkehrsordnung nicht beachtet	Fahrer des Lkw	Individualverkehr	BÜ missachtet	keine
65	07.04.2010	Personenzug	Zugentgleisung wegen unzeitiger Weichenbedienung	unzeitiges Umstellen der Weiche unter dem vorletzten Wagen durch den Weichenwärter des Stellwerks, Einfahrsignal hatte eine Störung (Signal nicht mehr bedienbar, Störung wurde 3 Monate nicht behoben), einschlägige Vorschriften der Richtlinie 408.01-09 für die Durchführung von Zugfahrten ohne Bedienung des Hauptsignals, sowie für das Auflösen von Zugfahrstraßen vom Weichenwärter und mit großer Wahrscheinlichkeit auch vom Fahrdienstleiter wurden nicht beachtet	Weichenwärter, Fahrdienstleiter des Stellwerks	EIU - Fdl	Unzeitige Fahrstraßenauflösung	keine
66	10.07.2010	IC	Sonstiger Unfall im Eisenbahnbetrieb	Ausfall der Klimaanlagen in mehreren Wagen, hohe Außentemperaturen -> Hitzestau im Inneren der einzelnen Wagen	nicht definiert	EVU	Fehlerhafte technische Konstruktion (Fahrzeug)	keine
67	27.06.2009	Personenzug	Sonstiger Unfall im Eisenbahnbetrieb	Regionalexpress kommt aufgrund einer festen Zusatzbremse und hieraus resultierenden Rauchentwicklung im Fahrgastraum auf der freien Strecke zum Stehen; Tf hat vergessen diese zu lösen, technisch bedingt lag die Luftansaugung bei dieser Bremse, außerdem gab es keinen Melder, der im Führerstand anzeigt, dass die Bremse nicht gelöst ist	Tf, Konstruktionsfehler	EVU	Fehlerhafte technische Konstruktion (Fahrzeug)	keine
68	05.03.2010	Güterzug	Zugentgleisung wegen mechanischer Störung	Die Ursache für die Entgleisung ist eindeutig in der Zerstörung des Achslagers am 3. Radsatz des 3. Wagens durch Käfigbruch mit anschließendem Heißläufer und Achsschenkelbruch begründet. Der Abstand der HOA war größer als vorgeschrieben, dadurch haben diese nicht angesprungen	EVU - IH, Planer der Strecke	Planer, EVU - IH	Fehlerhafte Streckenplanung, Fehlerhafte Fahrzeugwartung	keine

