Modulare Systemarchitektur für einen robusten vollautomatisierten Bahnbetrieb

Zur Erlangung des akademischen Grades Doktor-Ingenieurs (Dr.-Ing.) genehmigte Dissertation von M.Sc. Bilal Üyümez, geb. am 20.06.1990 in Groß-Gerau

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

Tag der Einreichung: 05.09.2023
Tag der Disputation: 15.12.2023

TECHNISCHE UNIVERSITÄT DARMSTADT

Institut für Bahnsysteme und Bahntechnik

Darmstadt 2023

Üyümez, Bilal: Modulare Systemarchitektur für einen robusten vollautomatisierten Bahnbetrieb

Darmstadt, Technische Universität Darmstadt
Jahr der Veröffentlichung auf Tuprints: 2024

Schriftenreihe des Instituts für Verkehr,
Fachgebiet Bahnsysteme und Bahntechnik

Heft B16
ISSN 1614-9300
URN: urn:nbn:de:tuda-tuprints-266719
URI: https://tuprints.ulb.tu-darmstadt.de/id/eprint/26671
Tag der mündlichen Prüfung: 15.12.2023

Kurzfassung

Die Verkehrsnachfrage auf der Schiene ist in den vergangenen Jahrzehnten stetig gewachsen. Um mehr Betrieb aufgrund der steigenden Verkehrsnachfrage ohne Neu- und Ausbau von Verkehrsinfrastruktur realisieren zu können, bietet die zunehmende Digitalisierung des Verkehrs die Chance, die Kapazität durch eine automatisierte Betriebsführung auf der heute bereits hoch ausgelasteten Verkehrsinfrastruktur markant zu steigern. Durch die zunehmende Automatisierung der Betriebsführung (bis hin zum vollautomatisierten Betrieb) wird auch angestrebt, die Folgen des demografischen Wandels und der sich verändernden Arbeitswelt in der Bahnbranche auszugleichen.

Ein vollautomatisierter Bahnbetrieb ist nur dann effektiv, wenn die Nutzer den darin agierenden technischen Systemen vertrauen können. Dieses Vertrauen kann jedoch abnehmen, wenn die technischen Systeme im vollautomatisierten Betrieb häufig Störungen – mit z.T. sicherheitskritischen Auswirkungen – aufweisen und für den Umgang damit keine angemessenen Lösungen vorhanden sind.

Für Störungssituationen mit z.T. sicherheitskritischen Auswirkungen gibt es heute bereits betrieblich-technische Rückfallebenen, mit denen der Betrieb unter der Verantwortung des involvierten Betriebspersonals (Triebfahrzeugführer und Fahrdienstleiter) fortgeführt werden kann. Aufgrund der Tatsache, dass die gegenwärtigen betrieblich-technischen Rückfallebenen historisch gewachsen und in natürlich-sprachlichen Regelwerken festgehalten sind sowie eine intensive zwischenmenschliche Interaktion zwischen einem Fahrdienstleiter und einem Triebfahrzeugführer erfordern, sind sie für den vollautomatisierten Bahnbetrieb nicht geeignet. Für den vollautomatisierten Bahnbetrieb sind daher betrieblich-technische Rückfallebenen erforderlich, die notwendigerweise weitgehend automatisiert und auch unabhängig von den natürlich-sprachlichen Regelwerken sowie mit geringer menschlicher Intervention – z. B. auch bei Störung der Kommunikation – ablaufen müssen.

Im Rahmen dieser Doktorarbeit wurde ein Ansatz für eine weitgehend automatisierte Reaktion auf Störungssituationen im vollautomatisierten Bahnbetrieb entwickelt. Aufgrund der fehlenden Betriebserfahrung mit dem vollautomatisierten Bahnbetrieb bei Vollbahnen wurden relevante Störungssituationen (z.B. Ausfall der Kommunikation oder Störung der Sensoren zur Hinderniserkennung) anhand der systemtheoretischen Prozessanalyse (engl. System Theoretic Process Analysis, STPA) systematisch hergeleitet.

Die automatisierte Reaktion auf die relevanten Störungssituationen stützt sich methodisch auf die dynamische Adaption der Systemarchitektur zur Laufzeit. Bei einer dynamischen Adaption zur Laufzeit können sich die technischen Systeme in der Systemarchitektur in Abhängigkeit der vorliegenden Störung und des damit verletzten Schutzziels derart anpassen, sodass eine Betriebsführung weiterhin gewährleistet wird. Die technischen Systeme können dabei entweder das eigene Verhalten oder ihre Beziehung zu den benachbarten technischen Systemen anpassen.

Die automatisierte Reaktion auf Störungssituationen auf Basis der dynamischen Adaption stellt mit ihren regelbasierten und generischen Abläufen einen allgemeingültigen Ansatz dar und zahlt damit in das Ziel der betrieblichen Interoperabilität ein. Durch die automatisierte Reaktion auf Störungssituationen sind zudem signifikante Zeiteinsparungen erzielbar, die zur Erreichung der Kapazitäts- und Pünktlichkeitsziele beitragen können.

Abstract

Demand for rail transport has grown steadily over the past decades. To further increase the quality of mainline operations and the capacity of the already highly utilized transport infrastructure in the face of growing demand, efforts are being made to automate the operation of train services.

The increasing automation of rail operations (up to and including fully automated operations) is also intended to mitigate the consequences of demographic change and the changing work environment in the rail industry.

Fully automated rail operations are effective if users have confidence on automated technical systems. However, this confidence can diminish if the technical systems frequently fail during operation – sometimes with safety-critical effects – and no appropriate solutions are available for dealing with them.

For disruptive situations with potentially safety-critical effects, there are already operational and technical fallback solutions that enable operations to continue under the responsibility of the staff involved (train drivers and train controllers). Due to the fact that the current operational-technical fallback solutions have evolved historically and are defined in natural language regulations, they are not suitable for fully automated rail operations. They also require intensive interpersonal interaction between a train controller and a train driver, who will no longer take on an active role in fully automated rail operations.

Fully automated rail operations also require operational and technical fallback solutions, which must necessarily be extensively automated and also operate independently of the natural language rules and with reduced human intervention.

Within the scope of this doctoral thesis, an approach for an extensively automated response to disruptive situations in fully automated rail operations was developed. Due to the lack of experience with fully automated mainline rail operations, relevant disruptive situations (e.g. communication failure or disruption of obstacle detection sensors) were systematically derived using system theoretical process analysis (STPA). The automated response to disruptive situations is methodically based on the dynamic adaptation of the system architecture at runtime. In the case of dynamic adaptation at runtime, the technical systems in the system architecture can adapt themselves depending on the existing disruption and the violated protection objective in such a way that the operation is still ensured. The technical systems can either adapt their own behavior or their relationship to the adjacent technical systems.

With its rule-based and generic processes, the automated response to disruptive situations based on dynamic adaptation represents a generally valid approach and thus contributes to the goal of operational interoperability. Furthermore, significant time savings can be achieved, which may contribute to the achievement of capacity and punctuality objectives.

Özet

Demiryolu taşımacılığa olan talep son yıllarda sürekli olarak artış göstermiştir. Ulaşımın artan dijitalleşmesi, halihazırda yüksek oranda dolu olan kapasitenin otomatikleştirilmiş bir işletmeyle belirgin olarak arttırılması için bir şans sunmaktadır. İşletmedeki otomasyonun artması ile (tam otomatik işletmeye kadar) demografik ve iş dünyasındaki değişimin demiryolları için telafi edilmesi de hedeflenmektedir.

Tam otomatik bir işletme etkili olabilmesi için kullanıcıların teknik sistemlere güvenmesi gerekir. Ancak bu güven, işletmedeki teknik sistemlerin sık sık arıza çıkarması – kısmen emniyet-kritik etkilerle – ve bununla başa çıkmak için yeterli çözümlerin olmaması ile azalabilir.

Kısmen emniyet kritik etkileri olan arıza durumları için günümüzde de personelin (makinist ve trafik kontrolörü) sorumluluğu altında yürütülebilen yedek işletim prosedürleri (fallback-level) bulunmaktadır.

Eski yönetmelikler, tarihsel olarak ilerlemeleri ve dil bazlı kurallarla sabit olmaları sebebiyle tam otomatik bir demiryolu işletmesine uygun değildir. Bununla birlikte, tam otomatik işletmede aktif bir rol oynamayacak olan trafik kontrolörü ve makinist arasında yoğun bir insan iletişimine gerek duymaktadır. Tam otomatik bir işletme için mecburi olarak daha az insan müdahalesiyle gerçekleşen, büyük ölçüde otomatik ve insan iletişimiyle çalışan kurallara bağlı olmayan yedek işletim prosedürlerine ihtiyaç vardır.

Bu doktora tezi kapsamında tam otomatik demiryolu işletmesinde arıza durumlarına büyük ölçüde otomatik işletim prosedürleri (otomatik tepkiler) geliştirilmiştir. Ana hat demiryollarında tam otomatik demiryolu işletimi ile ilgili operasyonel deneyim eksikliği nedeniyle, önemli arıza durumları (örneğin iletişim arızası veya engel tespiti için sensörlerin arızalanması) sistem teorik analizi (STPA) yöntemini kullanılarak olarak belirlenmiştir. Arıza durumlarına otomatik tepkiler, metodik olarak sistem mimarisinin çalışma süresi esnasında dinamik adaptasyonuna dayanmaktadır.

Sistem mimarisindeki teknik sistemler, kendilerini oluşan arızaya ve kaybedilen güvenlik hedeflerine göre düzenleyerek işletmenin devamlılığını sağlayabilir. Teknik sistemler, adaptasyon esnasında kendi davranışlarını veya komşu teknik sistemlerle ilişkisini düzenleyebilir.

Arıza durumlarına dinamik adaptasyonla verilen otomatik tepkiler, kural bazlı ve standart işlemleriyle genel bir yaklaşım sunarken işletmede ülkeler arası uyumluluk hedefine de katkıda bulunmaktadır. Arıza durumlarına otomatik tepkiler sayesinde kapasite ve dakiklik hedeflerine katkı sağlayabilecek büyük ölçüde zaman tasarrufları da sağlanabilmektedir.

Danksagung

Die Verfassung dieser Dissertation markiert einen bedeutenden Meilenstein in meinem akademischen Werdegang, und ich möchte die Gelegenheit nutzen, all den Menschen zu danken, die mich auf diesem anspruchsvollen Weg begleitet und unterstützt haben.

Ein besonderer Dank gebührt meinem Doktorvater, Herrn Prof. Oetting für die Möglichkeit der Promotion am Institut für Bahnsysteme und Bahntechnik der TU Darmstadt und für die Betreuung während des gesamten Bearbeitungszeitraums sowie Herrn Prof. Pachl für die Übernahme des Zweitgutachtens.

Ein großes Dankeschön geht an Frederik Düpmeier als Mentor für das Korrekturlesen und für die fachlichen Diskussionen zu den inhaltlichen Kernkapiteln. Außerdem geht ein großer Dank an Arturo Crespo Materna für die fachlichen Diskussionen und für seine konstruktiven Impulse zu den eisenbahnbetriebswissenschaftlichen Themen.

Mein Dank gilt auch den heutigen und ehemaligen Kollegen und Kolleginnen am Institut für Bahnsysteme und Bahntechnik der TU Darmstadt, die immer für Fragen offen waren und für ein gutes Arbeitsklima gesorgt haben.

Die private Unterstützung trägt ebenfalls erheblich zum Erfolg einer umfangreichen wissenschaftlichen Arbeit bei. Besonderer Dank gilt daher auch meiner Familie und meinen Freunden. Sie haben mich durch alle Höhen und Tiefen begleitet und gerade in der Endphase auch viel auf mich verzichtet.

Ich danke meinen Eltern, die mir ein Studium ermöglicht haben und immer an mich geglaubt haben. Außerdem danke ich für ihre unerschütterliche Unterstützung und Ermutigung. Ihre Geduld und Liebe haben mir die notwendige Stabilität und Zuversicht in den herausfordernden Phasen der Doktorarbeit geschenkt. Zu Guter Letzt möchte ich mich insbesondere bei meiner Frau Çağla für ihre grenzlose Unterstützung und für ihre Geduld während der Anfertigung der Doktorarbeit bedanken.

Bilal Üyümez

1 Einführung

1.1 Ausgangssituation

Beschreibung der aktuellen Situation

Das Bahnsystem ist in seiner aktuellen Ausführung ein soziotechnisches System, das durch die digitale Transformation zunehmend von technischen Systemen dominiert wird. Dennoch ist der Mensch aktuell ein notwendiger Bestandteil des Bahnsystems, ohne dessen Mitwirkung das Ziel der Transportleistung nicht erfüllt werden kann.

Die Verkehrsnachfrage ist in den vergangenen Jahrzehnten stetig gewachsen. Die Bewältigung dieser auch zukünftig wachsenden Verkehrsmengen und der steigenden Komplexität verlangt nach neuen Lösungen, die ergänzend zum gesellschaftlich oft problematischen Neu- und Ausbau eine intensivere Nutzung der vorhandenen, aus Steuermitteln finanzierten Verkehrsinfrastruktur ermöglichen.

Um mehr Betrieb aufgrund der steigenden Verkehrsnachfrage ohne Neu- und Ausbau von Verkehrsinfrastruktur realisieren zu können, bietet die zunehmende Digitalisierung des Verkehrs die Chance, die Kapazität durch eine automatisierte Regelung des Betriebs auf der heute bereits hoch ausgelasteten Verkehrsinfrastruktur markant zu steigern. Deshalb werden seit einigen Jahren weltweit innovative Lösungen für einen digitalen Bahnbetrieb erforscht oder bereits in der Praxis erprobt.

Während der vollautomatisierte Bahnbetrieb bei Nahverkehrssystemen schon länger existiert, ist die Entwicklung bei Vollbahnen weniger fortgeschritten. Dieser Unterschied ist hauptsächlich auf die folgenden Gründe zurückzuführen.

Bei Vollbahnen ist die Ausdehnung des Netzes im Vergleich zu Nahverkehrssystemen größer und es interagieren unterschiedliche Infrastrukturbetreiber mit zahlreichen Verkehrsunternehmen. Es liegt somit ein Mischverkehr vor. Außerdem ist die Infrastruktur auch von außen zugänglich, sodass jederzeit Hindernisse, die eine Zugfahrt gefährden können, in den Lichtraum hineinragen bzw. eindringen können. Des Weiteren ist ein vollautomatisierter Bahnbetrieb mit der aktuellen Systemarchitektur der Leit- und Sicherungstechnik (LST), die z.T. noch mechanische Stellwerke umfasst, nicht sinnvoll. Daher gibt es bereits Bestrebungen hinsichtlich der Spezifikation einer Systemarchitektur für den digitalen Bahnbetrieb. Darunter ist ein Paradebeispiel die Erprobung des hochautomatisierten Fahrens bei der S-Bahn Hamburg. Das Pilotprojekt zeigt, wie neue Technologien den Bahnbetrieb leistungsfähiger machen können. In der Fachwelt wird auch bereits über den vollautomatisierten Bahnbetrieb nachgedacht und an geeigneten Lösungen geforscht.

Die zunehmende Automatisierung des Bahnbetriebs wird nicht nur aus Gründen der Kapazitätssteigerung angegangen, sondern die Automatisierung bietet auch eine Möglichkeit, die Folgen des demografischen Wandels und der sich verändernden Arbeitswelt in der Bahnbranche auszugleichen.

Problemfelder

Durch die zunehmende Automatisierung des Bahnbetriebs können zwar ein Beitrag zur Steigerung der Kapazität der Infrastruktur geleistet und die Folgen des demografischen Wandels und der sich verändernden Arbeitswelt in der Bahnbranche ausgeglichen werden, jedoch ist ein vollautomatisierter Bahnbetrieb nur dann sinnvoll, wenn die Nutzer den darin agierenden technischen Systemen vertrauen. Das Vertrauen in den vollautomatisierten Bahnbetrieb kann zurückgehen, wenn die darin agierenden technischen Systeme häufig Störungen aufweisen und für den Umgang damit keine Lösungen vorhanden sind.

Prinzipiell können zwar Störungen an technischen Systemen mit sogenannten Redundanzen in der Systemarchitektur kompensiert werden, jedoch verursachen Redundanzen erhebliche Kosten.

Das Bahnsystem als komplexes soziotechnisches System erfordert bereits heute eine enge Zusammenarbeit zwischen verschiedenen Stakeholdern. Zu den Stakeholdern des Bahnsystems gehören neben den Eisenbahninfrastrukturunternehmen (EIU) und Eisenbahnverkehrsunternehmen (EVU) auch Fahrgäste und öffentliche Behörden sowie die Gesellschaft.

Von den Störungssituationen können sowohl die Eisenbahninfrastrukturunternehmen als auch die Kunden (Fahrgäste und Eisenbahnverkehrsunternehmen) betroffen sein. Störungssituationen können während des Betriebs nicht nur gefährlich sein, sondern sie können zudem die Betriebsqualität durch Pünktlichkeitsabweichungen beeinträchtigen und können dadurch die durch die Automatisierung angestrebte Kapazitätssteigerung verhindern.

1.2 Motivation

Der Beitrag des vollautomatisierten Bahnbetriebs zur Kapazitätssteigerung resultiert primär aus den harmonisierten Fahrzeugbewegungen (präzises Abfahren von Geschwindigkeitsprofilen) und der Möglichkeit, dadurch Pufferzeiten einzusparen. Harmonisierte Fahrzeugbewegungen dienen auch der Energieeinsparung im Betrieb.

Um jedoch von den genannten Nutzenpotenzialen des vollautomatisierten Bahnbetriebs vollständig profitieren zu können, sind auch Lösungen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb erforderlich.

Um die mit Redundanzen verbundenen hohen Kosten zu minimieren, sind im vollautomatisierten Bahnbetrieb auch Lösungen für den Umgang mit Störungssituationen an nicht redundant ausgelegten technischen Systemen erforderlich. Dabei steht primär die schnelle Reaktion auf Störungssituationen im Fokus, um die Betriebsqualität nicht zu beeinträchtigen.

Heute gibt es zwar bereits betrieblich-technische Rückfallebenen, mit denen der konventionelle Betrieb in Störungssituationen fortgeführt werden kann, diese sind jedoch historisch gewachsen und in natürlich-sprachlichen Regelwerken festgehalten. Sie erfordern zudem eine intensive zwischenmenschliche Interaktion zwischen einem Fahrdienstleiter und einem Triebfahrzeugführer.

Für den vollautomatisierten Bahnbetrieb sind ebenfalls betrieblich-technische Rückfallebenen erforderlich, die notwendigerweise weitgehend automatisiert und auch unabhängig von den natürlich-sprachlichen Regelwerken sowie mit reduzierter menschlicher Intervention ablaufen müssen.

1.3 Ziel

In dieser Arbeit sollen aus den oben genannten Gründen weitgehend automatisierte betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb unter Berücksichtigung des Grundprinzips „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“ entwickelt werden.

1.4 Nutzen

Sofern Lösungen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb existieren, können die in Kapitel 1.1 und 1.2 genannten Nutzen voll ausgeschöpft werden. Insbesondere das Vertrauen der Nutzer in den vollautomatisierten Bahnbetrieb kann gesteigert werden.

Durch weitgehend automatisierte betrieblich-technische Rückfallebenen kann zum einen die Zuverlässigkeit des Betriebs durch Minimierung der menschlichen Fehlerhäufigkeit erhöht werden. Zum anderen ermöglicht eine weitgehend automatisierte Reaktion auf Störungssituationen, auch weniger Verspätungen zu verursachen, und beeinträchtigt dadurch weniger die Betriebsqualität aus dem Regelbetrieb. Weitgehend automatisierte Reaktion auf Störungssituationen trägt ebenfalls zu der angestrebten Kapazitätssteigerung im vollautomatisierten Bahnbetrieb wesentlich bei. Insbesondere die schnelle und automatisierte Reaktion auf Störungssituationen kann die Kapazitätseinschränkung bei ggf. reduzierten Pufferzeiten reduzieren.

Außerdem bieten weitgehend automatisierte betrieblich-technische Rückfallebenen – losgelöst von historisch gewachsenen nationalen betrieblichen Regelwerken – die Möglichkeit, länderübergreifend einheitliche Lösungen zu entwickeln und dadurch die von den Bahnbetreibern geforderte betriebliche Interoperabilität zu erreichen.

1.5 Gliederung der Arbeit

Die systematische Vorgehensweise zur Erreichung des Ziels wird in Kapitel 3.4 ausführlich hergeleitet. Um den Lesenden bereits zu Beginn einen Überblick über den Aufbau der Arbeit zu geben, findet sich in diesem Kapitel eine kurze Übersicht.

Das Hauptkapitel 2 enthält einen Überblick über den Stand der Forschung und Entwicklung im Kontext des vollautomatisierten Bahnbetriebs. Dabei werden bestehende Technologien und Spezifikationen sowie aktuelle Forschungsprojekte mit Fokus auf dem vollautomatisierten Bahnbetrieb vorgestellt.

Auf Basis der identifizierten Forschungslücken sind dann in Hauptkapitel 3 die Aufgabenstellung, die Anforderungen an die Lösung der Aufgabenstellung einschließlich der Methode und Vorgehensweise sowie die inhaltliche Abgrenzung der Arbeit festzulegen.

Die Hauptkapiteln 4 – 7 bilden den Kern der Arbeit. In Hauptkapitel 8 wird die im Rahmen dieser Arbeit entwickelte Lösung anhand eines Anwendungsbeispiels bewertet. In Hauptkapitel 9 ist die Zusammenfassung und der Ausblick der Arbeit zu finden.

1.6 Hinweise zum Verständnis der Arbeit

Die erste nummerierte Gliederungsebene in der Arbeit wird als Hauptkapitel bezeichnet. In jedem Hauptkapitel können mehrere Kapitel vorkommen, die der zweiten nummerierten Gliederungsebene zugeordnet werden. Jedes Kapitel kann zudem Unterkapitel enthalten, die ebenfalls nummeriert sind und der dritten Gliederungsebene entsprechen.

Die Anforderungen und einzelne Schlüsselwörter bzw. Teilsätze werden in den jeweiligen Hauptkapiteln **fett** gestellt.

Einige Begriffe, die in der Arbeit verwendet werden, können von verschiedenen Personen oder in verschiedenen Kontexten unterschiedlich verstanden werden. Deshalb werden diese Begriffe für die Verwendung in der Arbeit in Kapitel 3.6 definiert.

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

Diese Dissertation beinhaltet Erkenntnisse, die im Verlauf der Bearbeitung der Promotion bereits auf Konferenzen vorgestellt wurden. Hierzu sind die Veröffentlichungen *(Üyümez 2019)*, *(Üyümez & Oetting 2019)*, *(Essid, Klaus & Üyümez 2020)* und *(Slamal, Wala & Üyümez 2022)* entstanden. Die Referenzen zu diesen Veröffentlichungen sind in der Arbeit an der entsprechenden Stelle gekennzeichnet.

Des Weiteren wurden während der Anfertigung dieser Dissertation einige studentische Arbeiten betreut oder mitbetreut, die thematisch einen Bezug zum Promotionsthema haben und zudem die eigenen Gedanken des Autors unterstützt haben.

Tabelle 1 Liste der betreuten studentischen Arbeiten mit Bezug zum Promotionsthema

Autor	**Titel**	**Abschluss**
Martial Lumineau	Untersuchung von möglichen Kapazitätssteigerungen durch das autonome Fahren im Schienenverkehr	09/17
Sinan Kücük	Entwicklung von automatisierten Rückfallebenen bei Abweichungen vom Regelbetrieb	09/17
Philipp Schuster	Entwicklung einer kontinuierlichen Ortungseinheit für das Eisenbahnbetriebsfeld Darmstadt	12/17
Dajana Martens	Faseroptisches Sensorsystem für sicherheitsrelevante Anwendungen im Eisenbahnsektor	11/17
Benedetta De Creszenco	modelling of critical situations in fully automated railway operation	02/18
Choudhry Sharjeel Ahmad	Robuste Lokalisierung und Markerdetektion für das Eisenbahnbetriebsfeld Darmstadt	08/18
Laurenz Bremer	Integration des automatisierten Fahrens in den Fahrsimulator unter Berücksichtigung der energiesparsamen Fahrweise	02/19
Amin Essid	Entwicklung einer Kommunikationsstruktur zur Fortführung des automatisierten Bahnbetriebs im Störungsfall	04/20
Marco Umstädter	Entwicklung eines Verfahrens zur situationsbasierten Risikoabschätzung beim vollautomatisierten Betrieb in der Rückfallebene	03/22
Georg Gratz	Bewertung von betrieblich-technischen Rückfallebenen für den vollautomatisierten Bahnbetrieb	09/22
Moritz Tomberger	Entwicklung der Betriebsart „Fahren auf Sicht“ für den vollautomatisierten Betrieb	10/22

2 Stand der Forschung und Entwicklung

In diesem Hauptkapitel werden bestehende Technologien und Spezifikationen sowie aktuelle Forschungsprojekte vorgestellt, die für die vorliegende Dissertation von Relevanz sind. Der gesamte Fokus dieses Hauptkapitels liegt dabei auf den Bereich des vollautomatisierten Bahnbetriebs im Schienenverkehr.

In Kapitel 2.1 wird zunächst der Automatisierungsbegriff samt des aktuellen Automatisierungsgrades bei Vollbahnen eingeführt und einige Pilotprojekte kurz vorgestellt.

Wie bereits in Kapitel 1.1 eingeführt, können bei den Vollbahnen unterschiedliche Zuggattungen (Personenzüge und Güterzüge) auf derselben Strecke fahren (Mischverkehr). In Kapitel 2.2 wird daher der Mischverkehr im Kontext dieser Dissertation kurz erläutert.

In Kapitel 2.3 werden dann bereits durchgeführte oder parallellaufende Forschungsprojekte aus dem Bereich des Schienenverkehrs vorgestellt, in denen Technologien und Spezifikationen, die für den vollautomatisierten Bahnbetrieb erforderlich sind, erforscht bzw. entwickelt werden.

Im Vordergrund dieser Arbeit steht die Entwicklung von geeigneten Lösungsansätzen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb. Daher werden in Kapitel 2.4 auch bereits bestehende Lösungen aus dem gegenwärtigen Betrieb kurz vorgestellt, die beim Umgang mit Störungssituationen aus dem gegenwärtigen Betrieb eingesetzt werden. Des Weiteren werden aus den Forschungsprojekten, sofern vorhanden, auch für den vollautomatisierten Bahnbetrieb vorgeschlagene Lösungsansätze für den Umgang mit Störungssituationen kurz vorgestellt.

Da die Automatisierung auch in den beiden bedeutenden Verkehrssystemen Straßenverkehr und Luftverkehr vorangetrieben wird, erfolgt in Kapitel 2.5 auch ein Benchmarking dahingehend, welche Lösungsansätze für den Umgang mit Störungssituationen im automatisierten Straßen- und Luftverkehr derzeit erarbeitet werden.

Nachdem in Kapitel 2.6 mögliche Methoden für die Entwicklung von geeigneten Lösungsansätzen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb beschrieben werden, erfolgt in Kapitel 2.7 eine Zusammenfassung dieses Hauptkapitels, woraus dann in Hauptkapitel 3 die genaue Aufgabenstellung für diese Dissertation definiert werden kann.

2.1 Stand der Automatisierung im Schienenverkehr

Das vorliegende Kapitel führt den Automatisierungsbegriff im Schienenverkehr ein und geht auf die unterschiedlichen Automatisierungsgrade bei Vollbahnen ein. Außerdem werden in diesem Kapitel einige Pilotprojekte zum vollautomatisierten Bahnbetrieb bei Vollbahnen kurz vorgestellt.

2.1.1 Automatisierungsbegriff im Schienenverkehr

Der Automatisierungsgrad im Schienenverkehr wird von dem internationalen Verband für öffentliches Verkehrswesen (engl. International Association of Public Transport, UITP) definiert *(IEC 62267:2009)*. Die Automatisierung im Schienenverkehr wird dabei auf bestimmte Funktionen, die fahrzeugseitig erfüllt werden, bezogen. Diese Funktionen umfassen die Geschwindigkeitsregelung einschließlich aller Fahrphasen (Beschleunigen, Beharren, Ausfahren und Bremsen), Türsteuerung und den Bahnbetrieb in Störungssituationen.

Der UITP definiert dazu insgesamt fünf Automatisierungsgrade für den Schienenverkehr, die im Folgenden kurz erläutert werden.

Im **Automatisierungsgrad 0** (engl., Grade of Automation 0, GoA0) wird der Zug komplett manuell unter der Verantwortung eines Triebfahrzeugführers geführt. Bei diesem Automatisierungsgrad gibt es kein Zugbeeinflussungssystem, sodass der Triebfahrzeugführer auch für die Zugsicherung verantwortlich ist.

Der **Automatisierungsgrad 1** (engl., Grade of Automation 1, GoA1) unterscheidet sich von GoA0 darin, dass die Zugsicherung durch technische Systeme übernommen wird, sodass der Triebfahrzeugführer für die Geschwindigkeitsregelung, Türsteuerung und für den Betrieb in Störungssituationen zuständig ist.

Im **Automatisierungsgrad 2** (engl., Grade of Automation 2, GoA2) wird der Triebfahrzeugführer weiter entlastet, da in dieser Stufe die Geschwindigkeitsregelung von dem sogenannten Automatic Train Operation System (ATO-System) übernommen wird. Der Triebfahrzeugführer ist in diesem Automatisierungsgrad weiterhin im Führerstand anwesend, erteilt in der Station nach Abfertigung des Zuges und dem Türenschließen den Fahrtauftrag für eine sichere Abfahrt des Zuges aus der Haltestelle und überwacht zudem die Fahrt bis zur nächsten Station, sodass er in Gefahrensituationen sofort eingreifen kann *(Rumsey 2010)*. Für den Betrieb in Störungssituationen ist der Triebfahrzeugführer weiterhin verantwortlich.

Erst mit dem **Automatisierungsgrad 3** (engl., Grade of Automation 3, GoA3) werden elementare Änderungen in den fahrzeugseitigen Verantwortlichkeiten verzeichnet. In diesem Automatisierungsgrad ist der Triebfahrzeugführer nicht mehr im Führerstand anwesend, sodass das ATO-System neben der Geschwindigkeitsregelung auch die Türsteuerung, die Überwachung der Profilfreiheit übernimmt und beim Betrieb in Störungssituationen zum Teil mitwirken muss. Dieser Automatisierungsgrad wird auch als begleiteter fahrerloser Zugbetrieb (engl., driverless train operation, DTO) bezeichnet und ist daher für Personenzüge prädestiniert.

Der letzte **Automatisierungsgrad 4** (engl., Grade of Automation 4, GoA4) basiert auf einem Betrieb ohne Betriebspersonal an Bord, bei dem der Zug sowohl im Regelbetrieb als auch in Störungssituationen vollautomatisiert betrieben wird. Dieser Automatisierungsgrad wird auch als unbegleiteter fahrerloser Zugbetrieb (engl., unattended train operation, UTO) bezeichnet und ist daher für Güterzüge prädestiniert, kann jedoch bei Personenzügen ebenfalls angewandt werden.

Da, wie in Kapitel 1.1 erwähnt, der vollautomatisierte Bahnbetrieb im Fokus steht und dieser entsprechend der Definition oben die beiden Automatisierungsgrade GoA3 und GoA4 umfasst, beschränkt sich die Arbeit auf die Automatisierungsgrade GoA3 und GoA4.

2.1.2 Stand der Automatisierung bei Vollbahnen

Aufgrund der hohen Sicherheitsanforderungen wird eine Zugfahrt im Regelbetrieb in GoA0 nicht mehr durchgeführt. Sowohl bei Nahverkehrssystemen als auch bei Vollbahnen sind die Züge heute in der Regel mit Zugsicherungssystemen ausgestattet.

Erste Erfahrungen mit dem vollautomatisierten Bahnbetrieb (GoA4) gibt es bei Stadtbahnen (vor allem bei
U-Bahnen) und den People-Mover-Systemen. Letzteres System gibt es beispielsweise seit 1994 am Frankfurter Flughafen. In Nürnberg fährt die U-Bahn-Linie (U3) seit 2007 vollautomatisiert.

Für das Jahr 2025 werden von der UITP schätzungsweise 2300 km vollautomatisiert betriebene U-Bahn-Linien erwartet. Nach Angaben aus dem Jahr 2018 (April 2018) haben vollautomatisierte U-Bahn-Linien in der ganzen Welt zusammen bereits 1.000 km erreicht *(Grey 2018)*.

Den Grund für die weit verbreitete Automatisierung von Nahverkehrssystemen sehen *(Nießen et al. 2017)* darin, dass diese Systeme von anderen Verkehrssystemen und von der Umwelt abgeschottet sind

und dass ein artreiner Verkehr stattfindet. Außer den Haltestellen gibt es keine Schnittstellen zu anderen Verkehrsträgern. Um sicherzustellen, dass Fahrgäste an Haltestellen (Bahnsteigen) nicht von Schienenfahrzeugen erfasst werden oder in das Gleis fallen, werden bei den vollautomatisierten Nahverkehrssystemen technische Überwachungssysteme eingesetzt. Beispielsweise wird dazu bei U-Bahn Nürnberg ein radarbasiertes Bahnsteigüberwachungssystem *(Gunther 2007)* eingesetzt. Zur Sicherstellung, dass Fahrgäste an Haltestellen (Bahnsteigen) nicht von Schienenfahrzeugen erfasst werden oder in das Gleis fallen, gibt es bei anderen Metro-Systemen (z.B. Barcelona oder Istanbul) auch sogenannte Bahnsteigtüren als Schutzmaßnahmen.

Entsprechend der Definition der Automatisierungsgrade aus dem vorigen Unterkapitel entspricht GoA2 einer automatisierten Geschwindigkeitsregelung. Demnach besteht bei Vollbahnen bereits mit der Einführung der linienförmigen Zugbeeinflussung, ergänzt um die sogenannte Automatische Fahr- und Bremssteuerung (AFB), der Automatisierungsgrad GoA2. Durch die Vorgabe der Sollgeschwindigkeit kann die AFB die Zugkraft entsprechend der Streckenverhältnisse automatisiert regeln.

Seit einigen Jahren gibt es zudem vereinzelt Pilotanwendungen des vollautomatisierten Bahnbetriebs bei Vollbahnen. So erfolgt die erste Anwendung von GoA4-Betrieb im Güterverkehr seit 2018 durch das Bergbauunternehmen Rio Tinto in Australien, das Eisenerzzüge videoüberwacht zu den Hafenanlagen fahren lässt *(Smith 2019)*. Im Jahr 2018 konnte eine Fahrt zwischen dem Ort des Bergbauunternehmens und dem Zielort (Cape Lambert) auf einer Länge von 280 km durchgeführt werden.

Eine weitere Pilotanwendung gibt es in Deutschland. Im Jahr 2021 konnte im Rahmen des Forschungsprojekts „Digitale S-Bahn Hamburg“ das hochautomatisierte Fahren in Hamburg vorgeführt werden *(Schröder et al. 2021)*. Durch die Premierenfahrt des hochautomatisierten Fahrens wurde ein wichtiger Meilenstein für die Einführung von ATO im deutschen Schienennetz erreicht. Das ATO-System hatte dabei die Aufgabe, das Geschwindigkeitsprofil auf Basis der von einem streckenseitig verbauten ATO-Computer empfangenen Fahrplandaten zu erstellen und daraufhin die Geschwindigkeit des Zuges automatisiert zu regeln. Wenngleich eine automatisierte Geschwindigkeitsprofilerstellung und -regelung erfolgte, begleitete ein Triebfahrzeugführer die Premierenfahrt im Führerstand. Lediglich die Depotfahrt erfolgte – nachdem die Fahrgäste ausgestiegen waren – vollautomatisiert.

Des Weiteren hat der Bahntechnikhersteller AŽD im tschechischen Netz auf der Strecke zwischen Cížkovice und Most erste öffentliche Fahrt im Automatisierungsgrad GoA4 durchgeführt. Die Niederländischen Eisenbahnen NS und Arriva haben ebenfalls gemeinsam mit der ProRail eine fahrerlose, jedoch ferngesteuerte Fahrt durchgeführt *(Eurail Press 2022)*. Eine ähnliche Pilotanwendung wird auch derzeit von DB Cargo und ProRail mit Güterzügen auf der Betuweroute zwischen dem Hafen Rotterdam und dem Ruhrgebiet erprobt *(Jacob 2022)*.

Bei allen Pilotanwendungen werden die Funktionalitäten des ATO-Systems jedoch für jeden Anwendungsfall proprietär entwickelt. Außerdem geht es bei den Pilotanwendungen derzeit nur darum, die Geschwindigkeitsregelung zu testen. Weitere relevante Aufgaben des Triebfahrzeugführers, wie z.B. Gefahrenerkennung oder der Umgang mit Störungssituationen, stehen nicht im Vordergrund.

2.2 Mischverkehr im Kontext des vollautomatisierten Bahnbetriebs

Wie zu Beginn des Hauptkapitels erwähnt, können unterschiedliche Zuggattungen (Personenzüge und Güterzüge) auf derselben Strecke fahren. Dieser Betrieb wird als Mischverkehrsbetrieb oder Mischverkehr bezeichnet. Im Mischverkehr weisen die Züge unterschiedliche Geschwindigkeiten auf *(DB Netz AG)*.

Entsprechend der Strategie der europäischen Bahnbranche wird das europäische Zugsicherungssystem (ETCS-System) bei der Einführung des halbautomatisierten Bahnbetriebs GoA2 als Zugsicherungssystem zugrunde gelegt. Auch der vollautomatisierte Bahnbetrieb (GoA3 und GoA4) wird aktuell von der europäischen Bahnbranche mit ETCS als Zugsicherungssystem spezifiziert.

Dadurch können auf einer mit ETCS ausgerüsteten Strecke Züge in unterschiedlichen Automatisierungsgraden verkehren. Das bedeutet, dass in Zukunft der Mischverkehr neben den Charakteristika der Züge auch anhand der Automatisierungsgrade definiert werden kann.

Die unterschiedlichen Automatisierungsgrade der Zuggattungen führen auch Veränderungen in der Betriebsführung herbei. Nicht nur die Schnittstellen der technischen Systeme ändern sich durch die Einführung des ATO-Systems, sondern auch die Zusammenarbeit zwischen EIU und EVU – insbesondere in Störungssituationen – ist in Abhängigkeit der unterschiedlichen Automatisierungsgrade neu zu gestalten.

2.3 Existierende Spezifikation des ATO-Systems in aktuellen Forschungsprojekten auf dem Weg zum digitalen Bahnbetrieb

Auf dem Weg zum digitalen Bahnbetrieb gibt es bereits europaweit Bestrebungen, die parallel zu dieser Dissertation laufen, um europaweit eine standardisierte Referenzarchitektur für den digitalen Bahnbetrieb zu entwickeln. Diese standardisierte Referenzarchitektur des digitalen Bahnbetriebs umfasst auch das ATO-System. In diesem Kapitel werden Forschungsinitiativen und die darin vorangetriebenen Spezifikationen des ATO-Systems vorgestellt.

In Unterkapitel 2.3.1 werden die beiden Forschungsinitiativen Digitale Schiene Deutschland (DSD) und smartRail 4.0 aus der Schweiz kurz vorgestellt. Daraufhin werden in Unterkapitel 2.3.2 die Forschungsinitiativen Open Command, Control, and Signalling (CCS) Reference Architecture (RCA) und Open CCS On-board Reference Architecture (OCORA) vorgestellt. Anschließend wird in Unterkapitel 2.3.3 das Europes-Rail Joint Undertaking (ERJU) als Nachfolge der RCA und OCORA vorgestellt. Danach werden in den Unterkapiteln 2.3.4 und 2.3.5 das europäische Zugsicherungssystem ETCS und das kommunikationsbasierte Zugsicherungssystem (CBTC) im Kontext des vollautomatisierten Fahrens vorgestellt.

2.3.1 ATO-System bei Digitale Schiene Deutschland (DSD) und smartRail 4.0

Digitale Schiene Deutschland (DSD)

Bei der Deutschen Bahn werden im Rahmen des Konzernprogramms „Digitale Schiene Deutschland“ Zukunftstechnologien in das zukünftige System Bahn eingebracht. Dazu werden verschiedene Forschungsprojekte – darunter auch hinsichtlich des vollautomatisierten Bahnbetriebs – durchgeführt.

Kernthemen im Zusammenhang mit dem vollautomatisierten Bahnbetrieb bei DSD sind neben dem **digitalen Stellwerk** (DSTW) auch **Sensoren** für **Hinderniserkennung (Umfeldwahrnehmung)** und **Ortung** sowie die **digitale Karte**.

Im Forschungsprojekt Sensors4Rail werden verschiedene Technologien zur Hinderniserkennung erprobt. Mit den erprobten Technologien sollen Informationen über das Umfeld des Zuges und eine präzise Zugposition in Echtzeit zur Verfügung gestellt werden. Während die Rohdaten aus den Ortungssensoren zur Verarbeitung in eine digitale Karte eingehen, sollen aus den Rohdaten der unterschiedlichen Sensoren zur Hinderniserkennung durch Sensordatenfusion statische und

dynamische Hindernisse auf und neben dem Gleis erkannt werden sowie deren Gefahreneinschätzung möglich sein.

Da die Forschungsprojekte parallel zu dieser Dissertation laufen, werden mit Versuchsfahrzeugen bereits Testfahrten durchgeführt, um betriebliche Daten zu sammeln und diese über eine Cloudschnittstelle bereitzustellen. In diesem Zusammenhang wird bei DSD auch eine sogenannte **Data-Factory** aufgebaut. Die Data-Factory soll große Datenmengen enthalten und diese für das Training von KI-Software für Objekterkennung und Zuglokalisierung bereitstellen.

Das Ziel dabei ist es, den Bahnbetrieb flüssiger und zuverlässiger zu gestalten, indem z.B. im vollautomatisierten Bahnbetrieb Störungen durch Zuhilfenahme dieser Daten schneller bearbeitet und die Zugdisposition optimiert werden kann.

Auch das Thema **ATO** wird bei DSD erarbeitet. Dabei wird die Automatisierung der Geschwindigkeitsregelung vorangetrieben, sodass ein Triebfahrzeugführer zwar weiterhin im Führerstand präsent ist, jedoch zukünftig nur noch bei Störungen eingreifen soll.

Da in der Fachwelt hinsichtlich der Obsoleszenz der GSM-R als Kommunikationssystem für den digitalen Bahnbetrieb Einklang besteht und die oben vorgestellten technischen Systeme (insbesondere die Sensordaten) steigende Datenraten erfordern, wird das nachfolgende Kommunikationssystem unter dem Namen **Future Rail Mobile Communication System (FRMCS)** spezifiziert. Das FRMCS soll auf 5G basieren und ist zum Zeitpunkt des Verfassens dieser Arbeit noch nicht endgültig spezifiziert. Eine wesentliche Eigenschaft von FRMCS soll es sein, verschiedene Kommunikationsanwendungen (z.B. Mission Critical Services) modular anzubieten, darunter z.B. die Fernsteuerung von Zügen in Störungssituationen *(UIC 2018)*.

Wenngleich die für einen vollautomatisierten Bahnbetrieb erforderlichen Kernthemen innerhalb der DSD adressiert werden, stehen Betriebsprozesse für den vollautomatisierten Bahnbetrieb bei DSD aktuell noch nicht im Fokus.

smartRail 4.0

SmartRail 4.0 ist das Pendant zu DSD in der Schweiz. Darin soll auch der Grundstein für die digitale Zukunft der Bahn gelegt werden.

Im Rahmen von smartrail 4.0 wird der Automatisierungsgrad GoA2 angestrebt, weshalb ein Triebfahrzeugführer weiterhin präsent und für die Zugfahrt verantwortlich ist.

Im Rahmen von smartrail 4.0 wurden verschiedene Testfahrten u.a. mit DB Cargo durchgeführt, bei denen der Test der Geschwindigkeitsregelung durch das ATO-System im Vordergrund stand.

Im Jahr 2020 wurde jedoch von der SBB angekündigt, dass ATO-Projekte nicht mehr weiterverfolgt werden, da dadurch zum Triebfahrzeugführermangel beigetragen wurde *(Fischer 2020)*. Die bis dahin gesammelten Erfahrungen von smartRail 4.0 wurden dennoch auf die europäischen Forschungsinitiativen RCA, OCORA und ERJU übertragen.

2.3.2 ATO-System in RCA und OCORA

Während die zuvor in Unterkapitel 2.3.1 vorgestellten Forschungsinitiativen national agieren, gibt es auch europaweit Bestrebungen hinsichtlich der Vereinheitlichung und Automatisierung des Bahnbetriebs. Als Quelle für dieses Unterkapitel kommen hauptsächlich die Spezifikationsdokumente von RCA und OCORA *(EUG & EULYNX 2020a), (EUG & EULYNX 2022) und (OCORA 2022b)* in Frage.

RCA

Seit 2018 gibt es Bestrebungen, mit der Open Command, Control, and Signalling (CCS) Reference Architecture (RCA) eine europaweit standardisierte Referenzarchitektur für die infrastrukturseitige Leit- und Sicherungstechnik zu definieren. Die Referenzarchitektur soll eine standardisierte Grundlage für die Gestaltung der Deployment[1] Systemarchitektur für einen digitalen Bahnbetrieb in den beteiligten Ländern ermöglichen.

Da die Schnittstellen innerhalb der RCA vorkommenden technischen Systeme standardisiert werden, können nationale Betreiber technische Systeme von Herstellern erwerben, die über die standardisierten Schnittstellen miteinander agieren. Dabei ist jeder Betreiber frei in der Wahl des Herstellers. Durch die Standardisierung sollen insbesondere Innovationen leichter eingebracht (flexibel) und die Sicherheit von technischen Systemen getrennt voneinander (modular safety) nachgewiesen werden können.

Das ATO-System, das für den vollautomatisierten Bahnbetrieb erforderlich ist und somit im Vordergrund dieser Arbeit steht, ist nach dem System-of-Systems Ansatz in der RCA Referenzarchitektur eingebettet. Das darin eingebettete ATO-System umfasst ein infrastrukturseitiges **ATO-TS** (engl., ATO Trackside System) und ein fahrzeugseitiges **ATO-OBU** (engl., ATO On-board Unit) Teilsystem.

Die Spezifikation der beiden Teilsysteme **ATO-TS** und **ATO-OBU** ist aus den Systemspezifikationen „ATO over ETCS“ (SUBSET 125 und 126) übernommen worden.

Das infrastrukturseitige Teilsystem ATO-TS wird in der RCA Referenzarchitektur als **ATO-AT** (ATO Transactor) bezeichnet. Das Teilsystem ATO-TS befindet sich in der RCA-Referenzarchitektur auf der „Movement Control“ Schicht und weist Schnittstellen zum TMS und zum Teilsystem ATO-OBU auf. Das Teilsystem ATO-TS hat die Aufgabe, die von dem Teilsystem **ATO-Execution** (Teil des TMS) generierten betrieblichen- und infrastrukturbezogenen Daten (Journey-Profiles und Segment-Profiles) an die mit dem ATO-TS verbundenen Züge zu übertragen. Journey-Profiles enthalten dabei die sogenannten Fahrschranken, Haltepositionen, Entfernung zu den Fahrschranken und zu Haltepositionen.

Im Gegenzug leitet das Teilsystem ATO-TS die von den Zügen empfangenen Statusdaten an das TMS, um daraus in Echtzeit die Journey-Profiles (JP) anzupassen. Das Teilsystem ATO-TS fungiert also als ein standardisierter Vermittler zwischen dem TMS und den einzelnen Zügen, die mit ATO-OBU ausgestattet sind.

Das fahrzeugseitige Teilsystem ATO-OBU befindet sich in der RCA-Referenzarchitektur auf der „Device Control“ Schicht und weist Schnittstellen zur Fahrzeugleittechnik und zum Teilsystem ATO-TS auf. Das Teilsystem ATO-OBU hat die Aufgabe aus den empfangenen Fahraufträgen und Infrastrukturdaten ein Geschwindigkeitsprofil zu erstellen und die Geschwindigkeit des Zuges entsprechend des erstellten Geschwindigkeitsprofils zu regeln. Dazu werden von dem Teilsystem ATO-OBU Steuerbefehle an die Fahrzeugleittechnik übertragen *(ERA 2018)*. Wie bereits oben erwähnt, hat das Teilsystem ATO-OBU zudem die Aufgabe in regelmäßigen zeitlichen Abständen Statusmeldungen an das Teilsystem ATO-TS zu übertragen und ggf. Fahraufträge anzufordern.

Die RCA-Referenzarchitektur mit den beiden ATO-Teilsystemen wird in der Abbildung 1 dargestellt. Da die anderen technischen Systeme innerhalb der RCA-Referenzarchitektur nicht im Fokus der Arbeit liegen, wird auf ihre Beschreibung an dieser Stelle verzichtet.

[1] Deployment Architektur oder Physikalische Systemarchitektur ist die Organisation von (physischen) technischen Systemen, die aus konkreter Hardware bestehen. D.h., dass die funktionale Systemarchitektur mit konkreten Hardwaresystemen einschließlich der Art der Daten und ihrer Allokationplattform realisiert wird, sodass daraus ein Produkt bzw. ein Prozess entsteht.

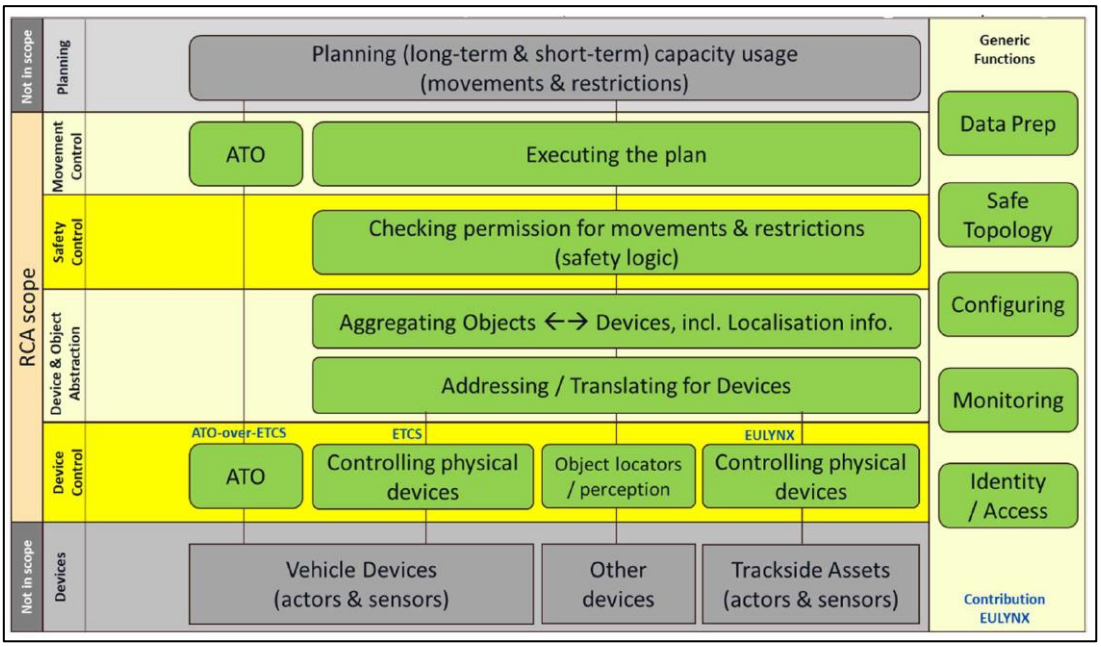

Abbildung 1 Das ATO-System in der RCA-Referenzarchitektur *(EUG 2020a)*

Entsprechend der RCA ist bei der Spezifikation des ATO-Systems im aktuellen Forschungsstand nur der Automatisierungsgrad GoA2 durchgeführt worden *(ERA 2018)*.

Wenngleich der vollautomatisierte Bahnbetrieb nicht im Fokus der RCA ist, wird darin auch – unabhängig von dem Automatisierungsgrad – die Relevanz von Lösungsansätzen für den Umgang mit Störungssituationen adressiert *(EUG & EULYNX 2020b)*. Die im Rahmen dieser Arbeit zu entwickelnden betrieblich-technischen Rückfallebenen zahlen somit in die Ziele der Forschungsinitiative RCA ein.

Insbesondere hinsichtlich der Zuverlässigkeit und Verfügbarkeit wird von der RCA für den vollautomatisierten Bahnbetrieb für Störungssituationen, bei denen ein menschlicher Eingriff nicht oder nur bedingt möglich ist, Redundanzen in der Systemarchitektur gefordert *(EUG & EULYNX 2020b)*.

Wegen des Betriebskontinuitätsmanagements (engl. Business Continuity Management, BCM) als auch aufgrund der rechtlichen Forderung sind neben Redundanzen in der Systemarchitektur auch Betriebsprozesse für den Umgang mit Störungssituationen (betrieblich-technische Rückfallebenen) erforderlich. Die Spezifikation von derartigen Betriebsprozessen für Störungssituationen ist nicht im Fokus der RCA. Statt Betriebsprozesse zu definieren, legt die RCA – wie bereits oben erwähnt – den Fokus darauf, die für den digitalen und vollautomatisierten Bahnbetrieb relevanten technischen Systeme und ihre Schnittstellen zueinander einheitlich zu definieren. Die Entwicklung von Betriebsprozessen für Störungssituationen wird auf die nationalen Infrastrukturbetreiber übertragen *(EUG & EULYNX 2020b)*

OCORA

OCORA ist eine Ergänzung zur RCA, bei der sich verschiedene europäische Eisenbahnverkehrsunternehmen (DB, SNCF, NS, ÖBB und SBB) zusammengeschlossen haben, um eine einheitliche Referenzarchitektur für die nächste Generation der Fahrzeugausrüstung zu spezifizieren.

OCORA hat zum Ziel, durch die einheitliche Referenzarchitektur die für den digitalen Bahnbetrieb erforderlichen fahrzeugseitigen technischen Systeme (u.a. ATO-OBU) leicht zu migrieren. Dies soll in Übereinstimmung mit und ergänzend zur RCA erfolgen.

Im Vergleich zur RCA umfasst die Spezifikation der fahrzeugseitigen Referenzarchitektur bereits den vollautomatisierten Bahnbetrieb. Die Spezifikation der für den digitalen Bahnbetrieb erforderlichen

fahrzeugseitigen technischen Systeme für den vollautomatisierten Bahnbetrieb erfolgt mit abstrakt funktionalen Blöcken (engl. Building Blocks).

Diese funktionalen Blöcke sind losgelöst von konkreter Soft- und Hardware (Deployment) auf einem höheren Abstraktionslevel spezifiziert. Die funktionalen Blöcke weisen genau definierte Schnittstellen zu anderen funktionalen Blöcken in der OCORA-Referenzarchitektur auf.

Folgende funktionale Blöcke werden bei OCORA im Zusammenhang mit den beiden Automatisierungsgraden GoA3 und GoA4 spezifiziert *(OCORA 2022b)*.

Perception Sensors (P-Sensors): Hierbei handelt es sich um verschiedene Sensoren, mit denen – wie bereits in Unterkapitel 2.4.1 erläutert, die Hinderniserkennung übernommen wird. Die genauen Sensorarten werden dabei nicht näher spezifiziert.

„Perception System (PSs)“ ist ein weiterer funktionaler Block im Zusammenhang mit den beiden Automatisierungsgraden GoA3 und GoA4. Dieser funktionale Block hat die Aufgabe, die von den Sensoren (P-Sensors) bereitgestellten Sensordaten zu fusionieren und den fusionierten Sensordaten eine Bedeutung zuzuordnen.

Neben den Sensoren zur Hinderniserkennung gibt es im Rahmen von OROCA auch einen funktionalen Block zu den Ortungssensoren (**engl. Vehicle Localisation Sensors, VL Sensors).** Ortungssensoren liefern dem **Vehicle Localisation Systems** (VLS) Sensordaten zur Bestimmung von Geschwindigkeit, Fahrtrichtung, Beschleunigung und Position. Das VLS fusioniert daraufhin diese Sensordaten und stellt diese den anderen funktionalen Blöcken (z.B. ATO Vehicle) zur Weiterverarbeitung bereit.

In dem funktionalen Block **ATO-Vehicle** wird dann das Geschwindigkeitsprofil, das abgefahren werden soll, erstellt.

In Bezug auf die Störungssituationen im vollautomatisierten Bahnbetrieb gibt es bei der aktuellen Version von OCORA (Gamma) noch keine Bestrebungen. Es werden lediglich die beiden funktionalen Blöcke **Automatic Train Operation Monitoring (ATOM) und Remote Manual Train Operation (RMTO)** spezifiziert. Der funktionale Block ATOM soll Zugfahrten im vollautomatisierten Bahnbetrieb aus der Leitstelle der EVU überwachen. Der funktionale Block RMTO soll dann im Falle von Störungen eine Fernsteuerung aus der Leitstelle ermöglichen.

Schließlich wird bei OCORA auch die fahrzeugseitige Kommunikationsarchitektur spezifiziert. Die funktionalen Blöcke sollen mit der spezifizierten fahrzeugseitigen Kommunikationsarchitektur innerhalb einer Hardware-Rechenplattform oder zwischen mehreren Hardware-Rechenplattformen miteinander kommunizieren können. Als Kommunikationsschnittstelle zwischen den fahrzeugseitigen- und den infrastrukturseitigen technischen Systemen soll das bereits oben vorgestellte **FRMCS** eingesetzt werden.

Die in OCORA für den vollautomatisierten Bahnbetrieb spezifizierten fahrzeugseitigen funktionalen Blöcke (engl. Building Blocks,) können wie folgt aufgelistet werden:

- Perception Sensors (P-Sensors)
- Perception System (PSs)
- Vehicle Localization Sensors
- Vehicle Localization System
- Digital Map
- Vehicle Supervisor (VS) (ETCS-OBU)
- ATO-Vehicle und
- FRMCS Mobile Gateway.

Analog zur RCA werden bei OCORA auch keine Betriebsprozesse definiert. Stattdessen werden die funktionalen Blöcke in der OCORA-Systemarchitektur nach bestimmten Gestaltungsprinzipien, die als Anforderungen von den Stakeholdern zusammengestellt wurden, spezifiziert *(OCORA 2020a)*. Diese Anforderungen können daher auch im weiteren Verlauf der Arbeit bei der Entwicklung von Lösungsansätzen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb zugrunde gelegt werden.

2.3.3 ATO-System in Europes-Rail Joint Undertaking (ERJU)

Seit Herbst 2022 gibt es eine weitere europäische Partnerschaft (engl. Europes-Rail Joint Undertaking, ERJU) für Forschung und Innovation im Schienenverkehr, die als Nachfolge von Shift2Rail im Rahmen von Horizon Europe gegründet wurde.

ERJU zielt darauf ab, die Forschung und Entwicklung innovativer Technologien und betrieblicher Lösungen zu beschleunigen und die Wettbewerbsfähigkeit des Eisenbahnsektors und der europäischen Eisenbahnzulieferindustrie zu fördern.

Das ERJU ist organisatorisch in den sogenannten System-Pillar (SysP) und den Innovation-Pillar (IP) unterteilt.

Das System-Pillar stellt eine europaweite Plattform dar und bietet dem Eisenbahnsektor die Möglichkeit, sich über die Entwicklung des zukünftigen Eisenbahnsystems zu verständigen. Die Entwicklung umfasst dabei die Betriebskonzepte und die zugrundeliegende Systemarchitektur des digitalen Bahnbetriebs. Um sowohl technische als auch betriebliche Interoperabilität zu erreichen, sollen im System-Pillar die grundlegenden Gestaltungsprinzipien für eine harmonisierte Systemarchitektur des digitalen Bahnbetriebs festgelegt und Betriebskonzepte erarbeitet werden. Die Betriebskonzepte umfassen dabei sowohl den Regelbetrieb als auch den Betrieb in Störungssituationen.

Zwischen dem System-Pillar und dem Innovation-Pillar herrscht eine intensive Zusammenarbeit. Das System-Pillar liefert Inputs an das Innovation-Pillar, das dann anhand der Inputs Ergebnisse an das System-Pillar zurückliefert.

Als Inputs werden im System-Pillar Anforderungen an die harmonisierte Referenzarchitektur des digitalen Bahnbetriebs und Anforderungen an die harmonisierten Betriebskonzepte definiert und dabei sichergestellt, dass die Modularität für die notwendige Flexibilität eingehalten wird, um langfristig Innovationen zu gewährleisten. Das Innovation-Pillar hat dann die Aufgabe, anforderungsgerechte Forschung durchzuführen und das Ergebnis der jeweiligen Forschungstätigkeit an das System-Pillar zu liefern.

Aktuell sind insgesamt fünf Forschungsbereiche definiert worden, von denen sich ein Forschungsbereich mit dem vollautomatisierten Bahnbetrieb (engl., Digital and Automated Train Operation, Digital ATO) beschäftigt.

Innerhalb des Forschungsbereichs Digital ATO sollen zum einen die in RCA und OCORA entstandenen Referenzarchitekturen weiter im Detail spezifiziert werden. Zum anderen sollen harmonisierte Betriebskonzepte für den vollautomatisierten Bahnbetrieb erarbeitet werden.

Zum Zeitpunkt des Verfassens dieser Arbeit gibt es jedoch von der ERJU noch keine Veröffentlichungen zu den geplanten Forschungsprojekten, die in das Ziel dieser Arbeit einzahlen würden (z.B. geplante Betriebskonzepte für den vollautomatisierten Bahnbetrieb).

2.3.4 ETCS als zugrundeliegendes Zugsicherungssystem

Das europäische Zugsicherungssystem (engl., European Train Control System, ETCS), das in Zukunft von den europäischen Bahnbetreibern als einheitliches Zugsicherungssystem verwendet werden soll, soll die nationalen Zugsicherungssysteme (z.B. in PZB oder LZB in Deutschland) ablösen und somit einen interoperablen Bahnbetrieb ermöglichen.

Das ETCS-System besteht aus einem infrastrukturseitigen (ETCS-Zentrale) und einem fahrzeugseitigen Teilsystem (ETCS-OBU). Die beiden Teilsysteme können in weitere Systemelemente unterteilt werden. Das ETCS-System bildet damit die Schnittstelle zwischen der fahrzeugseitigen und der infrastrukturseitigen Sicherungstechnik (DSTW). Im Folgenden erfolgt eine Kurze Beschreibung des ETCS-Systems im Zusammenhang mit dem ATO-System. Dabei dienen die bereits veröffentlichten Systemanforderungsspezifikationen (engl., System Requirements Specification, SRS) und die Quellen *(Trinckauf et al. 2020)* und *(Schnieder 2019)* als Grundlage.

Das ETCS-System umfasst drei verschiedene Ausrüstungsstufen, sogenannte Level. Bei der ersten Ausrüstungsstufe (**ETCS Level 1)** sind ortsfeste Signale weiterhin vorhanden und die Übermittlung von Fahrterlaubnissen (engl., Movement Authorities, MA) erfolgt über eine am Fahrweg verbaute Balise. Dazu ist zunächst erforderlich, die Zustimmung zur Fahrt am Signal oder im Stellwerk auszulesen. Dazu wird eine Lineside Electronic Unit (LEU) installiert, welche in Abhängigkeit der Signal- oder Fahrstraßeninformation die Fahrterlaubnis (auch andere ETCS-Datentelegramme) an die Balisen übermittelt.

Bei der zweiten Ausrüstungsstufe (**ETCS Level 2)** erfolgt die Übermittlung dagegen über eine funkbasierte Kommunikationsschnittstelle. Dabei fungiert die ETCS-Zentrale (engl., Radio Block Center, RBC) als Vermittler zwischen dem ETCS-OBU und der Sicherungstechnik. Aufgrund der durchgehenden Kommunikationsverbindung zwischen der ETCS-Zentrale und den Zügen können die Züge kontinuierlich überwacht und mit den relevanten Führungsgrößen versorgt werden. Daher ist prinzipiell eine ortsfeste Signalisierung nicht mehr erforderlich (ETCS Level 2 ohne Signale). Diese werden heute dennoch teilweise als Rückfallebene oder für den Mischverkehr beibehalten. Die sichere Abstandsregelung (im Raumabstand) besteht bei ETCS Level 2 weiterhin. Die fahrwegseitigen Balisen dienen zur Ortung und zur Kalibrierung des fahrzeugseitigen Odometer-Systems.

Schließlich gibt es auch die dritte Ausrüstungsstufe (**ETCS Level 3)**, die sich von ETCS Level 2 darin unterscheidet, dass neben der ortsfesten Signalisierung zusätzlich auch die Gleisfreimeldeeinrichtungen nicht mehr erforderlich sind. Die Ortung der Züge erfolgt über zugseitige Ortungssysteme.

Damit die sichere Abstandshaltung zwischen den Zügen weiterhin sichergestellt werden kann, ist bei ETCS Level 3 eine kontinuierliche Zugintegritätsprüfung erforderlich. Die Fahrterlaubnisse werden bei ETCS Level 3 nur versendet, wenn die Züge ihre aktuelle Position einschließlich der Zugintegritätsbestätigung an die ETCS-Zentrale übermittelt haben.

Prinzipiell ist es möglich, in allen drei Ausrüstungsstufen einen vollautomatisierten Bahnbetrieb durchzuführen, jedoch wird in der aktuellen Spezifikation der ATO-over-ETCS die zweite Ausrüstungsstufe (ETCS Level 2) ohne Signale zugrunde gelegt *(ERA 2018)*. Die Spezifikation von ETCS Level 3 ist noch nicht abgeschlossen. Deshalb bezieht sich im weiteren Verlauf der Arbeit der ETCS-Begriff immer auf ETCS Level 2 ohne Signale.

Im ETCS-System sind zur Abbildung von unterschiedlichen betrieblichen Anforderungen auch verschiedene Betriebsarten definiert. Während die Betriebsart Full-Supervision (FS) im Regelbetrieb eine Zugfahrt vollüberwacht, gibt es zwei Betriebsarten, die auch im Kontext dieser Arbeit relevant sind,

da für diese im vollautomatisierten Bahnbetrieb Lösungen erforderlich sind. Diese Betriebsarten sind On-Sight (OS) und Staff-Responsible (SR).

Die Betriebsart OS repräsentiert das Fahren auf Sicht aus dem gegenwärtigen Bahnbetrieb und wird daher bei nicht mehr Sicherstellung der Abstandshaltung zwischen zwei Zügen – z.B. aufgrund von Störungen an Gleisfreimeldeeinrichtungen – angewendet. Für die Betriebsart OS existiert eine Höchstgeschwindigkeit (in Deutschland 40 km/h), die von der ETCS-OBU überwacht wird. Dennoch ist im gegenwärtigen Bahnbetrieb ein Triebfahrzeugführer für die Überwachung des Freiseins des vorausliegenden Streckenabschnitts verantwortlich. Wenngleich die Betriebsart OS auch im vollautomatisierten Bahnbetrieb weiterhin angewandt werden kann, sind noch Lösungsansätze für die Überwachung des Freiseins des vorausliegenden Streckenabschnitts durch technische Systeme zu entwickeln.

Die Betriebsart SR wird beim Fehlen von Fahrterlaubnis angewandt. Die Ursachen dafür können z.B. Aufrüsten des Fahrzeugs, Verlust der Kommunikationsverbindung oder durch anderweitige Störungen am ETCS-System sein. Für die Betriebsart SR gibt es bereits Lösungsansätze für die Fortführung des Betriebs, die im nächsten Kapitel vorgestellt werden. Für den vollautomatisierten Bahnbetrieb sind jedoch insbesondere im Falle von Verlust der Kommunikationsstörung Lösungen zur Fortführung des Betriebs erforderlich.

2.3.5 ATO-System in Communication-Based-Train Control System (CBTC)

Wie bereits in Unterkapitel 2.1.2 vorgestellt, wird bei Nahverkehrsbahnen (Metro-Systemen) der Betrieb seit über drei Jahrzenten vollautomatisiert durchgeführt. Die dabei dem vollautomatisierten Betrieb zugrundeliegende Systemarchitektur ist das sogenannte Communication-Based-Train Control System (CBTC). Innerhalb der CBTC-Systemarchitektur werden dem ATO-System nach *IEEE (2005)* folgende Funktionen zugewiesen:

- Bestimmung des Geschwindigkeitsprofils
- Bestimmung der Haltepositionen (Betriebsstellen)
- Geschwindigkeitsregelung
- Türsteuerung und
- Datenmanagement (fahrzeugseitige Verarbeitung und Übertragung an die Leitstelle)

Aus den Spezifikationsdokumenten des CBTC-Systems *(IEEE 2005)* und *(IEEE 2003)* können jedoch keine Betriebsprozesse – insbesondere für Störungssituationen – entnommen werden.

2.3.6 Zwischenfazit Kapitel 2.3

Das Zwischenfazit bisher aus dem Kapitel 2.3 ist, dass in den nationalen und europäischen Forschungsinitiativen die für den vollautomatisierten Bahnbetrieb relevanten technischen Systeme spezifiziert werden. Jedoch ist die Interaktion (Schnittstellen zueinander und Art des Datenaustausches) der technischen Systeme untereinander nicht vorhanden. Diese Interaktion ist erforderlich, um Störungssituationen im vollautomatisierten Bahnbetrieb aus den technischen Systemen erarbeiten zu können. Außerdem existieren aus den bisherigen Forschungsaktivitäten in RCA und OCORA noch keine Betriebsprozesse für den vollautomatisierten Bahnbetrieb. Dass noch keine Betriebsprozesse für den vollautomatisierten Bahnbetrieb existieren, wird damit verargumentiert, dass die Gestaltung von Betriebsprozessen mit vielen nationalen Besonderheiten (z.B. unterschiedliche technische Systeme, Sicherheitsanforderungen, gesetzliche und regulatorische Vorgaben, etc.) verbunden ist *(EUG 2020a)*.

Damit Betriebsprozesse für den vollautomatisierten Bahnbetrieb entwickelt werden können, ist das Zusammenspiel (logische Beziehung) der in Kapitel 2.4 vorgestellten technischen Systeme zueinander erforderlich *(Hirshorn 2007, S. 62)*. Ausgehend von der in RCA und OCORA angefangener Spezifikation der für den vollautomatisierten Bahnbetrieb relevanten technischen Systeme steht die Entwicklung von Betriebsprozessen für den vollautomatisierten Bahnbetrieb bei ERJU im Fokus, jedoch gibt es zum Zeitpunkt des Verfassens dieser Arbeit noch keine Veröffentlichungen zu den geplanten Betriebsprozessen.

2.4 Lösungen für den Umgang mit Störungssituationen im Bahnbetrieb

Unabhängig von den zuvor vorgestellten Forschungsinitiativen gibt es auch vereinzelt Veröffentlichungen zu möglichen Lösungsansätzen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb, die hauptsächlich auf die Lösungen aus dem gegenwärtigen Bahnbetrieb beruhen. Daher werden in diesem Kapitel Lösungen für den Umgang mit Störungssituationen im gegenwärtigen Bahnbetrieb und darauf basierend mögliche Lösungsansätze für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb (GoA3 und GoA4), die in der Literatur vorgeschlagen werden, vorgestellt.

Zunächst wird in Unterkapitel 2.4.1 die Relevanz von betrieblich-technischen Rückfallebenen im gegenwärtigen Bahnbetrieb vorgestellt. Daraufhin werden in Unterkapitel 2.4.2 die gegenwärtigen betrieblich-technischen Rückfalleben vorgestellt. Danach werden in Unterkapitel 2.4.3 mögliche Lösungsansätze für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb, die in der Literatur vorgeschlagen werden, vorgestellt.

Schließlich werden in Unterkapitel 2.4.5 relevante Bewertungsziele beim Umgang mit Störungssituationen im Bahnbetrieb und dazugehörige Bewertungsverfahren vorgestellt.

2.4.1 Relevanz von Rückfallebenen und ihre Anwendung im Bahnbetrieb

Aufgrund der Tatsache, dass der Bahnbetrieb nicht auf Vorrat produziert, sind für Störungssituationen entsprechende betrieblich-technische Rückfallebenen erforderlich. Bei den heutigen betrieblich-technischen Rückfallebenen nimmt ein Triebfahrzeugführer eine wesentliche Rolle ein. Mit der Einführung des vollautomatisierten Bahnbetriebs fällt damit eine wesentliche Ressource in Störungssituationen weg. Da technische Systeme in ihrem Lebenszyklus nicht vollständig störungsfrei funktionieren werden, bleibt der Bedarf an betrieblich-technischen Rückfallebenen weiterhin.

Der Begriff „Rückfallebene“ wird im Allgemeinen häufig im Zusammenhang mit sicherheitsrelevanten Systemen verwendet und ist daher ein wesentlicher Bestandteil der Informationstechnik und der Eisenbahndomäne.

In der Informationstechnik wird die Rückfallebene definiert als *„Verhinderung des Totalausfalls eines Systems. Oft besitzt die Rückfalllösung einen verminderten oder eingeschränkten Funktionsumfang, ist aber dennoch in der Lage, den Betrieb des Systems mit den wichtigsten Funktionen über einen bestimmten Zeitraum aufrecht zu erhalten. Nach der Wiederherstellung der primären Versorgung wird die Fallbacklösung deaktiviert und der ursprüngliche Betrieb wiederaufgenommen“ (NFON 2023)*.

In der Automobildomäne wird der Begriff bei sicherheitsrelevanten Komponenten verwendet und nach *Winner et al. (2015)* gleichgesetzt mit der Restverfügbarkeit der Systemfunktionalität.

Auch in der Eisenbahndomäne ist der Begriff der Rückfallebene geläufig. So definiert *Pachl (2011, S. 87)* den Begriff als *“Weiterführung des Betriebs mit eingeschränktem Leistungsverhalten“*

und *Maschek (2015, S. 191)* als *„Verfahren, um den Betrieb bei Ausfall von Systemen oder Komponenten weiterzuführen“*.

Aus den drei Definitionen lässt sich ableiten, dass Rückfallebenen als ein Sekundärsystem oder als eine Ersatzfunktionalität dienen, um bei Störungen von sicherheitsrelevanten technischen Systemen die Verfügbarkeit des Betriebs zu gewährleisten und dabei den Totalausfall des Gesamtsystems zu verhindern.

Damit kann – auch in Anlehnung an EN 50126 und RCA – zwischen zwei Arten von Rückfallebenen differenziert werden, von denen beide im Bahnbetrieb angewandt werden. Diese sind technische Rückfallebenen und betrieblich-technische Rückfallebenen.

Technische Rückfallebenen werden in Form von technischen Redundanzen in der Systementwicklungsphase berücksichtigt und können durch geeignete Designmuster in der Hardware oder Software wie z.B. strukturelle Redundanz, funktionelle Redundanz, Informationsredundanz und Zeitredundanz realisiert werden *(Bertsche 2009, S. 94)*. Während bei einer strukturellen Redundanz ein technisches System mehrfach vorhanden ist, umfasst die funktionelle Redundanz zusätzliche, für den Regelbetrieb nicht erforderliche Funktionen. Informationsredundanz bezeichnet das Vorhandensein zusätzlicher, über den Nutzinhalt hinausgehender, Informationen in einer Funktion oder in einem technischen System. Die Zeitredundanz beschreibt die Zeit, die für die Erbringung der funktionellen Redundanz zur Verfügung steht.

Durch diese Designmuster ist es möglich, sowohl systemimmanente systematische als auch zufällige Fehler zu erkennen und adäquat darauf zu reagieren. Bei sicherheitsrelevanten technischen Systemen ist die Reaktion häufig, dass sich ein Ausfall immer zur sicheren Seite auswirkt (im Bahnbetrieb meist der energielose Zustand). Sofern vorhanden, erfolgt aus Verfügbarkeitsgründen die Aktivierung des sekundären technischen Systems zur Übernahme der Funktion des gestörten primären technischen Systems (z.B. zweiter Glühfaden in einem Signal oder Ersatzsignal im Falle von Störungen am Hauptsignal). Technische Rückfallebenen werden bei der Entwicklung von sicherheitsrelevanten technischen Systemen für den Bahnbetrieb von den Forschungsinitiativen und von den Normen 50128 und 50129 gefordert (*DIN EN 50128:2011*) und *(DIN EN 50129:2018)*.

Wie bereits oben erwähnt, produzieren Verkehrssysteme nicht auf Vorrat. Sofern ein technisches System aufgrund einer Störung eine Fail-Safe Reaktion auslöst, ist das Warten bis zur Instandsetzung des gestörten technischen Systems aufgrund der Verfügbarkeitsforderung der Stakeholder nicht hinnehmbar. Daher sind zur Weiterführung des Betriebs Verfahren in Form von betrieblich-technischen Rückfallebenen erforderlich. Entsprechend der Definition oben soll durch betrieblich-technische Rückfallebenen der Betrieb auch mit verminderter Sicherheit und Betriebsqualität fortgeführt werden. Dass in den gegenwärtigen betrieblich-technischen Rückfallebenen potenziell von einem geringeren Sicherheitsniveau als im Regelbetrieb ausgegangen wird, liegt daran, dass das Betriebspersonal (Triebfahrzeugführer und Fahrdienstleiter) die Verantwortung über die Funktionen des primären technischen Systems übernimmt und es in Abhängigkeit der Auslastung fehleranfällig sein kann. Betrieblich-technische Rückfallebenen können in drei Tätigkeitsfelder unterteilt werden, die in *Huang (2020)* beschrieben werden. Diese drei Tätigkeitsfelder umfassen die Betriebsleitung, die Betriebsführung und die Ereignisbehandlung. Die Abbildung 2 stellt die drei Tätigkeitsfelder grafisch dar.

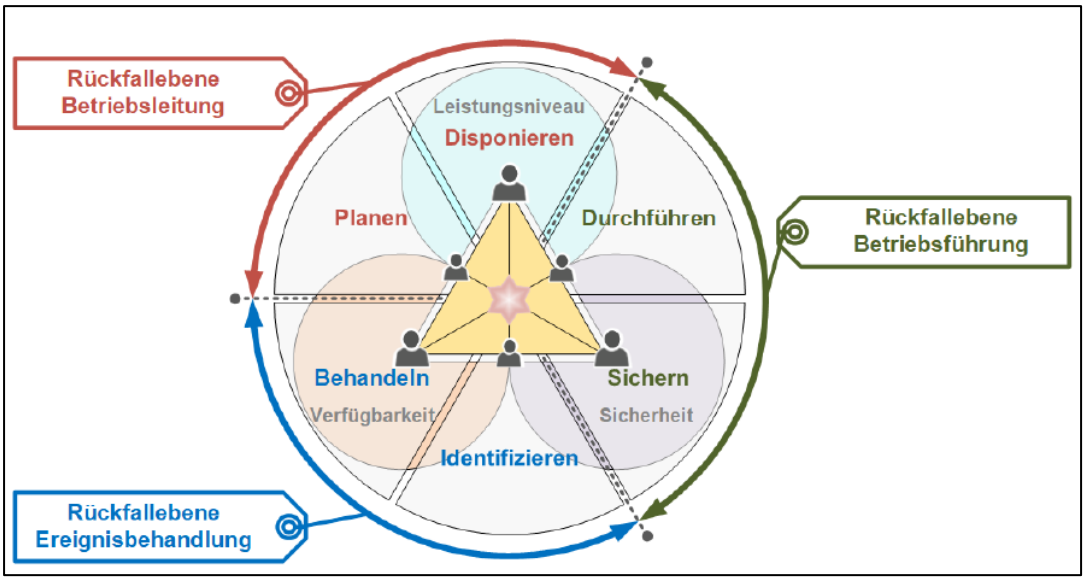

Abbildung 2 Tätigkeitsfelder innerhalb der betrieblichen-technischen Rückfallebene nach *Huang (2020)*

In der Betriebsleitung stehen Aufgaben der Disposition, bei denen Störfallprogramme angewandt werden, wodurch die Zugfahrten entsprechend der vorliegenden Störungssituation ggf. abweichend vom ursprünglichen Fahrplan erneut geplant werden. Dabei können beispielsweise Zugfahrten vorzeitig ausfallen, wenden oder ihre Reihenfolge geändert werden.

In der Betriebsführung hingegen geht es – wie bereits oben erwähnt – darum, die Schutzziele, die durch das gestörte technische System im Regelbetrieb erfüllt wurden, ersatzweise durch das Betriebspersonal zu übernehmen und die Zugfahrten ggf. ohne technische Sicherung durchzuführen. In der Betriebsführung arbeiten Fahrdienstleiter und Triebfahrzeugführer zusammen. Sie übernehmen in der Betriebsführung ersatzweise sicherungstechnische Funktionen, um den Betrieb weiterhin mit ggf. reduzierter Betriebsqualität aufrechterhalten zu können.

Die Ereignisbehandlung als drittes Tätigkeitsfeld befasst sich damit, die Ursachen und Folgen der Störungssituation zu identifizieren und die voraussichtliche Dauer einer Störungssituation einzuschätzen sowie das Beheben der vorliegenden Störung zu initiieren. Die voraussichtliche Dauer einer Störungssituation hat entsprechend Auswirkungen auf die Dauer der Betriebsführung in der betrieblich-technischen Rückfallebene.

Wie bereits in Unterkapitel 2.3.2 erwähnt, sind sowohl wegen des Betriebskontinuitätsmanagements als auch aufgrund der rechtlichen Forderung betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im Bahnbetrieb vorzuhalten. Mit dem Betriebskontinuitätsmanagement haben Betreiber die Pflicht und Verantwortung, den regulären Betrieb nach störungsbedingter Unterbrechung in kürzester Zeit wiederaufzunehmen, um dabei die verletzten Schutzziele der LST ersatzweise zu gewährleisten und die Abweichung von der vereinbarten Betriebsqualität zu minimieren *(Pachl 2007)*.

Die rechtliche Forderung geht auf EU-Richtlinien und auf die technische Spezifikation der Interoperabilität (TSI) zurück.

In der EU-Richtlinie EU 2016/797 Anhang III, Abschnitt 2.3.1 wird folgendes bezüglich der betrieblich-technischen Rückfallebenen vorgeschrieben: *„Die Anlagen und Verfahren der Zugsteuerung/Zugsicherung*

und Signalgebung müssen einen Zugverkehr entsprechend den Sicherheitsvorgaben für das Netz ermöglichen. Die Zugsteuerungs-/Zugsicherungs- und Signalgebungssysteme müssen weiterhin den sicheren Verkehr von Zügen ermöglichen, deren Weiterfahrt unter vorgegebenen Einschränkungen gestattet ist" (Europäische Union 2016, S. 91).

Eine weitere Forderung nach betrieblich-technischen Rückfallebenen ist in derselben Richtlinie im Anhang II, Abschnitt 2.5 (Betriebsführung und Verkehrssteuerung) zu finden: *„Verfahren und zugehörige Ausrüstungen, die eine kohärente Nutzung der verschiedenen strukturellen Teilsysteme erlauben, und zwar sowohl im Normalbetrieb als auch bei Betriebsstörungen, einschließlich insbesondere der Zugbildung und Zugfahrten, der Planung und der Abwicklung der Betriebsführung" (Europäische Union 2016, S. 87)*.

Ferner regelt auch der Artikel §54 der Richtlinie 2012/34/EU, dass *„bei technisch bedingten oder unfallbedingten Störungen der Zugbewegungen der Infrastrukturbetreiber alle erforderlichen Maßnahmen zu treffen hat, um die Situation wieder zu normalisieren" (Europäische Union 2012b, S. 57)*.

Nach der Technischen Spezifikation für die Interoperabilität müssen *„der Infrastrukturbetreiber in Verbindung mit allen Eisenbahnverkehrsunternehmen, die seine Infrastruktur benutzen, und ggf. benachbarte Infrastrukturbetreiber gemeinsam geeignete Wiederherstellungsmaßnahmen festlegen, veröffentlichen und verfügbar machen sowie die jeweiligen Verantwortlichkeiten festlegen, um der Forderung nach Verringerung der negativen Auswirkungen bei gestörtem Betrieb zu entsprechen" (Europäische Union 2012a, S. 30)*.

Da bereits Lösungen für die Betriebsleitung in diversen Forschungsprojekten am Institut für Bahnsysteme und Bahntechnik erforscht werden *(Crespo 2020)* und *(Brauner 2022)*, stehen die beiden Tätigkeitsfelder Betriebsleitung und Ereignisbehandlung im Weiteren verlauf der Arbeit nicht im Fokus.

Im nächsten Unterkapitel werden einige betrieblich-technische Rückfallebenen aus dem gegenwärtigen Bahnbetrieb (Betriebsführung) für den Umgang mit Störungssituationen vorgestellt.

2.4.2 bestehende betrieblich-technische Rückfallebenen aus dem gegenwärtigen Bahnbetrieb für den Umgang mit Störungssituationen

Nach *Pachl (2017, S. 18)* sind im vollautomatisierten Bahnbetrieb *„nur diejenigen Rückfallebenen relevant, bei denen [heute] ein Triebfahrzeugführer mitwirken muss". Keine Relevanz haben Rückfallebenen, bei denen der Fahrdienstleiter zwar in Personalverantwortung Hilfshandlungen zur ersatzweisen Fahrweg- und Zugfolgesicherung ausführen muss, die Zugfahrt aber trotzdem durch Signaleinrichtungen zugelassen wird."* Daher werden in diesem Unterkapitel diejenigen betrieblich-technischen Rückfallebenen vorgestellt, bei denen ein Triebfahrzeugführer im gegenwärtigen Betrieb aktiv mitwirken muss, um ein Grundverständnis über die Verantwortung und Aufgaben eines Triebfahrzeugführers in Störungssituationen zu schaffen. Damit ein Triebfahrzeugführer Handlungsanweisungen von einem Fahrdienstleiter in Störungssituationen erhalten kann, wird der sogenannte Befehlsvordruck verwendet. Um die Sicherheit des Betriebs in Störungssituationen möglichst nicht zu beeinträchtigen, gibt es zudem die Möglichkeit, sofern im Stellwerk projektiert, Handlungsanweisungen mit Zusatzsignalen zu ermöglichen. Daher werden zunächst beide Möglichkeiten der Handlungsanweisungen vorgestellt. Auf Basis des Befehls oder der Zusatzsignale können spezielle, auf die Störungssituation abgestimmte, Handlungen angewiesen werden. Diese werden ebenfalls vorgestellt.

Weiterfahrt mit Befehl oder Zusatzsignal

Eine Weiterfahrt mit Befehl beschreibt eine Zugfahrt mit besonderem Auftrag. Eine Zugfahrt mit besonderem Auftrag ist eine Zugfahrt, bei der die technische Sicherung der Zugfolge nicht mehr gewährleistet ist und der Fahrdienstleiter daher eine Fahrterlaubnis über Signalisierung oder in ETCS (über die ETCS-Zentrale) nicht erteilen kann. Der Befehl ist dabei eine schriftliche Zustimmung zur Weiterfahrt, die von einem Fahrdienstleiter an den Triebfahrzeugführer des von der Störung betroffenen Zuges ausgestellt wird.

Der Triebfahrzeugführer hat dabei die Aufgabe, den diktierten schriftlichen Befehl aufzuschreiben und die Befehlsangaben aus Sicherheitsgründen durch Wiederholen auf Plausibilität zu prüfen sowie die Weiterfahrt entsprechend des Befehls durchzuführen.

Mit dem Befehl werden insbesondere Betriebsparameter (z.B. Geschwindigkeit oder Zielpunkt, bis zu dem gefahren werden darf) angepasst. Zur Übermittlung eines Befehls ist eine Kommunikationsverbindung zwischen einem Fahrdienstleiter und einem Triebfahrzeugführer des von der Störung betroffenen Zuges erforderlich.

Sofern im Stellwerk projektiert, kann ein Fahrdienstleiter einen Triebfahrzeugführer eine Weiterfahrt auch mit Zusatzsignalen (z.B. Ersatzsignal (Zs1) oder Vorsichtssignal (Zs7)) im Falle einer Signalstörung erteilen. Ein Fahrauftrag mit Vorsichtsignal erfordert ein Fahren auf Sicht, das als nächstes erläutert wird.

Im Kontext des vollautomatisierten Bahnbetriebs, bei dem die Rolle eines Fahrdienstleiters durch eine Sicherungslogik (vgl. RCA-Referenzarchitektur aus 2.4) und die Rolle eines Triebfahrzeugführers durch das ATO-System übernommen wird, kann eine Befehlsfahrt und auch eine Fahrt mit Ersatzsignal oder Vorsichtsignal in der gegenwärtigen Form nicht umgesetzt werden.

Fahren auf Sicht

Die Betriebsart „Fahren auf Sicht“ stellt eine betrieblich-technische Rückfallebene dar, die durch einen Befehl erteilt werden kann. Die Betriebsart „Fahren auf Sicht“ wird insbesondere dann angewandt, wenn die Streckenbeobachtung die einzige Möglichkeit ist, das Schutzziel „Schutz vor Kollision“ zu erfüllen. Das kann dann vorliegen, wenn beispielsweise in ein möglicherweise besetztes Gleis eingefahren werden soll oder die Gleisfreimeldesysteme gestört sind, sodass eine sichere Abstandshaltung nicht mehr möglich ist.

Beim Fahren auf Sicht trägt der Triebfahrzeugführer eine signifikante Verantwortung. Er ist dafür verantwortlich, die Geschwindigkeit des Zuges so zu regeln, dass er vor Hindernissen jederzeit sicher zum Stehen kommen kann. Dazu überwacht er während der Fahrt kontinuierlich das Freisein des Lichtraums von Hindernissen und regelt gleichzeitig die Geschwindigkeit des Zuges. Er ist dabei verpflichtet, bei gefahrdrohenden Situationen *„in eigener Verantwortung umsichtig und entschlossen alles zu tun, um die Gefahr abzuwenden oder zu mindern“ (DB Netz AG 2016, S. 217)*. Gefahrdrohende Situationen können durch Abweichungen an der Infrastruktur, wie beispielsweise Verformungen an den Schienen (vertikale und horizontale) oder Schienenbrüche, verursacht werden. Beim Fahren auf Sicht kann heute ein Triebfahrzeugführer auch beauftragt werden, das Gleis zu erkunden und das Ergebnis der Erkundung an den zuständigen Fahrdienstleiter zu melden *(DB Netz AG 2016)*. Auch beim Fahren auf Sicht ist die Kommunikation zwischen dem Triebfahrzeugführer und dem zuständigen Fahrdienstleiter notwendig.

Die Betriebsart „Fahren auf Sicht“ ist – wie bereits in Unterkapitel 2.3.4 erläutert – ebenfalls in ETCS als Betriebsart OS spezifiziert. Die ETCS-OBU überträgt in der Betriebsart OS die Verantwortung über die

sichere Abstandshaltung des Zuges an den Triebfahrzeugführer. Die ETCS-OBU überwacht dabei lediglich die Einhaltung der maximal zulässigen Geschwindigkeit. Die Höchstgeschwindigkeit in der Betriebsart OS beim ETCS geführten Zug ist mittels des nationalen Werts V_NVONSIGHT festgelegt *(ERA 2016a, S. 185)*. Manche EVU schränken die Höchstgeschwindigkeit beim Fahren auf Sicht gegenüber den Vorschriften des Infrastrukturunternehmens weiter ein. So wird beispielsweise im Triebfahrzeugführerheft vorgeschrieben, bei Dunkelheit höchstens mit 15 km/h, bei „unsichtigem Wetter“ höchstens mit Schrittgeschwindigkeit und bei „extrem unsichtigem Wetter“ gar nicht zu fahren *(DB Fernverkehr AG 2010)*. Bei einem ETCS geführten Zug kann die Betriebsart OS nicht durch den Triebfahrzeugführer ausgewählt werden, sondern muss von der ETCS-Zentrale angeordnet werden *(ERA 2016b, S. 24)*.

Durch den Wegfall des Triebfahrzeugführers aus dem Führerstand im vollautomatisierten Bahnbetrieb kann jedoch die Betriebsart OS nur durch entsprechende Sensoren zur Hinderniserkennung durchgeführt werden. Die wesentliche Herausforderung beim Fahren auf Sicht im vollautomatisierten Bahnbetrieb liegt darin, die gefahrdrohenden Situationen im Lichtraum mit Hilfe von automatisierten Algorithmen, die mit den Methoden des maschinellen Lernens oder des Deep-Learnings realisiert werden, zuverlässig zu erkennen und adäquat darauf zu reagieren *(Slamal et al. 2022)*.