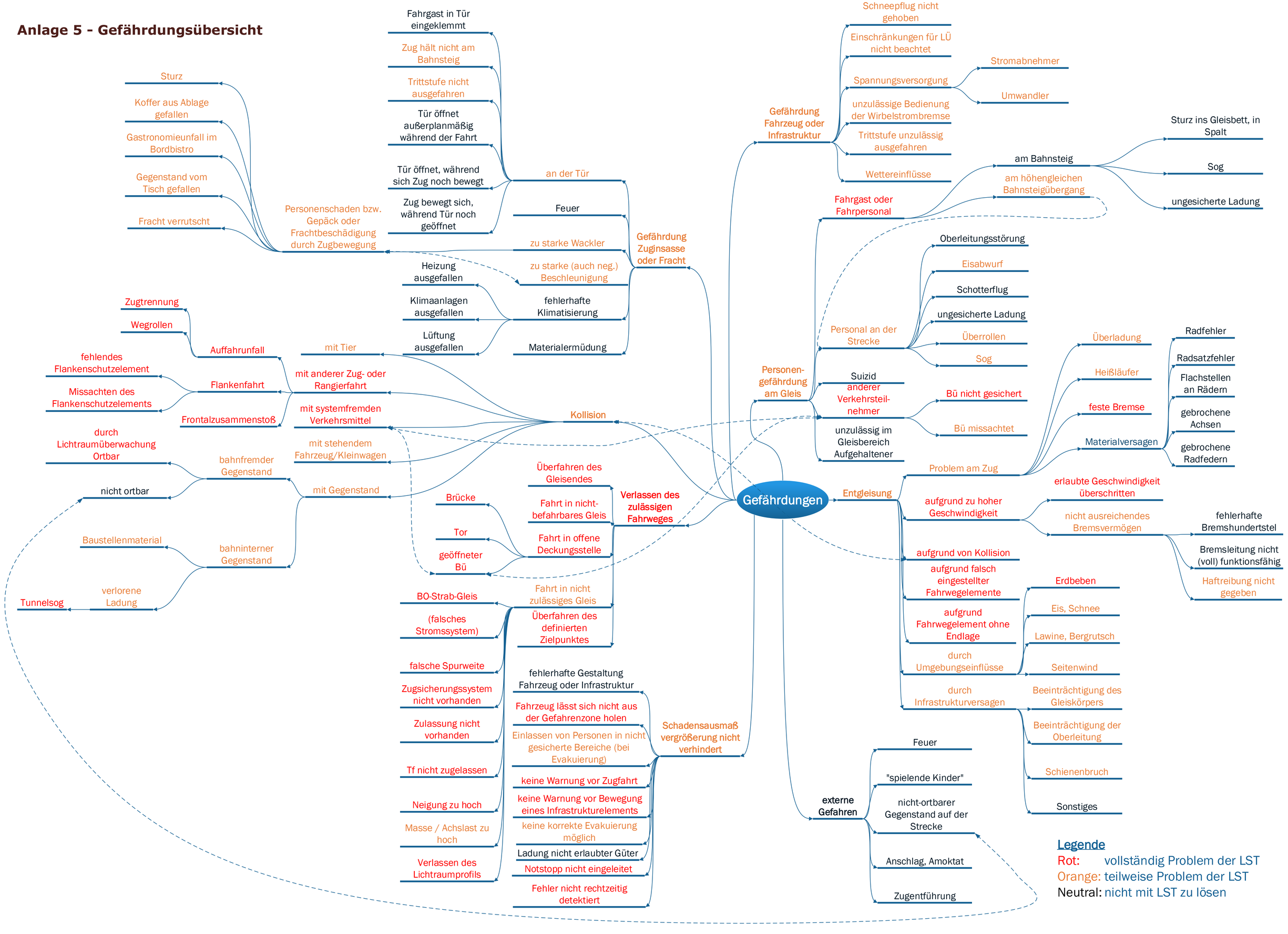
ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer	
69	28.02.2007	Güterzug	Zugentgleisung wegen mechanischer Störung	Die Zugentgleisung des Zuges ist zweifelsfrei auf einen Heißläufer bedingten Radsatzschenkelbruch am 23.Wagen zurückzuführen. HOA zu weit voneinander entfernt.	EVU - IH	EVU - IH	Heißläufer, undetektiert	keine	
70	17.04.2010	ICE	Gefährliches Ereignis im Eisenbahnbetrieb	Bei der Begegnung von zwei ICE in einem Tunnel wird durch Sog-/Druckwirkung das linke Türblatt 1 R aus seiner Verankerung im Portal gerissen, hoch geschleudert und kollidiert mit der Oberleitung und Tunneldecke. Ursache: Instandhaltungsfehler bei der Einstellung der Koppelstange an der Tür, wurde nicht durch die an der Tür vorhandenen Überwachungseinrichtungen erkannt.	EVU - IH	EVU - IH	Fahrzeugmangel, Fehlerhafte Fahrzeugwartung	keine	
71	21.09.2011	Güterzüge	Auffahrunfall	Unzulässige Einfahrt in einen besetzten Gleisabschnitt. Es wurden Unstimmigkeiten in den örtlichen Richtlinien in Bezug auf die Grenzen der Fahrwegprüfbezirke festgestellt. Im Bahnhof erfolgt die Feststellung, dass Fahrweg, Durchrutschweg etc. frei von Fahrzeugen sind, durch Hinsehen. Beide Stellwerkspersonale haben unabhängig voneinander ihren jeweiligen Fahrwegprüfbezirk nicht richtig ausgewertet. Ein Fdl war alkoholisiert und daher nicht dienstfähig.	Fahrdienstleiter des Stellwerks, Weichenwärter	EIU - Fdl, Ww	fehlerhafte Fahrwegprüfung	keine	
72	09.01.2013	Personenzug, Pk	BÜ-Unfall	Am BÜ prallt eine Regionalbahn mit einem Pkw zusammen. Fahrerin des Pkw hatte den BÜ befahren, obwohl dieser durch Posten mittels Absperrband und einer rot leuchtenden Lampe für die Zugfahrt gesichert war. Alle Hilfsmittel waren jedoch schlecht zu sehen. Daher führte der Unfall zu umfangreichen Sicherheitsempfehlungen.	Fahrer des PKW	Vorgaben, Individualverkehr	BÜ missachtet		1
73	11.02.2011	Güterzug	Zugentgleisung wegen Gleislagefehler	Gleislagefehler teilweise ohne Hilfsmittel visuell sichtbar. Gleislage war bekannt, eine Unterhaltungsmaßnahme hätte durchgeführt werden müssen, was das EIU nicht nachweisen konnte. Neben Überschreitung der Grenzwerte ist das relativ geringe Eigengewicht der vor- bzw. nachlaufenden leeren Wagen verantwortlich für den Unfall.	EIU	EIU - IH	Versagen des Bahnkörpers	keine	
74	16.06.2010	Güterzug, Persor	Zugentgleisung durch losen Radreifen, Zugkollision	Die Entgleisung des Güterzuges wurde verursacht durch einen losen Radreifen am rechten Rad des vorlaufenden Radsatzes des 10. Wagens. Die Kollision des Regionalexpresses mit anschließender Entgleisung wurde durch den 11. Wagen des Güterzuges verursacht, der als Unfallfolge der Güterzugentgleisung nach links in das Gegengleis gekippt war. Die Kollision des RE hätte verhindert werden können, wenn die Beteiligten Fdl & Tf Maßnahmen bei Gefahr ergriffen hätten	EVU IH, EVU Wagenvorbereitung, EVU Tf, EIU Fdl	EVU - IH	Fahrzeugmangel, Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	
75	26.07.2011	Personenzug	Fahrzeugbrand	Bei der Zugfahrt geriet das am Ende des Zuges fahrende Tfz in Brand. Ursache: fehlerhafte Kontakte, bzw. schlechte Verbindung der Kabelschuhanschlüsse an die Alustromschienen an der Fahrmotorklemmstelle 1 in Höhe des Führerstandes 1 des Tfz.	nicht definiert	EVU - IH	Fahrzeugmangel	keine	
76	21.08.2012	S-Bahn	Zugentgleisung wegen unzeitiger Weichenbedienung	Die Weiche wurde von der Spitze aus befahren und unter dem fahrenden Zug umgestellt. Voraussetzung war eine Auflösung der Fahrstraße vor Abwarten der Rückmeldung. Die S-Bahn stand ca. 7 Minuten, weil der Tf einen Fahrgast versorgen musste. Da die Zugfahrt nicht auf Signal erfolgte, sondern auf Ersatzsignal – Zs1 -, wegen gestörter Gleisfreimeldeanlage, war für die Auflösung des Zuges die Mitwirkung des Fahrdienstleiters erforderlich. Die vorgefundene Situation, insbesondere die Ausleuchtung auf dem Stelltisch belegen dies. Dabei handelt es sich um nachweispflichtige Tastenbedienungen, die nicht dokumentiert wurden.	Fahrdienstleiter des Stellwerks	EIU - Fdl	Unzeitige Fahrstraßenauflösung	keine	

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer	
77	05.09.2013	Personenzug	Zugentgleisung wegen unzeitiger Weichenbedienung	Während der Einfahrt in den Bahnhof entgleiste auf der Weiche das führende Tfz und der erste Wagen. Die Weiche konnte umlaufen, da die eingestellte Zugfahrstraße vorzeitig mittels Fahrstraßenhilfsauflösung aufgelöst und die Weiche aufgrund einer programmierten Vorzugslage für die andere Stellung den Umstellbefehl bekam. Der Vorfall wurde begünstigt, da Hilfshandlungen im Regelbetrieb erforderlich waren	Fahrdienstleiter des Stellwerks, Planer haben Hilfshandlungen im Regelbetrieb vorgesehen	EIU - Fdl, EIU-Planer	Unzeitige Fahrstraßenauflösung	keine	
78	22.06.2013	Personenzug, Lkw	BÜ-Unfall	Der Unfall wurde durch den Fahrer des Lkw verursacht. Dieser hatte den BÜ trotz eingeschalteter Blinklichter mit seinem Fahrzeug befahren.	Fahrer des Lkw	Individualverkehr	BÜ missachtet		1
79	26.07.2012	Güterzüge	Flankenfahrt	Primärursächlich ist die Zugkollision auf ein Bremsversagen des einen Gz zurückzuführen. Es wird vermutet, dass eine vorherige Bremsprobe durch den Tf nicht umgesetzt wurde.	Tf des Güterzugs	EVU - Tf	Fehlerhafte Bremsprobe		1
80	13.05.2013	Personenzug	Zugentgleisung wegen unzeitiger Weichenbedienung	Die Zugentgleisung (Leerzug, Rangierfahrt?) wurde verursacht durch eine vorzeitige Auflösung einer Fahrstraße. Durch die Fahrstraßenauflösung lief die Weiche in die projektierte Grundstellung um. Infolgedessen fuhren das Triebfahrzeug und die beiden nachfahrenden Reisezugwagen mit allen Drehgestellen sowie der dritte nachfahrende Reisezugwagen mit dem vorderen Drehgestell zweigleisig .Dies war möglich, weil die Fahrstraße zwischen den genannten Signalen nicht festgelegt war (blinkender FÜM) und von Hand aufgelöst werden konnte, ohne die Hilfstaste zu bedienen. Es ist in diesem Fall von einem Bedienfehler durch den özF auszugehen.	Fahrdienstleiter des Stellwerks	EIU - Fdl	Unzeitige Fahrstraßenauflösung	keine	
81	21.01.2012	Güterzug	Zugentgleisung	Die Entgleisung ist auf einen Radsatzlagerschaden an der vierten Radsatzwelle infolge eines Heißläufers zurückzuführen. Eine eindeutige Ursache des Vorspannungsverlustes konnte nicht ermittelt werden. HOA haben nicht angesprungen, da die gemessene Temperatur unter dem Schwellenwert lag	EIU - IH	EIU - IH	Heißläufer, undetektiert	keine	
82	25.03.2010	Güterzug	Zugentgleisung wegen mechanischer Störung	Zweifaches Entgleisen des Gz, verursacht durch einen Heißläufer in Verbindung mit dem Bruch des Wellenschenkels am vorderen Radsatz des vorlaufenden Drehgestells des 13. Wagens.	EIU - IH	EIU - IH	Heißläufer, undetektiert	keine	
83	02.07.2014	Güterzug	Zugentgleisung	Weiche hat sich nicht in Endlage befunden. Entgleisung ist mit hoher Wahrscheinlichkeit auf die Fehlhandlungen des Fdl zurückzuführen. Das Anbringen von Schutzkappen, Fahrwegprüfung und Räumungsprüfung wurden nicht durchgeführt. Der Fahrweg des Zuges war somit weder gesichert noch war der vorliegende Zugfolgeabschnitt geprüft worden.	Fahrdienstleiter des Stellwerks	EIU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	
84	04.06.2014	Personenzug	Fahrzeugbrand	Aufgrund eines Kabelbrandes am Tfz blieb der RE auf der Strecke liegen. Ursache war die mangelhafte Arbeitsausführung durch die Nichtbeachtung von vorgeschriebenen Instandhaltungsanweisungen durch die Mitarbeiter der zuständigen Werkstatt (Kontrolle der Fahrmotorklemmstellen an den Stromschienen wurde nicht durchgeführt).	Mitarbeiter der zuständigen Werkstatt	EVU - IH	Fahrzeugmangel	keine	
85	17.07.2009	Güterzug (Kesselwagen)	Zugentgleisung	Es ist von einem Heißläufer in Folge eines Schadens am Radsatzlager an Radsatz 1R des entgleisten Kesselwagens auszugehen. Der HOA-Abstand war zu groß. Die HOA hat aber ordnungsgemäß angesprungen und der Zug wurde auch gebremst, allerdings 2 km zu spät.	EVU - IH	EVU - IH	Heißläufer, undetektiert	keine	