Durchführen von Sperrfahrten

Im Bahnbetrieb kann es auch vorkommen, dass Züge auf der Strecke aufgrund eines technischen Defekts liegengeblieben sind und daher ihre Fahrt nicht fortsetzen können oder dass beispielsweise ein Gleis unbefahrbar ist oder sich Personen im Gleis befinden *(DB Netz AG 2016)*.

Die betrieblich-technische Rückfallebene, die in solchen Störungssituationen zur Geltung kommt, ist die sogenannte Sperrfahrt. Während einer Sperrfahrt nimmt ein Triebfahrzeugführer eine aktive Rolle ein. Die Sperrfahrt wird ebenfalls durch einen Befehl erteilt. Für die Durchführung einer Sperrfahrt ist es erforderlich, das entsprechende Gleis, auf dem die Sperrfahrt durchgeführt werden soll, zu sperren. Die Sperrung wird durch den zuständigen Fahrdienstleiter durchgeführt. Damit wird sichergestellt, dass nur ein Zug oder eine Hilfslok in das gesperrte Gleis einfährt.

Die wesentlichen Aufgaben des Triebfahrzeugführers bei einer Sperrfahrt umfassen die Kommunikation mit dem zuständigen Fahrdienstleiter, die Kommunikation mit dem Triebfahrzeugführer der Hilfslok und die Sicherstellung, dass die gekuppelten Züge vollständig sind. Diese Vollständigkeitsmeldung ist erforderlich, damit der Fahrdienstleiter die Sperrung aufheben und weitere Züge in das Gleis einlassen kann. Die Sperrfahrt wird mit einer reduzierten Geschwindigkeit – bei geschobenen Sperrfahrten maximal 30 km/h und bei gezogenen Sperrfahrten maximal 50 km/h – durchgeführt.

Die wesentliche Herausforderung bei der Durchführung einer Sperrfahrt im vollautomatisierten Bahnbetrieb liegt darin, dass sich zwei Fahrzeuge (Hilfslok und liegengebliebener Zug) ggf. unbegleitet kuppeln müssen und statt einer verbalen Zustimmung für eine Rück- oder Weiterfahrt eine datenbasierte Zustimmung erforderlich ist.

Sichern von Bahnübergängen (durch Tf)

Bahnübergänge befinden sich auf Strecken, bei denen die zulässige Geschwindigkeit unter 160 km/h ist *(Bundesamt für Justiz 2019)*. Durch Bahnübergänge wird verhindert, dass andere Verkehrsteilnehmer oder Personen unbeaufsichtigt in den Gefahrenbereich (Lichtraum) hineinragen und dadurch eine Gefährdung für den Bahnbetrieb verursachen. In der Regel handelt es sich um technisch gesicherte Bahnübergänge, jedoch können auch nicht technisch gesicherte Bahnübergänge existieren.

Nach *(Trinckauf 2013)* gehört die Sicherung von Gefahrenbereichen nicht zu der Kernaufgabe einer Sicherungstechnik. Es ist die Aufgabe einer Bahnübergangssicherungsanlage, einen herannahenden Zug zu erkennen und diesen als Warnung an die Personen oder andere Verkehrsteilnehmer auszugeben. Die Systemphilosophie besteht dann in dem Vertrauen dahingehend, dass die Personen und Gegenstände nach der Warnung unverzüglich sich aus dem Gefahrenbereich entfernen (*Trinckauf 2013)*.

Sofern aber ein technisch gesicherter Bahnübergang gestört ist, kann ein Triebfahrzeugführer (mit einem Befehl) beauftragt werden, diesen nachzusichern. Dazu muss ein Triebfahrzeugführer nach *DB Netz AG (2016)* vor Bahnübergängen mit offenen Schranken anhalten, bis die Schranken geschlossen sind.

Im vollautomatisierten Bahnbetrieb stellt diese Betriebssituation insofern eine Herausforderung dar, da dafür Sensoren zur Hinderniserkennung erforderlich sind und ein unbegleiteter Zug ggf. die Verkehrsteilnehmer oder Personen warnen muss. Zudem kann es vorkommen, dass der Betrieb aufgrund unvernünftiger Verhaltensweise von anderen Verkehrsteilnehmern gefährdet wird.

Ausfall der Kommunikation bei ETCS geführten Zügen

Im vollautomatisierten Bahnbetrieb ist davon auszugehen, dass der Betrieb unter ETCS Level 2 ohne Signale durchgeführt wird und daher die ortsfesten Signale als Quelle für Führungsgrößen (Fahrterlaubnis) nicht mehr relevant sind. Das Kommunikationssystem GSM-R ist bereits heute ein essenzielles System für den Betrieb unter ETCS Level 2, da die Fahraufträge über Funk übermittelt werden.

Wenngleich im vollautomatisierten Bahnbetrieb das GSM-R System durch das FRMCS abgelöst wird, führt eine Störung des Kommunikationssystems unabhängig vom Kommunikationsstandard bereits heute im Allgemeinen zu großen Betriebseinschränkungen. Aufgrund der zentralen Betriebsführung im Bahnbetrieb und der Tatsache, dass Züge im vollautomatisierten Bahnbetrieb in Zukunft zunehmend anhand von technischen Systemen gesteuert werden, gewinnt die Kommunikation zwischen den Zügen und der Betriebszentrale noch mehr an Bedeutung. Daher ist im vollautomatisierten Bahnbetrieb damit zu rechnen, dass eine Störung des Kommunikationssystems zu großen Betriebseinschränkungen führt. Für den Fall, dass das Kommunikationssystem gestört ist, gibt es heute betrieblich-technische Rückfallebenen, um den Betrieb fortsetzen zu können.

Nach *Haas (2015)* werden zwischen klein– und großräumigen Störungen des Kommunikationssystems unterschieden.

Kleinräumige Störungen liegen vor, wenn eine Funkbasisstation eines begrenzten Streckenbereichs gestört ist. In diesem Fall wirkt sich die Störung beim GSM-R örtlich auf etwa 8 – 12 km aus *(Brandau 2011)*. Nach *Cellarius et al. (2021)* werden die Funkbasisstationen im FRMCS-5G Standard mit 1,9 GHz funken und einen Abstand (engl. inter-site distance) von 4 km zueinander aufweisen. Demnach würde sich eine kleinräumige Störung im FRMCS örtlich auf 4 km auswirken. Großräumige Störungen, die sich aufgrund von Störungen an mehreren Funkbasisstationen oder der ETCS-Zentrale ergeben können, wirken sich örtlich auf mehr als 32 km aus *(Trinckauf et al. 2020, S.232)*

Wenn eine oder mehrere Funkbasisstationen gestört ist, werden die Züge, die entweder im Funkloch fahren oder kurz davor sind, in das Funkloch einzufahren, die Kommunikationsstörung nach Ablauf der Funküberwachungszeit (T_NVCONTACT = 40 s) entdecken und eine Zwangsbremsung einleiten *(ERA 2016a)*. Deswegen werden diese Züge nach *Haas (2015)* auch als „Entdeckerzüge“ bezeichnet.

Die Fahrterlaubnis wird nach dem Stillstand entsprechend der ETCS-Spezifikation auf die Zugspitze gekürzt und beim Überschreiten von 5 min werden die Entdeckerzüge aus dem Speicher der ETCS-Zentrale gelöscht, sodass sie keine Fahrterlaubnisse mehr erhalten können (*Haas 2015)*.

Die Weiterfahrt des Entdeckerzuges erfolgt dann in Betriebsart Staff-Responsible (SR). Dazu kontaktiert der Triebfahrzeugführer den zuständigen Fahrdienstleiter über das öffentliche Mobilfunknetz (Roaming-Netz), der einen Befehl zur Weiterfahrt in der Betriebsart SR erteilt. Die Weiterfahrt erfolgt mit der nach ETCS-Spezifikation maximal zulässigen Geschwindigkeit von V_NVSTFF = 40 km/h bis zur nächsten ETCS-Halttafel *(ERA 2016c)*. Dieser Prozess erfolgt für alle Entdeckerzüge, die sich im Funkloch befinden.

Für die nachfolgenden Züge sind ebenfalls betrieblich-technische Rückfallebenen erforderlich. Sofern die Störung am Kommunikationssystem kürzer als 15 min andauert, kann die betrieblich-technische Rückfallebene „Durchfahren gestörter Funkbereiche“ eingerichtet werden *(Haas 2015)*.

Beim Durchfahren gestörter Funkbereiche richtet der zuständige Fahrdienstleiter einen sogenannten betrieblichen Funklochbereich ein, der größer ist als das tatsächliche Funkloch. Der Beginn und das Ende eines betrieblichen Funklochbereichs müssen am Standort einer ETCS-Halt-Tafel oder eines Blockkennzeichens liegen *(Trinckauf et al. 2020, S. 230)*. Das betriebliche Funkloch ist in seiner Ausdehnung größer als das tatsächliche Funkloch. Die Ausdehnung erfolgt auf beiden Seiten des tatsächlichen Funklochs und überlappen zwei benachbarte und funktionierende Funkzellen. Dadurch kann eine reguläre Verbindung zur ETCS-Zentrale aufgebaut werden. Nachdem der betriebliche Funklochbereich eingerichtet wurde, erhalten die nachfolgenden Züge eine Fahrterlaubnis über das betriebliche Funkloch hinweg. Die maximal zulässige Geschwindigkeit ist dabei auf 160 km/h begrenzt.

Sofern es sich jedoch bei der Störung am Kommunikationssystem um eine großräumige Störung handelt, können Fahrterlaubnisse nicht mehr übertragen werden. In diesem Fall wird in *Haas (2015)* und *(Trinckauf et al. 2020)* die betrieblich-technische Rückfallebene „Fahrt in Betriebsart SR“ vorgeschlagen. Somit ist zwar möglich, den gestörten Funkbereich zu befahren, jedoch führt das aufgrund der maximal zulässigen Geschwindigkeit von V_NVSTFF = 40 km/h zu starken Einschränkungen der Streckenkapazität (Trinckauf et al. 2020).

Auf konventionellen Strecken mit Class-B Systemen (z.B. PZB) sieht die Richtlinie 408 zudem als betrieblich-technische Rückfallebene im Falle einer Kommunikationsstörung den Wechsel in den Modus ETCS Level NTC (PZB/LZB) vor. Der Wechsel in den Level NTC erfolgt ebenfalls über eine Befehlsübermittlung und erfordert daher eine Kommunikation über das öffentliche Mobilfunknetz *DB Netz AG (2016)*.

2.4.3 Aufgaben eines Triebfahrzeugführers während der Zugfahrt in Störungssituationen

Aus dem vorigen Unterkapitel ist bekannt, dass ein Triebfahrzeugführer eine signifikante Rolle während der Betriebsführung in Störungssituationen verantwortet. Dafür übernimmt er sogenannte betriebliche Aufgaben, die in diesem Unterkapitel kurz beschrieben werden. Aus den bisherigen betrieblich-technischen Rückfallebenen (vgl. Unterkapitel 2.4.2) können folgende Aufgaben eines Triebfahrzeugführers in Störungssituationen abgeleitet werden.

Die Wahrnehmung stellt eine unverzichtbare Aufgabe sowohl im Regelbetrieb für die Überwachung des Lichtraums als auch in der betrieblich-technischen Rückfallebene dar. Insbesondere wenn Störungen während der Zugfahrt an fahrzeugseitigen Systemen oder entlang des Fahrwegs (im Lichtraum) auftreten, erfolgt die Lokalisierung und Identifizierung dieser Störungen durch den Triebfahrzeugführer, weshalb die Wahrnehmung unabdingbar ist. Sowohl die Lokalisierung als auch

die Identifikation erfordern die Erfassung von Reizen und daraus die Wahrnehmung für ein richtiges Situationsverständnis.

Im Kern der betrieblich-technischen Rückfallebene kommt es neben der zwischenmenschlichen Kommunikation auch auf die Planungsfähigkeit des Menschen an. Mit der Planung werden Maßnahmen und mögliche Handlungsalternativen anhand der vorliegenden Störung und der Handlungsregeln in den Richtlinien abgewogen und eine zu der aktuellen Störungssituation passende Maßnahme und Handlung ausgewählt. Für die Planung und für das Situationsverständnis ist vom Triebfahrzeugführer betriebliches Wissen bereitzustellen.

Handlungen in der betrieblich-technischen Rückfallebene sind meist sicherheitskritisch und erfordern daher eine besonders hohe Konzentration und Risikobewusstsein der Beteiligten. Deshalb sind verbindlich definierte Handlungsregeln vorhanden. Diese Handlungsregeln liegen in natürlich-sprachlicher Form vor und werden zusätzlich durch die Betriebspersonale erlernt (betriebliches Wissen).

Die Kommunikation zwischen den Beteiligten in der betrieblich-technischen Rückfallebene ist unerlässlich, dabei ist ein Triebfahrzeugführer nicht nur eine Informationssenke, sondern auch eine entscheidende Informationsquelle. Es ist ein hoher Grad an Zusammenarbeit zwischen dem Triebfahrzeugführer und dem Fahrdienstleiter mit konstanter Interaktion gefordert und dabei können einzelne Aufgaben separat ausgeführt dann in Kooperation zu einem Ganzen gefügt werden. Die Zusammenarbeit zwischen dem Triebfahrzeugführer und dem Fahrdienstleiter ist aber hierarchisch geprägt, da z.B. der Fahrdienstleiter immer die Entscheidungshoheit in der betrieblichen Rückfallebene hat. In der Abbildung 3 sind die Aufgaben eines Triebfahrzeugführers in Störungssituationen zusammengefasst dargestellt.

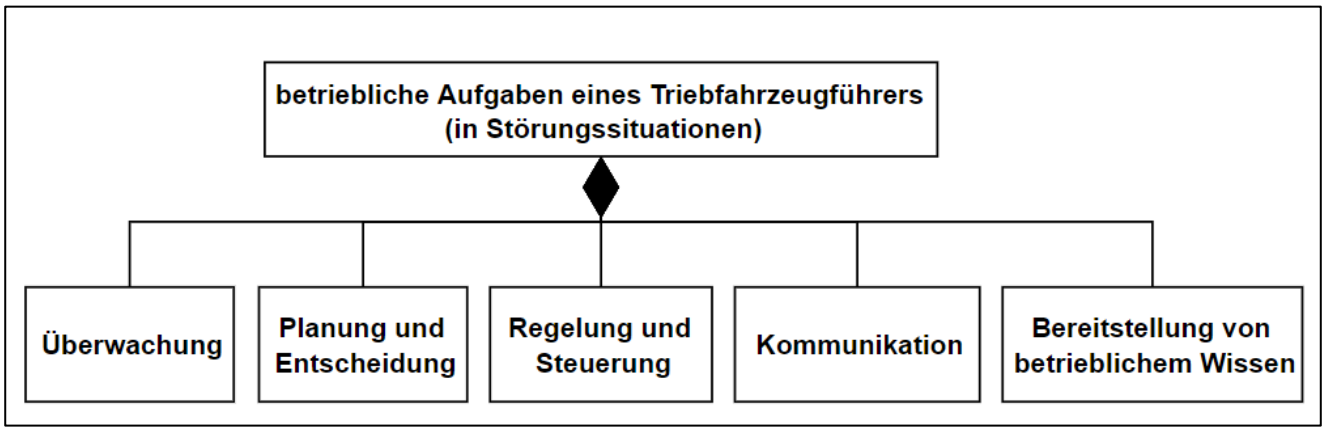

Abbildung 3 Aufgaben eines Triebfahrzeugführers in Störungssituationen (Eigene Darstellung in Anlehnung an *Brandenburger et al. 2016)*

2.4.4 Lösungsvorschläge für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb

Neben den bereits für den gegenwärtigen Betrieb existierenden betrieblich-technischen Rückfallebenen gibt es in der Literatur auch Vorschläge für potenziell im vollautomatisierten Bahnbetrieb umsetzbaren betrieblich-technischen Rückfallebenen. Diese werden in diesem Unterkapitel kurz vorgestellt.

Bei CBTC basiertem Betrieb werden betrieblich-technische Rückfallebenen hauptsächlich für den Fall, dass CBTC-geführte Züge ihre Position nicht mehr melden, eingerichtet. Das geschieht dadurch, dass die Züge von funkbasierter Positionsmeldung auf konventionelle Gleisfreimeldeeinrichtungen zurückfallen *(Naeem 2017)*.

Der Umgang mit Störungssituationen bei den vollautomatisiert betriebenen U-Bahnen in Nürnberg, Barcelona oder in Istanbul erfolgt hauptsächlich durch das Betriebspersonal. So gibt es in Nürnberg Mitarbeiter der zentralen Serviceleitstelle der VAG, die den Betrieb aus der Leitstelle kontinuierlich überwachen und daher im Ereignisfall tätig werden können *(Gunther 2007)*. Da die Bahnsteige bei U-Bahn Nürnberg durch Bahnsteigsensoren überwacht werden, sind die Züge nicht mit fahrzeugseitigen Sensoren zur Hinderniserkennung ausgestattet. Stattdessen sind die Züge mit einem Notfallpult ausgestattet, sodass die dezentral verteilten Mitarbeiter als Kunden- und Systembetreuer (KUSS) der VAG jederzeit sich zum Zug begeben können, um eine sogenannte Profilprüffahrt (z.B. bei Durchquerung von Baustellenbereichen) durchzuführen *(Gunther 2007)*.

Um die Weiterfahrt in Störungssituationen möglichst gewährleisten zu können, werden auch bei der vollautomatisierten Metro in Barcelona sogenannte mobile Mitarbeiter eingesetzt, die von der Betriebszentrale lokalisiert werden können *(Morant 2017)*. Im Falle einer Störungssituation wird die Person, die sich am nächsten zu der Störungssituation befindet, schnell ermittelt und aktiviert. Außerdem gibt es einige Mitarbeiter, die sich ständig an den stark frequentierten Bahnhöfen oder zu Spitzenzeiten aufhalten.

In einem CBTC-basierten vollautomatisierten Bahnbetrieb fordert *Fabbian (2006)* zudem hochverfügbare Kommunikationssysteme für eine Fernsteuerung von Zügen und für die Kommunikation mit den Fahrgästen im Störungsfall.

Wenngleich das Betriebspersonal immer als Rückfallebene in Störungssituationen eingebunden werden kann, ist der vollständige Rückfall auf menschliche Ressource nicht nur aufgrund der höheren Fehlerrate sicherheitskritisch, sondern bei Vollbahnen kann der menschliche Eingriff zudem aufgrund der größeren Entfernung zu den Zügen sehr viel Zeit in Anspruch nehmen.

Bei der Automatisierung der Vollbahnen wurde ein erster Ansatz für den Umgang mit Störungssituationen von dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) vorgeschlagen. Dabei handelt es sich um einen sogenannten Train-Operator (TO), dessen Arbeitsplatz in der Leitstelle (z.B. der EVU) ist und der die Verantwortung als auch die manuelle Geschwindigkeitsregelung vorübergehend im Falle von unerwarteten Ereignissen (z.B. extremes Wetter, Türstörungen, Verbindungsverlust zu ETCS-Zentrale) übernimmt. Die Motivation von *Brandenburger et al. (2017)* für die Einführung eines Train-Operators ist, dass menschliche Fähigkeiten in der Situationsbeurteilung und Entscheidungsfindung genutzt werden können, um den Betrieb in Störungssituationen aufrechtzuerhalten. Weiterführende Arbeiten zur Gestaltung eines Train-Operator Arbeitsplatzes und zum situativen Eingriff in Störungssituationen sind in *Brandenburger et al. (2018a), Brandenburger et al. (2018b)* und *Adebahr et al. (2023)* zu finden. Eine derartige Fernüberwachung und Fernzugriff auf Züge ist in dem Zielbild der DB Cargo beim vollautomatisierten Bahnbetrieb von Güterzügen zu finden. In dem Forschungsprojekt „Erprobung von Automatic Train Operation Technologies for Cargo“ wird eine sogenannte Fernsteuerzentrale (engl., Remote Supervision and Control Center eingerichtet *(Jacob 2022)*.

In *Pachl (2017)* werden nur diejenigen Rückfallebenen für den vollautomatisierten Bahnbetrieb als relevant angesehen, bei denen heute ein Triebfahrzeugführer mitwirken muss. Dazu zählt z.B. das zuvor vorgestellte Fahren auf Sicht, die Weiterfahrt nach einer Zwangsbremsung oder die Sicherung eines gestörten Bahnübergangs. Während die Sicherung eines gestörten Bahnübergangs nur bei Personenzügen, bei denen ein Zugpersonal mitfährt, möglich ist, kann nach *Pachl (2017)* eine Fahrt auf Sicht auch im vollautomatisierten Bahnbetrieb durch eine Fernsteuerung erfolgen. Bei GoA4 geführten Zügen (z.B. Güterzüge), die von einem gestörten Bahnübergang betroffen sind, fordert Pachl die

Einrichtung von alternativen Informationskanälen zur ersatzweisen Sicherung des gestörten Bahnübergangs oder schlägt die Fahrt auf Sicht vor.

Auch in *Emery (2017)* werden Störungssituationen als Herausforderungen des vollautomatisierten Bahnbetriebs thematisiert, jedoch sind darin keine Lösungsansätze für den Umgang damit vorhanden. In dem Artikel werden insbesondere fahrzeugseitige Störungen hervorgehoben. Sowohl die Überwachung des eigenen Zuges als auch der vorbeifahrenden Züge gehört zu den Aufgaben eines Triebfahrzeugführers. Störungen an der Außenseite der Züge können nur durch visuelles Hinsehen oder durch Hinhören erkannt werden. Für den vollautomatisierten Bahnbetrieb schlägt *Emery* dazu infrastrukturseitige Überwachungssysteme vor. Des Weiteren wird in ebd. zur Erkennung von Hindernissen – dazu zählen externe Einflüsse auf die Infrastruktur (z.B. Felssturz) – das Fahren auf Sicht vorgeschlagen.

Vergleichbare Überlegungen hinsichtlich der Herausforderungen des vollautomatisierten Bahnbetriebs sind in *Meyer zu Hörste (2017)* zu finden. Auch hier wird die Erkennung von Hindernissen hervorgehoben. *Meyer zu Hörste* thematisiert zudem das Erfordernis von betrieblichen Regeln – insbesondere für Störungssituationen – im vollautomatisierten Bahnbetrieb. Denn die gegenwärtigen betrieblichen Regeln sind in natürlich sprachlicher Form gestaltet und gelten daher nur für das Betriebspersonal. Eine konkrete Lösung hinsichtlich der Störungssituationen und der betrieblichen Regeln im vollautomatisierten Bahnbetrieb wird in ebd. jedoch nicht vorgeschlagen.

Neue betriebliche Regeln für den vollautomatisierten Betrieb werden auch in *Morast und Nießen (2020)* gefordert. In Bezug auf den Umgang mit Störungssituationen im vollautomatisierten Betrieb werden betrieblich-technische Rückfallebenen aus dem gegenwärtigen Betrieb wie z.B. Durchführen von Sperrfahrten vorgeschlagen.

Um die Verfügbarkeit der Kommunikation mit FRMCS in Zukunft auf einem möglichst hohen Level gewährleisten zu können, wird in *Aebersold und Schubert (2023)* empfohlen, eine Mischung aus bahneigenem Funkspektrum und dem des Public Mobile Network Operator (PMNO) zu nutzen. In dem Artikel wird insbesondere hervorgehoben, dass durch die Mischung beider Funkspektren ein fehlertolerantes Kommunikationssystem realisiert werden kann, indem das PMNO-Spektrum als Rückfallebene zum bahneigenen Funkspektrum eingesetzt wird.

Nach *Haas (2015)* ist jedoch ein Roaming der ETCS-Datenfunkgeräte im ETCS-Standard nicht vorgesehen. Für die Weiterfahrt der von der Kommunikationsstörung betroffenen Züge bleibt nur die in Unterkapitel 2.4.2 vorgestellte Rückfallebene (Befehlserteilung und Betriebsart SR).

Genaue Lösungsvorschläge für den Umgang mit Störungssituationen im vollautomatisierten Betrieb sind zwar in *Wolf und Langer (2022)* nicht gegeben, jedoch sollten nach ebd. für den vollautomatisierten Betrieb vereinheitlichte Betriebskonzepte – einschließlich von gemeinsamen betrieblichen Regeln – erarbeitet und standardisiert werden, um die Fahrzeuge weitergehend auch funktional und kosteneffizient auf einen vollautomatisierten Bahnbetrieb vorbereiten zu können.

2.4.5 Kenngrößen zur Bewertung der Lösungen für den Umgang mit Störungssituationen im Bahnbetrieb und dazugehörige Bewertungsverfahren

Aus den in Unterkapitel 2.4.2 vorgestellten betrieblich-technischen Rückfallebenen ist ersichtlich, dass von den Störungssituationen die bereits in Kapitel 1.1 eingeführten Stakeholder (EIU, EVUs, Fahrgäste, öffentliche Behörden und Gesellschaft) betroffen sein können.

Da der vollautomatisierte Bahnbetrieb noch nicht migriert ist, stehen die Betreiber (EIU und EVU) bei der Migration des vollautomatisierten Bahnbetriebs vor einer Entscheidung, welche betrieblich-technische Rückfallebenen migriert werden sollen. Damit die Entscheidung auf Basis einer Bewertung erfolgen kann, werden daher in diesem Unterkapitel einige Kenngrößen, die bei der Bewertung der Lösungen für den Umgang mit Störungssituationen im Bahnbetrieb herangezogen werden können, und dazugehörige Bewertungsverfahren vorgestellt. Entsprechend der Zielsetzung aus dem Kapitel 1.3 werden dabei nur jene Kenngrößen vorgestellt, die dem Grundprinzip des Bahnbetriebs „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“ beschreiben. Die Reihenfolge der Vorstellung im weiteren Verlauf des Unterkapitels entspricht vereinfacht dem Grundprinzip des Bahnbetriebs „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“. Anschließend werden noch die in der Literatur vorhandenen Bewertungsverfahren vorgestellt, bei denen die vorgestellten Kenngrößen vorkommen.

Sicherheit im Bahnbetrieb

Unter den Stakeholdern ist es indiskutabel, dass die Sicherheit der Betriebsführung das oberste und gemeinsame Ziel aller Stakeholder ist. Die Sicherheit wird nach EN 50126 definiert als die *„Freiheit von inakzeptablem Risiko“* und sie kommt sowohl in der Entwicklungsphase von sicherheitskritischen Systemen als auch während der Betriebsführung zur Geltung.

In der Entwicklungsphase von sicherheitskritischen technischen Systemen für den Bahnbetrieb werden Risiko- und Gefährdungsanalysen durchgeführt, um für jedes sicherheitskritische technische System eine sogenannte tolerierbare Gefährdungsrate (THR) zu bestimmen. Mit der THR wird angegeben, wie häufig eine Gefährdung (z.B. vollständiger Verlust des Bremsvermögens) auftreten darf (toleriert wird).

Die Sicherheit der Betriebsführung im Regelbetrieb wird dadurch definiert, dass die technischen Systeme ihre THR einhalten und während der Betriebsführung das vorliegende Risiko stets unterhalb des Grenzrisikos liegt. Sofern jedoch ein technisches System gestört ist, muss dieses entsprechend der EN 50126 in den sicheren Zustand (Fail-Safe) überführt werden, da sonst das für den Regelbetrieb geforderte Sicherheitsniveau nicht mehr eingehalten werden kann.

Anders als das Risiko, das für die technischen Systeme während der Entwicklungsphase ermittelt wird, führt *Huang (2020)* zur Gestaltung von Betriebskonzepten das sogenannte Betriebsrisiko ein. Das Betriebsrisiko gilt während der Betriebsführung (darunter auch in der betrieblich-technischen Rückfallebene) und umfasst die Handlungen der Akteure (technische Systeme und Betriebspersonal) während der Betriebsführung einschließlich ihrer Dauer in einem bestimmten Betrachtungsbereich über einen bestimmten Betrachtungszeitraum.

Neben der sicheren Gestaltung und Durchführung des Bahnbetriebs sollen die Eisenbahnbetriebsanlagen nach *DB Netz AG (2022)* so dimensioniert bzw. ausgelastet werden, dass die beiden Oberziele Sicherung der Funktionsfähigkeit des Systems Bahn bei einer betrieblich optimalen Zugzahl und Gewährleistung einer wirtschaftlich optimalen Kapazitätsnutzung bei einer wirtschaftlich optimalen Zugzahl (Betriebsqualität) erfüllt werden.

Im Bahnbetrieb gibt es einige Kenngrößen für Leistungsuntersuchungen, die je nach Aufgabenstellung unterschiedlich eingesetzt werden können. Da der Fokus dieser Arbeit auf betrieblich-technischen Rückfallebenen für Störungssituationen im vollautomatisierten Bahnbetrieb liegt, werden im Weiteren betriebliche Kenngrößen und eine Kenngröße zur Beschreibung der Wirtschaftlichkeit vorgestellt, die aufgrund von betrieblich-technischen Rückfallebenen beeinflusst werden können.

Urverspätung

Im Falle von Störungen bei den jeweiligen betroffenen Zügen kommt es zu Urverspätungen, die sich dann auf die Beförderungszeit auf dem Streckenabschnitt auswirken können. Urverspätungen stellen außerplanmäßige Halte- oder Fahrzeiten dar. Die Folge von Urverspätungen ist, dass die Anzahl der Züge, die innerhalb eines Zeitraums den Streckenabschnitt befahren können, sinkt. Dadurch reduziert sich die ursprünglich geplante Kapazität des Streckenabschnitts (ungeplanter Kapazitätsverbrauch). Mit der Urverspätung kann der jeweils zugspezifisch einhergehende Zeitverlust für die unmittelbar von der Störung betroffenen Züge quantitativ ausgedrückt und zugleich eine unmittelbare Vergleichbarkeit der Ergebnisse in Abhängigkeit der einzurichtenden betrieblich-technischen Rückfallebene geschaffen werden. Urverspätungen können anhand der Verspätungsänderung zwischen zwei Messpunkten im Betrachtungsraum ermittelt werden. Dazu wird die Differenz zwischen dem Zeitbedarf für die unbehinderte Fahrt eines Zuges im Regelbetrieb und dem Zeitbedarf für die Fahrt in der betrieblich-technischen Rückfallebene herangezogen.

Behinderungsgrad nach (Martin)

Um die Wirkung durch Störungssituationen auftretende Behinderungen bei Leistungsuntersuchungen berücksichtigen zu können, wurde in *Martin und Li (2014)* die Kenngröße Behinderungsgrad eingeführt. *„Der Behinderungsgrad beschreibt den zeitlichen Anteil der auf einem Belegungselement auftretenden behinderungsbedingten Wartezeit innerhalb eines Untersuchungszeitraum“ (Martin und Li 2014)*.

Die Ermittlung des Behinderungsgrades erfolgt aus dem Verhältnis der Behinderungszeit zu dem Untersuchungszeitraum. Die Behinderungszeit eines Zuges auf einer Fahrwegkomponente ist die Differenz aus der Ist- und der Soll-Belegungszeit. Die Behinderungszeit wird dann über alle Züge im Untersuchungszeitraum aufsummiert und in das Verhältnis zum Untersuchungszeitraum gesetzt, um daraus den Behinderungsgrad zu ermitteln. Wenn in einer Störungssituation die dynamische Adaption zur Laufzeit im Stillstand der betroffenen Züge erfolgt, werden die betroffenen Züge eine Fahrwegkomponente länger belegen, wodurch Behinderungszeiten entstehen können.

Außerplanmäßige Wartezeiten

Nicht nur die von Störungssituationen direkt betroffenen Züge erhalten Urverspätungen oder ändern ihre Relativzeit, sondern auch nachfolgende Züge können von der Störungssituation betroffen sein und dadurch außerplanmäßige Halt- oder Fahrzeitverlängerungen haben (außerplanmäßige Wartezeit). Außerplanmäßige Wartezeit beeinträchtigen die Flüssigkeit des Betriebes und damit die Attraktivität des Angebotes für Reisende und Kunden des Güterverkehrs.

Die zulässige Summe der außerplanmäßigen Wartezeiten in einem Betriebsprogramm bei einer vereinbarten Betriebsqualität ist ein Qualitätsmaßstab zur Beurteilung des Leistungsverhaltens von Netzelementen *(Schwanhäußer 1974)*. Aus dem Verhältnis der Summe der tatsächlichen außerplanmäßigen Wartezeiten und der zulässigen Summe der außerplanmäßigen Wartezeiten ergibt sich die Betriebsqualität. Sofern die tatsächliche Summe der außerplanmäßigen Wartezeiten größer als

die zulässige Summe der außerplanmäßigen Wartezeiten ist, wird die im Regelbetrieb vereinbarte Betriebsqualität beeinträchtigt.

Nach *Hansen und Pachl (2014)* kann ein EIU mit außerplanmäßigen Wartezeiten die Robustheit eines Fahrplans auf einer bestimmten Eisenbahninfrastruktur beurteilen.

Während die Abweichung von der planmäßigen Beförderungszeit bei den EIUs zur Abweichung von der Betriebsqualität führt, leiden die EVUs bei der Abweichung von der planmäßigen Beförderungszeit ggf. unter Pönale-Zahlungen *(Ackermann 1998)*. Die Abweichung von der planmäßigen Beförderungszeit kann bei den Fahrgästen die Fahrgastpünktlichkeit und die Anschlusssicherheit gefährden.

Kosten für die Migration (Lebenszykluskosten)

Mit der Migration des vollautomatisierten Bahnbetriebs werden entsprechend des Kapitels 2.3 auch neue technische Systeme eingeführt, die menschliche Aufgaben verantworten. Neben dem Sicherheitsaspekt beeinflussen demnach auch die mit der Einführung des vollautomatisierten Bahnbetriebs verbundenen Kosten die Migrationsentscheidung der Betreiber.

Die Kosten werden dabei häufig mit sogenannten Lebenszykluskosten (LCC) beschrieben. Lebenszykluskosten sind die Gesamtkosten von der Anschaffung bis zur Entsorgung von Betriebsmitteln und Vorhaben. Lebenszykluskosten umfassen in der Regel die Entwicklungs- Beschaffungs- und Betriebskosten sowie die Kosten für Entsorgung eines Betriebsmittels. Mit der Kenngröße Lebenszykluskosten können Lösungsalternativen – im Rahmen dieser Arbeit betrieblich-technische Rückfallebenen für den vollautomatisierten Bahnbetrieb – gegenübergestellt und jene Lösungen gewählt, wodurch die geringsten langfristigen Betriebskosten entstehen.

Im Weiteren werden Bewertungsverfahren vorgestellt, die zur Bewertung der zu entwickelnden betrieblich-technischen Rückfallebenen für den vollautomatisierten Bahnbetrieb herangezogen werden können und bei denen die zuvor vorgestellten Kenngrößen vorkommen.

Bewertungsverfahren

Insbesondere zur Gestaltung und Entscheidungsfindung von betrieblich-technischen Rückfallebenen wurde in *Huang (2020)* ein Bewertungsverfahren entwickelt, anhand dessen das Betriebsrisiko während der Betriebsführung bestimmt und dieses anschließend in das Verhältnis zu einem Risikogrenzwert gesetzt wird, um einen sogenannten Risikoindex einer betrieblich-technischen Rückfallebene bestimmen zu können.

Der Risikogrenzwert soll dabei als ein Bezugswert dienen und wird in ebd. anhand von Eisenbahnunfallstatistiken in Deutschland aus den Jahren 2006 – 2017 Jahren ermittelt.

Huang (2020) passt das Betriebsrisiko in Abhängigkeit von Streckenstandards der DB Netz AG an, da jeder Streckenstandard eine unterschiedliche planerische Betriebsdichte und Betriebsgeschwindigkeit hat. Dementsprechend ermittelt er für jeden Streckenstandard einen Risikogrenzwert pro Kalenderjahr. Mit Hilfe des Risikoindexes kann nach ebd. eine Aussage darüber getroffen werden, wie viel Prozent des zur Verfügung stehenden Risikobudgets (Risikogrenzwert) in einem Kalenderjahr auf einem bestimmten Netzelement durch ein Betriebskonzept (z.B. in der Rückfallebene) verbraucht wird. Dazu wird das Betriebsrisiko in einem Kalenderjahr kumuliert und wie folgt in das Verhältnis zum Risikogrenzwert gesetzt.

$$RI = \frac{\sum BR_i}{R_{Grenz}} \qquad 2.4.1$$

RI = Risikoindex eines Betriebskonzepts über einem Kalenderjahr

R_{Grenz}= Risikogrenzwert auf einem Netzelement mit einem bestimmten Streckenstandard

$\sum BR_i$ = kumuliertes Betriebsrisiko eines Betriebskonzepts (z.B. einer betrieblich-technischen Rückfallebene) über einem Kalenderjahr.

In *Lindner (2012)* wird ein Bewertungsverfahren vorgestellt, das den Vergleich verschiedener Rückfallebenen ermöglichen soll. Der Autor vertritt die Meinung, dass Rückfallebenen nicht auf der Grundlage einer einzigen Kenngröße bewertet werden können und führt daher zur Bewertung von Rückfallebenen die folgenden vier Kenngrößen ein:

- Der betriebliche Nutzen der Rückfallebene (Fallback Operational Benefit FOB),
- die Normalkosten der Rückfallebene (Fallback Normal Costs FNC),
- der Nutzfaktor der Rückfallebene (Fallback Benefit Quotient FBQ) sowie
- der Indikator der technischen Lösung zur Bewertung der Belastung des Bedienpersonals (Technical Solution Indicator TechSI).

Der betriebliche Nutzen wird durch die prozentuale Veränderung der Infrastrukturkapazität in einer betrieblich-technischen Rückfallebene im Verhältnis zum Regelbetrieb beschrieben. Die Normalkosten einer Rückfallebene werden mit dem Verhältnis der für die Rückfallebene erforderlichen Kosten und den Kosten für den Regelbetrieb beschrieben (Fallback Normal Costs, FNC). Der Vergleich zwischen zwei Rückfallebenen erfolgt anhand des sogenannten Nutzfaktors, der sich aus dem Verhältnis zwischen FOB und FNC ist. Die Auswirkung einer Rückfallebene auf die Sicherheit wird mit der Belastung des Bedienpersonals bestimmt. Ein hoher Belastungswert bedeutet eine Zunahme der Beanspruchung des Bedienpersonals in der Rückfallebene im Vergleich zum Regelbetrieb.

Der Zusammenhang der eingeführten Kenngrößen und das dazugehörige genaue Berechnungsverfahren ist nicht gegeben. Außerdem ist die Anwendbarkeit dieses Bewertungsverfahrens bei den betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb ungewiss.

Es gibt Bewertungsverfahren aus dem RAMS-Bereich, das herangezogen werden kann, um die Effektivität von neu eingeführten Systemen bei der Erfüllung einer bestimmten Aufgabe (im Rahmen dieser Arbeit Zugfahrt in Störungssituationen) zu bewerten.

Ein Bewertungsverfahren aus dem RAMS-Bereich wurde in *Blanchard et al. (1995)* vorgestellt. Mit diesem Bewertungsverfahren kann die Effektivität eines Systems in das Verhältnis zu den damit verbundenen Lebenszykluskosten gesetzt werden, um die Effektivität eines Systems gegenüber einem anderen System zu bewerten. Dabei ist die Systemeffektivität das Produkt aus der sogenannten Design-Integrität (engl., Design integrity), bestehend aus RAMS-Werten, und der Fähigkeit des Systems (engl., Capability), seine beabsichtigte Aufgabe in einer bestimmten Zeit bei einer bestimmten Auslastung zu erfüllen. Das Produkt wird dann in das Verhältnis zu den damit verbundenen Lebenszykluskosten (LCC) gesetzt. Mathematisch lässt sich die Systemeffektivität nach *Blanchard et al. (1995)* folgendermaßen ausdrücken:

$$SE = \frac{Design\ integrity * Capability}{LCC} = \frac{R * A * M * S * C}{LCC} \qquad 2.4.2$$

SE = Effektivität des betrachteten Systems

C = Fähigkeit des betrachteten Systems, seine beabsichtigte Aufgabe in einer bestimmten Zeit bei einer bestimmten Auslastung zu erfüllen

RAM = Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit des betrachteten Systems

S = Kenngrößer zur Beschreibung der Sicherheit des betrachteten Systems

LCC = Lebenszykluskosten des betrachteten Systems.

Des Weiteren ist aus dem Kapitel 2.3 bekannt, dass zur Erhöhung der Zuverlässigkeit und der Verfügbarkeit des vollautomatisierten Bahnbetriebs technische Redundanzen in die Systemarchitektur integriert werden können. Jeder Betreiber kann aus der Referenzarchitektur von RCA bzw. OCORA die eigene physikalische Systemarchitektur einschließlich der technischen Redundanzen entwickeln. Aber die Art und der Umfang der technischen Redundanz ist noch ungewiss. Durch technische Redundanzen kann zwar die Zuverlässigkeit und die Verfügbarkeit erhöht werden, jedoch verursachen technische Redundanzen erhebliche Kosten. Das Verfahren des sogenannten Redundanz-Allokation-Problems (RAP) bietet die Möglichkeit, die Effektivität der technischen Redundanzen in einer Systemarchitektur in Abhängigkeit der Art und dem Umfang zu bewerten.

2.4.6 Zwischenfazit Kapitel 2.4

Aus diesem Kapitel lässt sich zusammenfassen, dass betrieblich-technische Rückfallebenen das Rückgrat des Bahnbetriebs im Falle von Störungssituationen bilden, weshalb auch im vollautomatisierten Bahnbetrieb sowohl zur Erfüllung der Vorgaben des Betriebskontinuitätsmanagements als auch zur Erfüllung der hier aufgeführten rechtlichen Forderungen geeignete betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen notwendig sind.

Im Kern der gegenwärtigen betrieblichen Rückfallebene kommt es neben der zwischenmenschlichen Kommunikation auch auf die Planungsfähigkeit des Menschen an. Mit der Planung werden Maßnahmen und mögliche Handlungsalternativen anhand der vorliegenden Störung und der Handlungsregeln in den Richtlinien abgewogen und eine zu der aktuellen Störungssituation passende Maßnahme und Handlung ausgewählt.

Für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb wird in diversen Literaturen die Fernsteuerung von Zügen durch einen Train-Operator oder das Fahren auf Sicht als Lösungsansatz vorgeschlagen. Darüber hinaus wird insbesondere die Gestaltung von betrieblichen Regeln für den vollautomatisierten Bahnbetrieb hervorgehoben.

2.5 Ansätze für den Umgang mit Störungssituationen in anderen Verkehrssystemen

Da auch der Straßen- und der Luftverkehr zunehmend automatisiert werden, sollen in diesem Kapitel – in Hinblick auf das Ziel dieser Arbeit – einige Lösungsansätze für den Umgang mit Störungssituationen im vollautomatisierten Straßen- und Luftverkehr vorgestellt werden.

2.5.1 Ansätze für den Umgang mit Störungssituationen im vollautomatisierten Straßenverkehr

Wenngleich im Schienenverkehr die Grundvoraussetzungen (Schienenführung und zentral-geregelt) für einen vollautomatisierten Betrieb gegeben sind, ist der Automatisierungsgrad im Straßenverkehr in den letzten Jahren rasch angestiegen. Deshalb werden in diesem Unterkapitel bereits existierende Lösungsansätze für den Umgang mit Störungssituationen im vollautomatisierten Straßenverkehr vorgestellt.

Anders als im Schienenverkehr verfügt das Fahrzeug im Straßenverkehr über zwei translatorische Freiheitsgrade (Längs- und Querbewegung). Trotz des hohen Automatisierungsgrades im Straßenverkehr sitzt dennoch ein Fahrer ständig vor dem Lenkrad. Deshalb werden bei unbekannten Situationen für das autonome Fahrzeug oder bei Störungssituationen sogenannte Übergabeanfragen (engl., Take-Over-Request) an den Fahrer gestellt. Dazu werden in verschiedenen wissenschaftlichen Arbeiten die Herausforderungen beim Take-Over adressiert.

So gibt es beispielsweise in *Gold et al. (2013)* Untersuchungen dahingehend, wie lange es dauert, bei unbekannten Situationen einen Fahrer erneut in die Regelungsschleife der Fahrzeugbewegung einzubinden. Der Fokus dabei liegt auf der Reaktionsfähigkeit des menschlichen Fahrers.

Vergleichbare Lösungsansätze gibt es auch in *Bazilinskyy et al. (2017)*. Darin werden verschiedene Technologien zur Übergabeanfragen untersucht, mit dem Ziel, die Reaktionsfähigkeit des menschlichen Fahrers zu erhöhen.

Auch in dem Entwurf des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes von Bundesregierung wird im autonomen Straßenverkehr eine permanente Überwachung durch eine technische Aufsicht gefordert. Im Falle von Störungen soll sich das Fahrzeug unverzüglich in einen risikomindernden Zustand versetzen und dabei soll die technische Aufsicht jederzeit in der Lage sein, die Fahrzeugsteuerung zu übernehmen. Alternativ kann die technische Aufsicht auch ein Fahrmanöver vorgeben, das dann automatisiert abgefahren wird *(Bundestag 2021)*.

Neben der Übergabe an einen menschlichen Fahrer in Störungssituationen gibt es in einigen wissenschaftlichen Arbeiten auch andere Ansätze für den Umgang mit Störungssituationen im autonomen Straßenverkehr.

So wurde beispielsweise in *Frtunikj et al. (2014)* ein modellbasiertes Framework entwickelt, anhand dessen verschiedene Sensorkonfigurationen im Falle einer Störung zur Laufzeit eingerichtet werden können. Das erarbeitete Framework enthält ein Meta-Modell der verschiedenen Sensoren in der Systemarchitektur und kann daraus im Falle von Störungen auf die Informationen von den noch verfügbaren Sensoren, die für eine neue Konfiguration erforderlich sind, zugreifen.

Ausgehend von der Argumentation, dass Störungen nicht vorhersehbar sind und daher Lösungen dafür in der Entwicklungsphase nicht effektiv entwickelt werden können, wird in der Arbeit von *Weiss et al. (2020)* vorgeschlagen, im Falle von Störungen im Steuergerät (engl. electronic control unit, ECU) dessen Softwareanwendungen zur Laufzeit auf andere verfügbare Steuergeräte zu allokieren. Dadurch reduziert sich die Rechenleistung auf den anderen Steuergeräten, d.h. es kommt zu einer Degradierung der Steuergeräte.

In *Xue et al. (2018)* hingegen wurde ein konkreter Lösungsansatz für den Umgang eines autonomen Fahrzeugs im Falle von Sensorstörungen (Frontsensoren) erarbeitet. Die Betriebssituation konzentriert sich auf die Phasen des Spurhaltens und des Spurwechsels. Bei dem vorgestellten Lösungsansatz wird unmittelbar nach der Sensorstörung ein virtuelles Abbild der umliegenden Fahrzeuge anhand der letzten bekannten Sensordaten gebildet. Daraufhin läuft ein Prädiktionsalgorithmus, der das Verhalten (Geschwindigkeit und Position) der umliegenden Fahrzeuge schätzt. Um das Risiko für eine Kollision zu reduzieren, wurde ein sicherer Steueralgorithmus erarbeitet, der bei der Geschwindigkeit und bei der Position der umliegenden Fahrzeuge von einem worst-case Fall ausgeht. D.h., das Ego-Fahrzeug geht davon aus, dass sich die virtuellen Fahrzeuge in einer Bremsphase befinden und bremst daher auch selbst. Anhand der anderen Sensoren am Ego-Fahrzeug (z.B. Seitensensoren) wird der Prädiktionsalgorithmus mit aktuellen Daten angepasst. Trotz des Ansatzes für eine autonome Rückfallebene in Störungssituation wird in der Zusammenfassung des Artikels hervorgehoben, dass ein menschlicher Fahrer die Kontrolle des Fahrzeugs in Störungssituationen übernehmen sollte.

Ein vergleichbarer Ansatz – Rückfallebene ohne menschlichen Eingriff – wird auch in *Völp und Verissimo (2018) vorgestellt*. Im Vergleich zu *Xue et al. (2018)* schlagen die Autoren hier vor, dedizierte Rückfallmanöver auf dem Fahrzeug vorzuhalten. In dem Artikel wird die Fail-Safe Reaktion als Rückfallmanöver vorgestellt. Demnach soll das autonome Fahrzeug im Falle von Störungen sofort als Rückfallmanöver auf einen Seitenstreifen fahren und dort das Fahrzeug zum Halten bringen.

2.5.2 Ansätze für den Umgang mit Störungssituationen im vollautomatisierten Luftverkehr

Anders als im Schienen- und Straßenverkehr bewegt sich ein Luftfahrzeug im dreidimensionalen Raum. Auch der Luftverkehr ist wie der Schienenverkehr zentral-geregelt.

Trotz des Autopiloten bei Luftfahrzeugen gibt es als Rückfallebene in Störungssituationen immer die Piloten im Cockpit. Diese werden in Störungssituationen (z.B. Triebwerksstörung) durch ein Handbuch (Checklist) für Rückfallebenen (engl., Quick Reference Handbook, QRH) geleitet, um die Störungssituation sicher zu bewältigen. In modernen Luftfahrzeugen wird das Handbuch digital auf einer elektronisch zentralisierten Flugzeuganzeige (engl., Electronic Centralized Aircraft Monitor, ECAM) bereitgestellt *(Skybrary, o.D.)*. Das Handbuch liegt auch in Papierform im Cockpit vor, auf das dann zugegriffen werden kann, wenn kein ECAM verfügbar ist *ebd.*

In der Arbeit von *Ehrmanntraut (2010)* wird u.a. auf die Frage „was passiert, wenn die Automatisierungssysteme in Luftfahrzeugen gestört sind?“ eingegangen. Dazu schlägt der Autor in der Arbeit drei mögliche Lösungsansätze vor. Der erste Lösungsansatz sieht eine menschenzentriere Redundanz vor, bei der im Falle von Störungen an Automatisierungssystemen die Steuerung durch menschliche Bediener übernommen wird. Der zweite Lösungsansatz sieht eine volle Redundanz in den Automatisierungssystemen vor. Der dritte Lösungsanasatz stellt schließlich eine Kombination aus voller Redundanz und menschlicher Beteiligung vor. Da der Luftverkehr – wie bereits oben erwähnt – auch zentral geregelt ist, soll beim dritten Lösungsansatz verhindert werden, dass die Luftfahrzeuge im Falle von Kommunikationsstörung nicht eigenständig Planungen vornehmen und Entscheidungen treffen. Als Planer und Entscheider des Vorgehens soll ein Mensch aus der Leitstelle fungieren.

Es gibt auch kleine unbenannte Luftfahrzeuge, die auch als Drohnen oder Multikopter bezeichnet werden. Seit 2015 setzt die DB Sicherheit derartige Multikopter zur Vegetationskontrolle oder Inspektion von Brücken und Bauwerken ein *(DB Sicherheit, o.D.)*. Der Einsatzbereich der Drohnen streckt sich aber auch darüber hinaus.

Mit Drohnen können demnach auch in Katastrophensituationen, in denen keine normale Kommunikationsinfrastruktur zur Verfügung steht, ein schnell einsetzbares, flexibles, selbst konfigurierbares Ad-Hoc-Netzwerk mit geringen Betriebskosten bereitgestellt werden *(vgl. Khan et al. 2017)*.

Da sich Betriebskonzepte für Drohnen noch nicht etabliert haben, gibt es auch keine Rückfallebenen im Betrieb. Jedoch besitzen einige Drohnen bereits die sogenannte Rückkehrfunktion (engl., Return-to-Home, RTH), die als Rückfallebene bei einigen Störungssituationen dienen. Die Rückkehrfunktion sorgt dafür, dass die Drohne zum zuletzt aufgezeichneten Startpunkt zurückkehrt *(vgl. Blazhko et al. 2017)*. Die RTH-Funktion kann nach *earthofdrones (2022)* in drei Situationen aktiviert werden. Zum einen kann die RTH-Funktion im Falle von niedrigem Batteriezustand aktiviert werden. Dabei berechnet die Drohne den schnellsten und sichersten Weg, um zum Startpunkt zurückzukehren. Die RTH-Funktion kann zum anderen auch im Falle einer Kommunikationsstörung aktiviert werden. Auf dem Weg zurück zum Startpunkt versucht die Drohne eine Kommunikation aufzubauen. Schließlich ist es auch möglich, die RTH-Funktion manuell durch den menschlichen Benutzer zu aktivieren, um die Drohne zum Startpunkt zurückzuholen.

2.5.3 Zwischenfazit Kapitel 2.5

Aus dem Kapitel 2.5 kann zusammengefasst werden, dass bei der Automatisierung des Straßen- und Luftverkehrs ebenfalls Störungssituationen einen besonderen Stellenwert haben. Die Übergabe der Kontrolle im Falle von Störungen auf einen Menschen ist in beiden Verkehrssystemen zu finden. Während für den Straßenverkehr der Fahrer des Straßenfahrzeugs im Falle von Störungen die Kontrolle über das Fahrzeug bekommt, ist im Luftverkehr aufgrund der zentralen Betriebsführung ein Eingriff aus der Ferne vorgesehen.

Im Vergleich zum Luftverkehr gibt es für den autonomen Straßenverkehr auch erste innovative Ansätze, die eine automatisierte Reaktion auf Störungssituationen ohne menschlichen Eingriff ermöglichen sollen.

Zusammenfassend kann festgehalten werden, dass für alle Verkehrssysteme – unabhängig von der Systemgestaltung (zentral oder dezentral) – Rückfallebenen für Störungssituationen erforderlich sind. Dabei können sich zwar die Ursachen für Störungssituationen systemspezifisch unterscheiden, jedoch können sich die Störungssituationen, für die Rückfallebenen erforderlich sind, ähneln (z.B. Kommunikationsstörung). Wenngleich die Betriebsführung der Vollbahnen vergleichbar mit der Betriebsführung im Luftverkehr ist, können auch die Lösungen für den Umgang mit Störungssituationen aus dem autonomen Straßenverkehr als Anknüpfungspunkte bei der Lösungsfindung für den vollautomatisierten Bahnbetrieb im Rahmen dieser Arbeit dienen.

2.6 Mögliche Methoden zur Entwicklung von Lösungsansätzen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb

In der Arbeit sollen entsprechend des Kapitels 1.3 betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb entwickelt werden. Mit der Einführung des vollautomatisierten Bahnbetriebs werden aber notwendigerweise neue technische

Systeme migriert. Es sind daher Methoden erforderlich, mit denen betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb unter Berücksichtigung von neuen technischen Systemen entwickelt werden können.

In diesem Kapitel werden mögliche Methoden, die im Rahmen dieser Arbeit zur Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb verwendet werden können, vorgestellt. Da betrieblich-technische Rückfallebenen Betriebsprozesse umfassen und das Bahnsystem sicherheitsrelevante Systeme erfordert, die bei der Ausführung von Betriebsprozessen maßgebend beteiligt sind, werden Methoden aus dem Bereich der Prozessgestaltung und der Entwicklung von sicherheitsrelevanten technischen Systemen vorgestellt.

Da bereits im gegenwärtigen Bahnbetrieb betrieblich-technische Rückfallebenen existieren, die in den vollautomatisierten Bahnbetrieb überführt werden könnten, wird zunächst in Unterkapitel 2.6.1 eine Methode vorgestellt, anhand derer Betriebsprozesse (um)gestaltet werden können.

Wie bereits oben erwähnt, werden mit der Einführung des vollautomatisierten Bahnbetriebs notwendigerweise neue technische Systeme migriert, die zum Teil in den Forschungsinitiativen RCA und OCORA spezifiziert wurden. Unter Berücksichtigung der Tatsache, dass für den vollautomatisierten Bahnbetrieb neue technische Systeme spezifiziert werden, und der vollautomatisierte Bahnbetrieb noch nicht migriert ist, werden in den Unterkapiteln 2.6.2 und 2.6.3 zwei mögliche Methoden vorgestellt, mit denen betrieblich-technische Rückfallebenen vor der Migration und mit den neuen technischen Systemen entwickelt werden können.

2.6.1 Prozess-Reengineering

Prozess-Reengineering ist ein im Zusammenhang mit Business-Management häufig verwendeter Begriff. Nach *Schawel (2011, S.49)* beinhaltet ein Prozess-Reengineering *„das systematische Überarbeiten bzw. die komplette Neugestaltung von Geschäftsprozessen mit dem Ziel, die Leistungserbringung zu optimieren.“*

Durch Prozess-Reengineering ist es möglich, Transparenz über den Ist-Zustand von Prozessen zu schaffen und dadurch die darin vorkommenden Ressourcen und insbesondere den Zeitverbrauch der Prozesse zu optimieren (Ineffizienzen zu beseitigen).

Die Anwendung der Prozess-Reengineering Methode im Rahmen dieser Arbeit würde bedeuten, existierende betrieblich-technische Rückfallebenen transparent darzustellen und daraus mögliche Lösungen für den vollautomatisierten Bahnbetrieb zu entwickeln.

2.6.2 Systems Engineering nach EN 50126

Um bei der Entwicklung von technischen Systemen für den Bahnbetrieb die immer mehr ansteigende Komplexität strukturiert bewältigen zu können, gibt es auch die Systems Engineering Methode nach EN 50126, die auch als V-Modell bekannt ist.

Die Systems Engineering Methode nach EN 50126 hat als Ausgangspunkt die Anforderungserhebungsphase. In dieser Phase werden die Anforderungen an das System von unterschiedlichen Stakeholdern des Systems zusammengestellt. Das Ergebnis dieser Phase ist eine Anforderungsliste. Diese Anforderungen stellen zugleich den Maßstab dar, nach dem das spätere System bewertet werden kann.

In der nächsten Phase erfolgt auf Basis der Anforderungen der grobe Systementwurf. Hierbei werden die zusammengestellten funktionalen Anforderungen durch Zerlegung und Modularisierung auf die

Systemelemente des späteren Systems allokiert, sodass daraus zunächst eine funktionale Systemarchitektur und später auch eine physikalische Systemarchitektur entsteht.

Nachdem die physikalische Systemarchitektur entworfen wurde, beginnt die konkrete Implementierungsphase, die an der unteren Spitze des V-Modells platziert ist. Die Implementierung erfolgt dabei domänenspezifisch. Zur Entwicklung von geeigneten betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb ist es zunächst erforderlich, die potenziellen Störungssituationen im vollautomatisierten Bahnbetrieb zu kennen.

Die Systems Engineering Methode nach EN 50126 bietet dazu in den Phasen bis zur Implementierung eine Risiko- und Gefährdungsanalyse an, anhand derer die potenziellen Störungssituationen im vollautomatisierten Bahnbetrieb erarbeitet werden können. Die Risikoanalyse wird auf der Bahnsystemebene durchgeführt. Die Risikoanalyse schließt die Gefährdungsidentifikation, die Auswirkungsanalyse und die Auswahl des Risikoakzeptanzkriteriums (RAC) ein. Die Festlegung von Sicherheitsanforderungen ist das finale Ergebnis der Risikoanalyse.

Die Gefährdungsanalyse wird im Vergleich zu der Risikoanalyse für ein bestimmtes technisches System durchgeführt. Dabei werden die internen Ursachen aus dem betrachteten technischen System für die während der Risikoanalyse identifizierten Gefährdungen auf der Bahnsystemebene eruiert. Als Ergebnis können dann Kontrollmaßnahmen aufgrund der gegebenen Sicherheitsanforderungen für das betrachtete technische System abgeleitet werden.

Während der Risiko- und Gefährdungsanalyse innerhalb der Systems Engineering Methode nach EN 50126 werden Erfahrungen aus dem gegenwärtigen Betrieb genutzt, um daraus die in der Vergangenheit entstandenen Gefährdungen im Bahnbetrieb zu erarbeiten. Da jedoch noch keine Erfahrung mit dem vollautomatisierten Bahnbetrieb bei Vollbahnen existiert und die für den vollautomatisierten Bahnbetrieb relevanten technischen Systeme signifikante Änderungen im Bahnbetrieb verursachen, können die Erfahrungen aus dem gegenwärtigen Bahnbetrieb nicht oder nur teilweise genutzt werden. Daher sollten auch alternative Methoden bei der Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb untersucht werden.

2.6.3 STPA integriertes Systems Engineering

Eine weitere mögliche Methode zur Lösung der Aufgabenstellung ist die „Systemtheoretische Prozessanalyse“ (engl. System-Theoretic Process Analysis, STPA). Die STPA wurde im Jahre 2012 von *Leveson (2012)* entwickelt. Die STPA ist eine Methode, die die Gefährdungsanalyse bereits in die frühe Entwicklungsphase der funktionalen Systemarchitektur integriert und ermöglicht somit, Gefährdungen bereits in der frühen Entwicklungsphase (ohne vollständige Spezifikation) der Systemarchitektur des betrachteten technischen Systems zu untersuchen. Der besondere Fokus der STPA-Methode ist die Berücksichtigung der Interaktion zwischen den technischen Systemen oder deren Systemelementen während der Gefährdungsanalyse.

Statt lediglich die Gefährdungsursachen auf die Störung von technischen Systemen oder deren Systemelementen und auf die Verkettung einzelner Fehler darin zurückzuführen, werden Störungen von technischen Systemen unterschiedlicher Ausprägung in der Analyse betrachtet. Bei der

STPA-Methode kann somit der Mensch mit seinen Handlungen ebenso in der Analyse betrachtet werden wie technische Systeme.

Das betrachtete System wird bei der STPA-Methode in Form einer hierarchischen Regelungsstruktur im Sinne der Regelungstechnik modelliert. Die hierarchische Regelungsstruktur besteht allgemein aus Regler und Regelstrecken und die Verbindungen dazwischen. Bei den Verbindungen handelt es sich um die Kontrollaktionen (engl. Control Action) und Rückkopplung (engl. Feedback). Die hierarchische Darstellung hat eine Absicht. Demnach steuert das hierarchisch höher liegende technische System oder dessen Systemelement das darunterliegende technische System oder dessen Systemelement. Die Modellierung erfolgt auf einem hohen Abstraktionslevel, weshalb die vollständige Spezifikation des betrachteten technischen Systems nicht erforderlich ist.

Die STPA-Methode erlaubt somit, potenzielle Unfallursachen während der Entwicklung eines Systems ohne vollständige Spezifikation zu erarbeiten. Damit kann sie in die zuvor beschriebene Systems-Engineering Methode nach EN 50126 integriert werden.

Die Abbildung 4 stellt eine allgemeine (abstrakte) hierarchische Regelungsstruktur eines Systems nach der STPA-Methode dar.

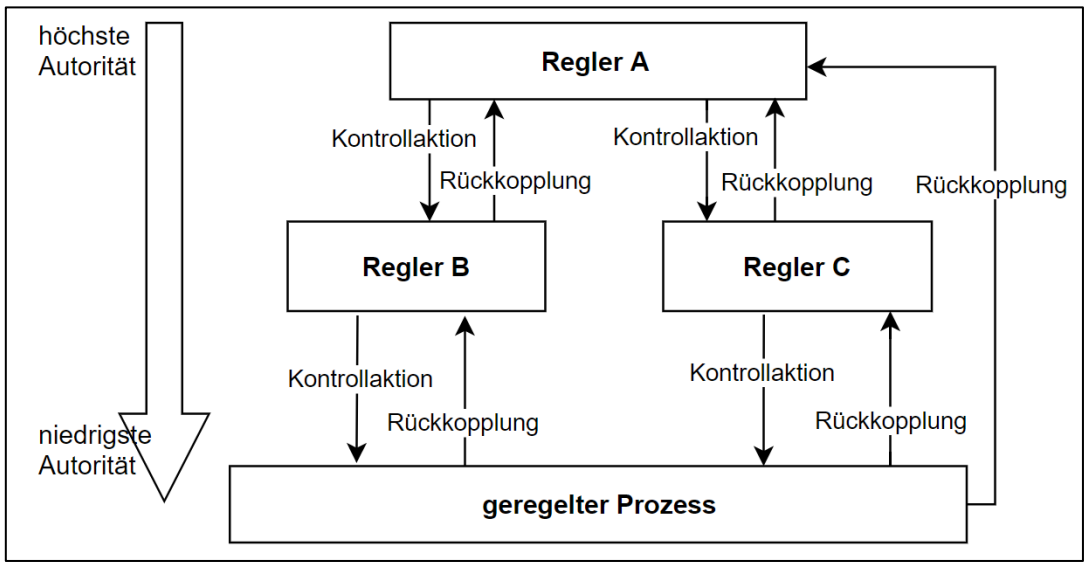

Abbildung 4 allgemeine (abstrakte) hierarchische Regelungsstruktur eines Systems nach der STPA-Methode. (Eigene Darstellung in Anlehnung nach *Leveson und Thomas (2018)*)

Die Abbildung 5 stellt eine beispielhafte hierarchische Regelungsstruktur einer vereinfachten Zugfahrt nach der STPA-Methode mit ETCS-Zentrale, ETCS-OBU und ATO-OBU dar. Aus dieser Abbildung ist ersichtlich, dass die ETCS-Zentrale dem fahrzeugseitigen ETCS-System (ETCS-OBU) hierarchisch überlegen ist. Die ETCS-Zentrale übermittelt Fahrterlaubnisse als Kontrollaktionen und erhält von der ETCS-OBU als Rückkopplung die Position des Zuges übermittelt. Die ETCS-OBU ist dem fahrzeugseitigen ATO-System überlegen. Die ETCS-OBU versorgt die ATO-OBU mit Zugdaten und Fahrterlaubnissen. Erst wenn eine Fahrterlaubnis vorliegt, darf die ATO-OBU die Geschwindigkeit des Zuges regeln. Die ATO-OBU generiert Steuerbefehle, um die Zugfahrt durchführen zu können. Aus der Zugfahrt werden mit Hilfe von Sensoren dann fahrdynamische Daten (z.B. Geschwindigkeit und Position des Zuges) an

die ATO-OBU rückgekoppelt. Bei diesem Beispiel nach Abbildung 5 hat die ETCS-Zentrale die höchste und die ATO-OBU hingegen die niedrigste Autorität.

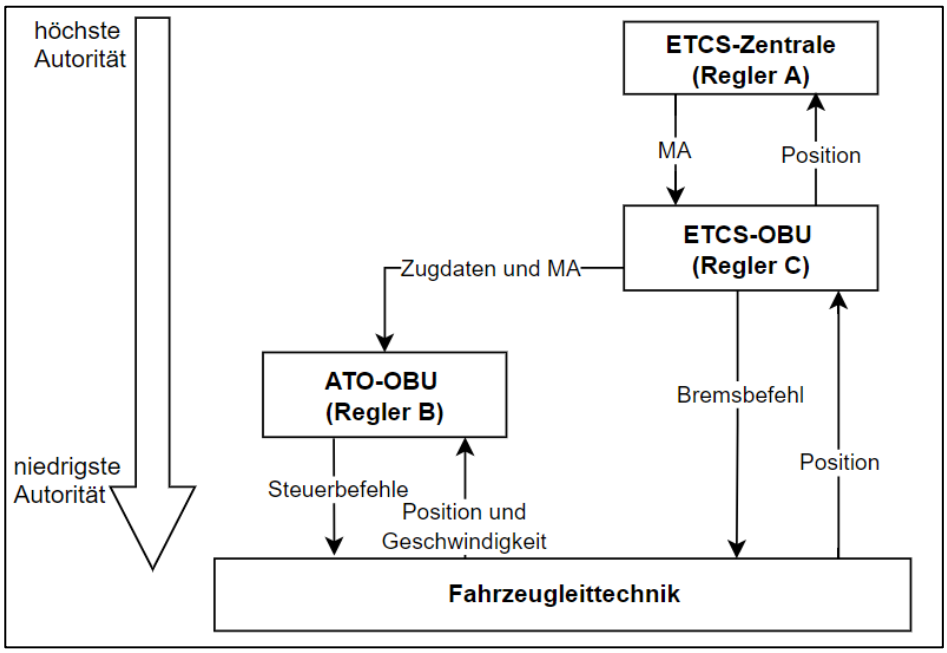

Abbildung 5 beispielhafte hierarchische Kontrollstruktur einer vereinfachten Zugfahrt nach der STPA-Methode mit ETCS-Zentrale, ETCS-OBU und ATO-OBU. (Eigene Darstellung)

2.7 Zusammenfassung des Forschungsstandes

Aus der Literaturrecherche lässt sich zusammenfassen, dass bei einigen Nahverkehrssystemen (z.B. Metro) bereits über drei Jahrzehnte Erfahrungen mit dem vollautomatisierten Bahnbetrieb existieren, während der Automatisierungsgrad bei Vollbahnen bisher nicht über die Fahrfunktion (mit AFB) hinaus flächendeckend migriert wurde. Die aktuellen Bestrebungen bei Vollbahnen sind in einigen Ländern die Einführung eines ATO-Systems, das die Geschwindigkeitsregelung unter Aufsicht eines Triebfahrzeugführers übernimmt (GoA2). Auf europäischer Ebene werden zudem bereits grundlegende Vorarbeiten zum vollautomatisierten Bahnbetrieb in einigen Forschungsinitiativen geleistet (RCA, OCORA und ERJU).

Innerhalb dieser Forschungsinitiativen wurden Referenzarchitekturen (infrastrukturseitig und fahrzeugseitig) für den digitalen Bahnbetrieb spezifiziert und die ersten Prototypen mit Probefahrten (z.B. auf der Teststrecke in Annaberg-Buchholz) getestet. Gleichzeitig ist aber auch erkennbar, dass weiterer Forschungsbedarf – insbesondere hinsichtlich der Gestaltung von Betriebsprozessen – auf dem Weg zum vollautomatisierten Bahnbetrieb besteht. Aus dem Kapitel 2.4 ist bekannt, dass betrieblich-technische Rückfallebenen das Rückgrat des Bahnbetriebs im Falle von Störungssituationen bilden, weshalb auch im vollautomatisierten Bahnbetrieb sowohl zur Erfüllung der Vorgaben des Betriebskontinuitätsmanagements als auch zur Erfüllung der aufgeführten rechtlichen Forderungen geeignete betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen notwendig sind.

Die Forschungsinitiativen RCA und OCORA fordern zwar betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen, jedoch übertragen sie die Verantwortung bei der Entwicklung von betrieblich-technischen Rückfallebenen auf nationale Bahnbetreiber und geben dazu lediglich die Referenzarchitektur vor. Demnach besteht insbesondere ein Forschungsbedarf in der Entwicklung von

betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb.

Die Tatsache, dass die Spezifikation der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme noch nicht vollständig abgeschlossen ist, und daher keine Erfahrung mit dem vollautomatisierten Bahnbetrieb besteht, erfordert neue Ansätze für die Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb.

Denn die gegenwärtigen betrieblich-technischen Rückfallebenen wurden aus Erfahrungen mit unerwünschten Ereignissen heraus entwickelt und entsprechend nach neu eintretenden Ereignissen angepasst. Der wesentliche Nachteil der gegenwärtigen betrieblich-technischen Rückfallebenen ist, dass sie in natürlich-sprachlichen Regelwerken mit historisch gewachsener Struktur niedergeschrieben sind und eine intensive Zusammenarbeit zwischen einem Fahrdienstleiter und einem Triebfahrzeugführer erfordern. Für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb wird zwar in diversen Literaturquellen die Fernsteuerung von Zügen durch einen Train-Operator oder das Fahren auf Sicht als betrieblich-technische Rückfallebene vorgeschlagen. Jedoch ist die Vollständigkeit dieser Lösungsansätze nicht sichergestellt, zumal mit der Einführung des vollautomatisierten Bahnbetriebs notwendigerweise neue technische Systeme eingeführt werden und sich daher die Ursachen für Störungssituationen systemspezifisch unterscheiden können. Somit besteht ein Bedarf an einem neuen Ansatz zur Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb, damit der Betrieb in Störungssituationen auch ohne menschlichen Eingriff mit weitgehend automatisierten betrieblich-technischen Rückfallebenen fortgeführt werden kann.

3 Aufgabenstellung und Anforderungen an die Lösung der Aufgabenstellung

Ausgehend von dem in Hauptkapitel 2 identifizierten Forschungsbedarf wird in diesem Hauptkapitel zunächst die Aufgabenstellung festgelegt. Anschließend werden Anforderungen an die Lösung der Aufgabenstellung strukturiert zusammengestellt. Des Weiteren werden in diesem Hauptkapitel Methoden zur Lösung der Aufgabenstellung diskutiert und eine geeignete Methode ausgewählt sowie die Vorgehensweise im Rahmen der Arbeit vorgestellt. Aufgrund der zeitlichen Rahmenbedingungen der Arbeit wird zudem eine inhaltliche Eingrenzung vorgenommen. Damit im Rahmen der Arbeit die Verständlichkeit vereinfacht wird, erfolgt am Ende dieses Hauptkapitels eine kurze Definition von häufig verwendeten Begriffen.

3.1 Aufgabenstellung

Aus dem Unterkapitel 2.4.1 wird deutlich, dass mit der Einführung des vollautomatisierten Bahnbetriebs der Triebfahrzeugführer und damit eine wesentliche Ressource in Störungssituationen wegfällt. Außerdem ist bekannt, dass technische Systeme in ihrem Lebenszyklus nicht vollständig störungsfrei funktionieren werden.

Störungssituationen im laufenden Betrieb können nicht nur sicherheitskritisch sein, sondern auch zur Abweichung von der vereinbarten Betriebsqualität führen. Das Ziel der Bahnbetreiber ist es daher, den Betrieb auch in Störungssituationen – unter Einhaltung des Grundprinzips „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“ – mit betrieblich-technischen Rückfallebenen fortzuführen.

Da entsprechend des Kapitels 2.7 die für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme noch nicht vollständig spezifiziert sind und daher noch keine Erfahrung mit dem vollautomatisierten Bahnbetrieb besteht, stehen nationale Bahnbetreiber vor der Herausforderung, geeignete betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb zu entwickeln.

Das Ziel dieser Arbeit ist daher – unter Berücksichtigung der Tatsache, dass die für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme noch nicht vollständig spezifiziert sind und daher noch keine Erfahrung mit dem vollautomatisierten Bahnbetrieb besteht – die Entwicklung von geeigneten betrieblich-technischen Rückfallebenen für den weitgehend automatisierten Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb.

Die Randbedingung zur Erreichung des Ziels ist, dass technische Redundanzen bei der Entwicklung von betrieblich-technischen Rückfallebenen nicht berücksichtigt werden.

Zur Erreichung des Ziels sind folgende Herausforderungen zu lösen, die als Unterziele dienen:

- Da die für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme noch nicht vollständig spezifiziert sind, sind auch die Störungssituationen, die erst mit der Einführung des vollautomatisierten Bahnbetriebs entstehen können, unbekannt. Um geeignete betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb entwickeln zu können, sind daher die Störungssituationen zu identifizieren, für die betrieblich-technische Rückfallebenen erforderlich sind.
- Ein weiteres Unterziel ist es, betrieblich-technische Rückfallebenen anhand einer Systematik zu entwickeln, statt wie bisher basierend auf Erfahrungen und historisch gewachsenen Regeln.
- Damit die im Rahmen dieser Arbeit zu entwickelnden betrieblich-technischen Rückfallebenen in anderen Forschungsarbeiten (z.B. ERJU) für eine Migration weiter ausgearbeitet werden

können, sollen die im Rahmen dieser Arbeit zu entwickelnden betrieblich-technischen Rückfallebenen für eine Migrationsentscheidung (z.B. im Rahmen von ERJU) bewertet werden können.

3.2 Anforderungen an die Lösung

Auf Basis der Aufgabenstellung werden in diesem Kapitel Anforderungen an die Lösung zusammengestellt. Dazu enthält das Unterkapitel 3.2.1 zunächst die Anforderungsstruktur einschließlich der Stakeholder, von denen die Anforderungen zusammengestellt wurden. In den Unterkapiteln 3.2.2 – 3.2.5 sind die von den Stakeholdern zusammengestellten Anforderungen zu finden.

3.2.1 Strukturierung der Anforderungen

Die Logik der Strukturierung lehnt sich an das Standardvorgehen bei der Anforderungsanalyse im Systems-Engineering-Prozess an. Bei der Strukturierung werden demnach zum einen die relevanten Stakeholder identifiziert und zum anderen ihre Anforderungen an die Entwicklung von geeigneten betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb zusammengestellt.

In Kapitel 2.4 wurden bereits Forschungsinitiativen vorgestellt, die an der Entwicklung einer einheitlichen europäischen Referenzarchitektur für den digitalen Bahnbetrieb arbeiten. Bei der RCA sind hauptsächlich EIUs beteiligt, während in OCORA EVUs zusammenarbeiten. Da auch die Experten innerhalb der DSD in der RCA und OCORA agieren, sowie die Ergebnisse von RCA und OCORA in ERJU eingebracht werden sollen, werden die genannten **Forschungsinitiativen und Experten darin** als Stakeholder für die Erhebung von Anforderungen im Rahmen dieses Kapitels herangezogen.

EIU und EVU wirken bei den Forschungsinitiativen mit, um den digitalen Bahnbetrieb zu gestalten. Wie bereits aus dem Kapitel 2.4 bekannt, existieren heute bereits betrieblich-technische Rückfallebenen, die in Regelwerken niedergeschrieben sind und von Betriebspersonalen (Fahrdienstleiter und Triebfahrzeugführer) im operativen Betrieb (in Störungssituationen) umgesetzt werden. Die Entwicklung und Umsetzung der Regeln für die betrieblich-technischen Rückfallebenen werden von Eisenbahnbetriebsleiter überwacht. Um die Erfahrungen mit den gegenwärtigen betrieblich-technischen Rückfallebenen bei der Entwicklung von betrieblich-technischen Rückfallebenen für den vollautomatisierten Betrieb einbringen zu können, ist es wertvoll, auch **Experten aus dem gegenwärtigen Betrieb** als Stakeholder zur Erhebung von Anforderungen heranzuziehen. Zu den Experten aus dem gegenwärtigen Betrieb gehören neben dem Eisenbahnbetriebsleiter auch Fahrdienstleiter, Triebfahrzeugführer und eine Führungskraft.

Die Gewährleistung eines sicheren Betriebs und das reibungslose Zusammenspiel von EIU und EVU erfolgt in einem gesetzlichen Rahmen. Schließlich werden daher auch **gesetzliche Anforderungen** zusammengestellt, die bei der Gestaltung des vollautomatisierten Bahnbetriebs eingehalten werden müssen. Dazu dienen das Allgemeine Eisenbahngesetz (AEG), die relevanten EU-Richtlinien und die Eisenbahnbau- und Betriebsordnung (EBO) als Anforderungsquellen.

Die von den drei identifizierten Stakeholdern zu erhebenden Anforderungen werden anschließend gegen **Leitlinien zur Gestaltung von Systemarchitekturen und Grundsätze zur Gestaltung von guten Prozessen** aus der Literatur geprüft. Damit soll die Vollständigkeit der zusammengestellten Anforderungen möglichst sichergestellt werden. Die Literatur, aus der sich die Leitlinien zur Gestaltung von Systemarchitekturen und Grundsätze zur Gestaltung von guten Prozessen ergeben, sind daher ebenfalls Anforderungsquellen. Die Abbildung 6 stellt die relevanten Stakeholder zur Erhebung von

Anforderungen an die Entwicklung von geeigneten betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb dar.

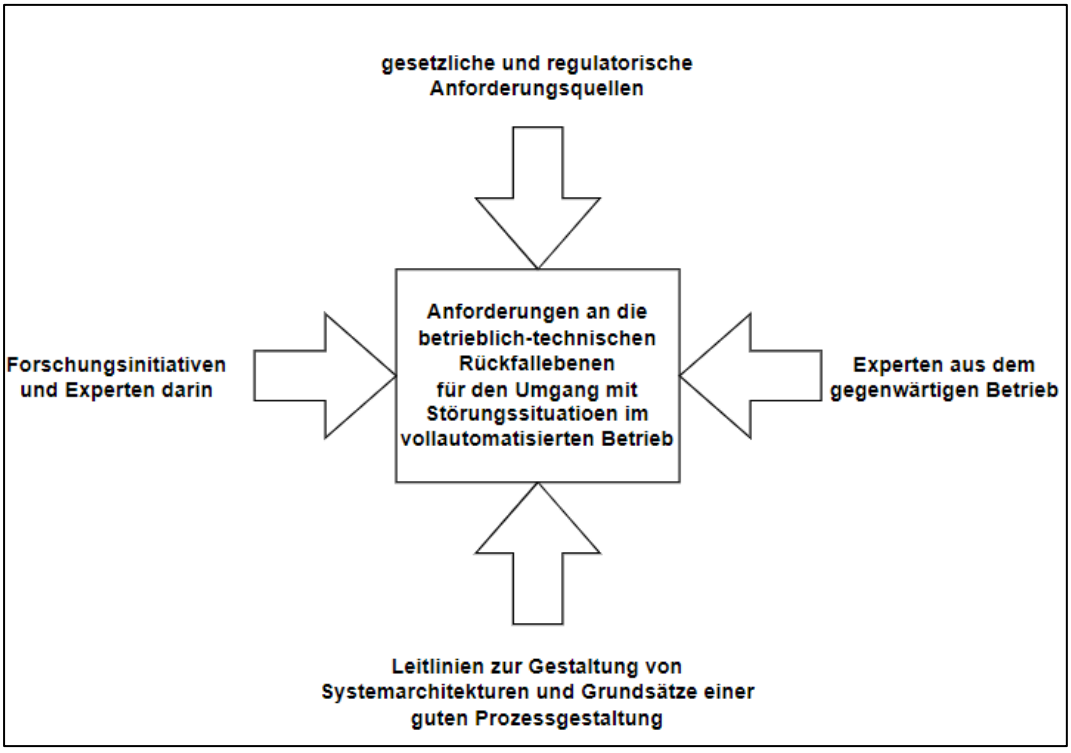

Abbildung 6 relevante Stakeholder zur Erhebung von Anforderungen an die Entwicklung von geeigneten betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb (eigene Darstellung)

In Unterkapitel 2.3.5 wurde zusammengefasst, dass in den nationalen und europäischen Forschungsinitiativen die für den vollautomatisierten Bahnbetrieb relevanten technischen Systeme spezifiziert werden. Dabei war die wesentliche Erkenntnis, dass zwar die technischen Systeme und ihre Schnittstellen zueinander spezifiziert werden (d.h. die Struktur der Systemarchitektur ist vorhanden), jedoch Betriebsprozesse noch nicht adressiert werden. Die Referenzarchitekturen von RCA und OCORA beschreiben die Beziehungen der darin vorkommenden technischen Systeme zueinander. Da darin auch die beiden ATO-Teilsysteme vorkommen, werden von den Forschungsinitiativen **Anforderungen an die Struktur der Systemarchitektur** in Störungssituationen zusammengestellt.

Wie bereits in Unterkapitel 2.3.2 von RCA gefordert, wird die Entwicklung von Betriebsprozessen für Störungssituationen auf die nationalen Infrastrukturbetreiber übertragen. Aus dem Kapitel 2.4 ist zudem bekannt, dass betrieblich-technische Rückfallebenen Ersatzverfahren zur Fortführung des Betriebs in Störungssituationen sind und dass dabei Triebfahrzeugführer und Fahrdienstleiter im gegenwärtigen Bahnbetrieb unabdingbar sind. Trotz des hohen Automatisierungsgrades ist das Bahnsystem aktuell ein soziotechnisches System. Für die Betriebsführung – im Regelbetrieb und in Störungssituationen – sind daher Triebfahrzeugführer und Fahrdienstleiter unabdingbar.

Entsprechend der Definition aus dem Unterkapitel 2.1.1 ist eine Mensch-Maschine Wechselbeziehung während einer Zugfahrt in GoA4-Regelbetrieb nicht mehr erforderlich. Dennoch ist es absehbar, dass das Bahnsystem auch in Zukunft ein soziotechnisches System bleibt, da neben den Zugfahrten in

GoA4-Betrieb auch Zugfahrten in GoA3 oder GoA2 stattfinden können, bei denen das Betriebspersonal – z.B. in Störungssituationen – eine wesentliche Rolle einnimmt. Aus diesem Grund umfassen die Anforderungen an die Betriebsführung in Störungssituationen auch menschliche Aktivitäten.

Um die Erfahrungen mit den gegenwärtigen betrieblich-technischen Rückfallebenen bei der Entwicklung von betrieblich-technischen Rückfallebenen für den vollautomatisierten Bahnbetrieb einbringen zu können, werden auch Anforderungen an die Betriebsführung (Betriebsprozesse) in Störungssituationen von den Experten aus dem gegenwärtigen Betrieb zusammengestellt. Im Gegensatz zu den Forschungsinitiativen RCA und OCORA werden in ERJU Betriebskonzepte für den vollautomatisierten Bahnbetrieb adressiert. Daher werden auch von ERJU Anforderungen an die Betriebsführung (Betriebsprozesse) in Störungssituationen zusammengestellt.

Prozesse werden allgemein in der Notation der Systemarchitekturentwicklung als Systemverhalten bezeichnet. Folglich werden die Anforderungen von den Experten aus dem gegenwärtigen Betrieb und von ERJU an die Betriebsführung als **Anforderungen an das Systemverhalten** in Störungssituationen bezeichnet.

Die Quellen der gesetzlichen und regulatorischen Anforderungen an den vollautomatisierten Bahnbetrieb sind, wie oben erwähnt, das allgemeine Eisenbahngesetz, die EU-Richtlinien, die Eisenbahn Bau- und Betriebsordnung und die Richtlinien 408 und 418. Entsprechend des Kapitels 2.4 beziehen sich die gesetzlichen und regulatorischen Anforderungen auf das Systemverhalten in Störungssituationen.

Um die Vollständigkeit der zusammenzustellenden Anforderungen an die Systemstruktur und an das Systemverhalten in Störungssituationen möglichst gewährleisten zu können, werden Leitlinien zur Gestaltung von Systemarchitekturen und Grundsätze zur Gestaltung von guten Prozessen aus der Literatur herangezogen, die sich aus jahrelanger Erfahrung von Experten aus unterschiedlichen Domänen akkumuliert haben.

Mit den **Leitlinien zur Gestaltung von Systemarchitekturen** werden die an die Systemstruktur in Störungssituationen zusammengestellten Anforderungen gegengeprüft. Schließlich werden anhand der **Grundsätze zur Gestaltung von guten Prozessen** die Anforderungen an das Systemverhalten in Störungssituationen gegengeprüft.

Das Anforderungsdiagramm in Abbildung 7 stellt die Strukturierung der Anforderungen nach

- Anforderungen an das Systemverhalten in Störungssituationen und
- Anforderungen an die Systemstruktur in Störungssituationen dar.

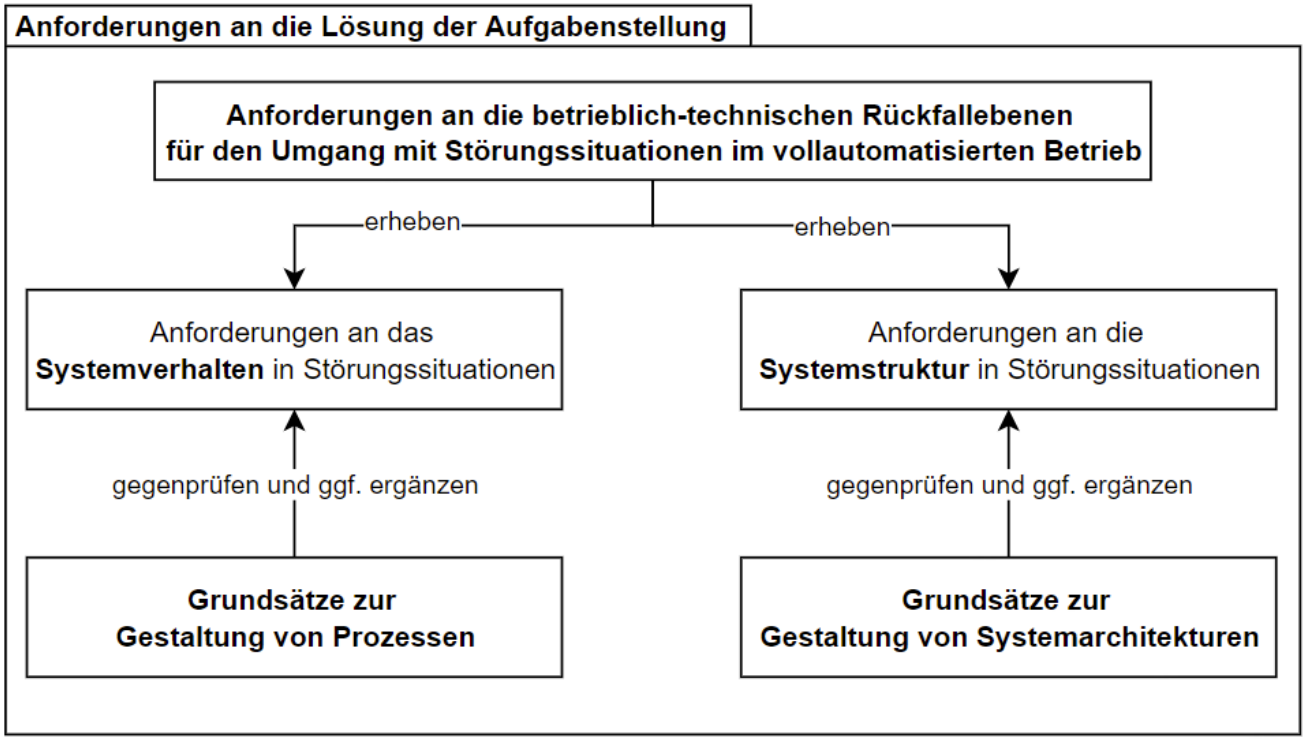

Abbildung 7 Anforderungsdiagramm zur Strukturierung der Anforderungen an die Lösung der Aufgabenstellung (eigene Darstellung)

3.2.2 Anforderungen an die Systemstruktur in Störungssituationen

Nachdem zuvor die Anforderungen strukturiert wurden, erfolgt in diesem Unterkapitel die Zusammenstellung der Anforderungen an die Systemstruktur in Störungssituationen. Die Quellen der Anforderungen an die Systemstruktur in Störungssituationen sind, wie zuvor erarbeitet, die Forschungsinitiativen.

Interoperabilität ist bereits heute ein angestrebtes Ziel der Betreiber. Um die **Interoperabilität** des europaweiten Eisenbahnbetriebs auch bei einer Vollautomatisierung gewährleisten zu können, sollten gemäß den Experten-Interviews und der beiden Forschungsinitiativen die zu entwickelnden betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb mit den europaweiten Referenzarchitekturen RCA und OCORA kompatibel sein.

Demnach soll das ATO-System ein **softwarebasiertes System** sein und dabei die hierarchische Struktur aus der RCA-Referenzarchitektur beibehalten. Damit verbunden sollen durch Verwendung von standardisierten Schnittstellen aus RCA und OCORA auch die **Komplexität** der Systemarchitektur des digitalen Bahnsystems minimiert werden.

Um die Dynamik der digitalen Entwicklung bei unterschiedlichen Lebenszyklen zu bewältigen, werden von den beiden Forschungsinitiativen **modulare Gestaltung der zukünftigen Systemarchitektur** der LST gefordert. Dabei wird gefordert, dass in sich geschlossene Softwareanwendungen bereitgestellt werden sollen, welche dann möglichst auf kommerziell verfügbare Hardware betrieben werden können. Damit wird insbesondere die **Austauschbarkeit** von unterschiedlichen Systemen sowie das **Plug & Play** Prinzip angestrebt.

Modularität wird nicht nur aus Gründen der Austauschbarkeit gefordert, sondern gemäß dem Experten für Systemarchitektur bei Digitale Schiene Deutschland steigern vollautomatisierte Systeme in Zukunft

den Anteil der Software und diese sollen sich auf eine Vielzahl von Betriebssituationen (z.B. Störungssituationen) anpassen können, d.h., **flexibel** sein.

Im Zusammenhang mit der Modularität wird ebenfalls gefordert, dass die in sich geschlossenen technischen Systeme unabhängig von anderen technischen Systemen auf Sicherheit zugelassen werden sollen (engl. **Modular Safety**).

Die RCA und ERJU Forschungsinitiativen fordern zudem die **wirtschaftliche Gestaltung und Durchführung** des vollautomatisierten Bahnbetriebs. Dazu wird gefordert, dass so wenig wie möglich infrastrukturseitige technische Systeme vorhanden sein sollen. Damit wird neben der Wirtschaftlichkeit auch die Steigerung der Zuverlässigkeit angestrebt, da weniger störanfällige technische Systeme existieren. Zudem sollen auf bereits existierende (kommerziell verfügbare, engl. off-the-shelf products) standardisierte technische Systeme zurückzugegriffen werden. Damit soll eine möglichst schnelle Migration des vollautomatisierten Bahnbetriebs erzielt werden.

Sowohl aus RCA als auch aus OCORA ist bekannt, dass die technischen Systeme in den Referenzarchitekturen unterschiedliche Lebenszyklen aufweisen können und dass Softwareanwendungen aufgrund der **technologischen Entwicklungen** ständigen Wandel erleben. Bei der Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb ist daher die Tatsache zu berücksichtigen, dass die technischen Systeme ständig technologische Entwicklungen erleben.

Die Vollständigkeit der bisher zusammengestellten Anforderungen an die Systemstruktur in Störungssituationen wird anhand von Leitlinien zur Gestaltung von Systemarchitekturen gegengeprüft.

Abbildung 8 zeigt die Leitlinien zur Gestaltung von Systemarchitekturen, die sich aus jahrelanger Erfahrung von Experten aus unterschiedlichen Domänen akkumuliert haben.

Leitlinien zur Gestaltung von Systemarchitekturen											
Modularität					Komplexität			Flexibilität			
Berücksichtigung unterschiedlicher Lebenszyklen	Trennung von sicherheitskritisch und nicht-sicherheitskritischen Funktionen	unabhängig austauschbare Funktionsmodule (Plug & Play)	zweckorientierte Modularisierung	unabhängige Entwicklung und Test	Kommunikation zwischen den Systemelementen reduzieren	reduzierte Anzahlvon Schnittstellen	schlanke Schnittstellen (geringe Kopplung)	Erweiterbarkeit (upgrade)	Aktualisierbarkeit (update)	Kompatibilität	

Abbildung 8 Leitlinien zur Gestaltung von Systemarchitekturen. Erarbeitet aus den folgenden Quellen: (*Goll und Dausmann 2013), (Kossiakoff et al. 2011), (Maier und Eberhardt 2000)* und (Smith und Simpson 2011)

Die Leitlinien zur Gestaltung von Systemarchitekturen umfasst drei Hauptgruppen, die jeweils in weitere Untergruppen subsumiert sind.

Die Hauptgruppe **Modularität** aus den Leitlinien zur Gestaltung von Systemarchitekturen, die bereits von den Forschungsinitiativen (siehe oben) gefordert wird, zielt im Allgemeinen darauf ab, technische Systeme mit unterschiedlichen Lebenszyklen bei der Systementwicklung zu berücksichtigen. Mit der Modularisierung wird zudem bezweckt, dass Softwareanwendungen zweckorientiert gekapselt werden, sodass sie unabhängig voneinander entwickelt, implementiert und getestet (zugelassen) werden können. Außerdem ist die zweckorientierte Kapselung dafür da, die sicherheitsrelevanten Funktionen von den nicht-sicherheitsrelevanten zu trennen, um Rückwirkungsfreiheit gewährleisten zu können. Nicht zuletzt soll durch die Modularisierung auch die Austauschbarkeit der einzelnen Systeme ermöglicht werden, ohne dabei andere Systeme innerhalb einer Systemarchitektur zu beeinflussen.

Die **Komplexität** als die zweite Hauptgruppe der Leitlinie zielt auf die Wechselwirkung zwischen den Systemen in einer Systemarchitektur ab. Mit dieser Anforderung soll daher die Anzahl der Schnittstellen zwischen den Systemen reduziert werden. Nicht nur die reduzierte Anzahl an Schnittstellen beschreibt eine geringe Komplexität, sondern auch schlanke Schnittstellen mit geringem Kommunikationsaufwand oder mit reduziertem Datenaustausch sind für eine reduzierte Komplexität erforderlich.

Die dritte Hauptgruppe stellt die **Flexibilität** dar und resultiert aus der Forderung, dass Softwareanwendungen von rascher und kontinuierlicher Entwicklung geprägt sind. Die rasche Entwicklung von Softwareanwendungen fordert daher eine flexible Systemarchitektur, in der die Softwareanwendungen jederzeit unabhängig voneinander aktualisiert (update) und erweitert (upgrade) werden können. Mit der Flexibilität sollen daher neue Funktionen hinzugefügt oder bereits vorhandene Funktionen durch neue Funktionen ersetzt werden können.

Zusätzlich mit der **Kompatibilität** soll sichergestellt werden, dass neu hinzugefügte oder ersetzte Funktionen sofort mit anderen bereits vorhandenen Funktionen kommunizieren können, ohne dabei Anpassungen durchgeführt werden zu müssen. Flexibilität und Modularität sollen daher die Interoperabilität sicherstellen.

Als Fazit kann festgehalten werden, dass die von den Forschungsinitiativen geforderten Anforderungen an die Systemstruktur in Störungssituationen mit den allgemeinen Leitlinien zur Gestaltung von Systemarchitekturen, die sich aus jahrelanger Erfahrung von Experten aus unterschiedlichen Domänen akkumuliert haben, deckungsgleich sind.

3.2.3 Anforderungen an das Systemverhalten in Störungssituationen

Nachdem zuvor die Anforderungen an die Systemstruktur in Störungssituationen zusammengestellt wurden, werden in diesem Unterkapitel die Anforderungen an das Systemverhalten in Störungssituationen zusammengestellt. Die Quellen der Anforderungen an das Systemverhalten in Störungssituationen sind, wie zuvor erarbeitet, die Experten aus dem gegenwärtigen Betrieb, die ERJU, in denen auch Experten der nationalen Bahnbetreiber (z.B. DSD) mitwirken und die gesetzlichen und regulatorischen Dokumente.

In *Pachl (2017, S. 18)* wird die Forderung nach Lösungen zur Behandlung von Störungssituationen bestätigt. Der Autor ist der Ansicht, dass im vollautomatisierten Bahnbetrieb nur ***„diejenigen Rückfallebenen relevant [sind], bei denen der Triebfahrzeugführer mitwirken muss****. Keine Relevanz haben Rückfallebenen, bei denen der Fahrdienstleiter zwar in Personalverantwortung Hilfshandlungen zur ersatzweisen Fahrweg- und Zugfolgesicherung ausführen muss, die Zugfahrt aber trotzdem durch Signaleinrichtungen zugelassen wird.“* Demnach sollen im vollautomatisierten Bahnbetrieb nur für jene

Störungssituationen betrieblich-technische Rückfallebenen entwickelt werden, bei denen das fahrzeugseitige ATO-System aktiv mitwirken muss.

Wie bereits in der Aufgabenstellung aus dem Kapitel 3.1 bekannt, müssen die gegenwärtigen **Schutzziele** der Leit- und Sicherungstechnik auch im vollautomatisierten Bahnbetrieb weiterhin sichergestellt werden. Sofern ein Schutzziel aufgrund einer Störung nicht mehr erfüllt werden kann, soll mit einer entsprechenden betrieblich-technischen Rückfallebene ersatzweise das Schutzziel erfüllt werden können. Dabei ist das oberste Ziel aller Stakeholder die Gewährleistung der **Sicherheit des Betriebs**.

Wenngleich sowohl EIU als auch EVU im Betrieb für eine sichere Betriebsführung interagieren, ist die Gestaltung von betrieblich-technischen Rückfallebenen im Aufgabengebiet der EIU. Damit das EIU allen Kunden ein gerechtes Angebot unterbreiten und die Nutzung der Infrastruktur bei vereinbarter Betriebsqualität (z.B. wirtschaftlich optimaler Bereich) gewährleisten kann, ist nach *DB Netz AG (2022, S.5)* die Einhaltung der vereinbarten Beförderungszeiten notwendig. Daher soll nach den Experten aus dem gegenwärtigen Bahnbetrieb statt eines Stillstandes – der vollautomatisierte Bahnbetrieb auch in Störungssituationen – unter Einhaltung des Grundprinzips „**Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit**“ – mit möglichst hoher **Kapazität** fortgeführt werden.

Zur Einhaltung der Pünktlichkeit und zur Gewährleistung der Stabilität des Fahrplans wird daher von den Experten aus dem gegenwärtigen Betrieb gefordert, dass der vollautomatisierte Regelbetrieb nach Störungseintritt innerhalb kürzester Zeit wiederhergestellt werden soll. Demnach soll eine **möglichst kurze Dauer der Betriebsführung in Störungssituationen** angestrebt werden. Die Dauer einer vorliegenden Gefährdungssituation ist außerdem aus Sicherheitsgründen relevant. Denn die Expositionszeit, in der Schutzbedürftige (z.B. Fahrgäste) der möglichen Gefährdung ausgesetzt sind, sollte möglichst kurz sein. Nach *EBA (2012)* ist die Expositionszeit *„kurz, wenn diese klein im Vergleich zur gesamten Aufenthaltszeit im Fahrzeugbereichs ist und lang, wenn die Schutzbedürftigen während der überwiegenden Aufenthaltsdauer im Fahrzeugbereich der möglichen primären Gefährdung ausgesetzt sind“*.

Die technische Interoperabilität, die mit den Referenzarchitekturen von RCA und OCORA angestrebt wird, ist für einen europaweit einheitlichen Bahnbetrieb allein nicht ausreichend. Daher ist eine weitere Forderung der ERJU, dass auch die Betriebsprozesse für den vollautomatisierten Bahnbetrieb europaweit harmonisiert werden sollen, um die **betriebliche Interoperabilität** zu erreichen. Es soll daher auf Basis der Referenzarchitekturen von RCA und OCORA möglich sein, möglichst **allgemeingültige betrieblich-technische Rückfallebenen** zu entwickeln, die europaweit gültig sind.

Da der Betrieb in betrieblich-technischen Rückfallebenen – zumindest im gegenwärtigen Betrieb – aufgrund der Sicherheitsverantwortung des Betriebspersonals (Tf und Fdl) fehleranfällig ist und ihre Vorhaltung Kosten verursachen, sollen **so wenig wie möglich** und **nur so viel wie nötig** betrieblich-technische Rückfallebenen im vollautomatisierten Bahnbetrieb existieren.

Die Tatsache, dass technische Systeme von rascher und kontinuierlicher Entwicklung geprägt sind, ist bereits im vorigen Unterkapitel bei der Erhebung der Anforderungen an die Systemstruktur berücksichtigt worden. Sofern technische Systeme aufgrund fortschreitender Technologie weiterentwickelt werden, sollten nach ERJU auch die betrieblich-technischen Rückfallebenen mit fortschreitender Technologie mitwachsen können. Das bedeutet, dass auch die **Betriebsprozesse flexibel angepasst** werden sollen.

Des Weiteren wird in *Milius und Huang (2017)* explizit gefordert, dass betrieblich-technische Rückfallebenen im Zeitalter der Automatisierung von Cyber-Angriffen (**Security**) geschützt sein sollten.

Die Quelle der gesetzlichen Anforderungen an den vollautomatisierten Bahnbetrieb sind das allgemeine Eisenbahngesetz (AEG), die EU-Richtlinien, die untergeordnete Eisenbahn Bau- und Betriebsordnung (EBO) und die Richtlinien 408 und 418.

Im AEG wird im §4 Absatz 3 gefordert, dass *„die Eisenbahnen und Halter von Eisenbahnfahrzeugen verpflichtet sind, ihren **Betrieb sicher zu führen**“ (Bundesamt für Justiz 2021, S. 5)*. Weitere gesetzliche Anforderungen sind in der Eisenbahn Bau- und Betriebsordnung (EBO) zu finden. Dort wird im §47 Absatz (2) gefordert, dass *„die Betriebsbeamten für die **sichere und pünktliche Durchführung** des Eisenbahnbetriebs verpflichtet sind (Bundesamt für Justiz, 2019, S. 25).“* Außerdem wird im §47 Absatz (3) gefordert, dass *„die Betriebsbeamten in der zur sicheren Durchführung des Betriebs erforderlichen Anzahl einzusetzen sind (Bundesamt für Justiz, 2019, S. 25).“* Diese Anforderung ist für den vollautomatisierten Bahnbetrieb wichtig, da dadurch die **erforderliche Anzahl an Ressourcen zur sicheren Betriebsführung** in Störungssituationen beeinflusst wird. Auch in der EU-Richtlinie 2016/797 Anhang III Abschnitt 2.3.1 wird in Störungssituationen eine *„**Weiterfahrt** unter vorgegebenen Einschränkungen“* gefordert *(Europäische Union 2016, S. 91)*.

Als Zwischenfazit für die Anforderungen an das Systemverhalten in Störungssituationen können folgende zwei Punkte festgehalten werden:

- In Störungssituationen wird eine **Weiterfahrt** – unter Einhaltung des Grundprinzips „**Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit**“ – mit möglichst hoher **Kapazität** gefordert.
- Die Betriebsprozesse zur Weiterfahrt sollen unter Berücksichtigung der Tatsache, dass technische Systeme von rascher und kontinuierlicher Entwicklung geprägt sind, entwickelt werden.

Wie bereits in Unterkapitel 3.2.1 erwähnt, werden die von Stakeholdern an das Systemverhalten in Störungssituationen zusammengestellten Anforderungen gegen die Grundsätze einer guten Prozessgestaltung geprüft. In *Becker (2008)* werden dazu insgesamt 10 Grundsätze einer guten Prozessgestaltung definiert. Diese sind in der Abbildung 9 dargestellt.

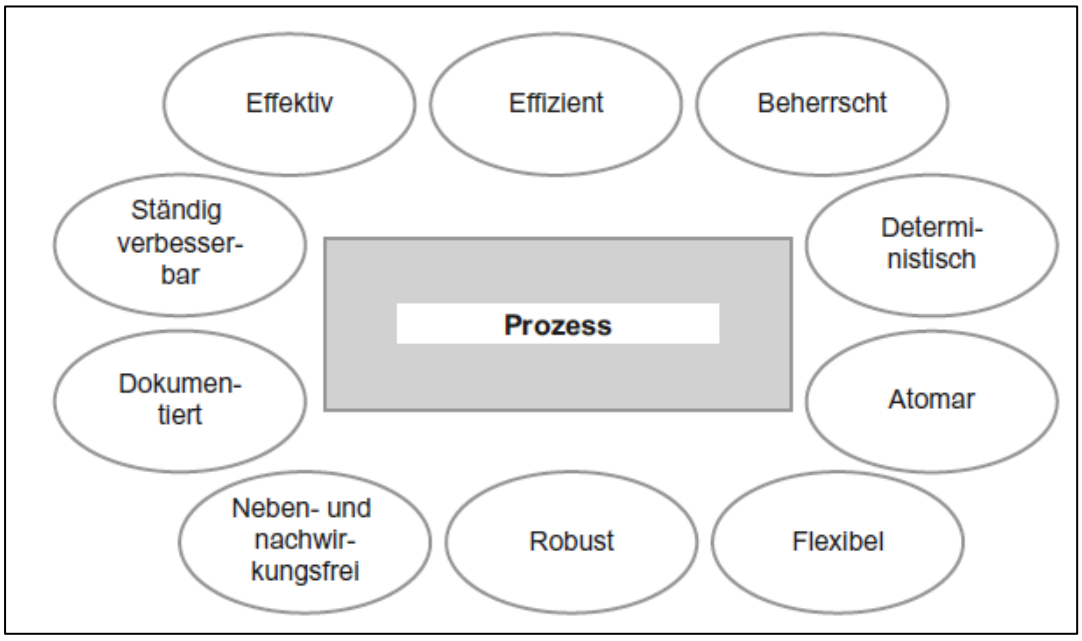

Abbildung 9 10 Grundsätze einer guten Prozessgestaltung *(Becker 2018)*

Im Allgemeinen sollte ein guter Prozess **effektiv**, **effizient** und zugleich **robust** sein. Diese drei Grundsätze widerspiegeln das Grundprinzip des Bahnbetriebs „**Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit**“ sowie die von den Forschungsinitiativen geforderte **wirtschaftliche Gestaltung und Durchführung** des Bahnbetriebs.

Ein guter Prozess sollte zudem **beherrscht, deterministisch, atomar und dokumentiert** sein. Demnach soll die Streuung der Prozessergebnisse minimal gehalten werden und das Ergebnis eines Prozesses sollte vorhersehbar sein. Insgesamt darf der Prozess nicht instabil werden und die äußeren Ereignisse dürfen die normale Prozessabwicklung nicht stören, sondern das erwartete Prozessergebnis muss in der vorhergesehenen Zeit erzeugt werden. Dabei sollte der Prozess aus beliebig vielen Einzelschritten bestehen, die jeweils spezielle Eingangsgrößen verarbeiten und jeweils eine einzelne Ausgangsgröße erzeugen. D.h. dass zwischen den Ressourcen, die bei der Betriebsführung in Störungssituationen eingesetzt werden, die Einzelschritte abgestimmt sind, sodass jede Ressource jeweils spezielle Eingangsgrößen verarbeitet und jeweils eine einzelne Ausgangsgröße erzeugt. Zudem soll ein beherrschter, deterministischer und atomarer Prozess so dokumentiert sein, wie er ausgeführt wird.

Die hier beschriebenen Grundsätze decken sich mit der Forderung, dass **so wenig wie möglich** und **nur so viel wie nötig** betrieblich-technische Rückfallebenen im vollautomatisierten Bahnbetrieb entwickelt werden sollen. Außerdem decken sich diese Grundsätze mit der geforderten **Allgemeingültigkeit** und der **Interoperabilität** der zu entwickelnden betrieblich-technischen Rückfallebenen.

Ein guter Prozess sollte außerdem **flexibel** und **ständig verbesserbar** sein, d.h. die zu entwickelnden betrieblich-technischen Rückfallebenen sind so zu gestalten, dass sie sich an geänderte Anforderungen schnell anpassen lassen und dass sie bei fortgeschrittener Technik (z.B. beim Update von Software) verbessert werden können. Diese beiden Grundsätze decken sich mit der von ERJU geforderten **Flexibilität**.

Ein guter Prozess sollte schließlich auch **neben- und nachwirkungsfrei** sein, d.h. laufende Prozesse dürfen nicht den Ablauf eines anderen Prozesses behindern. Die Neben- und Nachwirkungsfreiheit deckt sich nicht nur mit der geforderten **Sicherheit**, sondern adressiert auch die Anforderungen hinsichtlich der **Minimierung der Abweichung von der vereinbarten Betriebsqualität**.

Als Fazit kann festgehalten werden, dass die von den Experten aus dem gegenwärtigen Betrieb und von der ERJU geforderten Anforderungen an das Systemverhalten in Störungssituationen mit den allgemeinen Grundsätzen zur Gestaltung von guten Prozessen deckungsgleich sind.

3.2.4 Priorisierung der Anforderungen

Nachdem zuvor die Anforderungen an die Lösung der Aufgabenstellung zusammengestellt wurden, werden sie in diesem Unterkapitel für die Zielerreichung im Rahmen dieser Arbeit nach ihrer Relevanz priorisiert. Bei der Priorisierung wird der einfachen dreistufigen Anforderungsstruktur aus dem Anforderungsmanagement bedient.

- Anforderungen, deren Erfüllung für die Zielerreichung im Rahmen dieser Arbeit unabdingbar ist, werden als **Muss-Anforderungen** bezeichnet.
- **Soll-Anforderungen** hingegen sollten erfüllt werden. Es kann jedoch darauf verzichtet werden, sofern sie – z.B. aus zeitlichen Gründen – im Rahmen dieser Arbeit nicht erreichbar sind.
- Anforderungen, deren Erfüllung optional ist und somit keine signifikante Auswirkung auf die Zielerreichung hat, werden als **Kann-Anforderungen** bezeichnet.

Muss-Anforderungen an das Systemverhalten in Störungssituationen:

Eine wesentliche Muss-Anforderung an das Systemverhalten in Störungssituation ergibt sich aus den gesetzlichen und regulatorischen Forderungen.

Demnach wird im Rahmen dieser Arbeit die Weiterfahrt in Störungssituationen – unter Einhaltung des Grundprinzips „**Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit**“ – mit möglichst hoher **Kapazität** als **Muss-Anforderung** festgelegt.

Muss-Anforderungen an die Systemstruktur in Störungssituationen:

Um in Zukunft den ständigen technologischen Entwicklungen gerecht werden zu können, ist eine wesentliche Muss-Anforderung bei der Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb **die Einhaltung der Spezifikation hinsichtlich der Referenzarchitekturen** aus den Forschungsinitiativen RCA, OCORA und ERJU. Damit soll insbesondere eine Parallelentwicklung von Systemarchitekturen vermieden werden, damit die Ergebnisse dieser Arbeit in die Forschungsvorhaben in ERJU einfließen können.

Soll-Anforderung

Auch im Hinblick auf die Aussage aus *EUG (2020a)*, dass die Gestaltung von Betriebsprozessen mit vielen Abhängigkeiten verbunden ist, wird die Forderung hinsichtlich der **Interoperabilität als Soll-Anforderung priorisiert**. Die Erreichung der Interoperabilität ist zwar relevant, jedoch kann aufgrund fehlender physikalischer Systemarchitektur und fehlender Betriebserfahrung mit dem vollautomatisierten Bahnbetrieb die Erreichung der Interoperabilität nicht validiert werden.

Die restlichen Anforderungen aus den Unterkapiteln 3.2.2 – 3.3.3 gelten im weiteren Verlauf der Arbeit als Kann-Anforderungen.

3.3 Wahl der globalen Methode und Vorgehensweise zur Lösung der Aufgabenstellung

Unter Berücksichtigung der zuvor zusammengestellten Anforderungen sollen im Rahmen dieser Arbeit geeignete betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb entwickelt werden.

Dazu werden in diesem Kapitel zunächst die bereits in Kapitel 2.6 vorgestellten Methoden zur Lösung der Aufgabenstellung vergleichend diskutiert und darauf basierend eine geeignete Methode ausgewählt. In Kapitel 2.6 wurden bereits folgende Methoden zur Lösung der Aufgabenstellung vorgestellt:

- Prozess-Reengineering,
- Systems-Engineering nach EN 50126 und
- STPA-Methode

Zur Auswahl einer geeigneten Methode zur Lösung der Aufgabenstellung sind Kriterien erforderlich. Diese werden zunächst in Unterkapitel 3.3.1 aufgestellt. Die vergleichende Diskussion und Wahl der globalen Methode zur Lösung der Aufgabenstellung erfolgt in Unterkapitel 3.3.2. Die innerhalb der ausgewählten Methode vorkommenden Schritte zur Lösung der Aufgabenstellung werden anschließend in Kapitel 3.4 vorgestellt und den entsprechenden Hauptkapiteln zugeordnet.

3.3.1 Kriterien für die Wahl der globalen Methode

Die Kriterien für die Wahl der globalen Methode beruhen hauptsächlich auf der Zielsetzung und auf den in Kapitel 3.2 zusammengestellten Anforderungen sowie auf sonstigen Anforderungen. Kriterien aus der Zielsetzung und den daraus zusammengestellten Anforderungen sind wie folgt:

- Durch den Wegfall des Triebfahrzeugführers im Führerstand werden – wie bereits in Kapitel 2.4 vorgestellt – menschliche Fähigkeiten auf technische Systeme u.a. auf das ATO-System übertragen. Bei den in den Forschungsinitiativen (vgl. Kapitel 2.3) spezifizierten technischen Systeme für den vollautomatisierten Bahnbetrieb ist die logische Beziehung dieser technischen Systeme zueinander während einer Zugfahrt nicht vollständig vorhanden. Daher soll mit der ausgewählten Methode möglich sein, die Interaktion der im vollautomatisierten Bahnbetrieb vorhandenen technischen Systeme zu modellieren und zu beschreiben.
- Gefährliche Betriebssituationen, für die betrieblich-technische Rückfallebenen erforderlich sind, entstehen während einer Zugfahrt (vgl. Kapitel 2.4). Daher soll mit der ausgewählten Methode möglich sein, **gefährliche Betriebssituationen im vollautomatisierten** Bahnbetrieb **während einer Zugfahrt** – unter Berücksichtigung der Interaktion der im vollautomatisierten Bahnbetrieb vorhandenen technischen Systeme – **zu erarbeiten.**
- Nachdem die gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb während einer Zugfahrt erarbeitet werden, soll es **mit der Methode** auch möglich sein, **betrieblich-technische Rückfallebenen für die erarbeiteten Betriebssituationen zu entwickeln**.
- Es handelt sich zwar prinzipiell um eine Forschungsarbeit, jedoch soll mit der ausgewählten Methode auch möglich sein, die entwickelten betrieblich-technischen Rückfallebenen für eine Migrationsentscheidung hinsichtlich den Anforderungen **Sicherheit und Betriebsqualität zu bewerten.**

Sonstige Kriterien:

- Da es sich um eine Forschungsarbeit handelt, muss die Arbeit keine produktiven Lösungen für die Migration entwickeln. Daher muss mit der ausgewählten Methode nicht der vollständige Lösungsraum der betrieblich-technischen Rückfallebenen entwickelt werden, sondern es soll eine wissenschaftliche Grundlage dafür geschaffen werden, wie potenzielle betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb entwickelt werden können. Dennoch sollen mit der Methode die getroffenen Entscheidungen systematisch nachvollziehbar sein.
- Mit der ausgewählten Methode soll schließlich auch die Bearbeitungszeit berücksichtigt werden. Demnach soll die vorliegende Arbeit **im Wesentlichen durch den Autor allein durchführbar** sein (mit Unterstützung durch studentische Arbeiten und bei bestimmten Hilfstätigkeiten durch studentische Mitarbeiter und bei Implementierungsfragen z. B. durch einen Fachinformatiker).

3.3.2 Diskussion und Wahl der globalen Methode zur Lösung der Aufgabenstellung

Das Ziel dieser Arbeit ist es, geeignete betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb zu entwickeln. Die Diskussion und Auswahl der dafür geeigneten globalen Methode erfolgt in diesem Unterkapitel.

Aus dem Kapitel 2.4 ist bekannt, dass betrieblich-technische Rückfallebenen ein wesentlicher Bestandteil des gegenwärtigen Betriebs sind. Diese betrieblich-technischen Rückfallebenen beruhen auf jahrelangen Erfahrungen. Deshalb wäre es prinzipiell möglich, eine prozessorientierte Transformation vorzunehmen **(Prozess-Reengineering),** um die darin vorkommenden Prozessschritte auf die technischen Systeme im vollautomatisierten Bahnbetrieb zu allokieren.

Da die betrieblich-technischen Rückfallebenen aus dem gegenwärtigen Betrieb auf schriftlich niedergeschriebene Regeln beruhen, müssten dabei diese Regeln formalisiert und als Algorithmen beschrieben werden, damit die betrieblich-technischen Rückfallebenen automatisiert ablaufen können. Die strukturierte Formalisierung der gegenwärtigen betrieblich-technischen Rückfallebenen wäre im Rahmen dieser Arbeit durch den Autor durchführbar.

Die gegenwärtigen betrieblich-technischen Rückfallebenen wurden aus Erfahrungen heraus entwickelt, die aus zahlreichen Betriebsjahren und vor allem aus Unfällen und gefährlichen Ereignissen gewonnen wurden. Hinzu kommt, dass sie entsprechend nach neu eintretenden Ereignissen angepasst wurden.

Sofern also eine prozessorientierte Transformation als Methode gefolgt wird, existiert kein systematischer Ansatz, der bei der Entwicklung von betrieblich-technischen Rückfallebenen verfolgt werden kann. Damit wäre die Anforderung der europäischen Forschungsinitiative ERJU aus dem Kapitel 3.2 bezüglich der harmonisierten Betriebskonzepte im vollautomatisierten Bahnbetrieb nicht erfüllt. Es ist aus Sicherheitsgründen auch inakzeptabel, den vollautomatisierten Bahnbetrieb zu migrieren und erst nach dem ersten unerwünschten Ereignis die dafür geeignete betrieblich-technische Rückfallebene zu entwickeln.

Des Weiteren sind die bestehenden betrieblich-technischen Rückfallebenen für Störungen aus dem gegenwärtigen Betrieb entwickelt worden und stützen dabei auf eine intensive Kommunikation und Interaktion zwischen einem Triebfahrzeugführer und einem Fahrdienstleiter.

Entsprechend den Referenzarchitekturen von RCA und OCORA fallen einige technische Systeme aus dem gegenwärtigen Betrieb im vollautomatisierten Bahnbetrieb weg. Dazu gehören beispielsweise Signale oder PZB-Magneten. Infolge von neuen technischen Systemen im vollautomatisierten Bahnbetrieb – darunter insbesondere das ATO-System – sind jedoch auch neue Störungen denkbar, während einige Störungen aus dem gegenwärtigen Betrieb wegfallen (z.B. Signalstörungen).

Es ist nicht gewiss, ob mit einer prozessorientierten Transformation als Methode auch die neuen Störungen im vollautomatisierten Bahnbetrieb aufgefangen werden können. Dennoch kann eine Weitefahrt im Falle von Störungssituationen mit der betrieblich-technischen Rückfallebene „Fahren auf Sicht“ aus dem gegenwärtigen Betrieb fortgeführt werden, weshalb diese Betriebsart auch in die ETCS-Spezifikation aufgenommen wurde. Daher scheint es sinnvoll, die Betriebsart „Fahren auf Sicht“ im vollautomatisierten Bahnbetrieb nicht auszuschließen.

Bevor potenziell umsetzbare betrieblich-technische Rückfallebenen für den vollautomatisierten Bahnbetrieb entwickelt werden können, sollte unabhängig der Betriebsart „Fahren auf Sicht“ zunächst eruiert werden, für welche der neu erscheinenden Störungen betrieblich-technische Rückfallebenen erforderlich sind (d.h. gefährliche Betriebssituationen entstehen). Mit dem Prozess-Reengineering der gegenwärtigen betrieblich-technischen Rückfallebenen können neue Störungssituationen, die zu gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb führen können, jedoch nicht erarbeitet werden.

Eine weitere Methode, die insbesondere zur Erarbeitung von gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb herangezogen werden kann, wurde in Kapitel 2.6 als

Systems-Engineerings Methode nach EN 50126 vorgestellt. In der Systems-Engineerings Methode nach EN 50126 gibt es eine Phase der Gefährdungsanalyse. Darin können Störungen auf Basis einer Systemdefinition systematisch erarbeitet werden.

Da die Systemarchitektur des digitalen Bahnbetriebs noch nicht vollständig spezifiziert ist und Gefährdungen im Bahnbetrieb während einer Zugfahrt auftreten können, kann mit Hilfe der bereits in den Forschungsinitiativen für den vollautomatisierten Bahnbetrieb spezifizierten technischen Systemen eine funktionale Systemarchitektur der Zugfahrt erstellt werden. Auf Basis der funktionalen Systemarchitektur können strukturiert neue Störungen, die zu gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb während der Zugfahrt führen können, erarbeitet werden.

Damit wäre zwar der Nachteil der Prozess-Reengineering Methode kompensiert. Die Phase der Gefährdungsanalyse in EN 50126 basiert jedoch auf Daten aus der Vergangenheit (z.B. Unfalldaten) oder Erfahrungen von Domain-Experten und erfordert eine intensive Abstimmung zwischen diesen Domain-Experten. Da jedoch mit dem vollautomatisierten Bahnbetrieb noch keine Betriebserfahrung vorliegt, können auch auf vorhandene Daten nicht zurückgegriffen werden. Außerdem ist eine normbasierte Vorgehensweise durch den Autor allen aus Zeitgründen und aufgrund der vorgeschriebenen Kontrollmechanismen durch weitere Domain-Experten nicht möglich.

Wenngleich mit der Systems-Engineerings Methode nach EN 50126 ein vorläufiges System definiert und daraus systematisch Störungen erarbeitet werden können, bietet diese Methode ebenfalls keinen systematischen Ansatz zur Entwicklung von betrieblich-technischen Rückfallebenen.

Um Gefährdungen aus der funktionale Systemarchitektur der Zugfahrt im vollautomatisierten Bahnbetrieb bereits in der frühen Entwicklungsphase (ohne vollständige Spezifikation) der Systemarchitektur erarbeiten zu können, kann die ebenfalls in Kapitel 2.6 vorgestellte **STPA-Methode** herangezogen werden. Im Vergleich zu der Systems-Engineering Methode nach EN 50126 erfolgt die Modellierung der funktionalen Systemarchitektur nach einer strukturierten Notation aus der Regelungstechnik.

Die mit der STPA-Methode erstellte funktionale Systemarchitektur ordnet die darin vorkommenden technischen Systeme und ihre Funktionen in eine Hierarchie (hierarchische Regelungsstruktur). Dabei entstehen in der funktionalen Systemarchitektur verschiedene Regelungspfade. Die Absicht der STPA-Methode ist es, die Gefährdungsanalyse in die frühe Entwicklungsphase zu integrieren, um bereits in der Entwicklungsphase sicherheitsorientierte Design-Entscheidungen getroffen werden können.

Die Gefährdungsanalyse mit der SPTA-Methode erfolgt systematisch. Die SPTA-Methode hat ein klares Endkriterium hinsichtlich der Gefährdungsanalyse. Denn sobald alle Regelungspfade in einer funktionalen Systemarchitektur abgearbeitet sind, liegen alle potenziellen Gefährdungsursachen vor. Aufgrund der hierarchischen Darstellung erlaubt die STPA-Methode herauszufinden, welche Regelungspfade und Regelungsaktionen eine übergeordnete Rolle bei der Entstehung einer Gefährdung spielen.

Der wesentliche Vorteil der STPA-Methode im Vergleich zur Systems-Engineering-Methode nach EN 50126 besteht darin, dass das potenzielle Systemverhalten und die Gefährdungen in einem System durch die Analyse der Wechselwirkungen zwischen den darin enthaltenen Systemelementen erarbeitet werden, anstatt das Systemverhalten in Ereignisketten zu zerlegen. Die Ereignisketten resultieren aus den Verhalten der einzelnen Systemelemente innerhalb eines Systems. Außerdem erlaubt die STPA-Methode herauszufinden, welche Regelungspfade in der hierarchischen Regelungsstruktur die größte Rolle bei der Verursachung einer Gefährdung spielen. Der Fokus der STPA-Methode liegt somit

auf dem sicherheitsorientierten Systementwurf, um in der Entwurfsphase eines Systems bereits potenzielles gefährliches Systemverhalten antizipieren zu können.

Die STPA-Methode bietet zwar wie bei der Systems-Engineerings Methode nach EN 50126 ebenfalls keinen systematischen Ansatz zur Entwicklung von betrieblich-technischen Rückfallebenen, jedoch können mit der STPA-Methode bereits in der Entwicklungsphase sogenannte Sicherheitsbedingungen für das identifizierte gefährliche Systemverhalten, die von den technischen Systemen einzuhalten sind, erarbeitet werden.

Um auch bei unvollständiger Spezifikation der Systemarchitektur des digitalen Bahnbetriebs eine möglichst vollständige Gefährdungsanalyse durchführen zu können und somit die Nachteile der Systems-Engineering Methode nach EN 50126 zu kompensieren, wird die funktionale Systemarchitektur der Zugfahrt im vollautomatisierten Bahnbetrieb mit Hilfe der strukturierten Notation nach STPA entwickelt. Da die Gefährdungsanalyse nach der STPA-Methode auf unterschiedlichen Abstraktionsebenen durchgeführt werden kann, ist eine wiederholende Anwendung der Gefährdungsanalyse nach STPA-Methode auch bei fortlaufender Spezifikation der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme möglich. Aufgrund der strukturierten Notation ist die STPA-Methode auch durch den Autor allein durchführbar.

Da sowohl die Systems-Engineering Methode nach EN 50126 als auch die STPA-Methode keine Phase zur Entwicklung von betrieblich-technischen Rückfallebenen vorgeben und die Methode des Prozess-Reengineerings aus den oben genannten Gründen nicht geeignet ist, erfolgt im Rahmen dieser Arbeit die Entwicklung eines systematischen Ansatzes, anhand dessen betrieblich-technische Rückfallebenen für den vollautomatisierten Bahnbetrieb anforderungsgerecht entwickelt werden können. Dabei werden die zuvor in Kapitel 3.2 zusammengestellten Anforderungen bei der Entwicklung des systematischen Ansatzes verarbeitet.

Wie beim Prozess-Reengineering, ist auch bei der Systems-Engineering Methode nach EN 50126 und bei der STPA-Methode keine Bewertungsphase vorgesehen. Somit können auch bei der Anwendung der Systems-Engineering Methode nach EN 50126 oder STPA-Methode die zu entwickelnden betrieblich-technischen Rückfallebenen für eine Migrationsentscheidung in der Forschungsphase nicht bewertet werden.

Um dennoch eine Bewertung der zu entwickelnden betrieblich-technischen Rückfallebenen hinsichtlich der Auswirkung auf die Sicherheit der Betriebsführung und auf die Betriebsqualität für eine Migrationsentscheidung zu ermöglichen, werden die in Unterkapitel 2.4.5 vorgestellten Bewertungsverfahren anhand der Anforderungen diskutiert und daraus ein Bewertungsverfahren ausgewählt, anhand dessen die zu entwickelnden betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb hinsichtlich der Auswirkung auf die Sicherheit der Betriebsführung und hinsichtlich der Auswirkung auf die Betriebsqualität bewertet werden können.

Da die STPA-Methode im Vergleich zu den anderen beiden Methoden die in Unterkapitel 3.3.1 aufgestellten Kriterien mehrheitlich erfüllt, wird die Aufgabenstellung anhand der STPA-Methode gelöst. Die STPA-Methode ist in der Abbildung 10 grafisch dargestellt.

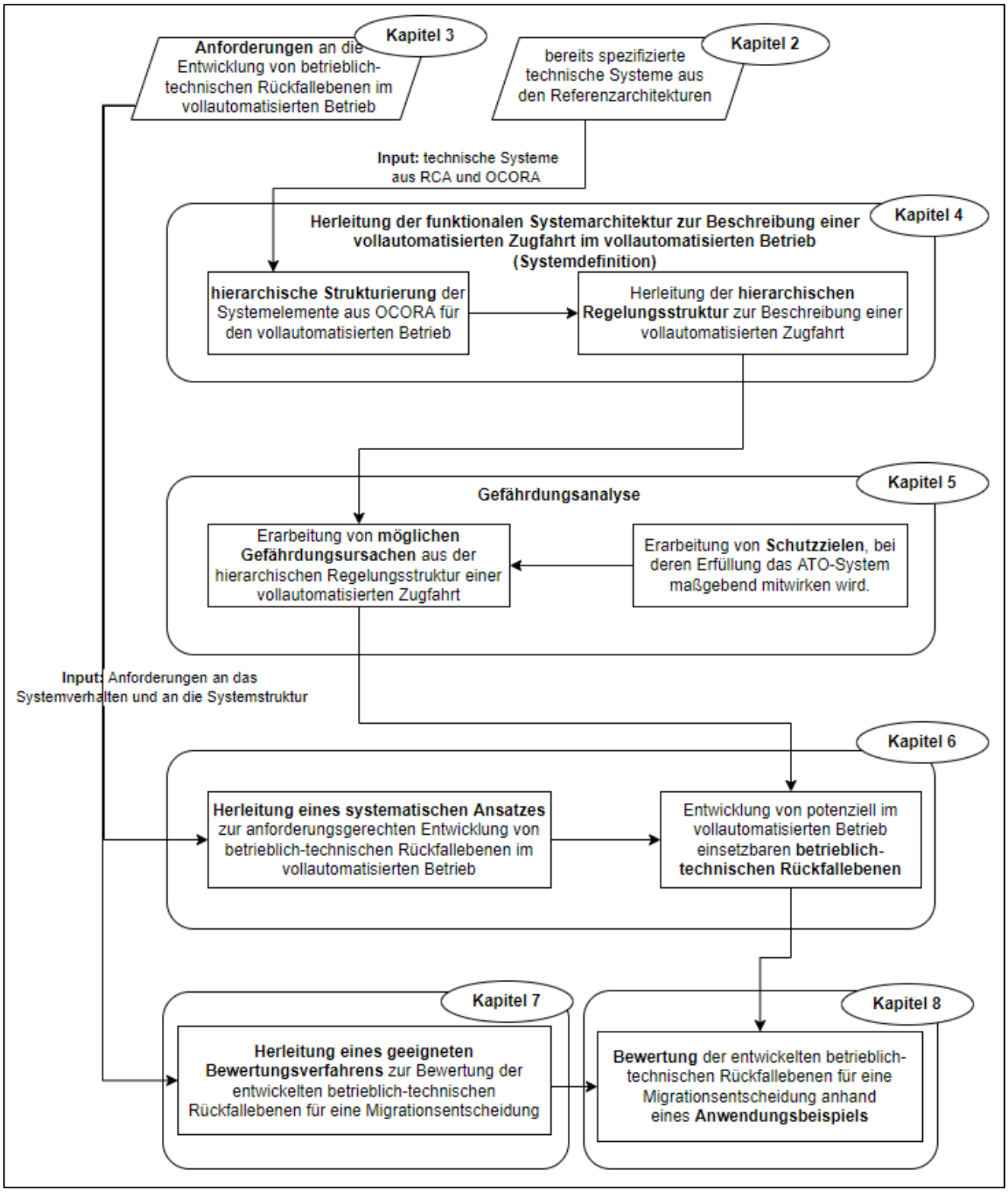

Abbildung 10 globale Methode zur Lösung der Aufgabenstellung (STPA-Methode)

3.4 Beschreibung der Vorgehensweise innerhalb der STPA-Methode und Aufbau der Arbeit

Auf Basis der gewählten Methode werden in diesem Kapitel die einzelnen Schritte zur Lösung der Aufgabenstellung beschrieben und den entsprechenden Hauptkapiteln zugeordnet. Die Hauptkapitel 3 bis 8 bilden zusammen den Kern der Arbeit.

Auf Basis der in **Hauptkapitel** 2 identifizierten Forschungslücke enthält das **Hauptkapitel 3** die Formulierung der Aufgabenstellung, die Anforderungsanalyse und die Auswahl der globalen Methode zur Lösung der Aufgabenstellung sowie die inhaltliche Abgrenzung der vorliegenden Arbeit.

Die STPA-Methode umfasst im Allgemeinen vier Hauptschritte. In einem ersten Schritt werden entsprechend der Abbildung 9 aus dem Kapitel 3.3 die bereits für den vollautomatisierten Bahnbetrieb spezifizierten technischen Systeme hierarchisch strukturiert. Dazu dienen die in den Forschungsinitiativen RCA und OCORA (vgl. Kapitel 2.3) bereits spezifizierten technischen Systeme als Eingangsgrößen. Im zweiten Schritt wird dann auf Basis der hierarchischen Strukturierung die funktionale Systemarchitektur zur Beschreibung der Zugfahrt im vollautomatisierten Bahnbetrieb in Form einer hierarchischen Regelungsstruktur (STPA-Notation) hergeleitet. Die ersten beiden Schritte sind in **Hauptkapitel 4** zu finden.

Die Schritte drei und vier der STPA-Methode sind in **Hauptkapitel 5** zu finden. Dazu werden im dritten Schritt zunächst die Schutzziele erarbeitet, bei deren Erfüllung das ATO-System im vollautomatisierten Bahnbetrieb maßgebend mitwirken wird. Danach werden im vierten Schritt die möglichen Gefährdungsursachen aus der hierarchischen Regelungsstruktur zur Beschreibung der Zugfahrt im vollautomatisierten Bahnbetrieb, wodurch die zuvor erarbeiteten Schutzziele verletzt werden können (gefährliche Betriebssituationen). Die Eingangsgröße für das Hauptkapitel 5 ist die in Hauptkapitel 4 hergeleitete hierarchischen Regelungsstruktur zur Beschreibung der Zugfahrt.

Das Ergebnis der Gefährdungsanalyse wird dann verwendet, um in **Hauptkapitel 6** betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb zu entwickeln. Wie bereits in Unterkapitel 3.3.2 erwähnt, wird in Hauptkapitel 6 zunächst ein systematischer Ansatz hergeleitet, anhand dessen die Entwicklung von potenziell einsetzbaren betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb erfolgt. Nachdem in Hauptkapitel 6 einige potenziell umsetzbare betrieblich-technische Rückfallebenen beispielhaft vorgestellt wurden, sollen diese entsprechend der Methode für eine Migrationsentscheidung hinsichtlich der Sicherheit und Betriebsqualität bewertet werden.

Daher werden in **Hauptkapitel 7** die in Unterkapitel 2.4.5 vorgestellten Bewertungsverfahren aufgegriffen, anhand der Anforderungen diskutiert und daraus ein Bewertungsverfahren ausgewählt. Sofern erforderlich, erfolgt vor der Auswahl die Anpassung des Bewertungsverfahrens entsprechend den Anforderungen aus dem Unterkapitel 2.4.5.

In **Hauptkapitel 8** werden dann die in Hauptkapitel 6 entwickelten betrieblich-technischen Rückfallebenen anhand eines Anwendungsbeispiels mit dem in Hauptkapitel 7 hergeleiteten Bewertungsverfahren bewertet.

Die Arbeit schließt in **Hauptkapitel 9** mit einer Zusammenfassung und einem Ausblick.

3.5 Inhaltliche Eingrenzung der Arbeit

Auf Basis der zusammengestellten Anforderungen und der hergeleiteten globalen Methode zur Lösung der Aufgabenstellung wird in diesem Kapitel aufgrund der zeitlichen Rahmenbedingungen der Arbeit eine inhaltliche Eingrenzung vorgenommen. Die inhaltliche Eingrenzung wird kapitelweise vorgenommen.

Eine vollständige Spezifikation der funktionalen Systemarchitektur des ATO-Systems für den vollautomatisierten Bahnbetrieb steht aus Zeitgründen nicht im Fokus des **Hauptkapitels 4**. Daher wird die funktionale Systemarchitektur zur Beschreibung einer Zugfahrt im vollautomatisierten Bahnbetrieb lediglich anhand der bereits in den Forschungsinitiativen spezifizierten technischen Systeme für den vollautomatisierten Bahnbetrieb und den Umsystemen, zu denen das ATO-System nach der RCA-Referenzarchitektur direkte Schnittstellen aufweist, auf einem höheren Abstraktionslevel modelliert. Die Granularität der funktionalen Systemarchitektur beruht auf der in RCA und OCORA definierten Systemelemente (engl. Building Blocks). Demnach werden technologische Lösungen, d.h. die Zuordnung der in Hauptkapitel 4 zu erarbeitenden funktionalen Systemarchitektur auf konkrete Hard- und Software (physikalische Systemarchitektur) ebenfalls nicht behandelt. Des Weiteren ist die Auswahl und Implementierung von geeigneten Algorithmen in den jeweiligen Systemelementen nicht Gegenstand des 4. Hauptkapitels.

Bei der Herleitung der funktionalen Systemarchitektur zur Beschreibung einer Zugfahrt im vollautomatisierten Bahnbetrieb werden zudem jegliche Prozesse vor und nach einer Zugfahrt (Rangierfahrten oder Abstell- und Bereitstellungsfahrten) im Rahmen dieser Arbeit nicht betrachtet.

Bei der Gefährdungsanalyse in **Hauptkapitel 5** werden lediglich Ursachen aus der in Hauptkapitel 4 hergeleiteten funktionalen Systemarchitektur der Zugfahrt im vollautomatisierten Bahnbetrieb erarbeitet. Da für das ETCS-System und für die Sicherungslogik bereits Gefährdungsanalysen durchgeführt wurden, müssen diese beiden Systeme mit den zugehörigen Systemelementen im Rahmen dieser Arbeit nicht erneut einer Gefährdungsanalyse unterzogen werden. Aus diesem Grund werden Gefährdungsursachen nur aus den beiden ATO-Systemen erarbeitet.

Mit der STPA-Methode ist es zwar auch möglich, externe Gefährdungsursachen (z.B. Cyber-Angriffe) zu erarbeiten. Jedoch stellt Security einen eigenen Forschungsbereich dar und wird daher aus Zeitgründen nicht betrachtet. Wenngleich keine konkreten Cyber-Angriffsvektoren bei der Gefährdungsanalyse erarbeitet werden, ist es sinnvoll, die möglichen Schwachstellen aus der in Hauptkapitel 4 hergeleiteten funktionalen Systemarchitektur hinsichtlich Cyber-Angriffe zu kennen. Daher werden die Gefährdungen deren Ursachen Cyber-Angriffe sein können, kurz erwähnt. Sowohl in Hauptkapitel 5 als auch im gesamten Verlauf der Arbeit sind planbare Ereignisse, wie z.B. Baustellen oder Abweichungen aufgrund von Großveranstaltungen sowie sich anbahnende Abweichungen (z.B. aufgrund von Unwetter) nicht im Fokus.

In Kapitel 2.5 wurde bereits erläutert, dass die Rückfallebenen im Bahnbetrieb im Wesentlichen drei Tätigkeitsfelder (Betriebsleitung, Betriebsführung und Ereignisbehandlung) umfassen. Im Rahmen dieser Arbeit werden in **Hauptkapitel 6** betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb für die Betriebsführung erarbeitet.

Entsprechend der Anforderung aus dem Unterkapitel 3.2.3 sind im vollautomatisierten Bahnbetrieb „*nur diejenigen Rückfallebenen relevant, bei denen [heute] ein Triebfahrzeugführer mitwirken muss“. Keine Relevanz haben Rückfallebenen, bei denen der Fahrdienstleiter zwar in Personalverantwortung Hilfshandlungen zur ersatzweisen Fahrweg- und Zugfolgesicherung ausführen muss, die Zugfahrt aber trotzdem durch Signaleinrichtungen zugelassen wird (Pachl 2017, S. 18).“* Demnach werden nur für jene Störungssituationen betrieblich-technische Rückfallebenen entwickelt, bei denen das fahrzeugseitige ATO-System aktiv mitwirken muss. Störungen z.B. an der Sicherungslogik, wodurch die sichere Abstandsregelung der Züge nicht mehr gewährleistet werden kann und dafür Fahrterlaubnisse mit reduzierter Geschwindigkeit (z.B. Fahren auf Sicht) erteilt werden müssen, sind nicht Gegenstand dieser Arbeit.

Die in Unterkapitel 2.4.1 erläuterten technischen Rückfallebenen in Form von Redundanzen in der Systemarchitektur sind ebenfalls nicht im Fokus dieser Arbeit, da sie bei der Entwicklung von sicherheitsrelevanten technischen Systemen für den Bahnbetrieb von den Forschungsinitiativen und von den Normen EN 50128 und EN 50129 sowieso gefordert werden. Ebenfalls sind Lösungen für Betriebsleitung, die u.a. Störfallprogramme enthalten und Lösungen für Ereignisbehandlung, die Ursachen der Störungen und Maßnahmen durch Entstörungspersonal umfassen, nicht Gegenstand dieser Arbeit.

Die in Kapitel 3.2 zusammengestellten Anforderungen bezüglich der Bewertung der betrieblich-technischen Rückfallebenen basieren auf dem Grundprinzip des Bahnbetriebs „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“. Daher werden in **Hauptkapitel 7** nur Bewertungsverfahren berücksichtigt, die dieses Grundprinzip berücksichtigen können. Bewertungen hinsichtlich der energiesparsamen Fahrweise oder der Gestaltung eines robusten Fahrplans für den vollautomatisierten Bahnbetrieb sind nicht Gegenstand dieser Arbeit. Es gibt bereits unterschiedliche eisenbahnbetriebswissenschaftliche Verfahren zur Bestimmung von bahnbetrieblichen Kenngrößen. Da diese Verfahren hauptsächlich toolbasiert durchgeführt werden und die Herleitung und Anwendung nicht den Kern dieser Arbeit darstellen, ist die Diskussion und Anwendung jeglicher eisenbahnbetriebswissenschaftlicher Verfahren nicht Gegenstand dieser Arbeit.

Da die Ergebnisse **in Hauptkapitel 8** von den Ergebnissen aus den Hauptkapiteln 6 und 7 abhängig sind, kann keine Abgrenzung im Voraus vorgenommen werden. Die Abbildung 11 soll die inhaltliche Abgrenzung der Arbeit darstellen.

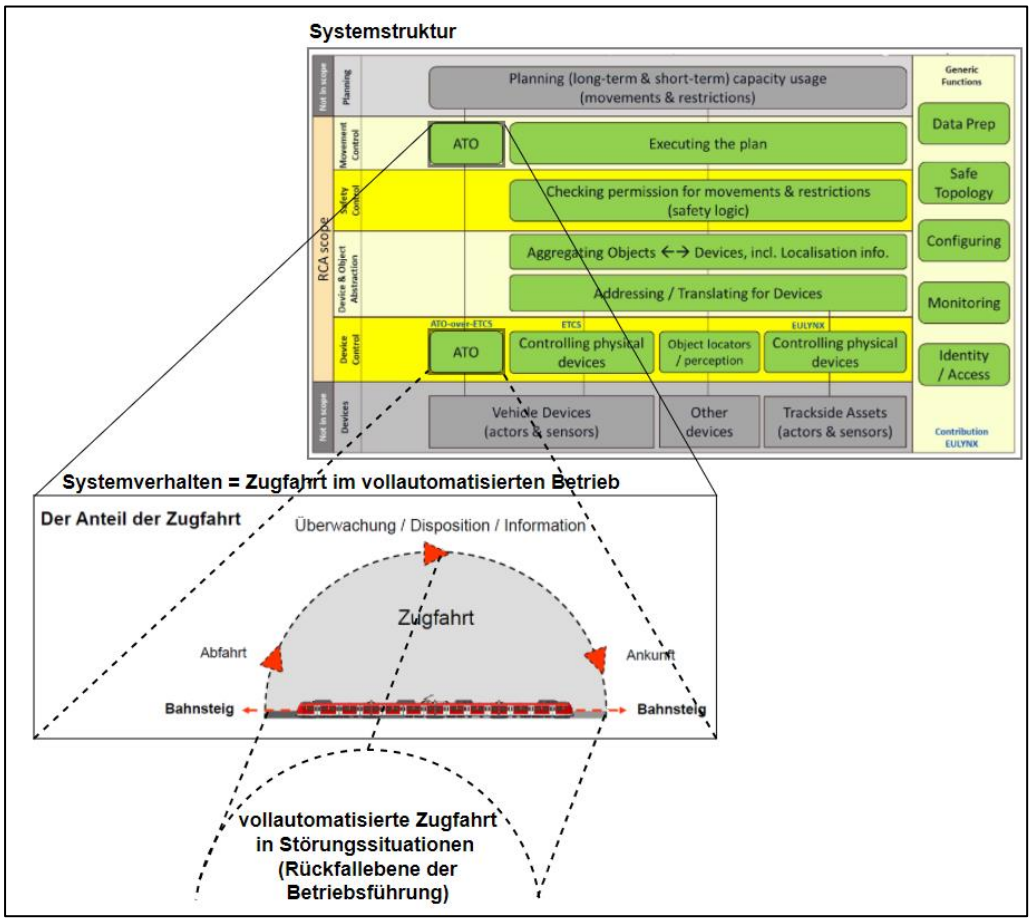

Abbildung 11 grafische Darstellung der inhaltlichen Abgrenzung in der Arbeit. Modifiziert in Anlehnung an *EUG (2020a)* und *Fassel (2008)*

3.6 Definition häufig verwendeter Begriffe

An dieser Stelle erscheint es für das Verständnis der Arbeit sinnvoll, häufig verwendete und in der Literatur zum Teil unterschiedlich verstandene Begriffe zu definieren. Dabei handelt es sich insbesondere um Begriffe aus der Systemarchitektur.

Zum Zwecke der Übersichtlichkeit erfolgt die Definition der Begriffe kapitelweise. Außerdem wird die Beziehung der häufig verwendeten Begriffe in ein Diagramm dargestellt, damit das Verständnis beim Lesen erleichtert wird.

In **Hauptkapitel 4** kommen folgende Begriffe häufig vor.

Technische Systeme:

Als technische Systeme im Rahmen dieser Arbeit werden jegliche durch Menschen erstellte Artefakte bezeichnet, die wiederum aus Systemelementen bestehen können. In einer logischen Beziehung zueinander verfolgen die technischen Systeme gemeinsam ein Ziel (im Rahmen dieser Arbeit Durchführung von vollautomatisierten Zugfahrten). Technische Systeme kommen entsprechend der Spezifikation in RCA und OCORA in Form von Hard- oder Software vor.

ATO-System:

Zur Durchführung von vollautomatisierten Zugfahrten wird durch die Abwesenheit des Triebfahrzeugführers entsprechend des Kapitels 2.3 das sogenannte ATO-System eingeführt. Anders als in der Literatur, wird im Rahmen dieser Arbeit das ATO-System nicht nur als ein technisches System zur Geschwindigkeitsregelung verstanden, sondern bildet darüber hinaus auch weitere Fähigkeiten eines Triebfahrzeugführers ab und ermöglicht dadurch einen vollautomatisierten Zugbetrieb.

Das ATO-System ist entsprechend den Anforderungen von RCA und OCORA ein softwarebasiertes technisches System, das aus den beiden Teilsystemen **ATO-TS und ATO-OBU** besteht. Jedes Teilsystem umfasst wiederum Systemelemente.

Systemelement:

Entsprechend des Hierarchie-Prinzips der Systeme stellen Systemelemente eine Teilmenge von technischen Systemen dar. Systemelemente werden im Rahmen dieser Arbeit als hardwarebasierte und softwarebasierte Systemelemente bezeichnet.

Funktionale Systemarchitektur:

Eine funktionale Systemarchitektur beschreibt die **organisatorische Struktur** eines Systems hinsichtlich der Abbildung der Vernetzung der Einzelfunktionen und ihrer Abbildung (Allokation) auf Systemelemente. Im Rahmen dieser Arbeit wird mit der funktionalen Systemarchitektur die organisatorische Struktur der für eine Zugfahrt im vollautomatisierten Bahnbetrieb erforderlichen Systemelemente beschrieben.

Hierarchische Regelungsstruktur:

Die funktionale Systemarchitektur zur Beschreibung einer Zugfahrt im vollautomatisierten Bahnbetrieb wird anhand der STPA-Methode hergeleitet. Entsprechend der STPA-Methode werden das Zusammenwirken und die Vernetzung der Systemelemente hierarchisch dargestellt. Die hierarchische Darstellung hat die Absicht, dass das hierarchisch höher liegende Systemelement das darunterliegende Systemelement mit sogenannten Kontrollaktionen steuert. Im Gegenzug übermitteln die in der Hierarchieebene gesteuerten Systemelemente sogenannte Rückkopplungen. Die so entstandene organisatorische Struktur wird als hierarchische Regelungsstruktur bezeichnet.

Zugfahrt:

Eine Zugfahrt beschreibt gemäß der Definition *„auf die freie Strecke übergehende oder innerhalb von Bahnhöfen nach einem Fahrplan verkehrende, aus Regelfahrzeugen bestehende, durch Maschinenkraft bewegte Einheiten und einzeln fahrende Triebfahrzeuge“ (Pachl 2011, S. 12)*, die nur mit einem gültigen Fahrplan verkehren darf.

Die Abbildung 12 zeigt die kausale Beziehung der in Hauptkapitel 4 häufig verwendeten Begriffe.

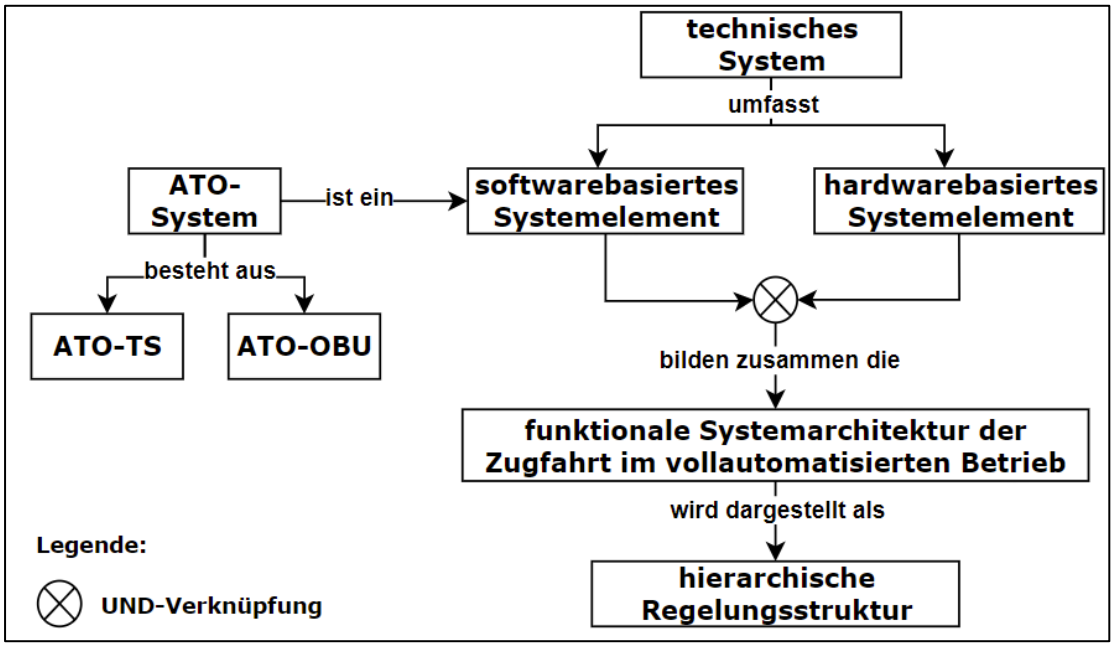

Abbildung 12 die kausale Beziehung der in Hauptkapitel 4 häufig verwendeten Begriffe (eigene Darstellung)

In **Hauptkapitel 5** kommen folgende Begriffe häufig vor.

Gefährdung:

Eine Gefährdung beschreibt nach EN 50126 die aus den Fehlern und Ausfällen resultierenden betrieblichen Verhältnisse, die zu einem Unfall führen können.

Gefährdungsraum:

Der Begriff Gefährdungsraum wird im Rahmen dieser Arbeit für Gefährdungen in einem bestimmten betrieblichen und umgebungsbedingten Kontext, die aus den Systemelementen der beiden ATO-Systeme im vollautomatisierten Bahnbetrieb verursacht werden können, verwendet.

Betrieblicher- und umgebungsbedingter Kontext:

Nach EN 50126 legt der betriebliche und umgebungsbedingte Kontext fest, wo und wann eine Gefährdung auf der Ebene des Bahnsystems sich zu einem Unfall entwickeln kann.

Minimaler Betrachtungsraum:

Ein minimaler Betrachtungsraum stellt eine Teilmenge des betrieblichen- und umgebungsbedingten Kontextes dar und ist für eine objektive Begründung, inwiefern die zu erarbeitenden Gefährdungsursachen im Rahmen dieser Arbeit im vollautomatisierten Bahnbetrieb eine gefährliche Betriebssituation darstellen, ausreichend.

Die Abbildung 13 zeigt die kausale Beziehung der in Hauptkapitel 5 häufig verwendeten Begriffe.

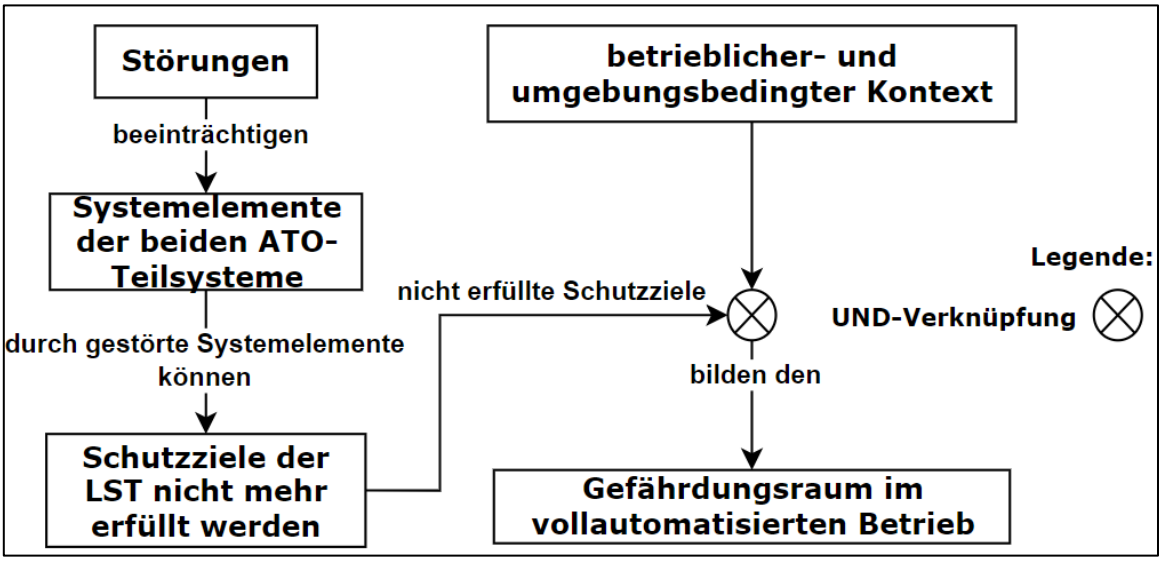

Abbildung 13 kausale Beziehung der in Hauptkapitel 5 häufig verwendeten Begriffe (eigene Darstellung)

In **Hauptkapitel 6** kommen folgende Begriffe häufig vor.

Dynamische Adaption:

Die dynamische Adaption beschreibt im Allgemeinen die Anpassung eines technischen Systems oder dessen Systemelemente an seine aktuelle Umgebung. Das technische System kann entweder das eigene Verhalten oder seine Beziehung zum benachbarten technischen System anpassen. Beim ersteren liegt eine Rekonfiguration und beim letzteren eine kompositionale Anpassung vor. Im Rahmen dieser Arbeit wird unter der dynamischen Adaption die situationsabhängige Anpassung der funktionalen Systemarchitektur der Zugfahrt im vollautomatisierten Bahnbetrieb verstanden.

Rekonfiguration:

Rekonfiguration ist eine Teilmenge der dynamischen Adaption und beschreibt im Rahmen dieser Arbeit einen Prozess, der ein hardwarebasiertes oder softwarebasiertes Systemelement innerhalb der funktionalen Systemarchitektur zur Laufzeit verändert (z.B. deaktiviert).

Kompositionale Anpassung:

Kompositionale Anpassung ist ebenfalls eine Teilmenge der dynamischen Adaption und beschreibt im Rahmen dieser Arbeit einen Prozess, bei dem die Schnittstellen zwischen den hardwarebasierten oder softwarebasierten Systemelementen in der funktionalen Systemarchitektur vorübergehend verändert werden (strukturelle und funktionelle Rekonfiguration).

Laufzeit:

Der Begriff Laufzeit wird im Allgemeinen definiert als die Zeit, die seit der Aktivierung eines Systems vergangen ist. Im Rahmen dieser Arbeit wird unter dem Begriff Laufzeit die Zeit nach der Migration des vollautomatisierten Bahnbetriebs verstanden. Darunter fällt auch die Zeit während einer Zugfahrt.

Ressource:

Als Ressource wird im Rahmen dieser Arbeit im Allgemeinen ein Betriebsmittel bezeichnet, welches während einer vollautomatisierten Zugfahrt – sowohl im Regelbetrieb als auch in Störungssituationen – eingesetzt werden kann. Die Ressource selbst umfasst technische Systeme und das Betriebspersonal.

Fähigkeit:

Fähigkeit im Rahmen dieser Arbeit beschreibt das Imstande sein einer Ressource, eine bestimmte betriebliche Funktion zu erfüllen.

Betriebspersonal:

Das Betriebspersonal stellt eine Ressource dar, welches während einer vollautomatisierten Zugfahrt – insbesondere in Störungssituationen – eingesetzt werden kann. Als Betriebspersonal kommen im Rahmen dieser Arbeit der in Kapitel 2.5 vorgestellte Train-Operator und das Zugpersonal, das bei GoA3 geführten Personenzügen im Zug anwesend ist, in Frage.

Betrieblich-technische Rückfallebene:

Betrieblich-technische Rückfallebenen stellen Ersatzverfahren zur Durchführung des vollautomatisierten Bahnbetriebs in Störungssituationen dar, bei dem die Schutzziele, die durch das gestörte technische System im Regelbetrieb erfüllt wurden, ersatzweise durch anderweitige Ressourcen übernommen werden.

Die Abbildung 14 zeigt die kausale Beziehung der in Hauptkapitel 6 häufig verwendeten Begriffe.

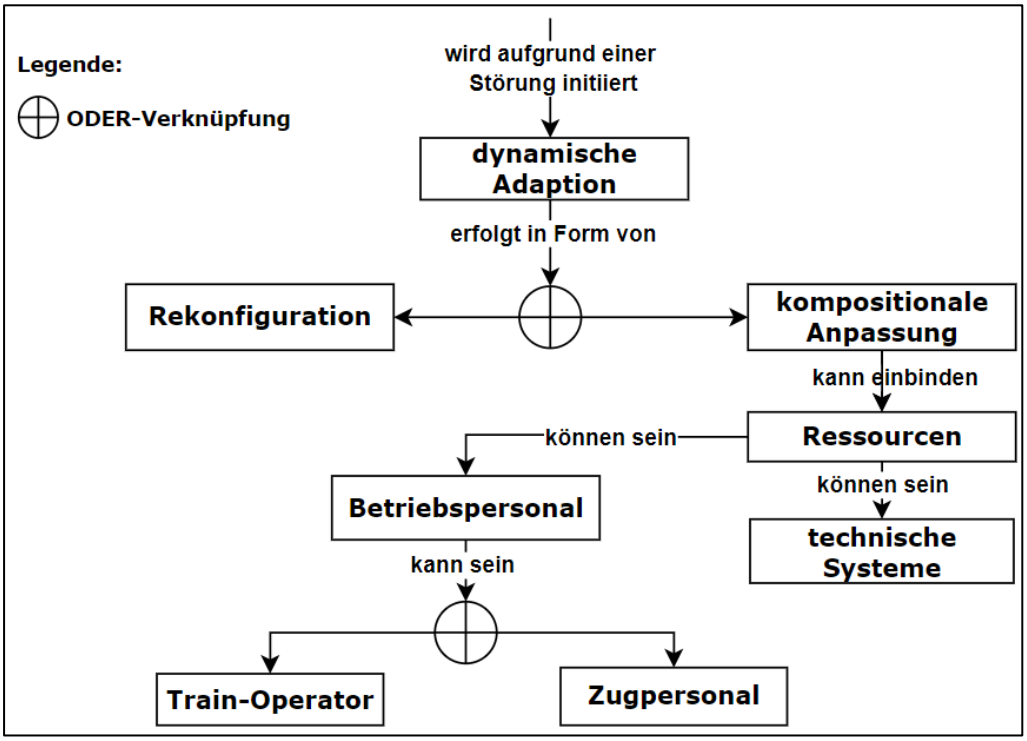

Abbildung 14 kausale Beziehung der in Hauptkapitel 6 häufig verwendeten Begriffe (eigene Darstellung)

4 Funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt

4.1 Ziele des Kapitels

Aus dem Kapitel 2.3 ist bekannt, dass in den Forschungsinitiativen RCA und OCORA bereits technische Systeme für den vollautomatisierten Bahnbetrieb spezifiziert wurden.

Da Gefährdungen im Bahnbetrieb während einer Zugfahrt auftreten können, ist entsprechend der globalen Methode (STPA-Methode) aus dem Kapitel 3.3 zunächst die logische Beziehung der für den vollautomatisierten Bahnbetrieb spezifizierten technischen Systeme zueinander erforderlich.

Durch die logische Beziehung der für den vollautomatisierten Bahnbetrieb spezifizierten technischen Systeme zueinander entsteht eine funktionale Systemarchitektur. Diese dient dann als Grundlage für die systematische Gefährdungsanalyse im nächsten Hauptkapitel.

Das Ziel dieses Hauptkapitels ist die Herleitung einer funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt. Dazu dienen die in den Forschungsinitiativen RCA und OCORA (vgl. Kapitel 2.3) bereits spezifizierten technischen Systeme als erste Grundlage. Da die technischen Systeme in den Forschungsinitiativen RCA und OCORA als Systemelemente bezeichnet wurden, wird diese Bezeichnung im weiteren Verlauf des Hauptkapitels und der Arbeit verwendet.

Entsprechend der STPA-Methode aus dem Kapitel 3.3 können die Inhalte dieses Hauptkapitels den ersten beiden Schritten innerhalb der STPA-Methode zugeordnet werden.

4.2 Anforderungen an die Herleitung einer funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt

Die in diesem Hauptkapitel herzuleitende funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt ist lediglich eine notwendige Vorarbeit für systematische Gefährdungsanalyse im nächsten Hauptkapitel, weshalb in Hauptkapitel 3 keine Anforderungen an die Entwicklung einer funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt zusammengestellt wurden.

In diesem Kapitel werden dennoch einige relevante Anforderungen aus dem Kapitel 3.2 an die Herleitung einer funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt zusammengestellt.

Aus den in Kapitel 3.2 zusammengestellten Anforderungen sind nur jene für die Herleitung der funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt relevant, die an die Gestaltung der Systemarchitektur des digitalen Bahnbetriebs aufgestellt wurden. Diese Anforderungen ergeben sich primär aus den Forschungsinitiativen RCA, OCORA und ERJU und orientieren sich an die allgemeinen Leitlinien zur Gestaltung von Systemarchitekturen.

- Damit zu den Forschungsinitiativen RCA und OCORA keine Parallelentwicklung stattfindet und die technische sowie die betriebliche Interoperabilität im zukünftigen digitalen Bahnbetrieb sichergestellt werden kann, sollen die bereits in RCA und OCORA für den vollautomatisierten Bahnbetrieb spezifizierten Systemelemente auch in diesem Hauptkapitel weiterverwendet werden.
- Da in RCA mit der Referenzarchitektur bereits eine **hierarchische Struktur für die zukünftige Leit- und Sicherungstechnik** vorgegeben wird, soll diese auch im Rahmen dieses Hauptkapitels berücksichtigt werden.

- Gemäß der Anforderung aus dem Unterkapitel 3.2.2 soll die **Modularität** der funktionalen Systemarchitektur sichergestellt und dabei die **Interaktion** der Systemelemente darin mit **möglichst generischen** Schnittstellen beschrieben werden.
- Aufgrund der Tatsache, dass Systemelemente ständigen technologischen Entwicklungen ausgesetzt sind, sollen die Systemelemente und damit auch die in diesem Hauptkapitel herzuleitende funktionale Systemarchitektur **flexibel** sein.
- Des Weiteren wird in den Leitlinien zur Gestaltung von Systemarchitekturen gefordert, dass die funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt nicht nur **verständlich**, sondern auch **eindeutig** und **konsistent** (widerspruchsfrei) beschrieben werden soll. Da die natürliche Sprache anfällig für Mehrdeutigkeiten ist und die Systemelemente für den vollautomatisierten Bahnbetrieb zum Teil mit unterschiedlichen Bezeichnungen spezifiziert wurden, die Mehrdeutigkeiten enthalten, (vgl. Kapitel 2.4), soll in diesem Kapitel durch eine einheitliche Bezeichnung der jeweiligen Systemelemente die Eindeutigkeit und Konsistenz sichergestellt werden.

Unter Berücksichtigung dieser Anforderungen wird in diesem Hauptkapitel eine funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt hergeleitet.

4.3 Vorgehensweise bei der Herleitung der funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt

Die Herleitung der funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt erfolgt entsprechend der STPA-Methode, die eine strukturierte Notation aufweist. Die Abbildung 15 stellt den Ausschnitt aus der globalen Methode dar, der für dieses Hauptkapitel relevant ist.

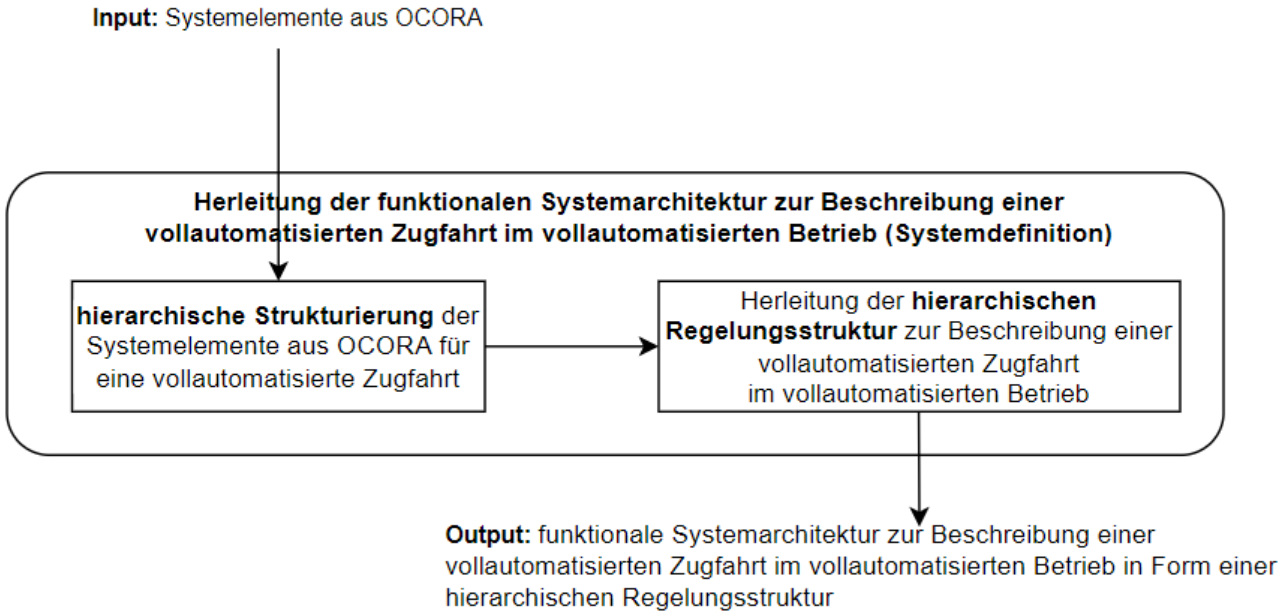

Abbildung 15 Ausschnitt aus der globalen Methode zur Herleitung der funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt im vollautomatisierten Bahnbetrieb (eigene Darstellung)

Wie aus dem Kapitel 3.3 bekannt, umfasst die STPA-Methode insgesamt vier Schritte, von denen zwei für dieses Hauptkapitel relevant sind.

In einem ersten Schritt erfolgt zunächst die hierarchische Strukturierung der Systemelemente. In der RCA-Referenzarchitektur aus dem Unterkapitel 2.3.2 liegt bereits eine hierarchische Strukturierung der darin vorkommenden Systemelemente vor. Da eine hierarchische Strukturierung der fahrzeugseitigen Systemelemente in OCORA nicht vorhanden ist, erfolgt zunächst innerhalb des ersten Schritts der STPA-Methode zunächst in Kapitel 4.4 die hierarchische Strukturierung der Systemelemente aus OCORA für eine vollautomatisierte Zugfahrt. Damit soll die logische Beziehung der darin vorkommenden Systemelemente für eine vollautomatisierte Zugfahrt beschrieben werden.

Bei der hierarchischen Strukturierung geht es darum, die Rollen und Befugnisse der einzelnen Systemelemente während einer vollautomatisierten Zugfahrt zu ermitteln. Es geht also darum, zu erarbeiten, welche Kontrollaktionen die für den vollautomatisierten Bahnbetrieb erforderlichen Systemelemente brauchen, um ihre Funktionen auszuführen und welche Kontrollaktionen sie als Ausgabe generieren sowie an welches Systemelement diese Kontrollaktionen gerichtet sind.

Entsprechend der STPA-Methode entsteht bei der hierarchischen Strukturierung eine hierarchische Regelungsstruktur. Alle Systemelemente in einer hierarchischen Regelungsstruktur haben die Kontrolle über das unmittelbar untergeordnete Systemelement. Da das Verhalten eines Triebfahrzeugführers während einer Zugfahrt mit einem Mensch-Maschine System beschrieben werden kann, und ein Mensch-Maschine System eine Regelungsstruktur darstellt, wird die hierarchische Strukturierung der Systemelemente aus OCORA mit Hilfe des Modells der menschlichen Informationsverarbeitung vorgenommen. Dazu dienen die in OCORA (vgl. Kapitel 2.4) bereits spezifizierten Systemelemente als erste Grundlage.

Im zweiten Schritt wird dann auf Basis der hierarchischen Strukturierung in Kapitel 4.5 die funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt in Form einer hierarchischen Regelungsstruktur hergeleitet. Dazu werden sowohl die Systemelemente aus der RCA-Referenzarchitektur als auch die in Kapitel 4.4 hierarchisch strukturierten Systemelemente aus OCORA entsprechend der STPA-Notation in eine hierarchische Regelungsstruktur überführt.

In Kapitel 4.6 ist die Zusammenfassung des Hauptkapitels zu finden.

4.4 Hierarchische Strukturierung der Systemelemente aus OCORA für eine vollautomatisierte Zugfahrt

Entsprechend der OCORA-Referenzarchitektur aus dem Unterkapitel 2.3.2 können die bereits in OCORA für den vollautomatisierten Bahnbetrieb spezifizierten Systemelemente wie folgt aufgelistet werden:

- Perception Sensors (P-Sensors)
- Perception System (PSs)
- Vehicle Localization Sensors
- Vehicle Localization System
- Digital Map
- Vehicle Supervisor (VS) (ETCS-OBU)
- ATO-Vehicle und
- FRMCS Mobile Gateway.

Da für diese Systemelemente die logische Beziehung zueinander für eine vollautomatisierte Zugfahrt noch nicht besteht, wird im Folgenden entsprechend der Vorgehensweise aus dem Kapitel 4.3 die

hierarchische Strukturierung dieser Systemelemente mit Hilfe des Modells der menschlichen Informationsverarbeitung vorgenommen.

Aus dem vereinfachten Modell der menschlichen Informationsverarbeitung, wie es in Abbildung 16 dargestellt ist, liegt das perzeptuelle Systemelement am Anfang des Informationsflusses. Das perzeptuelle Systemelement weist zum einen Schnittstellen zu den angeschlossenen Sensoren auf. Es ist dafür zuständig, die von den Sensoren aus der Umwelt erfassten Rohdaten zu verarbeiten und das Ergebnis für das nachfolgende Systemelement bereitzustellen. Das nachfolgende Systemelement zum perzeptuellen Systemelement stellt in der Abbildung 16 das kognitive Systemelement dar.

Im kognitiven Systemelement werden dann die vorverarbeiteten Rohdaten zu Informationen transformiert, woraus dann Entscheidungen getroffen werden können. Im Kontext einer Zugfahrt repräsentiert das kognitive Systemelement die Planungs- und Entscheidungsfähigkeit eines Triebfahrzeugführers.

Das Ergebnis des kognitiven Systemelements wird in dem Modell der menschlichen Informationsverarbeitung an das Aktor-Systemelement übertragen. Das Aktor-Systemelement löst Aktionen aus und repräsentiert die betriebliche Funktion Regelung und Steuerung, zu denen die Geschwindigkeitsregelung und die Steuerung der Fahrzeugkomponenten gehören.

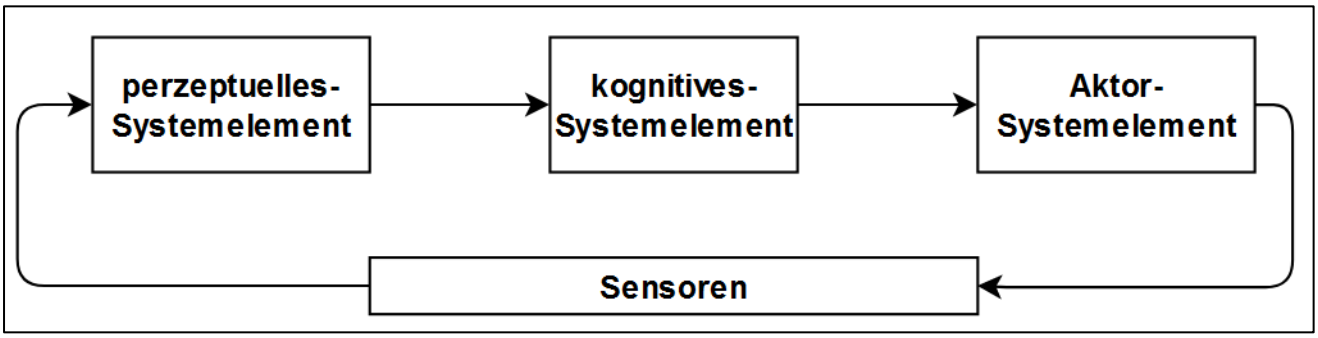

Abbildung 16 vereinfachtes Modell der menschlichen Informationsverarbeitung zur Kategorisierung der für eine vollautomatisierte Zugfahrt erforderlichen Systemelemente

Wie aus dem Unterkapitel 2.3.4 bekannt, überwacht die fahrzeugseitige Zugsicherung (ETCS-OBU) bereits heute das Fahrverhalten eines Triebfahrzeugführers und greift im Falle einer Geschwindigkeitsüberschreitung bremsend in die Fahrzeugleittechnik ein. Damit stellt die ETCS-OBU entsprechend der STPA-Notation heute einem Triebfahrzeugführer und in Zukunft dem fahrzeugseitigen ATO-Teilsystem Kontrollaktionen bereit, weshalb sie entsprechend der STPA-Notation in der hierarchischen Regelungsstruktur (Teil Fahrzeug) oberhalb des kognitiven Systemelements platziert ist.

Aus dem Unterkapitel 2.4.3 ist bekannt, dass ein Triebfahrzeugführer im gegenwärtigen Bahnbetrieb für die Durchführung einer sicheren und pünktlichen Zugfahrt unabdingbar ist und dafür die in Unterkapitel 2.4.3 vorgestellten betrieblichen Aufgaben verantwortet.

Aufgrund der inhärenten menschlichen Eigenschaft gibt es bei der Ausführung der betrieblichen Aufgabe keine klare Trennung zwischen den einzelnen Handlungen, wie z.B. Reizaufnahme, Wahrnehmung oder Bedienung. Trotzdem kann – z.B. mit dem Modell der Informationsverarbeitung nach Abbildung 16 – eine kausale Abhängigkeit zwischen den einzelnen Handlungen eines Triebfahrzeugführers entnommen werden.

In Anlehnung an die Anforderung aus dem Kapitel 4.2, dass die für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme modular ausgelegt sein sollen und in Anlehnung an das Modell der

Informationsverarbeitung nach Abbildung 16 wird die logische Beziehung zwischen den Systemelementen zur Durchführung einer vollautomatisierten Zugfahrt im Weiteren modular beschrieben.

Demnach stellen die Sensoren zur Hinderniserkennung (Perception Sensors) und die Ortungssensoren (Vehicle Localization Sensors) als hardwarebasierte Systemelemente in der hierarchischen Regelungsstruktur den zugehörigen softwarebasierten Systemelementen Rohdaten aus dem Umfeld bereit. Da es sich dabei nach der STPA-Notation um Rückkopplungen handelt, befinden sich die Sensoren in der hierarchischen Regelungsstruktur ganz unten.

Da die Rohdaten aus den Sensoren entsprechend des Modells nach Abbildung 16 an das perzeptuelle Systemelement gerichtet sind und die beiden Systemelemente Perception System und Vehicle Localization System entsprechend der Spezifikation aus dem Unterkapitel 2.3.2 eingehende Sensordaten verarbeiten sollen, befinden sich diese beiden Systemelemente nach der STPA-Notation über den Sensoren. Da das Systemelement „Vehicle Localization System“ zusätzlich auf die Daten von „Digital Map“ zugreift, befindet sich das Systemelement „Digital Map“ in der hierarchischen Regelungsstruktur oberhalb von „Vehicle Localization System“.

Entsprechend des Unterkapitels 2.4.3 ist ein Triebfahrzeugführer für eine pünktliche und möglichst energiesparsame Geschwindigkeitsregelung unterhalb der maximal zulässigen ETCS-Geschwindigkeit verantwortlich. Dabei generiert ein Triebfahrzeugführer implizit ein Geschwindigkeitsprofil. Während der Geschwindigkeitsregelung muss eine vorliegende gefahrdrohende Situation durch eine sofortige Reduzierung der aktuellen Geschwindigkeit verhindert werden.

Im Gegensatz dazu wird entsprechend der OCORA Spezifikation in dem Systemelement ATO-Vehicle zunächst ein Geschwindigkeitsprofil erstellt, das dann abgefahren wird. Das Systemelement ATO-Vehicle hat demnach Schnittstellen zur Fahrzeugleittechnik, die es mit Kontrollaktionen versorgt und Schnittstellen zu den beiden Systemelementen Perception System und Vehicle Localization System, von denen es mit Kontrollaktionen versorgt wird.

Zur Reduzierung der Komplexität der funktionalen Systemarchitektur und aus Gründen der Verständlichkeit werden im weiteren Verlauf des Kapitels einige Vereinfachungen vorgenommen. Dazu werden die beiden Systemelemente Perception Sensors und Localization Sensors vereinfacht zu Sensoren zusammengefasst. Die Systemelemente „Perception System“ und „Vehicle Localization System“ werden entsprechend des Modells nach Abbildung 16 zum perzeptuellen Systemelement zusammengefasst. Das Systemelement ATO-Vehicle wird entsprechend des Modells nach Abbildung 16 zum kognitiven Systemelement zusammengefasst. Das Aktor-Systemelement repräsentiert schließlich die Fahrzeugleittechnik. Die in Abbildung 16 dargestellten Systemelemente aus dem Modell der menschlichen Informationsverarbeitung stellen somit Generalisierungen von spezifischen Systemelementen dar. Die spezifischen Systemelemente der generalisierten Systemelemente sind zusammenfassend in der Abbildung 17 dargestellt.

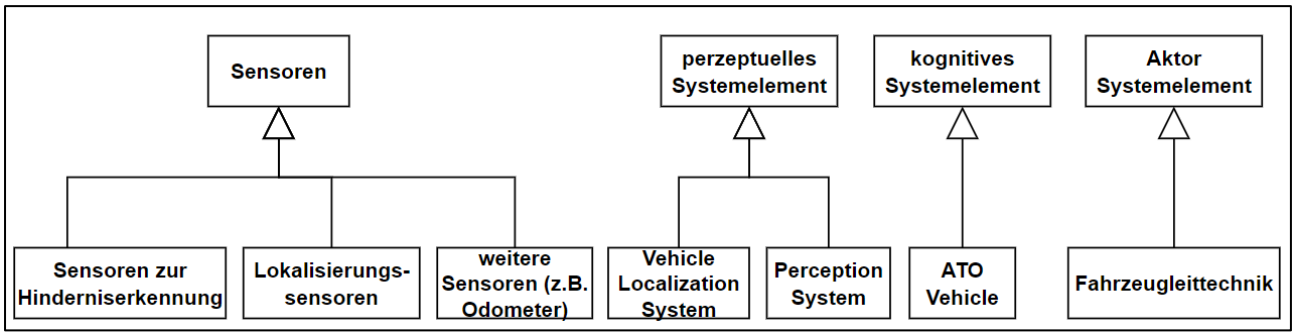

Abbildung 17 generalisierte Systemelemente aus dem Modell der menschlichen Informationsverarbeitung mit ihren spezifischen Systemelementen (eigene Darstellung)

4.5 Herleitung der funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt

Nachdem zuvor die Systemelemente aus OCORA hierarchisch strukturiert und anhand des Modells nach Abbildung 16 kategorisiert wurden, ist das Ziel dieses Kapitels die Herleitung der jeweiligen Kontrollaktionen und Rückkopplungen aus den Systemelementen. Daraus ergibt sich dann die funktionale Systemarchitektur einer vollautomatisierten Zugfahrt in der STPA-Notation. Zur Herleitung der funktionalen Systemarchitektur einer vollautomatisierten Zugfahrt werden in Anlehnung an die Vorgehensweise aus dem Kapitel 4.3 neben den zuvor hierarchisch strukturierten Systemelementen aus OCORA auch die bereits in Kapitel 2.3.2 vorgestellten Systemelemente aus RCA herangezogen. Wie bereits in Kapitel 4.3 erwähnt, sind die Systemelemente in der RCA-Referenzarchitektur hierarchisch strukturiert und können daher als Grundlage für die Herleitung der jeweiligen Kontrollaktionen und Rückkopplungen verwendet werden.

Die fahrzeugseitigen und infrastrukturseitigen Systemelemente aus dem Kapitel 2.3 sind im Weiteren aufgelistet.

Infrastrukturseitige Systemelemente (aus RCA)

- TMS
- ATO Execution (ATO-AE)
- ATO Transactor (ATO-AT)
- Sicherungslogik
- ETCS-Zentrale (RBC)
- Automatic Train Operation Monitoring (ATOM)
- Remote Manual Train Operation (RMTO)
- Future Rail Mobile Communication System (FRMCS).

fahrzeugseitige Systemelemente (aus OCORA)

- Perception Sensors (P-Sensors)
- Vehicle Localization Sensors
- Perception System (PSs)
- Vehicle Localization System
- Digital Map
- Vehicle Supervisor (VS) (ETCS-OBU)
- ATO-Vehicle
- FRMCS Mobile Gateway.