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer
86	30.10.2014	Güterzug	Zugentgleisung wegen unzeitiger Weichenbedienung	Die Fahrstraße, die für die Fahrt des Gz eingestellt und festgelegt war, wurde aufgelöst, obwohl der Zug weder an der Signal-Zugschlussstelle vorbeigefahren war noch die Fahrstraßen-Zugschlussstelle erreicht hatte. Genauer: Zur Entgegennahme eines Befehls war der Tf mit seinem Zug nicht bis zum gewöhnlichen Halteplatz vorgefahren, sondern hatte seine Lok bereits ca. 250 m vorher auf Höhe des Stellwerkes angehalten (um Fußwege möglichst kurz zu halten). Folge: Zug war nicht vollständig in das Gleis eingefahren, durch den nicht vorgesehen Halt des Gz wurde eine Sicherungseinrichtung in Form einer Mitwirktaste baurtbedingt vorzeitig freigeschaltet -> Fahrstraße konnte aufgelöst werden	Fahrdienstleiter des Stellwerks, auch EVU-Tf (aber Fdl trägt Hauptverantwortung)	EIU - Fdl, Vorgaben	Unzeitige Fahrstraßenauflösung	keine
87	04.10.2011	Güterzug	Zugentgleisung	Als Ursache für die Zugentgleisung ist ein gebrochener Achsschenkel am hinteren Drehgestell des achten, im Zugverband eingestellten, Wagen festgestellt worden.	EVU - IH	EVU - IH	Fahrzeugmangel	keine
88	01.12.2012	Güterzug	Zugentgleisung	Die Entgleisung des 21. Wagens wurde durch einen Bruch des Wellenschenkels an der ersten Achse des vorderen Drehgestells in Fahrtrichtung rechts verursacht. Der Bruch war Folge einer thermischen Überbeanspruchung des Wellenschenkels im Radsatzlager (Heißläufer). HOA waren ausreichend vorhanden, haben aber keine Auffälligkeiten feststellen können.	EVU - IH	EVU - IH	Heißläufer, undetektiert	keine
89	25.06.2012	Personenzug	Fahrzeugbrand	Der Zug kam in Folge der Brandentwicklung aufgrund einer Zwangsbremsung zum Stehen. Ursache des Fahrzeugbrandes: Isolationsfehler in beiden Triebzügen.	EVU - IH	EVU - IH	Fahrzeugmangel	keine
90	21.04.2015	Güterzug	Zugentgleisung wegen unzeitiger Weichenbedienung	Die Zugentgleisung war Folge einer unzeitigen Weichenbedienung durch den Weichenwärter des Stellwerks. Dieser hatte die gegen die Spitze befahrene Weiche umgestellt, obwohl diese noch durch den letzten Wagen besetzt war. Ww überzeugte sich auch vor dem Umstellen der Weiche nicht vom Freisein durch Hinsehen. Letzteres wäre auf Grund der geringen Entfernung von Stellwerk und Weiche bei den bestehenden Sichtverhältnissen problemlos möglich gewesen. Ww hat den Fahrweg, in dem der Zug noch stand nicht gesichert, Fdl hat unterlassen ihn dazu aufzufordern (kein Zugfunkgespräch belegt). Fahrweg wurde nicht ordnungsgemäß gesichert. Darüber hinaus war das Gleis nicht für die Ein- und anschließenden Ausfahrten der Züge geeignet (Gleis zu kurz für Gz), sodass bei nahezu jedem Gz die Einfahrzugstraße mittels Bedienung der FHT aufgelöst werden musste. Gleislängen waren falsch angegeben, deshalb ragte der Zug immer in den Weichenbereich hinaus	Weichenwärter, Fahrdienstleiter des Stellwerks, Planer	EIU - Ww, EIU - Fdl, EIU - Planer	fehlerhafte Fahrwegprüfung	keine
91	25.04.2015	Personenzug	Fahrzeugbrand	Der Brandherd befand sich am Powerback B des B-Wagens. Ausgelöst durch eine undichte Stelle der Diesel-Leckleitung konnte sich ein Aerosol mit sehr hohem thermischem Energieanteil bilden. Die Abdrift erfolgte in Richtung Abgasrohr/Turbolader, an welchem es zur Zündung kam und einen andauernden Abbrand des permanent austretenden Kraftstoffs nach sich zog.	EVU - IH	EVU - IH	Fahrzeugmangel	keine
92	11.04.2014	S-Bahn	Zugentgleisung wegen unzeitiger Weichenbedienung	Arbeitsfehler des diensthabenden Fdl: Mangelhafte Einstellung, Prüfung und Sicherung des Fahrweges für die Einfahrt der S-Bahn auf Signal Zs 1 in den Bf durch den Fdl, mit der Folge, dass eine unzulässige Umstellung der spitz befahrenen Weiche unter dem einfahrenden Zug durch den Fdl erfolgen konnte. Der Fdl hat den Zug mit Zs1 in ein falsches Gleis geleitet. Als er diesen Fehler bemerkte, stellte er noch schnell die maßgebliche Weiche um, allerdings zu spät	Fahrdienstleiter des Stellwerks	EVU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine

ID	Datum	Zugart(en)	Unfallart	Vorgang	Verursacher	Zuständigkeit	Ursache	Todesopfer	
93	24.02.2016	Personenzüge	Störung durch betriebliche Fehlhandlung	Fdl hat den ausfahrenden Zügen absichtlich die Fahrt auf die eingleisige Strecke erlaubt, obwohl die aus der Gegenrichtung einfahrenden Züge den gewöhnlichen Halteplatz im Bahnhof noch nicht erreicht hatten und diese Züge noch nicht zurückgemeldet worden waren, um den Betriebsablauf zu beschleunigen	Fahrdienstleiter des Stellwerks	EVU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	
94	02.09.2014	Rangierlok, Trakt	BÜ-Unfall	Der Fahrer der landwirtschaftlichen Zugmaschine beachtete mehrere Pfeifsignale der Rangierlok und das Andreaskreuz zur Sicherung des BÜ nicht. Beim Heranfahren an den BÜ übersah er auch die Rangierlok.	Fahrer des Traktors	Individualverkehr	BÜ missachtet	keine	
95	02.12.2014	Güterzug	Zugentgleisung wegen unzeitiger Weichenbedienung	Die Entgleisung wurde verursacht durch eine betriebliche Fehlhandlung im Stellwerk. Aufgrund einer Störung konnte das Einfahrsignal nicht bedient werden. Der Gz musste auf Zs 1 einfahren -> Weiche lag nicht unter Verschluss. Das Signal Zs 1 wurde bedient, ohne das dafür die notwendigen Voraussetzungen gegeben waren. Bei Ankunft des Notfallmanagers auf dem Stellwerk war keine Hilfssperre am Weichenhebel der Weiche angebracht.	Fahrdienstleiter des Stellwerks	EVU - Fdl	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	
96	24.02.2016	ICE	Beinahe-Kollision mit RB durch Einfahrt in besetzten Gleisabschnitt	Die RB wurde außerplanmäßig im Bf getrennt. Die dazugehörige Betra lag nicht aus. Nach der Trennung war das Gleis noch rotausgeleuchtet. Der Fdl hat jedoch den Zugschluss des ersten Zugteils beobachtet und daraus geschlossen, dass eine Störung vorlag und den Gleisabschnitt mit der AzGT freigegeben. Der Tf des ICE konnte rechtzeitig bremsen. Die Fahrdienstvorschrift enthält äußerst komplexe Regeln zum Sachverhalt einer möglichen Zugtrennung. Beide Fdl haben dies fehlinterpretiert.	Fahrdienstleiter des Stellwerks	EIU - Fdl, Betra-Ersteller, EIU Betra-Aussendestelle, Vorgaben	Fehlerhaftes Handeln bei Abweichungen vom Regelbetrieb	keine	der Tf sollte hier immer an den Fdl melden, dass er den Zug getrennt hat

Anlage 5 - Gefährdungsübersicht



Topology

Anlage 6: Klassendiagramm topologisches Modell

hellpink: Beispielelemente (nicht vollständig)