Da die fahrzeugseitigen Systemelemente aus OCORA zuvor in Kapitel 4.4 anhand des Modells der menschlichen Informationsverarbeitung zu generalisierten Systemelemente zusammengefasst wurden, werden im weiteren Verlauf des Hauptkapitels in Anlehnung an die Abbildung 17

- die Perception Sensors und Vehicle Localization Sensors als Sensoren,
- das Perception System als perzeptuelles Systemelement,
- das ATO-Vehicle als kognitives Systemelement und
- die Fahrzeugleittechnik als Aktor-Systemelement

bezeichnet.

Entsprechend der STPA-Notation hat jedes Systemelement (Building Block) ein internes Prozessmodell mit den zugehörigen Algorithmen, aus denen die Kontrollaktionen bzw. Rückkopplungen an den Schnittstellen generiert werden. Die Kontrollaktionen bzw. Rückkopplungen werden im weiteren Verlauf des Kapitels fett formatiert. Nach der STPA-Notation entsteht eine hierarchische Regelungsstruktur dadurch, dass die Systemelemente über Pfeile miteinander verbunden werden. Die nach unten gerichteten Pfeile repräsentieren dabei Kontrollaktionen während die nach oben gerichteten Pfeile Rückkopplungen repräsentieren.

Wie bereits in Unterkapitel 2.3.2 erläutert, werden im TMS der Fahrplan und das aktuelle operative Trassengefüge, das die Grundlage für die Durchführung von Zugfahrten im vollautomatisierten Bahnbetrieb bildet, verwaltet. Das aktuelle **operative Trassengefüge (Tagesfahrplan)** dient daher als Kontrollaktion zur Durchführung von vollautomatisierten Zugfahrten. Diese Kontrollaktion ist als Pfeil an das Systemelement ATO-AE als Input gerichtet. Das Systemelement ATO-AE enthält einen Algorithmus zur Generierung von betrieblichen Daten für die vollautomatisierten Züge. Dieser Algorithmus wird im weiteren Verlauf dieser Arbeit als Journey-Profile Management bezeichnet. Die betrieblichen Daten umfassen entsprechend des Unterkapitels 2.3.2 die Journey-Profiles (Fahrschranken, Haltepositionen, Entfernung zu den Fahrschranken und zu Haltepositionen). Die durch das Journey-Profile Management generierten **Journey-Profiles** repräsentieren im Sinne der STPA-Notation eine Kontrollaktion und werden an das Systemelement ATO-AT übermittelt. Dieses Systemelement verteilt dann die Journey-Profiles zu den entsprechenden Zügen, die eine Kommunikationsverbindung zum Systemelement ATO-AT haben.

Im Gegenzug leitet das Systemelement ATO-AT die von den Zügen erhaltenen Statusdaten als Rückkopplung an das Systemelement ATO-AE, um daraus in Echtzeit die Journey-Profiles (JP) anpassen zu können. Auch die Infrastrukturdaten (**Segment-Profiles**) werden von dem TMS an die beiden Systemelemente ATO-AE und ATO-AT bereitgestellt und von dem Systemelement ATO-AT zusätzlich an die Züge verteilt. Entsprechend der OCORA Spezifikation werden die Infrastrukturdaten an das Systemelement Digital Map übermittelt. Die Infrastrukturdaten stellen daher im Sinne der STPA-Notation ebenfalls eine Kontrollaktion dar.

Bevor eine Fahrterlaubnis von der Sicherungslogik an die ETCS-Zentrale und von dort an die ETCS-OBU übermittelt wird, fragt das TMS zunächst nach einer Fahrterlaubnis bei der Sicherungslogik an *(vgl. Düpmeier 2022)*. Erst wenn die Voraussetzungen für eine sichere Zugfahrt gegeben sind, die durch die Sicherungslogik geprüft werden, wird eine Fahrterlaubnis von der ETCS-Zentrale an die ETCS-OBU übermittelt. Die Fahrterlaubnis stellt im Sinne der STPA-Notation eine Kontrollaktion dar, die von der Sicherungslogik an die ETCS-Zentrale und von dort an die ETCS-OBU gerichtet ist.

Fahrzeugseitig kann dann auf Basis der empfangenen Journey-Profiles und Segment-Profiles in dem kognitiven Systemelement das abzufahrende Geschwindigkeitsprofil generiert werden. Demnach umfasst das kognitive Systemelement einen Algorithmus zur Generierung von Geschwindigkeitsprofilen und einen Algorithmus zur Regelung der Geschwindigkeit entsprechend des Geschwindigkeitsprofils. Damit das kognitive Systemelement das Geschwindigkeitsprofil erstellen kann, sind neben den Journey-Profiles und Segment-Profiles auch **Zugdaten** sowie das **ETCS-Geschwindigkeitsprofil** erforderlich. Diese werden von der ETCS-OBU als Kontrollaktion bereitgestellt.

Für eine sichere Geschwindigkeitsregelung werden im perzeptuellen Systemelement zudem verschiedene Sensordaten von Perception Sensors und Localization Sensors fusioniert und daraus die **aktuelle Position des Zuges** und **erkannte und klassifizierte Objekte** (Gefährdungssituation im Lichtraum) sowie die Angabe über den aktuellen **Zustand der Fahrzeugkomponenten** einschließlich der **Zugintegrität** an das kognitive Systemelement bereitgestellt. Bei der Erkennung von Objekten im Lichtraum werden den erkannten Objekten im aktuellen Zeitpunkt und am aktuellen Ort eine Bedeutung zugeordnet. Die Objektklassifizierung erfolgt dann durch Korrelation der erkannten Objekte mit ihren physikalischen Merkmalen (z.B. Position, Größe, Geschwindigkeit oder Beschleunigung). Um eine Objektklassifizierung zu ermöglichen, können die Objekte anhand ihrer physikalischen Merkmale z.B. formal abgebildet werden. Die Ausgänge des perzeptuellen Systemelements stellen im Sinne der STPA-Notation Kontrollaktionen dar, die als Pfeil an das kognitive Systemelement gerichtet sind.

Mit den Kontrollaktionen von dem perzeptuellen Systemelement und dem ATO-AT (Journey-Profiles) steuert dann das kognitive Systemelement anhand des erstellten Geschwindigkeitsprofils das darunterliegende Aktor-Systemelement (Fahrzeugleittechnik). Dazu werden **Steuerbefehle** als Kontrollaktion **an die Fahrzeugleittechnik** übermittelt. Daneben können auch Steuerbefehle für die Steuerung von Fahrzeugkomponenten an die Fahrzeugleittechnik übermittelt werden, die ebenfalls Kontrollaktionen darstellen.

Für die Abfahrt des Zuges wird die von der ETCS-Zentrale empfangene **Fahrterlaubnis** von der ETCS-OBU als Kontrollaktion an das kognitive Systemelement bereitgestellt. Bei Nichteinhaltung der Kontrollaktion von der ETCS-OBU kann diese auch bremsend in die Fahrzeugleittechnik eingreifen. Daher ist auch eine Kontrollaktion **bremsen** von der ETCS-OBU zum Aktor-Systemelement gerichtet.

Bisher wurden die Kontrollaktionen für die Beschreibung einer vollautomatisierten Zugfahrt hergeleitet. Die Rückkopplungen werden, wie bereits oben erläutert, durch Pfeile, die nach oben gerichtet sind, repräsentiert.

Rückkopplungen kommen von den Sensoren. Diese erfassen Zustandsgrößen aus unterschiedlichen Quellen (z.B. aus dem Fahrzeugumfeld) und übermitteln diese als Rückkopplungen an die zugehörigen Systemelemente. Während die Sensoren zur Hinderniserkennung Rohdaten über das Fahrzeugumfeld (**Objekte im Lichtraumprofil**) rückkoppeln, werden von den Ortungssensoren Rohdaten bezüglich der **aktuellen Position des Zuges** an das perzeptuelle Systemelement rückgekoppelt.

Aber auch von der Fahrzeugleittechnik erfassen die angeschlossenen Sensoren aktuelle Zustandsgrößen, wie z.B. **fahrdynamische Zustandsgrößen** oder **Zustandsgrößen aus den Fahrzeugkomponenten** (z.B. Zugintegrität oder Türstatus) und übermitteln diese als Rückkopplungen sowohl an das perzeptuelle Systemelement als auch an ETCS-OBU.

Für eine Betriebsüberwachung in Echtzeit durch das TMS und das Systemelement ATOM übermittelt das kognitive Systemelement die **aktuelle Position des Zuges** und die Angabe darüber, ob das erstellte Geschwindigkeitsprofil Abweichungen aufweist, d.h. die Journey-Profiles eingehalten werden oder

nicht, als Rückkopplung an die Systemelemente ATO-AE und ATOM. In dem Systemelement ATO-AE erfolgt dann – wie zuvor erläutert – die dynamische Anpassung der Journey-Profiles. Für Konflikterkennung- und Lösung werden die **aktuelle Position des Zuges und der Zustand der Journey-Profiles** von dem Systemelement ATO-AE auch an das TMS übermittelt**.**

Bei Bedarf kann dann entsprechend der OCORA Spezifikation das Systemelement ATOM über das Systemelement RMTO eine **Fernsteuerung** des Zuges **aktivieren**. Die Aktivierung der Fernsteuerung stellt im Sinne der STPA-Notation eine Kontrollaktion dar und ist an das Systemelement RMTO gerichtet. Daraufhin werden dann von dem Systemelement RMTO Kontrollaktionen zur Geschwindigkeitsregelung direkt an die Fahrzeugleittechnik übermittelt. Auch die ETCS-OBU übermittelt die aktuelle Position des Zuges an die ETCS-Zentrale, um daraus dann eine neue Fahrterlaubnis erstellen zu können.

Aufgrund der zentralen Betriebsführung im Schienenverkehr werden sowohl Kontrollaktionen als auch Rückkopplungen zwischen den fahrzeugseitigen und den infrastrukturseitigen Systemelementen über eine funkbasierte Kommunikationsschnittstelle übermittelt. Deshalb befindet sich das Systemelement FRMCS als Kommunikationssystem in der hierarchischen Regelungsstruktur zwischen den infrastrukturseitigen und den fahrzeugseitigen Systemelementen und ermöglicht dadurch eine netzwerkbasierte Regelung von vollautomatisierten Zugfahrten.

Die Systemelemente einschließlich ihrer Kontrollaktionen bzw. Rückkopplungen werden in der Tabelle 2 zusammengefasst. Die Tabelle enthält in der ersten Spalte die Systemelemente. In der zweiten Spalte der Tabelle wird der Schnittstellentyp dargestellt. Hierbei kann es sich um die oben genannten Kontrollaktionen oder um Rückkopplungen handeln. In der dritten Spalte sind dann die konkreten Kontrollaktionen bzw. Rückkopplungen aufgetragen. In der vierten Spalte wird schließlich auch die Senke beschrieben, zu der das jeweilige Systemelement eine Schnittstelle aufweist.

Tabelle 2: Kontrollaktionen und Rückkopplungen in der hierarchischen Regelungsstruktur einer vollautomatisierten Zugfahrt

System-elemente	**Schnittstellen-typ**	**Kontrollaktionen/Rückkopplungen**	**Senke**
TMS	Kontrollaktion	Tagesfahrplan	ATO-AE
		Segment-Profile	ATO-AE und ATO-AT
		Anfrage Fahrterlaubnis (Movement Permission)	Sicherungslogik
ATO-AE	Kontrollaktion	Journey Profile	ATO-AT
ATO-AT	Kontrollaktion	Segment-Profile	Digital Map
	Kontrollaktion	Journey Profile	kognitives Systemelement
ATOM	Kontrollaktion	Aktivierung der RMTO	RMTO
RMTO	Kontrollaktion	Steuerbefehle für die Geschwindigkeitsregelung	Fahrzeugleittechnik

Digital Map	Kontrollaktion	Segment-Profile	kognitives Systemelement
Perzeptuelles Systemelement	Kontrollaktion	aktuelle Position des Zuges	kognitives Systemelement
		erkannte und klassifizierte Objekte	
		Zustandsgrößen aus den Fahrzeugkomponenten, fahrdynamische Zustandsgrößen einschließlich der Zugintegrität	
ETCS-OBU	Kontrollaktion	Zugdaten	kognitives Systemelement
		ETCS-Geschwindigkeitsprofil	
kognitives Systemelement	Kontrollaktion	Steuerbefehle für die Geschwindigkeitsregelung	Aktor Systemelement (Fahrzeugleittechnik)
		Steuerbefehle für die Fahrzeugkomponenten	
ETCS-OBU	Kontrollaktion	Steuerbefehl (Bremsung)	Aktor Systemelement (Fahrzeugleittechnik)
Sicherungslogik	Kontrollaktion	Fahrterlaubnis (MA)	ETCS-Zentrale
ETCS-Zentrale	Kontrollaktion	Fahrterlaubnis (MA)	ETCS-OBU
		Zugdaten	
Sensoren	Rückkopplung	fahrdynamische Zustandsgrößen, Objekte im Lichtraumprofil und aktuelle Position des Zuges	Perzeptuelles Systemelement
		Zustandsgrößen aus den Fahrzeugkomponenten und fahrdynamische Zustandsgrößen einschließlich der Zugintegrität	ETCS-OBU
kognitives Systemelement	Rückkopplung	Zustand der Journey-Profiles	ATO-AE /ATOM
		aktuelle Position des Zuges	
ATO-AE	Rückkopplung	Zustand der Journey-Profiles	TMS
		aktuelle Position des Zuges	
ETCS-OBU	Rückkopplung	aktuelle Position des Zuges	ETCS-Zentrale

Die Abbildung 18 auf Seite 73 stellt die funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt in Form einer hierarchischen Regelungsstruktur (STPA-Notation) dar. Die Anwendung der STPA-Notation führte dazu, dass aus der Interaktion der einzelnen Systemelemente in der hierarchischen Regelungsstruktur insgesamt vier Regelkreise entstanden sind.

Der erste Regelkreis ist der sogenannte **ATO-Regelkreis**. In dem ATO-Regelkreis sind TMS, ATO-AE, ATO-AT, das Kommunikationssystem, das perzeptuelle Systemelement, das kognitive Systemelement,

das Aktor-Systemelement, die Sensoren, das Systemelement ATOM und das Systemelement RMTO enthalten.

Der zweite Regelkreis ist die Untersetzung des ersten Regelkreises und stellt den **fahrzeugseitigen ATO-Regelkreis** dar. Darin sind das perzeptuelle Systemelement, das kognitive Systemelement, das Aktor-Systemelement und die Sensoren enthalten.

Der dritte Regelkreis ist der **ETCS-Regelkreis**. Darin sind neben der Sicherungslogik, die ETCS-Zentrale, die ETCS-OBU, das Kommunikationssystem, Aktor-Systemelement und die Sensoren enthalten.

Im vierten Regelkreis, dem **fahrzeugseitigen ETCS-Regelkreis** sind neben der ETCS-OBU das Aktor-Systemelement und die Sensoren enthalten.

Die hierarchische Regelungsstruktur aus Abbildung 18 dient als Grundlage für die Durchführung einer Gefährdungsanalyse im nächsten Hauptkapitel.

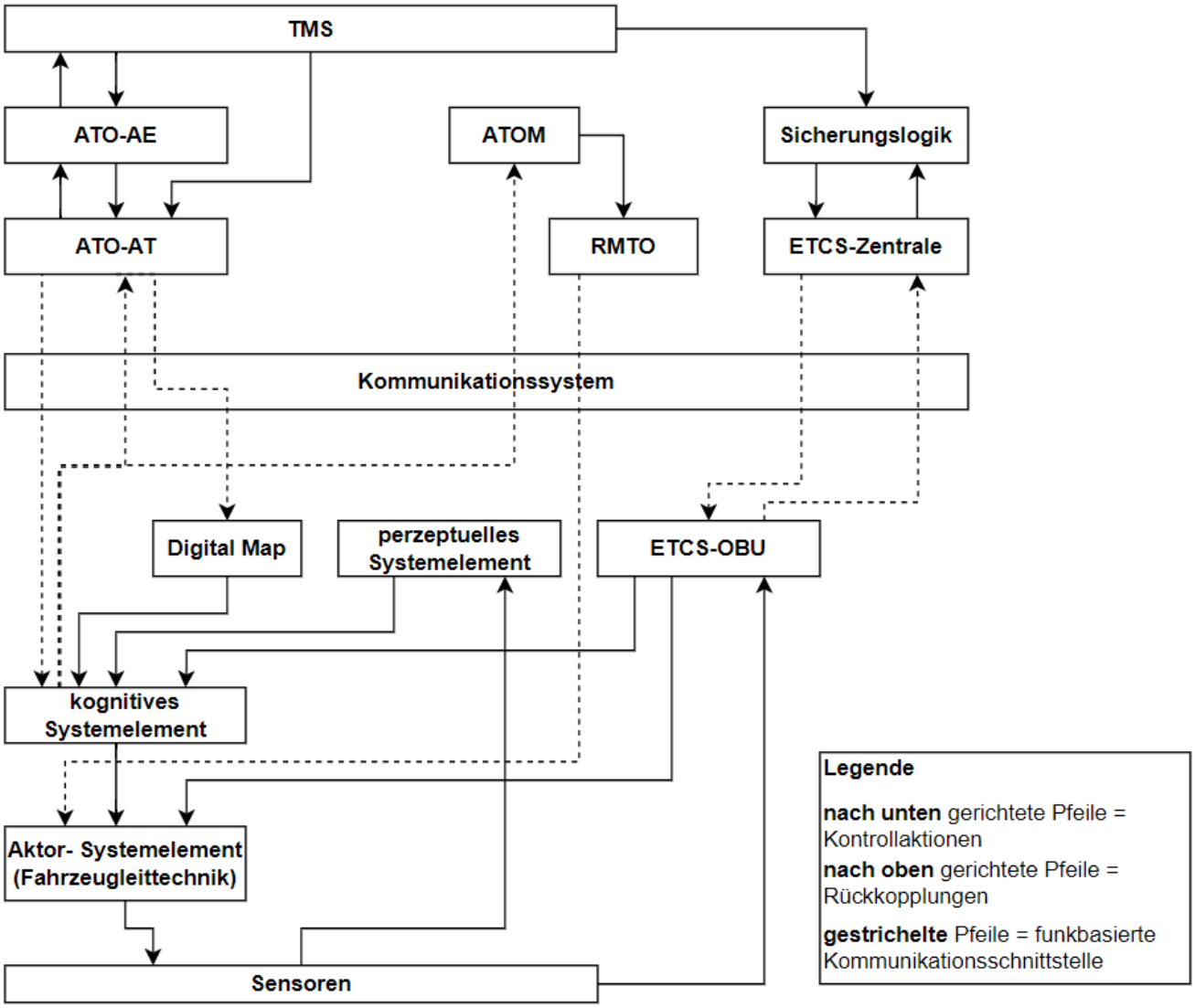

Abbildung 18 funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt in Form einer hierarchischen Regelungsstruktur (STPA-Notation)

4.6 Zusammenfassung des Hauptkapitels

Im vorliegenden Hauptkapitel wurde die funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt in Form einer hierarchischen Regelungsstruktur hergleitet.

Als Grundlage dafür wurden die in den Forschungsinitiativen RCA und OCORA (vgl. Kapitel 2.3) bereits spezifizierten Systemelemente verwendet.

In einem ersten Schritt erfolgte zunächst die hierarchische Strukturierung der Systemelemente aus OCORA. Mit der hierarchischen Strukturierung konnten die fahrzeugseitigen Systemelemente entsprechend ihrer Hierarchie für eine vollautomatisierte Zugfahrt in eine logische Beziehung zueinander gesetzt werden.

Im zweiten Schritt wurde dann auf Basis der hierarchischen Strukturierung die funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt in Form einer hierarchischen Regelungsstruktur hergeleitet.

Die Anwendung der STPA-Notation führte dazu, dass aus der Interaktion der einzelnen Systemelemente in der hierarchischen Regelungsstruktur insgesamt vier Regelkreise entstanden sind.

Auf Basis der in diesem Hauptkapitel hergeleiteten funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt in Form einer hierarchischen Regelungsstruktur können nun entsprechend der STPA-Methode Gefährdungsursachen aus den Regelkreisen systematisch erarbeitet werden. Die Durchführung einer Gefährdungsanalyse ist Gegenstand des nächsten Hauptkapitels.

5 Herleitung des potenziellen Gefährdungsraums im vollautomatisierten Bahnbetrieb

5.1 Ziel des Kapitels

Im vorigen Hauptkapitel wurde die funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt in Form einer hierarchischen Regelungsstruktur hergleitet.

Mit einem ATO-System wird ein neues technisches System in das bestehende Bahnsystem eingeführt, welches, wie bereits in Hauptkapitel 4 gezeigt, im vollautomatisierten Bahnbetrieb u.a. menschliche Aufgaben verantworten wird. Dadurch ergeben sich technische und betriebliche Änderungen im Bahnsystem. Damit ändern sich auch die Störungssituationen und die damit verbundenen Gefährdungen.

Bevor betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb entwickelt werden können, muss zunächst der Gefährdungsraum im vollautomatisierten Bahnbetrieb bekannt sein.

Das Ziel dieses Kapitels ist daher die Herleitung des Gefährdungsraums im vollautomatisierten Bahnbetrieb. Dabei bildet die in Kapitel 4.5 hergeleitete funktionale Systemarchitektur einer vollautomatisierten Zugfahrt eine wesentliche Grundlage für die Gefährdungsanalyse. Entsprechend der inhaltlichen Eingrenzung in Kapitel 3.5 liegt der Fokus bei der Gefährdungsanalyse auf den beiden ATO-Regelkreisen aus dem vorigen Hauptkapitel.

Die Inhalte dieses Hauptkapitels können entsprechend der STPA-Methode der Gefährdungsanalyse zugeordnet werden.

5.2 Anforderungen an die Gefährdungsanalyse zur Herleitung des Gefährdungsraums im vollautomatisierten Bahnbetrieb

Die in Hauptkapitel 3 zusammengestellten Anforderungen beziehen sich auf die Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb. Die in diesem Hauptkapitel durchzuführende Gefährdungsanalyse ist lediglich eine notwendige Vorarbeit für die Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb, weshalb in Hauptkapitel 3 keine Anforderungen an die Gefährdungsanalyse zusammengestellt wurden.

Es können dennoch spezifische Anforderungen an die Gefährdungsanalyse aus der Norm DIN EN 50126 entnommen werden. Diese sind wie folgt:

- Die wichtigste spezifische Anforderung ist die **Sicherstellung der Vollständigkeit** bei der Herleitung des Gefährdungsraums.
- Mit der ersten Anforderung verbunden wird in der Norm auch angemerkt, dass es nicht das Ziel ist, „*jede banale Gefährdung zu katalogisieren, auch nicht wird erwartet, dass immer alle Gefährdungen jenseits der Grenzen der aktuellen Kenntnisse zu identifizieren“ (DIN EN 50126-2:2017, S. 12)*.
- Eine angemessene und ausreichende Gefährdungsanalyse **sollte eine begründete Analyse der Gefährdungen** auf der Ebene des betrachteten Systems und der damit verbundenen Gefährdungen auf der Ebene des Bahnsystems wiedergeben.
- Um eine vertrauenswürdige Grundlage für die Risikobewertung zu schaffen, **sollte** die Gefährdungsanalyse schließlich auch **objektiv** gestaltet sein.

5.3 Vorgehensweise bei der Gefährdungsanalyse

Die Durchführung der Gefährdungsanalyse erfolgt entsprechend der STPA-Methode anhand der STPA-Notation. Die Abbildung 19 stellt den Ausschnitt aus der STPA-Methode dar, der für dieses Hauptkapitel relevant ist.

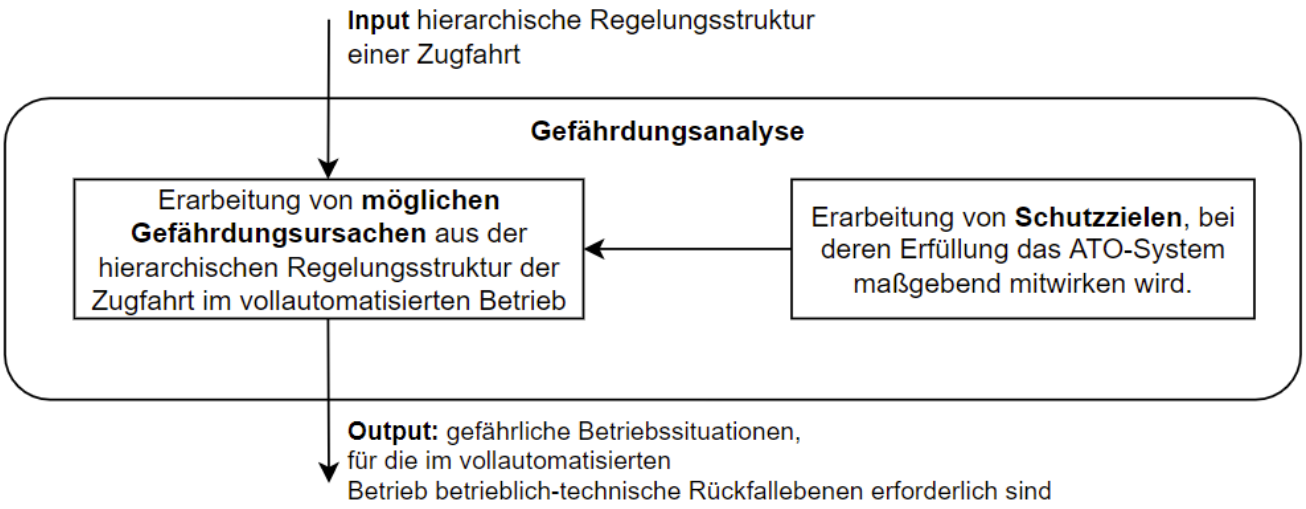

Abbildung 19 Ausschnitt aus der globalen Methode aus Kapitel 3.3 zur Durchführung einer Gefährdungsanalyse

Von den insgesamt vier Schritten innerhalb der STPA-Methode sind die Schritte drei und vier in diesem Hauptkapitel relevant.

Entsprechend der Norm EN 50126 können Gefährdungen auf unterschiedlichen Ebenen eines Systems entstehen. Bereits in Kapitel 2.4 wurde erläutert, dass betrieblich-technische Rückfallebenen im gegenwärtigen Betrieb dann erforderlich sind, wenn die Schutzziele der LST verletzt werden. Die Verletzung der Schutzziele der LST stellen somit Gefährdungen auf der Bahnsystemebene dar, die auch im Rahmen der Gefährdungsanalyse in diesem Hauptkapitel zugrunde gelegt werden. Zunächst (im dritten Schritt der STPA-Methode) werden daher die Schutzziele erarbeitet, bei deren Erfüllung das ATO-System im vollautomatisierten Bahnbetrieb maßgebend mitwirken wird. Die Erarbeitung der ATO relevanten Schutzziele im vollautomatisierten Bahnbetrieb erfolgt in Kapitel 5.4.

Prinzipiell kann die Annahme getroffen werden, dass jede Gefährdung auf der Ebene des betrachteten Systems die Schutzziele der LST verletzt (Gefährdung auf der Bahnsystemebene) und immer zu einem unerwünschten Ereignis führt. Dieser Umstand entspricht nach der Norm EN 50126 dem „ungünstigsten Szenario“ (vgl. *DIN EN 50126-2:2017, S. 33)*. Da nicht jede Gefährdung auf der Bahnsystemebene immer zu einem unerwünschten Ereignis führt, ist ein betrieblicher und umgebungsbedingter Kontext – wie er in der Norm EN 50126 beschrieben wird – erforderlich. Auch gemäß der STPA-Methode ist der Kontext, indem eine Gefährdungsursache entsteht, relevant. Denn beispielsweise stellt die Nichtverfügbarkeit der Sensoren zur Hinderniserkennung beim Stillstand eines Zuges am Bahnsteig zunächst keine Gefährdung dar, während bei einer Fahrt (z.B. auf einem Bahnübergang) die Nichtverfügbarkeit der Sensoren zur Hinderniserkennung eine Gefährdung auf der Bahnsystemebene darstellen würde. Die Herleitung eines betrieblichen und umgebungsbedingten Kontextes für die Gefährdungsanalyse erfolgt in Kapitel 5.5.

Die Anwendung der STPA-Notation im vorigen Hauptkapitel führte dazu, dass aus der Interaktion der einzelnen Systemelemente in der hierarchischen Regelungsstruktur insgesamt vier Regelkreise entstanden sind. Diese entstandenen Regelkreise bzw. Regelungspfade bilden die Grundlage für die

Erarbeitung von möglichen Gefährdungsursachen aus der Interaktion der einzelnen Systemelemente. Auf Basis der hierarchischen Regelungsstruktur aus dem Hauptkapitel 4 werden in Kapitel 5.6 die möglichen Gefährdungsursachen aus den darin vorkommenden Systemelementen erarbeitet, die in einem betrieblichen- und umgebungsbedingten Kontext zu gefährlichen Betriebssituationen führen können.

Die hierarchische Regelungsstruktur aus dem Hauptkapitel 4 enthält vier Regelkreise (vgl. Kapitel 4.5). Da für die beiden ETCS-Regelkreise bereits bei der Entwicklung des ETCS-Systems oder in anderen Forschungsarbeiten *(vgl. Düpmeier 2022)* eine Gefährdungsanalyse durchgeführt wurde, wird keine erneute Gefährdungsanalyse für die beiden ETCS-Regelkreise durchgeführt. Der Fokus bei der Gefährdungsanalyse liegt – wie zu Beginn dieses Hauptkapitels erwähnt – auf den beiden ATO-Regelkreisen. In Kapitel 5.7 ist die Zusammenfassung des 5. Hauptkapitels zu finden.

5.4 Erarbeitung von ATO relevanten Schutzzielen in Abwesenheit eines Triebfahrzeugführers

Entsprechend der inhaltlichen Eingrenzung in Kapitel 3.5 steht die Erarbeitung von Gefährdungen während einer vollautomatisierten Zugfahrt im Vordergrund dieses Hauptkapitels. Wie bereits zu Beginn dieses Hauptkapitels erwähnt, wird mit einem ATO-System ein neues technisches System in das bestehende Bahnsystem eingeführt, welches, wie bereits in Hauptkapitel 4 gezeigt, im vollautomatisierten Bahnbetrieb u.a. menschliche Aufgaben verantworten wird. Ziel dieses Kapitels ist es, die Schutzziele der LST zu erarbeiten, bei deren Erfüllung das ATO-System im vollautomatisierten Bahnbetrieb maßgebend mitwirkt.

Aus dem Kapitel 2.4 ist bekannt, dass Rückfallebenen im gegenwärtigen Betrieb dann erforderlich sind, wenn die Schutzziele der LST zu denen die Kollisionsvermeidung und Entgleisungsschutz gehören, nicht mehr erfüllt werden können. Die Kollision mit systeminternen Fahrzeugen kann auf verschiedene Weise entstehen, deshalb wird die Kollisionsvermeidung nach *Düpmeier (2022)* auch in Folgefahrschutz, Gegenfahrschutz und Flankenschutz unterteilt. Neben der Kollision mit systeminternen Fahrzeugen gibt es auch die Einteilung nach Kollision mit systemexternen Fahrzeugen und mit der übrigen Umwelt.

In *Düpmeier (2022)* wurde bereits eine ausgiebige Gefährdungsanalyse für die Sicherungslogik durchgeführt, bei der ein Gefährdungskatalog mit verschiedenen Gefährdungsgruppen entstanden ist.

Prinzipiell ist es möglich, die Gefährdungsursachen aus den beiden ATO-Regelkreisen hinsichtlich aller Gefährdungsgruppen nach *ebd.* zu erarbeiten. Mit der RCA-Referenzarchitektur und der zentralen Betriebsführung im Bahnbetrieb gibt es jedoch schon eine klare Zuordnung der Erfüllung der obigen Schutzziele zu technischen Systemen. So ist es beispielsweise die Aufgabe der Sicherungslogik, u.a. eine Kollision mit systeminternen Fahrzeugen zu vermeiden. Außerdem ist entsprechend des Unterkapitels 2.4.3 ein Triebfahrzeugführer auch nicht zur Erfüllung aller oben genannten Schutzziele verantwortlich. Die Erarbeitung von Gefährdungsursachen aus den beiden ATO-Regelkreisen hinsichtlich aller Gefährdungsgruppen nach *ebd.* erscheint daher weniger geeignet.

Stattdessen sind nur jene Schutzziele relevant, die alleine durch die Sicherungslogik und durch das ETCS-System nicht gewährleistet werden können sowie deren Gefährdungsursachen primär fahrzeugseitig entstehen.

Wenngleich die Entgleisung und die Kollision mit systeminternen Fahrzeugen durch die Sicherungslogik und durch das ETCS-System vermieden werden, kann eine Kollision mit systemfremden Fahrzeugen oder der übrigen Umwelt alleine durch Sicherungslogik und durch das ETCS-System nicht vollständig

vermieden werden, da dazu während einer Zugfahrt eine kontinuierliche Lichtraumüberwachung erforderlich ist. Beispielsweise kann eine Kollision mit Tieren, Personen oder anderen Objekten am Gleis nicht durch die Sicherungslogik oder durch das ETCS-System vermieden werden.

Prinzipiell ordnet *Trinckauf (2013)* die Lichtraumüberwachung nicht zu den Kernaufgaben der Sicherungstechnik (Anforderungen zweiter Ordnung). Jedoch ist aus dem Kapitel 2.4 bereits bekannt, dass die Lichtraumüberwachung zu den wesentlichen betrieblichen Aufgaben eines Triebfahrzeugführers gehört, weshalb dafür auch in anderen Forschungsinitiativen Sensortechnologien erprobt werden (z.B. Sensors4Rail). Ein Verzicht auf die Lichtraumüberwachung im vollautomatisierten Bahnbetrieb ist daher nicht akzeptabel. Denn in Abwesenheit eines Triebfahrzeugführers muss die Gesamtsicherheit des vollautomatisierten Bahnbetriebs mindestens die gleiche Sicherheit wie das aktuelle Bahnsystem mit einem Triebfahrzeugführer haben *(vgl. DIN EN 50126-1:2017*).

Entsprechend der funktionalen Systemarchitektur aus dem Hauptkapitel 4 nehmen die Sensoren gemeinsam mit dem perzeptuellen Systemelement in Abwesenheit eines Triebfahrzeugführers eine wesentliche Rolle bei der Lichtraumüberwachung ein. Des Weiteren erfolgt die Geschwindigkeitsregelung in Abwesenheit eines Triebfahrzeugführers durch das kognitive Systemelement auf dem Triebfahrzeug. Wenngleich eine Geschwindigkeitsüberwachung durch die ETCS-OBU erfolgt, kann es unterhalb der maximal zulässigen Geschwindigkeit dazu kommen, dass der vollautomatisierte Zug den Zielpunkt verfehlt, sofern eine Reibwertänderung (Reibwertabweichung zwischen dem von ETCS-Zentrale übermittelten und dem tatsächlich vorliegenden Wert) vorliegt. Eine Reibwertänderung kann durch die Sicherungslogik nicht überwacht werden.

Da die Sensoren, das perzeptuelle Systemelement und das kognitive Systemelement im fahrzeugseitigen ATO-Regelkreis integriert sind, wirkt das ATO-System dementsprechend während einer vollautomatisierten Zugfahrt bei der **Kollisionsvermeidung** mit.

Wie bereits oben erwähnt, erfolgt die Entgleisungsvermeidung prinzipiell durch die Sicherungslogik. Es kann jedoch auch an stetigen Stellen entlang des Fahrwegs zu einer Entgleisung kommen, wenn die Geschwindigkeit des Zuges im Vergleich zur zulässigen Streckengeschwindigkeit aufgrund von fahrdynamischen Umgebungseinflüssen (z.B. Seitenwind) überhöht ist. Als reales Beispiel für eine Entgleisung in einem Gleisbogen kann der Unfall von Santiago de Compostela aus dem Jahr 2013 aufgeführt werden. Durch die Entgleisung waren nicht nur Menschen (Zuginsassen) verunglückt, sondern auch die Infrastruktur und das Fahrzeug wurden beschädigt. Wenngleich die Entstehung von Umgebungseinflüssen nicht durch die Gestaltung der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systemen beeinflusst werden kann, ist es entsprechend der funktionalen Systemarchitektur aus dem Hauptkapitel 4 die Aufgabe des kognitiven Systemelements, die Geschwindigkeitsregelung in Abwesenheit eines Triebfahrzeugführers zu übernehmen. Um das Schadensausmaß durch Gefährdungen aufgrund von Umgebungseinflüssen nicht zu erhöhen, wirkt das ATO-System daher auch bei der **Entgleisungsvermeidung aufgrund von Umgebungseinflüssen** mit.

Zu den beiden Gefährdungen auf der Bahnsystemebene Kollision und Entgleisung kann es aufgrund der kinetischen Energie während einer vollautomatisierten Zugfahrt kommen.

Da während einer vollautomatisierten Zugfahrt entsprechend der Definition für GoA4 aus dem Unterkapitel 2.1.1 die direkte menschliche Interaktion zwischen den Zuginsassen und dem Zugpersonal fehlt, können auch Gefährdungen entstehen, wenn ein vollautomatisierter Zug nicht weiterfährt und die Kommunikation zum Zugpersonal fehlt. Denn der Stillstand eines Zuges führt nicht nur zur Abweichung von der im Regelbetrieb festgelegten Betriebsqualität, sondern kann auch in Abhängigkeit des Ortes, an dem ein Zug steht, Gefährdungen verursachen. Beispielsweise ist der Stillstand eines Zuges auf einer

Weiche, im Tunnel oder auf einem Bahnübergang nicht sicher. Außerdem kann der Stillstand eines unbegleiteten Zuges aufgrund fehlender menschlicher Interaktion psychische Belastungen bei den Reisenden (Zuginsassen) auslösen. Beispielsweise empfinden einige Menschen in geschlossenen und engen Räumen eine unverhältnismäßig große Angst (Klaustrophobie). Eine ähnliche Situation liegt vor, wenn ein Zug auf einer Brücke zum Stehen kommt. Auf einer Brücke kann eine Klaustrophobie bei Reisenden zusätzlich durch eine Höhenangst (Akrophobie) begleitet werden. Ferner können Fahrgäste unter physischen Belastungen leiden, wenn hinreichend gute klimatische Bedingungen (z.B. durch unzureichende Belüftung) nicht gewährleistet werden können.

Aus diesem Grund ist es auch relevant, neben den beiden Gefährdungen auf der Bahnsystemebene Kollision und Entgleisung, herauszufinden, durch welche Ursachen aus den beiden ATO-Regelkreisen die Weiterfahrt eines Zuges verhindert werden kann. Da die Weiterfahrt eines vollautomatisierten Zuges durch den im fahrzeugseitigen Regelkreis vorhandenen Systemelementen erfolgt, wirkt das ATO-System auch bei der **Vermeidung von Gefährdungen von Zuginsassen** mit.

Als Fazit dieses Kapitels lässt sich festhalten, dass das ATO-System im vollautomatisierten Bahnbetrieb in Abwesenheit eines Triebfahrzeugführers an der Vermeidung einer Kollision und Entgleisung während einer Zugfahrt und an der Vermeidung von Gefährdungen von Zuginsassen aufgrund eines unerwünschten Stillstands maßgebend beteiligt ist. Die Abbildung 20 fasst grafisch zusammen, bei welchen Schutzzielen das ATO-System im vollautomatisierten Bahnbetrieb für deren Erfüllung maßgebend mitwirkt.

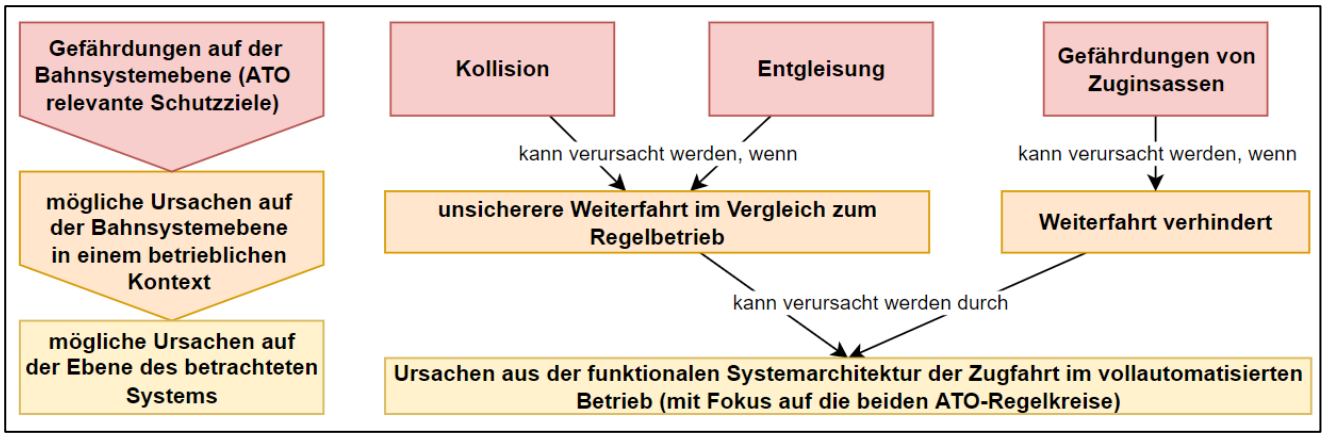

Abbildung 20 Schutzziele, bei deren Erfüllung das ATO-System im vollautomatisierten Bahnbetrieb maßgebend mitwirkt

5.5 Betrieblicher und umgebungsbedingter Kontext für Gefährdungen im vollautomatisierten Bahnbetrieb

Um einschätzen zu können, welche Ursachen aus den beiden ATO-Regelkreisen die zuvor erarbeiteten ATO relevanten Schutzziele während einer vollautomatisierten Zugfahrt verletzen können und in welchem betrieblichen und umgebungsbedingten Kontext tatsächlich eine Gefährdung (gefährliche Betriebssituation) vorliegt, wird in diesem Kapitel ein betrieblicher und umgebungsbedingter Kontext hergeleitet.

Aufgrund der Komplexität und der Vielzahl von möglichen Betriebsszenarien kann ein vollständiger betrieblicher und umgebungsbedingter Kontext in begrenzter Zeit im Rahmen dieser Arbeit nicht

hergeleitet werden, zumal für eine objektive Abschätzung der Auswirkungen der Gefährdungen gemäß der Norm EN 50126 verschiedene Domain-Experten einzubinden sind.

Um entsprechend den Anforderungen aus dem Kapitel 5.2 dennoch möglichst objektiv begründen zu können, inwiefern die Gefährdungsursachen aus den beiden ATO-Regelkreisen eine gefährliche Betriebssituation darstellen und um nicht jede banale Gefährdungsursache zu berücksichtigen, wird im Weiteren ein minimaler Betrachtungsraum für den relevanten betrieblichen und umgebungsbedingten Kontext erarbeitet.

Aus dem Unterkapitel 3.3.2 ist bekannt, dass die STPA-Methode mit der hierarchischen Regelungsstruktur bei der Erarbeitung von Gefährdungsursachen ein Endkriterium aufweist. Durch die endlichen Gefährdungsursachen aus der hierarchischen Regelungsstruktur und dem minimalen Betrachtungsraum für den relevanten betrieblichen und umgebungsbedingten Kontext kann die Anforderung hinsichtlich der Sicherstellung der Vollständigkeit erfüllt werden.

Wenngleich der betriebliche und umgebungsbedingte Kontext bei einer Gefährdungsanalyse in der Norm EN 50126 hervorgehoben wird, gibt es darin keine Systematik, anhand derer ein betrieblicher und umgebungsbedingter Kontext definiert werden kann. Gemäß der Norm EN 50126 *„legt der betriebliche und umgebungsbedingte Kontext fest, wo und wann eine Gefährdung auf der Ebene des Bahnsystems sich zu einem Unfall entwickeln kann“* (*DIN EN 50126-2:2017, S. 23*). Die genauen Bestandteile eines betrieblichen und umgebungsbedingten Kontexts sind in der Norm EN 50126 jedoch nicht vorgegeben. Die Einschätzung, ob eine Gefährdungsursache tatsächlich eine gefährliche Betriebssituation erzeugt, erfolgt vielmehr im Ermessen der in die Gefährdungsanalyse eingebundenen Experten.

Prinzipiell könnten die Gefährdungsursachen aus den beiden ATO-Regelkreisen ebenfalls durch Experten hinsichtlich der gefährlichen Betriebssituation engeschätzt werden. Dadurch kann es jedoch aufgrund von unterschiedlichem Wissensstand und subjektiven Erfahrungen der Experten zu Doppeldeutigkeiten und zum Meinungsunterschied kommen. Um Doppeldeutigkeiten und Meinungsunterschiede zu vermeiden und dadurch eine objektive Einschätzung der Gefährdungsursachen zu erreichen, bietet es sich an, stattdessen eine einheitliche Taxonomie für den betrieblichen und umgebungsbedingten Kontext im vollautomatisierten Bahnbetrieb herzuleiten.

Da auch im autonomen Straßenverkehr sicherheitskritische Betriebssituationen entstehen können, hat das britische Institut für Standardisierung (engl., The British Standards Institution, bsi) eine Taxonomie für die Definition von Betriebsszenarien im autonomen Straßenverkehr entwickelt *(PAS 1883:2020)*. Außerdem werden nach der STPA-Notation zur Entwicklung eines Kontextes Schlüsselwörter, wie *„when“, „while“* oder *„during“* vorgegeben *(Leveson und Thomas 2018, S. 37)*. Die Taxonomie nach *PAS 1883:2020* und die Schlüsselwörter nach der STPA-Methode eignen sich als Grundlage, um im Weiteren den betrieblichen und umgebungsbedingten Kontext für Gefährdungen im vollautomatisierten Bahnbetrieb herzuleiten.

Die Taxonomie nach *PAS 1883:2020* umfasst zur Beschreibung eines betrieblichen und umgebungsbedingten Kontextes neben den **festen Bestandteilen einer Straßeninfrastruktur** (z.B. Kreuzung, Fahrspur oder Straßenschilder), die in einem bestimmten Betrachtungsraum im autonomen Straßenverkehr vorkommen, auch sogenannte **dynamische Elemente** im autonomen Straßenverkehr (z.B. Verhalten anderer Straßenverkehrsteilnehmer) und die **Umgebungseinflüsse** (z.B. Wetterbedingungen) auf den Straßenverkehr. Dynamische Elemente umfassen neben dem Verhalten anderer Straßenverkehrsteilnehmer auch die eigene Fahrdynamik des Ego-Fahrzeugs und haben somit einen zeitlichen Einfluss auf die vorliegende gefährliche Betriebssituation. Bei der Übertragung dieser

Taxonomie auf den vollautomatisierten Bahnbetrieb sind aufgrund der unterschiedlichen Systemeigenschaften einige Anpassungen – insbesondere bei den festen Bestandteilen der Schieneninfrastruktur und den dynamischen Elementen – erforderlich, die im Weiteren durchgeführt werden.

Während Personenzüge im vollautomatisierten Bahnbetrieb mit den beiden Automatisierungsgraden GoA3 und GoA4 ausgestattet sein können, ist bei Güterzügen entsprechend der Definition nach dem Unterkapitel 2.1.1 nur der Automatisierungsgrad GoA4 möglich. Dennoch können sowohl Personen- als auch Güterzüge mit unterschiedlichen Automatisierungsgraden auf der gleichen Strecke fahren. Damit liegt, wie in Kapitel 2.2 erläutert, ein Mischverkehr vor. Im Mischverkehr fahren die Züge mit unterschiedlichen Geschwindigkeiten. Da das Risiko für ein unerwünschtes Ereignis (z.B. Kollision) nicht nur von der Eintrittswahrscheinlichkeit des unerwünschten Ereignisses, sondern auch von dem damit verbundenen Schadensausmaß abhängt und das Schadensausmaß wiederum von der Masse und der Geschwindigkeit der Züge abhängig ist, können die zu erarbeitenden Gefährdungsursachen aus den beiden ATO-Regelkreisen bei den Zügen auf einer Mischverkehrsstrecke unterschiedliche Risiken hervorrufen.

Um im Rahmen dieser Arbeit trotz der fehlenden Betriebserfahrung mit dem vollautomatisierten Bahnbetrieb erarbeiten zu können, inwiefern sich die gleichen Gefährdungsursachen aus den beiden ATO-Regelkreisen bei unterschiedlichen Zuggattungen auswirken, wird der Mischverkehr im betrieblichen Kontext zugrunde gelegt. Für einen Mischverkehr werden die Standardelemente einer Strecke nach *DB Netz AG (2022)* durch den sogenannten Streckenstandard (früher M160 für den Mischverkehr, heute P3/P4/F1) vorgegeben.

Durch die Standardelemente einer Mischverkehrsstrecke (M160) ist es möglich, die für eine Gefährdungsanalyse relevanten festen Bestandteile – wie im autonomen Straßenverkehr – zu definieren. An dieser Stelle wird hervorgehoben, dass ein Streckenstandard nach *DB Netz AG (2022)* 27 Vorgaben für eine Mischverkehrsstrecke enthält, von denen nicht alle im Rahmen der Gefährdungsanalyse relevant sind. Denn entsprechend der Taxonomie nach *PAS 1883:2020* und der Definition nach EN 50126 von oben stehen der Ort entlang der Infrastruktur und die darin vorkommenden Bahnanlagen, an denen es zu einer Kollision, Entgleisung oder zur Gefährdung von Zuginsassen (vgl. Kapitel 5.4) kommen kann, im Fokus. Daher werden im Weiteren nur die Bahnanlagen entlang einer Mischverkehrsstrecke herangezogen, bei denen es zu einer Kollision, Entgleisung oder zur Gefährdung von Zuginsassen kommen kann.

Bei einer Mischverkehrsstrecke handelt es sich um eine **zweigleisige Strecke**, die zwei oder mehr Betriebsstellen (z.B. Bahnhöfe, Haltestellen oder Haltepunkte) miteinander verbindet. Aufgrund der Zweigleisigkeit und der unterschiedlichen Geschwindigkeiten der Züge sind auf einer Mischverkehrsstrecke Überholungen möglich. Für Überholungen sind demnach Weichen erforderlich. Zudem ist es möglich, dass Züge von einer Mischverkehrsstrecke auf eine andere Strecke abzweigen können. Die Abzweigung erfolgt ebenfalls über Weichen auf einer freien Strecke. Daher werden **Weichen** auf der freien Strecke (Fahrstraßenknoten) bei der Erarbeitung von Gefährdungsursachen aus den beiden ATO-Regelkreisen als Bestandteil des betrieblichen Kontexts herangezogen.

Wenngleich bei Neubauten und bei Strecken mit einer Höchstgeschwindigkeit von mehr als 160 km/h Bahnübergänge nicht erlaubt sind, können Mischverkehrsstrecken im Streckenstandard M160 nach EBO auch Bahnübergänge enthalten. Bahnübergänge sind bei einer Gefährdungsanalyse insofern wichtig, da dort systemexterne Objekte angetroffen werden können und es dadurch zu einer Kollision kommen

kann. Daher wird ebenfalls ein **Bahnübergang** bei der Erarbeitung von Gefährdungsursachen aus den beiden ATO-Regelkreisen als Bestandteil des betrieblichen Kontexts herangezogen.

Des Weiteren gibt es relevante Orte entlang der Infrastruktur, die entsprechend der EBO §4 nicht als Bahnanlagen gelten und deren Eigenschaften durch einen Streckenstandard nicht vorgegeben werden, diese jedoch in Hinblick auf die Gefährdung von Zuginsassen aus dem vorigen Kapitel bei der Gefährdungsanalyse relevant sind. Wie bereits in Kapitel 5.4 erläutert, können Zuginsassen aufgrund der erschwerten Erreichbarkeit der Züge im Falle einer Störung und aufgrund der fehlenden menschlichen Interaktion mit dem Zugpersonal Gefährdungen ausgesetzt sein. Da die Erreichbarkeit der Züge im Falle einer Störung auf Brücken oder in Tunneln erschwert ist und dadurch insbesondere bei Personenzügen im Falle eines Stillstands die Zuginsassen gefährdet sein können, werden **Brücken** und **Tunneln** bei der Erarbeitung von Gefährdungsursachen aus den beiden ATO-Regelkreisen als Bestandteil des betrieblichen Kontexts ebenfalls herangezogen.

Entsprechend der Taxonomie nach *PAS 1883:2020* und der STPA-Notation sind neben den festen Bestandteilen der Infrastruktur auch die dynamischen Elemente bei einer vollautomatisierten Zugfahrt erforderlich. Dazu zählt – wie bereits oben erläutert – die **Fahrdynamik eines vollautomatisierten Zuges**, die sich kontinuierlich in dem betrieblichen Kontext ändern kann. Dabei kommen nach *Wende (2003)* die Fahrzustände beschleunigen, beharren, ausrollen, bremsen und Stillstand vor.

Nicht nur die Fahrdynamik eines vollautomatisierten Zuges ist bei der Gefährdungseinschätzung relevant, sondern es spielt auch eine wesentliche Rolle, ob sogenannte **Barrieren** existieren, wodurch trotz einer vorliegenden gefährlichen Betriebssituation ein Unfall vermieden werden kann. Zu den Barrieren können im Schienenverkehr technische Systeme – wie z.B. das ETCS-System – aber auch sogenannte betriebliche Barrieren gehören. Betriebliche Barrieren werden nach *VDE V 0831-101:2020 (2022)* im Wesentlichen durch die Betriebsdichte und durch die Infrastruktur bestimmt. Beispielsweise kann die topographische Lage einer Infrastruktur (Steigung oder Gefälle) eine betriebliche Barriere darstellen. Denn eine Steigung kann das Schadensausmaß – z.B. im Falle einer zu späten Bremsung – als eine passive Barriere verringern, während ein Gefälle das Inverse bewirkt. Auch die Existenz von Tieren oder von Personen im Gefahrenbereich (insbesondere an Bahnübergängen) stellen Barrieren dar. Nach *Trinckauf (2013)* besteht zwar die Systemphilosophie in dem Vertrauen dahingehend, dass sich Personen bei einem herannahenden Zug unverzüglich aus dem Gefahrenbereich entfernen, jedoch kann das Verhalten von Personen schlecht im Voraus eingeschätzt werden. Aufgrund des offenen Zugangs zu der Eisenbahninfrastruktur – auch im vollautomatisierten Bahnbetrieb – wird das Verhalten von Personen im Gefahrenbereich neben der topographischen Lage als eine Barriere zur Beschreibung des betrieblichen Kontexts ebenfalls herangezogen.

Entsprechend der inhaltlichen Eingrenzung in Kapitel 3.5, wird das ETCS-System Level 2 ohne Signale im Rahmen dieser Arbeit als Zugsicherung herangezogen. Folglich ist es wichtig zu berücksichtigen, ob und unter welchen Bedingungen das ETCS-System beim Vorliegen einer Störung in den beiden ATO-Regelkreisen eingreifen kann, um eine Gefährdung zu verhindern (z.B. bremsender Eingriff durch die ETCS-OBU im Falle einer Geschwindigkeitsüberschreitung). Daher wird das ETCS-System als eine technische Barriere während einer vollautomatisierten Zugfahrt herangezogen.

Der umgebungsbedingte Kontext (**Umgebungseinflüsse**) enthält Bestandteile, die unabhängig von dem Betrieb zu jedem Zeitpunkt an jedem Ort existieren können und den Betrieb von außen beeinflussen. Dazu zählen **Wetterbedingungen**. Zur Beschreibung eines umgebungsbedingten Kontexts werden daher Wetterbedingungen (z.B. Tag mit sichtigem oder unsichtigem Wetter versus Dunkel und unsichtiges Wetter) und **topographische Lage der Infrastruktur** (Ebene Strecke, Gefälle oder Steigung) herangezogen.

Mit dem hergeleiteten betrieblichen und umgebungsbedingten Kontext können die Gefährdungsursachen aus den beiden ATO-Regelkreisen hinsichtlich der Verletzung der in Abbildung 20 dargestellten Schutzziele erarbeitet werden. Mit dem dadurch entstandenen minimalen Betrachtungsraum wird die Anforderung hinsichtlich der Vollständigkeit des erforderlichen betrieblichen und umgebungsbedingten Kontextes erfüllt. Denn gemäß der Norm EN 50126 *„ist nicht das Ziel, jede banale Gefährdung zu katalogisieren, auch nicht wird erwartet, dass immer alle Gefährdungen jenseits der Grenzen der aktuellen Kenntnisse zu identifizieren“* (*DIN EN 50126-2:2017, S.12*). Zudem kann ein tiefer Detaillierungsgrad in begrenzter Zeit im Rahmen dieser Arbeit nicht erreicht werden.

Eine Mischverkehrsstrecke mit dem hergeleiteten betrieblichen und umgebungsbedingten Kontext, der bei der Erarbeitung von Gefährdungsursachen aus den beiden ATO-Regelkreisen herangezogen wird, ist in der Abbildung 21 dargestellt. Die Abbildung 21 stellt auf der horizontalen Achse die Bahnanlagen und die beiden exponierten Orte (Brücke und Tunnel) entlang einer Eisenbahninfrastruktur dar. Es handelt sich dabei um eine zweigleisige Mischverkehrsstrecke, die zwei Betriebsstellen miteinander verbindet. Der auf der freien Strecke befindliche Bahnübergang (Bü) repräsentiert einen Ort entlang der freien Strecke, an dem im Falle einer Gefährdung eine Kollision (Zusammenprall) mit Straßenverkehrsteilnehmern entstehen kann. Die Abzweig- oder Überleitstelle (Abzw. oder Überleitst.) repräsentiert exemplarisch einen Fahrstraßenknoten, an dem es im Falle einer Gefährdung zu einer Entgleisung kommen kann.

Auf der vertikalen Achse der Abbildung sind neben der Fahrdynamik eines vollautomatisierten Zuges die Barrieren und die Umgebungseinflüsse dargestellt. Der betriebliche und umgebungsbedingte Kontext zur Gefährdungseinschätzung im vollautomatisierten Bahnbetrieb ergibt sich spaltenweise, ähnlich wie in einer Entscheidungstabelle.

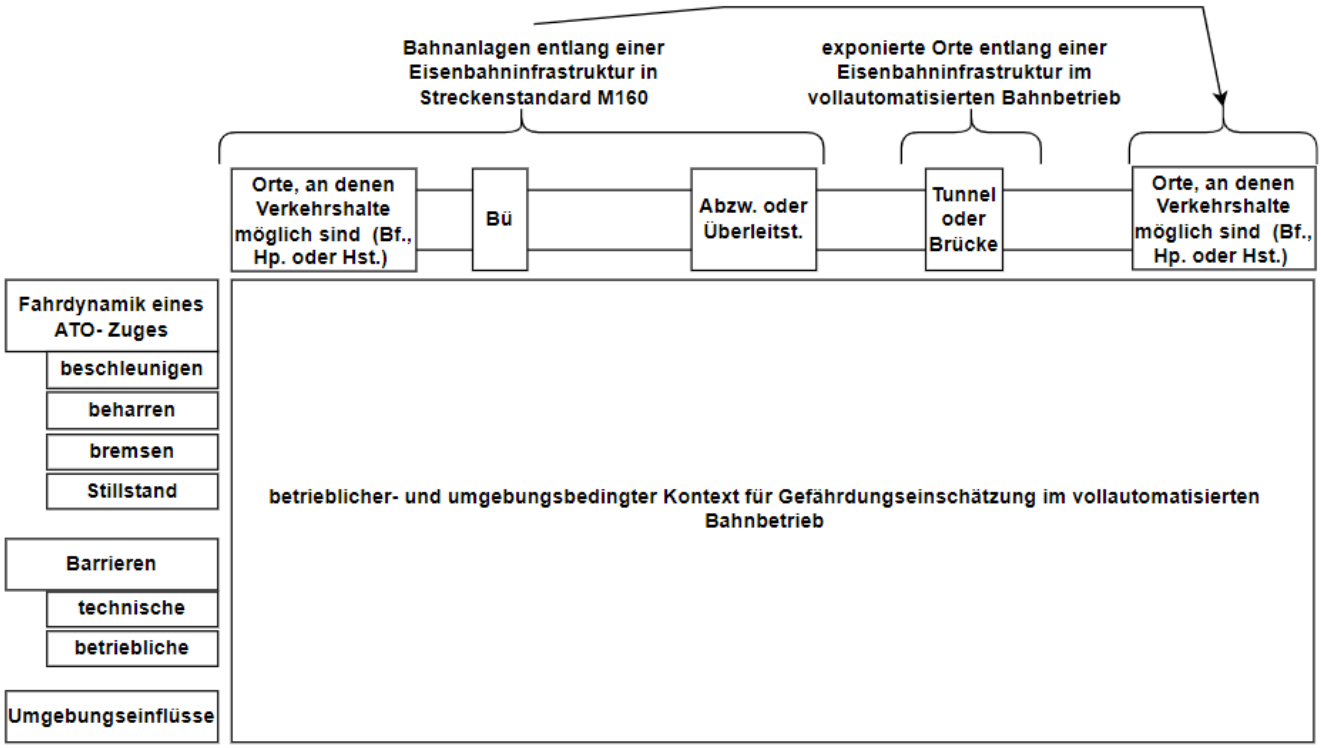

Abbildung 21 zweigleisige Strecke, die zwei Betriebsstellen miteinander verbindet und mit der Fahrdynamik eines Zuges, mit den Barrieren und Umgebungseinflüssen verknüpft wird, um exemplarisch einen betrieblichen und umgebungsbedingten Kontext zu beschreiben (eigene Darstellung)

Nachdem in diesem Kapitel der betriebliche und umgebungsbedingte Kontext für Gefährdungen im vollautomatisierten Bahnbetrieb hergeleitet wurde, werden im nächsten Kapitel mögliche gefährliche Betriebssituationen und ihre Gefährdungsursachen aus den beiden ATO-Regelkreisen erarbeitet.

5.6 Gefährdungsraum im vollautomatisierten Bahnbetrieb

Entsprechend der STPA-Methode werden die gefährlichen Betriebssituationen in einem betrieblichen- und umgebungsbedingten Kontext erarbeitet. Da der betriebliche- und umgebungsbedingte Kontext bereits in dem vorigen Kapitel hergeleitet wurde, ist das Ziel dieses Kapitels, die gefährlichen Betriebssituationen und die möglichen Gefährdungsursachen aus den beiden ATO-Regelkreisen zu erarbeiten, die im vollautomatisierten Bahnbetrieb zu vermeiden sind. Zunächst werden in Unterkapitel 5.6.1 entsprechend der STPA-Methode die gefährlichen Betriebssituationen erarbeitet. Danach wird in Unterkapitel 5.6.2 untersucht, welche Gefährdungsursachen aus den beiden ATO-Regelkreisen zu den gefährlichen Betriebssituationen führen können.

5.6.1 Potenzielle gefährliche Betriebssituationen in dem erarbeiteten betrieblichen- und umgebungsbedingten Kontext

Entsprechend des betrieblichen- und umgebungsbedingten Kontextes aus der Abbildung 21 werden die möglichen gefährlichen Betriebssituationen ausgehend von einer Betriebsstelle über die Mischverkehrsstrecke zu der anderen Betriebsstelle systematisch erarbeitet. Wie bereits in Kapitel 5.4 erläutert, liegt eine gefährliche Betriebssituation aus Sicht eines vollautomatisierten Zuges dann vor, wenn es in einem betrieblichen- und umgebungsbedingten Kontext entweder zu einer Kollision oder zu einer Entgleisung oder zu Gefährdungen von Zuginsassen kommt.

Ausgehend von den erarbeiteten ATO-relevanten Schutzziele aus dem Kapitel 5.4 und anhand des betrieblichen und umgebungsbedingten Kontexts aus der Abbildung 21 werden im Weiteren einige gefährliche Betriebssituationen im vollautomatisierten Bahnbetrieb erarbeitet.

Gefährliche Betriebssituationen an einer Betriebsstelle (Gefährdung 1)

Gefährdung (1.1)

Unter der Annahme, dass ein vollautomatisierter Zug an einer Betriebsstelle startet und eine Zugfahrt im Regelbetrieb nur unter der ETCS-Überwachung durchgeführt wird, die als technische Barriere wirkt, kann es **im Beschleunigungszustand** eines vollautomatisierten Zuges an der Betriebsstelle nur dann zu einer gefährlichen Betriebssituation kommen, **wenn plötzlich Personen, Tiere oder externe bewegliche Objekte sich in den Gefahrenbereich begeben und der vollautomatisierte Zug nicht rechtzeitig bremsen kann**, sodass es zu einer **Kollision** kommt. Diese gefährliche Betriebssituation wird umso prekärer, je schlechter die Wetterbedingungen, die Sichtverhältnisse der Sensoren sind und je stärker ein vorliegendes Gefälle ist. Die Gefährdung kann durch die ETCS-OBU als technische Barriere nicht verhindert werden.

Gefährdung (1.2)

Zu **Gefährdungen von Zuginsassen** kann es an einer Betriebsstelle nur dann kommen, wenn ein **vollautomatisierter Personenzug** trotz der vorliegenden Fahrterlaubnis **nicht anfährt bzw. weiterfährt** und entsprechend des Kapitels 5.4 **hinreichend gute klimatische Bedingungen** (z.B.

durch unzureichende Belüftung) **nicht gewährleistet** werden können. Im Vergleich zu einem Bahnhof kann diese Gefährdung an einer Haltestelle oder an einem Haltepunkt besonders signifikant sein, da ein nicht anfahrender Zug in einem Bahnhof von außenstehenden Menschen aufgrund der höheren Betriebsdichte (betriebliche Barriere) schneller erkannt werden kann als an einer Haltestelle oder an einem Haltepunkt.

Gefährliche Betriebssituationen auf einer freien Strecke (Gefährdung 2)

Gefährdung (2.1)

Analog zu einer Betriebsstelle kann es auf einer freien Strecke durchgehend zu einer Kollision und demnach zu einer gefährlichen Betriebssituation kommen. Im Gegensatz zu der Betriebsstelle, an der eine vollautomatisierte Zugfahrt beginnt (Beschleunigungszustand), liegt eine Kollisionsgefahr auch im Falle einer **Beharrungsfahrt oder im Bremszustand** vor, **wenn plötzlich Personen, Tiere oder externe bewegliche Objekte sich in den Gefahrenbereich begeben und der vollautomatisierte Zug nicht rechtzeitig oder nicht mit der erforderlichen Bremskraft bremst.** Diese gefährliche Betriebssituation wird umso prekärer, je schlechter die Wetterbedingungen, die Sichtverhältnisse der Sensoren sind und je stärker ein vorliegendes Gefälle ist. Wie bei der Gefährdung 1.1 greift die ETCS-OBU als technische Barriere nicht ein, solange die Geschwindigkeit des Zuges unter der zulässigen Geschwindigkeit liegt.

Gefährdung (2.2)

Anders als an einer Betriebsstelle kann es auf einer freien Strecke auch an stetigen Stellen (z.B. in Gleisbögen) zu einer **Entgleisung** kommen, wenn die Geschwindigkeit des vollautomatisierten Zuges aufgrund von Umgebungseinflüssen höher ist als die maximal zulässige Geschwindigkeit im Gleisbogen.

Gefährdung (2.3)

Zu **Gefährdungen von Zuginsassen** kann es entlang der freien Strecke kommen, wenn ein **vollautomatisierter Personenzug** trotz der vorliegenden Fahrterlaubnis **nicht anfährt bzw. weiterfährt** und entsprechend des Kapitels 5.4 **hinreichend gute klimatische Bedingungen** (z.B. durch unzureichende Belüftung) **nicht gewährleistet** werden können. Im Vergleich zu einem Bahnhof, kann die Zugänglichkeit des Zuges auf einer freien Strecke reduziert sein, weshalb die Zuginsassen dieser Gefährdung länger ausgesetzt sein können. Eine mögliche technische Barriere in diesem Fall könnte zwar sein, dass sich die Türen des Zuges öffnen, jedoch kann es dadurch zu weiteren Gefährdungen im Gleisbereich kommen, sofern Zuginsassen den Zug auf der freien Strecke verlassen.

Gefährliche Betriebssituationen auf einem Bahnübergang (Gefährdung 3)

Ein Bahnübergang ist eine Bahnanlage auf einer freien Strecke, deshalb gelten die Gefährdungen hinsichtlich der Kollision und der Gefährdungen von Zuginsassen wie auf einer freien Strecke von oben auch auf einem Bahnübergang. Da es auf einem Bahnübergang zu einem Zusammenprall mit Straßenverkehrsteilnehmern kommen kann, ist hinsichtlich der Kollision auf einem Bahnübergang eine weitere Ergänzung erforderlich.

Gefährdung (3.1)

Sofern ein vollautomatisierter Zug an einem Bahnübergang **unerwartet zum Stillstand** kommt und **nicht weiterfahren** kann, kann es zu einem Zusammenprall mit Straßenverkehrsteilnehmern kommen, wenn die Bahnschranken bei einem technisch gesicherten Bahnübergang wieder öffnen oder es sich um einen nicht technisch gesicherten Bahnübergang handelt. Diese gefährliche Betriebssituation wird umso prekärer, je **schlechter die Wetterbedingungen** sind, sodass auch die Straßenverkehrsteilnehmer den haltenden Zug **nicht rechtzeitig sehen** können. Lediglich eine Gefahrenraumüberwachung an technisch gesicherten Bahnübergängen könnte als eine technische Barriere fungieren. Um jedoch herannahende Straßenverkehrsteilnehmer vor dem Zug am Bahnübergang mittels der Gefahrenraumüberwachung zu warnen, ist eine entsprechende Kommunikationsschnittstelle zwischen der Gefahrenraumüberwachung und den Straßenverkehrsteilnehmern erforderlich.

Gefährliche Betriebssituationen auf einer Weiche (Abzweig- oder Überleitstelle) (Gefährdung 4)

Auch die Abzweig- oder Überleitstelle befindet sich auf einer freien Strecke, sodass die Gefährdungen hinsichtlich der Kollision und der Gefährdungen von Zuginsassen wie auf einer freien Strecke von oben auch auf einer Weiche gelten. Hinsichtlich der Entgleisung ist jedoch – wie bei einem Bahnübergang – eine Ergänzung erforderlich.

Gefährdung (4.1)

Ein vollautomatisierter Zug, der unerwartet **auf einer Weiche zum Stillstand** gekommen ist, kann entgleisen, wenn dieser **nicht weiterfahren** kann und dieser Zug **nicht auf einer Weiche geortet** wird, sodass die Weiche von der Sicherungslogik für eine andere Zugfahrt freigegeben wird. Außerdem kann es in so einem Fall auch zu einer Kollision (Flankenfahrt) kommen. Eine betriebliche Barriere greift hier nur, wenn die Betriebsdichte entsprechend der VDE V 0831-103 sehr gering oder unterdurchschnittlich ist, sodass die Weiche für keinen anderen Zug während der Störungssituation freigegeben wird.

Gefährliche Betriebssituationen auf einer Brücke oder in einem Tunnel (Gefährdung 5)

Entsprechend des Kapitels 5.5 sind Brücken und Tunneln besonders exponierte Orte auf einer freien Strecke, an denen es während einer vollautomatisierten Zugfahrt zu **Gefährdungen von Zuginsassen** kommen kann.

Gefährdung (5.1)

Wie bereits in Kapitel 5.4 erläutert, können Zuginsassen aufgrund der erschwerten Erreichbarkeit der Züge im Falle einer Störung und aufgrund der fehlenden menschlichen Interaktion mit dem Zugpersonal Gefährdungen ausgesetzt sein. Dazu kann es kommen, wenn ein vollautomatisierter Zug unerwartet auf einer **Brücke** oder in einem **Tunnel zum Halten** kommt und **nicht weiterfahren** kann sowie die **Kommunikation** zu einem zuständigen Betriebspersonal **nicht möglich** ist.

Gefährdung (5.2)

Außerdem liegt eine Gefährdung vor, wenn ein vollautomatisierter Zug außerhalb des Tunnels geortet wird, obwohl dieser sich im Tunnel befindet. Dabei liegt insbesondere eine Gefährdung aufgrund des Tunnelbegegnungsverbots zwischen Personen- und Güterzügen vor. Eine betriebliche Barriere greift hier

nur, wenn die Betriebsdichte entsprechend der VDE V 0831-103 sehr gering oder unterdurchschnittlich ist, sodass kein anderer Zug während der Störungssituation entgegenfährt.

Mit dem betrieblichen- und umgebungsbedingten Kontext und den Schutzzielen, bei deren Erfüllung das ATO-System mitwirkt, konnten in diesem Unterkapitel einige gefährliche Betriebssituationen erarbeitet werden, die es zu vermeiden gilt. Die Ursachen für diese gefährlichen Betriebssituationen können trotz vorliegender Barrieren in den beiden ATO-Regelkreisen liegen. Deshalb werden im nächsten Unterkapitel mögliche Gefährdungsursachen aus den beiden ATO-Regelkreisen erarbeitet.

5.6.2 Gefährdungsursachen aus den beiden ATO-Regelkreisen

In diesem Kapitel werden aus den beiden ATO-Regelkreisen mögliche Gefährdungsursachen erarbeitet, wodurch es zu den gefährlichen Betriebssituationen aus dem vorigen Unterkapitel kommen kann.

Entsprechend der STPA-Notation ergeben sich Gefährdungsursachen aus Kontrollaktion und Rückkopplungen. Dazu gibt es in der STPA-Notation eine Liste von etablierten Störungen, die herangezogen werden könnten.

Da die Gesamtanzahl der möglichen Gefährdungsursachen aus der Multiplikation der etablierten Störungen mit den Kontrollaktionen bzw. Rückkopplungen aus der funktionalen Systemarchitektur ergibt, würde eine derartige Gefährdungsanalyse den Umfang dieser Arbeit sprengen. Anhand einer Beispielrechnung soll an dieser Stelle die Anzahl von möglichen Gefährdungsursachen aus den beiden ATO-Regelkreisen verdeutlicht werden:

Aus den beiden ATO-Regelkreisen können 11 Pfeile für Kontrollaktionen und 5 Pfeile für Rückkopplungen sowie aus der Tabelle 2 auf Seite 71 insgesamt 14 verschiedene dazugehörige Kontrollaktionen und Rückkopplungen entnommen werden.

In der Bahnfachwelt sind für Gefährdungsanalysen 28 etablierte Störungen definiert *(vgl. DB Netz AG 2014)*. Darin sind auch die in der STPA-Methode verwendeten Störungen enthalten. Durch Multiplikation der etablierten Störungen mit den 14 Kontrollaktionen bzw. Rückkopplungen ergeben sich aus den beiden ATO-Regelkreisen insgesamt 392 mögliche Gefährdungsursachen.

Sofern mehrere Gefährdungsursachen – beispielsweise aus zwei Regelungspfaden – kombiniert betrachtet werden, steigt die Anzahl n_{Kombi} der möglichen Gefährdungsursachen unter Vernachlässigung der Reihenfolge auf

$$n_{Kombi} = \binom{392}{2} = 76636.$$

Aus dieser Beispielrechnung heraus wird deutlich, dass in begrenzter Zeit so viele Gefährdungsursachen nicht bearbeitet werden können. Folglich wird im Rahmen der Gefährdungsanalyse nur für den Worst-Case-Fall **„Kontrollaktion/Rückkopplung wird nicht ausgeführt bzw. nicht verfügbar“** untersucht, in welchem betrieblichen und umgebungsbedingten Kontext eine tatsächliche Gefährdung vorliegt.

Die Abbildung 22 zeigt die funktionale Systemarchitektur aus dem Hauptkapitel 4. Darin sind die beiden ATO-Regelkreise, die einer Gefährdungsanalyse unterzogen werden, farbig markiert. Der fahrzeugseitige ATO-Regelkreis ist rot markiert. Die blauen Pfeile verdeutlichen den infrastrukturseitigen ATO-Regelkreis.

Entsprechend den Kontrollaktionen und Rückkopplungen aus der hierarchischen Regelungsstruktur (vgl. Kapitel 4.5) sind die Gefährdungsursachen aus den beiden ATO-Regelkreisen in der Tabelle 3 zusammengefasst. Die Gefährdungsursachen in blauer Markierung ergeben sich aus dem infrastrukturseitigen ATO-Regelkreis, während die Gefährdungsursachen in roter Markierung im fahrzeugseitigen ATO-Regelkreis entstehen können.

Tabelle 3 Gefährdungsursachen aus den beiden ATO-Regelkreisen. Rot: Gefährdungsursachen aus dem fahrzeugseitigen ATO-Regelkreis. Blau: Gefährdungsursachen aus dem infrastrukturseitigen ATO-Regelkreis.

Gefährdungsursachen aus dem **infrastrukturseitigen Regelkreis**	Tagesfahrplan nicht verfügbar	Journey-Profile nicht verfügbar	Segment-Profile nicht verfügbar
	Statusdaten nicht verfügbar	Movement Permission nicht verfügbar	
Gefährdungsursachen aus dem **fahrzeugseitigen Regelkreis**	aktuelle Position des Zuges nicht verfügbar	Objekterkennung und Objektklassifizierung nicht verfügbar	Zustand der Zugintegrität nicht verfügbar
	Steuerbefehle für die Geschwindigkeitsregelung nicht verfügbar	Steuerbefehle für die Fahrzeugkomponenten nicht verfügbar	Fahrdynamische Zustandsgrößen nicht verfügbar
	Zustandsgrößen Lichtraumüberwachung nicht verfügbar	Zugdaten nicht verfügbar	Zustand der Fahrzeugkomponenten nicht verfügbar

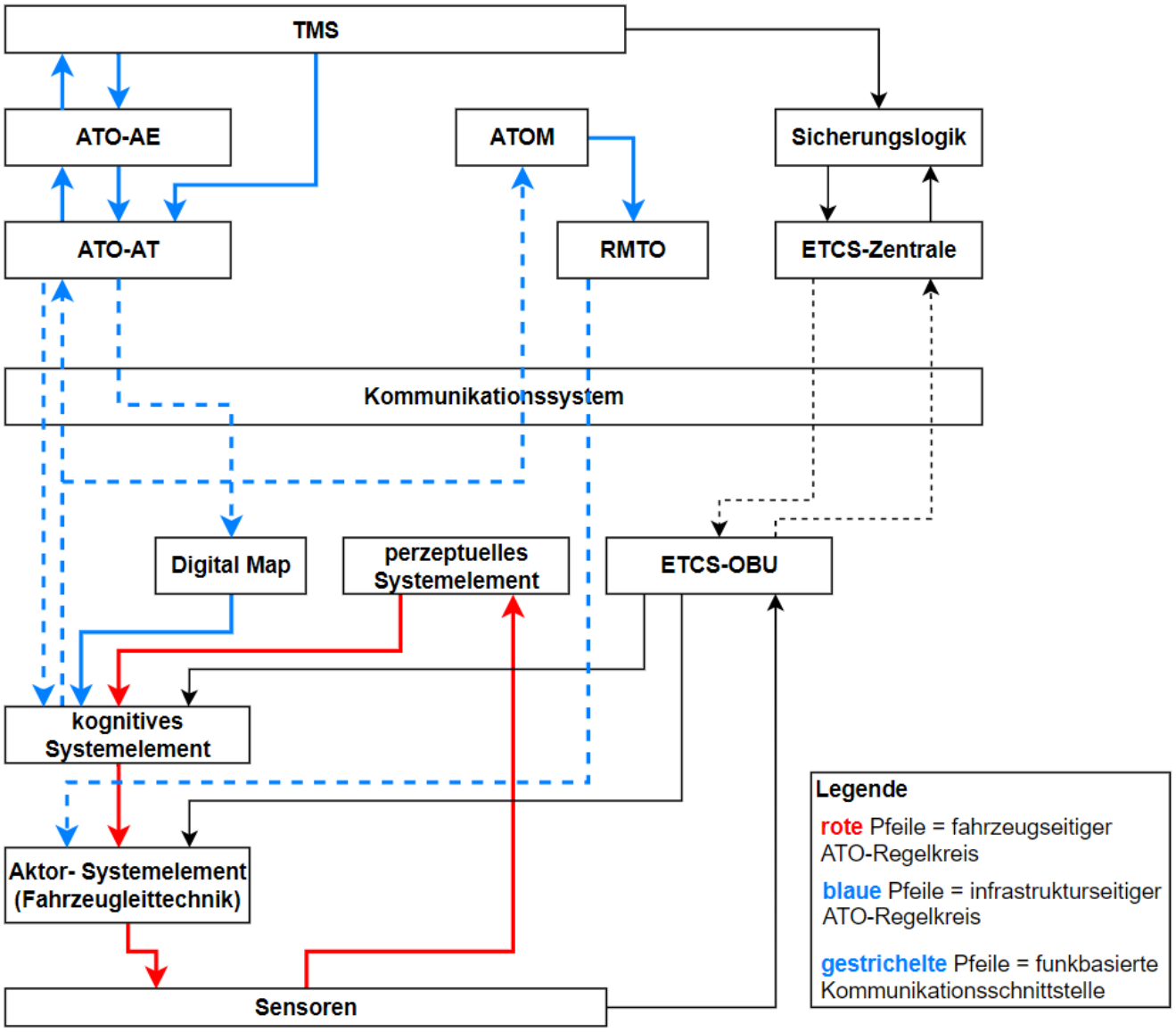

Abbildung 22 funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt mit Hervorhebung der beiden ATO-Regelkreise für die Gefährdungsanalyse (STPA-Notation)

Im Weiteren wird untersucht, durch welche der Gefährdungsursachen aus Tabelle 3 es zu den gefährlichen Betriebssituationen aus dem vorigen Unterkapitel kommen kann.

Wie aus dem vorigen Unterkapitel bekannt, können die gefährlichen Betriebssituationen **1.2, 2.3, 3.1, 4.1 und 5.1** aufgrund des Stillstandes eines vollautomatisierten Zuges entstehen. Es werden daher zunächst die Gefährdungsursachen aus den beiden ATO-Regelkreisen untersucht, wodurch eine Weiterfahrt der vollautomatisierten Züge vorübergehend nicht mehr möglich ist.

Die gefährlichen Betriebssituationen **1.1, 2.1, 2.2 und 5.2** können während einer Fahrt entstehen. Daher werden auch die Gefährdungsursachen dafür untersucht, wodurch zwar eine Weiterfahrt der vollautomatisierten Züge möglich jedoch nicht mehr so sicher wie im Regelbetrieb ist.

Ursachen aus den beiden ATO-Regelkreisen, die eine Weiterfahrt der Züge verhindern können

Ursache: Tagesfahrplan oder Movement Permission (MP) nicht verfügbar

Bereits aus dem Kapitel 4.5 ist bekannt, dass ein Tagesfahrplan bereits vor einer Zugfahrt vorliegen sollte. Sofern also **kein Tagesfahrplan** als Kontrollaktion vorliegt, kann das Systemelement ATO-AE daraus keine Journey-Profiles generieren, sodass vollautomatisierte Züge nicht fahren können. Während ein Tagesfahrplan bereits vor einer Zugfahrt vorliegen sollte, kann es während einer Zugfahrt (z.B. auf der freien Strecke) dazu kommen, dass das TMS eine Fahrterlaubnisanfrage (MP) bei der Sicherungslogik stellen muss. Sofern eine **Fahrterlaubnisanfrage nicht verfügbar** ist und ein Personenzug daher auf der freien Strecke nicht mehr weiterfahren kann, können die gefährlichen Betriebssituationen 1.2, 2.3, 3.1, 4.1 und 5.1 entstehen.

Ursache: Journey-Profile oder Segment-Profile nicht verfügbar

Auf Basis eines Tagesfahrplans werden entsprechend der hierarchischen Regelungsstruktur aus dem Kapitel 4.5 durch das Systemelement ATO-AE für die im ATO-AT-Zuständigkeitsbereich angemeldeten ATO Züge Journey-Profiles generiert.

Sofern **Journey-Profiles nicht generiert** werden (z.B. aufgrund von Fehler in dem zuständigen Algorithmus) oder aufgrund von **fehlenden Statusdaten** aus den ATO-Zügen, kann das zuletzt aktive Geschwindigkeitsprofil bei den betroffenen Zügen nicht mehr aktualisiert werden, sodass die Weiterfahrt der betroffenen Züge verhindert sein kann, nachdem das zuletzt aktive Geschwindigkeitsprofil abgefahren wurde.

Auch die Segment-Profiles werden zur Generierung von Journey-Profiles verwendet. Sofern also Segment-Profiles nicht verfügbar sind, können keine Journey-Profiles erstellt werden. Während einer Zugfahrt werden die Segment-Profiles von dem Systemelement Digital Map dem kognitiven Systemelement zur Erstellung eines Geschwindigkeitsprofils zur Verfügung gestellt. Da ein Segment Profile u.a. die maximal erlaubte Geschwindigkeit auf der Strecke, das Gradientenprofil und die erlaubte Oberstrombegrenzung der Strecke enthält, könnte der Algorithmus zur Erstellung eines Geschwindigkeitsprofils bei Nichtverfügbarkeit dieser Informationen **kein Geschwindigkeitsprofil** erstellen, sodass dadurch die gefährlichen Betriebssituationen 1.2, 2.3, 3.1, 4.1 und 5.1 entstehen können.

Ursache: Kommunikationssystem nicht verfügbar

Aus der hierarchischen Regelungsstruktur ist zudem ersichtlich, dass die Kommunikationsverbindung zwischen Zug und dem TMS (ATO-Regelkreis) oder der ETCS-Zentrale (ETCS-Regelkreis) aufgrund der zentralen Systemarchitektur des Bahnbetriebs für eine sichere Zugfahrt unabdingbar ist. Deshalb können Störungen im Kommunikationssystem Gefährdungen verursachen, da dadurch nicht nur vorübergehend die zentrale Betriebsführung unterbrochen wird, sondern auch simultan mehrere Züge betroffen sein können.

Außerdem ist die Kommunikationsverbindung insbesondere beim Verdacht auf eine ungewollte Zugtrennung essenziel, da die infrastrukturseitigen Systemelemente aus der hierarchischen Regelungsstruktur – wie zuvor erwähnt – aus der Ferne keine Möglichkeit haben, den Verdacht auf eine ungewollte Zugtrennung zu bestätigen.

Wenngleich – insbesondere für den ETCS-Regelkreis – hohe Anforderungen an die Verfügbarkeit des Kommunikationssystems gestellt wird, können auch externe Ursachen (z.B. Cyber-Angriffe) die

Verfügbarkeit des Kommunikationssystems beeinträchtigen. Dabei sind sowohl punktuelle Angriffe (nur zugseitiges Kommunikationssystem) als auch Angriffe mit klein- oder großräumigen Auswirkungen (vgl. Kapitel 2.4 z.B. Funkstation oder ETCS-Zentrale) denkbar.

Wie in Kapitel 2.5 vorgestellt und in der hierarchischen Regelungsstruktur vorhanden, kann eine ferngesteuerte Zugfahrt durch das Systemelement RMTO nicht durchgeführt werden, sofern das Kommunikationssystem nicht verfügbar ist.

Da die Journey-Profiles, Segment-Profiles und die Fahrterlaubnisse über ein funkbasiertes Kommunikationssystem an das kognitive Systemelement oder an die ETCS-OBU übertragen werden, können **Störungen am Kommunikationssystem** eine wesentliche Ursache für die gefährlichen Betriebssituationen 1.2, 2.3, 3.1, 4.1 und 5.1 sein.

Ursache: Steuerbefehle für die Geschwindigkeitsregelung und für die Fahrzeugkomponenten nicht verfügbar

Aus der hierarchischen Regelungsstruktur ist ersichtlich, dass eine Weiterfahrt des Zuges verhindert sein kann, wenn zwar Journey-Profiles als auch das Segment-Profile verfügbar sind, jedoch die Steuerbefehle für die Geschwindigkeitsregelung nicht verfügbar sind, denn die ETCS-OBU kann nur bremsend in die Fahrzeugleittechnik eingreifen.

Da der Regelungsalgorithmus im kognitiven Systemelement die Steuerbefehle für die Geschwindigkeitsregelung generiert, können Steuerbefehle für die Geschwindigkeitsregelung nicht vorliegen, wenn der Regelungsalgorithmus im kognitiven Systemelement nicht verfügbar ist. Sofern jedoch der Regelungsalgorithmus verfügbar ist, kann die Ursache für die Nichtverfügbarkeit der Steuerbefehle entsprechend der STPA-Notation im Algorithmus zur Generierung von Geschwindigkeitsprofilen liegen.

Das kognitive Systemelement generiert auch Steuerbefehle zur Steuerung der an der Fahrzeugleittechnik angebundenen Fahrzeugkomponenten. Dazu gehören für eine Zugfahrt insbesondere die Türsteuerung und die Steuerung des Stromabnehmers. Während die Türschließung vor der Zugfahrt sichergestellt werden muss, kann es während der Fahrt vorkommen, dass der Stromabnehmer durch die automatische Stromabnehmersenkeinrichtung (AS) gesenkt wird. Dadurch wird eine Vollbremsung eingeleitet und somit der Zug automatisch zum Halten gebracht. Sofern der Stromabnehmer anschließend durch Steuerbefehle vom kognitiven Systemelement nicht mehr gehoben werden kann (**Steuerbefehle für die Fahrzeugkomponenten nicht verfügbar**), ist eine Weiterfahrt des Zuges aufgrund fehlender Antriebsleistung nicht möglich. Dadurch können ebenfalls die gefährlichen Betriebssituationen 1.2, 2.3, 3.1, 4.1 und 5.1 entstehen.

Ursache: Zustandsdaten aus den Sensoren nicht verfügbar

Außerdem wird das kognitive Systemelement von dem übergeordneten perzeptuellen Systemelement mit fahrdynamischen Zustandsdaten, mit Zustandsdaten der Fahrzeugkomponenten einschließlich der Zugintegrität sowie mit erkannten und klassifizierten Objekten im Lichtraumprofil versorgt. Aber auch die aktuelle Position der Züge ist für die sichere Geschwindigkeitsregelung besonders relevant.

Die Erstellung des Geschwindigkeitsprofils bzw. die Geschwindigkeitsregelung kann insbesondere bei Nichtverfügbarkeit von fahrdynamischen Zustandsdaten beeinträchtigt werden. Als Sicherheitsreaktion könnte das kognitive Systemelement eine Bremsung einleiten, sofern keine fahrdynamischen Zustandsdaten vorliegen, sodass eine sichere Geschwindigkeitsregelung nicht möglich ist.

Eine Sicherheitsreaktion durch das kognitive Systemelement könnte auch dann erfolgen, wenn **keine Zustandsdaten** bezüglich der Lichtraumüberwachung vorliegt oder sogenannte Randfälle (Edge-Cases)

erkannt wurden. Sofern bei den genannten Ursachen nach einem Stillstand keine erneute Weiterfahrt erfolgt, können die gefährlichen Betriebssituationen 1.2, 2.3, 3.1, 4.1 und 5.1 entstehen. Die gefährlichen Betriebssituationen 3.1 und 4.1 werden insbesondere dadurch begünstigt, wenn zusätzlich zu den fehlenden Steuerbefehlen für die Geschwindigkeitsregelung und für die Fahrzeugkomponenten auch die **aktuelle Position des Zuges** aus dem aus den Sensoren oder dem perzeptuellen Systemelement **nicht verfügbar** ist.

Nachdem in diesem Unterkapitel die möglichen Ursachen aus den beiden ATO-Regelkreisen untersucht wurden, die eine Weiterfahrt der Züge im vollautomatisierten Bahnbetrieb verhindern können und dadurch die gefährlichen Betriebssituationen 1.2, 2.3, 3.1, 4.1 und 5.1 verursachen, werden als nächstes die Ursachen untersucht, wodurch eine Weiterfahrt der Züge zwar möglich, jedoch im Vergleich zum Regelbetrieb nicht mehr sicher ist.

Ursachen aus den beiden ATO-Regelkreisen, die eine im Vergleich zum Regelbetrieb sichere Weiterfahrt der Züge verhindern kann

Da eine Weiterfahrt möglich ist, wird im weiteren Verlauf auch angenommen, dass

- ein Fahrplan vorliegt,
- Journey-Profiles generiert werden können,
- eine Fahrterlaubnisanfrage (MP) und Fahrterlaubnis vorliegen.

Ursache: Steuerbefehle für die Geschwindigkeitsregelung und für die Fahrzeugkomponenten nicht verfügbar

Wenngleich die Geschwindigkeit eines Zuges durch die Zugsicherung überwacht wird (Barriere), gibt es Situationen, bei denen eine Geschwindigkeitsüberwachung durch die Zugsicherung nicht greift. Das ist dann der Fall, wenn die ETCS-OBU nicht verfügbar ist und daher das ETCS-System in die Betriebsart Staff-Responsible wechselt. Sofern das kognitive Systemelement die Geschwindigkeit in der Betriebsart SR regeln muss, ist es für die sichere Geschwindigkeitsregelung unterhalb der maximal zulässigen ETCS-Geschwindigkeit zuständig. Daher kann es zu der gefährlichen Betriebssituation 2.2 kommen, wenn die **maximal zulässige ETCS-Geschwindigkeit nicht bekannt** ist und die Geschwindigkeit insbesondere an Fahrstraßenknoten z.B. aufgrund schlechter Wetterbedingungen (z.B. zu starker Seitenwind) und ungünstiger topologischer Lage der Infrastruktur (z.B. Gefälle) – nicht eingehalten werden kann.

Sofern beispielsweise ein kurzzeitig erhöhter Seitenwind in einem bestimmten Abschnitt auf einen fahrenden Zug einwirkt, kann die Geschwindigkeitsregelung korrektiv eingreifen. Wenn aber hingegen ein längerer Seitenwind über einen längeren Abschnitt auf einen fahrenden Zug einwirkt und das **kognitive Systemelement keine Steuerbefehle** für die Geschwindigkeitsregelung an die Fahrzeugleittechnik übermittelt, kann es zu Entgleisung führen, insbesondere an Gleisbögen, wenn die maximal zulässige Geschwindigkeit in Abhängigkeit des Bogenradius überschritten wird.

Wenngleich die Zugsicherung im Modus „Post Trip“ die Geschwindigkeit des Zuges überwacht, stellt die Nichtverfügbarkeit von Steuerbefehlen für die Geschwindigkeitsregelung auch dann eine Gefährdung dar, wenn der Zug von dem fahrdynamischen Zustand „beharren“ oder „ausfahren“ in die Bremsung übergehen soll. Denn **fehlende Steuerbefehle für die Bremsung** stellen insbesondere bei Einfahrten in Bahnhöfen eine Gefährdung dar, wenn trotz der Einhaltung der zulässigen „Post Trip“ Geschwindigkeit

bei einem geplanten Halt am Bahnhof kein Halt oder ein später Halt (aufgrund einer Zwangsbremsung durch die ETCS-OBU) erfolgt.

Eine wesentliche Ursache für die fehlenden Steuerbefehle für die Geschwindigkeitsregelung können in der **fehlenden Information über den aktuellen Reibwert** entlang der Infrastruktur (fahrdynamische Zustandsgrößen) liegen. Insbesondere bei schlechten Wetterbedingungen (z.B. zu starker Seitenwind) und ungünstigen topologischen Lage der Infrastruktur (z.B. Gefälle) stellt die fehlende Information über den aktuellen Reibwert eine Gefährdung dar, da dadurch der Zielpunkt verfehlt und somit eine Kollision verursacht werden kann.

Das kognitive Systemelement generiert während der Fahrt auch Steuerbefehle zur Steuerung der an der Fahrzeugleittechnik angebundenen Fahrzeugkomponenten. Unter der Annahme, dass die Türen vor einer Zugfahrt verschlossen sind, kann die Steuerung des Stromabnehmers durch das Aktor-Systemelement eine Gefährdung verursachen. Wenn beispielsweise **kein Steuersignal an die Stromabnehmersenkeinrichtung** generiert wird, obwohl eine Absenkung von der Zugsicherung kommandiert wurde, kann es zu einer Kollision des Zuges mit der Oberleitung kommen und die Dachausrüstung des Zuges durch elektrische Einflüsse (z.B. Funken oder Stromüberlastung) beschädigt werden. Dadurch kann auch die Weiterfahrt des betroffenen Zuges verhindert sein.

Ursache: Zustandsdaten aus den Sensoren nicht verfügbar

Insbesondere die Geschwindigkeitsregelung erfolgt auf Basis der Rückkopplungen aus den Sensoren und den daraus generierten Kontrollaktionen von dem perzeptuellen Systemelement.

Die Nichtverfügbarkeit der aktuellen Position des Zuges stellt nicht nur im Stillstand an den oben genannten Orten eine Gefährdung dar, sondern auch während der Fahrt kann eine Gefährdung durch die Nichtverfügbarkeit der aktuellen Zugposition vorliegen. Demnach kann während der Geschwindigkeitsregelung durch das kognitive Systemelement eine Gefährdung vorliegen, wenn das kognitive Systemelement bei **Nichtverfügbarkeit der aktuellen Zugposition** den letzten Steuerbefehl weiterhin ausführt und dieser beharren oder beschleunigen ist, obwohl eine Bremsphase – aufgrund von Personen, Tieren oder Objekte im Gefahrenbereich – ansteht. Diese Betriebssituation führt insbesondere dann zu einer Gefährdung, wenn zudem die ETCS-OBU nicht verfügbar ist, die rechtzeitig bremsend eingreifen könnte.

Weitere Rückkopplungen aus den Sensoren, die in das perzeptuelle Systemelement eingespeist werden, sind Zustandsgrößen bezüglich der Lichtraumüberwachung (Objekterkennung und Objektklassifizierung). Prinzipiell hätte eine kurzzeitige Nichtverfügbarkeit der Zustandsgrößen bezüglich der Lichtraumüberwachung keine Gefährdung zur Folge, wenn der Lichtraum aufgrund von baulicher Lage (ob natürlich oder künstlich) schwer von externen Objekten, Tieren oder Personen erreichbar ist. Beispielsweise kann in Tunneln aufgrund der baulichen Lage davon ausgegangen werden, dass keine Hindernisse von außen hineinragen können. Daher stellt die Nichtverfügbarkeit der Zustandsgrößen bezüglich der Lichtraumüberwachung bis zum Verlassen eines Tunnels nicht notwendigerweise eine Gefährdung dar.

Jedoch kann die **Nichtverfügbarkeit der Zustandsgrößen bezüglich der Lichtraumüberwachung** – insbesondere bei unsichtigen Wetterbedingungen – die gefährlichen Betriebssituationen 1.1 und 2.1 verursachen.

Wie bereits in Kapitel 2.5 erläutert, ist die Betriebsart On-Sight (Fahren auf Sicht) im ETCS-System integriert, die häufig für das Fahren in ein möglicherweise besetztes Gleis verwendet wird. Sofern die maximal zulässige Geschwindigkeit in der Betriebsart On-Sight gering (40 km/h) ist, liegt eine Gefährdung vor, wenn das perzeptuelle Systemelement keine Kontrollaktion bezüglich der erkannten

und klassifizierten Objekte liefert. Die Ursachen können dafür beispielsweise in dem zugrundeliegenden Algorithmus (perzeptuelles Systemelement) liegen, aber auch die Sensoren, die nicht verfügbar sind, können fehlende Zustandsdaten verursachen.

Eine weitere relevante Zustandsgröße, deren Nichtverfügbarkeit eine Gefährdung darstellen kann, ist die Information über die Zugintegrität. Wenn keine Rückkopplung der Zugintegrität vorliegt, erfolgt als Fail-Safe Reaktion eine Zwangsbremsung. Im Anschluss könnte das kognitive Systemelement zwar ein Geschwindigkeitsprofil erstellen, jedoch wäre eine Weiterfahrt aufgrund der vorliegenden Gefährdung (Zugtrennung) ohne Erlaubnis nicht sicher.

Da aus der Ferne (TMS, Sicherungslogik oder ATOM) keine Möglichkeit besteht, eine Zugtrennung zu bestätigen, ist eine Zugtrennung unverzüglich dem TMS und der Sicherungslogik sowie dem Systemelement ATOM zu melden. Daher stellt die fehlende Information über die Zugintegrität in eine Gefährdung dar.

Die Sensoren können nicht nur von schlechten Wetterbedingungen beeinflusst werden, sondern sie können auch durch Cyber-Angriffe von außen beeinträchtigt werden. Beispielsweise definiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Kontext des automatisierten Fahrens (aus dem Straßenverkehr) neuartige Cyber-Angriffe (z.B. Adversarial Attacks) auf Sensoren einschließlich des perzeptuellen Systemelements, wodurch die Umgebungsdaten bewusst manipuliert werden können. Ein Beispiel hierfür aus dem Straßenverkehr stellt die bewusste Manipulation eines Verkehrsschildes dar.

Aber auch technologieunabhängige Angriffe von außen (z.B. Graffiti) können die Funktionsweise von Sensoren beeinträchtigen. Durch Graffiti werden Züge oder andere Bahnanlagen mit Farben besprüht. Graffiti hat nicht nur wirtschaftliche Folgen, sondern stellt im vollautomatisierten Bahnbetrieb auch eine Gefährdung dar, wenn die Sensoren derart besprüht werden, dass ihr Sichtfeld durch Besprühung eingeschränkt ist und sie daher keine Zustandsgrößen liefern können.

Während die erwartete Häufigkeit von Gefährdungsursachen aus den Systemelementen mit Ausfallraten abgeschätzt werden kann, ist eine Aussage über die Häufigkeit und Eintrittswahrscheinlichkeit von Cyber-Angriffen nicht möglich. Das bedeutet, dass die oben genannten Systemelemente nicht nur häufig, sondern auch simultan angegriffen werden können.

Ursache: Kommunikationssystem nicht verfügbar

Durch eine fehlende Kommunikation zwischen den ATO geführten Zügen und den infrastrukturseitigen Systemelementen (TMS und Sicherungslogik und ATOM), können auch keine Statusdaten an die infrastrukturseitigen Systemelemente übermittelt werden, sodass die betriebsrelevanten Daten (Journey-Profiles und Segment-Profiles) nicht aktualisiert werden können. Außerdem können aufgrund fehlender Kommunikation auch keine Nothaltaufträge an die ETCS-OBU übermittelt werden, sodass es zu einer Kollision kommen kann. Daher stellt eine fehlende Kommunikation – unabhängig von dem Ort entlang der Eisenbahninfrastruktur und unabhängig den Wetterbedingungen – immer eine Gefährdung dar.

5.7 Zusammenfassung des Hauptkapitels

Ziel dieses Hauptkapitels war es, den Gefährdungsraum im vollautomatisierten Bahnbetrieb systematisch herzuleiten. Dabei bildete die in Kapitel 4.5 hergeleitete funktionale Systemarchitektur einer Zugfahrt im vollautomatisierten Bahnbetrieb eine wesentliche Grundlage für die Gefährdungsanalyse.

Die Herleitung des Gefährdungsraums im vollautomatisierten Bahnbetrieb erfolgte systematisch anhand der STPA-Methode. Da die Gefährdungsanalyse mit der STPA-Methode ein Top-Down Vorgehen ist, wurden zunächst die Schutzziele erarbeitet, bei deren Erfüllung das ATO-System im vollautomatisierten Bahnbetrieb maßgebend mitwirken wird. Denn die nicht Erfüllung der Schutzziele stellt Gefährdungen auf der Bahnsystemebene dar.

Dabei hat sich herausgestellt, dass das ATO-System im vollautomatisierten Bahnbetrieb in Abwesenheit des Triebfahrzeugführers an der Vermeidung einer **Kollision und Entgleisung** während der Fahrt und an der Vermeidung von **Gefährdungen von Zuginsassen** aufgrund eines unerwünschten Stillstands maßgebend beteiligt sein wird. Zudem hat sich herausgestellt, dass diese Schutzziele entweder im Falle eines Stillstands (Weiterfahrt nicht möglich) oder im Falle einer nicht sicheren Weiterfahrt verletzt werden können.

Entsprechend der STPA-Methode wurde in Anlehnung an eine Systematik aus dem autonomen Straßenverkehr ein betrieblicher und umgebungsbedingter Kontext erarbeitet. Dabei wurde eine Mischverkehrsstrecke mit dem Streckenstandard M160 bei der Erarbeitung von Gefährdungsursachen aus den beiden ATO-Regelkreisen zugrunde gelegt. Der betriebliche und umgebungsbedingte Kontext auf dieser Mischverkehrsstrecke wurde mit fahrdynamischen Zuständen der Züge, mit Wetterbedingungen, mit der topographischen Lage der Infrastruktur und mit Bahnanlagen entlang der Infrastruktur beschrieben.

Danach wurden mögliche gefährliche Betriebssituationen und ihre Gefährdungsursachen aus den beiden ATO-Regelkreisen erarbeitet. Mit dem betrieblichen- und umgebungsbedingten Kontext und den Schutzzielen, bei deren Erfüllung das ATO-System mitwirkt, konnten insgesamt 9 gefährliche Betriebssituationen erarbeitet werden, die aus den beiden ATO-Regelkreisen verursacht werden können und daher zu vermeiden sind.

Bei der Erarbeitung von Gefährdungsursachen für die 9 gefährlichen Betriebssituationen aus den beiden ATO-Regelkreisen konnte anhand einer kleinen Beispielrechnung gezeigt werden, dass sehr viele Gefährdungsursachen aus den beiden ATO-Regelkreisen entstehen können, deren Analyse den Rahmen dieser Arbeit sprengen würde. Daher wurde im Rahmen der Gefährdungsanalyse nur der Worst-Case-Fall „Kontrollaktion/Rückkopplung wird nicht ausgeführt bzw. nicht-verfügbar“ herangezogen.

Eine wesentliche Erkenntnis aus der Gefährdungsanalyse ist es, dass die Kommunikationsverbindung zwischen einem Zug und dem TMS oder der ETCS-Zentrale aufgrund der zentralen Systemarchitektur des Bahnbetriebs für eine sichere Zugfahrt unabdingbar ist.

Sofern im vollautomatisierten Bahnbetrieb das Kommunikationssystem nicht verfügbar ist, können davon nicht nur mehrere Züge im Zuständigkeitsbereich gleichzeitig betroffen sein, sondern auch die Funktionen in den infrastrukturseitigen und fahrzeugseitigen Regelkreisen können beeinträchtigt werden. Die Nichtverfügbarkeit des Kommunikationssystems ist eine wesentliche Ursache für die fehlende Übertragung von sicherheitsrelevanten (MA) und betriebsrelevanten Daten (JP/SP).

Da bei fehlender Kommunikation die zentrale Betriebsführung vorübergehend unterbrochen wird, kann auch die bereits in Kapitel 2.5 erläuterte Fernsteuerung über das Systemelement RMTO aus der Leitstelle nicht durchgeführt werden.

Wenngleich hohe Verfügbarkeiten für die Kommunikationssysteme im Bahnbetrieb gefordert werden, stellen Kommunikationssysteme bevorzugte Angriffsziele für Cyberkriminelle dar, weshalb in Zukunft häufiger mit Cyber-Angriffen auf Kommunikationssysteme im Bahnbetrieb gerechnet werden kann.

Für die Entwicklung von betrieblich-technischen Rückfallebenen bedeutet die Nichtverfügbarkeit des Kommunikationssystems, **dass Lösungen für alternative Datenübertragung zwischen Zug und TMS bzw. ETCS-Zentrale erforderlich sind.**

Eine weitere Erkenntnis aus der Gefährdungsanalyse ist es, dass im fahrzeugseitigen ATO-Regelkreis die Sensoren – insbesondere für Ortung und Lichtraumüberwachung – und das perzeptuelle Systemelement kritische Systemelemente darstellen. Im Gegensatz zu den traditionellen softwarebasierten Systemelementen unterliegt das perzeptuelle Systemelement bei der Objekterkennung und Objektklassifizierung stochastischen Unsicherheiten (vgl. Kapitel 2.4). Sofern die Daten des perzeptuellen Systemelements von außen – wie z.B. in Unterkapitel 5.6.2 erwähnt durch Adversarial Attacks – manipuliert werden, kann die Unsicherheit bei dem Output im perzeptuellen Systemelement steigen. Dadurch können auch die nachfolgenden Systemelemente in der hierarchischen Regelungsstruktur ihre Funktionen nicht oder nicht richtig ausführen.

Das Beispiel des perzeptuellen Systemelements zeigt, dass die Ursachen für Gefährdungen im vollautomatisierten Bahnbetrieb nicht nur in hardwarebasierten Systemelementen liegen müssen, sondern auch aufgrund der stochastischen Eigenschaft in den Algorithmen verursacht werden können.

Da neben der Kommunikationsverbindung auch Sensoren bzw. das perzeptuelle Systemelement für eine Fernsteuerung notwendig sind, kann eine Fernsteuerung von außen auf den betroffenen Zug nicht erfolgen, wenn Sensoren oder das perzeptuelle Systemelement nicht verfügbar sind.

Während die systematischen Fehler in traditioneller Software bereits vor der Inbetriebnahme beseitigt werden müssen und daher im laufenden Betrieb keine Fehler – z.B. aufgrund der Alterungsprozesse entstehen können – können Unsicherheiten im perzeptuellen Systemelement zur Laufzeit im vollautomatisierten Bahnbetrieb eine Weiterfahrt oder eine im Vergleich zum Regelbetrieb sicherere Weiterfahrt verhindern.

Für die Entwicklung von betrieblich-technischen Rückfallebenen bedeutet das, **dass neben alternativen Lösungen für hardwarebasierte Störungen (z.B. Sensoren) auch Lösungen für softwarebasierte Störungen erforderlich sind, um insbesondere die Lichtraumüberwachung ersatzweise erfüllen zu können.**

Nicht nur für die Lichtraumüberwachung sind alternative Lösungen erforderlich, sondern auch die Position der Züge und insbesondere die Information über den aktuellen Reibwert sind signifikante Kontrollaktionen für eine sichere Geschwindigkeitsregelung. Die Ursachen für die fehlende Position der Züge und des aktuellen Reibwerts können wiederum in Sensoren aber auch in den zuständigen Algorithmen liegen.

Die hier zusammengefassten Erkenntnisse bilden eine solide Basis, um geeignete betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im nächsten Hauptkapitel entwickeln zu können.

6 Lösungsansätze für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb

6.1 Ziel des Kapitels

Im vorangegangenen Hauptkapitel wurde eine Gefährdungsanalyse auf Basis der in Hauptkapitel 4 hergeleiteten funktionalen Systemarchitektur der Zugfahrt im vollautomatisierten Betrieb durchgeführt, bei der potenziell gefährliche Betriebssituationen im vollautomatisierten Bahnbetrieb systematisch erarbeitet wurden.

Dabei hat sich gezeigt, dass Störungen, die in den beiden ATO-Regelkreisen im vollautomatisierten Bahnbetrieb auftreten können, entweder zu einem Stillstand oder zu einer im Vergleich zum Regelbetrieb unsichereren Weiterfahrt der Züge führen können, sodass dadurch im Falle eines Stillstands insbesondere Zuginsassen gefährdet (vgl. Kapitel 5.4) werden können, während eine im Vergleich zum Regelbetrieb unsicherere Weiterfahrt zu einer Kollision oder zu einer Entgleisung führen kann.

Die Forderung nach betrieblich-technischen Rückfallebenen ist bereits aus dem Kapitel 2.4 bekannt. Um in den gefährlichen Betriebssituationen aus dem Hauptkapitel 5 die ATO relevanten Schutzziele ersatzweise erfüllen zu können, sind betrieblich-technische Rückfallebenen im vollautomatisierten Bahnbetrieb erforderlich.

Auf Basis der Erkenntnisse aus dem Hauptkapitel 5 ist das Ziel dieses Hauptkapitels die Entwicklung von geeigneten betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb.

6.2 Anforderungen an die Entwicklung betrieblich-technischer Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb

Die Anforderungen an die Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb ergeben sich aus den bereits in Kapitel 3.2 zusammengestellten Anforderungen an das Systemverhalten und an die Systemstruktur sowie aus den Grundsätzen einer guten Prozessgestaltung.

Aus dem Kapitel 2.5 ist bekannt, dass betrieblich-technische Rückfallebenen im gegenwärtigen Betrieb als Ersatzverfahren im Vergleich zum Regelbetrieb aufgrund des menschlichen Eingriffs (Betriebspersonal) eine Betriebsführung i.d.R. mit verminderter Sicherheit ermöglichen.

In Anlehnung an die Anforderung aus dem Unterkapitel 3.2.3 – **Sicherheit** hat die höchste Priorität – soll auch bei der Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb die Verminderung der Sicherheit des Betriebs möglichst minimal gehalten werden.

Neben einer hinreichenden Sicherheit in der betrieblich-technischen Rückfallebene wird entsprechend der priorisierten Anforderung aus dem Unterkapitel 3.2.4 **die Fortführung des Betriebs** auch im Falle von Störungssituationen gefordert. Damit soll insbesondere die Abweichung von der vereinbarten Betriebsqualität minimiert werden.

Entsprechend der Grundsätze einer guten Prozessgestaltung aus dem Unterkapitel 3.2.3 sollen die zu entwickelnden betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb möglichst **deterministisch** und **neben- sowie nachwirkungsfrei** sein.

Um die Abweichung von der vereinbarten Betriebsqualität und die Verminderung der Sicherheit zu minimieren, wird eine möglichst kurze **Dauer der Betriebsführung in Störungssituationen** gefordert.

Die Neugestaltung des digitalen Bahnbetriebs zielt u.a. darauf ab, ein nachhaltiges Bahnsystem zu etablieren, das aus Sicht der Betreiber die Wirtschaftlichkeit steigert (vgl. Anforderung aus ERJU in 3.2.3). Das betrifft auch die Gestaltung von Betriebsprozessen für Störungssituationen. Dabei wird konkret gefordert, dass die **Kosten für die Ressourcen,** die in den betrieblich-technischen Rückfallebenen eingesetzt werden, **möglichst niedrig** gehalten werden sollen.

Für schnell migrierbare und langfristige Innovationen für den digitalen Bahnbetrieb wird von den Forschungsinitiativen RCA, OCORA und ERJU sowie aus den Grundsätzen einer guten Prozessgestaltung gefordert (vgl. Unterkapitel 3.2.3), dass die **Komplexität der funktionalen Systemarchitektur des digitalen Bahnbetriebs nicht erhöht** wird, damit eine **Interoperabilität auf europäischer Ebene** erleichtert werden kann (vgl. Unterkapitel 3.2.3). Bei der Interoperabilität steht dabei – wie in Unterkapitel 3.2.3 erläutert – nicht nur die technische Interoperabilität, sondern auch die **betriebliche Interoperabilität** im Fokus. Es soll daher auf Basis der Referenzarchitekturen von RCA und OCORA möglich sein, möglichst **allgemeingültige betrieblich-technische Rückfallebenen** zu entwickeln, die europaweit gültig sind.

Eine weitere Forderung besteht darin, **so wenig wie möglich** und **nur so viel wie nötig** betrieblich-technische Rückfallebenen im vollautomatisierten Bahnbetrieb zu etablieren. Diese Forderung ist insbesondere auf die möglichen Unterhaltungskosten der für die betrieblich-technische Rückfallebenen erforderlichen Ressourcen und auf die mögliche Fehlerhaftigkeit von menschlichen Ressourcen zurückzuführen.

Aufgrund der Tatsache, dass technische Systeme von rascher und kontinuierlicher Entwicklung geprägt sind, wird von den Forschungsinitiativen – zur Sicherstellung von langfristigen Innovationen im digitalen Bahnbetrieb – gefordert, dass auch die betrieblich-technischen Rückfallebenen mit fortschreitender Technologie mitwachsen können. Das führt zu den Forderungen, dass auch die **Betriebsprozesse flexibel** sein sollen.

Schließlich wird auch als eine Anforderung angenommen, dass im vollautomatisierten Bahnbetrieb mindestens eine betrieblich-technische Rückfallebene immer anwendbar (verfügbar) ist, da auch im gegenwärtigen Betrieb immer eine Rückfallebene existiert.

Unter Berücksichtigung dieser Anforderungen werden in diesem Kapitel betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb entwickelt.

6.3 Vorgehensweise bei der Entwicklung von betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb

Aus dem Kapitel 2.5 ist bekannt, dass es derzeit keinen analytischen Ansatz bei der Entwicklung von betrieblich-technischen Rückfallebenen gibt, dem systematisch gefolgt werden kann. Die Abbildung 23 stellt den Ausschnitt der Vorgehensweise innerhalb der globalen Methode dar, der für dieses Hauptkapitel relevant ist.

Damit die betrieblich-technischen Rückfallebenen für den vollautomatisierten Bahnbetrieb im Gegensatz zu den betrieblich-technischen Rückfallebenen für den gegenwärtigen Bahnbetrieb auf Basis einer Systematik entwickelt werden können, wird zunächst in Kapitel 6.4 unter Berücksichtigung der Anforderungen aus dem Kapitel 6.2 – ein systematischer Ansatz hergeleitet.

Die einzelnen Bestandteile des systematischen Ansatzes werden dann in Kapitel 6.5 näher ausgearbeitet. In Folge der in Kapitel 6.4 gewonnenen Erkenntnisse, wird hierzu ein Konzept der dynamischen Adaption der Systemarchitektur zur Laufzeit erarbeitet.

Anschließend werden in Kapitel 6.6 für die in Kapitel 5.7 erarbeiteten Betriebssituationen im vollautomatisierten Bahnbetrieb beispielhafte betrieblich-technische Rückfallebenen auf Basis des zuvor in Kapitel 6.5 erarbeiteten Konzepts der dynamischen Adaption ausgearbeitet. Die Zusammenfassung des Hauptkapitels ist in Kapitel 6.7 zu finden.

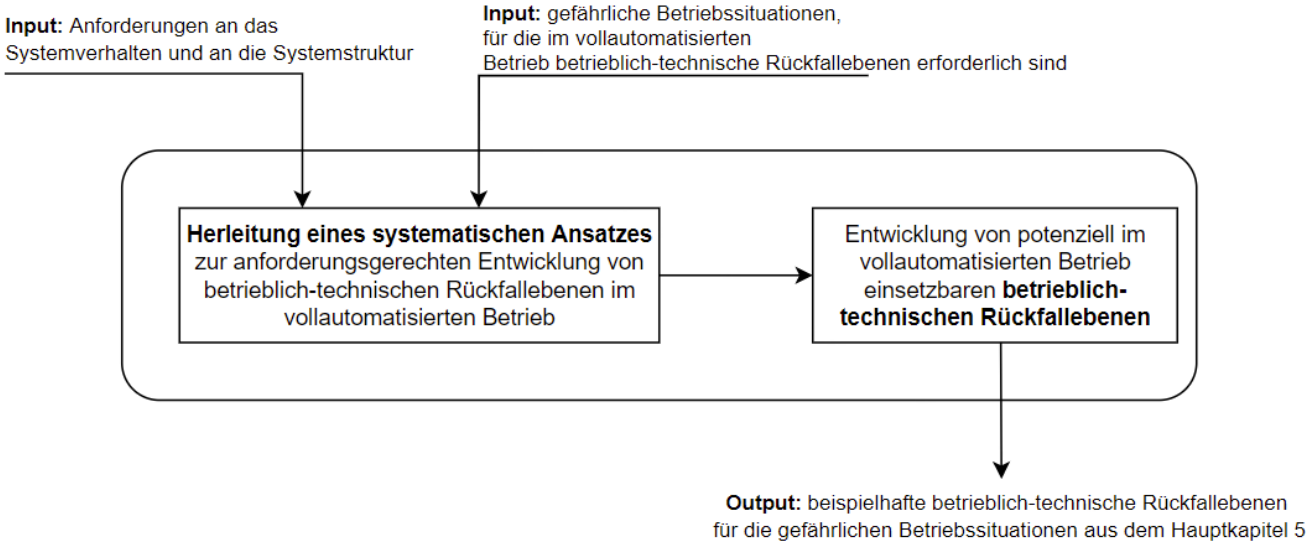

Abbildung 23 Ausschnitt aus der globalen Methode aus Kapitel 3.3 zur Entwicklung von betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb

6.4 Herleitung eines systematischen Ansatzes zur anforderungsgerechten Entwicklung von betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb

In diesem Kapitel wird ein systematischer Ansatz erarbeitet, mit dem betrieblich-technische Rückfallebenen im vollautomatisierten Bahnbetrieb gestaltet werden können.

Aus dem gegenwärtigen Bahnbetrieb ist bekannt, dass die sicherheitsrelevanten technischen Systeme in der Systemarchitektur redundant ausgelegt (z.B. zwei Glühlampen am Signal oder Stellwerksrechner mit 2 aus 3 Redundanz) sind. Aufgrund des Betriebskontinuitätsmanagements sind zusätzlich die bereits in Kapitel 2.4 vorgestellten betrieblich-technischen Rückfallebenen vorhanden.

Entsprechend des GAMAB-Prinzips (Generell mindestens so gut) nach *DIN EN 50126-2:2017* sollte der vollautomatisierte Bahnbetrieb mindestens den Sicherheitsstand aus dem gegenwärtigen Bahnbetrieb erfüllen. Daher sind sowohl technische Redundanzen als auch betrieblich-technische Rückfallebenen erforderlich.

Technische Rückfallebenen in Form von Redundanzen können zur Erhöhung der Zuverlässigkeit und der Verfügbarkeit des vollautomatisierten Bahnbetriebs in die Systemarchitektur integriert werden. Jeder Betreiber kann aus der Referenzarchitektur von RCA bzw. OCORA die eigene physikalische Systemarchitektur einschließlich der technischen Redundanzen entwickeln. Da die Spezifikation der Referenzarchitektur von RCA bzw. OCORA noch nicht endgültig abgeschlossen ist, kann im aktuellen Stand der Arbeit auch keine Entscheidung über die Art und Anzahl von technischen Redundanzen

getroffen werden. Daher stehen – auch in Anlehnung an die inhaltliche Abgrenzung aus dem Kapitel 3.5 – technische Rückfallebenen in Form von Redundanzen nicht im Fokus dieses Hauptkapitels.

Wie bereits in Kapitel 2.4 erläutert, kommt es im Kern der gegenwärtigen betrieblich-technischen Rückfallebene neben der zwischenmenschlichen Kommunikation auch auf die Planungsfähigkeit des Menschen an. Mit der Planung werden Maßnahmen und mögliche Handlungsalternativen anhand der vorliegenden Störung und der Handlungsregeln der Richtlinien (z.B. Ril 408 und 418) abgewogen und zu der aktuellen Störungssituation passende Maßnahmen und Handlungen ausgewählt.

Durch den Wegfall der Triebfahrzeugführer im vollautomatisierten Bahnbetrieb ändern sich die Systemstruktur und das Systemverhalten entsprechend der funktionalen Systemarchitektur aus dem Kapitel 4.5. Jedes Systemelement in der funktionalen Systemarchitektur erfüllt dabei eine bestimmte betriebliche Funktion, um eine sichere Zugfahrt durchführen zu können. Es können aber auch mehrere Systemelemente zur Erfüllung einer betrieblichen Funktion sich die Funktionen teilen. Beispielsweise wird die Lichtraumüberwachung als betriebliche Funktion durch Sensoren und durch die entsprechenden Softwareanwendungen erfüllt. Zum Wegfall des Triebfahrzeugführers kommt im vollautomatisierten Bahnbetrieb der Wegfall des Fahrdienstleiters, dessen Aufgaben die Sicherungslogik (vgl. Kapitel 4.5) übernimmt.

Da die beiden wesentlichen menschlichen Ressourcen (Fahrdienstleiter und Triebfahrzeugführer) während einer Zugfahrt im vollautomatisierten Bahnbetrieb nicht mehr wie in der aktuellen Form fungieren werden, können auch die betrieblich-technischen Rückfallebenen aus dem gegenwärtigen Bahnbetrieb in ihrer aktuellen Form im vollautomatisierten Bahnbetrieb nicht angewandt werden.

Ausgehend von der Annahme, dass der vollautomatisierte Bahnbetrieb im Regelbetrieb den höchsten Automatisierungsgrad (GoA4 bei Güterzügen und GoA3 bei Personenzügen) aufweist und der Tatsache, dass Fahrdienstleiter und Triebfahrzeugführer im vollautomatisierten Bahnbetrieb nicht mehr wie in der aktuellen Form fungieren, sind die im Weiteren vorgestellten Ansätze für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb denkbar.

Zum einen ist es denkbar, im Falle von Störungen an technischen Systemen den Fail-Safe Zustand zu erzwingen und die Verantwortung über die fortzuführende Zugfahrt an eine menschliche Ressource (Betriebspersonal) zu übertagen. Das bedeutet, dass der vollautomatisierte Bahnbetrieb von GoA4 bzw. GoA3 auf GoA1 oder GoA2 zurückfällt. Dieser Ansatz wird bereits bei Nahverkehrssystemen angewandt und wurde auch in Unterkapitel 2.4.4 einschließlich seiner Nachteile vorgestellt.

Damit der vollautomatisierte Bahnbetrieb nicht jedes Mal im Falle von Störungen auf fehleranfällige (insbesondere in Stresssituationen) menschliche Ressourcen zurückfällt, können zum anderen die betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb auch derart gestaltet werden, dass die menschlichen Ressourcen in Störungssituationen von den technischen Systemen weitgehend unterstützt werden. Hierbei ist es beispielsweise denkbar, dass ein GoA4 geführter Güterzug im Falle von Störungssituationen eine menschliche Ressource zur Übernahme der Steuerung auffordert. Da jedoch entsprechend der Definition des Automatisierungsbegriffs im Schienenverkehr bei GoA4 geführten Güterzügen kein Betriebspersonal vorhanden ist, muss der Güterzug eine externe menschliche Ressource auffordern, die Steuerung zu übernehmen. Bei GoA3 geführten Personenzügen ist hingegen die Aufforderung eines Zugpersonals zur Übernahme der Steuerung möglich *(vgl. Üyümez 2019)*.

Neben den beiden Ansätzen, bei denen die Verantwortung einer Zugfahrt im Falle von Störungssituationen vollständig auf eine menschliche Ressource (z.B. Zugpersonal) übertragen wird, ist

es außerdem denkbar, dass im Falle von Störungssituationen der Automatisierungsgrad aus dem Regelbetrieb (d.h. GoA4 bei Güterzügen und GoA3 bei Personenzügen) beibehalten wird und die betrieblich-technischen Rückfallebenen automatisiert ablaufen.

Der Rückfall von GoA4 bzw. GoA3 auf GoA1 oder GoA2 im Falle von Störungssituationen bietet zwar den Vorteil, dass sich das Betriebspersonal aufgrund der inhärenten Intelligenz an unbekannte Situationen flexibel anpassen kann. Trotz der Anpassungsfähigkeit des Betriebspersonals erfolgt jedoch die Betriebsführung in Störungssituationen unter einem Zeitdruck, weshalb die Sicherheit der Betriebsführung aufgrund der erhöhten Fehleranfälligkeit des Betriebspersonals darunter leiden könnte. Im Vergleich zu Nahverkehrssystemen erfolgt zudem die Betriebsführung bei Vollbahnen über größere geographische Entfernungen. Daher würde das Betriebspersonal länger brauchen, um einen gestörten Zug (z.B. auf der freien Strecke) zu erreichen und dadurch die Anforderung aus dem Kapitel 6.2 hinsichtlich der möglichst kurzen Dauer der Betriebsführung in Störungssituationen nicht erfüllen. Zudem erfordert der Rückfall von GoA4 bzw. GoA3 auf GoA1 oder GoA2 viel Betriebspersonal. Betriebspersonal verursacht nicht nur Kosten, sondern es kann auch altersbedingt zu Personalfluktuation kommen.

Da die Systemarchitektur des digitalen Bahnbetriebs entsprechend der Anforderung von RCA und OCORA aus dem Kapitel 3.3 modular sein soll, wodurch die technischen Systeme darin flexibel ausgetauscht (Plug & Play) bzw. in ihrem Funktionsumfang erweitert bzw. reduziert werden können, müsste sich das Betriebspersonal jedes Mal in Störungssituationen aufgrund von neuen betrieblichen Regeln zum Umgang mit den neuen technischen Systemen neu zurechtfinden. Die ständige Anpassung der betrieblichen Regeln für das Betriebspersonal in Abhängigkeit der Systemarchitektur erfüllt die Anforderung hinsichtlich der betrieblichen Interoperabilität nicht.

Um einen vollständigen Rückfall auf das Betriebspersonal im Falle von Störungssituationen aufgrund der oben genannten Überlegungen zu vermeiden, können die betrieblich-technischen Rückfallebenen – ausgehend von den Anforderungen der RCA und OCORA an die technischen Systeme im vollautomatisierten Bahnbetrieb – auch automatisiert ablaufen. Im Weiteren werden ausgehend von den Anforderungen der RCA und OCORA einige sogenannte „Enabler“ beschrieben, die einen automatisierten Ablauf von betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb ermöglichen würden.

Entsprechend der Spezifikation nach RCA und OCORA werden die softwarebasierten Systemelemente (Softwareanwendungen) aus der in Kapitel 4.5 hergeleiteten funktionalen Systemarchitektur auf einer sogenannten sicheren Rechenplattform (Safe Computing Plattform, CCU) laufen.

Außerdem sollen mit der einheitlichen Rechenplattform die Anwendungen von der zugrundeliegenden Rechenplattform entkoppelt werden, wodurch eine schnelle und flexible Austauschbarkeit (Plug & Play) von Softwareanwendungen angestrebt wird.

Entsprechend der OCORA Spezifikation sollen die Softwareanwendungen über den Communication Stack der Laufzeitumgebung nach dem Publish & Subscribe Kommunikationsprotokoll, das detailliert in *(Tanenbaum und Van Steen 2007, S. 589ff)* erläutert wird, miteinander kommunizieren. Die hardwarebasierten Systemelemente sind an die bereits in Kapitel 2.3 vorgestellte Busstruktur im Fahrzeug angebunden (engl., Universal Vehicle Command and Control Bus, UVCCB) und kommunizieren über das sogenannte Train Real Time Data Protocol (TRDP 2.0). Abbildung 24 stellt die

abstrakte Darstellung der modularen Integration der softwarebasierten und hardwarebasierten Systemelemente auf der sicheren Rechenplattform dar.

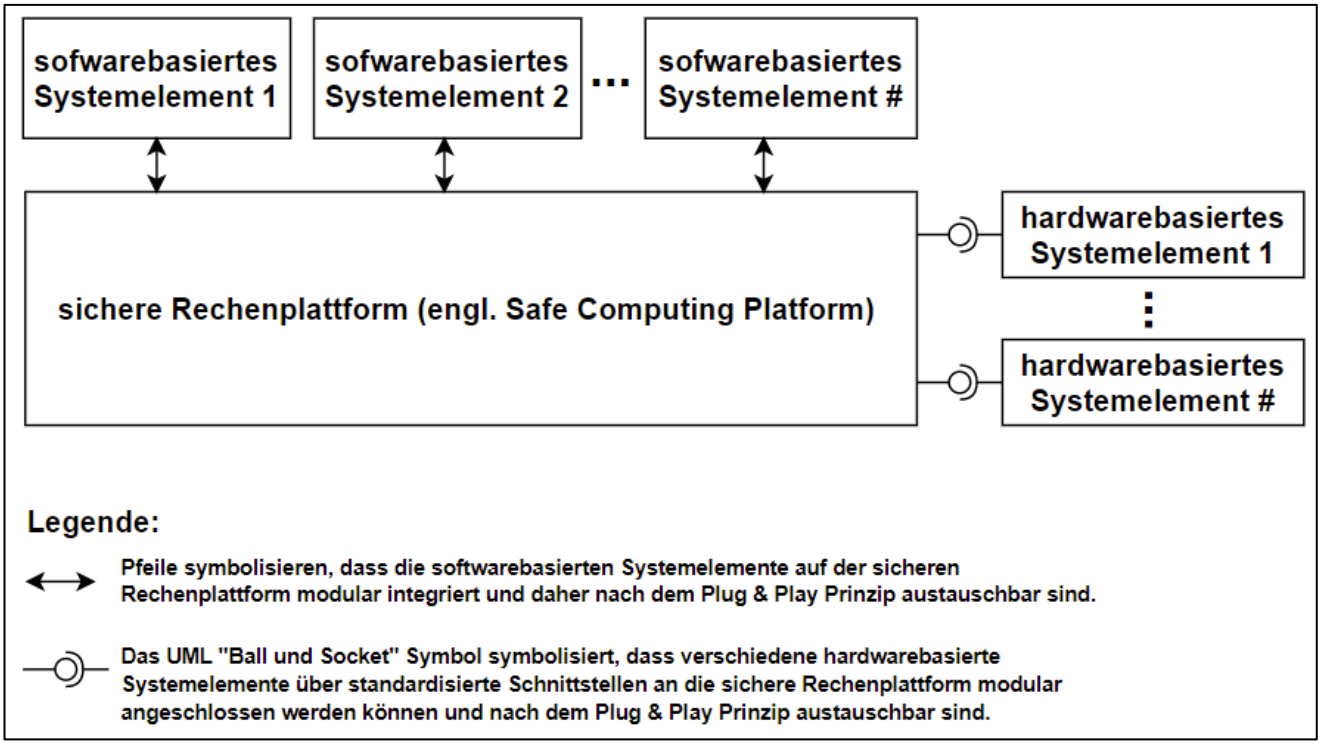

Abbildung 24 abstrakte Darstellung der modularen Integration der softwarebasierten und hardwarebasierten Systemelemente auf der sicheren Rechenplattform

Sofern im Falle von Störungssituationen die Systemelemente ihren Zustand ändern und daher ihre beabsichtigten Funktionen nicht mehr erfüllen können, kann es vorkommen, dass darunter auch ein zu erfüllendes Schutzziel leidet. Durch die Änderung einer Eigenschaft in einem Systemelement kann die für den Regelbetrieb geforderte Systemarchitekturkonfiguration nicht mehr sichergestellt werden.

Statt im Falle einer Störungssituation vollständig auf eine menschliche Ressource zurückzufallen, können sich die Systemelemente aufgrund der genannten „Enabler“ situationsabhängig und automatisiert an die Betriebsbedingung anpassen (dynamische Adaption zur Laufzeit), sodass die Zugfahrt mit einer vorübergehend neuen Systemarchitekturkonfiguration durchgeführt werden kann, um das entsprechende Schutzziel zu erfüllen.

Durch eine situationsabhängige und automatisierte Anpassung der Systemarchitektur zur Laufzeit müssen nationale Bahnbetreiber keine proprietären Lösungen für den Umgang mit Störungssituationen entwickeln, bei denen das Betriebspersonal vollständig die Verantwortung in Störungssituationen trägt. Dadurch wird insbesondere die betriebliche Interoperabilität erleichtert.

Mit einer dynamischen Adaption zur Laufzeit ist es zudem möglich, eine vorübergehend neue Systemarchitekturkonfiguration – auch unter Einbindung einer menschlichen Ressource – zu erstellen.

Dadurch kann auf der einen Seite bei GoA3 geführten Personenzügen das Zugpersonal in die neue Systemarchitekturkonfiguration vorübergehend eingebunden und auf der anderen Seite bei GoA4 geführten Güterzügen die betrieblich-technischen Rückfallebenen mit der neuen Systemarchitekturkonfiguration vollständig automatisiert ablaufen.

Ausgehend von den Enablern und den zugehörigen Überlegungen wird von dem Autor als systematischer Ansatz eine **dynamische Adaption der Systemarchitektur zur Laufzeit** für die Einrichtung von betrieblich-technischen Rückfallebenen vorgeschlagen.

Die in den Forschungsinitiativen geforderten und oben genannten Enabler sind in der Abbildung 25 als Input für die Entwicklung des Konzepts einer dynamischen Adaption der Systemarchitektur zur Einrichtung von betrieblich-technischen Rückfallebene zur Laufzeit dargestellt. In den folgenden Kapiteln werden diese Enabler und die Anforderungen aus dem Kapitel 6.2 herangezogen, um das Konzept einer dynamischen Adaption der Systemarchitektur zur Einrichtung von betrieblich-technischen Rückfallebene zur Laufzeit zu erarbeiten.

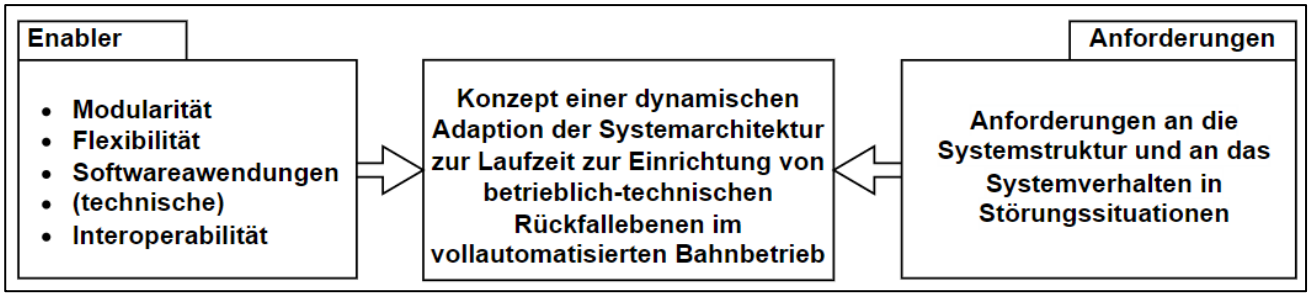

Abbildung 25 Enabler und Anforderungen für eine dynamische Adaption der Systemarchitektur zur Laufzeit

6.5 Konzept einer dynamischen Adaption der Systemarchitektur zur Einrichtung von betrieblich-technischen Rückfallebene zur Laufzeit

Das Ziel dieses Kapitels ist die Erarbeitung eines Konzepts für den im vorigen Kapitel als zielführend bestimmten systematischen Ansatz der dynamischen Adaption der Systemarchitektur zur Einrichtung von betrieblich-technischen Rückfallebene zur Laufzeit.

Die Systemarchitektur des digitalen Bahnbetriebs umfasst hardwarebasierte und softwarebasierte Systemelemente. Damit eine dynamische Adaption der Systemarchitektur zur Laufzeit erfolgen kann, muss das Konzept der dynamischen Adaption zum einen die möglichen Arten von dynamischer Adaption zur Laufzeit bei hardwarebasierten und softwarebasierten Systemelementen umfassen. Daher werden zunächst in Unterkapitel 6.5.1 die möglichen Arten der dynamischen Adaption zur Laufzeit hergeleitet.

Entsprechend der RCA-Referenzarchitektur weist der gegenwärtige Bahnbetrieb eine zentrale Betriebsführung auf. Dabei hat das EIU die Entscheidungshoheit bei der Einrichtung von betrieblich-technischen Rückfallebenen. Damit die dynamische Adaption zur Laufzeit weitgehend automatisiert, aber zugleich koordiniert ablaufen kann, muss das Konzept der dynamischen Adaption zum anderen eine koordinierende Ressource vorsehen. Die koordinierende Ressource für die dynamische Adaption zur Laufzeit wird in Unterkapitel 6.5.2 erarbeitet.

Wie bereits in Unterkapitel 2.4.3 erläutert, beschreibt der Übergang vom Regelbetrieb in eine betrieblich-technische Rückfallebene einen Prozess. Damit der Übergang vom Regelbetrieb in die betrieblich-technische Rückfallebene auch im vollautomatisierten Bahnbetrieb weitgehend automatisiert erfolgen kann, muss das Konzept der dynamischen Adaption außerdem den Ablauf für die jeweilige dynamische Adaptionsart umfassen, der entsprechend den Anforderungen aus dem Kapitel 6.2 nach bestimmten Designprinzipien erfolgen muss. Als sinnvolle Vorgehensweise zur Herleitung des Ablaufs der jeweiligen Adaptionsart eignet es sich, zunächst die Designprinzipien zu erarbeiten.

Dadurch ist es möglich, den Ablauf der jeweiligen dynamischen Adaptionsart anforderungsgerecht und möglichst generisch zu entwickeln. Die Erarbeitung von möglichen Designprinzipien erfolgt in Unterkapitel 6.5.3. Anschließend wird der Ablauf der jeweiligen dynamischen Adaptionsart in Unterkapitel 6.5.4 erarbeitet.

6.5.1 Arten von dynamischer Adaption zur Laufzeit

Das Ziel dieses Unterkapitels ist es, die möglichen Arten einer dynamischen Adaption zur Laufzeit herzuleiten. Da die Systemarchitektur des digitalen Bahnbetriebs noch nicht final spezifiziert ist, dient die in Kapitel 4.5 hergeleitete funktionale Systemarchitektur der Zugfahrt im vollautomatisierten Bahnbetrieb als Grundlage für die herzuleitenden Adaptionsarten.

Wie bereits in Kapitel 6.4 erwähnt, können zur Erfüllung von betrieblichen Funktionen

- hardwarebasierte Systemelemente,
- softwarebasierte Systemelemente (Softwareanwendungen) oder
- hardware- und softwarebasierte Systemelemente

eingesetzt werden.

In Anlehnung an die Ergebnisse aus dem Kapitel 5.7 können Störungen und somit Gefährdungsursachen sowohl aus hardwarebasierten als auch aus softwarebasierten Systemelementen entstehen. Folglich können Adaptionen zur Laufzeit in hardware- und/oder in softwarebasierten Systemelementen vorgenommen werden. Bevor die möglichen Adaptionsarten hergeleitet werden, wird sowohl bei hardwarebasierten als auch bei softwarebasierten Systemelementen die Annahme getroffen, dass ein Neustartversuch im Falle von Störungen nicht erfolgreich ist und dass die Störungen zuverlässig offenbart werden *(vgl. DIN EN 50129:2018)*.

Hardwarebasierte Systemelemente sind über standardisierte Schnittstellen mit anderen hardwarebasierten Systemelementen verbunden und erfüllen somit die Form Fit Function Interface Specification (FFFIS). Die dynamische Adaption von hardwarebasierten Systemelementen kann aufgrund der Plug & Play Eigenschaft und in Anlehnung an die Definition der Modularität aus dem Kapitel 3.6 durch **Ersetzen** oder durch **Deaktivierung** erfolgen.

Sofern sich im hardwarebasierten Systemelement aufgrund einer Störung die Eigenschaften aus dem formalen Tupel (vgl. Kapitel 6.4) geändert haben, kann dieses durch ein alternatives hardwarebasiertes Systemelement ersetzt werden. Wenngleich der Zustand des gestörten hardwarebasierten Systemelements vorübergehend z.B. auf „ersetzen“ wechselt und daher keine Inputs verarbeitet und auch keine Outputs generiert werden können, kehrt der Zustand des alternativen hardwarebasierten Systemelements nach dem Ersetzen zurück zu „aktiv“ und es können Inputs und Outputs wieder verarbeitet bzw. generiert werden.

Das Ersetzen des gestörten hardwarebasierten Systemelements käme dann in Frage, wenn ein alternatives hardwarebasiertes Systemelement zur Laufzeit bereitgestellt werden kann. Entsprechend der Forschungsinitiative OCORA werden die fahrzeugseitigen Softwareanwendungen weitgehend auf der CCU-Rechenplattform laufen, deren Integration einschließlich der technischen Redundanz die Aufgabe der Betreiber ist.

Entsprechend der Anforderung von OCORA ist zwar davon auszugehen, dass die Rechenplattform redundant integriert wird, jedoch sind Art und Umfang der technischen Redundanz abhängig von

Betreiber und daher noch ungewiss. Die Integration der technischen Redundanz ist nicht nur kostenintensiv, sondern erfordert auch mehr Platzbedarf in den Zügen und erhöht zudem die Komplexität der Systemarchitektur. Daher ist bei der Entscheidung für technische Redundanzen eine entsprechende Bewertung erforderlich.

Neben der CCU-Rechenplattform gibt es auch andere hardwarebasierte Systemelemente, die ebenfalls redundant ausgelegt werden können. Dazu gehören beispielsweise die verschiedenen Sensorsysteme am Zug. Um jedoch die Kosten im vollautomatisierten Bahnbetrieb nicht zu erhöhen und den begrenzten Platz in den Zügen nicht für technische Systeme zu beanspruchen, können sich Betreiber dafür entscheiden, nicht alle hardwarebasierten Systemelemente redundant auszulegen.

Durch gezielte Auswahl von technischen Redundanzen können zwar Kosten im vollautomatisierten Bahnbetrieb reduziert werden, jedoch sind zur Lösung des Zielkonflikts aus dem Kapitel 1.2 – schnelle Reaktion auf Störungssituationen auch ohne technische Redundanzen, um die Betriebsqualität nicht zu beeinträchtigen – betrieblich-technische Rückfallebenen erforderlich.

Denn im laufenden Betrieb könnte es vorkommen, dass das nicht redundant ausgelegte hardwarebasierte Systemelement gestört ist, sodass das Ersetzen zur Laufzeit nicht möglich wäre, da das Ersetzen von hardwarebasierten Systemelementen einen physikalischen Eingriff für Demontage und Montage von außen erfordert. Der Prozess des Ersetzens eines nicht redundant ausgelegten hardwarebasierten Systemelements kann im Zweifelsfall lange dauern. In Anlehnung an die Anforderung aus dem Kapitel 6.2, dass die betrieblich-technischen Rückfallebenen möglichst kurz dauern sollen, wäre das Ersetzen eines gestörten hardwarebasierten Systemelements zur Laufzeit durch ein alternatives hardwarebasiertes Systemelement daher nicht anforderungsgerecht.

Im Gegensatz zum Ersetzen liefert das entsprechende hardwarebasierte Systemelement bei der Deaktivierung keine Outputs und kann auch keine Inputs verarbeiten. Der Zustand des hardwarebasierten Systemelements ändert sich z.B. zu „deaktiviert“. Eine derartige Deaktivierung im Falle von Störungen ist auch entsprechend den Normen EN 50128 und EN 50129 wegen der Vermeidung von Fehlerfortpflanzung auf andere Systemelemente gefordert. Ein Beispiel für Deaktivierung von hardwarebasierten Systemelementen im vollautomatisierten Bahnbetrieb wären gestörte Sensoren, die deaktiviert werden, um keine fehlerhaften Rohdaten an die benachbarten technischen Systeme (z.B. perzeptuelles Systemelement) zu übermitteln.

Bei der Deaktivierung kann daher die entsprechende betriebliche Funktion, die durch das hardwarebasierte Systemelement im Regelbetrieb übernommen wurde, vorübergehend nicht mehr erfüllt werden (**Deaktivierung ohne Funktionsallokation**). Beispielsweise wird im Falle einer Sensorstörung (z.B. Kamerasensor) der Kamerasensor deaktiviert und der Betrieb mit den verbleibenden Sensoren (z.B. Lidar und Radar) weitergeführt. Eine Deaktivierung ohne Funktionsallokation könnte jedoch Auswirkungen auf die tolerierbare Gefährdungsrate haben, sofern die tolerierbare Gefährdungsrate einer betrieblichen Funktion auf mehrere Systemelemente aufgeteilt ist. Denn durch die Deaktivierung ohne Funktionsallokation kann die für den Regelbetrieb spezifizierte tolerierbare Gefährdungsrate nicht mehr eingehalten werden.

Um in Störungssituationen weiterhin die entsprechende betriebliche Funktion erfüllen zu können, gibt es bei einer Deaktivierung auch die Möglichkeit, die betriebliche Funktion des deaktivierten hardwarebasierten Systemelements an eine andere Ressource zu übertragen (**Deaktivierung mit Funktionsallokation**). Beispielsweise kann im Falle einer Sensorstörung (z.B. Kamerasensor) die Kamerafunktion auf andere Ressource allokiert werden, statt auf diese komplett zu verzichten. Deaktivierung mit Funktionsallokation bedeutet also, dass eine andere Ressource mit der gleichen

Fähigkeit die betriebliche Funktion übernimmt. Dabei kann die betriebliche Funktion auf ein anderes hardwarebasiertes Systemelement oder auf ein Betriebspersonal allokiert werden, sofern letzteres involviert werden kann. Während beim Ersetzen die Schnittstelle des ersetzten Systemelements nicht modifiziert wird, wird bei der Deaktivierung mit Funktionsallokation die Schnittstelle des deaktivierten Systemelements auch modifiziert. Der genaue Ablauf für eine Deaktivierung mit und ohne Funktionsallokation erfolgt in Unterkapitel 6.5.4.

Da auch Softwareanwendungen entsprechend der OCORA Spezifikation modular entwickelt werden sollen, gelten die beiden Adaptionsarten Ersetzen und Deaktivierung auch für Softwareanwendungen. Anders als bei hardwarebasierten Systemelementen kann bei Softwareanwendungen das Ersetzen zur Laufzeit durchgeführt werden. Hierbei ist es möglich, eine alternative Softwareanwendung mit der gleichen Fähigkeit auf die gleiche Rechenplattform zur Laufzeit einzuspielen und dabei die gestörte Softwareanwendung zu ersetzen. Der genaue Ablauf dazu erfolgt in Unterkapitel 6.5.3.

Beim Ersetzen einer Softwareanwendung muss die alternative Softwareanwendung nicht notwendigerweise eine Funktionserweiterung (Upgrade) beinhalten, sondern es ist ausreichend, wenn mit der alternativen Softwareanwendung lediglich die zu erfüllenden Funktionen bereitgestellt wird, sodass die betriebliche Funktion erfüllt werden kann. In Abhängigkeit davon, wie die Granularität der Modularisierung bei den Herstellern der jeweiligen Softwareanwendungen ist, kann auch eine Softwareanwendung mehrere kleine Anwendungen beinhalten. Beispielsweise könnte die Softwareanwendung des perzeptuellen Systemelements die Anwendungen Sensordatenfusion, Objekterkennung und Objektklassifizierung beinhalten. Es wäre demnach auch möglich, diese Anwendungen unabhängig voneinander zu ersetzen (teilweise Deaktivierung). Dadurch wird nicht die komplette Softwareanwendung deaktiviert, sondern aufgrund der Degradierung erfüllt sie ihre Funktionen nicht mehr wie ursprünglich für den Regelbetrieb spezifiziert.

Bei der Deaktivierung von Softwareanwendungen werden wie bei hardwarebasierten Systemelementen keine Inputs verarbeitet und keine Outputs generiert. Dadurch können andere Softwareanwendungen, die Daten mit der deaktivierten Softwareanwendung austauschen, nicht bedient werden. Auch hierbei ist eine Deaktivierung mit und ohne Funktionsallokation möglich.

Die möglichen Arten der dynamischen Adaption in hardwarebasierten und softwarebasierten Systemelementen ist in der Abbildung 26 dargestellt. Während beim Ersetzen einer Softwareanwendung eine funktionelle Rekonfiguration vorliegt, handelt es sich bei der Deaktivierung (sowohl bei hardwarebasierten als auch softwarebasierten Systemelementen) mit oder ohne Funktionsallokation um eine strukturelle und funktionelle Rekonfiguration. Eine strukturelle und funktionelle Rekonfiguration wird im weiteren Verlauf der Arbeit als kompositionale Anpassung bezeichnet.

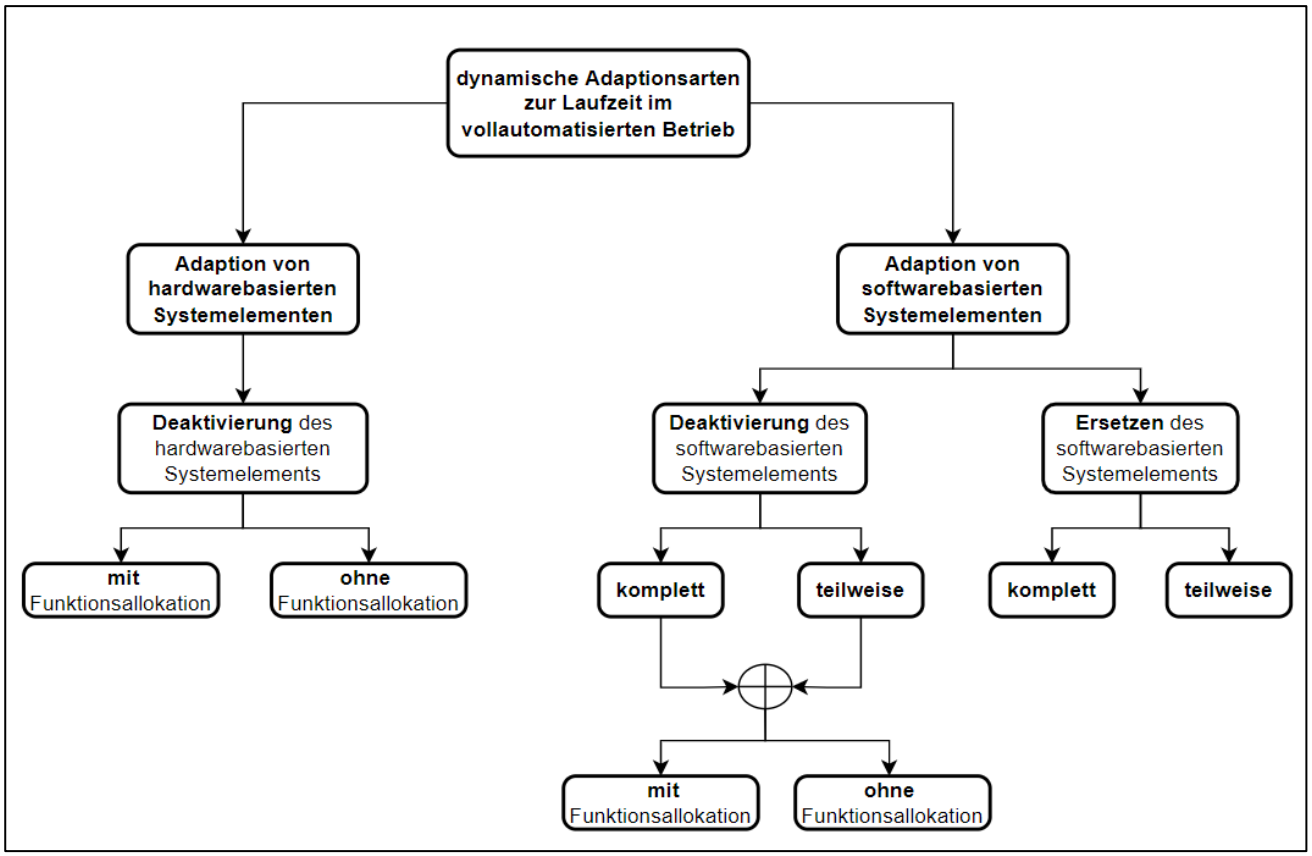

Abbildung 26 Arten von dynamischer Adaption zur Laufzeit im vollautomatisierten Bahnbetrieb

6.5.2 Verantwortliche Ressource für eine koordinierte dynamische Adaption

Nachdem nun die möglichen Adaptionsarten für hardwarebasierte und softwarebasierte Systemelemente im vorigen Unterkapitel hergeleitet wurden, ist es bei einer dynamischen Adaption zur Laufzeit auch von hoher Relevanz, durch welche Ressource eine derartige Adaption initiiert und auch koordiniert wird. Denn – wie bereits in Kapitel 2.4 erläutert – erfolgt die Betriebsführung in gegenwärtigen Störungssituationen durch eine intensive Zusammenarbeit zwischen Fahrdienstleiter und Triebfahrzeugführer. Dabei hat ein Fahrdienstleiter eine übergeordnete Befugnis als ein Triebfahrzeugführer, sodass er als koordinierendes Personal fungiert. In diesem Unterkapitel wird daher eine mögliche Ressource, die während einer vollautomatisierten Zugfahrt die dynamische Adaption zur Laufzeit koordinieren könnte, erarbeitet.

Wie bereits aus dem Kapitel 2.3 bekannt, wird im vollautomatisierten Bahnbetrieb ein Triebfahrzeugführer durch technische Systeme, die in Kapitel 4.5 hergeleitet wurden, ersetzt. Wie bereits in Kapitel 6.4 erläutert, ist es mit der Einführung der neuen Sicherungslogik auch zu erwarten, dass die Fahrdienstleiter – zumindest in ihrer aktuellen Rolle – wegfallen werden *(vgl. Düpmeier 2022)*. Damit im vollautomatisierten Bahnbetrieb betrieblich-technische Rückfallebenen durch dynamische Adaption zur Laufzeit eingerichtet werden können, sind Überlegungen dafür erforderlich, durch welche Ressource eine derartige Adaption initiiert und auch koordiniert werden kann und wo diese Ressource in der Systemarchitektur eingeordnet werden sollte. Im Weiteren wird daher eine mögliche Ressource, die während einer Zugfahrt die dynamische Adaption zur Laufzeit koordinieren kann, erarbeitet.

Im Bahnbetrieb liegt – auch in Anlehnung an die Referenzarchitekturen von RCA und OCORA– eine zentralisierte Betriebsführung vor. Wenngleich die Zusammenarbeit zwischen EIU und EVU bereits heute in Störungssituationen unabdingbar ist (vgl. Interaktion zwischen Tf und Fdl), hat das EIU bei der Gestaltung und Durchführung von betrieblich-technischen Rückfallebenen die Entscheidungshoheit. Prinzipiell kann dieser Gedanke auch im vollautomatisierten Bahnbetrieb weitergeführt werden, sodass die dynamische Adaption der Systemarchitektur durch eine Ressource, die in EIU-Entscheidungshoheit liegt, koordiniert wird. Ein wesentliches Argument dafür ist, dass die EIUs gemäß der Ril 405 für eine gerechte Nutzung der Infrastruktur durch die Kunden (EVUs) bei einer vereinbarten Betriebsqualität verantwortlich sind. Das hat zur Folge, dass sie den Prozess der dynamischen Adaption unter Berücksichtigung der Sicherheit und der vereinbarten Betriebsqualität gestalten können. Aufgrund der Möglichkeit, betrieblich-technische Rückfallebenen einheitlich aus „einer Hand“ bereitzustellen, kann insbesondere die von ERJU geforderte betriebliche Interoperabilität erreicht werden. Deshalb ist auch die Forderung von RCA in *EUG (2020b)*, dass die Infrastrukturbetreiber nach der Implementierung ihrer Systemarchitektur für die entsprechenden betrieblich-technischen Rückfallebenen verantwortlich sind, erfüllt.

Durch den Wegfall von Fahrdienstleitern stellt sich jedoch die Frage, welche Ressourcen aus der hierarchischen Regelungsstruktur, die der EIU-Entscheidungshoheit unterliegen, als Koordinator der dynamischen Adaption in Frage kommen. Die hierarchische Regelungsstruktur aus dem Kapitel 4.5 mit den Systemelementen, die potenziell als koordinierende Ressource in Frage kommen könnten, ist in der Abbildung 27 dargestellt.

In der hierarchischen Regelungsstruktur gehören das TMS (einschließlich ATO-AT und ATO-AE), die Sicherungslogik und die ETCS-Zentrale entsprechend des Kapitels 2.3 zu den infrastrukturseitigen Systemelementen der EIU. Demnach könnte prinzipiell die Koordinierungsaufgabe auf das TMS allokiert werden. Ein wesentliches Argument dafür, dass das TMS die Koordinierungsaufgabe übernehmen kann, ist, dass es sowohl zum infrastrukturseitigen ATO-System als auch zur sicherheitskritischen Sicherungslogik eine Schnittstelle aufweist und daher die für die dynamische Adaption erforderlichen Informationen aus unterschiedlichen Quellen einholen kann, ohne dafür eine zusätzliche Schnittstelle einrichten zu müssen. Die Koordinierungsaufgabe während der dynamischen Adaption könnte auch von dem TMS auf das infrastrukturseitige ATO-System (ATO-AT oder ATO-AE), das in der nächsten Hierarchieebene angeordnet ist, ausgelagert werden. Das infrastrukturseitige ATO-System hat jedoch keine Schnittstelle zur Sicherungslogik. Um eine neue Schnittstelle – auch wegen der Forderung hinsichtlich der Rückwirkungsfreiheit – und eine doppelte Datenhaltung sowie erhöhte Komplexität in der Systemarchitektur zu vermeiden, scheint es nicht sinnvoll, die dynamische Adaption auf das infrastrukturseitige ATO-System zu allokieren.

Aus dem Kapitel 5.5 ist jedoch bekannt, dass die zentrale Betriebsführung aufgrund einer Kommunikationsstörung vorübergehend unterbrochen sein kann. Diese Situation stellt eine Herausforderung dar, sofern eines der oben genannten infrastrukturseitigen Systemelemente (TMS oder ATO-AT oder ATO-AE) die Koordinierung der dynamischen Adaption übernehmen soll. Denn aufgrund der unterbrochenen Kommunikation befinden sich die Züge im sogenannten „Offline-Modus“ und es kann daher kein Datenaustausch zwischen den fahrzeugseitigen und den infrastrukturseitigen Systemelementen stattfinden. Damit die Züge im Falle einer Kommunikationsstörung nicht im Offline-Modus stehenbleiben und dadurch die Kapazität der Infrastruktur beeinträchtigen, ist sowohl eine zentrale als auch eine dezentrale Koordinierung bei der dynamischen Adaption zur Laufzeit erforderlich.

Da die alleinige Koordination durch infrastrukturseitige Systemelemente nicht in jeder Störungssituation möglich ist, kann auch eine alleinige Koordination durch das TMS nicht erfolgen.

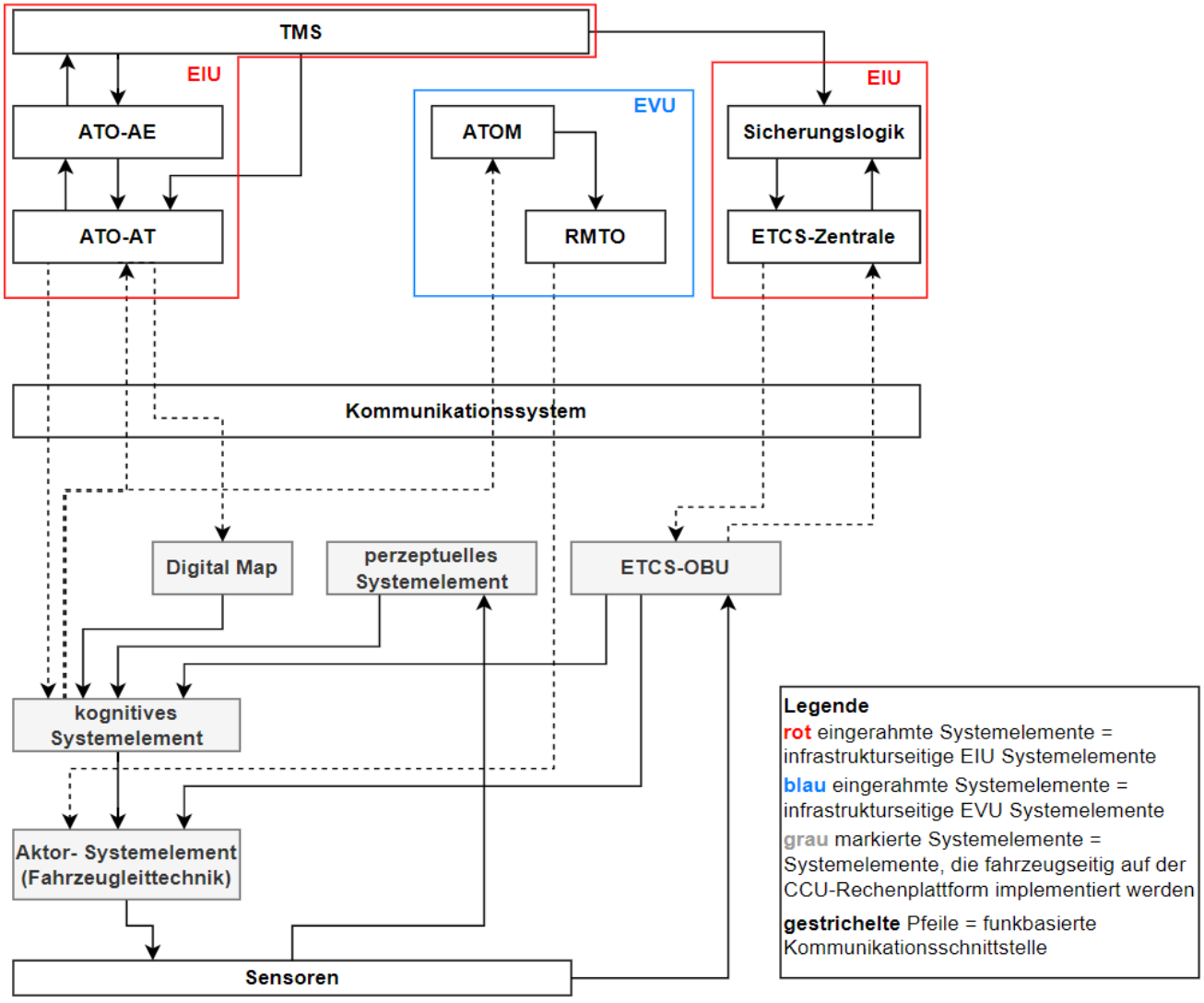

Abbildung 27 funktionale Systemarchitektur einer Zugfahrt in Form einer hierarchischen Regelungsstruktur aus dem Kapitel 4.5 mit Einteilung der Systemelemente nach EIU und EVU

Aufgrund der Tatsache, dass die modularen hardware- und softwarebasierten Systemelemente unterschiedliche betriebliche Funktionen übernehmen und dabei unterschiedliche Lebensdauern aufweisen, können sie auch zu unterschiedlichen Zeiten ersetzt werden. RCA und OCORA streben mit der Referenzarchitektur das Prinzip des modularen Sicherheitsnachweises (modular safety) an. Um den Sicherheitsnachweis modular gestalten zu können, ist es daher sinnvoll, die Koordination der dynamischen Adaption auf ein separates Systemelement zu allokieren, das in die Systemarchitektur eingebettet werden kann. Dieses Systemelement wird im Weiteren als **ATO Fallback-Management-Unit** (**ATO-FMU**) bezeichnet.

Der Vorteil eines separaten Systemelements zur Koordinierung der dynamischen Adaption besteht darin, dass es auf einem höheren Sicherheitslevel entwickelt werden kann, ohne andere Systemelemente mit niedrigem Sicherheitslevel in ihrer Funktionalität zu beschränken. Damit kann insbesondere die von RCA und OCORA geforderte modular safety erreicht werden.

Die ATO-FMU fungiert als eine Art Middleware und kennt die betrieblichen Funktionen und Fähigkeiten aller in der Systemarchitektur im Regelbetrieb vorhandenen Systemelemente. Aufgrund der Kenntnis über die betrieblichen Funktionen und Fähigkeiten der einzelnen Systemelemente kann die ATO-FMU gezielt – in Abhängigkeit der Störungssituation und der dadurch nicht erfüllten Schutzziele – die dynamische Adaption zur Laufzeit koordinieren. Sofern beispielsweise die Funktionen eines Systemelements geändert werden, müssen andere Systemelemente über diese Änderung nicht erfahren. Dies ist auch entsprechend des Plug & Play Prinzips aus dem Unterkapitel 3.2.2 nicht erforderlich. Es reicht, wenn nur die ATO-FMU die Änderung kennt, um in Störungssituationen gezielt die dynamische Adaption zur Laufzeit koordinieren zu können.

Eine ATO-FMU kann unabhängig von den für den Regelbetrieb erforderlichen Systemelementen entwickelt, verändert und bei Bedarf erweitert werden. Das gleiche gilt auch für die Systemelemente, die unabhängig von der ATO-FMU entwickelt, verändert und bei Bedarf erweitert werden können.

Da wie oben erwähnt, sowohl eine zentrale als auch eine dezentrale Koordination erforderlich ist, scheint es sinnvoll, in die Systemarchitektur eine fahrzeugseitige und eine infrastrukturseitige ATO-FMU einzubetten. Die fahrzeugseitige ATO-FMU repräsentiert folglich einen Triebfahrzeugführer in Störungssituationen. Das Verhalten der ATO-FMU wird im nächsten Unterkapitel hergeleitet.

Die infrastrukturseitige ATO-FMU übernimmt bei der Koordination der dynamischen Adaption die Rolle eines Fahrdienstleiters und eines Disponenten. Denn die infrastrukturseitige ATO-FMU koordiniert die fahrzeugseitige ATO-FMU derart, dass die fahrzeugseitigen Entscheidungen bei der dynamischen Adaption die Sicherheit der Betriebsführung nicht beeinträchtigen und dabei auch möglichst keine Konflikte mit anderen Zügen generieren. Im Falle von Ersetzen als Adaptionsart kann die ATO-FMU zudem über die alternativen Softwareanwendungen verfügen. Diese müssen dann nicht auf den jeweiligen Zügen existieren und können stattdessen aus einer sogenannten Datenbank für Services, die in der infrastrukturseitigen ATO-FMU implementiert ist, angefordert werden.

Für eine dezentrale Koordination der dynamischen Adaption ist es prinzipiell möglich, die sichere Rechenplattform auf den Fahrzeugen zu nutzen und die fahrzeugseitige ATO-FMU dort als eine sogenannte Middleware einzubetten, die unabhängig von den Softwareanwendungen auf einer sicheren Ebene, vergleichbar mit der Safety Services aus OCORA CCU, fungiert (vgl. OCORA). Die infrastrukturseitige ATO-FMU kann z.B. in eine Rechenplattform in der Betriebszentrale integriert werden.

Die funktionale Sicht der ATO-FMU einschließlich der Schnittstellen zu den Systemelementen (aus dem Hauptkapitel 4) ist in der Abbildung 28 dargestellt. Die infrastrukturseitige ATO-FMU weist Schnittstellen zu infrastrukturseitigen Systemelemente auf. Die fahrzeugseitige ATO-FMU ist auf der sicheren Rechenplattform nach OCORA als Middleware eingebracht und hat somit Schnittstellen zu den fahrzeugseitigen Systemelementen (auf der Rechenplattform laufenden Softwareanwendungen). Damit die Zustände von den hardwarebasierten Systemelementen auch überwacht werden können, besteht zudem eine Schnittstelle zu den Safety Services aus OCORA CCU. Die beiden ATO-FMUs sitzen zwischen dem Betriebssystem und der Anwendungsschicht und verrichten dort ihren Service. Die Kommunikation zwischen den beiden ATO-FMUs kann z.B. über eine Remote Procedure Call erfolgen, bei der die fahrzeugseitige ATO-FMU Services für die Rekonfiguration von der infrastrukturseitigen ATO-FMU anfordern kann. Die Pfeile in der Abbildung 28 zwischen den ATO-FMUs und den Systemelementen beschreiben die logische Schnittstelle, über die die Softwareanwendungen überwacht (Monitoring) und

in Störungssituationen entsprechend der Adaptionsarten aus dem Unterkapitel 6.5.1 rekonfiguriert werden können.

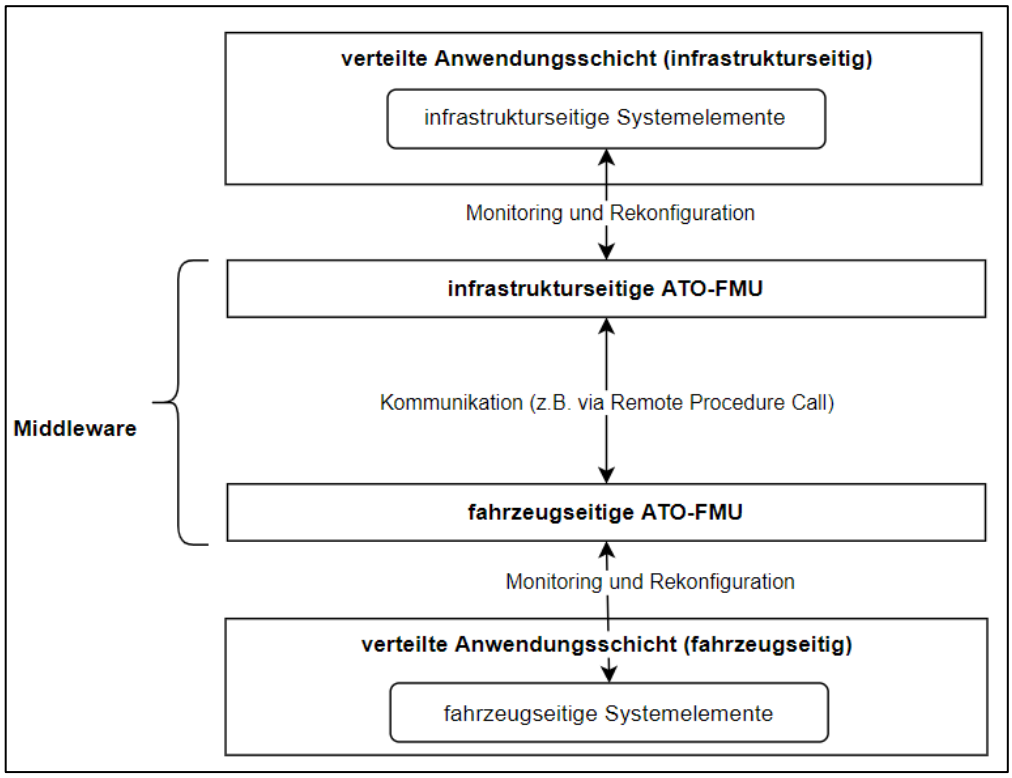

Abbildung 28 funktionale Sicht der ATO Fallback-Management-Unit (ATO-FMU) als Middleware einschließlich der Schnittstellen zu den Systemelementen

Der grundsätzliche Aufbau einer ATO-FMU (fahrzeugseitig und infrastrukturseitig) wird im Weiteren beschrieben.

Damit eine dynamische Adaption durchgeführt werden kann, muss zunächst die vorliegende Störungssituation bekannt sein. Dazu überwacht die ATO-FMU die Zustände der softwarebasierten Systemelemente auf der CCU-Rechenplattform und die Zustände der an die CCU-Rechenplattform angeschlossenen hardwarebasierten Systemelemente (z.B. Sensoren oder UVCCB). Aufgrund der Forderung aus den Normen EN 50128 und 50129 ist davon auszugehen, dass sowohl die hardwarebasierten als auch die softwarebasierten Systemelemente eine inhärente Eigenschaft der Fehleroffenbarung besitzen werden, sodass Fehlerzustände unmittelbar von der ATO-FMU erkannt werden können.

Nachdem die Störungssituation erkannt wurde, muss die ATO-FMU die Art der dynamischen Adaption auswählen. Um zuordnen zu können, für welche Störungssituation eine betrieblich-technische Rückfallebene erforderlich ist, brauchen die infrastrukturseitige und fahrzeugseitige ATO-FMU eine entsprechende Wissensbasis, auf die sie bei der Auswahl zugreifen können. Damit auch unabhängig von den in Kapitel 5.7 erarbeiteten Störungssituationen andere Störungssituationen von der ATO-FMU erkannt werden können, ist es sinnvoll, die Wissensbasis skalierbar zu gestalten. Die Erweiterung der Wissensbasis kann extern durch eine menschliche Ressource mit EIU-Zugehörigkeit vorgenommen werden. Um die Wissensbasis der fahrzeugseitigen ATO-FMU nicht zu überfrachten, ist es ausreichend, wenn diese nur die Störungen zu den Systemelementen, die auf den jeweiligen Zügen migriert sind,

enthält. Dagegen kann die infrastrukturseitige ATO-FMU eine größere Wissensbasis – z.B. Störungen von allen Systemelementen im ATO-Zuständigkeitsbereich – umfassen.

Neben der Wissensbasis umfasst die infrastrukturseitige ATO-FMU auch eine Datenbank für Services. Aufgrund der zentralen Betriebsführung im Bahnbetrieb ist es – sofern möglich – erforderlich, dass die infrastrukturseitige ATO-FMU bei der Koordination der dynamischen Adaption mitwirkt. Daher ist es ausreichend, wenn nur die infrastrukturseitige ATO-FMU über eine Datenbank für Services verfügt. Aufgrund der Möglichkeit, dass die Betreiber ihre Systemarchitektur auf Basis der RCA und OCORA Referenzarchitektur in ihrem eigenen Ermessen gestalten können und dabei die Modularität besonders im Fokus steht, kann es vorkommen, dass die für den vollautomatisierten Bahnbetrieb erforderlichen Systemelemente unterschiedlich entwickelt werden. Die Unterschiede in den jeweiligen softwarebasierten Systemelementen stellt bei der Aufnahme in Datenbank für Services keine Einschränkung dar, da sie nach dem Plug & Play Prinzip von OCORA (Anforderung aus dem Unterkapitel 3.2.3) austauschbar sein sollen.

Aus dieser Datenbank können beim Ersetzen die erforderlichen Services abgerufen werden. Auch die Datenbank für Services sollte im laufenden Betrieb – z.B. bei neuen Störungssituationen – aktualisiert werden. Die Datenbank für Services in der infrastrukturseitigen ATO-FMU ermöglicht es, dass die für den vollautomatisierten Bahnbetrieb erforderlichen Systemelemente – insbesondere die Softwareanwendungen – nicht redundant ausgelegt werden müssen, solange die Datenbank für Services der infrastrukturseitigen ATO-FMU regelmäßig gepflegt wird. Mit den in der Datenbank für Services abgelegten Softwareanwendungen können alle Züge im ATO-Zuständigkeitsbereich im Falle von Störungen versorgt werden, statt die Systemelemente bei allen Zügen vollredundant auszulegen.

Als letztes umfassen beide ATO-FMU noch die eigentliche Durchführung der dynamischen Adaption, um situationsabhängige betrieblich-technische Rückfallebenen einzurichten. Hiermit werden die entsprechenden Systemelemente in der Systemarchitektur für die Einrichtung einer betrieblich-technischen Rückfallebene koordiniert. Die beiden ATO-FMU mit ihren Bestandteilen ist in der Abbildung 29 dargestellt.

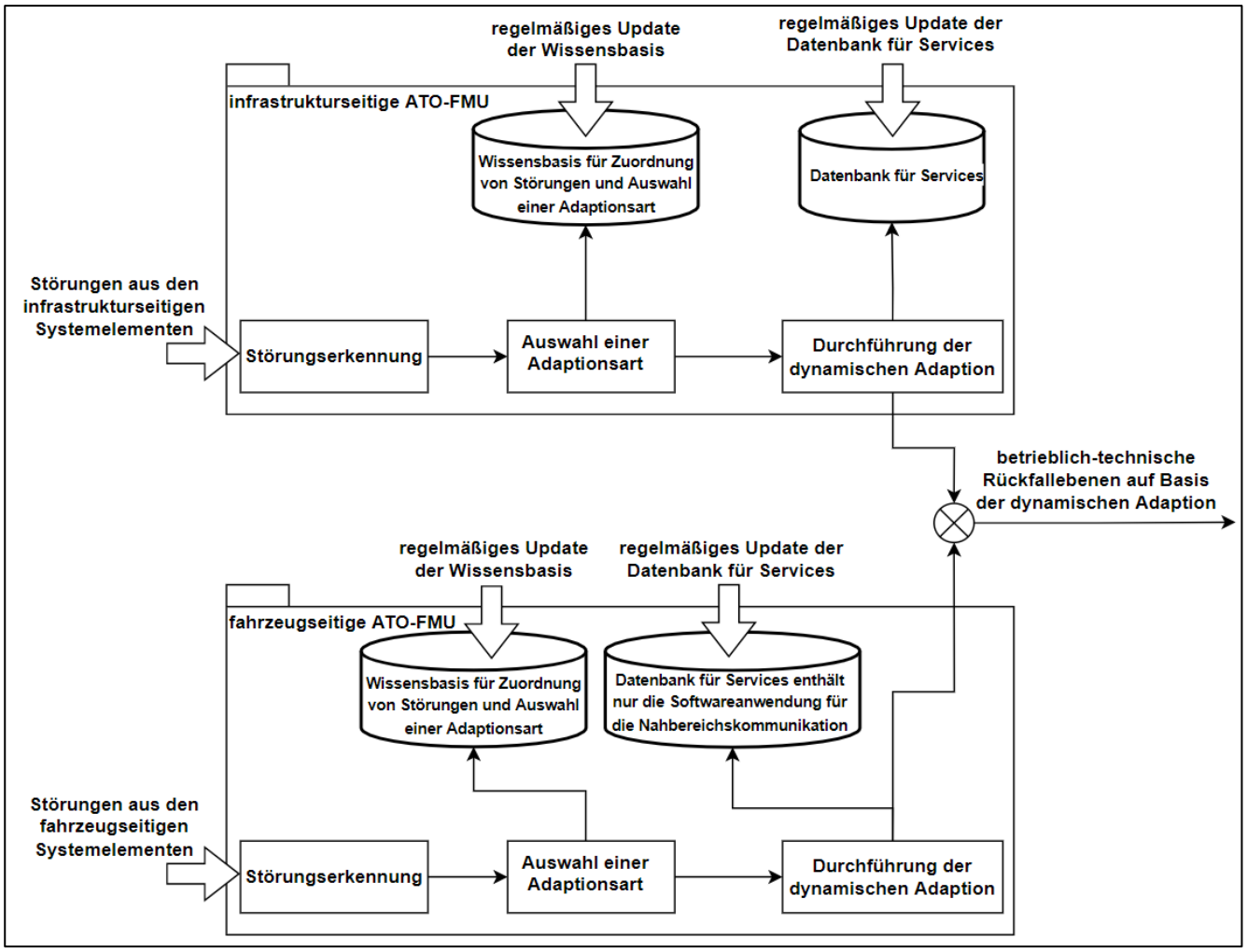

Abbildung 29 infrastruktur- und fahrzeugseitige ATO-FMU mit ihren Bestandteilen als Koordinator der dynamischen Adaption

Nachdem bisher die möglichen Arten der dynamischen Adaption der Systemarchitektur und die ATO-FMU als Koordinator der dynamischen Adaption hergeleitet wurden, ist es auch erforderlich, herzuleiten, wie eine entsprechende dynamische Adaption zur Laufzeit weitgehend automatisiert ablaufen kann.

6.5.3 Designprinzipien bei der dynamischen Adaption der Systemarchitektur zur Laufzeit für eine Betriebsführung in Störungssituationen

Nachdem nun die möglichen Adaptionsarten bekannt sind und in Unterkapitel 6.5.2 die ATO-FMU als koordinierende Ressource hergeleitet wurde, ist das Ziel dieses Unterkapitels die Herleitung von Designprinzipien, die bei der dynamischen Adaption zur Laufzeit durch die ATO-FMU berücksichtigt werden. Die Designprinzipien leiten sich aus den bereits in Unterkapitel 3.2.3 zusammengestellten Leitlinien zur Gestaltung von Systemarchitekturen und aus den Anforderungen aus dem Unterkapitel 3.2.2 ab.

Das wichtigste Ziel aller Stakeholder (EIU, EVUs und Fahrgäste) ist die **Gewährleistung der Sicherheit** in Störungssituationen. Da sich die Systemarchitektur aus dem Regelbetrieb bei einer dynamischen Adaption vorübergehend ändert, kann es vorkommen, dass die entsprechende betriebliche Funktion nicht mehr mit dem THR-Wert aus dem Regelbetrieb erfüllt wird. Dennoch muss der Ablauf für die

Durchführung einer dynamischen Adaption immer mit möglichst wenig Auswirkung auf die Sicherheit der Betriebsführung erfolgen. Zur Gewährleistung der Sicherheit in Störungssituationen geht es darum, das verletzte Schutzziel ersatzweise zu erfüllen.

Damit die betriebliche Funktion eines gestörten Systemelements bei der Deaktivierung mit Funktionsallokation vorübergehend durch eine andere Ressource übernommen werden kann, sollte die erforderliche **Fähigkeit** des gestörten Systemelements auch bei der einzubindenden Ressource vorliegen. Fähigkeiten können, wie bereits in Kapitel 2.4 erläutert, sensorische, perzeptuelle, kognitive, motorische oder kommunikative Fähigkeiten sein. Beispielsweise kann eine motorische Fähigkeit durch ein Zugpersonal oder durch einen Train-Operator bereitgestellt werden. Da eine Ressource entweder ein Systemelement oder ein Betriebspersonal sein kann, sollte jedes Systemelement bei der Spezifikation bzw. bei der Aufnahme in die Wissensbasis mit der jeweiligen betrieblichen Funktion und der zugehörigen Fähigkeit spezifiziert werden, damit die ATO-FMU bei der Koordination der dynamischen Adaption die für die betriebliche Funktion erforderliche Fähigkeit identifizieren kann. Auch die Fähigkeiten eines Betriebspersonals sollten in der in der Wissensbasis der ATO-FMU enthalten sein, damit es bei Bedarf durch die ATO-FMU eingebunden werden kann. Durch eine formale Spezifikation der Systemelemente bei der Aufnahme in die Wissensbasis kann eine regelbasierte Abfrage hinsichtlich des verletzten Schutzziels und der erforderlichen Fähigkeiten erfolgen, wodurch ein deterministischer Ablauf der dynamischen Adaption erreicht wird (vgl. Anforderung aus dem Kapitel 6.2).