RTM Package Base

RTM Package Positioning Systems

RTM Package Net Entities

RTM Package Topology

smartLogic Topology Model

smartLogic Infrastructure Model

smartLogic Movement Model

<<Interface>>
BaseObject
-id : UUID
-name : String
-lastUpdated : TimeStamp
-comment : String
-validFrom : Date
-validTo : Date

NetworkResource

NetElement

Relation

reine Nachbarschaftsbeziehung

PositionedRelation
-positionOnA : boolean
-positionOnB : boolean
-navigability : RelationNavigability
-vmax : int
-applicationDirection : ApplicationDirection

<<enumeration>>
RelationNavigability
AB
BA
BOTH
NONE

ControlledTrackElement
-operationTime : int

TrackElementStatus

CompositeNetElement

PositioningNetElement

EntityLocation
-applicationDirection : ApplicationDirection

NetEntity

LocatedNetEntity

PositioningSystem

AssociatedPositioningSystem

PositioningSystemCoordinate

LinearCoordinate
-lateralOffset : double
-measure : double
-verticalOffset : double

GeometricCoordinate
-x : double
-y : double
-z : double

IntrinsicCoordinate
-intrinsicCoord : double

NonLinearElement

AreaLocation

AssociatedNetElement
-intrinsicCoordBegin : double
-intrinsicCoordEnd : double
-keepOrientation : boolean

LinearElement

LinearLocation
-applicationDirection : ApplicationDirection

SpotLocation
-applicationDirection : ApplicationDirection

SpotElement
-location : SpotLocation

OrderedAssociatedNetElement
-sequence : int

ControlledElement
-availableStatus : ControlledE...
-label : String

MaintenanceOffice

ControlCenter

smartLogic

« Gleissegment » (TrackSegment)

TrackEdge
-internallyLocked : boolean

TrackEdgeSection

TrackArea
-applicationDirection : ApplicationDirection

LinearLocationCoordinate
-positioningSystemCoordinates : PositioningSystemCoordinate

SpotLocationIntrinsic
-intrinsicCoord : double

SpotLocationCoordinate
-positioningSystemCoordinate : PositioningSystemCoordinate

<<enumeration>>
ApplicationDirection
Nominal
Reverse
Both

prüfen, ob Element note-endig ist oder als TrackArea mit einer TrackEdgeSection mit begin = end vereinfacht werden kann

InformationPoint
-applicationDirection : ApplicationDirection

ContiguousTrackArea

LinearContiguousTrackArea

TrackZone

ControlArea

InterlockingSubArea

smartLogicArea
-blocked : boolean

TrackElementStatus

ControlledTrackElement
-operationTime : int
-occupations : CTEOccupation

StakeholderRegistration
-system : StakeholderSystem
-validityPeriod : TimePeriod
-deregistrationParameters : Set<DeregistrationParameters>
-actionInCaseOfCommunicationFailure : ActionPlan
-actionInCaseOfSystemFailure : ActionPlan

TrainAction
-validityArea : EffectiveArea
-deletionConditions : DeletionCondition[]

RestrictedArea
-deletionConditions : Set<DeletionCondition>

DangerArea
-deletionConditions : Set<DeletionCondition>
-reaction : ActionPlan

EffectiveArea
-validModes : Set<M_MODE>
-validLevels : Set<M_Level>

DetectionArea
-delay : int
-validModes : Set<M_Mode>
-validLevels : <M_Level>

TopologyOccupation
-begin : SpotLocationIntrinsic
-end : SpotLocationIntrinsic

DrivePrototectionSection

AllocationSection

DPSGroup
-dps : DrivePrototectionSection[]

AllocationSectionGroup
-as : AllocationSection[]

AxleLoadSpeedSegment
-q_FRONT
-m_AXLELOADCAT
-v_AXLELOAD

GradientSegment
-g_A : ETCS_GRADIENT
-q_GDIR : boolean

SpeedSegment
-v_STATIC : ETCS_SPEED
-q_FRONT
-nc_CDDIFF : NC_CDDIFF
-nc_DIFF : NC_DIFF

SpeedChange
-q_FRONT : boolean
-q_DIFF : boolean

AxleLoadSpeedChange
-q_FRONT : boolean

ETCSModeChange
-m_MAMODE : M_MA...
-v_MAMODE : ETCS_S...
-l_MAMODE : ETCS_L...
-t_ACKMODE : ETCS_...
-q_MAMODE : boolean

ETCSRouteSuitabilityDataPoint
-d_SUITABILITY : ETCS_DISTANCE
-q_SUITABILITY : Q_SUITABILITY

AllowedCurrentConsumptionChange
-m_CURRENT : M_CURRENT

LineGaugeChange
-m_LINEGAUGE : M_LINEGAUGE

AxleLoadCatChange
-m_AXLELOADCAT : M_AXLELOADCAT

VoltageChange
-m_VOLTAGE : M_VOLTAGE
-nid_CTRACTION : NID_CTRACTION

Information Points

VoltageSystem
-m_VOLTAGE : M_VOLTAGE
-nid_CTRACTION : NID_CTRACTION

NTC
-nid_NTC : NID_NTC

ETCS_TrainData
-nc_CDTRAIN : NC_CDTRAIN
-nc_TRAIN : NC_TRAIN
-l_TRAIN : ETCS_LENGTH
-v_NAXTRAIN : ETCS_SPEED
-m_LOADINGGAUGE : M_LOADINGGAUGE
-m_AXLELOADCAT : M_AXLELOADCAT
-m_AIRTIGHT : M_AIRTIGHT
-n_AXLE : int