Sofern möglich, sollte neben der Übereinstimmung der Fähigkeit auch – unter Berücksichtigung des Sicherheitsprinzips in Störungssituationen – während der vorübergehenden dynamischen Adaption die auf eine andere Ressource allokierte betriebliche Funktion überwacht werden. Beispielsweise überwacht die ETCS-OBU das Aktor-Systemelement bei der Einhaltung der zulässigen Geschwindigkeit. Eine vergleichbare **Überwachung und Ausführung** ist daher auch in Störungssituationen sinnvoll.

Außerdem ist es wichtig, dass von einer vorübergehend eingebundenen Ressource zur Übernahme einer betrieblichen Funktion keine Gefahr auf andere Systemelemente ausgeht (**Rückwirkungsfreiheit**). Insbesondere, wenn Betriebspersonal eingebunden wird und dieses mit Systemelementen interagieren wird, darf sich die Bedienung durch das Betriebspersonal in keiner Form auf ein Systemelement negativ auswirken.

Entsprechend der Leitlinien zur Gestaltung von Systemarchitekturen aus dem Unterkapitel 3.2.3 sollte die **Komplexität** der Systemarchitektur durch die dynamische Adaption möglichst nicht erhöht werden. Das kann dadurch erreicht werden, dass möglichst wenig neue Schnittstellen bei der Deaktivierung mit Funktionsallokation entstehen. Zur Bewältigung der Komplexität sollte zudem möglichst eine **direkte Kommunikation** zwischen den Systemelementen und den eingebundenen Ressourcen vorliegen. Dadurch wird nicht nur die Komplexität bewältigt, sondern auch die Latenzzeit möglichst reduziert. Um zu verhindern, dass die ATO-FMU ständig die gleiche Art der dynamischen Adaption (z.B. Deaktivierung ohne Funktionsallokation) vornimmt, sollte auf der anderen Seite die **Komplexität** auch **nicht deutlich reduziert** werden. Denn bei einer Deaktivierung ohne Funktionsallokation sind keine vorübergehend neuen Schnittstellen erforderlich, jedoch kann eine Weiterfahrt in Störungssituationen ohne Ersetzen oder Deaktivierung mit Funktionsallokation erhöhtes Betriebsrisiko aufweisen und daher dem Sicherheitsprinzip widersprechen.

Wie bereits im vorigen Unterkapitel erwähnt, ist es zudem relevant, dass bei der dynamischen Adaption aufgrund der zentralen Betriebsführung – sofern möglich – immer die infrastrukturseitige ATO-FMU mitwirkt.

Beim Ersetzen eines Systemelements sollte das Systemelement, das die betriebliche Funktion vorübergehend übernehmen soll, in der Datenbank für Services vorhanden sein. Nach dem Ersetzen muss das Systemelement entsprechend des Designprinzips Informationskapselung sofort mit den anderen Systemelementen kommunizieren können. Die **reibungslose Interaktion** gilt auch im Falle der Einbindung von Betriebspersonal.

Das in der Datenbank für Services vorhandene Systemelement sollte zudem vor dem Ersetzen **getestet** werden können, um sicherheitskritische Fehler nach dem Ersetzen zu vermeiden.

Damit die Abweichung von der vereinbarten Betriebsqualität in der betrieblich-technischen Rückfallebene möglichst gering bleibt, ist es zudem wichtig, dass die dynamische Adaption in einer **möglichst kurzen Zeit** erfolgt. Das bedeutet, dass die Zeit zum Ersetzen und die Zeit zum Einbinden einer alternativen Ressource möglichst kurz sein sollte.

Bereits in Kapitel 3.2.3 wurde gefordert, dass betrieblich-technische Rückfallebenen im Zeitalter der Automatisierung von Cyber-Angriffen (**Security**) geschützt sein sollten. Aus diesem Grund darf die dynamische Adaption nicht ohne Autorisierung erfolgen. Die ATO-FMU sollte daher während des Ersetzens oder während der Deaktivierung mit Funktionsallokation eine Verifikation vornehmen.

6.5.4 Ablauf einer dynamischen Adaption der Systemarchitektur zur Laufzeit für eine Betriebsführung in Störungssituationen

Unter Berücksichtigung der Designprinzipien aus dem vorigen Unterkapitel und der Anforderungen aus dem Kapitel 6.2 wird in diesem Unterkapitel der Ablauf der jeweiligen Adaptionsart aus dem Unterkapitel 6.5.1 hergeleitet. Bevor im Weiteren der spezifische Ablauf für die jeweilige Adaptionsart aus dem Unterkapitel 6.5.1 hergeleitet wird, erfolgt zunächst die Erarbeitung eines allgemeinen Ablaufs, der für alle Adaptionsarten aus dem Unterkapitel 6.5.1 gilt.

Allgemeiner Ablauf der dynamischen Adaption zur Laufzeit

Der allgemeine Ablauf, der für alle Adaptionsarten aus dem Unterkapitel 6.5.1 gilt, beschreibt die Identifikation des gestörten Systemelements (hardware- oder softwarebasiertes Systemelement), die Zuordnung dieser Störung zum entsprechenden Schutzziel und darauf basierend die Auswahl der geeigneten Adaptionsart.

Wie bereits bei den Designprinzipien in Unterkapitel 6.5.3 erwähnt, ist das wichtigste Ziel aller Stakeholder (EIU, EVUs und Fahrgäste) die Gewährleistung der Sicherheit in Störungssituationen. Zur Gewährleistung der Sicherheit in Störungssituationen geht es darum, das verletzte Schutzziel ersatzweise zu erfüllen.

Unabhängig davon, ob es sich um ein Ersetzen oder um eine Deaktivierung mit oder ohne Funktionsallokation handelt, ist es wichtig, zunächst die vorliegende Störungssituation hinsichtlich des verletzten Schutzziels richtig einzuordnen. Dazu wurde in Abbildung 29 aus dem Unterkapitel 6.5.2 eine Wissensbasis in der ATO-FMU vorgesehen.

Damit die vorliegende Störungssituation einem verletzten Schutzziel zugeordnet werden kann, wird in der Wissensbasis der entsprechenden ATO-FMU anhand der Spezifikation des Systemelements abgefragt, welche Schutzziele es verantwortet oder bei welchen Schutzzielen es indirekt mitwirkt. Ein Beispiel für indirekte Mitwirkung bei der Erfüllung eines Schutzziels wäre das Systemelement ATO-AE, das Journey-Profiles generiert. Das Systemelement ATO-AE verantwortet zwar direkt kein Schutzziel,

sofern jedoch Journey-Profiles nicht verfügbar sind, kann – wie bereits in Kapitel 5.7 hergeleitet – ein Zug nicht mehr weiterfahren, wodurch dann bei Personenzügen die Zuginsassen gefährdet werden können. Dahingegen verantworten die Sensoren sowie das perzeptuelle Systemelement das Schutzziel Kollisionsvermeidung. Durch eine Spezifikation der betrieblichen Funktionen der für den vollautomatisierten Bahnbetrieb erforderlichen Systemelemente in der Entwicklungsphase kann die Zuordnung zur Laufzeit regelbasiert erfolgen. Die Wissensbasis der infrastrukturseitigen ATO-FMU wird bei der Spezifikation der infrastrukturseitigen Systemelemente mit den zugehörigen Metadaten angereichert. Die Wissensbasis der fahrzeugseitigen ATO-FMU wird hingegen mit den zugehörigen Metadaten der fahrzeugseitigen Systemelemente angereichert.

Die Metadaten enthalten übergreifende Informationen über ein Systemelement. Wie bereits in Unterkapitel 6.5.2 erwähnt, kann auch das Betriebspersonal in Störungssituationen eingebunden werden. Dazu ist es auch erforderlich, dass die ATO-FMU die Fähigkeiten des Betriebspersonals und dessen betriebliche Funktionen in der Wissensbasis enthält.

Die relevanten Metadaten eines Systemelements zur Zuordnung der vorliegenden Störungssituation zu einem verletzten Schutzziel können in Anlehnung an die allgemeinen Eigenschaften eines Systemelements wie folgt sein:

Metadaten eines Systemelements:

- Art des Systemelements = {hardwarebasiert, softwarebasiert},
- verantwortete betriebliche Funktionen = {Geschwindigkeitsüberwachung, Geschwindigkeitsregelung, Lichtraumüberwachung, …},
- interne Funktionen = {Funktion 1, Funktion 2, …, Funktion #},
- Fähigkeiten = {sensorische, perzeptuelle, kognitive, motorische, kommunikative} und
- Zustand = {verfügbar, nicht verfügbar}.

Anhand der durch das gestörte Systemelement zu erfüllenden betrieblichen Funktionen und durch Zuhilfenahme des betrieblichen und umgebungsbedingten Kontextes aus dem Kapitel 5.5 kann die vorliegende Störungssituation einem verletzten Schutzziel zugeordnet werden. Die Kenntnis der von dem gestörten Systemelement erfüllten betrieblichen Funktionen ist zwar ausreichend, um das verletzte Schutzziel zu identifizieren, jedoch ist der betriebliche und umgebungsbedingte Kontext insofern relevant, da damit entschieden werden kann, ob für die vorliegende Störungssituation eine betrieblich-technische Rückfallebene tatsächlich erforderlich ist. Denn beispielsweise ein Zug, der in einen Bahnhof einfährt und dann im Anschluss abgestellt werden soll, aber dessen Geschwindigkeitsüberwachung gestört ist, stellt keine Gefährdung dar, da die Abstellfahrt ohne Zuginsassen erfolgt und daher das Schadensausmaß im Falle einer Geschwindigkeitsüberschreitung entsprechend gering ausfällt. Für derartige Betriebssituationen ist nicht notwendigerweise eine dynamische Adaption in Form von Deaktivierung mit Funktionsallokation oder Ersetzen erforderlich.

Nachdem die vorliegende Störungssituation einem verletzten Schutzziel zugeordnet wurde, wird als nächstes in der Wissensbasis anhand der Metadaten des Systemelements abgefragt, welche Fähigkeiten dieses Systemelement aufweist. Denn sofern entsprechend des Designprinzips aus dem Unterkapitel 6.5.3 das Ersetzen oder die Deaktivierung mit Funktionsallokation als dynamische Adaption durchgeführt werden soll, müssen die alternativen Ressourcen dazu fähig sein, die Funktionen des deaktivierten Systemelements zu übernehmen. Bei der Strukturierung der Systemelemente mit einem vereinfachten Modell der menschlichen Informationsverarbeitung für den vollautomatisierten

Bahnbetrieb in Kapitel 4.4 konnten die möglichen Fähigkeiten identifiziert werden. Durch eine formale Spezifikation dieser Fähigkeiten in Form von Metadaten bei der Aufnahme in die Wissensbasis kann

eine regelbasierte Abfrage hinsichtlich des verletzten Schutzziels und der Fähigkeiten erfolgen, wodurch ein deterministischer Ablauf der dynamischen Adaption erreicht wird (vgl. Anforderung aus dem Kapitel 6.2).

Anhand des zu erfüllenden Schutzziels und der dafür erforderlichen Fähigkeiten werden dann verfügbare und potenziell einsetzbare Ressourcen gesucht. Dazu kooperieren die beiden ATO-FMUs dahingehend, dass die infrastrukturseitige ATO-FMU mögliche infrastrukturseitige Ressourcen und die fahrzeugseitige ATO-FMU mögliche fahrzeugseitige Ressourcen suchen. Die Auswahl der Ressource bedingt die Adaptionsart. Sofern mehr als eine Ressource gefunden wurde, kann auch mehr als eine Adaptionsart vorliegen. In so einem Fall erfolgt eine Bewertung vor der Auswahl einer Adaptionsart. Bei der Entscheidung für eine Adaptionsart wird die Invariante „möglichst hohe Sicherheit sicherstellen“ an oberster Stelle berücksichtigt. Demnach erfolgt eine Bewertung bei der dynamischen Adaption, wie durch die jeweilige Adaptionsart die Sicherheit der Betriebsführung beeinflusst wird, sofern mehr als eine Adaptionsart in der vorliegenden Störungssituation möglich ist. Das entsprechende Bewertungsverfahren, das bei der dynamischen Adaption zugrunde gelegt werden kann, wird im nächsten Hauptkapitel hergeleitet. Entsprechend des Bewertungsergebnisses wird dann eine Adaptionsart ausgewählt.

Entsprechend der Anforderung aus dem Kapitel 6.2 wird im vollautomatisierten Bahnbetrieb bei der dynamischen Adaption zur Laufzeit davon ausgegangen, dass mindestens eine der drei Adaptionsarten anwendbar ist und daher ausgewählt wird.

Der hier beschriebene allgemeine Ablauf einer dynamischen Adaption, der für alle Adaptionsarten gilt, ist in der Abbildung 30 als ein Aktivitätsdiagramm dargestellt.

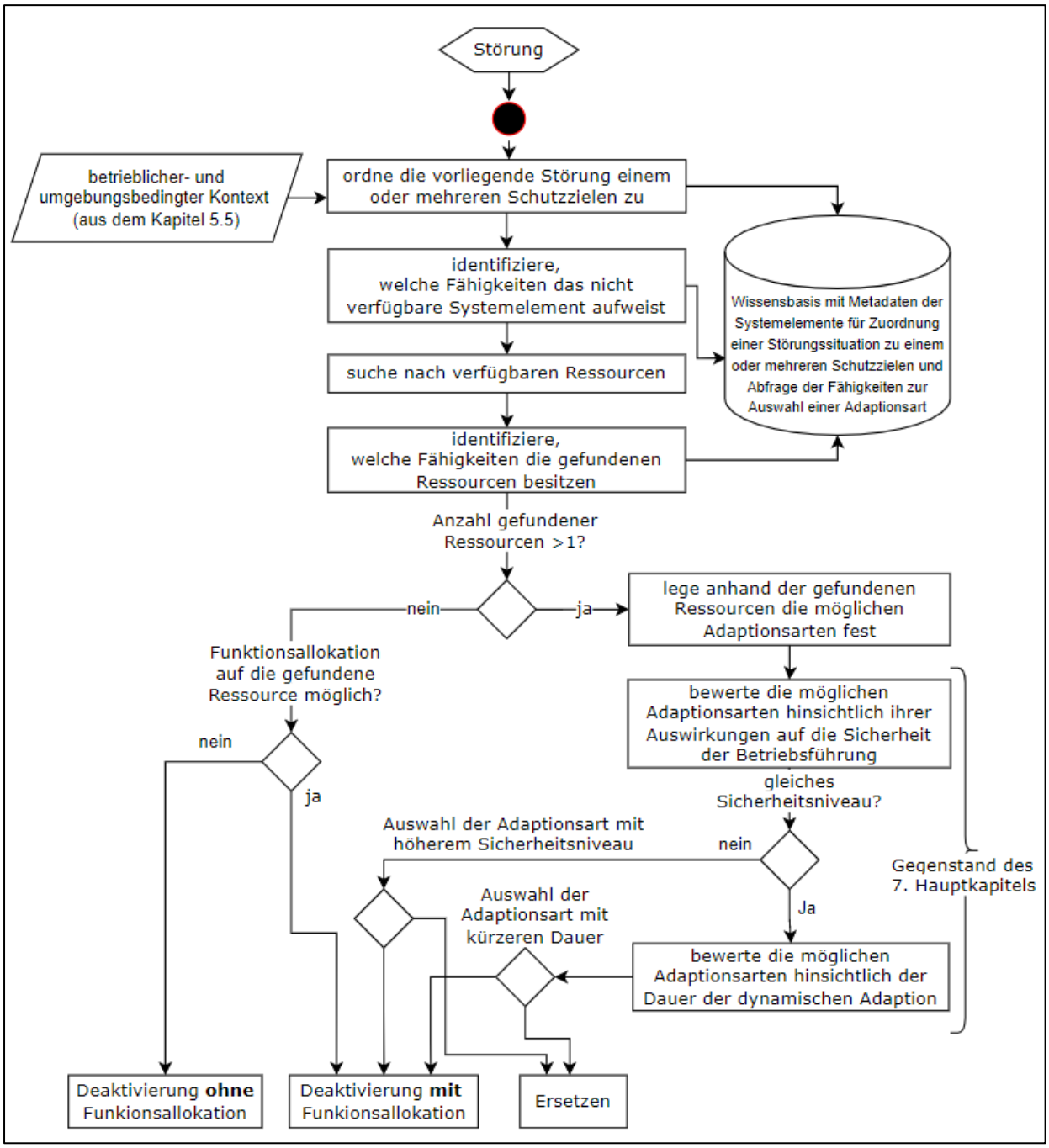

Abbildung 30 allgemeiner Ablauf einer dynamischen Adaption, der für alle Adaptionsarten gilt

Ablauf der dynamischen Adaptionsart: Ersetzen

In diesem Abschnitt wird der Ablauf der Adaptionsart Ersetzen beschrieben. Wie bereits aus dem Unterkapitel 6.5.1 bekannt, kann das Ersetzen zur Laufzeit nur bei Softwareanwendungen durchgeführt werden. Beim Ersetzen geht es darum, die Softwareanwendung nach dem Plug & Play Prinzip zu ersetzen. Das bedeutet, dass die neue Softwareanwendung entsprechend der Anforderung aus dem Unterkapitel 3.2.2 die Schnittstellen zu den benachbarten Systemelementen weiterhin bedient.

Das Ersetzen kann prinzipiell während der Fahrt erfolgen, sofern die zu ersetzende Softwareanwendung keine sicherheitskritische Funktion erfüllt und das Ersetzen entsprechend des Designprinzips aus dem vorigen Unterkapitel in einer endlichen Zeit erfolgt. Um das Betriebsrisiko während des Ersetzens

möglichst gering zu halten, kann aber auch die Geschwindigkeit des betroffenen Zuges reduziert werden. Sofern das Ersetzen während der Fahrt erfolgreich abgeschlossen wird, kann die Fahrt uneingeschränkt weitergeführt werden.

Sollte jedoch die zu ersetzende Softwareanwendung eine sicherheitskritische Funktion erfüllen und das Ersetzen in einer endlichen Zeit nicht erfolgen können, so ist es sinnvoll, eine Zwangsbremsung einzuleiten, um das Betriebsrisiko nicht weiter zu erhöhen. Ist nach der Zwangsbremsung weiterhin kein Ersetzen möglich, so kann die Adaptionsart geändert werden, um die Anforderung aus dem Kapitel 6.2 (Weiterfahrt in Störungssituationen) einhalten zu können. In so einem Fall kommt eine Deaktivierung mit oder ohne Funktionsallokation in Frage. Der entsprechende Ablauf für eine Deaktivierung mit oder ohne Funktionsallokation wird in den nächsten beiden Abschnitten erarbeitet.

Nachdem die Störung an der zu ersetzenden Softwareanwendungen erkannt wurde, erfolgt zunächst die Benachrichtigung der benachbarten Softwareanwendungen darüber, dass die primäre Softwareanwendung aus dem Regelbetrieb ersetzt wird und daher keine Inputs verarbeiten und Outputs generieren kann. Auf Basis dieser Benachrichtigung können dann die benachbarten Systemelemente ebenfalls ihren Zustand (z.B. zum „warten auf Service von Systemelement mit der ID ##“) ändern, solange das Ersetzen durchgeführt wird.

Die Attribute der zu ersetzenden Softwareanwendung können zum Zeitpunkt des Ersetzens bestimmte Werte haben. Bei den Attributen geht um die Werte bzw. Wertebereiche eines bestimmten Objekts innerhalb der Softwareanwendung, die zur Erfüllung der Funktionen relevant sind, besitzt. Ein konkretes Beispiel ist die Softwareanwendung zur Generierung eines Geschwindigkeitsprofils. In der Softwareanwendung zur Generierung eines Geschwindigkeitsprofils braucht der Algorithmus Informationen über die aktuelle Position des Zuges, die letzte gültige Geschwindigkeit, verfügbares Beschleunigungsvermögen, das zuletzt als Referenz angenommene Journey-Profile und das Segment-Profile. Das bedeutet, dass die hier beispielhaft genannten Objekte Attribute besitzen. Damit entsprechend des Kompatibilitätsprinzips (vgl. Unterkapitel 3.2.2) die ersetzte Softwareanwendung sofort mit anderen bereits vorhandenen Softwareanwendungen kommunizieren kann, müssen die letzten gültigen Attribute der zu ersetzenden Softwareanwendung auf die neue Softwareanwendung übertragen werden, sofern die Störung in der primären Softwareanwendung nicht aufgrund falscher Attribute verursacht wurde. Im Falle einer Störung in der primären Softwareanwendung aufgrund falscher Attribute ist es erforderlich, die Plausibilität der letzten gültigen Attribute vor der Übertragung auf die neue Softwareanwendung zu prüfen. Die Prüfung kann beispielsweise anhand von Default-Werten, die in die Datenbank für Services der infrastrukturseitigen ATO-FMU abgelegt wurden, erfolgen.

Unter der Annahme, dass das Ersetzen in einer endlichen Zeit erfolgt und es sich um eine Störung im fahrzeugseitigen Systemelement handelt, wird daraufhin die alternative Softwareanwendung aus der Datenbank für Services der infrastrukturseitigen ATO-FMU angefordert und dabei die letzten gültigen Attribute der zu ersetzenden Softwareanwendung an die infrastrukturseitige ATO-FMU übermittelt. Entsprechend der Designprinzipien aus dem vorigen Unterkapitel wird die in der Datenbank für Services vorhandene Softwareanwendung vor dem Ersetzen zunächst auf Plausibilität der Attribute getestet. Nachdem erfolgreichen Test wird die neue Softwareanwendung mit den letzten gültigen und plausiblen Attributen zum Ersetzen an die fahrzeugseitige ATO-FMU übermittelt.

Im Falle einer Störung an einem infrastrukturseitigen Systemelement kann die nicht verfügbare Softwareanwendung ohne die Mitwirkung der fahrzeugseitigen ATO-FMU durch die infrastrukturseitige ATO-FMU ersetzt werden.

Wenn die neue Softwareanwendung erfolgreich ersetzt wurde, erfolgt eine Benachrichtigung der benachbarten Systemelemente darüber. Abschließend wird das Ersetzen entsprechend des Designprinzips (Security) geprüft. Dabei werden insbesondere das korrekte Verhalten der alternativen Softwareanwendung und die Schnittstellen einschließlich der ausgetauschten Kontrollaktionen bzw. Rückkopplungen zu den benachbarten Systemelementen geprüft. Der Ablauf der Adaptionsart Ersetzen ist in der Abbildung 31 in Form eines Aktivitätsdiagramms dargestellt.

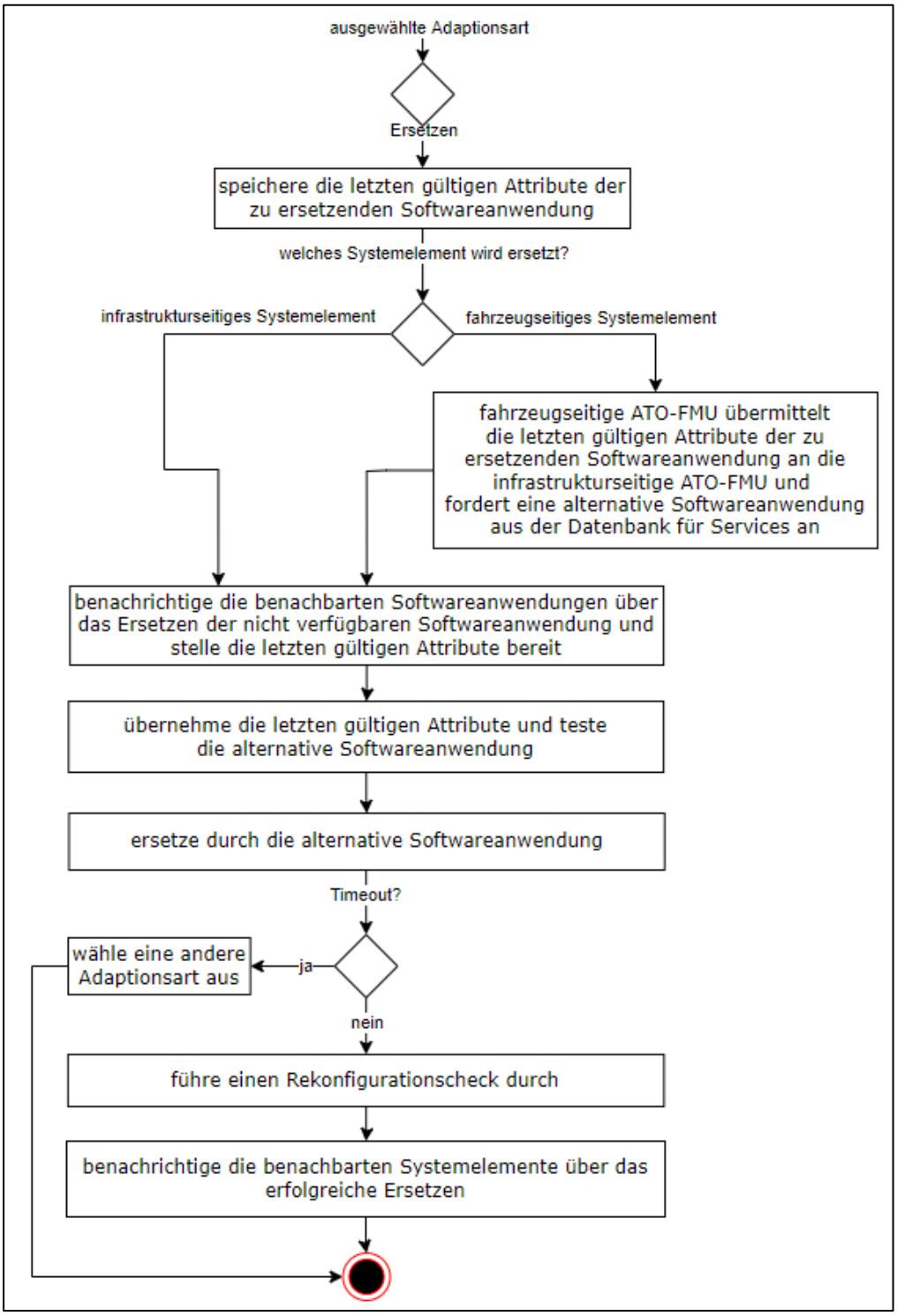

Abbildung 31 Ablauf der Adaptionsart Ersetzen in Form eines Aktivitätsdiagramms

Ablauf der dynamischen Adaptionsart: Deaktivierung ohne Funktionsallokation

In diesem Abschnitt wird der Ablauf der Adaptionsart Deaktivierung ohne Funktionsallokation beschrieben. Wie bereits aus dem Unterkapitel 6.5.1 bekannt, kann eine Deaktivierung ohne Funktionsallokation zur Laufzeit sowohl bei hardwarebasierten als auch bei softwarebasierten Systemelementen durchgeführt werden.

Nachdem die Störung an dem zu deaktivierenden Systemelement erkannt wurde, erfolgt wie beim Ersetzen zunächst die Benachrichtigung der benachbarten Systemelemente darüber, dass das primäre Systemelement aus dem Regelbetrieb deaktiviert wird und daher keine Inputs verarbeiten und Outputs generieren kann. Aufgrund der geforderten Sicherheit sollte die Deaktivierung ohne Funktionsallokation im Fail-Safe Zustand erfolgen.

Der wesentliche Unterschied der Deaktivierung ohne Funktionsallokation zum Ersetzen ist die Tatsache, dass die benachbarten Systemelemente ebenfalls keine Inputs von dem deaktivierten Systemelement erhalten und dadurch ihr Verhalten beeinflusst wird. Damit trotz des deaktivierten Systemelements die benachbarten Systemelemente weiterhin funktionieren können, ist es sinnvoll, einen Mechanismus für sogenannte Ausnahmen (Exception Handler) zu implementieren. Beispielsweise könnte ein einfacher Exception Handler bei Deaktivierung eines benachbarten Systemelements die Nutzung von Default-Werten bei der Ausführung der eigenen Funktionen sein.

Ein konkretes Beispiel wäre die Deaktivierung der Objektklassifizierung innerhalb des perzeptuellen Systemelements. Da das Ergebnis der Objektklassifizierung dem kognitiven Systemelement zur Geschwindigkeitsregelung nicht zur Verfügung gestellt werden kann, wird in dem Exception Handler angenommen, dass jedes erkannte Objekt ein schweres und ein großes Objekt ist, sodass das damit verbundene Schadensaumaß hoch ist. Dieser Exception Handler hätte zur Folge, dass die Geschwindigkeit im kognitiven Systemelement reduziert wird.

Wenn das Systemelement erfolgreich deaktiviert wurde, erfolgt eine Benachrichtigung der benachbarten Systemelemente über die Deaktivierung. Abschließend wird die Deaktivierung geprüft. Dabei wird geprüft, dass das deaktivierte Systemelement keine Outputs generiert und dass das Exception Handler der benachbarten Systemelemente der Spezifikation entspricht.

Der Ablauf der Adaptionsart Deaktivierung ohne Funktionsallokation ist in der Abbildung 32 in Form eines Aktivitätsdiagramms dargestellt.

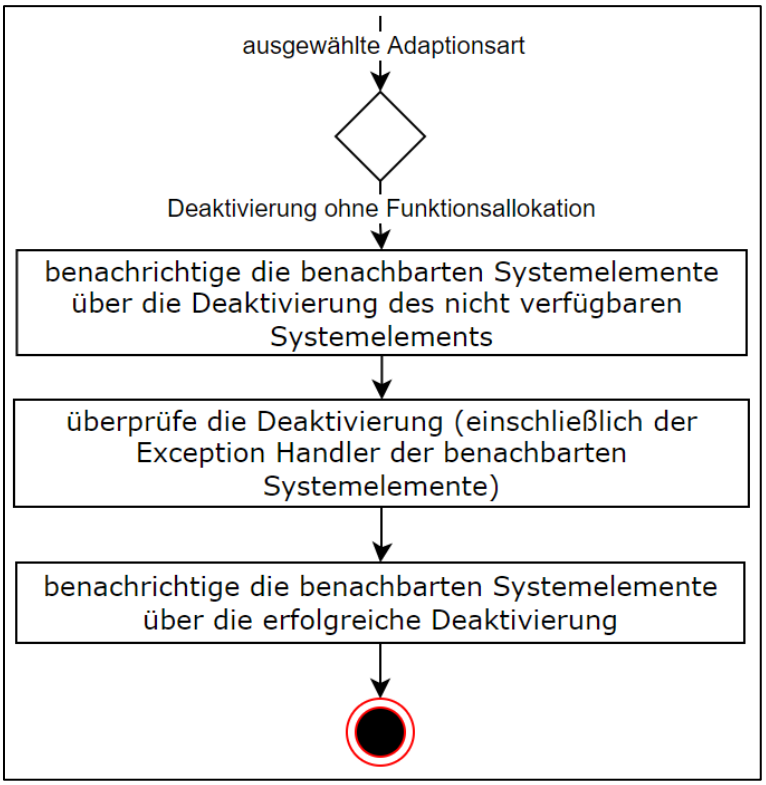

Abbildung 32 Ablauf der Adaptionsart Deaktivierung ohne Funktionsallokation in Form eines Aktivitätsdiagramms

Ablauf der dynamischen Adaptionsart: Deaktivierung mit Funktionsallokation

In diesem Abschnitt wird der Ablauf der Adaptionsart Deaktivierung mit Funktionsallokation beschrieben. Wie bereits aus dem Unterkapitel 6.5.1 bekannt, kann eine Deaktivierung mit Funktionsallokation zur Laufzeit sowohl bei hardwarebasierten als auch bei Softwareanwendungen durchgeführt werden. Wie bereits in Unterkapitel 6.5.1 erläutert, gibt es bei einer Deaktivierung auch die Möglichkeit, die betriebliche Funktion von deaktivierten hardwarebasierten Systemelementen an eine andere Ressource zu übertragen, um in Störungssituation weiterhin die entsprechende betriebliche Funktion erfüllen zu können. Anders als bei der Deaktivierung ohne Funktionsallokation können sich bei der Deaktivierung mit Funktionsallokation die Schnittstellen zwischen den Systemelementen in der betrieblich-technischen Rückfallebene vorübergehend ändern.

Nachdem entsprechend des Unterkapitelanfangs im allgemeinen Ablauf die möglichen alternativen Ressourcen zur Übernahme der betrieblichen Funktionen des gestörten Systemelements gefunden und bewertet wurden, erfolgt zunächst eine Bereitschaftsanfrage an die Ressource mit höchster Sicherheit zur Einbindung und Übernahme der betrieblichen Funktionen des gestörten Systemelements. Eine Bereitschaftsanfrage ist erforderlich, da die gefundene Ressource zum Zeitpunkt der Anfrage noch mit ihrer primären Funktion beschäftigt sein kann. Erst wenn die Bereitschaft zur Einbindung bestätigt wurde, erfolgt die dynamische Adaption.

Parallel dazu erfolgt – wie beim Ersetzen – die Benachrichtigung der benachbarten Systemelemente darüber, dass das primäre Systemelement aus dem Regelbetrieb deaktiviert wird und daher keine Inputs verarbeiten und Outputs generieren kann.

Bei einer Deaktivierung mit Funktionsallokation kann es vorkommen, dass eine Ressource außerhalb der Systemarchitektur aus dem Regelbetrieb gefunden wird. In diesem Fall kann mit mehr Zeitverbrauch

für die Funktionsallokation gerechnet werden als bei der Deaktivierung ohne Funktionsallokation. Aufgrund der geforderten Sicherheit und der Tatsache, dass die Einbindung einer alternativen Ressource länger dauern kann als das Ersetzen, sollte die Deaktivierung ohne Funktionsallokation daher im Fail-Safe Zustand erfolgen.

Wenn demnach die angefragte Ressource nach einer bestimmten Zeit nicht antwortet oder die Ausführung ihrer primären Funktion länger als eine festgelegte Zeit (Timeout) dauert, kann die nächste gefundene Ressource angefragt werden, um die Abweichung von der vereinbarten Betriebsqualität zu minimieren. An dieser Stelle soll jedoch hervorgehoben werden, dass entsprechend der Anforderung aus dem Kapitel 3.2 im vollautomatisierten Bahnbetrieb weiterhin das Grundprinzip „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“ gilt. Das bedeutet, dass eine Ressource mit erhöhtem Einfluss auf die Sicherheit nur dann eingebunden werden darf, wenn das damit verbundene Risiko der Betriebsführung unter einem bestimmten Risikogrenzwert liegt. Ein entsprechendes Bewertungsverfahren dazu wurde bereits in *Huang (2020)* entwickelt.

Sofern innerhalb einer festgelegten Zeit (Timeout) keine der angefragten Ressourcen die Bereitschaft bestätigt, kann bei hardwarebasierten Systemelementen alternativ die Deaktivierung ohne Funktionsallokation und bei Softwareanwendungen das Ersetzen oder ebenfalls Deaktivierung ohne Funktionsallokation ausgewählt werden. Dadurch wird die Anforderung hinsichtlich der Betriebsführung in Störungssituation eingehalten. Unter der Annahme, dass eine Bereitschaftsanfrage durch die angefragte Ressource bestätigt wurde, erfolgt im nächsten Schritt die Festlegung der Schnittstellen der eingebundenen Ressource zu den verfügbaren Systemelementen.

Dabei ist insbesondere festzulegen, welche Art von Nachrichten zwischen der eingebundenen Ressource und den Systemelementen, zu denen die eingebundene Ressource Schnittstellen aufweist, ausgetauscht werden. Außerdem ist festzulegen, welcher Übertragungskanal dabei zur Geltung kommt. Bei dem Übertragungskanal kann eine direkte oder indirekte Übertragung stattfinden. Zur Bewältigung der Komplexität werden entsprechend des Designprinzips (reduzierte Komplexität) aus dem vorigen Unterkapitel möglichst geringe Anzahl an Schnittstellen und eine möglichst direkte Kommunikation zwischen der eingebundenen Ressource und den vorhandenen Systemelementen gefordert.

Bei einem direkten Übertragungskanal sind Sender und Empfänger direkt über die vorübergehende Schnittstelle miteinander verbunden. Das liegt beispielsweise dann vor, wenn die Funktionsallokation auf ein Systemelement erfolgt, das im Regelbetrieb ohnehin eine Schnittstelle zu dem deaktivierten Systemelement aufweist.

Bei einem indirekten Übertragungskanal liegt zwischen dem Sender und dem Empfänger ein Vermittler. Das liegt beispielsweise dann vor, wenn die Funktionsallokation auf eine externe Ressource (z.B. Betriebspersonal) erfolgt und dieses in der betrieblich-technischen Rückfallebene über eine Mensch-Maschine Schnittstelle mit den entsprechenden Systemelementen interagiert.

Wenn das Systemelement erfolgreich deaktiviert und die alternative Ressource eingebunden wurde, erfolgt eine Benachrichtigung der benachbarten Systemelemente darüber. Abschließend wird die Deaktivierung entsprechend des Designprinzips (Security) geprüft. Dabei wird geprüft, dass das deaktivierte Systemelement keine Outputs generiert und sofern ein Betriebspersonal als Ressource eingebunden wurde, eine Bestätigung durch das Betriebspersonal eingeholt wird, damit die Sicherheit der Betriebsführung in Störungssituation nicht beeinträchtigt wird. Der Ablauf der Adaptionsart Deaktivierung mit Funktionsallokation ist in der Abbildung 33 in Form eines Aktivitätsdiagramms dargestellt.

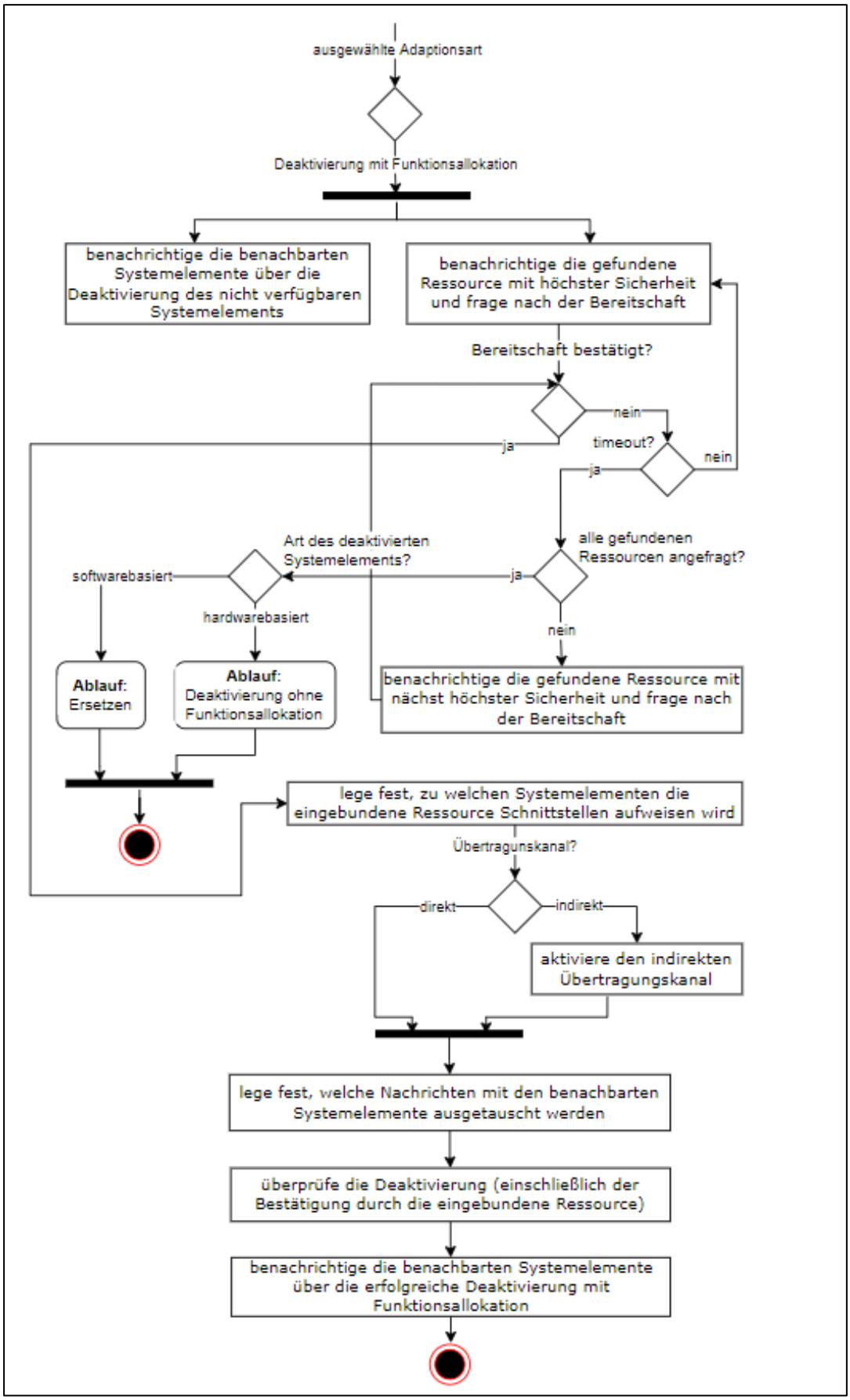

Abbildung 33 Ablauf der Adaptionsart Deaktivierung mit Funktionsallokation in Form eines Aktivitätsdiagramms

Rückkehr zum Regelbetrieb

Damit der Betrieb bei allen Adaptionsarten nicht dauerhaft in der Rückfallebene durchgeführt wird, ist entsprechend des Kapitels 2.5 nach Störungsbehebung der Regelbetrieb schnell wiederherzustellen.

Im Falle der dynamischen Adaptionsart – Ersetzen – erfolgt die Rückkehr in den Regelbetrieb dadurch, dass die Softwareanwendung oder Teile davon mit der ursprünglichen Spezifikation erneut anstelle der alternativen Softwareanwendung oder Teile davon eingespielt wird.

Im Falle der dynamischen Adaptionsart – Deaktivierung ohne Funktionsallokation– erfolgt die Rückkehr in den Regelbetrieb dadurch, dass das deaktivierte Systemelement nach Störungsbehebung erneut aktiviert wird.

Sofern eine Deaktivierung mit Funktionsallokation vorliegt, erfolgt die Rückkehr in den Regelbetrieb dadurch, dass die eingebundene Ressource aus der betrieblich-technischen Rückfallebene entfernt wird.

Auf Basis der Abläufe für die drei dynamischen Adaptionsarten zur Laufzeit werden im nächsten Kapitel beispielhafte betrieblich-technische Rückfallebenen für die in Kapitel 5.8 zusammengefassten gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb erarbeitet.

6.6 Beispielhafte betrieblich-technische Rückfallebenen im vollautomatisierten Bahnbetrieb auf Basis der dynamischen Adaption der Systemarchitektur zur Laufzeit

Bereits in Kapitel 5.4 wurden die ATO-relevanten Schutzziele erarbeitet. Die gefährlichen Betriebssituationen und ihre Gefährdungsursachen aus den beiden ATO-Regelkreisen wurden in Kapitel 5.6 erarbeitet. Die möglichen Gefährdungsursachen aus den beiden ATO-Regelkreisen sind in der Abbildung 34 auf der Seite 127 gelb dargestellt.

Ausgehend von der Erkenntnis aus dem Kapitel 5.6, dass die Kommunikationsverbindung zwischen einem ATO-Zug und dem TMS bzw. der ETCS-Zentrale unabdingbar ist (z.B. für die Übertragung von Journey-Profiles oder Fahrterlaubnissen) und eine Kommunikationsstörung auch eine Ursache für fehlende Journey-Profiles oder Fahrterlaubnisse sein kann, werden in Unterkapitel 6.6.1 zunächst für eine Kommunikationsstörung beispielhafte betrieblich-technische Rückfallebenen entwickelt. Durch betrieblich-technische Rückfallebenen für eine Kommunikationsstörung können mehrere gefährliche Betriebssituationen aus dem Kapitel 5.6 (z.B. verhinderte Weiterfahrt oder im Vergleich zum Regelbetrieb unsicherere Weiterfahrt) abgedeckt werden.

Eine weitere Erkenntnis aus dem Kapitel 5.6 ist es, dass im fahrzeugseitigen ATO-Regelkreis die Sensoren – insbesondere für Ortung und Lichtraumüberwachung – und das perzeptuelle Systemelement kritische Systemelemente darstellen, deren Rückkopplungen bzw. Kontrollaktionen das Verhalten des kognitiven Systemelements (Geschwindigkeitsprofil und Geschwindigkeitsregelung) beeinflussen. Trotz der verfügbaren Kommunikationsverbindung zwischen einem ATO-Zug und dem TMS bzw. der ETCS-Zentrale kann eine sichere und vollautomatisierte Zugfahrt aus dem Regelbetrieb im Falle von nicht verfügbaren Rückkopplungen aus den Sensoren oder Kontrollaktionen aus dem perzeptuellen Systemelement nicht gewährleistet werden. Unter der Annahme, dass eine Kommunikationsverbindung besteht, werden daher in Unterkapitel 6.6.2 beispielhafte betrieblich-technische Rückfallebenen für den Fall, dass entweder Sensoren oder die Kontrollaktionen aus dem perzeptuellen Systemelement nicht verfügbar sind, entwickelt.

Schließlich kann es auch vorkommen, dass eine Weiterfahrt verhindert ist, obwohl eine Kommunikationsversbindung besteht und die Sensoren sowie das perzeptuelle Systemelement funktionieren. Da die Ursachen für eine verhinderte Weiterfahrt auch im kognitiven Systemelement

(Geschwindigkeitsprofil oder Geschwindigkeitsregelung nicht verfügbar) liegen können, werden schließlich in Unterkapitel 6.6.3 beispielhafte betrieblich-technische Rückfallebenen für ein nicht-verfügbares kognitives Systemelement entwickelt.

Die Reihenfolge der in diesem Kapitel zu entwickelnden **beispielhaften** betrieblich-technischen Rückfallebenen auf Basis der dynamischen Adaption aus dem vorigen Kapitel ist zusammengefasst wie folgt:

- Weiterfahrt für mehrere Züge im gesamten ATO und ETCS Zuständigkeitsbereich nicht möglich oder im Vergleich zum Regelbetrieb unsicherere Weiterfahrt aufgrund einer Störung am infrastrukturseitigen Kommunikationssystem.
- im Vergleich zum Regelbetrieb unsicherere Weiterfahrt aufgrund von Störung an Sensoren zur Hinderniserkennung oder Störung am perzeptuellen Systemelement und
- Weiterfahrt nicht möglich aufgrund von nicht verfügbaren kognitiven Systemelement

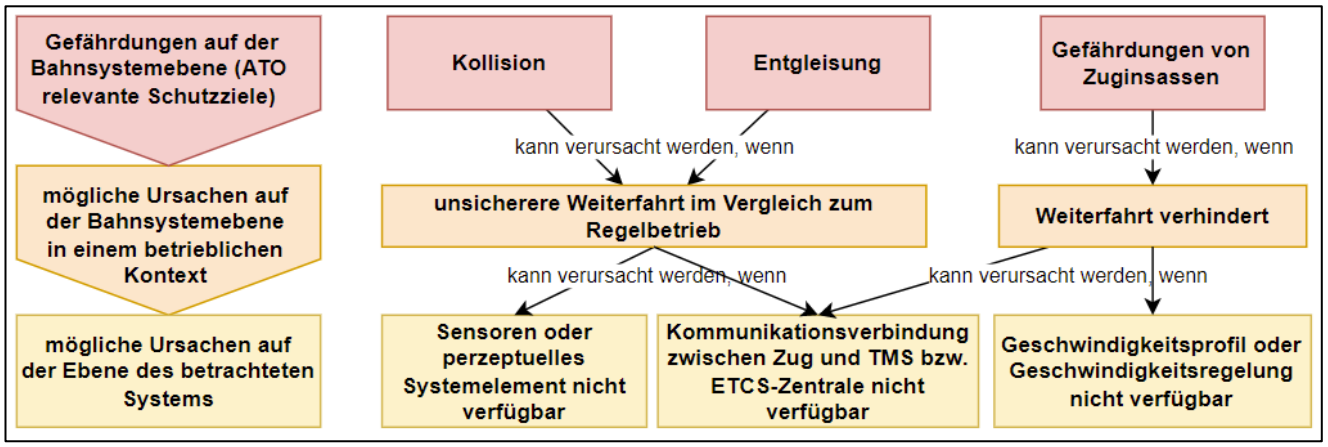

Abbildung 34 Gefährdungsursachen aus den beiden ATO-Regelkreisen, die gefährliche Betriebssituationen aus dem Kapitel 5.6 verursachen können, für die beispielhaft betrieblich-technische Rückfallebenen erarbeitet werden

6.6.1 Weiterfahrt nach dynamischer Adaption im Falle einer Kommunikationsstörung

Wie bereits aus dem Kapitel 5.6 bekannt, kann aufgrund von Störungen im Kommunikationssystem die zentrale Betriebsführung vorübergehend unterbrochen werden, sodass die Journey-Profiles oder Fahrterlaubnisse nicht übermittelt werden können. Für die Entwicklung von betrieblich-technischen Rückfallebenen bedeutet die Nichtverfügbarkeit des infrastrukturseitigen Kommunikationssystems, dass Lösungen für alternative Datenübertragung zwischen den betroffenen Zügen und TMS bzw. ETCS-Zentrale erforderlich sind, damit die betroffenen Züge erneut in den „Online-Modus“ wechseln können.

Aus dem Kapitel 2.4 ist bekannt, dass eine betrieblich-technische Rückfallebene im Falle einer Kommunikationsstörung nur für den ersten Zug (Entdeckerzug) erforderlich ist, sofern die Kommunikationsstörung infrastrukturseitig verursacht wurde. Für die restlichen Züge, die nicht von der Kommunikationsstörung betroffen sind, gibt es die bei ETCS L2 bereits etablierte und in Kapitel 2.4 vorgestellte betrieblich-technische Rückfallebene „Durchfahren gestörter Funkbereiche“.

Trotz der in Kapitel 2.4 vorgestellten betrieblich-technischen Rückfallebene „Durchfahren gestörter Funkbereiche“ kann es vorkommen, dass aufgrund eines Cyber-Angriffs nicht nur ein Zug unter der Kommunikationsstörung leidet, sondern die Kommunikationsstörung eine großflächige Auswirkung hat (z.B. gesamter ATO und ETCS Zuständigkeitsbereich > 32 km). Da eine Fahrterlaubnis nicht über 32 km hinweg erteilt werden kann, kann in diesem Fall die betrieblich-technische Rückfallebene

„Durchfahren gestörter Funkbereiche“ aus dem Kapitel 2.4 nicht mehr angewandt werden *(Trinckauf, 2020, S. 230)*.

Außerdem kann es vorkommen, dass sich ein Entdeckerzug nach am Ablauf der 40 s und der anschließenden Zwangsbremsung 5 min lang im Funkloch aufhält. In diesem Fall wird dieser Entdeckerzug entsprechend des Unterkapitels 2.4.2 aus dem ETCS-Speicher gelöscht, sodass keine Fahrterlaubnis mehr erteilt werden kann.

Prinzipiell ist es möglich, den Lösungsansatz nach *Aebersold und Schubert (2023)* aus dem Unterkapitel 2.4.4, der die Umschaltung des bahneigenen Funkspektrums auf das PMNO-Funkspektrum im Falle einer Kommunikationsstörung als Rückfallebene vorsieht, auch im vollautomatisierten Bahnbetrieb umzusetzen. Wie bereits oben erwähnt, kann aufgrund eines Cyber-Angriffs nicht nur ein Zug unter der Kommunikationsstörung leiden, sondern die Kommunikationsstörung kann eine großflächige Auswirkung haben. Sofern in diesem Fall die Umschaltung auf das öffentliche Kommunikationsnetz (PMNO-Funkspektrum) erfolgt, das ohnehin belastet ist, können Anforderungen hinsichtlich der Latenz und Bandbreite nicht erfüllt werden. Da die Funkfeldversorgung eine zentrale Rolle bei der Übertragung von Informationen zwischen den Zügen und der TMS bzw. ETCS-Zentrale spielt, kann die zur Verfügung stehende Bandbreite (10 MHz bei FRMCS Funkfrequenz von 1900 MHz vorgesehen) überlastet sein. Insbesondere für sogenannte Mission-Critical Communication, zu der die Videoübertragung im Falle einer Fernsteuerung von vollautomatisierten Zügen gehört, könnte nicht mehr gewährleistet sein bzw. nur dann gewährleistet sein, wenn andere nicht kritische Applikationen vorübergehend deaktiviert werden.

Ausgehend von dem Nachteil der basisstationsabhängigen Kommunikation im Falle einer Kommunikationsstörung werden in diesem Unterkapitel **zwei beispielhafte** betrieblich-technische Rückfallebenen auf Basis der dynamischen Adaption für eine alternative Datenübertragung zwischen den betroffenen Zügen und TMS bzw. ETCS-Zentrale beschrieben, die unabhängig von einer Basisstation fungieren.

Da durch eine infrastrukturseitige Kommunikationsstörung die funkbasierte Schnittstelle zwischen den Zügen und TMS bzw. ETCS-Zentrale unterbrochen wird, ist entsprechend des Ablaufdiagramms aus der Abbildung 30 die Adaptionsart Deaktivierung mit Funktionsallokation erforderlich. Die Funktionsallokation bedeutet hierbei, dass eine alternative Ressource einzubinden ist, die als Vermittler zwischen den betroffenen Zügen und dem TMS bzw. der ETCS-Zentrale fungiert, d.h. kommunikative Fähigkeiten aufweist. Bei der Funktionsallokation als Vermittler zwischen den betroffenen Zügen und dem TMS bzw. der ETCS-Zentrale kann es zudem vorkommen, dass Softwareanwendungen, die für die Kommunikation zuständig sind, ersetzt werden müssen.

In den nächsten beiden Abschnitten wird jeweils eine betrieblich-technische Rückfallebene zur Einrichtung eines Ad-Hoc Netzwerks im Falle einer infrastrukturseitigen Kommunikationsstörung beschrieben.

Weiterfahrt nach einem Ad-Hoc Netzwerk mit einem infrastrukturseitigen technischen System im Falle einer Kommunikationsstörung

Zunächst muss eine Kommunikationsstörung erkannt werden. Beim ETCS-System ist eine sogenannte Funküberwachungszeit vorhanden, die in Deutschland den nationalen Wert von 40 Sekunden hat. Bei Überschreitung dieser Funküberwachungszeit erfolgt eine Sicherheitsreaktion in Form einer Zwangsbremsung. Eine derartige Funküberwachungszeit ist zwar für das FRMCS noch nicht spezifiziert, jedoch wird in diesem Beispiel vereinfacht die 40 Sekunden angenommen.

Der Verbindungsabbruch wird sowohl von der infrastrukturseitigen als auch spätestens nach 40 Sekunden von der fahrzeugseitigen ATO-FMU erkannt.

Da das TMS die letzte Position der von der Kommunikationsstörung betroffenen Züge kennt, fordert die infrastrukturseitige ATO-FMU von dem TMS die Position der Züge an. Hierbei handelt es um eine geschätzte Position, da die Züge noch 40 Sekunden nach dem Verbindungsabbruch mit der letztbekannten Geschwindigkeit weiterfahren.

Bereits in *Essid, Klaus und Üyümez (2019)* wurden in Anlehnung an die RCA-Referenzarchitektur mögliche streckenseitige technische Systeme zum Aufbau eines Ad-Hoc Netzwerks im Falle einer Kommunikationsstörung vorgestellt. Demnach besteht im vollautomatisierten Bahnbetrieb im Falle einer infrastrukturseitigen Kommunikationsstörung für die betroffenen Züge die Möglichkeit, streckenseitige technische Systeme einzubinden, die über eine von der primären Funkschnittstelle unabhängige direkte Kommunikation zum DSTW und indirekt über das DSTW (bzw. Sicherungslogik) zum TMS verfügen. Dazu gehören beispielsweise die Object Controller (OC), die als Bindeglied zwischen den bereits installierten streckenseitigen Feldelementen (z.B. Weichen oder Bahnübergänge) und dem DSTW dienen. Ein Object Controller ist in einem Feldelemente-Anschlusskasten (FeAk) verortet und kann gleichzeitig mehrere streckenseitige Feldelemente ansteuern. Der Feldelemente-Anschlusskasten ist über das bahnbetriebliche IP-Netz mit dem Leit- und Bedienplatz des DSTW verbunden.

Nachdem die infrastrukturseitige ATO-FMU die geschätzte Position der Züge von dem TMS erhalten hat, fragt diese bei der Sicherungslogik die kompositionale Anpassung der Object Controller in dem Streckenabschnitt, indem sich die betroffenen Züge befinden, für eine Nahbereichskommunikation an. Die Object Controller bzw. die Sicherungslogik bestätigt die kompositionale Anpassung, sofern die primären Funktionen (z.B. Weichenumstellung oder Bahnübergangs-Schrankensteuerung) beendet sind.

Daraufhin erhalten die angefragten Object Controller von der infrastrukturseitigen ATO-FMU die Softwareanwendung für eine Nahbereichskommunikation. Damit können die Züge im Streckenabschnitt Anfragen für den Aufbau eines Ad-Hoc Netzwerkes an Object Controller stellen. Dazu ist es jedoch erforderlich, dass die betroffenen Züge auch eine Nahbereichskommunikation durchführen können. Nachdem die Softwareanwendung für eine Nahbereichskommunikation erfolgreich aktiviert wurde, erfolgt abschließend die Prüfung des Ersetzens. In diesem Beispiel wird geprüft, dass die Object Controller Anfragen für den Aufbau eines Ad-Hoc Netzwerkes annehmen können.

Die Nahbereichskommunikation auf den Zügen wird, nachdem die Funküberwachungszeit abgelaufen ist und die betroffenen Züge zwangsgebremst haben, durch die fahrzeugseitige ATO-FMU eingerichtet. Dazu ersetzt die fahrzeugseitige ATO-FMU die Softwareanwendung im fahrzeugseitigen Kommunikationssystem durch eine Softwareanwendung für eine Nahbereichskommunikation, die sie in ihrer Service-Datenbank hat.

Nachdem die Softwareanwendung für eine Nahbereichskommunikation erfolgreich aktiviert wurde, erfolgt auch fahrzeugseitig die Prüfung des Ersetzens. In diesem Beispiel wird geprüft, dass das fahrzeugseitige Kommunikationssystem keine Kommunikationsverbindung über den regulären Übertragungskanal (Funkbasisstation) aufbaut, damit es nicht zu einer Interferenz kommt.

Da die Reichweite von den Kommunikationsstandards zum Aufbau eines Ad-Hoc Netzwerks im aktuellen Entwicklungsstand kurz ist (z.B. 1000 m bei ITS-G5 Standard) *(Bilgin und Gungor 2013)*, begrenzt sich dadurch auch der Erkundungsraum. Es kann also vorkommen, dass die Züge mit ihren Anfragen für ein Ad-Hoc Netzwerk die Object Controller nicht erreichen.

Sofern ein Object Controller für ein Ad-Hoc Netzwerk gefunden und angefragt wurde, wird von dem Object Controller die Identifikation des Zuges angefordert. Die Identifikation kann dabei die Zugnummer oder die ATO-ID gemeinsam mit der ETCS-ID sowie eine Kombination davon sein.

Um einen sicherheitskritischen Eingriff von außen zu verhindern, wird die vom Zug empfangene ID für eine Verifikation an die Sicherungslogik weitergeleitet. Erst nachdem die Identifikation des Zuges durch die Sicherungslogik verifiziert wurde, darf das fahrzeugseitige Kommunikationssystem die neue Fahrterlaubnis und das Journey-Profile für die Weiterfahrt anfordern und an die ETCS-OBU sowie an das kognitive Systemelement weiterleiten.

Sobald der Object Controller die neue Fahrterlaubnis von der Sicherungslogik und das Journey-Profile von dem TMS empfangen und an das fahrzeugseitige Kommunikationssystem weitergeleitet hat, wird die Verbindung zwischen dem fahrzeugseitigen Kommunikationssystem und dem Object Controller sofort getrennt. Die Trennung der Verbindung wird aus Sicherheitsgründen (Security) durch den Object Controller aktiviert.

Nachdem die betroffenen Züge die Fahrterlaubnis und das Journey-Profile für eine Weiterfahrt erhalten haben, triggert die infrastrukturseitige ATO-FMU bei der Sicherungslogik die Rückkehr der rekonfigurierten Object Controller in den ursprünglichen Zustand. Ebenfalls ersetzt die fahrzeugseitige ATO-FMU die Softwareanwendung für eine Nahbereichskommunikation im fahrzeugseitigen Kommunikationssystem durch die ursprüngliche Softwareanwendung, damit erneut die reguläre Funkverbindung nach dem Verlassen des gestörten Funkbereichs aufgebaut werden kann.

Ebenfalls erfolgt abschließend sowohl fahrzeugseitig als auch infrastrukturseitig die Überprüfung der inversen Rekonfiguration des fahrzeugseitigen Kommunikationssystems und der Object Controller.

Die Koordination der Deaktivierung mit Funktionsallokation zum Aufbau eines Ad-Hoc Netzwerks mit einem Object Controller durch die infrastrukturseitige und fahrzeugseitige ATO-FMU ist in der Abbildung 35 als Kommunikationsdiagramm dargestellt.

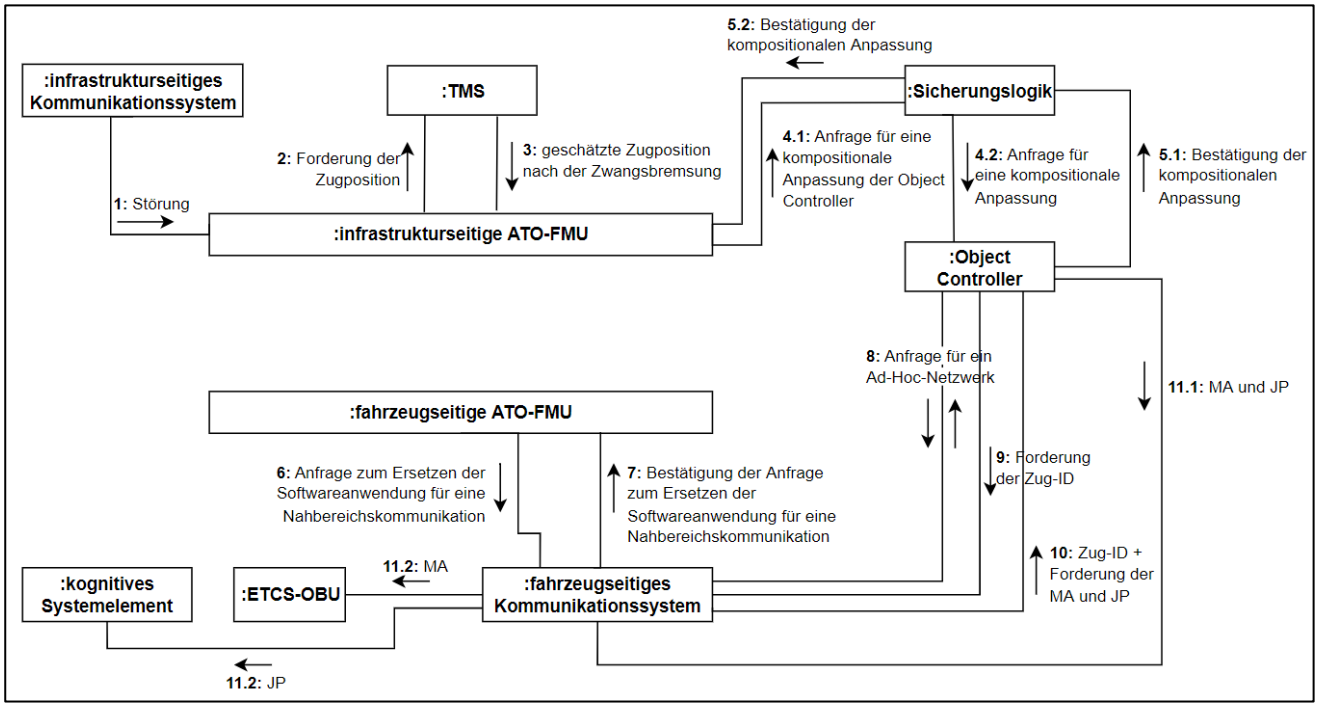

Abbildung 35 Kommunikationsdiagramm, das die Koordination zum Aufbau eines Ad-Hoc Netzwerks mit einem Object Controller darstellt

Weiterfahrt nach einem Ad-Hoc Netzwerk mit einem mobilen technischen System im Falle einer Kommunikationsstörung

Die bisher vorgestellte betrieblich-technische Rückfallebene zur Rückkehr der Züge in den „Online-Modus“ setzt voraus, dass sich die Object Controller nach dem Stillstand der Züge unmittelbar in der Nähe (im Erkundungsraum) befinden, sodass eine permissive Zwischenfahrt nicht erforderlich ist. Es kann jedoch vorkommen, dass die betroffenen Züge nach der Zwangsbremsung nicht in der Nähe eines Feldelements zum Stehen kommen und daher nicht direkt mit einem Object Controller kommunizieren können.

Prinzipiell ist es in diesem Fall zwar möglich, dass die Züge die Distanz bis zum Aufbau eines Ad-Hoc Netzwerks über eine vorübergehende Zwischenfahrt permissiv (z.B. ETCS OS-Modus auf Sicht) zurücklegen, jedoch ist eine derartige permissive Zwischenfahrt grundsätzlich risikobehaftet und auch nur dann möglich, wenn die Sensoren zur Hinderniserkennung und eine präzise Ortung des betroffenen Zuges verfügbar sind.

Um eine permissive Zwischenfahrt der betroffenen Züge zu vermeiden, könnten dichtere Kommunikationspunkte entlang der Infrastruktur eingerichtet werden, an denen die betroffenen Züge Ad-Hoc Netzwerke aufbauen können. Derartige dichtere Kommunikationspunkte erhöhen jedoch die Anzahl der Feldelemente und verursachen nicht vernachlässigbare Kosten.

Um eine permissive Zwischenfahrt der betroffenen Züge zu vermeiden und gleichzeitig die Anforderung aus dem Kapitel 6.2 hinsichtlich der möglichst niedrigen Kosten für die Ressourcen einhalten zu können, eignet es sich, auf Lösungen mit dynamischen Ad-Hoc Netzwerken zurückzugreifen.

Wie bereits in Kapitel 2.5 vorgestellt, können Drohnen im Falle von Kommunikationsstörungen ein fliegendes Ad-Hoc Netzwerk bilden und dabei als Vermittler eingesetzt werden. Der Einsatz von Drohnen im gegenwärtigen Bahnbetrieb ist entsprechend des Unterkapitels 2.5.2 auf Vegetationskontrolle oder Inspektion von Brücken und Bauwerken begrenzt. Das Potenzial für die Einbindung von Drohnen in die Betriebsführung ist zwar bisher nicht untersucht worden. Aufgrund ihrer mobilen Eigenschaft und aufgrund der Tatsache, dass prinzipiell mit einer Drohne ein Ad-Hoc Netzwerk mit mehreren Zügen gleichzeitig gebildet werden kann, eignet sich jedoch eine Drohne zum Aufbau eines Ad-Hoc Netzwerks mit Zügen, die von einer infrastrukturseitigen Kommunikationsstörung betroffen sind. Im Weiteren wird daher eine Drohne als ein mobiles technisches System zum Aufbau eines Ad-Hoc Netzwerks angenommen und der Ablauf der dynamischen Adaption zur Übermittlung von Journey-Profiles bzw. Fahrterlaubnissen erläutert.

Im Falle einer Kommunikationsstörung wird der Verbindungsabbruch sowohl von der infrastrukturseitigen als auch spätestens nach 40 Sekunden von der fahrzeugseitigen ATO-FMU erkannt und die infrastrukturseitige ATO-FMU fordert von dem TMS eine Drohne an die Position der betroffenen Züge an. Da die Züge noch 40 Sekunden nach dem Verbindungsabbruch mit der letztbekannten Geschwindigkeit weiterfahren, handelt es sich hierbei um eine geschätzte Position.

Das TMS sucht nach geeigneten Drohnen in der Umgebung und fragt die am nächsten zu den Zügen befindliche Drohne für eine Bereitschaft an. Nachdem die angefragte Drohne die Bereitschaft bestätigt hat, fordert die infrastrukturseitige ATO-FMU von der Sicherungslogik die Fahrterlaubnisse und von dem TMS die Journey-Profiles an.

Anschließend übermittelt die infrastrukturseitige ATO-FMU die empfangenen Fahrterlaubnisse und Journey-Profiles sowie die Anzahl und die aktuelle Position der betroffenen Züge einschließlich des gesamten Funklochbereichs an die Drohne.

Nachdem die Funküberwachungszeit abgelaufen ist und die betroffenen Züge zwangsgebremst haben, ersetzt die fahrzeugseitige ATO-FMU die Softwareanwendung im fahrzeugseitigen FRMCS durch eine alternative Softwareanwendung für eine Nahbereichskommunikation, die sie in ihrer Service-Datenbank hat *(vgl. Cellarius et al. 2021, S. 36)*.

Nachdem die Softwareanwendung für eine Nahbereichskommunikation erfolgreich aktiviert wurde, erfolgt auch fahrzeugseitig die Prüfung des Ersetzens. In diesem Beispiel wird geprüft, dass das fahrzeugseitige FRMCS keine Kommunikationsverbindung über den regulären Übertragungskanal (Funkbasisstation) aufbaut.

Sobald die Drohne bei den Zügen angekommen ist, fragt diese den betroffenen Zügen für ein Ad-Hoc Netzwerk an. Dazu ist eine Kommunikationsverbindung erforderlich. Da sowohl der Zug als auch die Drohne im gleichen Bahnnetz verbunden sind, wäre eine Kommunikation über FRMCS möglich. Um jedoch den langen Kommunikationsweg über eine Funkbasisstation wegen der Latenzzeit zu vermeiden, könnte eine direkte Nahfeldkommunikation zwischen der Drohne und dem Zug aktiviert werden. Das geschieht dadurch, dass die fahrzeugseitige ATO-FMU die Softwareanwendung im fahrzeugseitigen FRMCS durch eine alternative Softwareanwendung für eine Nahbereichskommunikation ersetzt *(vgl. Cellarius et al. 2021, S. 36)*.

Nach dem Aufbau der Nahbereichskommunikationsverbindung wird aus Security-Gründen eine ID-Verifizierung durchgeführt. Dazu vergleicht die fahrzeugseitige ATO-FMU die zuvor von der infrastrukturseitigen ATO-FMU empfangene Drohnen-ID mit der von der Drohne übermittelten ID. Erst nachdem die Identifikation der Züge durch die Drohne verifiziert wurde, erfolgt die Übermittlung der neuen Fahrterlaubnisse und der Journey-Profiles für die Weiterfahrt an das fahrzeugseitige Kommunikationssystem, das dann die Fahrterlaubnisse an die ETCS-OBU und die Journey-Profiles an das kognitive Systemelement weiterleitet.

Sobald die Fahrterlaubnisse an die ETCS-OBU und die Journey-Profiles an das kognitive Systemelement weitergeleitet wurden, wird die Verbindung zwischen dem fahrzeugseitigen Kommunikationssystem und der Drohne sofort getrennt. Die Trennung der Verbindung wird aus Sicherheitsgründen (Security) durch das fahrzeugseitige Kommunikationssystem aktiviert.

Die Drohne fliegt zum Ursprungsort und meldet anschließend die erfolgreiche Übermittlung der Fahrterlaubnisse und der Journey-Profiles an die infrastrukturseitige ATO-FMU. Die fahrzeugseitige ATO-FMU ersetzt die Softwareanwendung für eine Nahbereichskommunikation im fahrzeugseitigen Kommunikationssystem durch die ursprüngliche Softwareanwendung, damit erneut die reguläre Funkverbindung nach dem Verlassen des gestörten Funkbereichs aufgebaut werden kann.

Abschließend erfolgt fahrzeugseitig die Überprüfung der inversen Rekonfiguration des fahrzeugseitigen Kommunikationssystems.

Die Koordination der Deaktivierung mit Funktionsallokation zum Aufbau eines Ad-Hoc Netzwerks mit einer Drohne durch die infrastrukturseitige und fahrzeugseitige ATO-FMU ist in der Abbildung 36 als Kommunikationsdiagramm dargestellt.

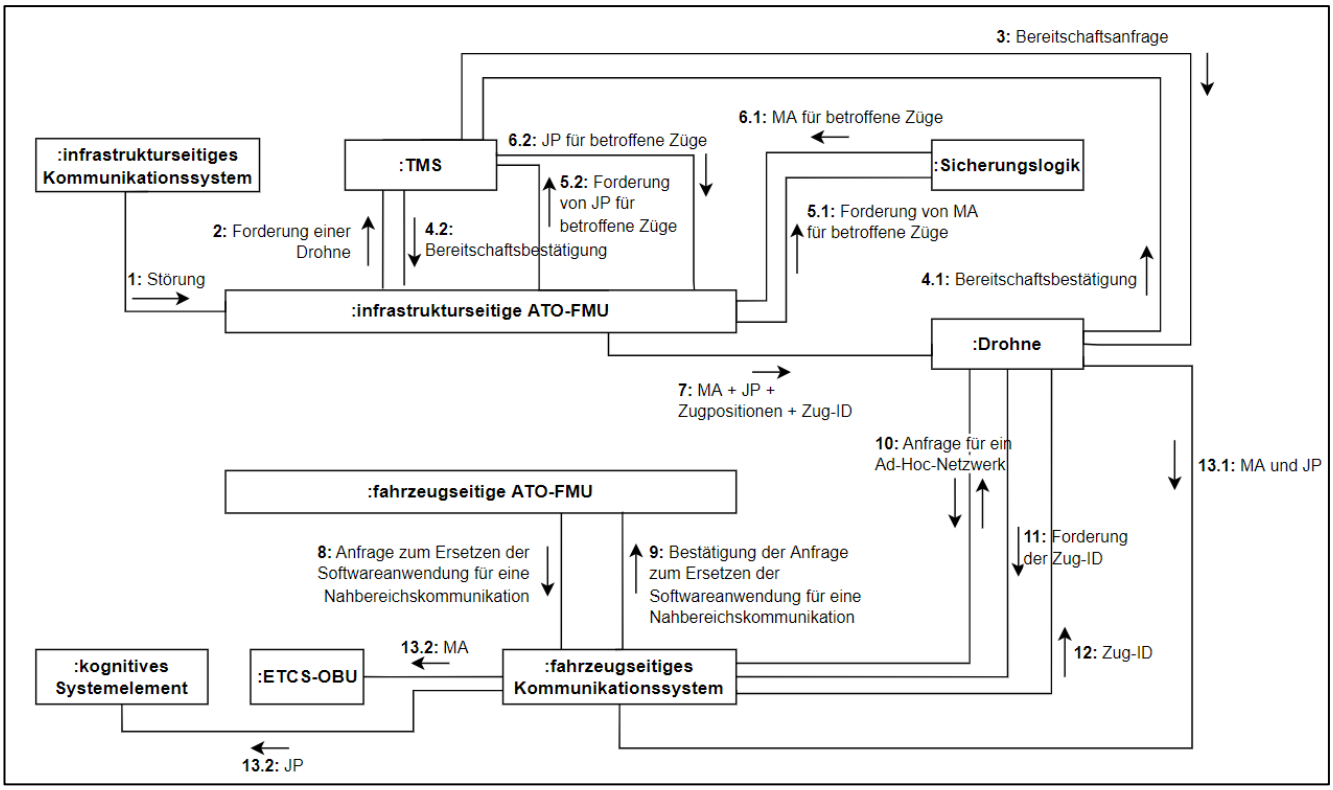

Abbildung 36 Kommunikationsdiagramm, das die Koordination zum Aufbau eines Ad-Hoc Netzwerks mit einer Drohne darstellt

Es ist absehbar, dass diese Art des Ad-Hoc Netzwerks von der Entfernung der Drohnen zu den betroffenen Zügen abhängig ist und daher länger als ein Ad-Hoc Netzwerk mit einem Object Controller andauern kann. Jedoch wäre damit eine vorübergehende risikobehaftete permissive Zwischenfahrt der Züge vermieden.

Mit den in diesem Unterkapitel entwickelten beispielhaften betrieblich-technischen Rückfallebenen für eine Kommunikationsstörung können mehrere gefährliche Betriebssituationen aus dem Kapitel 5.6 (z.B. verhinderte Weiterfahrt oder im Vergleich zum Regelbetrieb unsicherere Weiterfahrt) durch einen automatisierten Ablauf begegnet werden. Entsprechend der Vorgehensweise in Kapitel 6.6 erfolgt als nächster die Entwicklung von beispielhaften betrieblich-technischen Rückfallebenen für den Fall, dass entweder Sensoren oder die Kontrollaktionen aus dem perzeptuellen Systemelement nicht verfügbar sind.

6.6.2 Sichere Weiterfahrt nach dynamischer Adaption des perzeptuellen Systemelements

Wie bereits in Kapitel 5.6 erläutert, kann eine im Vergleich zum Regelbetrieb sichere Weiterfahrt verhindert sein, wenn entweder Sensoren zur Hinderniserkennung oder das zugehörige perzeptuelle Systemelement nicht verfügbar sind. Dadurch kann das Schutzziel Kollisionsvermeidung verletzt sein.

Da es sich bei den Sensoren um ein hardwarebasiertes Systemelement handelt, käme nur die Deaktivierung mit und ohne Funktionsallokation in Frage.

Wie bereits in Kapitel 2.3 vorgestellt, laufen immer noch Forschungsarbeiten über die konkrete Sensorkonstellation für die Hinderniserkennung. Bei Sensors4Rail werden dazu aktuell Radare, Lidare

und Kameras erprobt. Daher werden in den folgenden Abschnitten beispielhaft betrieblich-technische Rückfallebenen für die Störung an Kameras erarbeitet.

Weiterfahrt nach Deaktivierung der Sensoren ohne Funktionsallokation

Zunächst informiert die gestörte Kamera die fahrzeugseitige ATO-FMU darüber, dass es keine Rohdaten erfassen kann. Die ATO-FMU ordnet diese Störung dem entsprechenden Schutzziel aus der Abbildung 34 zu – in diesem Fall – sicherere Weiterfahrt (im Vergleich zum Regelbetrieb) verhindert und daher Kollisionsgefährdung.

Daraufhin erfolgt – wie beim Ersetzen – zunächst die Benachrichtigung der benachbarten Systemelemente darüber, dass die Kamera aus dem Regelbetrieb deaktiviert wird und daher keine Inputs verarbeiten und Outputs generieren kann. Dazu benachrichtigt die fahrzeugseitige ATO-FMU das perzeptuelle Systemelement darüber, dass die Kamera nicht mehr verfügbar ist.

Die Nichtverfügbarkeit der Kamera führt im perzeptuellen Systemelement dazu, dass die Objekte, die weiterhin durch die verbleibenden Sensoren (Radare und Lidare) erkannt werden, nicht klassifiziert werden können.

Deshalb ist – wie bereits in Unterkapitel 6.5.3 erläutert – ein Ausnahmemechanismus im perzeptuellen Systemelement erforderlich. Da im Falle einer Kamerastörung die Objekterkennung nicht mehr möglich ist, nutzt das perzeptuelle Systemelement Default-Werte der zu klassifizierenden Objekte. Wie in dem Beispiel in Unterkapitel 6.5.3 kurz genannt, kann das perzeptuelle Systemelement als Default-Wert annehmen, dass jedes erkannte Objekt ein schweres und ein großes Objekt ist, sodass damit verbundene Schadensausmaß hoch ist.

Nachdem die Kamera erfolgreich deaktiviert wurde, erfolgt abschließend die Prüfung der Deaktivierung. In diesem Beispiel wird geprüft, dass die deaktivierte Kamera keine Outputs generiert und dass der Ausnahmemechanismus im perzeptuellen Systemelement bestätigt wird und der Spezifikation entspricht. Wenngleich die Koordination der Deaktivierung ohne Funktionsallokation durch die fahrzeugseitige ATO-FMU durchgeführt werden kann, benachrichtigt die fahrzeugseitige ATO-FMU das TMS über die infrastrukturseitige ATO-FMU darüber, dass die Kamera deaktiviert und die Default-Werte im perzeptuellen Systemelement aktiviert wurden. Denn – wie bereits in Unterkapitel 6.5.3 erläutert – hätte die Deaktivierung ohne Funktionsallokation zur Folge, dass die Geschwindigkeit im kognitiven Systemelement reduziert wird. Die Koordination der dynamischen Adaptionsart Deaktivierung ohne Funktionsallokation durch die fahrzeugseitige ATO-FMU im Falle einer Kamerastörung ist in der Abbildung 37 als Kommunikationsdiagramm dargestellt.

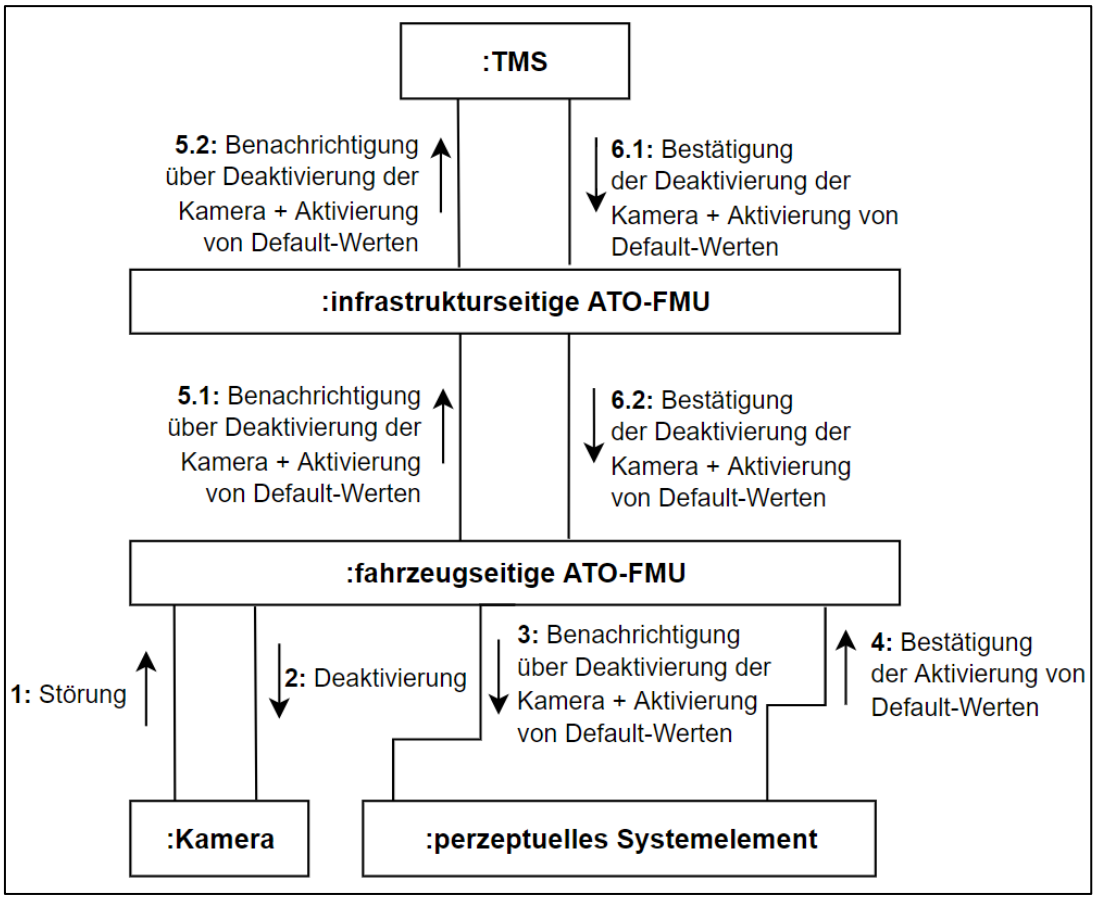

Abbildung 37 Kommunikationsdiagramm, das die Koordination während der Deaktivierung einer gestörten Kamera (**ohne** Funktionsallokation) darstellt

Am Ende der Fahrt in der betrieblich-technischen Rückfallebene mit deaktivierter Kamera, sollte die Kamera möglichst ersetzt werden, damit die Sicherheit des Betriebs nicht über einen längeren Zeitraum beeinträchtigt wird. Nach dem Ersetzen der gestörten Kamera durch eine alternative benachrichtigt die fahrzeugseitige ATO-FMU das perzeptuelle Systemelement darüber.

Weiterfahrt von GoA3 Personenzügen nach Deaktivierung der Kamera mit Funktionsallokation auf Zugpersonal

Im Vergleich zu der Deaktivierung der Kamera, wodurch die Sicherheit des Betriebs beeinträchtigt werden kann, gibt es auch die Möglichkeit, die Deaktivierung mit Funktionsallokation durchzuführen. Wie bereits in der Literatur vorgeschlagen und in Kapitel 2.4 vorgestellt, kann bei Personenzügen das Zugpersonal zur Übernahme der Lichtraumüberwachung vorübergehend eingebunden werden. Das Zugpersonal erfüllt das Designprinzip aus dem Unterkapitel 6.5.3. hinsichtlich der erforderlichen Fähigkeit, da es sowohl sensorische als auch perzeptuelle Fähigkeiten aufweist.

Die Koordination der Mensch-Maschine Kooperation zur Übernahme der Lichtraumüberwachung wird im Weiteren beschrieben.

Wie im vorigen Beispiel erfolgt zunächst die Benachrichtigung der benachbarten Systemelemente darüber, dass die Kamera aus dem Regelbetrieb deaktiviert wird und daher keine Inputs verarbeiten und Outputs generieren kann. Außerdem kann in diesem Beispiel auch das perzeptuelle Systemelement

deaktiviert werden, da das Zugpersonal neben sensorische auch perzeptuelle Fähigkeiten aufweist. Daher deaktiviert die fahrzeugseitige ATO-FMU auch das perzeptuelle Systemelement.

Da sich das Zugpersonal im Zug befindet, wird es anschließend von der fahrzeugseitigen ATO-FMU für die Bereitschaft angefragt. Die möglichen Arten der Einbindung eines Zugpersonals in eine betrieblich-technische Rückfallebene wurden in *Üyümez und Oetting (2019)* beschrieben. Ebenfalls in *Üyümez (2019)* wurden die möglichen Aufgabengebiete eines Zugpersonals in einer betrieblich-technischen Rückfallebene erarbeitet.

Das Zugpersonal begibt sich nach Bestätigung der Bereitschaft zum Führerstand, sobald seine primäre Aufgabe erledigt ist. Nachdem das Zugpersonal im Führerstand angekommen ist, bestätigt es die Ankunft über das DMI. Da das eingebundene Zugpersonal mit den fahrzeugseitigen Systemelementen nur über das DMI kommuniziert, kann das Designprinzip aus dem Unterkapitel 6.5.3 hinsichtlich der reduzierten Komplexität eingehalten werden.

Wenngleich die Koordination der Deaktivierung mit Funktionsallokation auf ein Zugpersonal durch die fahrzeugseitige ATO-FMU durchgeführt werden kann, benachrichtigt die fahrzeugseitige ATO-FMU das TMS über die infrastrukturseitige ATO-FMU darüber, dass die Kamera und das perzeptuelle Systemelement deaktiviert und ein Zugpersonal eingebunden wurde.

Nachdem die Kamera erfolgreich deaktiviert wurde, erfolgt abschließend die Prüfung der Deaktivierung. Auch in diesem Beispiel wird geprüft, dass die deaktivierte Kamera keine Outputs generiert. Außerdem wird geprüft, dass das perzeptuelle Systemelement ebenfalls keine Inputs verarbeitet und keine Outputs generiert. Schließlich erfolgt auch eine Bestätigung durch das Zugpersonal über das DMI, dass die sensorische und perzeptuelle Funktion vorübergehend durch das Zugpersonal übernommen wird.

Nach der Bestätigung der sensorischen und der perzeptuellen Funktion durch das Zugpersonal kann die Weiterfahrt gestartet werden, sofern die neue MA erhalten wurde. Die Aufgabe des eingebundenen Zugpersonals besteht darin, das Freisein des vorausliegenden Streckenabschnitts zu überwachen und bei gefahrdrohender Situation das Aktor-Systemelement für eine Zwangsbremsung zu aktivieren.

Die Koordination der Deaktivierung einer gestörten Kamera mit Funktionsallokation auf ein Zugpersonal durch die fahrzeugseitige ATO-FMU ist in der Abbildung 38 als Kommunikationsdiagramm dargestellt.

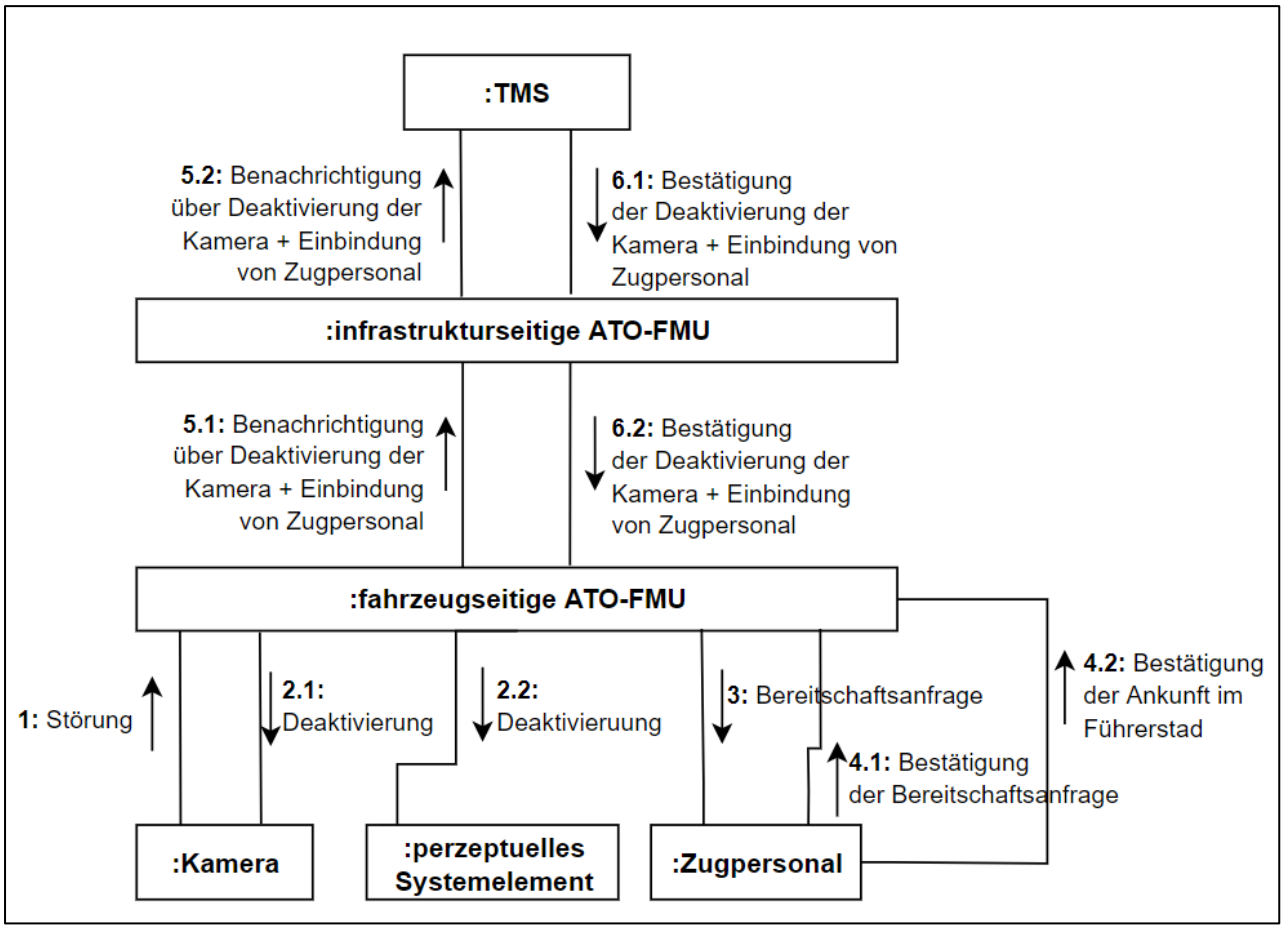

Abbildung 38 Kommunikationsdiagramm, das die Koordination während der Deaktivierung einer gestörten Kamera (mit Funktionsallokation auf Zugpersonal) darstellt

Am Ende der Fahrt in der betrieblich-technischen Rückfallebene mit deaktivierter Kamera, sollte die Kamera möglichst ersetzt werden, damit das Zugpersonal nicht durchgehend die Lichtraumüberwachung übernehmen muss und dadurch die Sicherheit des Betriebs nicht über einen längeren Zeitraum beeinträchtigt wird.

Wie bereits in *Üyümez (2019)* beschrieben, ist die alleinige Fernsteuerung durch den Train-Operator ist aus Sicherheitsgründen nicht sinnvoll, da keine vollständige Sicht auf den vorausliegenden Streckenabschnitt besteht. Dennoch kann bei Personenzügen im Falle einer Kamerastörung eine Fernsteuerung mit Unterstützung durch ein Zugpersonal vorgenommen werden.

Da das eingebundene Zugpersonal im Falle einer Kamerastörung primär als visueller Informationskanal für den Train-Operator wirken soll, der weiterhin die Geschwindigkeitsregelung vornimmt, ist eine Interaktion des Zugpersonals mit den technischen Systemen im Führerstand nicht notwendigerweise erforderlich. Das Kommunikationsdiagramm einer Mensch-Maschine Kooperation mit einem Train-Operator und einem Zugpersonal ist in Anhang 1 dargestellt.

Weiterfahrt von GoA4 Güterzügen nach Deaktivierung der Kamera mit Funktionsallokation auf eine Drohne

Die vorige beispielhafte betrieblich-technische Rückfallebene für die Lichtraumüberwachung durch ein Zugpersonal gilt nur bei den GoA3 geführten Personenzügen. Um die Abweichung von der vereinbarten Betriebsqualität im betroffenen Streckenabschnitt aufgrund des unerwünschten Stillstands zu reduzieren, sollten auch GoA4 geführte Güterzüge trotz der fehlenden Lichtraumüberwachung aufgrund einer Kamerastörung auch weiterfahren können.

Da sich auf GoA4 geführten Güterzügen entsprechend der Definition des Automatisierungsgrades kein Zugpersonal befindet, müsste sich zunächst ein Betriebspersonal zu dem betroffenen Güterzug begeben, um die betrieblich-technische Rückfallebene aus dem vorigen Beispiel umzusetzen.

Jedoch kann die Einbindung eines externen Betriebspersonals aufgrund größerer Entfernungen zum Güterzug lange dauern und dadurch kann das Designprinzip aus dem Unterkapitel 6.5.3 hinsichtlich der möglichst kurzen Dauer der betrieblich-technischen Rückfallebene nicht eingehalten werden.

Wie bereits in Kapitel 2.5 vorgestellt und in Unterkapitel 6.6.1 als mobiles technisches System zum Aufbau eines Ad-Hoc Netzwerks herangezogen, können Drohnen, die über verschiedene Kameratypen verfügen, in Zukunft auch als mobile Sensorsysteme ersatzweise die Lichtraumüberwachung übernehmen und den betroffenen Güterzug beispielsweise bis an die nächste Betriebsstelle führen. Im Gegensatz zum externen Betriebspersonal nutzt eine Drohne den Luftweg und kann daher den betroffenen Güterzug bei gleicher Entfernung schneller erreichen als das externe Betriebspersonal.

Sofern eine Drohne zur Übernahme der Lichtraumüberwachung eingebunden wird, entsteht eine funkbasierte Schnittstelle zwischen dem fahrzeugseitigen Kommunikationssystem und der Drohne. Bei der Einbindung eines externen Betriebspersonals ist hingegen wie bei dem vorigen Beispiel mit GoA3 geführten Personenzügen ein DMI erforderlich. Da in beiden Fällen die externen Ressourcen (Betriebspersonal und Drohne) bei der Interaktion mit den fahrzeugseitigen Systemelementen eine einzige Schnittstelle brauchen, ist die Komplexität gleich.

Die funkbasierte Schnittstelle zwischen dem fahrzeugseitigen Kommunikationssystem und einer Drohne ist tendenziell ein Angriffsziel für Cyber-Angreifer und bedarf daher einer geeigneten Sicherheitsmaßnahme. Bei der Einbindung eines externen Betriebspersonals kann die Handlungssicherheit von der Stresssituation des Betriebspersonals abhängen *(vgl. Lindner et al. 2014)*. Eine derartige stresssituationsabhängige Handlungssicherheit gibt es bei einer Drohne als eine technische Ressource hingegen nicht.

Damit GoA4 geführte Güterzüge im Falle einer fehlenden Lichtraumüberwachung aufgrund einer Kamerastörung weiterfahren können, ohne dabei lange auf ein Betriebspersonal zu warten, wird im Weiteren die Koordination der Deaktivierung der Kamera mit Funktionsallokation auf eine Drohne zur Übernahme der Lichtraumüberwachung beschrieben.

Zunächst erfolgt auch bei diesem Beispiel die Benachrichtigung des perzeptuellen Systemelements darüber, dass die Kamera aus dem Regelbetrieb deaktiviert wird und daher keine Inputs verarbeiten und Outputs generieren kann.

Daraufhin fragt die fahrzeugseitige ATO-FMU bei der infrastrukturseitigen ATO-FMU nach der Bereitschaftsanfrage einer Drohne für die Übernahme der Lichtraumüberwachung an. Da die Suche und Bereitschaftsanfrage über eine funkbasierte Schnittstelle erfolgt, sollten die Drohnen über Lokalisierungssensoren verfügen und im FRMCS Bahnnetz (5G) integriert sein.

Nach der Bereitschaftsbestätigung der gefundenen und angefragten Drohne, wird von dem TMS der Standort und die ID des gestörten Zuges, die Betriebsstelle bis zu der gefahren werden soll und die maximale Geschwindigkeit (hängt von der Fluggeschwindigkeit der Drohne ab), mit der der gestörte Zug geführt werden soll, an die Drohne übermittelt.

Wie bereits in Unterkapitel 6.6.1 erläutert, kann die Drohne, den Aufbau eines Ad-Hoc Netzwerks mit dem betroffenen Zug über eine direkte Nahfeldkommunikation anfragen. Nach dem Aufbau der Nahbereichskommunikationsverbindung wird aus Security-Gründen eine ID-Verifizierung durchgeführt. Dazu vergleicht die fahrzeugseitige ATO-FMU die zuvor von der infrastrukturseitigen ATO-FMU empfangene Drohnen-ID mit der von der Drohne übermittelten ID. Sobald diese übereinstimmt, wird anschließend eine Schnittstelle zwischen der Drohne und dem perzeptuellen Systemelement eingerichtet.

Nachdem die Deaktivierung der Kamera und die Einbindung der Drohne erfolgreich durchgeführt wurden, erfolgt abschließend die Prüfung der Deaktivierung und die Einbindung der Drohne. Auch in diesem Beispiel wird geprüft, dass die deaktivierte Kamera keine Outputs generiert. Außerdem wird geprüft, dass das perzeptuelle Systemelement ebenfalls keine Inputs von der gestörten Kamera verarbeitet und keine Outputs generiert. Zudem wird geprüft, ob die Drohne die für das perzeptuelle Systemelement relevanten Kameradaten (Inputs) liefert.

Die Koordination der Deaktivierung einer gestörten Kamera mit Funktionsallokation auf eine Drohne durch die fahrzeugseitige ATO-FMU ist in der Abbildung 39 als Kommunikationsdiagramm dargestellt.

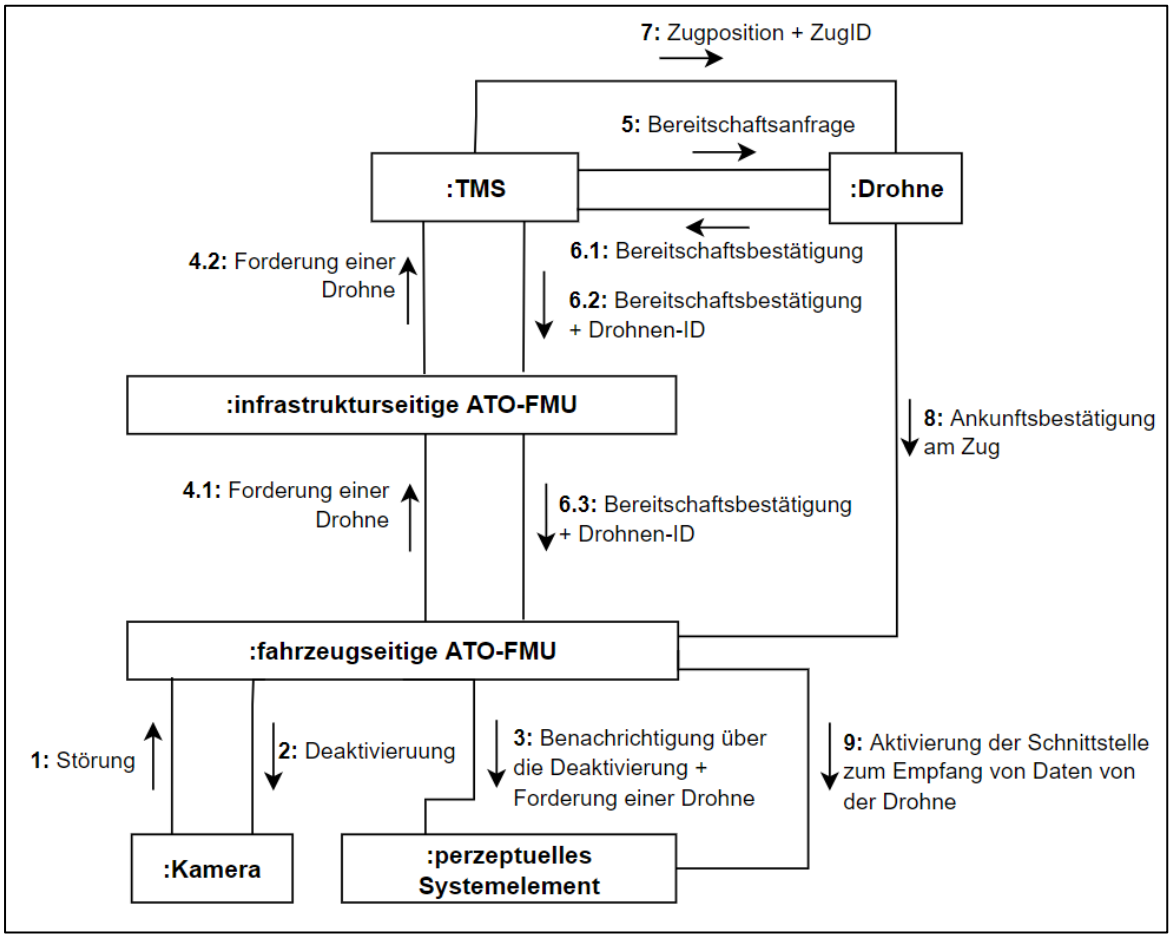

Abbildung 39 Kommunikationsdiagramm, das die Koordination während der Deaktivierung einer gestörten Kamera (mit Funktionsallokation auf eine Drohne) darstellt

Am Ende der Fahrt in der betrieblich-technischen Rückfallebene mit deaktivierter Kamera, sollte die Kamera möglichst ersetzt werden, damit die Zugfahrt nicht durchgehend drohnengeführt stattfindet und dadurch die Sicherheit des Betriebs und die Betriebsqualität nicht über einen längeren Zeitraum beeinträchtigt wird. Nachdem Ersetzen der gestörten Kamera durch eine alternative benachrichtigt die fahrzeugseitige ATO-FMU das perzeptuelle Systemelement darüber.

Mit den in diesem Unterkapitel entwickelten beispielhaften betrieblich-technischen Rückfallebenen für den Fall, dass entweder Sensoren oder die Kontrollaktionen aus dem perzeptuellen Systemelement nicht verfügbar sind, kann die Lichtraumüberwachung ersatzweise und weitgehend automatisiert übernommen werden, sodass die gefährlichen Betriebssituationen aus dem Kapitel 5.6, die aufgrund fehlender Lichtraumüberwachung entstehen können, begegnet werden. Entsprechend der Vorgehensweise in Kapitel 6.6 erfolgt schließlich noch die Entwicklung von beispielhaften betrieblich-technischen Rückfallebenen für den Fall, dass das kognitive Systemelement nicht verfügbar ist, sodass eine Weiterfahrt der vollautomatisierten Züge nicht möglich ist.

6.6.3 Weiterfahrt nach dynamischer Adaption des kognitiven Systemelements

Unter der Annahme, dass sowohl die Kommunikationsverbindung verfügbar ist als auch die Sensoren oder das perzeptuelle Systemelement die erforderlichen Rückkopplungen bzw. Kontrollaktionen liefern, kann eine Weiterfahrt auch dann verhindert sein, wenn das kognitive Systemelement nicht verfügbar ist und dadurch kein Geschwindigkeitsprofil erstellt werden kann.

Da es sich bei dem kognitiven Systemelement um eine Softwareanwendung handelt, kämen prinzipiell alle drei Adaptionsarten aus dem vorigen Kapitel in Frage. Da im Falle von Deaktivierung des kognitiven Systemelements ohne Funktionsallokation die Geschwindigkeitsregelung nicht erfolgen kann und damit eine Weiterfahrt verhindert wird, werden in diesem Unterkapitel beispielhafte betrieblich-technische Rückfallebenen auf Basis des Ersetzens und der Deaktivierung mit Funktionsallokation erarbeitet.

Weiterfahrt nach Ersetzen des Algorithmus zur Generierung eines Geschwindigkeitsprofils durch ein festes Geschwindigkeitsprofil im kognitiven Systemelement

In diesem Abschnitt wird beispielhaft für den Fall, dass in dem kognitiven Systemelement kein Geschwindigkeitsprofil generiert werden kann, der Ablauf des Ersetzens beschrieben.

Da es sich bei dem kognitiven Systemelement um eine Softwareanwendung handelt, kann das Ersetzen auch während der Fahrt erfolgen, sofern das zuletzt aktive Geschwindigkeitsprofil noch abgefahren wird. Das kognitive Systemelement informiert zunächst die fahrzeugseitige ATO-FMU darüber, dass es kein Geschwindigkeitsprofil erstellen kann. Die fahrzeugseitige ATO-FMU ordnet diese Störung dem entsprechenden Schutzziel aus der Abbildung 34 zu – in diesem Fall – verhinderte Weiterfahrt und daher mögliche Gefährdung von Zuginsassen.

Anschließend werden die benachbarten Systemelemente über das Ersetzen benachrichtigt. Dazu versendet die fahrzeugseitige ATO-FMU entsprechend der funktionalen Systemarchitektur aus dem Kapitel 4.5 eine Nachricht mit dem Inhalt „kein Geschwindigkeitsprofil vorhanden“ an die Softwareanwendung, die den Regelungsalgorithmus enthält, da dieser das Geschwindigkeitsprofil als Referenz verwendet.

Da es darum geht, ein Geschwindigkeitsprofil für den Regelungsalgorithmus bereitzustellen, kämen folgende Alternativlösungen in Frage.

Zum einen könnte das kognitive Systemelement von der ETCS-OBU das Most-Restrictive-Speed Profile (MRSP) als festes Geschwindigkeitsprofil über die fahrzeugseitige ATO-FMU anfordern.

Da die ETCS-OBU eine direkte Schnittstelle zum kognitiven Systemelement hat, könnte diese zum anderen von der infrastrukturseitigen ATO-FMU die Funktion „Geschwindigkeitsprofil erstellen“ vorübergehend bereitgestellt bekommen, um ein alternatives Geschwindigkeitsprofil zu erstellen.

In der Datenbank für Services der infrastrukturseitigen ATO-FMU könnte außerdem ein alternatives Geschwindigkeitsprofil vorliegen, dass im Falle von Störungssituationen von den Zügen abgefahren wird, welches dann von der infrastrukturseitigen ATO-FMU über die fahrzeugseitige ATO-FMU an das kognitive Systemelement übermittelt wird.

Entsprechend des Designprinzips aus dem Unterkapitel 6.5.3 kann die Erstellung des Geschwindigkeitsprofils nicht auf die ETCS-OBU allokiert werden, da die ETCS-OBU nur eine Überwachungsfunktion und ein erhöhtes SIL aufweist, sodass die ETCS-OBU nicht nur die erforderliche Fähigkeit nicht aufweist, sondern die Rekonfiguration der ETCS-OBU zur Laufzeit das Prinzip der Rückwirkungsfreiheit verletzen würde.

Da in dem MRSP betriebliche Halte nicht vorgesehen sind und ein vollautomatisierter Zug auch in Störungssituationen betriebliche Halte haben kann, eignet es sich, ein festes Geschwindigkeitsprofil, das in der Datenbank für Services der infrastrukturseitigen ATO-FMU liegt, anzufordern. Da die beiden Systemelemente ATO-AE und kognitives Systemelement bereits über ATO-AT eine Schnittstelle aufweisen, muss dazu auch keine neue Schnittstelle eingerichtet werden. Dadurch wird das Designprinzip hinsichtlich der reduzierten Komplexität eingehalten.

Folglich erfolgt das Ersetzen des Algorithmus „Geschwindigkeitsprofil erstellen“ im kognitiven Systemelement dadurch, dass ein alternatives Geschwindigkeitsprofil durch das Systemelement ATO-AE erstellt und durch die ATO-FMU an das kognitive Systemelement übermittelt wird. Diese Funktion muss nicht im Systemelement ATO-AE extra implementiert sein, sondern liegt in der Datenbank für Services der infrastrukturseitigen ATO-FMU. Die infrastrukturseitige ATO-FMU kann diese Funktion vorübergehend an das Systemelement ATO-AE bereitstellen.

Zur Generierung eines Geschwindigkeitsprofils braucht das Systemelement ATO-AE entsprechend dem Ablauf aus der Abbildung 31 in Unterkapitel 6.5.4 die letzten gültigen Attribute der zu ersetzenden Softwareanwendung zur Generierung eines Geschwindigkeitsprofils. Die letzten gültigen Attribute bei der Erstellung des Geschwindigkeitsprofils können die bereits in Unterkapitel 6.5.4 auf Seite 119 angegebenen Attribute sein. Dazu zählen die aktuelle Position des Zuges, die letzte gültige Geschwindigkeit, verfügbares Beschleunigungsvermögen, das zuletzt als Referenz angenommene Journey-Profile und das Segment-Profile. Denn nur so kann das Systemelement ATO-AE ein Geschwindigkeitsprofil bis zum nächsten Zielpunkt – unter Berücksichtigung der betrieblichen Situation (z.B. betriebliche Konflikte mit anderen Zügen) – erstellen.

Nach dem Empfang der letzten gültigen Attribute der zu ersetzenden Softwareanwendung wird dann das abzufahrende Geschwindigkeitsprofil erstellt und über die fahrzeugseitige ATO-FMU an das kognitive Systemelement versendet.

Darauf aufbauend führt die fahrzeugseitige ATO-FMU entsprechend des Designprinzips aus dem Unterkapitel 6.5.3 einen Rekonfigurationscheck durch. Dabei wird geprüft, ob das kognitive

Systemelement das Geschwindigkeitsprofil an die Softwareanwendung, die den Regelungsalgorithmus enthält, als Kontrollaktion bereitstellt.

Schließlich erfolgt noch die Benachrichtigung der Softwareanwendung, die den Regelungsalgorithmus enthält, dass das Ersetzen erfolgreich war.

Die Koordination der dynamischen Adaptionsart Ersetzen durch die fahrzeugseitige ATO-FMU ist in der Abbildung 40 als Kommunikationsdiagramm dargestellt.

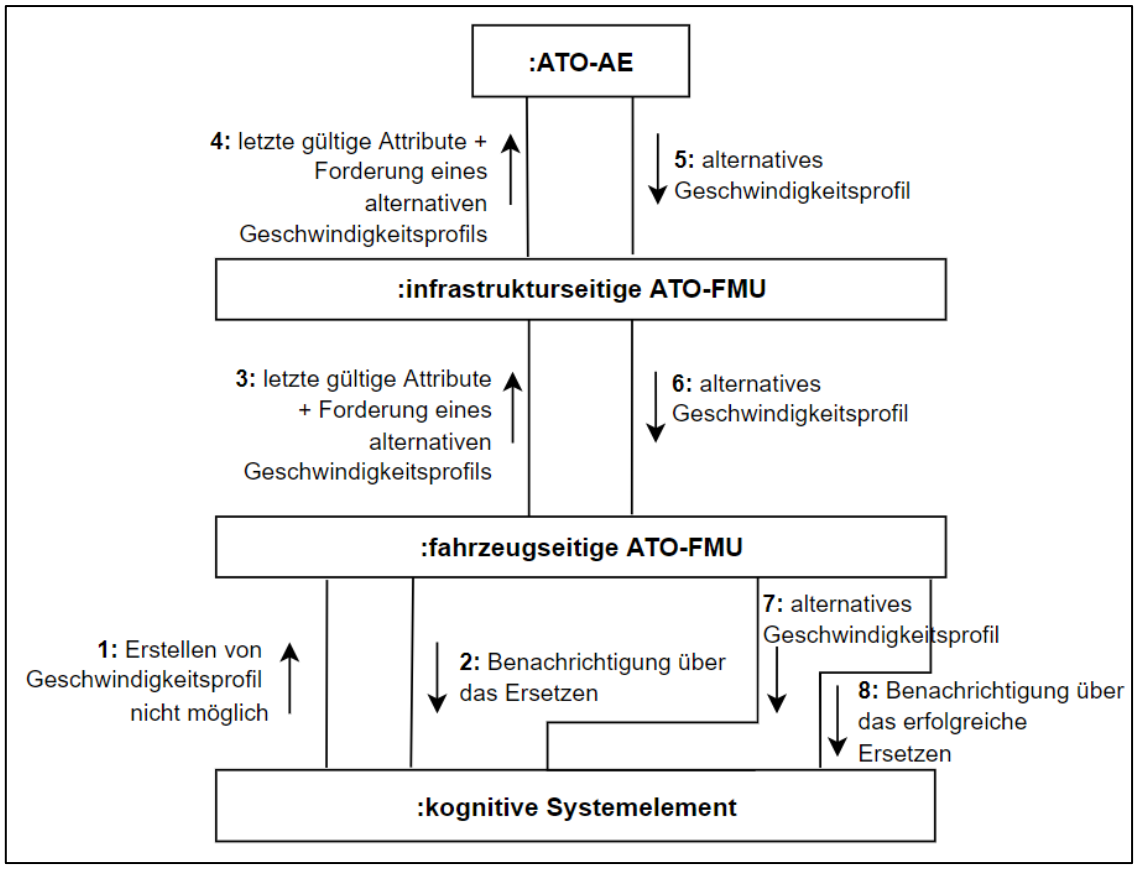

Abbildung 40 Kommunikationsdiagramm, das die Koordination während der dynamischen Adaption des kognitiven Systemelements (**Ersetzen**) darstellt

Am Ende der Fahrt in der betrieblich-technischen Rückfallebene mit einem festen Geschwindigkeitsprofil aktiviert die fahrzeugseitige ATO-FMU erneut das kognitive Systemelement und benachrichtigt zudem die Softwareanwendung mit dem Regelungsalgorithmus über die Beendigung der betrieblich-technischen Rückfallebene mit einem festen Geschwindigkeitsprofil.

Weiterfahrt nach Deaktivierung des kognitiven Systemelements mit Funktionsallokation

Statt des Ersetzens Algorithmus zur Generierung eines Geschwindigkeitsprofils im kognitiven Systemelement durch ein festes Geschwindigkeitsprofil wäre auch denkbar, das kognitive Systemelement zu deaktivieren und dessen betriebliche Funktion an eine andere Ressource zu allokieren.

Nachdem die Störungsmeldung durch das kognitive Systemelement wie beim Ersetzen bei der fahrzeugseitigen ATO-FMU eingetroffen ist und die Störung dem entsprechenden Schutzziel zugeordnet wurde, wird wie beim Ersetzen eine Nachricht mit dem Inhalt „kein Geschwindigkeitsprofil vorhanden“

an die Softwareanwendung, die den Regelungsalgorithmus enthält, versendet. Anders als beim Ersetzen wird in diesem Beispiel nun das komplette kognitive Systemelement deaktiviert, sodass auch keine Generierung von Steuerbefehlen an das Aktor-Systemelement erfolgt.

Wie bereits in Unterkapitel 2.4.4 vorgestellt, kann der Train-Operator zur Übernahme der Geschwindigkeitsregelung eingebunden werden. Die dafür erforderlichen Systemelemente sind bereits in der funktionalen Systemarchitektur aus dem Kapitel 4.5 vorhanden. Da ein Train-Operator mit den beiden Systemelementen ATOM und RMTO bereits im Regelbetrieb eine Schnittstelle zu den fahrzeugseitigen Systemelementen aufweist, wäre bei seiner Einbindung das Designprinzip hinsichtlich der reduzierten Komplexität eingehalten.

Da wie bereits in Kapitel 6.4 erläutert, das EIU bei der Einrichtung von betrieblich-technischen Rückfallebenen die Entscheidungshoheit hat, fragt die fahrzeugseitige ATO-FMU bei der infrastrukturseitigen ATO-FMU nach der Bereitschaftsanfrage eines Train-Operators für die Übernahme der Geschwindigkeitsregelung an. Die Bereitschaftsanfrage erfolgt dann über das TMS an das Systemelement ATOM (vgl. Kapitel 4.5) mit der Nachricht „Remote Control Request“.

Das Systemelement ATOM weist eine Schnittstelle zu dem entsprechenden Train-Operator auf. Dieser bestätigt daraufhin die Anfrage über die Übernahme der Geschwindigkeitsregelung mit der Nachricht „Remote Control Request Acknowledgement“. Die Bereitschaftsbestätigung wird an die fahrzeugseitige ATO-FMU weitergeleitet.

Da der Train-Operator nicht im Führerstand anwesend ist, braucht er die Sicht zum vorausliegenden Streckenabschnitt, weshalb die Rückkopplungen aus den Sensoren und die Kontrollaktionen vom perzeptuellen Systemelement an den Train-Operator übertragen werden müssen. Die fahrzeugseitige ATO-FMU beauftragt daher das perzeptuelle Systemelement, die von den Sensoren empfangenen Rückkopplungen an das Systemelement ATOM zu übertragen. Um jedoch dabei die Kommunikationsbandbreite nicht zu strapazieren, können die Rückkopplungen aus den Sensoren zunächst lokal auf dem Zug durch das perzeptuelle Systemelement vorverarbeitet und das Ergebnis an das Systemelement ATOM übertragen werden. Dadurch wird nicht nur Zeit eingespart und die begrenzte Kommunikationsbandbreite verschont, sondern auch die Fehlerwahrscheinlichkeit des Train-Operators reduziert.

Nachdem das perzeptuelle Systemelement über die neue Schnittstelle benachrichtigt wurde, versendet es die aktuelle Position des Zuges und die aktuelle Sicht auf den vorausliegenden Streckenabschnitt einschließlich der Eigenschaften der Sensoren (z.B. Auflösung, maximale Reichweite und maximale Winkelauflösung) an das Systemelement ATOM. Daraufhin bestätigt der Train-Operator die empfangenen Rückkopplungen. Dazu verschickt er über die infrastrukturseitige ATO-FMU eine Bestätigung an die fahrzeugseitige ATO-FMU.

Aus Sicherheitsgründen benachrichtigt die fahrzeugseitige ATO-FMU die ETCS-OBU über die Fernsteuerung mit der Nachricht, dass eine Fernsteuerung aktiviert wurde und die ETCS-OBU weiterhin in FS-Modus bleiben kann.

Nachdem sowohl die infrastrukturseitige als auch die fahrzeugseitige ATO-FMU die Bestätigung von dem Train-Operator erhalten haben, darf der Train-Operator das Systemelement RMTO aktivieren und somit die ferngesteuerte Geschwindigkeitsregelung starten.

Die Koordination der dynamischen Adaptionsart Deaktivierung mit Funktionsallokation durch die fahrzeugseitige ATO-FMU ist in der Abbildung 41 als Kommunikationsdiagramm dargestellt.

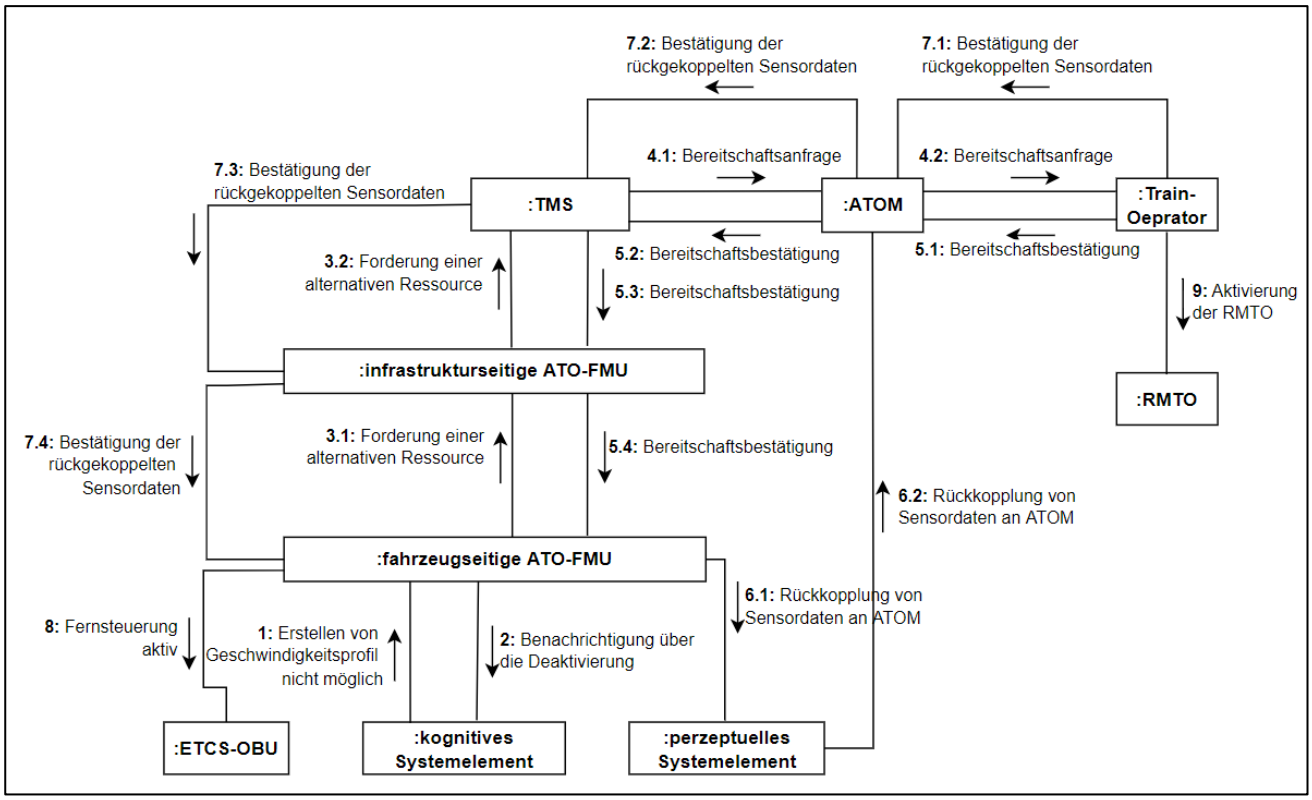

Abbildung 41 Kommunikationsdiagramm, das die Koordination während der dynamischen Adaption des kognitiven Systemelements (**Deaktivierung mit Funktionsallokation**) darstellt

Am Ende der Fahrt in der betrieblich-technischen Rückfallebene per Fernsteuerung benachrichtigt der Train-Operator die fahrzeugseitige ATO-FMU über die infrastrukturseitige ATO-FMU mit der Nachricht „Remote Control Termination“. Daraufhin aktiviert die fahrzeugseitige ATO-FMU erneut das kognitive Systemelement und benachrichtigt zudem das perzeptuelle Systemelement und die ETCS-OBU über die Beendigung der betrieblich-technischen Rückfallebene per Fernsteuerung.

Bei GoA3 geführten Personenzügen ist es auch denkbar, das Zugpersonal vorübergehend zu beauftragen, die Geschwindigkeitsregelung für eine Weiterfahrt in Störungssituation zu übernehmen. Damit bei der Mensch-Maschine Kooperation das eingebundene Zugpersonal in Störungssituation aufgrund der begrenzten Zeit nicht zu viele maschinelle Daten verarbeiten muss, wäre es sinnvoll, das Zugpersonal mit dem Train-Operator kooperieren zu lassen. Das eingebundene Zugpersonal kann verbale Anweisungen von dem Train-Operator empfangen, um die Geschwindigkeitsregelung ersatzweise zu übernehmen. Das Zugpersonal kann während der Geschwindigkeitsregelung gleichzeitig die Lichtraumüberwachung übernehmen und dabei das Freisein des vorausliegenden Streckenabschnitts an den Train-Operator verbal melden. Durch die Einbindung eines Zugpersonals wird zwar eine weitere Schnittstelle eingerichtet, jedoch erhöht sich die Komplexität der Systemarchitektur nicht erheblich, sofern das eingebundene Zugpersonal mit einem Train-Operator kooperiert. Das Kommunikationsdiagramm einer Mensch-Maschine Kooperation mit einem Zugpersonal ist in Anhang 1 dargestellt.

6.7 Zusammenfassung des Hauptkapitels

Ziel dieses Hauptkapitels war es, geeignete betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb zu entwickeln.

Da es keinen analytischen Ansatz bei der Entwicklung von betrieblich-technischen Rückfallebenen gibt, dem systematisch gefolgt werden kann, wurde in Kapitel 6.4 zunächst – unter Berücksichtigung der Anforderungen aus dem Kapitel 6.2 – ein systematischer Ansatz hergeleitet, anhand dessen die Entwicklung von potenziell einsetzbaren betrieblich-technischen Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb erfolgte.

Damit – entsprechend der Anforderung von ERJU – nationale Bahnbetreiber nicht proprietäre Lösungen für den Umgang mit Störungssituationen entwickeln, wodurch die betriebliche Interoperabilität gefährdet wird, wurde ausgehend von den Enablern der Forschungsinitiativen als systematischer Ansatz eine dynamische Adaption der Systemarchitektur zur Laufzeit für die Einrichtung von betrieblich-technischen Rückfallebenen entwickelt.

Zunächst wurden in Unterkapitel 6.5.1 mögliche dynamische Adaptionsarten zur Laufzeit hergeleitet. Bei den Adaptionsarten hat sich herausgestellt, dass Systemelemente entweder zur Laufzeit ersetzt oder deaktiviert werden können. Bei der Deaktivierung ist eine reine Deaktivierung ohne Funktionsallokation oder mit Funktionsallokation möglich. Beim letzteren wird die betriebliche Funktion des deaktivierten Systemelements auf eine andere Ressource übertragen. Dabei kann entweder auf Ressourcen technischer Art oder auf menschliche Ressourcen (z.B. Train-Operator oder Zugpersonal) zurückgegriffen werden. Das Ersetzen eines Systemelementes zur Laufzeit ist aufgrund der Anforderung, dass die betrieblich-technischen Rückfallebenen möglichst kurz dauern sollen, nur bei Softwareanwendungen sinnvoll.

Entsprechend der RCA-Referenzarchitektur weist der gegenwärtige Bahnbetrieb eine zentrale Betriebsführung auf. Dabei hat das EIU die Entscheidungshoheit bei der Einrichtung von betrieblich-technischen Rückfallebenen. Damit die dynamische Adaption zur Laufzeit weitgehend automatisiert, aber zugleich koordiniert ablaufen kann, wurde in Unterkapitel 6.5.2 eine sogenannte ATO Fallback-Management-Unit (ATO-FMU) eingeführt, die die dynamische Adaption der Systemarchitektur zur Laufzeit koordiniert. Da aufgrund einer Kommunikationsstörung die zentrale Betriebsführung vorübergehend unterbrochen werden kann, wurde eine infrastrukturseitige und eine fahrzeugseitige ATO-FMU eingeführt. Die ATO-FMU kann als eine sogenannte Middleware in die Systemarchitektur eingebettet werden, die unabhängig von den Softwareanwendungen auf einer sicheren Ebene fungiert und unabhängig von den für den Regelbetrieb erforderlichen Systemelementen entwickelt, verändert und bei Bedarf erweitert werden kann.

Die ATO-FMU umfasst ein Modul zur Störungserkennung. Die Störungserkennung wird dadurch erreicht, dass die Systemelemente an die Middleware (ATO-FMU) angebunden sind und daher die Störungsoffenbarung sofort bei der ATO-FMU eingeht. Des Weiteren umfasst die ATO-FMU eine Wissensbasis, um die vorliegende Störungssituation dem entsprechenden Schutzziel zuordnen und daraufhin eine geeignete Adaptionsart auswählen zu können. Neben der Wissensbasis umfasst die ATO-FMU auch eine Datenbank für Services. Aus dieser Datenbank können beim Ersetzen die erforderlichen Services abgerufen werden. Als letztes umfasst die ATO-FMU noch die eigentliche Durchführung der dynamischen Adaption, um situationsabhängige betrieblich-technische Rückfallebene einzurichten. Hiermit werden die entsprechenden Systemelemente in der Systemarchitektur für die Einrichtung einer betrieblich-technischen Rückfallebene koordiniert.

Die eigentliche Durchführung der dynamischen Adaption für die drei Adaptionsarten wurde dann in Unterkapitel 6.5.4 anhand von Ablaufdiagrammen erarbeitet. Dabei wurden für die drei Adaptionsarten

unter Berücksichtigung der in Unterkapitel 6.5.3 hergeleiteten Designprinzipien generische Abläufe erarbeitet. Die Designprinzipien leiten sich aus den bereits in Unterkapitel 3.2.3 zusammengestellten Leitlinien zur Gestaltung von Systemarchitekturen und von den Anforderungen aus dem Kapitel 3.2.2 ab und sollen die technische und betriebliche Interoperabilität im vollautomatisierten Bahnbetrieb – auch in Störungssituationen – ermöglichen.

Die generischen Abläufe aus dem Unterkapitel 6.5.4 wurden dann verwendet, um in Kapitel 6.6 für die in Kapitel 5.6 erarbeiteten gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb beispielhafte betrieblich-technische Rückfallebenen zu entwickeln. Wie bereits in Kapitel 5.6 erarbeitet und in Abbildung 42 dargestellt, ist zur Vermeidung von Kollision eine alternative Lichtraumüberwachung erforderlich. Durch ein alternatives Geschwindigkeitsprofil kann eine Entgleisung oder ein Stillstand vermieden werden. Ein Stillstand kann ebenfalls durch eine alternative Kommunikationsschnittstelle zur Datenübertragung (JP und MA) vermieden werden. Alternatives Geschwindigkeitsprofil oder eine alternative Geschwindigkeitsregelung können durch das Ersetzen des kognitiven Systemelements oder durch Deaktivierung mit Funktionsallokation gelöst werden. Eine alternative Lichtraumüberwachung kann durch Deaktivierung mit oder ohne Funktionsallokation gelöst werden. Eine alternative Kommunikationsschnittstelle zur Datenübertragung kann wiederum durch Deaktivierung mit Funktionsallokation und Ersetzen gelöst werden. Die beispielhaften betrieblich-technischen Rückfallebenen für die Betriebssituationen aus dem Kapitel 5.7 sind in Abbildung 42 blau markiert.

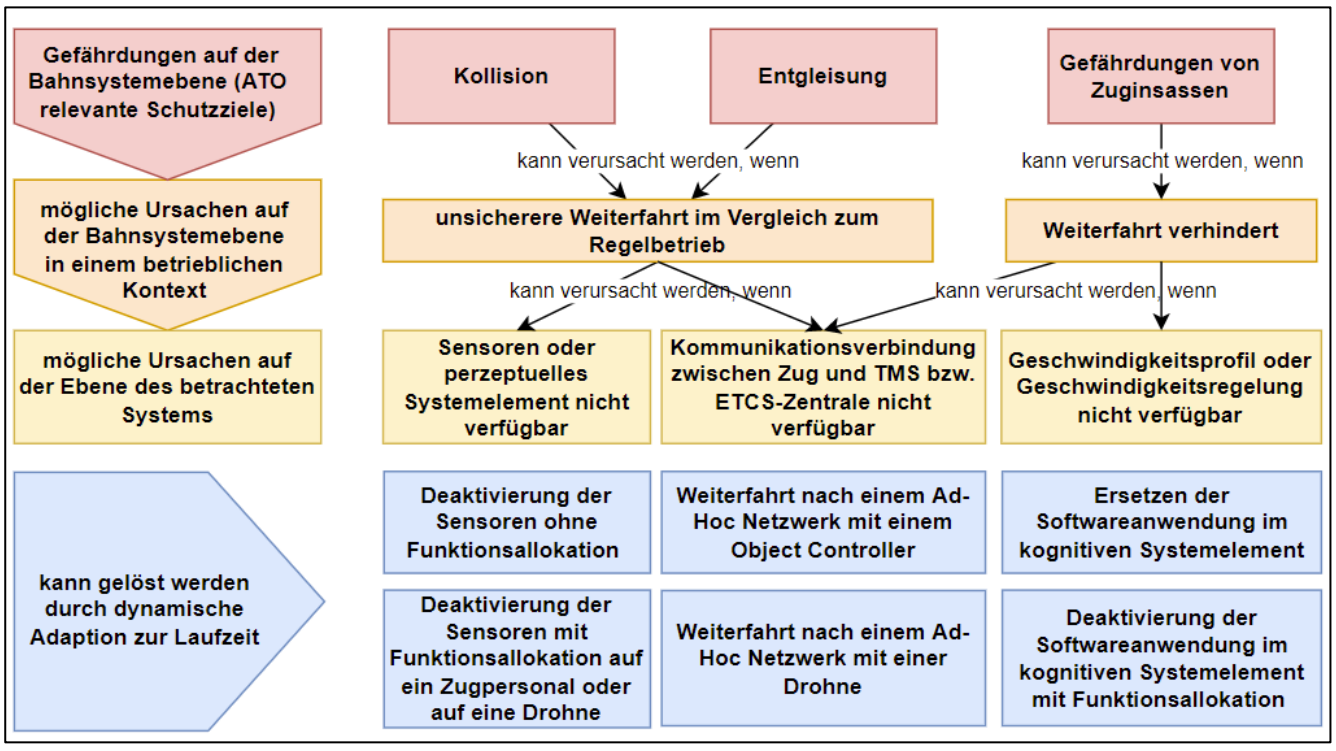

Abbildung 42 Zusammenfassung der ausgewählten gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb mit den zugehörigen beispielhaften betrieblich-technischen Rückfallebenen auf Basis einer dynamischen Adaption der Systemarchitektur zur Laufzeit

Mit dem systematischen Ansatz der dynamischen Adaption der Systemarchitektur zur Einrichtung von betrieblich-technischen Rückfallebenen zur Laufzeit wurde eine wissenschaftliche Grundlage dafür geschaffen, wie potenzielle betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb zur Laufzeit eingerichtet werden können. Die

dynamische Adaption ist im Einklang mit der auf europäischer Ebene geforderten Interoperabilität. Das bedeutet, dass aufgrund der standardisierten Schnittstellen innerhalb der RCA und OCORA alle Bahnbetreiber im Falle von Störungen auch grenzübergreifend dynamische Adaption vornehmen können.

Dadurch kann insbesondere die Entwicklung von proprietären Lösungen für den Umgang mit Störungssituationen vermieden werden. Außerdem müssen die für den vollautomatisierten Bahnbetrieb erforderlichen Systemelemente – insbesondere die Softwareanwendungen – nicht redundant ausgelegt werden, solange die Datenbank für Services der ATO-FMU regelmäßig gepflegt wird. Mit den in der Datenbank für Services abgelegten Softwareanwendungen können alle Züge im ATO-Zuständigkeitsbereich im Falle von Störungen versorgt werden, statt die Systemelemente bei allen Zügen vollredundant auszulegen.

Eine weitere Erkenntnis in diesem Hauptkapitel ist, dass mit der Einführung der ATO-FMU als Koordinator in Form einer Middleware Störungssituationen im vollautomatisierten Bahnbetrieb weitgehend automatisiert abgearbeitet werden können, statt auf manuelle Prozesse zurückzufallen. Die Beispiele in dem Kapitel 6.6 für betrieblich-technische Rückfallebenen auf Basis der dynamischen Adaption zeigen jedoch, dass auch eine Mensch-Maschine Kooperation möglich ist, bei der das Betriebspersonal von der ATO-FMU in die betrieblich-technische Rückfallebene eingebunden wird. Entsprechend der Beispiele aus dem Kapitel 6.6 hat sich gezeigt, dass sich eine Mensch-Maschine Kooperation insbesondere bei Personenzügen, die in GoA3 betrieben werden, aufgrund der Designprinzipien eignet.

Die in Kapitel 6.6 ausgearbeiteten beispielhaften betrieblich-technische Rückfallebenen sind nur für die in Kapitel 5.8 zusammengefassten gefährlichen Betriebssituationen gedacht. Jedoch können anhand der allgemeingültigen Abläufe der drei Adaptionsarten auch andere betrieblich-technische Rückfallebenen zur Laufzeit eingerichtet werden.

Wie bereits zu Beginn des Hauptkapitels erwähnt, hat bei der Betriebsführung in der betrieblich-technischen Rückfallebene die Sicherheit die oberste Priorität. Deshalb wurde bei den Abläufen für die drei Adaptionsarten ein Bewertungsschritt hinsichtlich der Sicherheit integriert.

Außerdem ist eine Aussage über die Dauer der Betriebsführung in den jeweiligen beispielhaften betrieblich-technischen Rückfallebenen aktuell nicht möglich. Die Dauer ist insofern relevant, da ungeplante Störungen zur Abweichung von der vereinbarten Betriebsqualität führen können.

Die Entwicklung eines geeigneten Bewertungsverfahrens, anhand dessen die in diesem Hauptkapitel beispielhaft entwickelten betrieblich-technischen Rückfallebenen hinsichtlich der Sicherheit und der Betriebsqualität bewertet werden können, erfolgt im nächsten Hauptkapitel.

7 Bewertung der auf Basis der dynamischen Adaption der Systemarchitektur entwickelten betrieblich-technischen Rückfallebenen

7.1 Ziel des Kapitels

Der vollautomatisierte Bahnbetrieb ist noch nicht migriert. Für eine Migrationsentscheidung, welche der im Rahmen dieser Arbeit entwickelten betrieblich-technischen Rückfallebenen migriert werden sollten, ist entsprechend des dritten Unterziels aus der Aufgabenstellung (Kapitel 3.1) eine Bewertung vor der Migration erforderlich.

Außerdem enthält die im vorigen Hauptkapitel erarbeitete dynamische Adaption der Systemarchitektur zur Laufzeit entsprechend der Abbildung 30 auf der Seite 118 einen Bewertungsschritt bei der Auswahl der geeigneten Adaptionsart und der entsprechenden Ressource.

Daher ist das Ziel dieses Kapitels, ein Bewertungsverfahren für die Bewertung der in Kapitel 6.6 erarbeiteten betrieblich-technischen Rückfallebenen zu entwickeln.

7.2 Anforderungen an das Bewertungsverfahren

Die Anforderungen an das Bewertungsverfahren ergeben sich aus den Anforderungen in Kapitel 3.3 und aus dem Ablaufdiagramm in Abbildung 30 auf der Seite 118 (Unterkapitel 6.5.4).

Wie bereits bei den Anforderungen aus dem Kapitel 3.3 bekannt, hat die Sicherheit bei der Betriebsführung in der betrieblich-technischen Rückfallebene die oberste Priorität. Deshalb wurde bei dem übergeordneten Ablauf während der dynamischen Adaption in Kapitel 6.4 ein Bewertungsschritt hinsichtlich der Sicherheit integriert. Das Bewertungsverfahren soll daher die Auswirkung der jeweiligen betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption auf die **Sicherheit während der Betriebsführung** in Störungssituationen bewerten können.

Bei der Migrationsentscheidung hat zwar die Sicherheit entsprechend des Grundprinzips „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“ die höchste Priorität. Eine weitere Muss-Anforderung aus dem Unterkapitel 3.2.4 ist zudem die Weiterfahrt in Störungssituationen mit möglichst geringer Auswirkung auf die Betriebsqualität. Bei der Bewertung kann es jedoch vorkommen, dass zwei Adaptionsarten das gleiche Sicherheitsniveau aufweisen. In diesem Fall soll das Bewertungsverfahren für die Migrationsentscheidung auch die **Auswirkung** der in Hauptkapitel 6 erarbeiteten betrieblich-technischen Rückfallebenen **auf die Betriebsqualität** bewerten können.

Entsprechend der beiden Referenzarchitekturen aus den Forschungsinitiativen RCA und OCORA kann jeder Betreiber aus den Referenzarchitekturen die eigene physikalische Systemarchitektur entwickeln und dabei technische Redundanzen integrieren. Sowohl die Integration von technischen Redundanzen in die Systemarchitektur als auch die dynamische Adaption zur Laufzeit verursachen aufgrund der erforderlichen ATO-FMU einschließlich der Ressourcen Kosten bei der Migration der physikalischen Systemarchitektur. Das Bewertungsverfahren soll daher auch die Auswirkung der für die dynamische Adaption erforderlichen ATO-FMU einschließlich der Ressourcen auf die **Kosten** bewerten können.

Entsprechend des Ablaufdiagramms aus dem Unterkapitel 6.5.4 ist schließlich eine wesentliche Anforderung an das Bewertungsverfahren bei der Auswahl der geeigneten Adaptionsart und der entsprechenden Ressource, dass es **zur Laufzeit ausführbar** sein soll.

Wenngleich die Bewertung für eine Migrationsentscheidung und zur Laufzeit zu unterschiedlichen Zeitpunkten erfolgt, ist es wichtig, dass die Bewertung hinsichtlich der Sicherheit und der Auswirkung auf die Betriebsqualität sowohl für die Migrationsentscheidung als auch zur Laufzeit zu gleichen Ergebnissen führt (widerspruchsfrei ist). Insofern muss das Bewertungsverfahren **konsistent** sein.

7.3 Vorgehensweise

In Anlehnung an die Anforderungen aus dem Kapitel 7.2 ist ein Bewertungsverfahren erforderlich, das zum einen eine Migrationsentscheidung der Betreiber ermöglicht. Damit entsprechend des Kapitels 6.5 die Einrichtung von betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb auch weitgehend automatisiert ablaufen kann und der Ablauf aus dem Unterkapitel 6.5.4 einen Bewertungsschritt zur Laufzeit enthält, ist zum anderen ein Bewertungsverfahren erforderlich, das zur Laufzeit ausgeführt werden kann.

Bevor die Auswahl eines geeigneten Bewertungsverfahrens erfolgt, werden zunächst mögliche Bewertungsverfahren aus dem Unterkapitel 2.4.5 aufgegriffen und in Kapitel 7.4 anhand der Anforderungen aus dem Kapitel 7.2 diskutiert und daraus ein geeignetes Bewertungsverfahren ausgewählt.

Sofern erforderlich, werden auf Basis des ausgewählten Bewertungsverfahrens schließlich die wesentlichen Bestandteile des ausgewählten Bewertungsverfahrens aus dem Kapitel 7.4 in den Kapiteln 7.5 – 7.6 untersetzt.

7.4 Wahl eines anforderungsgerechten Bewertungsverfahrens (Methode)

In diesem Kapitel werden mögliche Bewertungsverfahren aus dem Unterkapitel 2.4.5 aufgegriffen und anhand der Anforderungen aus dem Kapitel 7.2 diskutiert sowie ein geeignetes Bewertungsverfahren ausgewählt, das für eine Migrationsentscheidung herangezogen und bei der dynamischen Adaption zur Laufzeit angewandt werden kann.

Entsprechend den Anforderungen sollen bei der Migrationsentscheidung neben der Bewertung der Sicherheit auch Auswirkungen der in Hauptkapitel 6 erarbeiteten betrieblich-technischen Rückfallebenen auf Basis der dynamischen Adaption zur Laufzeit auf die Betriebsqualität und Kosten bei der Migration bewertet werden.

Von den in Unterkapitel 2.4.5 beschriebenen Bewertungsverfahren enthalten die beiden Bewertungsverfahren nach *Lindner (2012)* und *Blanchard et al. (1995)* Sicherheit, Kosten und eine betriebliche Kenngröße. In dem Bewertungsverfahren nach *Huang (2020)* steht als Kenngröße im Fokus die Sicherheit, welche mit dem Risikogrenzwert für ein Kalenderjahr budgetiert wird.

Wie in Unterkapitel 2.4.5 beschrieben, bewertet das Bewertungsverfahren nach *Lindner (2012)* den Nutzen einer betrieblich-technischen Rückfallebene über die prozentuale Veränderung der Infrastrukturkapazität in einer betrieblich-technischen Rückfallebene im Verhältnis zum Regelbetrieb und die Sicherheit mit der Belastung des Betriebspersonals. Die Kosten werden mit Zusatzkosten für eine betrieblich-technische Rückfallebene im Vergleich zu den Kosten für den Regelbetrieb bewertet. Die Bewertung hinsichtlich der drei Kenngrößen erfolgt jedoch getrennt.

Wenngleich es entsprechend des Kapitels 6.6 möglich ist, dass ein Betriebspersonal in eine betrieblich-technische Rückfallebene eingebunden werden kann, erfolgt die dynamische Adaption weitgehend automatisiert. Das bedeutet, dass mit der Belastung eines Betriebspersonals die Auswirkung einer betrieblich-technischen Rückfallebene auf die Sicherheit im vollautomatisierten Bahnbetrieb nicht

vollständig bewertet werden kann. Im Gegensatz zu dem Bewertungsverfahren nach *Lindner (2012)* ist es mit dem Bewertungsverfahren nach *Huang (2020)* möglich, die Sicherheit mit anhand des Betriebsrisikos – unter Berücksichtigung des Mensch-Maschine Zusammenwirkens – zu ermitteln. Jedoch werden in dem Bewertungsverfahren nach *Huang (2020)* Kosten und eine betriebliche Kenngröße bei der Bewertung nicht simultan berücksichtigt.

Hingegen umfasst das Bewertungsverfahren nach *Blanchard et al. (1995)* alle drei Kenngrößen in einer Bewertungsfunktion. Dadurch ist es möglich, die Systemeffektivität der im Rahmen dieser Arbeit entwickelten betrieblich-technischen Rückfallebenen unter simultaner Berücksichtigung der Kenngrößen Sicherheit, Betriebsqualität und Kosten einschließlich der Wechselwirkung zueinander zu bewerten. Damit erfüllt das Bewertungsverfahren nach *Blanchard et al. (1995)* die Anforderungen aus dem Kapitel 7.2 am besten und ist daher als Bewertungsverfahren im Rahmen dieser Arbeit geeignet.

Wie bereits in Unterkapitel 2.4.5 in der Formel 2.4.3 beschrieben, ergibt sich die Systemeffektivität nach *Blanchard et al. (1995)* aus dem Produkt von RAMS-Werten und der Fähigkeit des Systems, seine beabsichtigte Aufgabe in einer bestimmten Zeit bei einer bestimmten Auslastung zu erfüllen und dem Verhältnis zu den damit verbundenen Lebenszykluskosten. Da das ausgewählte Bewertungsverfahren bisher im Bahnbetrieb nicht angewandt wurde, ist es erforderlich, dessen Bestandteile mit bahnspezifischen Kenngrößen zu untersetzen.

7.5 Bewertung der betrieblich-technischen Rückfallebenen anhand der Systemeffektivität für eine Migrationsentscheidung

Entsprechend des im vorigen Kapitel ausgewählten Bewertungsverfahrens werden in diesem Kapitel die Bestandteile des ausgewählten Bewertungsverfahrens zur Ermittlung der Systemeffektivität der betrieblich-technischen Rückfallebenen für eine Migrationsentscheidung untersetzt.

Wie bereits in Unterkapitel 2.4.5 in Formel 2.4.3 beschrieben, lässt sich die Systemeffektivität nach *Blanchard et al. (1995)* mathematisch folgendermaßen ausdrücken:

$$SE = \frac{Design\ integrity * Capability}{LCC} = \frac{R * A * M * S * C}{LCC} \qquad 7.5.1$$

SE = Effektivität des betrachteten Systems

C = Fähigkeit des betrachteten Systems, seine beabsichtigte Aufgabe in einer bestimmten Zeit bei einer bestimmten Auslastung zu erfüllen

RAM = Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit des betrachteten Systems

S = Kenngröße zur Beschreibung der Sicherheit des betrachteten Systems

LCC = Lebenszykluskosten des betrachteten Systems.

Zur Bewertung der Systemeffektivität der betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6 werden im Weiteren die Kenngrößen *RAMS*, *C* und *LCC* untersetzt.

7.5.1 Abschätzung der Kenngröße RAMS

In diesem Unterkapitel wird entsprechend des Kapitels 7.4 die Kenngröße RAMS mit einer bahnspezifischen Kenngröße untersetzt.

Bahnbetreiber können mit Vorgaben für RAM-Werte an die technischen Systeme des vollautomatisierten Bahnbetriebs diese als Eingangsgröße für die Bewertung heranziehen. Mit den RAM-Werten ist es möglich, die Häufigkeit einer durch die jeweiligen technischen Systeme verursachten Störungssituationen abzuschätzen.

Die Häufigkeit einer technischen Störung hängt von der Zuverlässigkeit eines technischen Systems ab und kann durch technische Redundanzen beeinflusst werden. Die Häufigkeit einer Störungssituation im betrachteten Zeitraum kann aus der mittleren Zeit bis zum Ausfall eines technischen Systems (engl., Mean-Time-Between-Failures, MTBF) bestimmt werden. Das bedeutet, dass die Betreiber mit der Wahl der technischen Redundanz die MTBF und damit die Häufigkeit einer Störungssituation $n_{Störung,i}$ (aufgrund einer technischen Störung in einem Systemelement i) über die Lebensdauer eines technischen Systems beeinflussen können.

Die Häufigkeit einer Störungssituation $n_{Störung,i}$ über die Lebensdauer eines technischen Systems im vollautomatisierten Bahnbetrieb kann demnach vereinfacht wie folgt ermittelt werden:

$$n_{Störung,i} = \frac{T_{sys,i}}{MTBF_{sys,i}} \qquad 7.5.2$$

$n_{Störung,i}$ = Häufigkeit einer Störungssituation aufgrund einer Störung in einem Systemelement i

$T_{sys,i}$ = Lebensdauer eines technischen Systems

$MTBF_{sys,i}$ = Mittlere Zeit bis zum Ausfall eines technischen Systems.

Da die Häufigkeit einer Störungssituation von der Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit eines technischen Systems abhängt, kann die Kenngröße RAM aus der Formel 7.5.1 mit der Häufigkeit einer Störungssituation $n_{Störung,i}$ beschrieben und von den Betreibern als Eingangsgröße herangezogen werden.

Anders als die RAM-Werte kann sich die Sicherheit der Betriebsführung abhängig von der gewählten betrieblich-technischen Rückfallebene aus dem Kapitel 6.6 aufgrund der unterschiedlichen Gefährdungsraten der eingebundenen Ressourcen unterscheiden. Mit der Kenntnis der Häufigkeit einer durch die jeweiligen technischen Systeme verursachten Störungssituation kann bestimmt werden, wie häufig eine betrieblich-technische Rückfallebene aus dem Kapitel 6.6 in einem bestimmten Betrachtungszeitraum (z.B. gesamte Lebensdauer) angewandt wird und wie sich aufgrund der angewandten betrieblich-technischen Rückfallebene das Betriebsrisiko in dem Betrachtungszeitraum kumuliert. Es ist daher sinnvoll, die Kenngröße S aus der Formel 7.5.1 mit dem Betriebsrisiko, das sich aufgrund der geänderten Gefährdungsrate kumuliert, abzuschätzen.

Unter der Annahme, dass jedes Mal im Falle einer Störung an einem technischen System betrieblich-technische Rückfallebenen eingerichtet werden, kann das gesamte erwartete Betriebsrisiko der jeweiligen betrieblich-technischen Rückfallebene über die Lebensdauer wie folgt bestimmt werden:

$$BR_{ges} = n_{Störung,i} * BR_{D,i} \qquad 7.5.3$$

BR_{ges} = Erwartete Gesamterhöhung des Betriebsrisikos infolge einer betrieblich-technischen Rückfallebene über die Lebensdauer

$n_{Störung}$ = Häufigkeit einer Störungssituation aufgrund einer Störung in einem Systemelement i

$BR_{D,i}$ = Betriebsrisiko infolge einer betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption

$T_{sys,i}$ = Lebensdauer eines technischen Systems.

Da sich das Betriebsrisiko aufgrund der geänderten Gefährdungsrate ergibt und entsprechend des Unterkapitels 6.5.1 bei der dynamischen Adaption zur Laufzeit drei Adaptionsarten vorkommen, kann sich die adaptionsartspezifische Änderung der Gefährdungsrate unterscheiden. Deshalb wird in den weiteren Abschnitten die Änderung der Gefährdungsrate in Abhängigkeit der jeweiligen Adaptionsart aus dem Unterkapitel 6.5.4 hergeleitet.

Bestimmung der geänderten Gefährdungsrate bei der Adaptionsart Ersetzen

Zur Bestimmung von Gefährdungsraten in Softwareanwendungen werden in *Negaraju und Fiondella (2018)* einige quantitative Ansätze vorgestellt, deren Diskussion und Auswahl den Rahmen dieses Kapitels sprengen würde. Die darin vorgestellten Ansätze zeigen jedoch, dass es möglich ist, die Gefährdungsrate einer Softwareanwendung zur Laufzeit zu bestimmen.

Das Ersetzen als Adaptionsart ist entsprechend des Unterkapitels 6.5.1 für Softwareanwendungen geeignet. Beim Ersetzen einer Softwareanwendung würde sich das Betriebsrisiko aus dem Regelbetrieb nicht ändern, sofern die alternative Softwareanwendung vorher auf Fehlerfreiheit geprüft wurde. Trotz der Fehlerfreiheit ist es aber möglich, dass beim Ersetzen einer Softwareanwendung die alternative Softwareanwendung ein abweichendes SIL-Level aufweist.

Damit das Betriebsrisiko nach dem Ersetzen einer Softwareanwendung zur Laufzeit nicht erheblich steigt, ist es aus Sicherheitsgründen sinnvoll, die gestörte Softwareanwendung nur durch eine alternative Softwareanwendung mit gleichbleibenden nächst niedrigerem SIL-Level zu ersetzen. Wenn beispielsweise eine Softwareanwendung aus dem Regelbetrieb SIL 3 aufweist, muss die alternative Softwareanwendung mindestens SIL 2 aufweisen. Da zwischen dem SIL 3 und dem SIL 2 für die Gefährdungsrate ein Faktor f_{SIL} von maximal 100 liegt, kann sich also die Gefährdungsrate aus dem Regelbetrieb beim Ersetzen maximal um den Faktor f_{SIL} 100 erhöhen. Es ergibt sich also für die Gefährdungsrate nach dem Ersetzen:

$$\lambda_E = \lambda_{RB} * f_{SIL} \qquad 7.5.4$$

λ_E = Geänderte Gefährdungsrate aufgrund des Ersetzens zur Laufzeit

λ_{RB} = Gefährdungsrate des ersetzten Systemelements im Regelbetrieb

f_{SIL} = Faktor aufgrund einer Abstufung des SIL.

Bestimmung der geänderten Gefährdungsrate bei der Adaptionsart Deaktivierung (mit und ohne Funktionsallokation)

Anders als beim Ersetzen werden bei der Deaktivierung von Systemelementen (mit und ohne Funktionsallokation) auch die Schnittstellen der Systemarchitektur vorübergehend geändert. Während bei der Deaktivierung ohne Funktionsallokation die Schnittstelle des deaktivierten Systemelements nicht mehr bedient wird, entstehen bei der Deaktivierung mit Funktionsallokation vorübergehend neue Schnittstellen (vgl. Unterkapitel 6.5.1).

Da sich die resultierende Gefährdungsrate eines Systems aus den einzelnen Gefährdungsraten der Systemelemente in Abhängigkeit der logischen Verknüpfungen zueinander ergeben, und die Deaktivierung mit oder ohne Funktionsallokation die Systemstruktur vorübergehend ändert, liegt es nahe, zur Bestimmung der Änderung der Gefährdungsrate aufgrund der Adaptionsart Deaktivierung auf einen Ansatz aus der Zuverlässigkeitstechnik zurückzugreifen.

So kann nach *Cheok et al. (1998a, 1998b)* der sogenannte Risikoleistungswert (engl., Risk-Achievement-Worth, RAW) eines Systemelements in der Systemarchitektur bestimmt werden. Der RAW-Wert bestimmt die Erhöhung des Risikos, wenn ein Systemelement aus der Systemarchitektur ausgefallen (deaktiviert) wird.

Um jedoch den RAW-Wert zur Laufzeit bestimmen zu können, ist die logische Verknüpfung der Systemelemente, die gemeinsam eine betriebliche Funktion erfüllen, erforderlich. Im einfachsten Fall ergibt sich für die geänderte Gefährdungsrate aufgrund der Deaktivierung ohne Funktionsallokation 1 (d.h. die Wahrscheinlichkeit für den Ausfall des Systemelements ist 1), sofern das deaktivierte Systemelement eine betriebliche Funktion allein erfüllt.

Da auch aus der Norm EN 50126 bekannt ist, dass der THR-Wert einer betrieblichen Funktion auf mehrere Systemelemente verteilt wird, liegt eine logische Verknüpfung zwischen diesen Systemelementen vor. So ist z.B. auch aus dem Kapitel 4.7 bekannt, dass die Lichtraumüberwachung durch die Sensoren und durch das entsprechende perzeptuelle Systemelement erfüllt wird. Die logische Verknüpfung der Systemelemente kann durch Zuhilfenahme von Fehlerbäumen oder Zuverlässigkeitsblockdiagrammen zur Laufzeit ermittelt werden. Beispielsweise wird die Lichtraumüberwachung durch eine logische UND-Verknüpfung der Sensoren und des perzeptuellen Systemelements erfüllt. Innerhalb der Sensorkonfigurationen können jedoch andere logische Verknüpfungen vorkommen (vgl. mehrere Sensoren aus Sensors4Rail).

Nachdem die logische Verknüpfung der relevanten Systemelemente für die entsprechende betriebliche Funktion bekannt ist, lässt sich der RAW-Wert durch das Verhältnis der Wahrscheinlichkeit für das Top-Ereignis zum Zeitpunkt des deaktivierten Systemelements (betriebliche Funktion wird nicht erfüllt) und der Wahrscheinlichkeit für das Top-Ereignis aus dem Regelbetrieb mit der Formel 7.5.5 ermitteln. Hierbei wird die Ausfallwahrscheinlichkeit für das deaktivierte Systemelement auf 1 gesetzt.

$$RAW_{oFa}(i \mid t) = \frac{P_0(p_i, t)}{P_0(t)} \qquad 7.5.5$$

$RAW_{oFa}(i \mid t)$ = Risikoleistungswert bei Deaktivierung eines Systemelements i aus der Systemarchitektur ohne Funktionsallokation zum Zeitpunkt t

$P_0(p_i, t)$ = Wahrscheinlichkeit für das Top-Ereignis (betriebliche Funktion wird nicht erfüllt) bei Deaktivierung eines Systemelements (p_i =1) und

$P_0(t)$ = Wahrscheinlichkeit für das Top-Ereignis aus dem Regelbetrieb.

Die geänderte Gefährdungsrate nach der Deaktivierung eines Systemelements ohne Funktionsallokation ist dann das Produkt aus dem RAW-Wert und der ursprünglichen Gefährdungsrate aus dem Regelbetrieb (THR-Wert). Diese kann wie folgt ermittelt werden:

$$\lambda_{D,oFa} = \lambda_{RB} * RAW_{oFa}(i \mid t) \qquad 7.5.6$$

$\lambda_{D,oFa}$= Geänderte Gefährdungsrate aufgrund der Deaktivierung eines gestörten Systemelements ohne Funktionsallokation

λ_{RB}= Gefährdungsrate des deaktivierten Systemelements im Regelbetrieb.

Bei der Deaktivierung eines Systemelements mit Funktionsallokation wird eine neue Ressource in die Systemarchitektur eingebunden, sodass dadurch vorübergehend eine neue Schnittstelle entsteht. In Abhängigkeit der logischen Verknüpfung der eingebundenen Ressource mit den Systemelementen in der betrieblich-technischen Rückfallebene kann die geänderte Gefährdungsrate ebenfalls mit dem RAW-Wert ermittelt werden.

Statt die Ausfallwahrscheinlichkeit für das deaktivierte Systemelement auf 1 zu setzen, wird die Ausfallwahrscheinlichkeit der eingebundenen Ressource verwendet. Wie aus dem Kapitel 6.5 bekannt, kann bei der Deaktivierung mit Funktionsallokation eine Mensch-Maschine Kooperation zustande kommen. Die Änderung der Gefährdungsrate hängt daher von dem Anteil, der durch die Systemelemente beigetragen wird und von dem menschlichen Anteil ab.

Die Versagenswahrscheinlichkeit eines Betriebspersonals hängt – wie bereits in *Huang (2020)* hergeleitet – von der Anzahl der Handlungen, von der Dauer der Handlungen, von dem Umfang der Handlungen und von der Intensität der Handlungen ab. In ebd. sind ebenfalls konkrete Werte für die auslastungsbedingte Versagenswahrscheinlichkeit eines Betriebspersonals quantifiziert worden. Bei der Deaktivierung eines Systemelements mit Funktionsallokation ergibt sich für den RAW-Wert folglich:

$$RAW_{mFa}(i \mid t) = \frac{P_0(p_R, t)}{P_0(t)} \qquad 7.5.7$$

$RAW_{mFa}(i \mid t)$ = Risikoleistungswert bei Deaktivierung eines Systemelements i aus der Systemarchitektur mit Funktionsallokation zum Zeitpunkt t

$P_0(p_R, t)$ = Wahrscheinlichkeit für das Top-Ereignis (wird nicht erfüllt) bei Übernahme der betrieblichen Funktion durch eine andere Ressource und

$P_0(t)$ = Wahrscheinlichkeit für das Top-Ereignis aus dem Regelbetrieb.

Für die geänderte Gefährdungsrate nach einer Deaktivierung mit Funktionsallokation ergibt sich folglich:

$$\lambda_{D,mFa} = \lambda_{RB} * RAW_{mFa}(i \mid t) \qquad 7.5.8$$

$\lambda_{D,mFa}$ = Geänderte Gefährdungsrate aufgrund der Deaktivierung eines gestörten Systemelements mit Funktionsallokation

λ_{RB} = Gefährdungsrate des deaktivierten Systemelements im Regelbetrieb.

Betriebsrisiko der drei Adaptionsarten aufgrund der geänderten Gefährdungsrate

Die geänderten Gefährdungsraten sind auf eine Zeiteinheit bezogen. Zur Bestimmung des Betriebsrisikos wird auch in Anlehnung an *Braband (2019)* die Änderung der Gefährdungsrate der jeweiligen dynamischen Adaption $\lambda_{D,i}$ (λ_E oder $\lambda_{D,oFa}$ oder $\lambda_{D,mFa}$)mit der Dauer der betrieblich-technischen Rückfallebene sowie dem damit verbundenen Schadensausmaß (im Falle von einem unerwünschten Ereignis) multipliziert, sodass das jeweilige Betriebsrisiko einer betrieblich-technischen Rückfallebene aus der Formel 7.5.3 wie folgt ermitteln lässt:

$$BR_{D,i} = \lambda_{D,i} * t_{RFE,D,i} * S_i \qquad 7.5.9$$

$BR_{D,i}$ = Erhöhung des Betriebsrisikos infolge der jeweiligen dynamischen Adaption mit unterschiedlicher Gefährdungsrate

$\lambda_{D,i}$ = Gefährdungsrate der jeweiligen dynamischen Adaptionsart

$t_{RFE,D,i}$ = Dauer der betrieblich-technischen Rückfallebene auf Basis der jeweiligen Adaptionsart

S_i = Schadensausmaß im Falle von einem unerwünschten Ereignis während der jeweiligen betrieblich-technischen Rückfallebene.

Das Schadensausmaß der jeweiligen betrieblich-technischen Rückfallebene kann z.B. nach *VDE V 0831-103:2020 (2020)* ermittelt werden.

Mit der Formel 7.5.9 ist es prinzipiell möglich, das Betriebsrisiko der jeweiligen betrieblich-technischen Rückfallebene aus dem Kapitel 6.6 zu ermitteln. Um jedoch bewerten zu können, ob das jeweilige Betriebsrisiko sowohl für eine Migrationsentscheidung als auch entsprechend des Bewertungsschritts nach Abbildung 30 auf der Seite 118 zur Laufzeit akzeptabel ist, ist der Risikogrenzwert erforderlich. Dieser kann dem Bewertungsverfahren nach *Huang (2020)* entnommen werden. Demnach lässt sich der erwartete Risikoindex der jeweiligen betrieblich-technischen Rückfallebene aus dem Kapitel 6.6 in Abhängigkeit der Häufigkeit ihrer Anwendung entsprechend der Formel 2.4.1 aus dem Unterkapitel 2.4.5 folgendermaßen ermitteln:

$$RI_{dyn} = \frac{\sum BR}{R_{Grenz}} = \frac{n_{Störung_i} * BR_{D,i}}{R_{Grenz}} \qquad 7.5.10$$

RI_{dyn} = Erwarteter Risikoindex einer betrieblich-technischen Rückfallebene über die Lebensdauer

R_{Grenz} = Risikogrenzwert auf einem Netzelement mit einem bestimmten Streckenstandard

$n_{Störung_i}$ = Häufigkeit einer Störungssituation aufgrund einer Störung in einem Systemelement i

$\sum BR$ = kumuliertes Betriebsrisiko, aufsummiert von 0 bis $n_{Störung_i}$

$BR_{D,i}$ = Betriebsrisiko einer betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption.

Anhand der Formel 7.5.10 kann mit der Kenntnis der Häufigkeit einer Störungssituation – verursacht durch die jeweiligen technischen Systeme – bewertet werden, viel Prozent von einem Gesamten zur Verfügung stehenden Risikobudget (Risikogrenzwert pro Kalenderjahr) durch eine betrieblich-technische Rückfallebene aus dem Kapitel 6.6 in einem bestimmten Zeitraum voraussichtlich verbraucht wird.

In diesem Unterkapitel konnte die Kenngröße RAMS aus der Formel 7.5.1 untersetzt werden. Dabei hat sich herausgestellt, dass die RAM-Werte von den Betreibern an die technischen Systeme des vollautomatisierten Bahnbetriebs vorgegeben werden können und daher als Eingangsgröße für die Bewertung dienen. Hingegen ist die Kenngröße Sicherheit aus der Formel 7.5.1 eine von den betrieblich-technischen Rückfallebenen abhängige Kenngröße und wird durch das adaptionsartspezifische Betriebsrisiko bestimmt. Sofern durch die Anwendung einer betrieblich-technischen Rückfallebene das Betriebsrisiko nicht vollständig ausgeschöpft wird, scheint es sinnvoll eine betrieblich-technische Rückfallebene mit möglichst kurzer Dauer heranzuziehen, um die Auswirkung auf die Betriebsqualität möglichst minimal zu halten. Um die Auswirkung einer betrieblich-technischen Rückfallebene auf die Betriebsqualität bestimmen zu können, wird die Kenngröße Capability aus der Formel 7.5.1 im nächsten Unterkapitel abgeschätzt.

7.5.2 Abschätzung der Kenngröße Capability

Im Bahnbetrieb gibt es einige Kenngrößen für Leistungsuntersuchungen, die je nach Aufgabenstellung unterschiedlich eingesetzt werden können. In diesem Unterkapitel werden die in Unterkapitel 2.4.5 erläuterten Kenngrößen aus dem Bahnbetrieb auf ihre Eignung zur Abschätzung der Kenngröße Capability geprüft. Die Definition für Capability aus dem Unterkapitel 2.4.5 besagt, dass die Capability die Fähigkeit eines Systems, seine beabsichtigte Aufgabe in einer bestimmten Zeit bei einer bestimmten Auslastung zu erfüllen, repräsentiert.

Wie bereits aus dem Kapitel 2.4 bekannt, entstehen technische Störungen während der Betriebsführung, die nicht im ursprünglichen Fahrplan vorgesehen waren und daher die Betriebsqualität beeinträchtigen können. Mit den in Hauptkapitel 6 entwickelten betrieblich-technischen Rückfallebenen sollen durch eine weitgehend automatisierte Reaktion auf derartige Störungssituationen die Auswirkungen auf die Betriebsqualität möglichst minimal gehalten werden.

Züge, die von einer Störungssituation betroffen sind und daher eine Fail-Safe Reaktion auslösen (meist Erreichen des Stillstands) halten außerplanmäßig auf dem untersuchten Netzelement (z.B. freie Strecke) und setzen ihre Fahrt nach der Einrichtung einer betrieblich-technischen Rückfallebene aus dem Kapitel 6.6 fort. Dadurch kommt es bei den betroffenen Zügen zu Urverspätungen, die bereits in Unterkapitel 2.4.5 erläutert wurde. Bis eine betrieblich-technische Rückfallebene eingerichtet ist, beanspruchen die betroffenen Züge das untersuchte Netzelement bzw. eine Fahrwegkomponente davon länger als geplant, wodurch entsprechend des Unterkapitels 2.4.5 der Behinderungsgrad steigt.

Prinzipiell kann mit der Kenngröße Capability abgeschätzt werden, wie viel weniger eine betrieblich-technische Rückfallebene gegenüber einer anderen betrieblich-technische Rückfallebene Urverspätungen verursacht oder wie viel weniger das Netzelement je betrieblich-technische Rückfallebene beansprucht wird, d.h. wie viel weniger der erzeugte Behinderungsgrad ist. Das

außerplanmäßige Halten von Zügen bis zur Einrichtung einer betrieblich-technischen Rückfallebene und die im Anschluss ggf. mit reduzierter Geschwindigkeit fortgeführte Fahrt wirkt sich jedoch in Abhängigkeit der Zugfolgefälle auch auf die nachfolgenden Züge aus. Die Einrichtung einer betrieblich-technischen Rückfallebene und die im Anschluss ggf. mit reduzierter Geschwindigkeit fortgeführte Fahrt kann außerplanmäßige Wartezeiten bei nachfolgenden Zügen verursachen.

Die Einrichtung einer betrieblich-technischen Rückfallebene hat somit nicht nur Auswirkung auf einzelne Züge, die von der Störungssituation betroffen sind, sondern kann auch andere Züge in einem Betrachtungsraum betreffen.

Entsprechend des Unterkapitels 2.4.5 hat das EIU die Entscheidungsbefugnis bei der Gestaltung und Umsetzung von betrieblich-technischen Rückfallebenen, weshalb in Unterkapitel 6.5.2 eine EIU seitige Ressource zur Koordination der dynamischen Adaption zur Laufzeit erarbeitet wurde. Dadurch soll insbesondere die von ERJU geforderte betriebliche Interoperabilität erleichtert werden.

Bei der Dimensionierung der Eisenbahnbetriebsanlagen für den vollautomatisierten Bahnbetrieb macht es Sinn, dass die Betreiber die Auswirkungen der betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6 in verschiedenen Betriebsprogrammen vor der Migration bewerten. Dadurch ist es für die Betreiber möglich, die Abwicklung von verschiedenen Betriebsprogrammen – unter Berücksichtigung der Auswirkungen von betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6 – auf einer bestimmten Eisenbahninfrastruktur prüfen.

Aus dem Unterkapitel 2.4.5 ist bekannt, dass Betreiber das Leistungsverhalten auf einer bestimmten Eisenbahninfrastruktur bei einer bestimmten Betriebsqualität im Regelbetrieb mittels außerplanmäßiger Wartezeiten beurteilen können.

Es ist demnach sinnvoll – in Anlehnung an die Definition der Kenngröße Capability von oben – die Fähigkeit einer betrieblich-technischen Rückfallebene aus dem Kapitel 6.6 bei einer festgelegten Betriebsqualität im Regelbetrieb in verschiedenen Betriebsprogrammen dahingehend zu untersuchen, wie viel außerplanmäßige Wartezeiten bei einem bestimmten Betriebsprogramm und in einem Betrachtungsraum durch die Anwendung einer betrieblich-technischen Rückfallebene erzeugt werden.

Durch Vorgabe eines Betriebsprogramms kann die zulässige Summe der außerplanmäßigen Wartezeiten in einem Betriebsprogramm ermittelt werden. Mit dem Quotienten der tatsächlichen Summe der außerplanmäßigen Wartezeiten, die durch die Anwendung einer betrieblich-technischen Rückfallebene entstanden ist, und der zulässigen Summe der außerplanmäßigen Wartezeiten in einem Betriebsprogramm kann schließlich eine Aussage darüber getroffen werden, in wie fern sich die Betriebsqualität aufgrund der in Hauptkapitel 6 entwickelten betrieblich-technischen Rückfallebenen in einem Betrachtungszeitraum und einem Betrachtungsraum ändern wird *(vgl. DB Netz AG 2022)*. Dabei ist zu berücksichtigen, dass es zu einer Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb aufgrund von außerplanmäßigen Wartezeiten nur dann kommt, wenn die tatsächliche Summe der außerplanmäßigen Wartezeiten größer als die zulässige Summe der außerplanmäßigen Wartezeit ist.

Folglich kann die Kenngröße Capability C mit dem folgenden Ausdruck abgeschätzt werden:

$$\Delta Q_0 = \frac{\sum t_{Wa}}{\sum t_{Wa,zul}} - Q_0 \quad \forall \sum t_{Wa} > \sum t_{Wa,zul} \tag{7.5.11}$$

ΔQ_0 = Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb

Q_0= Festgelegte Betriebsqualität im Regelbetrieb (z.B. wirtschaftlich optimaler Bereich, $Q_0 = 0{,}5 - 1{,}2$)

$\sum t_{Wa,zul}$= Zulässige Summe der außerplanmäßigen Wartezeit in einem Betriebsprogramm

$\sum t_{Wa}$= Tatsächliche Summe der außerplanmäßigen Wartezeit in einem Betriebsprogramm.

Entsprechend der Formel 7.5.11 kann die Abweichung von der vereinbarten Betriebsqualität absolut betrachtet in das unendliche wachsen. Da der Risikoindex aus dem vorigen Unterkapitel prozentual angegeben ist und beide Kenngrößen in der Funktion für die Systemeffektivität miteinander verrechnet werden, ist es sinnvoll, die Abweichung von der vereinbarten Betriebsqualität ebenfalls relativ anzugeben.

Hierbei wird die im Regelbetrieb festgelegte Betriebsqualität als Referenz angenommen. Demnach ist der Wert für die Capability umso kleiner, je größer die Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb ist. Solange die Summe der tatsächlichen außerplanmäßigen Wartezeit kleiner oder gleich der zulässigen Summe der außerplanmäßigen Wartezeit entspricht, gilt für Capability = 1. Folglich kann die Kenngröße Capability, ausgedrückt durch die relative Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb, folgendermaßen abgeschätzt werden:

$$C = \frac{Q_0}{Q_0 + \Delta Q_0} \qquad \forall \sum t_{Wa} > \sum t_{Wa,zul} \tag{7.5.12}$$

C = Capability, ausgedrückt durch die relative Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb

Q_0= Festgelegte Betriebsqualität im Regelbetrieb (z.B. wirtschaftlich optimaler Bereich, $Q_0 = 0{,}5 - 1{,}2$)

$\sum t_{Wa,zul}$= Zulässige Summe der außerplanmäßigen Wartezeit in einem Betriebsprogramm

$\sum t_{Wa}$= Tatsächliche Summe der außerplanmäßigen Wartezeit in einem Betriebsprogramm.

Wie bereits im vorigen Unterkapitel zusammengefasst, scheint es sinnvoll, eine betrieblich-technische Rückfallebene heranzuziehen, die am geringsten außerplanmäßige Wartezeiten verursacht, sofern durch die Anwendung einer betrieblich-technischen Rückfallebene das Betriebsrisiko nicht vollständig ausgeschöpft wird.

Es gibt verschiedene eisenbahnbetriebswissenschaftliche Verfahren zur Bestimmung der Summe der tatsächlichen außerplanmäßigen Wartezeiten und damit die Abweichung der Betriebsqualität. Da diese Verfahren hauptsächlich toolbasiert durchgeführt werden, ist die Diskussion der Eignung der Verfahren entsprechend der inhaltlichen Eingrenzung aus dem Kapitel 3.5 nicht Gegenstand dieser Arbeit. Die Auswirkung einer betrieblich-technischen Rückfallebene auf die Betriebsqualität wird später im Anwendungskapitel exemplarisch anhand eines einfachen Anwendungsbeispiels ermittelt.

7.5.3 Abschätzung der Lebenszykluskosten

Die Lebenszykluskosten für die Migration des vollautomatisierten Bahnbetriebs sind für die Verwendung der Formel 7.5.1 abzuschätzen.

Für die Migration der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme (aus dem Kapitel 4.7) werden Lebenszykluskosten anfallen. Wie bereits zu Beginn des Hauptkapitels erwähnt, verursachen technische Redundanzen erhebliche Kosten.

Auch die im Rahmen dieser Arbeit (Hauptkapitel 6) entwickelten betrieblich-technischen Rückfallebenen auf Basis der dynamischen Adaption zur Laufzeit verursachen Kosten bei der Migration.

Damit entstehen Kosten sowohl für die technischen Redundanzen als auch für die ATO-FMU, mit der die dynamische Adaption zur Laufzeit erfolgt. Diese Kostenbestandteile addieren sich zu den Basiskosten der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme.

Die Summe der Lebenszykluskosten kann demnach folgendermaßen ermittelt werden:

$$LCC_{Gesamt} = LCC_{Basis} + LCC_{Redundanz} + LCC_{D,i} \quad 7.5.13$$

LCC_{Gesamt}=gesamte Lebenszykluskosten als Summe der Basiskosten für die Migration des vollautomatisierten Bahnbetriebs und der Kosten für die technischen Redundanzen sowie für die dynamische Adaption (ATO-FMU).

LCC_{Basis}= Basiskosten der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme

$LCC_{Redundanz}$=Zusatzkosten für die technischen Redundanzen

$LCC_{D,i}$= Zusatzkosten für die dynamische Adaption (ATO-FMU) einschließlich der erforderlichen Ressourcen für die betrieblich-technischen Rückfallebenen.

Jedoch sind keine Informationen über die erwarteten Kosten der technischen Redundanzen und der ATO-FMU mit den erforderlichen Ressourcen für die betrieblich-technischen Rückfallebenen aus dem Hauptkapitel 6 verfügbar.

Wie bereits zuvor in Unterkapitel 7.5.1 erwähnt, können die Betreiber durch die Vorgabe der RAM-Werte die Häufigkeit einer Störungssituation und der Anwendung einer betrieblich-technischen Rückfallebene beeinflussen. Die Variation der RAM-Werte bewirkt auch eine Änderung in den Lebenszykluskosten und der Risikoindex nach *(Huang 2020)* wird dadurch prozentual verändert. Prinzipiell könnte bewertet werden, welche Kosten eine bestimmte prozentuale Änderung in den RAM-Werten absolut verursachen. Auf der einen Seite liegen zwar noch keine Informationen über die erwarteten Kosten für den vollautomatisierten Bahnbetrieb vor. Auf der anderen Seite ist aber bekannt, dass die für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme sogenannte Kosten verursachen werden, die als Basiskosten für den Regelbetrieb angesehen werden können.

Um trotz fehlender Informationslage über die Lebenszykluskosten im Rahmen dieser Arbeit (in Hauptkapitel 8) die Systemeffektivität von ausgewählten betrieblich-technischen Rückfallebenen anhand eines Anwendungsbeispiels bewerten zu können, eignet es sich, die Lebenszykluskosten mit der Veränderung abzuschätzen.

Wie bereits oben in der Formel 7.5.13 angegeben, können dabei die Basiskosten der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme als Referenz herangezogen werden. Jede Erhöhung der Basiskosten aufgrund der Erhöhung der RAM-Werte oder der Kosten für die jeweilige dynamische Adaption kann prozentual angegeben werden. Das bedeutet, dass zu den erforderlichen Basiskosten für den Regelbetrieb (100 %) weitere Zusatzkosten hinzukommen können. Demnach kann die Änderung der Lebenszykluskosten gegenüber den Basiskosten für den Regelbetrieb folgendermaßen ermittelt werden:

$$LCC_{rel} = 1 + \frac{LCC_{Redundanz} + LCC_{D,i}}{LCC_{Basis}} \quad 7.5.14$$

LCC_{Gesamt} = gesamte Lebenszykluskosten aus der Summe der Basiskosten für die Migration des vollautomatisierten Bahnbetriebs und der Kosten für die technischen Redundanzen sowie für die dynamische Adaption (ATO-FMU)

LCC_{rel} = Prozentuale (relative) Änderung der Lebenszykluskosten im Vergleich zu den Basiskosten aufgrund der technischen Redundanzen und der dynamischen Adaption (ATO-FMU) einschließlich der erforderlichen Ressourcen für eine betrieblich-technische Rückfallebene

LCC_{Basis} = Basiskosten der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme

$LCC_{Redundanz}$ = Zusatzkosten für die technischen Redundanzen

$LCC_{D,i}$ = Zusatzkosten für die dynamische Adaption (ATO-FMU) einschließlich der erforderlichen Ressourcen für eine betrieblich-technische Rückfallebene

Die Erarbeitung von Einflussgrößen zur Ermittlung der Basiskosten für die Migration des vollautomatisierten Bahnbetriebs, der Kosten für die technischen Redundanzen und für die ATO-FMU, mit der die dynamische Adaption zur Laufzeit erfolgt, kann aufgrund der fehlenden Datengrundlage nicht im Rahmen dieser Arbeit nicht erfolgen.

7.5.4 Bewertungsverfahren zur Anwendung für eine Migrationsentscheidung und zur Laufzeit

Nachdem nun in den Unterkapiteln 7.5.1 – 7.5.3 die Bestandteile der Formel für Systemeffektivität untersetzt wurden, können diese Bestandteile nun in die Formel 7.5.1 aus dem Kapitel 7.5 eingesetzt werden.

Das Ziel der betrieblich-technischen Rückfallebenen ist, eine Betriebsführung in Störungssituationen zu gewährleisten. Daher ist eine Weiterfahrt in Störungssituationen auch eine Muss-Anforderung aus dem Unterkapitel 3.2.4. Ausgehend von dieser Muss-Anforderung gibt es bei der Bewertung der in Hauptkapitel 6 entwickelten betrieblich-technischen Rückfallebenen hinsichtlich ihrer Systemeffektivität mit der Formel 7.5.1 zwei Möglichkeiten, die im Weiteren vergleichend diskutiert werden.

In Anlehnung an das Prinzip der Risiko-Budgetierung nach *Huang (2020)* steht ein fester Risikogrenzwert für das gesamte Bahnnetz pro Kalenderjahr zur Verfügung. Demnach ist es zum einen möglich, mit dem fest zur Verfügung stehenden Risikobudget pro Kalenderjahr den maximalen Nutzen aus den betrieblich-technischen Rückfallebenen zu erzielen. Der maximale Nutzen einer betrieblich-technischen Rückfallebene ergibt sich dann, wenn die Summe aus der Abweichung der Betriebsqualität und der Lebenszykluskosten bei einem festen Risikobudget möglichst minimal gehalten wird.

Zum anderen ist es auch möglich, die Systemeffektivität der betrieblich-technischen Rückfallebenen aus der Perspektive der Aufwandsminimierung zu bewerten. Das bedeutet, die Muss-Anforderung mit möglichst minimalem Aufwand zu erfüllen.

Während die erste Möglichkeit mit dem festen Risikobudget eine Bewertung nach dem sogenannten Maximalprinzip vornimmt, liegt der Schwerpunkt der zweiten Möglichkeit auf der Aufwandsminimierung (Minimalprinzip) bei einem festgelegten Ziel (Erfüllung der Muss-Anforderung). Beim Minimalprinzip können alle Kenngrößen aus der Formel 7.5.1 variieren, während beim Maximalprinzip der Risikogrenzwert fest vorgegeben ist.