TrainParameters
-supportedGoa : Set<GoA>
-minNoiseRequirements : NoiseRequirement
- / brakingCapability : BrakingCapability
- / accelerationCapability : AccelerationCapability
- / BrakeTypes : BrakeType[]
- / availBrakeModes : BrakeMode[]
- / dangerousGoods : boolean
- / completeEmBrakeOverrideAvail : boolean
- / completeEzBrakeAvail : boolean

Requester
-maxContinuousUsageTime : Time
-minContinuousUsageTime : Time
-maximumTimeBetweenRequests : Time
-minimumTimeBetweenRequests : Time
-timeoutParameters : TimeoutParameters
-protectorRateFunction : ProtectionRateFunction

Listener

Supervisor
-reaction : ActionPlan

RequiredAction

Restriction

NotificationRequester

ApprovalRegistration

LevelCrossingOC
-availabilityStatus : LevelCrossingStatus
-currentStatus : LevelCrossingStatus

TractionControlCmd
-cmd : M_TRACKCOND
-system : M_VOLTAGE

ModeChange
-mode : M_MAMODE

RequiredVehicleFunction
-function : M_TRAXKCOND

GoAChange
-goa : ATOGoA

DriverInformation
-information : FixedTextMsg
-freetext : String
-ackReaction : Q_TEXTCONFIRM
-validLevel : M_LEVELTR

Train Actions

ETCSSpecialArea

WindRiskArea
-expectedWindSpeed : in
-vMax : int = DEFAULT.Wind...

ConstructionArea
-clearanceProcedure : ConstructionAreaClearanceProcedure

SnowRiskArea
-closedSnowCover : boolean
-vMax : int = DataModel.Topology.SnowRisk...

IcicleArea
-vMax : int

TrainCategoryRestrictionArea
-v_TCR : ETCS_SPEED

ETCSTrackCondItionAreas
-q_TRACKINIT
-d_TRACKINIT : ETCS_DISTANCE
-m_TRACKCOND : M_TRACKCOND

ETCSReducedAdhesionFactorArea
-m_ADHESION : boolean

ReversingArea
-d_REVERSE : ETCS_DISTANCE
-v_REVERSE : ETCS_SPEED

Special Track Areas

TemporarySpeedRestrictionArea
-v_TSR : ETCS_SPEED
-q_FRONT : boolean

NonStoppingArea

TunnelStoppingArea

PowerlessSection

MainswitchOff

SoundHornArea

RadioHole

AirTightness

NoRegenerativeBrake

NoEddyCurrentBrake

NoMagneticBrakeService

NoMagneticBrakeEmergency

PhysicallyNonTrafficable

LogicallyClosed

SpeedRestriction
-vMax : int

ProhibitedATOGoA
-goa : ATOGoA

ProhibitedETCSMode
-mode : M_MAMODE[]

Restricted Areas

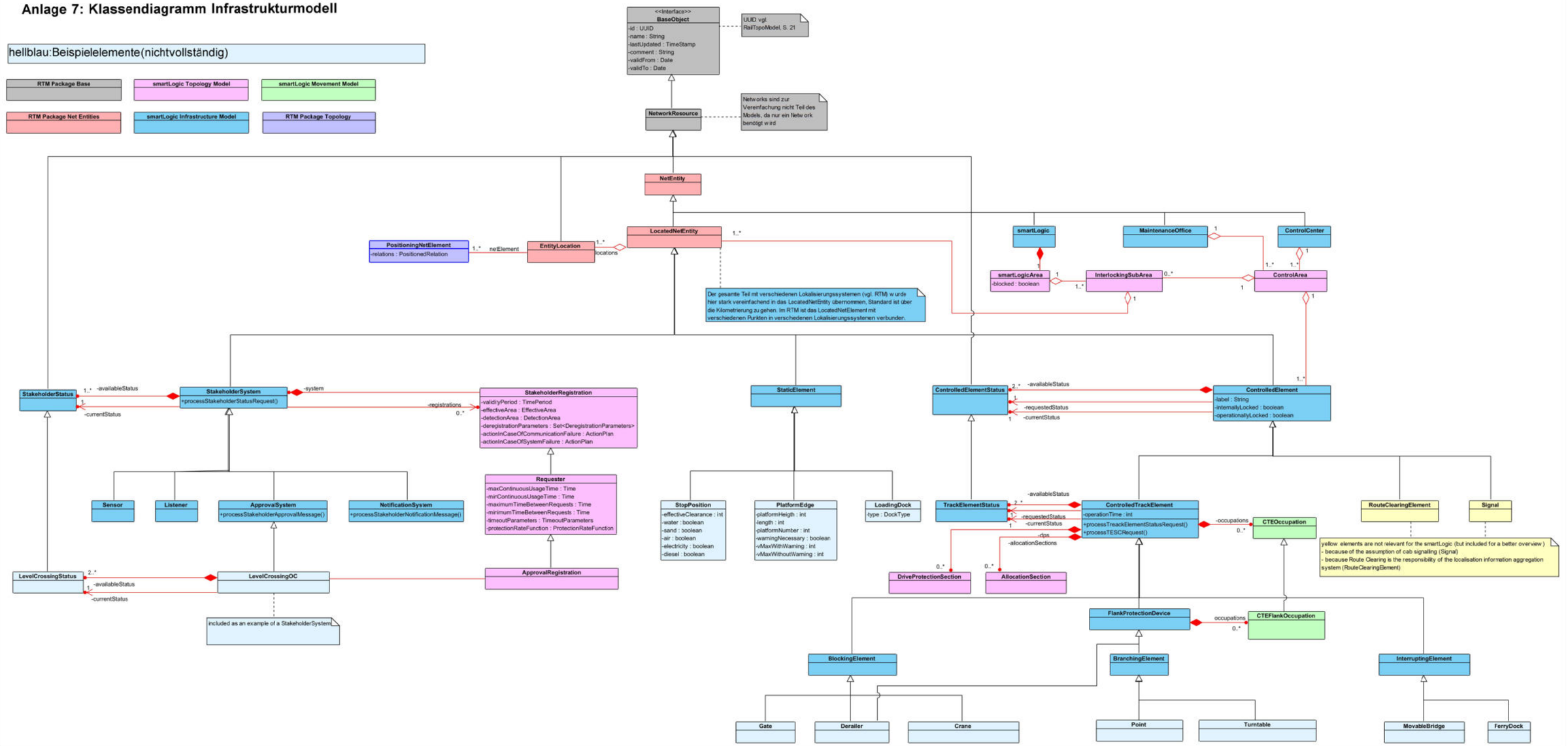
InfrastructureElements

Anlage 7: Klassendiagramm Infrastrukturmodell

hellblau:Beispielelemente(nichtvollständig)

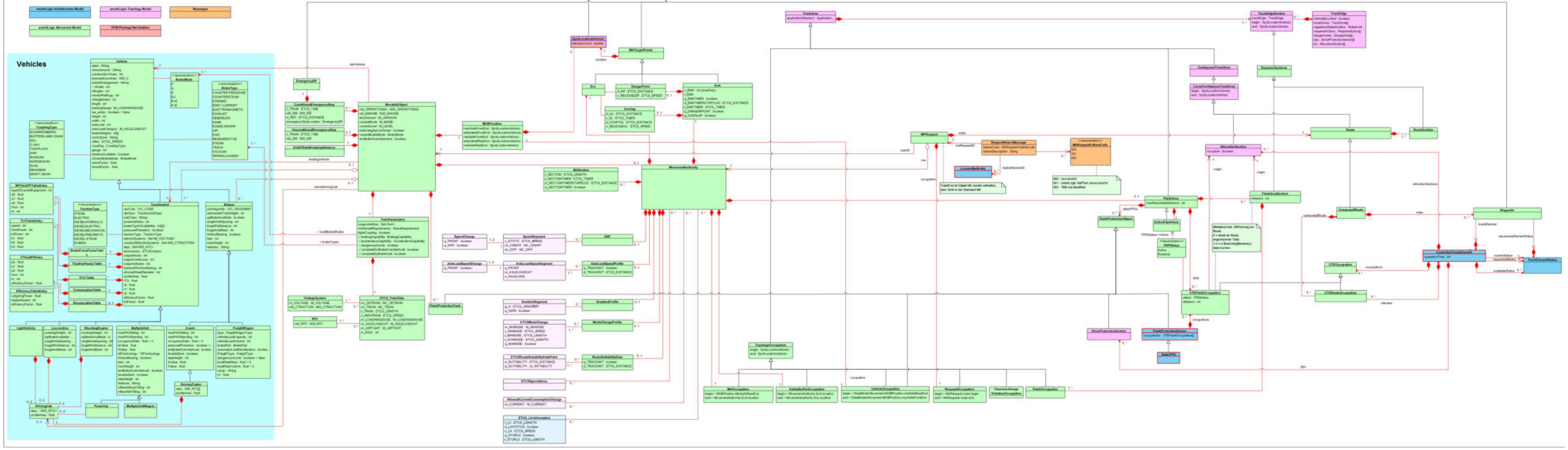
RTM Package Base | smartLogic Topology Model | smartLogic Movement Model

RTM Package Net Entities | smartLogic Infrastructure Model | RTM Package Topology



Anlage 8: Klassendiagramm Fahrzeug- und Fahrzeugbewegungsmodell

hellpink: Beispielelemente (nicht vollständig)



MP-Request2

Anlage 9: Aktivitätsdiagramm für den MP Request