Prinzipiell ist die Bewertung der betrieblich-technischen Rückfallebenen nach dem Maximalprinzip möglich. Dabei werden die betrieblich-technischen Rückfallebenen migriert bzw. ausgewählt, wodurch die Summe aus der Abweichung der Betriebsqualität und der Lebenszykluskosten – unter der Voraussetzung, dass die Erhöhung des Betriebsrisikos unter dem Risikogrenzwert liegt – am geringsten ist. Wie bereits in Unterkapitel 7.5.1 erläutert, kann sich die Sicherheit der Betriebsführung abhängig von der gewählten betrieblich-technischen Rückfallebene aus dem Kapitel 6.6 aufgrund der unterschiedlichen Gefährdungsraten der eingebundenen Ressourcen unterscheiden. Durch Bewertung nach dem Maximalprinzip kann es vorkommen, dass eine betrieblich-technische Rückfallebene einen höheren Nutzen erzielt, obwohl das Betriebsrisiko gegenüber einer anderen betrieblich-technischen Rückfallebene erhöht ist. Dadurch wird die Erhöhung des Betriebsrisikos bis zum Risikogrenzwert vernachlässigt. Diese Tatsache stellt insofern einen Nachteil dar, da nach *Huang (2020)* die gleichmäßige Aufteilung des Risikogrenzwerts des gesamten öffentlichen Schienennetzes pro Kalenderjahr auf kleinere Betrachtungsräume (im Rahmen dieser Arbeit z.B. Zuständigkeitsbereiche der jeweiligen ATO-TS) nicht zielführend ist, da Störungen in den kleineren Betrachtungsräumen in unterschiedlichem Maße auftreten können. Die Fixierung des gleichmäßig aufgeteilten Risikogrenzwertes nach dem Maximalprinzip würde bedeuten, dass zwei betrieblich-technische Rückfallebenen aus dem Kapitel 6.6 mit dem gleichen Betriebsrisiko in unterschiedlichen ATO-TS Zuständigkeitsbereichen unterschiedlich häufig angewandt werden dürfen.

Im Gegensatz zu der Bewertung nach dem Maximalprinzip, bei dem der gleichmäßig aufgeteilte Risikogrenzwert fixiert wird, wird bei der Bewertung nach dem Minimalprinzip versucht, sowohl die Erhöhung des Betriebsrisikos als auch die Summe aus der Abweichung der Betriebsqualität und der Lebenszykluskosten zu minimieren. Dadurch können alle drei Kenngrößen aus den Unterkapiteln 7.5.1, 7.5.2 und 7.5.3 simultan variieren. Da der vollautomatisierte Bahnbetrieb noch nicht migriert ist, kann mit dem Minimalprinzip der Risikogrenzwert für den vollautomatisierten Bahnbetrieb in Abhängigkeit der betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6 vor der Migration bestimmt werden. Denn der in *Huang (2020)* bestimmte Risikogrenzwert gilt für den gegenwärtigen Bahnbetrieb und wurde aus früheren Unfallstatistiken hergeleitet. Abhängig davon, wie häufig eine betrieblich-technische Rückfallebene im vollautomatisierten Bahnbetrieb angewandt wird und wie hoch dabei das verursachte Betriebsrisiko ist, kann mit dem Minimalprinzip der erwartete Risikogrenzwert des vollautomatisierten Bahnbetriebs, unter Berücksichtigung der anderen beiden Kenngrößen, abgeschätzt werden. Dadurch wäre der oben genannte Nachteil von dem Maximalprinzip kompensiert.

Nach dem Minimalprinzip ist die Systemeffektivität einer betrieblich-technischen Rückfallebene aus dem Kapitel 6.6 am höchsten, wenn die Erhöhung des Betriebsrisikos je Rückfallebene minimal ist und die Abweichung von der Betriebsqualität minimal ist und dabei so wenig wie möglich Kosten entstehen. Diese Art der Aufwandsminimierung stellt jedoch einen Idealfall (theoretischen Fall) dar und trifft in der Praxis nicht bzw. nur selten ein. Denn durch Erhöhung der RAM-Werte kann zwar der Nutzen hinsichtlich des Betriebsrisikos und der Betriebsqualität erhöht werden, jedoch steigen dadurch auch die Lebenszykluskosten, sodass die Systemeffektivität einen bestimmten Wertebereich einnimmt.

Von den drei Kenngrößen aus der Formel 7.5.1 ist nur der Risikogrenzwert des gesamten öffentlichen Schienennetzes pro Kalenderjahr vorgegeben und nach *Huang (2020)* auch verbindlich einzuhalten. Wenngleich dieser Risikogrenzwert für den gegenwärtigen Bahnbetrieb gilt, kann dieser im Rahmen dieser Arbeit in Anlehnung an das GAMAB-Prinzip aus *DIN EN 50126-2:2017* aufgrund der fehlenden Betriebserfahrung mit dem vollautomatisierten Bahnbetrieb verwendet werden.

Mit einem vorgegebenen Risikogrenzwert kann folglich die Bewertung der Systemeffektivität der betrieblich-technischen Rückfallebenen für die Migrationsentscheidung nach dem Maximalprinzip erfolgen. Der einzuhaltende Risikogrenzwert wird zwar fest vorgegeben, jedoch wird die jeweils von den betrieblich-technischen Rückfallebenen abhängige Erhöhung des Betriebsrisikos ebenfalls in der Bewertung mitberücksichtigt. Denn dadurch kann trotz des fixierten Risikogrenzwertes bestimmt werden, wie viel von dem zur Verfügung stehenden Risikobudget je betrieblich-technische Rückfallebene verbraucht wird und welche Lebenszykluskosten dafür zu erwarten sind.

Bei der Bewertung der Systemeffektivität der betrieblich-technischen Rückfallebenen für die Migrationsentscheidung ist jedoch die oben genannte Tatsache zu berücksichtigen, dass Störungen in den kleineren Betrachtungsräumen in unterschiedlichem Maße auftreten können und dass sich dadurch die Systemeffektivität einer betrieblich-technischen Rückfallebene in zwei unterschiedlichen Betrachtungsräumen unterscheiden kann.

Wie bereits zuvor in Unterkapitel 7.5.1 erwähnt, können die Betreiber durch die Vorgabe der RAM-Werte die Häufigkeit einer Störungssituation und der Anwendung einer betrieblich-technischen Rückfallebene beeinflussen. Da die Variation der RAM-Werte auch eine Änderung in den Lebenszykluskosten bewirkt und der Risikoindex nach *(Huang 2020)* dadurch prozentual verändert wird, wurden in den Unterkapitel 7.5.2 und 7.5.3 die Kenngrößen Capability und Lebenszykluskosten über die relative Veränderung abgeschätzt.

Um alle drei Kenngrößen RAMS, Capability und die Lebenszykluskosten einheitlich in die Formel für die Systemeffektivität einbringen und nach dem Maximalprinzip bewerten zu können, wird im Weiteren der Wertebereich der Systemeffektivität – auch unter Berücksichtigung der prozentualen Angabe des Risikoindexes – von 0 bis 1 festgelegt.

Damit bedeutet eine Systemeffektivität von 1, dass eine betrieblich-technische Rückfallebene keine Auswirkung auf die Sicherheit und auf die Betriebsqualität hat und zugleich keine Zusatzkosten verursacht. Wie bereits zuvor erläutert, stellt dieser Fall einen Idealfall dar. Eine Systemeffektivität von 0 bedeutet hingegen, dass eine betrieblich-technische Rückfallebene das Risikobudget (z.B. Pro Kalenderjahr) komplett verbraucht oder die Summe der tatsächlichen außerplanmäßigen Wartezeiten im Betrachtungsraum derart zunimmt, sodass die mittlere Wartezeit der betroffenen Züge im Betrachtungsraum gegen unendlich geht und dadurch die Betriebsqualität aus dem Regelbetrieb signifikant abweicht.

Folglich kann die Systemeffektivität einer betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption zur Laufzeit für eine Migrationsentscheidung – unter Berücksichtigung der Auswirkung auf die Sicherheit der Betriebsführung, Auswirkung auf die Betriebsqualität und den verursachten Zusatzkosten – mit der folgenden Funktion bewertet werden:

$$SE = \frac{\left[1 - \left(\frac{n_{Störung} * BR_{D,i}}{R_{Grenz}}\right)\right] * \left[\frac{Q_0}{Q_0 + \Delta Q_0}\right]}{1 + \frac{LCC_{Redundanz} + LCC_{D,i}}{LCC_{Basis}}} \quad \forall \frac{n_{Störung_i} * BR_{D,i}}{R_{Grenz}} \leq 1 \qquad 7.5.15$$

SE = Systemeffektivität einer betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption zur Laufzeit

$BR_{D,i}$ = Betriebsrisiko der jeweiligen dynamischen Adaption mit unterschiedlicher Gefährdungsrate

$n_{Störung_i}$ = Häufigkeit einer Störungssituation aufgrund einer Störung in einem Systemelement i

R_{Grenz} = Risikogrenzwert auf einem Netzelement mit einem bestimmten Streckenstandard

Q_0 = Festgelegte Betriebsqualität im Regelbetrieb (z.B. wirtschaftlich optimaler Bereich, $Q_0 = 0{,}5 - 1{,}2$)

ΔQ_0 = Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb

LCC_{Basis} = Basiskosten der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme

$LCC_{Redundanz}$ = Zusatzkosten für die technischen Redundanzen

$LCC_{D,i}$ = Zusatzkosten für die dynamische Adaption (ATO-FMU) einschließlich der erforderlichen Ressourcen für die betrieblich-technischen Rückfallebenen

Durch Zuhilfenahme der Formeln 7.5.10 und 7.5.14 lässt sich die Formel 7.5.15 zu dem folgenden Ausdruck vereinfachen:

$$SE = \frac{\left(1 - RI_{dyn}\right) * \left[\frac{Q_0}{Q_0 + \Delta Q_0}\right]}{LCC_{rel}} \qquad 7.5.16$$

SE = Systemeffektivität einer betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption zur Laufzeit

RI_{dyn} = Erwarteter Risikoindex einer betrieblich-technischen Rückfallebene über die Lebensdauer

Q_0 = Festgelegte Betriebsqualität im Regelbetrieb (z.B. wirtschaftlich optimaler Bereich, $Q_0 = 0{,}5 - 1{,}2$)

ΔQ_0 = Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb

LCC_{rel} = Prozentuale (relative) Änderung der Lebenszykluskosten im Vergleich zu den Basiskosten aufgrund der technischen Redundanzen und der dynamischen Adaption (ATO-FMU) einschließlich der erforderlichen Ressourcen für die betrieblich-technischen Rückfallebenen.

Mit der Formel 7.5.15 oder 7.5.16 können Betreiber vor der Migration die Systemeffektivität der im Rahmen dieser Arbeit entwickelten betrieblich-technischen Rückfallebenen bewerten. Das Verfahren dazu wird in der Abbildung 43 dargestellt und im Folgenden erläutert.

Entsprechend des Unterkapitels 7.5.1 hängt die Häufigkeit von Störungssituationen von der MTBF des jeweiligen technischen Systems ab. Daher können die Betreiber zunächst durch Vorgabe von Verfügbarkeitswerten (RAM-Werte) für die technischen Systeme oder durch die Wahl der Art und Umfang von technischen Redundanzen die erwartete Häufigkeit der Störungssituationen über die gesamte Lebensdauer oder über einen bestimmten Betrachtungszeitraum (engl., Period of Interest) ermitteln.

Parallel dazu werden ein Betrachtungsraum und ein Betrachtungszeitraum zur Bestimmung der aufgrund von Störungssituationen einschließlich der in Hauptkapitel 6 entwickelten betrieblich-technischen Rückfallebenen verursachten außerplanmäßigen Wartezeiten festgelegt. Damit die Auswirkung von Störungssituationen einschließlich der in Hauptkapitel 6 entwickelten betrieblich-technischen Rückfallebenen auf die Betriebsqualität bewertet werden kann, ist ebenfalls ein

Betriebsprogramm festzulegen, anhand dessen dann die zulässige Summe der außerplanmäßigen Wartezeiten ermittelt wird.

Durch Generierung von technischen Störungen können dann die für die Störungssituation geeigneten betrieblich-technischen Rückfallebenen aus dem Hauptkapitel 6 ausgewählt und entsprechend der Formel 7.5.3 das zugehörige Betriebsrisiko ermittelt werden.

Um in Abhängigkeit der Häufigkeit der Anwendung der jeweiligen betrieblich-technischen Rückfallebene das zusätzlich verursachte Betriebsrisiko zu ermitteln, ist der Risikogrenzwert in einem Betrachtungszeitraum nach *Huang (2020)* zu ermitteln.

Nachdem die Summe der außerplanmäßigen Wartezeiten und der Risikoindex der jeweiligen betrieblich-technischen Rückfallebene ermittelt wurde, kann schließlich die Systemeffektivität der jeweiligen betrieblich-technischen Rückfallebenen mit der Formel 7.5.15 oder 7.5.16 bewertet werden.

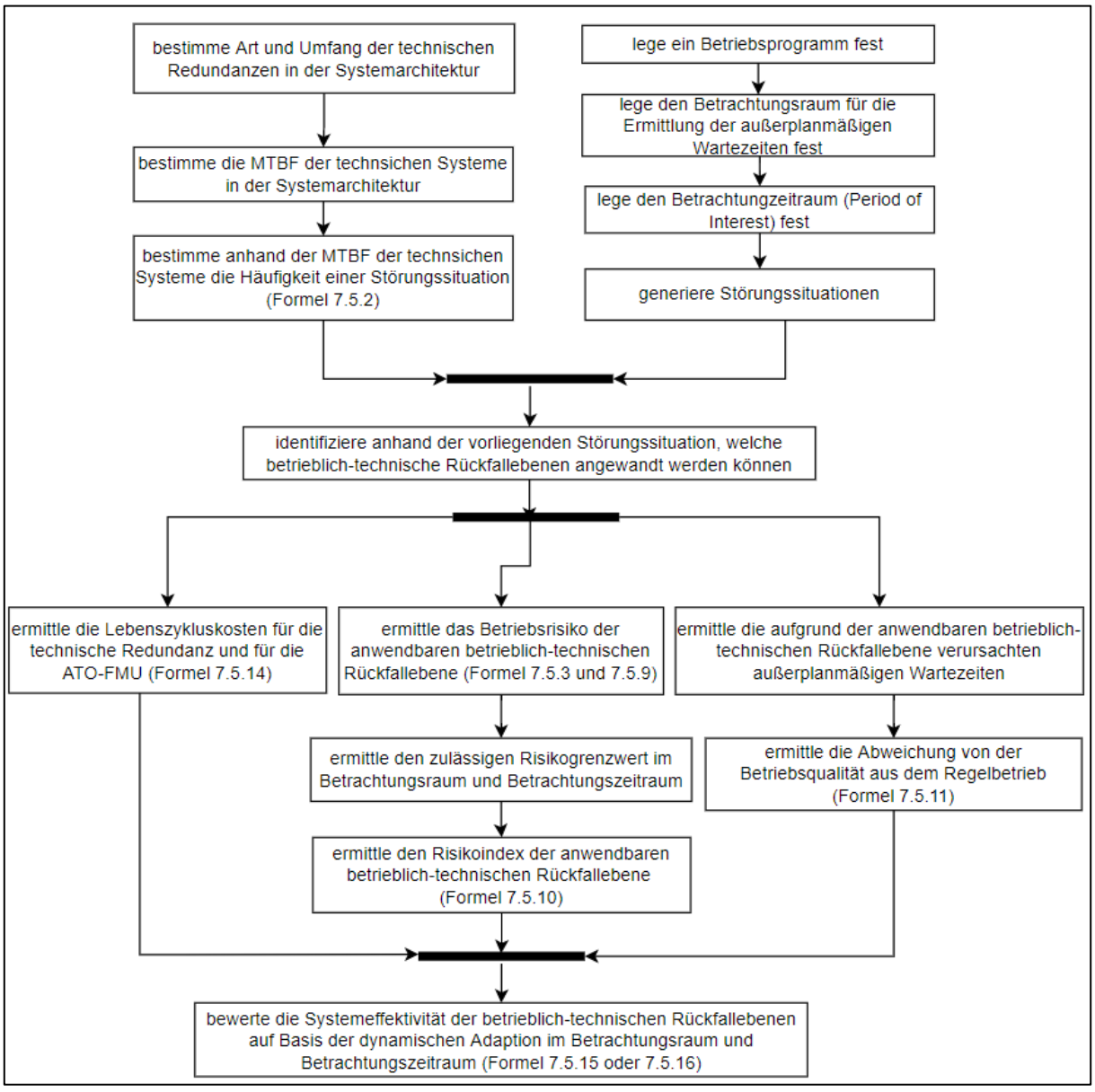

Abbildung 43 Bewertungsverfahren für eine Migrationsentscheidung

Schließlich erfolgt noch eine kurze Interpretation der Formel 7.5.16 für die Bewertung der Systemeffektivität.

Die Funktion für Systemeffektivität aus der Formel 7.5.16 ist in Abbildung 44 als Diagramm in Abhängigkeit erwarteter Risikoindex und der Abweichung von der Betriebsqualität für verschiedene Lebenszykluskosten dargestellt. Der Verlauf der Funktion für Systemeffektivität zeigt zwei wesentliche Erkenntnisse.

Die Wahl der Art und Umfang der technischen Redundanz beeinflusst die Systemeffektivität signifikant. Zum einen kann dadurch die Häufigkeit einer technischen Störung über die Lebensdauer des technischen Systems reduziert werden. Je weniger Störungssituationen im vollautomatisierten Bahnbetrieb auftreten, umso weniger müssen betrieblich-technische Rückfallebenen angewandt werden. Durch technische Redundanzen wird zum einen weniger zusätzliches Betriebsrisiko im Betriebsablauf generiert und zum anderen auch aufgrund des schnellen Umschaltens auf das redundante technische System die Betriebsqualität nicht beeinträchtigt. Jedoch sind technische Redundanzen mit signifikanten Kosten verbunden, weshalb dadurch die Systemeffektivität – wie zuvor erläutert – nie den Wert 1 erreicht.

Zum anderen verschwindet die Systemeffektivität bei der Anwendung einer betrieblich-technischen Rückfallebene, sofern das Risikobudget dadurch komplett verbraucht wird. Das hängt jedoch von der Häufigkeit der Anwendung und der Dauer der jeweiligen betrieblich-technischen Rückfallebene ab.

Eine entscheidende Frage bei der Bewertung nach der betrieblich-technischen Rückfallebene anhand der Formel 7.5.16 ist es, welche Kenngröße bei der Entscheidung maßgebend ist. Prinzipiell kann die Entscheidung entsprechend des Grundprinzips des Bahnbetriebs (Anforderung aus dem Kapitel 3.3) nach „Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“ getroffen werden. Das bedeutet, sofern die Systemeffektivität für zwei betrieblich-technische Rückfallebenen gleich ist, wird die mit dem geringsten Betriebsrisiko ausgewählt.

Wie bereits in Unterkapitel 7.5.2 erläutert, kann es in einer Störungssituation vorkommen, dass durch die Anwendung einer betrieblich-technischen Rückfallebene das zur Verfügung stehende Risikobudget nicht vollständig verbraucht wird. Dadurch ist es auch möglich, vor der Migration durch gezielte Simulation von Betriebssituationen (Störungssituationen), ein optimales Verhältnis zwischen Betriebsrisiko, Betriebsqualität und Lebenszykluskosten zu finden. Durch Anwendung des Bewertungsverfahrens aus der Abbildung 43 mit der zugehörigen Bewertungsfunktion für die Systemeffektivität (Formel 7.5.16) kann beispielsweise ein Betreiber auch die für einen robusten vollautomatisierten Bahnbetrieb erforderlichen Reservezeiten (z.B. Pufferzeiten) bei der Anwendung der betrieblich-technischen Rückfallebenen aus dem Hauptkapitel 6 proaktiv einplanen.

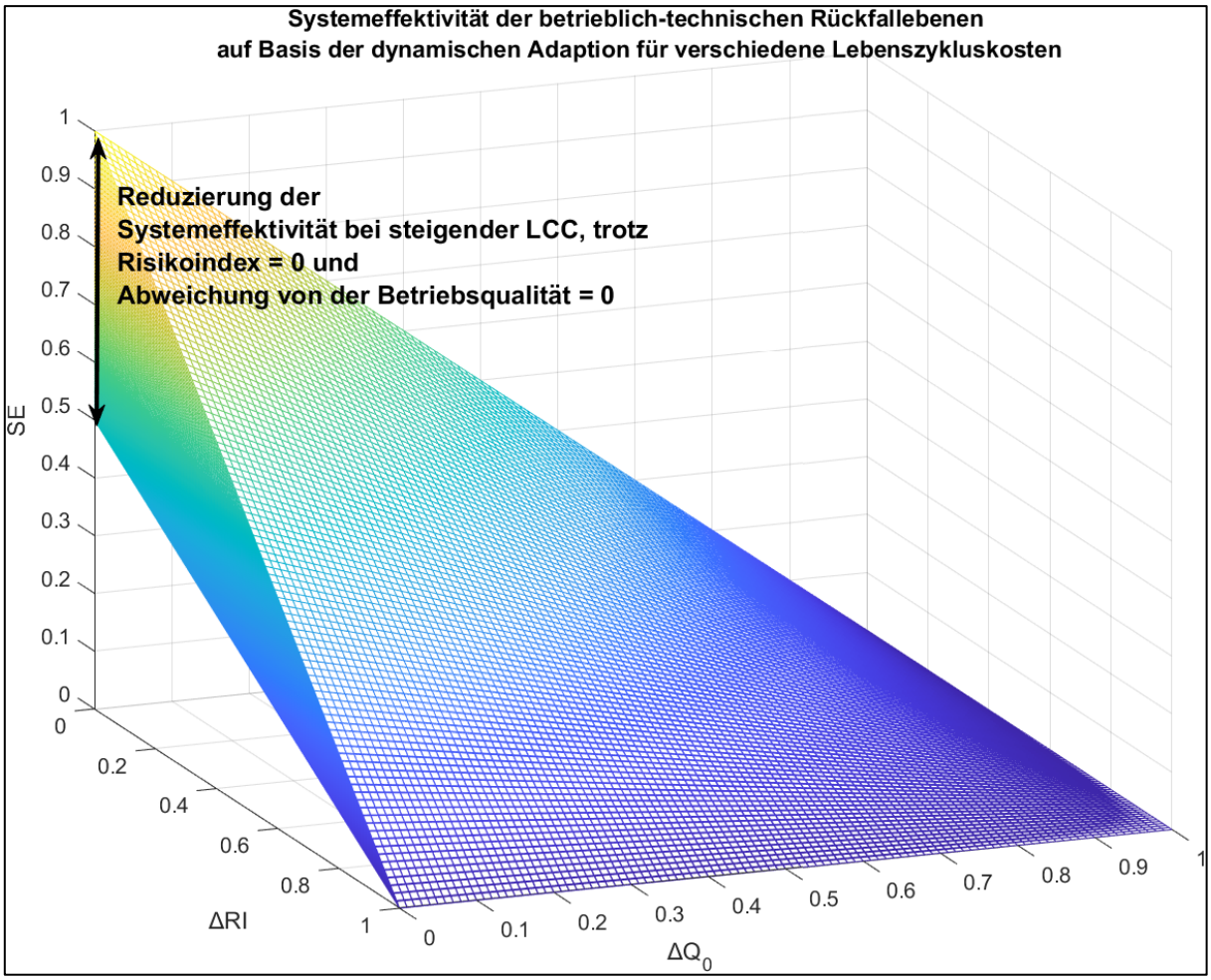

Abbildung 44 Systemeffektivität grafisch dargestellt in Abhängigkeit erwarteter Risikoindex und der Abweichung von der Betriebsqualität aus dem Regelbetrieb aufgrund von außerplanmäßigen Wartezeiten für verschiedene Lebenszykluskosten

Entsprechend der Anforderung aus dem Kapitel 7.2 soll das Bewertungsverfahren auch zur Laufzeit angewandt werden können.

Nachdem die Betreiber durch Bewertung der Systemeffektivität nach der Formel 7.5.16 eine Migrationsentscheidung getroffen haben, kann es vorkommen, dass mehrere betrieblich-technische Rückfallebenen in den vollautomatisierten Bahnbetrieb migriert werden.

Da sich die Bestandteile des Zählers aus der Formel 7.5.16 in Abhängigkeit der angewandten betrieblich-technischen Rückfallebene zur Laufzeit ändern kann, eignet es sich, die Bestandteile des Zählers bei der Bewertung der migrierten betrieblich-technischen Rückfallebenen zur Laufzeit heranzuziehen.

Das Betriebsrisiko einer betrieblich-technischen Rückfallebene hängt entsprechend der Formel 7.5.9 aus dem Unterkapitel 7.5.1 neben dem Schadensausmaß auch von der Dauer einer betrieblich-technischen Rückfallebene ab. Daher bedingen sich die beiden Kenngrößen im Zähler der Formel 7.5.16 nicht. Denn je kürzer eine betrieblich-technische Rückfallebene dauert, umso weniger wird das Betriebsrisiko erhöht und umso weniger kommt es zu einer Abweichung der Betriebsqualität.

Sofern entsprechend des Ablaufdiagramms in der Abbildung 30 auf der Seite 118 mehr als eine migrierte betrieblich-technische Rückfallebene in der vorliegenden Störungssituation anwendbar ist, erfolgt in Abhängigkeit der jeweiligen betrieblich-technischen Rückfallebene mit der Formel 7.5.6 zunächst die Bestimmung des adaptionsartspezifischen Betriebsrisikos.

Erst wenn das adaptionsartspezifische Betriebsrisiko der jeweiligen betrieblich-technischen Rückfallebene das zur Verfügung stehende Risikobudget nicht vollständig verbraucht, erfolgt im nächsten Schritt die Bestimmung der Dauer der jeweiligen betrieblich-technischen Rückfallebene, um daraus die tatsächlich verursachten außerplanmäßigen Wartezeiten zu bestimmen.

Entsprechend dieser sequenziellen Bewertung kann die Auswahllogik mit dem Ablaufdiagramm nach Abbildung 45 beschrieben werden, Der Ablauf nach Abbildung 45 untersetzt somit den Bewertungsschritt aus dem Unterkapitel 6.5.4.

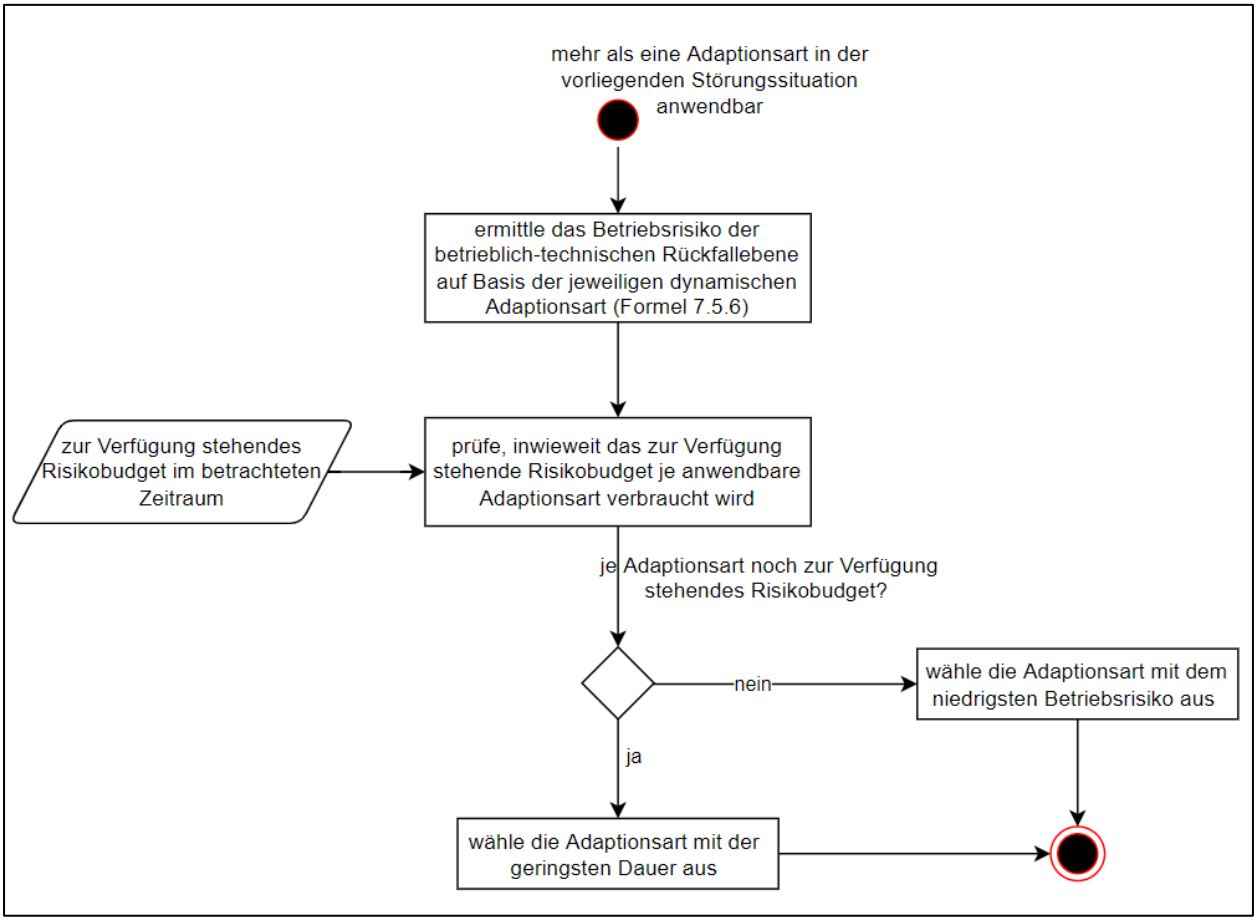

Abbildung 45 Ablauf der Bewertung, um das Betriebsrisiko der dynamischen Adaption zur Laufzeit in Abhängigkeit der Adaptionsart ermitteln zu können

7.6 Zusammenfassung des Hauptkapitels

Das Ziel dieses Kapitels war es, ein Bewertungsverfahren für die Bewertung der in Kapitel 6.6 erarbeiteten betrieblich-technischen Rückfallebenen vor einer Migration zu entwickeln.

Zunächst wurde ein geeignetes Bewertungsverfahren aus dem Unterkapitel 2.4.5 anhand seiner Eigenschaften und den Anforderungen aus dem Kapitel 7.2 ausgewählt. Mit dem ausgewählten Betriebsverfahren kann die Systemeffektivität einer betrieblich-technischen Rückfallebene in Abhängigkeit der Häufigkeit der Anwendung bewertet werden. Das ausgewählte Bewertungsverfahren berücksichtigt dabei die Kenngrößen Sicherheit, Betriebsqualität und Kosten simultan in einer Bewertungsfunktion. Dadurch wird eine Migrationsentscheidung mit drei wesentlichen Kenngrößen ermöglicht.

Da sich die Kenngröße Sicherheit während der Betriebsführung adaptionsartspezifisch unterscheiden kann, wurde diese Kenngröße mit dem adaptionsartspezifischen Betriebsrisiko abgeschätzt. Das adaptionsartspezifische Betriebsrisiko kann mit dem sogenannten Risikoleistungswert (RAW-Wert) in Abhängigkeit der logischen Verknüpfung der vorhandenen Systemelemente in der Systemarchitektur während einer betrieblich-technischen Rückfallebene bestimmt werden.

Nach dem Prinzip des Risikogrenzwerts *(Huang 2020)* kann es vorkommen, dass durch die Anwendung einer betrieblich-technischen Rückfallebene das Betriebsrisiko nicht vollständig ausgeschöpft wird. Um in so einer Betriebssituation eine betrieblich-technische Rückfallebene auszuwählen, wodurch die Betriebsqualität möglichst minimal beeinflusst wird, wurde die Auswirkung einer betrieblich-technischen Rückfallebene auf die Betriebsqualität mit den außerplanmäßigen Wartezeiten abgeschätzt.

Da die Lebenszykluskosten für die Migration des vollautomatisierten Bahnbetriebs noch nicht bekannt sind, aber dennoch Kosten sowohl für die technischen Redundanzen als auch für die ATO-FMU, mit der die dynamische Adaption zur Laufzeit erfolgt, entstehen, wurden die Lebenszykluskosten mit den prozentualen Zusatzkosten für die jeweilige dynamische Adaption und für die technischen Redundanzen abgeschätzt. Dabei wurden die Basiskosten für die Migration des vollautomatisierten Bahnbetriebs als Referenz herangezogen.

Die Systemeffektivität einer betrieblich-technischen Rückfallebene hinsichtlich der Sicherheit der Betriebsführung ist demnach hoch, je kleiner der Risikoindex ist. Beeinflussen lässt sich der Risikoindex dadurch, dass entweder die Anzahl der Störungen an den technischen Systemen durch technische Redundanzen reduziert wird oder dadurch, dass das Betriebsrisiko in der jeweiligen betrieblich-technischen Rückfallebene möglichst niedrig gehalten wird. Letzteres kann durch den Einsatz von Ressourcen mit niedriger Gefährdungsrate oder durch kurze Dauer der Betriebsführung in der betrieblich-technischen Rückfallebene erreicht werden.

Mit dem Bewertungsverfahren können Betreiber demnach Störungssituationen in verschiedenen Betriebsprogrammen simulieren und daraus eine Entscheidung treffen, welche Art der betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption zur Laufzeit migriert werden sollen. Außerdem kann mit dem erarbeiteten Bewertungsverfahren auch die Entscheidung über Art und Umfang der technischen Redundanz im vollautomatisierten Bahnbetrieb getroffen werden.

Schließlich ist es auch möglich, die Bestandteile des Zählers aus dem Bewertungsverfahren bei dem Bewertungsschritt entsprechend des Ablaufdiagramms in der Abbildung 30 auf der Seite 118 heranzuziehen. Die Auswahl einer betrieblich-technischen Rückfallebene zur Laufzeit erfolgt dann durch eine sequenzielle Bewertung hinsichtlich des Betriebsrisikos und der Auswirkung auf die Betriebsqualität.

8 Systemeffektivität von betrieblich-technischen Rückfallebenen auf Basis der dynamischen Adaption im vollautomatisierten Bahnbetrieb anhand eines Anwendungsbeispiels

8.1 Ziel des Kapitels

Nachdem in Hauptkapitel 6 betrieblich-technische Rückfallebenen auf Basis der dynamischen Adaption erarbeitet wurden, erfolgte in Hauptkapitel 7 die Entwicklung eines Bewertungsverfahrens, anhand dessen die Systemeffektivität der betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6 für eine Migrationsentscheidung bewertet werden kann.

Das Ziel dieses Kapitels ist nun, das Bewertungsverfahren aus dem Unterkapitel 7.5.4 anhand einer Störungssituation (Anwendungsbeispiel) anzuwenden.

8.2 Vorgehensweise und Rahmenbedingungen

Die Vorgehensweise für die Anwendung des Bewertungsverfahrens aus dem Unterkapitel 7.5.4 ergibt sich aus der Abbildung 43 auf der Seite 164.

Um das Betriebsszenario des Anwendungsbeispiels zu definieren, sind zunächst ein Betriebsprogramm, ein Betrachtungsraum einschließlich des Betrachtungszeitraums und eine Störungssituation festzulegen. Die Häufigkeit der zu definierenden Störungssituation wird dabei entsprechend des Unterkapitels 7.5.1 mit den Verfügbarkeitsangaben des für die Störungssituation relevanten technischen Systems abgeschätzt. Das Betriebsszenario für das Anwendungsbeispiel wird in Kapitel 8.3 definiert. In Unterkapitel 8.3.1 wird die Infrastruktur und somit der Betrachtungsraum (Auswerteraum) festgelegt. Daraufhin wird in Unterkapitel 8.3.2 das zugrundeliegende Betriebsprogramm festgelegt.

Nachdem in Unterkapitel 8.3.3 die beispielhafte Störungssituation vorgestellt wird, erfolgt in Kapitel 8.4 die Beschreibung der auf diese Störungssituation anwendbaren betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6. In Kapitel 8.4 werden die Kenngrößen in Anlehnung an die Ergebnisse aus dem Kapitel 7.5 quantifiziert.

Nachdem die für das Bewertungsverfahren erforderlichen Kenngrößen je vorzustellende betrieblich-technische Rückfallebene quantifiziert wurden, kann die Systemeffektivität der anwendbaren betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6 anhand der beispielhaften Störungssituation bewertet werden. Diese erfolgt dann in Kapitel 8.5.

Zuvor werden für das Anwendungsbeispiel einige Rahmenbedingungen festgelegt. Die Rahmenbedingungen für das Anwendungsbeispiel beruhen auf der inhaltlichen Eingrenzung der Arbeit aus dem Kapitel 3.5. Demnach liegt in dem Anwendungsbeispiel als Zugsicherung ETCS-L2 ohne Signale zugrunde. Der RBC Zuständigkeitsbereich erstreckt sich dabei auf 50 km und die maximale Länge einer Fahrterlaubnis, die durch das RBC für einen Zug ausgestellt werden kann auf 32 km *(vgl. Trinckauf et al. 2020, S. 78) und (DB Netz AG 2018, S. 6)*. Auf dem betrachteten Netzelement wird ein Mischverkehr ausschließlich mit GoA3 und GoA4 betriebenen Zügen angenommen.

8.3 Vorstellung des Betriebsszenarios

In diesem Kapitel wird das Betriebsszenario des Anwendungsbeispiels vorgestellt. In Unterkapitel 8.3.1 wird die Infrastruktur für den Auswerteraum festgelegt. Daraufhin wird in Unterkapitel 8.3.2 das zugrundeliegende Betriebsprogramm festgelegt. Anschließend wird in Unterkapitel 8.3.3 die beispielhafte Störungssituation vorgestellt.

8.3.1 Auswerteraum des Anwendungsbeispiels

Für die Bewertung wird zunächst der Bereich, für den Aussagen bezüglich des Betriebsrisikos und der Abweichung der Betriebsqualität getroffen werden soll, festgelegt.

In der Ril 405.0301 (3) nach *DB Netz AG (2022)* wird empfohlen, als Grenzen des Betrachtungsraumes Betriebsstellen zu wählen, in denen eine Reihenfolgeänderung möglich ist (Zugmeldestellen). Prinzipiell unterscheiden sich der Betrachtungsraum und der Auswerteraum. Jedoch können diese gemäß *DB Netz AG (2022)* auch identisch sein.

Damit auch bei der Bewertung des Betriebsrisikos und der Änderung der Betriebsqualität aus dem Regelbetrieb die Charakteristik des Betriebsprogramms möglichst gleichbleibt, wird in dem Anwendungsbeispiel das **Netzelement freie Strecke**, die zwei Betriebsstellen miteinander verbindet, als Auswerteraum zugrunde gelegt.

Entsprechend der Rahmenbedingung aus dem Kapitel 8.2 wird die Bewertung für einen Mischverkehrsbetrieb durchgeführt. Für Mischverkehrsstrecken werden in *DB Netz AG (2020)* Standardparameter für die Modellierung der Infrastruktur vorgeschrieben. Demnach hat das Netzelement freie Strecke

- insgesamt zwei Gleise und eine Länge von 20 km,
- einen Überholungsabstand von 20 km (Obergrenze),
- eine Blockabschnittslänge von 1,5 (Untergrenze) oder 4 km (Obergrenze) und
- einen Abstand für die Überleitverbindungen von 20 km (erst an der nächsten Betriebsstelle).

Die Blockabschnittslänge für einen Betrieb unter ETCS L2 oS kann jedoch aufgrund der Führerraumsignalisierung auch weiter reduziert werden. Da die Blockabschnittslänge in ETCS L2 u.a. von Ortungsfehler, von den im Fahrzeug hinterlegten ETCS-Bremsmodellen und von der Geschwindigkeit der Züge abhängt, wird für das Anwendungsbeispiel vereinfacht eine Blockabschnittslänge von $L_{Block,ETCS,L2} = 1{,}5$ km angenommen. Die Abbildung 46 stellt die dem Anwendungsbeispiel zugrundeliegende Infrastruktur dar.

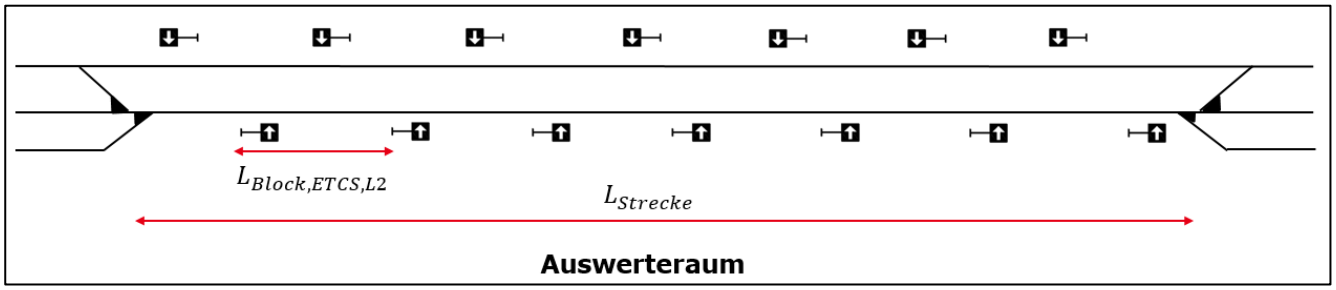

Abbildung 46: dem Anwendungsbeispiel zugrundeliegende Infrastruktur

8.3.2 Zugrundeliegendes Betriebsprogramm

Da der vollautomatisierte Bahnbetrieb noch nicht migriert ist, liegt auch kein Fahrplan zugrunde, anhand dessen die Bewertung durchgeführt werden kann. Daher ist für die Bewertung ein Betriebsprogramm festzulegen. In *DB Netz AG (2020)* gibt es für den Mischverkehrsbetrieb ebenfalls Angaben zum Betriebsprogramm. Neben den bereits oben angegebenen infrastrukturbezogenen Angaben sind darin Angaben zu

- der Streckengeschwindigkeit,
- den Modellzügen, bestehend aus unterschiedlichen Zuggattungen und

- der Anzahl der einzelnen Zuggattungen in dem Betriebsprogramm pro Zeiteinheit (in der Regel 24 h) enthalten.

Die Tabelle 4 enthält die relevanten Angaben des für die Bewertung zugrundeliegenden Betriebsprogramms. Als Modellzüge für den Mischverkehr werden Züge des Schienenpersonennahverkehrs (SPNV), Schienenpersonenfernverkehrs (SPFV) und Schienengüterverkehrs (SGV) herangezogen.

Tabelle 4 zugrundeliegendes Betriebsprogramm zur Bewertung der Systemeffektivität der dynamischen Adaption. Erstellt in Anlehnung an *DB Netz AG (2020)*

Betriebsprogramm für M160					
Modellzüge	SPFV: ICE	SPNV-S: RE	SPNV-L: RB	SGV-S	SGV-L
Höchstgeschwindigkeit der Modellzüge	250 km/h	160 km/h	120 km/h	100 km/h	80 km/h
Anzahl der Modellzüge / Richtung und h	4	2	1	2	1

Da für die Bewertung der Systemeffektivität der auf die beispielhafte Störungssituation anwendbaren betrieblich-technischen Rückfallebenen die Auswirkung auf die Betriebsqualität entsprechend der Formel 7.5.11 mit den außerplanmäßigen Wartezeiten abgeschätzt wird, ist zunächst in Abhängigkeit des festgelegten Betriebsprogramms die zulässige Summe der außerplanmäßigen Wartezeiten erforderlich. Diese wurde in Anhang 2 mit dem Mittelwertverfahren nach *Schwanhäußer (1974)* ermittelt und beträgt bei 1 Stunde und 10 Züge pro Stunde und Richtung $\sum \boldsymbol{t_{Wa,zul}} = \boldsymbol{44,3\ min.}$

8.3.3 Beispielhafte Störungssituation

In Hauptkapitel 5 wurden bereits die gefährlichen Betriebssituationen im vollautomatisierten Bahnbetrieb erarbeitet. Die wesentliche Erkenntnis aus der Gefährdungsanalyse ist, dass die Kommunikationsverbindung zwischen Zug und dem TMS oder der ETCS-Zentrale aufgrund der zentralen Systemarchitektur des Bahnbetriebs für eine sichere Zugfahrt unabdingbar ist. Bei fehlender bzw. unterbrochener Kommunikation zwischen Zug und dem TMS oder der ETCS-Zentrale müssen die vollautomatisierten Züge – insbesondere, die GoA4 geführten – vorübergehend selbstständig dezentral agieren.

Aufgrund der hohen Sicherheits- und Verfügbarkeitsanforderungen an die Kommunikation werden in ETCS-RAMS Dokumenten sehr hohe Werte für die mittlere Betriebsdauer zwischen den Ausfällen der ETCS-Systemelemente vorgeschrieben *(UIC 1998)*. So wird beispielsweise für die ETCS-Zentrale eine Nichtverfügbarkeit von $1 * 10^{-6}$ vorgeschrieben. Bei 5000 Betriebsstunden / Jahr entspricht dies pro ETCS-Zentrale eine Nichtverfügbarkeit von 0,3 min. Dieser Wert scheint nicht so hoch zu sein, sodass eine betrieblich-technische Rückfallebene nicht erforderlich ist.

Jedoch kommunizieren sowohl die ETCS-Zentrale als auch das Teilsystem ATO-TS über Funkbasisstationen mit den Zügen. Wie bereits in Kapitel 2.3 erwähnt, wird für den digitalen Bahnbetrieb der FRMCS-Standard als Kommunikationssystem spezifiziert. Die Funkbasisstationen im

FRMCS-5G Standard werden nach *Cellarius et al. (2021)* mit 1,9 GHz funken und die entsprechenden Funkbasisstationen eine Funkreichweite von 4 km aufweisen. Es liegen zwar noch keine Verfügbarkeitsanforderungen an das FRMCS System vor, jedoch kann im Weiteren ausgehend von der Anforderung der DB Netz AG an die Verfügbarkeit des GSM-R Dienstes grob abgeschätzt werden, wie oft Funkbasisstationen auf der Beispielstrecke in einem bestimmten Zeitraum ausfallen können.

Im Vergleich zu den ETCS-Zentralen haben Funkbasisstationen – zumindest beim aktuellen GSM-R Standard – höhere Ausfallraten. Die Anforderung der DB Netz AG an die Verfügbarkeit des GSM-R Dienstes ist, dass die GSM-R Dienste im Jahr 17 Minuten ausfallen dürfen *(Jurtz 2019)*. Nach GSM-R RAMS-Anforderungen (SUBSET-093) besteht ein direkter Einfluss der Verbindungsverlustrate und der Betriebsverspätungen von > 5 Min. Dort wird die Verbindungsverlustrate für den Fall, dass die MA den Zug nicht vor dem Stillstand erreicht (also T_NVCONTACT $>$ 40 s) als $2{,}7 * 10^{-4}/h$ angesetzt *(ERA 2005)*. Demnach können auf einer freien Strecke mit einer Länge von 20 km bei fünf Funkbasisstationen und mit 5000 Betriebsstunden pro Jahr 6,75 ($\sim$7) Verbindungsverluste erwartet werden.

Wenngleich auch die erwartete Anzahl von Verbindungsverlusten pro Jahr nicht hoch scheint, sind Kommunikationssysteme primäre Angriffsziele von Cyber-Angriffen. Für Cyber-Angriffe können keine Erwartungswerte abgeschätzt werden, dennoch kann davon ausgegangen werden, dass ein Cyber-Angriff nur eine Frage der Zeit ist und daher sicher zu erwarten ist. Durch Cyber-Angriffe können nicht nur Funkbasisstationen gestört werden, sondern auch ganze Zuständigkeitsbereiche der ETCS-Zentrale oder ATO-Zentrale können von Cyber-Angriffen betroffen sein.

Cyber-Angriffe haben die negative Eigenschaft, dass sie über einen längeren Zeitraum unbemerkt bleiben können. Außerdem können sie mehrere Systeme (z.B. mehrere Funkbasisstationen) gleichzeitig beeinträchtigen. Schließlich ist auch die Expositionsdauer eines Cyber-Angriffs schwer abschätzbar. Es kann daher vorkommen, dass in einem Kalenderjahr mehrere Cyber-Angriffe auf die Funkbasisstationen erfolgen und dabei Funklöcher für mehrere Stunden entstehen, die sich großflächig auswirken. Auch in *Trinckauf et al. (2020, S. 232)* werden großflächige Störungen am Kommunikationssystem nicht ausgeschlossen, weshalb dort auch für großflächige Störungen am Kommunikationssystem betrieblich-technische Rückfallebenen gefordert sind.

Als Störungssituation wird daher im Folgenden eine infrastrukturseitige Kommunikationsstörung – Störung von zwei Funkbasisstationen – zugrunde gelegt. Die Störungssituation ist in der Abbildung 47 dargestellt. Auf der freien Strecke sind insgesamt vier Funkbasisstationen einschließlich ihrer Funkbereiche als Ellipsen platziert, von denen zwei gestört sind. Die gestörten Funkbereiche sind rot markiert.

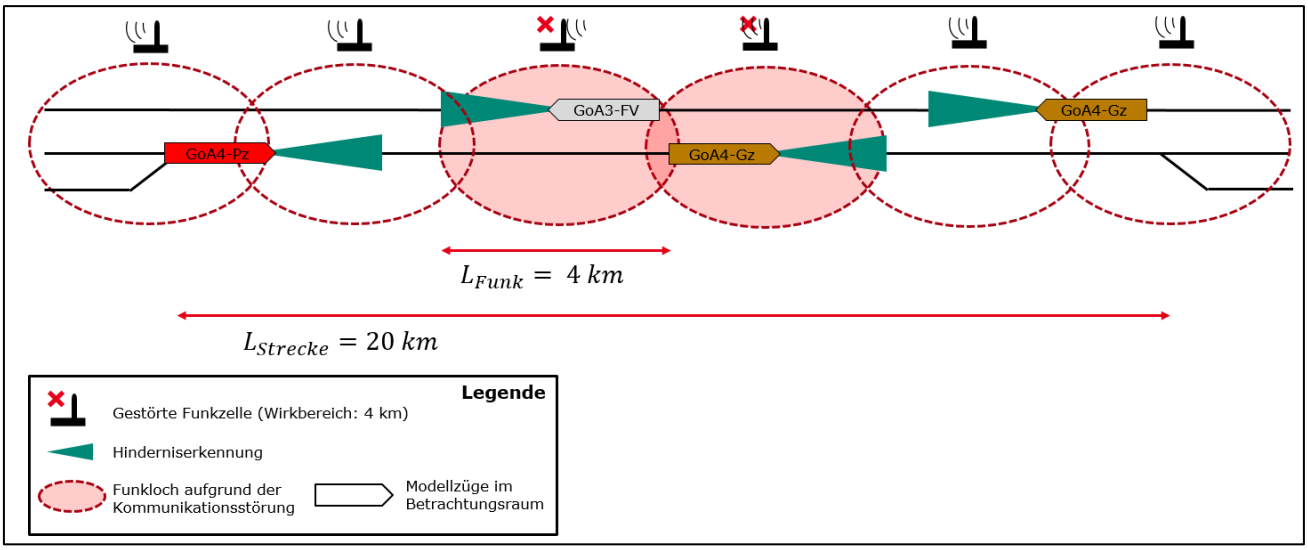

Abbildung 47 Anwendungsbeispiel mit Störung am infrastrukturseitigen Kommunikationssystem auf der freien Strecke. Zwei Funkbereiche in Länge von insgesamt 8 km sind gestört (eigene Darstellung)

Um das Betriebsrisiko und die verursachten außerplanmäßigen Wartezeiten ermitteln zu können, ist zunächst abzuschätzen, wie viele Züge pro Richtung von der beispielhaften Störungssituation betroffen sein können.

Die Berechnung der Mindestzugfolgezeit zwischen den verschiedenen Zugfolgefällen aus dem Betriebsprogramm und der mittleren Mindestzugfolgezeit ist in Anhang 2 zu finden. Daraus kann auch der verkettete Belegungsgrad auf der freien Strecke ermittelt werden. Anhand des Belegungsgrades und der mittleren Mindestzugfolgezeit kann der mittlere Ankunftsabstand der Züge pro Richtung in den beiden Funklöchern abgeschätzt werden. Die in Anhang 2 berechnete mittlere Mindestzugfolgezeit beträgt $\bar{z} = \mathbf{164,4\ s}$. Bei einer angenommenen Zugfolge-Pufferzeit von **1 min** beträgt der verkettete Belegungsgrad $\rho = \mathbf{0,73}$. Mit diesen Angaben beträgt der mittlere Ankunftsabstand dann

$$t_{Am} = \frac{\bar{z}}{\rho} = \frac{\mathbf{164,4\ s}}{\mathbf{0,73}} = \mathbf{225,2\ s\ (3,75\ min)}.$$

Das bedeutet, dass im Mittel alle 3,75 min ein Zug im Störungsbereich ankommt. Mit der mittleren Beförderungsgeschwindigkeit aus dem festgelegten Betriebsprogramm kann zudem abgeschätzt werden, wie lange ein Zug braucht, um durch das Funkloch durchzufahren. Die mittlere Beförderungsgeschwindigkeit ergibt sich aus dem gewichteten Mittelwert der Geschwindigkeiten der Modellzüge und beträgt in dem Betriebsprogramm aus dem Unterkapitel 8.3.2 $\bar{v} = \mathbf{172\ km/h}$. Demnach braucht ein Zug im mittel

$$t_{Funkloch} = \frac{\mathbf{8000\ m}}{\mathbf{172\ \frac{km}{h}}} = \mathbf{167,44\ s} \approx \mathbf{2,8\ min},$$

um durch das Funkloch durchzufahren.

Unter der Annahme, dass zum Zeitpunkt der Kommunikationsstörung (Funkloch) der Entdeckerzug pro Richtung unmittelbar vor dem Funklochbereich befindet und dieser nach 40 s zum Stillstand kommt, wäre schätzungsweise nur ein Zug (Entdeckerzug) pro Richtung von der beispielhaften

Störungssituation betroffen. Da es sich um eine zweigleisige Strecke handelt, kann auch ein Zug aus der Gegenrichtung betroffen sein. Demnach wird im Weiteren angenommen, dass von der beispielhaften Störungssituation **zwei Züge** (ein Zug pro Richtung) betroffen sind.

Anhand dieser Störungssituation und des zugrundeliegenden Betriebsprogramms erfolgt im nächsten Kapitel die Quantifizierung der Kenngrößen der anwendbaren betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6.

8.4 Mögliche betrieblich-technische Rückfallebenen für die vorliegende Störungssituation einschließlich der Quantifizierung der Kenngrößen

In Unterkapitel 8.4.1 erfolgt zunächst die Beschreibung der auf die zuvor vorgestellte beispielhafte Störungssituation anwendbaren betrieblich-technischen Rückfallebenen aus dem Kapitel 6.6. In Unterkapitel 8.4.2 werden dann die Kenngrößen in Anlehnung an die Ergebnisse aus dem Kapitel 7.5 quantifiziert.

8.4.1 Mögliche betrieblich-technische Rückfallebenen für die vorliegende Störungssituation

Wie bereits in Hauptkapitel 5 erläutert, führt eine infrastrukturseitige Kommunikationsstörung nach Ablauf der T_NVCONTACT (40 s bei DB) zu einer Zwangsbremsung der sich im Funkloch befindenden Züge, wodurch die Fahrterlaubnis der betroffenen Züge an die Zugspitze gekürzt wird. Unter der Annahme, dass die Kommunikationsverbindung auch nach den 40 s nicht aufgebaut werden kann, können die im Funkloch befindlichen Züge (Entdeckerzüge) nicht mehr sicher weiterfahren. Außerdem werden die Entdeckerzüge nach 5 min aus dem Speicher der ETCS-Zentrale gelöscht, sodass sie keine Fahrterlaubnis mehr erhalten (vgl. Kapitel 2.5).

Entsprechend des Unterkapitels 6.6.1 kann durch die dynamische Adaption entweder eine Drohne zur Übermittlung von Fahrterlaubnissen im Falle einer infrastrukturseitigen Kommunikationsstörung für ein Ad-Hoc Netzwerk eingebunden werden oder die Züge können über ein Ad-Hoc Netzwerk mit einem Object-Controller die Fahrterlaubnisse einfordern.

8.4.2 Quantifizierung der Kenngrößen eines Ad-Hoc Netzwerks mit einer Drohne

Betriebsrisiko des Ad-Hoc Netzwerks zur alternativen Übermittlung von Fahrterlaubnissen mit einer Drohne

Entsprechend der Formel 7.5.9 aus Unterkapitel 7.5.1 ergibt sich das Betriebsrisiko aus dem Produkt der geänderten Gefährdungsrate, der Dauer der betrieblich-technischen Rückfallebene und dem Schadensausmaß.

Da die von der infrastrukturseitigen Kommunikationsstörung betroffenen Züge nach dem Empfang der Fahrterlaubnisse ihre Fahrt im Regelbetrieb durchführen können, liegt das Betriebsrisiko bei einer drohnenbasierten Übermittlung von Fahrterlaubnissen nur während der Flugphase der Drohne zu den betroffenen Zügen vor. Somit besteht das Betriebsrisiko bei einer drohnenbasierten Übermittlung von Fahrterlaubnissen darin, dass die Drohne während der Flugphase zu den betroffenen Zügen unerwartet abstürzt. Aufgrund des unerwarteten Absturzes können Schaden an Personen oder an der Umwelt entstehen. Solange es sich bei den betroffenen Zügen um Personenzüge handelt, können zusätzlich die Zuginsassen entsprechend des Unterkapitels 5.6.1 im Stillstand auf der freien Strecke Gefährdungen ausgesetzt sein. Da jedoch die Wahrscheinlichkeit für schlechte klimatische Bedingungen in

Personenzügen nicht gegeben ist, wird im Weiteren **vereinfacht ein GoA4 geführter Güterzug** angenommen. Daher stellt der Stillstand eines Güterzugs keine Gefährdung dar.

Um das Betriebsrisiko des Ad-Hoc Netzwerks zur alternativen Übermittlung von Fahrterlaubnissen mit einer Drohne ermitteln zu können, ist die geänderte Gefährdungsrate der Drohne zu ermitteln. Zur Ermittlung der geänderten Gefährdungsrate ist die Kenntnis über die Wahrscheinlichkeit, dass eine Drohne auf dem Weg zu den Zügen abstürzen wird, erforderlich. Da jedoch keine Werte für die Ausfallwahrscheinlichkeiten der einzelnen Systemelemente einer Drohne vorliegen, kann vereinfacht eine Drohne mit einem bestimmten SIL-Level angenommen werden, woraus dann die Gefährdungsrate abgeschätzt werden kann. Unter der Annahme, dass Drohnen eingesetzt werden, die mindestens einen SIL von 1 aufweisen, hat die Gefährdungsrate einen Wertebereich von $\boldsymbol{\lambda_{Drohne} = 1 * 10^{-5} - 1 * 10^{-6}/h.}$

Neben der geänderten Gefährdungsrate ist auch die Kenntnis über das Schadensausmaß erforderlich. Da die Masse einer Drohne wesentlich niedriger ist als die eines Zuges, ist davon auszugehen, dass das Schadensausmaß S_{Drohne} ebenfalls niedriger ist als bei einem Zusammenstoß von zwei Zügen. Eine Drohne, die mit einer Geschwindigkeit zwischen 40 und 80 km/h fliegt, kann in die Geschwindigkeitsklasse 3 und nach *VDE V 0831-103:2020 (2020)* in die Unfallklasse D eingeordnet werden. Demnach kann das Schadensausmaß bei einer abgestürzten Drohne $\boldsymbol{S_{Drohne} = 0,1\, Opfer}$ angesetzt werden.

Schließlich ist auch die Dauer zur Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einer Drohne erforderlich.

Die Dauer zur Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einer Drohne ergibt sich entsprechend des Kommunikationsdiagramms aus dem Unterkapitel 6.6.1. Die Dauer setzt sich aus der Zeit für die Initialisierung einer Drohne (Bereitschaftsanfrage) $t_{init,Drohne}$, aus der Flugzeit $t_{Flug,1}$, aus der Zeit für die Bildung eines Ad-Hoc Netzwerks t_{Ad-Hoc} mit den Zügen und aus der Flugzeit zurück zum Ausgangspunkt der Drohne $t_{Flug,2}$ zusammen und kann mit der Formel 8.4.1 quantifiziert werden. Die Flugzeit einer Drohne zum Ausgangspunkt ist insofern relevant, da in der Zeit die Drohne auch abstürzen und dadurch Schaden verursachen kann.

$$t_{RFE,Drohne} = t_{init,Drohne} + t_{Flug,1} + t_{Ad-Hoc} + t_{Flug,2} \qquad 8.4.1$$

$t_{RFE,Drohne}$ = Dauer zur Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einer Drohne

$t_{init,Drohne}$ = Initialisierung einer Drohne (Bereitschaftsanfrage),

$t_{Flug,1}$ = Flugzeit der eingebundenen Drohne zu den betroffenen Zügen,

$t_{Flug,2}$ =Flugzeit der eingebundenen Drohne zurück zum Ausgangspunkt und

t_{Ad-Hoc} = Zeit für die Bildung eines Ad-Hoc Netzwerks.

Die Herleitung zur Bestimmung der Flugzeit einer Drohne zu dem Entdeckerzug ist in Anhang 3 zu finden. Demnach beträgt die Flugzeit einer Drohne zu dem Entdeckerzug im Funkloch – unter der Annahme, dass die Entfernung über die Luftlinie 10 km und die Luftgeschwindigkeit der Drohne 50 km/h beträgt – **12,19 min**. Da davon auszugehen ist, dass eine Drohne durch das TMS automatisiert initialisiert wird und die Vorbereitung und Übermittlung einer Fahrterlaubnis nach *Zimmermann und*

Hommel (2003) in der Regel 12 s dauert, kann für die verbindungspezifischen Zeitanteile $t_{init,Drohne}$ und t_{Ad-Hoc} aus der Formel 8.4.1 vereinfacht $\leq$ **1 min** angesetzt werden. Aus der Formel 8.4.1 ist ersichtlich, dass die Flugzeit der Drohne im Vergleich zu den verbindungsspezifischen Zeitanteilen dominiert.

Das resultierende Betriebsrisiko des Ad-Hoc Netzwerks zur alternativen Übermittlung von Fahrterlaubnissen mit einer Drohne pro Entdeckerzug beträgt dann bei einmaliger Anwendung dieser betrieblich-technischen Rückfallebene nach der Formel 7.5.9

$$\boldsymbol{BR_{Ad-Hoc,Drohne} = 1 * \frac{10^{-5}}{h} * \left(\frac{1}{60\frac{min}{h}}\right) * (2 * 12,19\ \text{min} + 1\ \text{min}) * 0,1\ Opfer = 4,23 * 10^{-7}\ Opfer}$$

Verursachte außerplanmäßige Wartezeiten bei der alternativen Übermittlung von Fahrterlaubnissen mit einer Drohne

Wie bereits in Unterkapitel 2.4.2 erwähnt, kommt ein Zug aufgrund einer Kommunikationsstörung nach 40 s zum Stillstand und wird dadurch zu einem Entdeckerzug. Entsprechend des Unterkapitels 6.6.1 aktiviert das TMS eine Drohne, um die Fahrterlaubnis für den Entdeckerzug zu übermitteln. Da der Entdeckerzug so lange wartet, bis die Drohne angekommen ist und die Fahrterlaubnis über das Ad-Hoc Netzwerk übermittelt, erleidet der Entdeckerzug eine Abweichung von der planmäßigen Beförderungszeit. Diese Abweichung von der planmäßigen Beförderungszeit wirkt sich in Abhängigkeit der Zugfolgefälle auf die nachfolgenden Züge unterschiedlich aus.

Die Überschreitung der planmäßigen Beförderungszeit des Entdeckerzuges ergibt sich aus der Differenz zwischen der tatsächlichen Beförderungszeit und der planmäßigen Beförderungszeit und kann vereinfacht mit

$$t_{Wa,Z1} = t_{Bef,ist} - t_{Bef,plan} \qquad 8.4.2$$

abgeschätzt werden.

$t_{Wa,Z1}$ = außerplanmäßige Wartezeit des Entdeckerzuges,

$t_{Bef,ist}$ = tatsächliche Beförderungszeit des Entdeckerzuges und

$t_{Bef,plan}$ = planmäßige Beförderungszeit des Entdeckerzuges

Die Beförderungszeit der Modellzüge aus dem Betriebsprogramm ist in Anhang 2 in der Tabelle 8 zu finden. Die Beförderungszeit des Entdeckerzuges (Güterzugs) in dem Betrachtungsraum beträgt nach Anhang 2 Tabelle 8 **14,35 min.** Die resultierende außerplanmäßige Wartezeit des Entdeckerzuges beträgt dann

$$\boldsymbol{t_{Wa,Z1} = (14,35\ min + 12,19\ min) - 14,35\ min = 12,19\ min.}$$

Im Falle der außerplanmäßigen Wartezeit des Entdeckerzuges ist nach *Schwanhäußer (1974)* das Betriebsgeschehen in dem Betrachtungsraum derart gestört, dass die nachfolgenden Züge nach dem First-Come-First-Serve Prinzip abgewickelt werden und es dadurch nicht zu einem Reihenfolgenwechsel

kommt. Die Folgeverspätung der nachfolgenden Züge aufgrund der Störungssituation kann nach *Schwanhäußer (1974)* in Abhängigkeit der zeitlichen Lage zueinander bestimmt werden. Unter der Annahme, dass zwei Züge (Entdeckerzug und der nachfolgende Zug) konfliktfrei in planmäßiger Reihenfolge hintereinanderliegen, ergibt sich die Folgeverspätung für den nachfolgenden Zug:

$$t_{VF,ij} = \left(t_{Vei} + t_{Wa,Z1}\right) - \left(t_{Pij} + t_{Vej}\right) \qquad 8.4.3$$

$t_{VF,ij}$ = Folgeverspätung des nachfolgenden Zuges aufgrund der außerplanmäßigen Wartezeit des Entdeckerzuges,

$t_{Wa,Z1}$ = außerplanmäßige Wartezeit des Entdeckerzuges,

t_{Pij} = Pufferzeit zwischen zwei Zügen,

t_{Vei} = Einbruchsverspätung des Entdeckerzuges,

t_{Vej} = Einbruchsverspätung der nachfolgenden Züge.

Unter der Annahme, dass in dem Betriebsprogramm die mittlere Zugfolge-Pufferzeit entsprechend der Ril 405.0103A02 (Tabelle 6) **1 min** beträgt und die nachfolgenden Züge im Mittel eine Einbruchsverspätung von **11,2 min**[2] aufweisen, beträgt die Folgeverspätung des nachfolgenden Zuges

$$\boldsymbol{t_{VF,2} = (11,2\ \text{min} + 12,19\ min) - (1\ min + 11,2\ min) = 11,19\ min.}$$

Es kann sein, dass der zweite Zug (dem Entdeckerzug nachfolgende Zug) diese Folgeverspätung auch auf weitere Züge überträgt. Um das zu prüfen, wird die Anzahl der von der Störungssituation betroffenen Züge $n_{betroffen}$ ermittelt. Diese beträgt

$$\boldsymbol{n_{betroffen} = \frac{t_{Vei} + t_{Wa,Z1}}{(t_{Pij} + t_{Vej})} + 1 = \frac{11,2\ \text{min} + 12,19\ min}{(1\ min + 11,2\ min)} + 1 = 2,9\ \approx 2.}$$

Das bedeutet, dass mit dem Entdeckerzug nur noch ein weiterer Zug eine Folgeverspätung erleidet. Das liegt daran, dass die Verspätungsübertragung durch die zwischen den einzelnen Modellzügen angeordnete Zugfolge-Pufferzeiten und den mittleren Einbruchsverspätungen der nachfolgenden Züge gedämpft wird. Die Summe der von den betroffenen Zügen erzeugten außerplanmäßigen Wartezeiten beträgt dann:

$$\boldsymbol{\sum t_{Wa} = (11,2\ \text{min} + 12,19\ min) + 11,19\ min = 34,58\ min}$$

[2] Die mittlere Einbruchsverspätung der verspäteten Züge wurde in Anlehnung an **405.0204A03** Tabelle 2 in Anhang 2 ermittelt

8.4.3 Quantifizierung der Kenngrößen eines Ad-Hoc Netzwerks mit einem Object-Controller

Betriebsrisiko des Ad-Hoc Netzwerks zur alternativen Übermittlung von Fahrterlaubnissen über einen Object-Controller

Da entsprechend des Netzelements freie Strecke keine Weichen bis zur nächsten Betriebsstelle vorhanden sind, ist für ein Ad-Hoc Netzwerk zwischen Zug und Object Controller – wie in Unterkapitel 6.6.3 beschrieben – eine Zwischenfahrt der Entdeckerzüge bis zum Erreichen des Erkundungsraums für ein Ad-Hoc Netzwerk erforderlich. Da die betroffenen Züge in diesem Fall ohne Fahrterlaubnis fahren würden, besteht das Betriebsrisiko darin, eine Kollision (z.B. mit einem vorausfahrenden Zug) zu verursachen.

Analog zum vorigen Unterkapitel wird das Betriebsrisiko der alternativen Übermittlung von Fahrterlaubnissen über einen Object-Controller wie folgt ermittelt:

Die geänderte Gefährdungsrate für eine Zwischenfahrt der betroffenen Züge zum Aufbau eines Ad-Hoc Netzwerks mit einem Object-Controller kann wie folgt abgeschätzt werden. Da die Fahrt ohne Fahrterlaubnis erfolgt, wechselt die ETCS-OBU in die Betriebsart Staff-Responsible (SR). Damit wird die Verantwortung für die Geschwindigkeitsüberwachung an das kognitive Systemelement übertragen. Zur Durchführung einer Zwischenfahrt ist ebenfalls die Lichtraumüberwachung erforderlich. Eine Kollision kann daher entstehen, wenn entweder die Geschwindigkeitsregelung- und überwachung (rechtzeitiges Abbremsen) oder die Lichtraumüberwachung nicht verfügbar sind. Demnach liegt in einem Fehlerbaum zur Laufzeit eine logische ODER-Verknüpfung für das Top-Ereignis Kollision. Unter der Annahme, dass das fahrzeugseitige ATO-System mindestens einen SIL von 2 aufweist, hat die Gefährdungsrate der Geschwindigkeitsregelung- und Überwachung einen Wertebereich von $\boldsymbol{\lambda_{ATO} = 1 * 10^{-6} - 1 * 10^{-7}/h.}$ Für die Gefährdungsrate der Lichtraumüberwachung kann der Wert aus *Braband et al. (2022)* angenommen werden. In *ebd.* wurde für die Gefährdungsrate der Lichtraumüberwachung beim Fahren auf Sicht $\boldsymbol{\lambda_{Sensor,OS} = 3 * 10^{-7}}$ ermittelt.

Die resultierende Gefährdungsrate für eine mögliche Kollision aufgrund der Zwischenfahrt ergibt sich dann je Zug zu:

$$\lambda_{Zfahrt} = \lambda_{ATO} + \lambda_{Sensor,OS} - \left(\lambda_{ATO} * \lambda_{Sensor,OS}\right) \qquad 8.4.2$$

$$\boldsymbol{\lambda_{Zfahrt} = 1 * 10^{-6} + 3 * 10^{-7} - \left(1 * 10^{-6} * 3 * 10^{-7}\right) = 1,3 * 10^{-6}/h}$$

Im Vergleich zu dem Schadensausmaß, das aufgrund eines Drohnenabsturzes entsteht, wird nach *VDE V 0831-103:2020 (2020)* eine Kollision beim Fahren auf Sicht (ca. 40 km/h) in die Unfallklasse E eingeordnet. Demnach kann das Schadensausmaß bei einer Kollision zwischen zwei Zügen $\boldsymbol{S_{Zfahrt} = 0,3 - 1\ Opfer}$ angesetzt werden.

Schließlich ist auch die Dauer zur Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einem Object-Controller erforderlich. Im Vergleich zu der Dauer zur Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einer Drohne, kann die Dauer der Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einem Object-Controller mit der Dauer der Zwischenfahrt der Züge zum Erkundungsraum abgeschätzt werden. Die Dauer der Zwischenfahrt hängt primär von der Distanz zum Erkundungsraum und von der Geschwindigkeit (Fahren auf Sicht 40 km/h) ab und kann unter

Vernachlässigung der detaillierten Fahrdynamik der betroffenen Züge vereinfacht mit der Zeit für Beschleunigungs- Beharrungs- und Bremsphase abgeschätzt werden.

$$t_{RFE,ZFahrt} = t_{Beschleunigen} + t_{Beharren} + t_{Bremsen} + t_{Ad-Hoc} \qquad 8.4.3$$

$t_{RFE,ZFahrt}$ = Dauer zur Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einem Object-Controller

$t_{Beschleunigen}$ = Dauer für eine Beschleunigung von 0 km/h auf 40 km/h,

$t_{Beharren}$ = Dauer der Beharrungsfahrt mit 40 km/h zum Object-Controller,

$t_{Bremsen}$ = Dauer der Bremsung von 40 km/h auf 0 km/h zum Aufbau eines Ad-Hoc Netzwerks und

t_{Ad-Hoc} = Zeit für die Bildung eines Ad-Hoc Netzwerks.

Anders als bei einer drohnenbasierten Übermittlung der Fahrterlaubnisse wartet der Entdeckerzug bei einem Ad-Hoc Netzwerk mit einem Object-Controller nicht, sondern führt einer Zwischenfahrt durch, um den Erkundungsraum zu erreichen. Die Dauer einer Zwischenfahrt hängt von der Geschwindigkeit des Entdeckerzuges und von der Entfernung zum Erkundungsraum ab. Unter der Annahme, dass der Entdeckerzug entsprechend der Abbildung 47 auf der Seite 172 etwa bei der Hälfte der freien Strecke zum Stillstand gekommen ist und sich 5 min lang im Funkloch aufhält, wird er entsprechend des Unterkapitels 2.4.2 aus dem ETCS-Speicher gelöscht. In diesem Fall muss der Entdeckerzug bis zum nächsten Object-Controller eine Zwischenfahrt durchführen. Die Entfernung zum nächsten Object-Controller beträgt unter den getroffenen Annahmen 10 km.

Die Dauer der Beschleunigung von 0 km/h auf 40 km/h beträgt – bei einer nach *(Hansen und Pachl 2014, S. 74)* angenommenen Anfahrbeschleunigung des Entdeckerzugs (Güterzug) von $a_{b,Gz} = 0{,}2\ m/s^2$– vereinfacht:

$$\boldsymbol{t_{Beschleunigen} = \frac{40\frac{km}{h}}{3{,}6} = 55{,}5\ s.}$$

Dabei wird eine Strecke von etwa **308 m** zurückgelegt. Für eine Bremsverzögerung eines Güterzugs kann nach *(Hansen und Pachl 2014, S. 74)* $a_{br,Gz} = 0{,}3\ m/s^2$ (Bremsart G) angenommen werden. Damit beträgt der Bremsweg etwa **206 m**. Das hat zur Folge, dass der Entdeckerzug etwa **9486 m (9,49 km)** in Beharrungszustand sein wird. Die Dauer der Beharrungsfahrt beträgt dann

$$\boldsymbol{t_{Beharren} = \frac{9486\ \mathrm{m}}{\frac{40\frac{km}{h}}{3{,}6}} = 853{,}74\ s.}$$

Die Dauer der Bremsung beträgt

$$t_{Bremsung} = \frac{40\frac{km}{h}}{\frac{3,6}{0,3\ m/s^2}} = 37,04\ s.$$

Die gesamte Dauer zur Übermittlung von Fahrterlaubnissen über ein Ad-Hoc Netzwerk mit einem Object-Controller nach einer Zwischenfahrt von 10 km beträgt – unter Verwendung von $\leq$ **1 min** für den verbindungspezifischen Zeitanteil t_{Ad-Hoc} – schließlich

$$t_{RFE,ZFahrt} = 55,5\ s + 853,74\ s + 37,04\ s + 60\ s = 1006,38\ s\ (16,77\ \text{min}).$$

Das resultierende Betriebsrisiko des Ad-Hoc Netzwerks zur alternativen Übermittlung von Fahrterlaubnissen mit einem Object-Controller und einer Zwischenfahrt beträgt dann bei einmaliger Anwendung dieser betrieblich-technischen Rückfallebene nach der Formel 7.5.9

$$BR_{Ad-Hoc,OC} = 1,3 * \frac{10^{-6}}{h} * \left(\frac{1}{60\frac{min}{h}}\right) * (16,77\ \text{min}) * 1\ Opfer = 3,6 * 10^{-7}\ \ Opfer.$$

Verursachte außerplanmäßige Wartezeiten bei der alternativen Übermittlung von Fahrterlaubnissen mit einem Object-Controller

Im Vergleich zu der vorigen betrieblich-technischen Rückfallebene, bei der ein Entdeckerzug so lange wartet, bis die Drohne angekommen ist, führt der Entdeckerzug zur alternativen Übermittlung von Fahrterlaubnissen über einen Object-Controller eine Zwischenfahrt durch. Die Dauer der Zwischenfahrt wurde bereits im vorigen Abschnitt ermittelt.

Da der Entdeckerzug bis zur Hälfte der Strecke mit der Geschwindigkeit aus dem Regelbetrieb gefahren ist, ergibt sich die tatsächliche Beförderungszeit aus der Summe der Beförderungszeit bis zur Hälfte der Strecke und der Dauer der Zwischenfahrt bis zum Object-Controller. Die daraus resultierende außerplanmäßige Fahrzeit kann wie folgt ermittelt werden:

$$t_{Wa,Z1} = \left(\frac{14,35\ min}{2} + 16,77\ min\right) - 14,35\ min = 9,6\ min.$$

Unter den gleichen Annahmen wie aus dem Unterkapitel 8.4.2 ergibt sich die Folgeverspätung für den nachfolgenden Zug:

$$t_{VF,2} = t_{VF,2} = (11,2\ \text{min} + 9,6\ min) - (1\ min + 11,2\ min) = 8,6\ min.$$

Auch bei der Anwendung dieser betrieblich-technischen Rückfallebene wird die Anzahl der von der Störungssituation betroffenen Züge $n_{betroffen}$ ermittelt. Diese beträgt ebenfalls

$$n_{betroffen} = \frac{t_{Vei} + t_{Wa,Z1}}{(t_{Pij} + t_{Vej})} + 1 = \frac{11,2 + 9,6\ min}{(1\ min + 11,2\ min)} + 1 = 2,7\ \approx 2.$$

Das bedeutet, dass auch bei der Anwendung dieser betrieblich-technischen Rückfallebene mit dem Entdeckerzug nur noch ein weiterer Zug eine Folgeverspätung erleidet. Die Summe der von den betroffenen Zügen erzeugten außerplanmäßigen Wartezeiten beträgt dann:

$$\sum \boldsymbol{t_{Wa}} = (\mathbf{11,2} + \mathbf{9,6}\ \boldsymbol{min}) + \mathbf{8,6}\ \boldsymbol{min} = \mathbf{29,4}\ \boldsymbol{min}.$$

Anhand der Ergebnisse aus den Unterkapiteln 8.4.2 und 8.4.3 erfolgt im nächsten Kapitel der Vergleich der Systemeffektivität der beiden Ad-Hoc-Netzwerke zur Übermittlung von Fahrterlaubnissen im Falle einer Kommunikationsstörung.

8.5 Systemeffektivität der beiden Ad-Hoc-Netzwerke zur Übermittlung von Fahrterlaubnissen im Falle einer Kommunikationsstörung

Nachdem nun das Betriebsrisiko und die verursachten außerplanmäßigen Wartezeiten der beiden möglichen Ad-Hoc Netzwerke mit einer Drohne und mit einem Object-Controller zur Übermittlung von Fahrterlaubnissen in den vorigen Unterkapiteln bestimmt wurden, soll schließlich ein Vergleich der Systemeffektivität der beiden Ad-Hoc Netzwerke durchgeführt werden.

Zur Bewertung der Systemeffektivität ist zunächst der Risikogrenzwert des Betrachtungsraums im Anwendungsbeispiel erforderlich. In Anlehnung an *Huang (2020)* entspricht eine freie Strecke mit einer Länge von 20 km etwa 0,03 % der gesamten Gleislänge des öffentlichen Schienennetzes nach *Destatis (2021)* von 61.300 km. Da der Risikogrenzwert für den Streckenstandard M160 nach *Huang (2020, S.57)* **14,37 Opfer/Kalenderjahr** beträgt, ergibt sich für den Risikogrenzwert $\boldsymbol{RG_{fS}}$ der im Anwendungsbeispiel betrachteten freien Strecke

$$\boldsymbol{RG_{fS}} = \mathbf{0,03}\ \% * \mathbf{14,37}\,\frac{\boldsymbol{Opfer}}{\boldsymbol{Kalenderjahr}} = \mathbf{4,7} * \mathbf{10^{-3}}\,\frac{\boldsymbol{Opfer}}{\boldsymbol{Kalenderjahr}}.$$

Der Vergleich der beiden betrieblich-technischen Rückfallebenen hinsichtlich des verbrauchten Risikobudgets, das in einem Kalenderjahr auf dieser Strecke zur Verfügung steht, ist in der Abbildung 48 dargestellt.

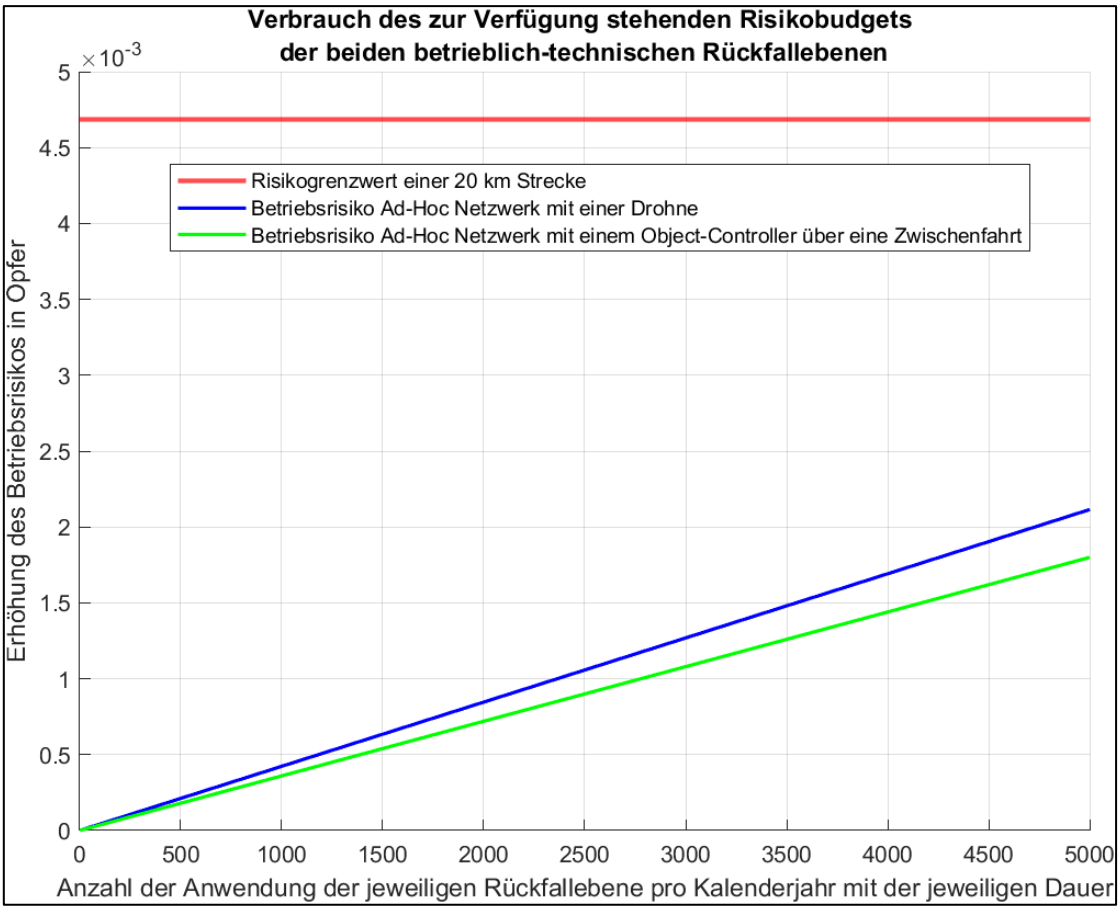

Abbildung 48 Darstellung des verbrauchten Risikobudgets durch die beiden betrieblich-technischen Rückfallebenen

Bei einer Anwendung der betrieblich-technischen Rückfallebene mit einer Drohne von **5000** Mal pro Kalenderjahr und der Dauer aus der Formel 8.4.1 wird etwa **44,5 %** des Risikogrenzwerts bei einer Gefährdungsrate von $\boldsymbol{\lambda_{Drohne} = 1 * 10^{-6}/h}$ verbraucht. Das Ad-Hoc Netzwerk mit einem Object-Controller mit einer Zwischenfahrt zuvor verbraucht bei einer Anwendung von **5000 M**al pro Kalenderjahr und der Dauer aus der Formel 8.4.3 etwa **38,3 %** des Risikogrenzwerts bei einer Gefährdungsrate von $\boldsymbol{\lambda_{Zfahrt} = 1.3 * 10^{-6}/h}$.

Prinzipiell wird mit beiden betrieblich-technischen Rückfallebenen im Falle einer infrastrukturseitigen Kommunikationsstörung das zur Verfügung stehende Betriebsrisiko-Budget pro Kalenderjahr nicht vollständig verbraucht. Es ist hervorzuheben, dass das Betriebsrisiko für eine einzelne Drohne oder bei einer Zwischenfahrt für einen einzelnen Zug gilt. Sofern mehrere Drohnen für ein Ad-Hoc Netzwerk aktiviert werden oder mehrere Züge gleichzeitig eine Zwischenfahrt durchführen müssen, erhöht sich das Betriebsrisiko ebenfalls.

Um das Betriebsrisiko eines drohnenbasierten Ad-Hoc-Netzwerks zu reduzieren, kann entweder die Geschwindigkeit der Drohnen oder die Dichte der Drohnen auf dem Bahnnetz (d.h. mehr Drohnen / Fläche bzw. Entfernung) erhöht werden. Letztere Maßnahme erhöht auch die Lebenszykluskosten.

Der Vergleich der Systemeffektivität der beiden betrieblich-technischen Rückfallebenen in dem Anwendungsbeispiel erfolgt anhand der Grafik in der Abbildung 49, bei der die Lebenszykluskosten für die erforderlichen Ressourcen der beiden betrieblich-technischen – wie bereits in Unterkapitel 7.5.3 erwähnt – prozentual abgeschätzt werden.

Bei dem Vergleich der Systemeffektivität der beiden betrieblich-technischen Rückfallebenen beträgt der Risikoindex des Ad-Hoc Netzwerkes mit einer Drohne **44,5 %** und der Risikoindex des Ad-Hoc

Netzwerkes mit einem Object Controller **38,3 %.** Capability ist in beiden betrieblich-technischen Rückfallebenen entsprechend der Ergebnisse aus den Unterkapiteln 8.4.2 und 8.4.3 **C = 1**.

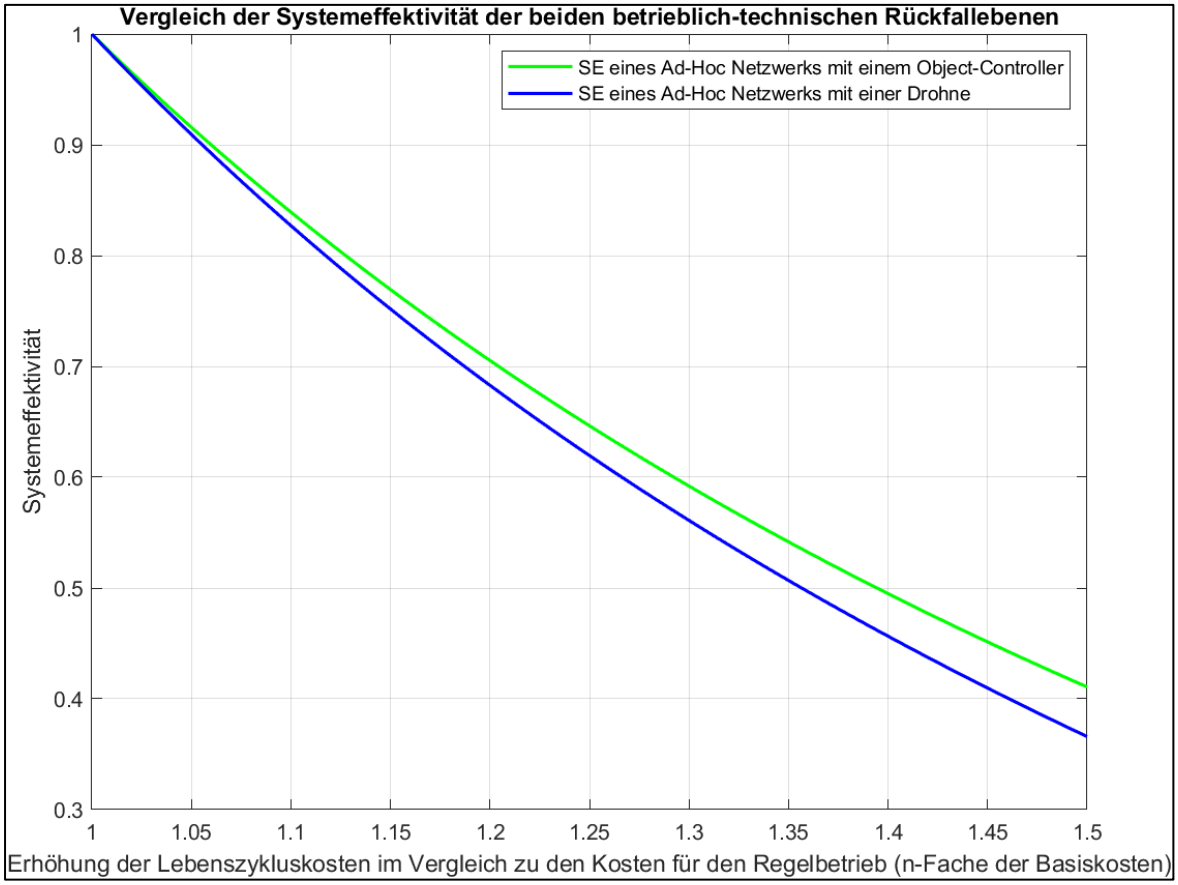

Abbildung 49 Verlauf der Systemeffektivität in Abhängigkeit der steigenden Lebenszykluskosten der beiden betrieblich-technischen Rückfallebenen. **Risikoindex** des Ad-Hoc Netzwerkes mit einer Drohne **44,5** % und des Ad-Hoc Netzwerkes mit einem Object Controller **38,3** %. Capability der beiden betrieblich-technischen Rückfallebenen = 1.

Aus der Abbildung 49 ist ersichtlich, dass die Systemeffektivität des Ad-Hoc-Netzwerks mit einem Object-Controller bei einer Anwendung von 5000 Mal pro Kalenderjahr und der Dauer aus der Formel 8.4.3 höher ist als die Systemeffektivität des Ad-Hoc-Netzwerks mit einer Drohne. Im Vergleich zu den Drohnen, müssen bei der betrieblich-technischen Rückfallebene mit einem Object-Controller, die Object-Controller um die Softwareanwendung für ein Ad-Hoc Netzwerk ertüchtigt werden. Da die Object-Controller die Softwareanwendung für ein Ad-Hoc Netzwerk entsprechend des Unterkapitels 6.6.1 von der infrastrukturseitigen ATO-FMU erhalten, werden die Zusatzkosten für ein Ad-Hoc Netzwerk mit einem Object-Controller geringer sein als die für ein Ad-Hoc Netzwerk mit einer Drohne. Denn für ein Ad-Hoc Netzwerk mit einer Drohne sind sowohl Investitionen in die Softwareanwendung als auch in die Hardware (Drohne) zu tätigen.

Sofern jedoch die Zusatzkosten für die Drohnen weniger als 5 % der Kosten für die technischen Systeme des vollautomatisierten Bahnbetriebs betragen, können auch Drohnen als mögliche Ressourcen für betrieblich-technische Rückfallebenen migriert werden, da diese entsprechend der Abbildung 49 nahezu gleiche Systemeffektivität aufweisen wie bei einem Ad-Hoc-Netzwerk mit einem Object-Controller. Außerdem können Drohnen entsprechend des Unterkapitels 6.6.2 auch als Ressourcen im Falle von Störungen an fahrzeugseitigen Sensoren eingesetzt werden, wodurch die Lichtraumüberwachung nicht mehr erfüllt werden kann.

Schließlich ist es auch möglich, beide betrieblich-technische Rückfallebenen zu migrieren. Das kumulierte Betriebsrisiko in Abhängigkeit der Häufigkeit der Anwendung pro Kalenderjahr ergibt sich aus der Summe der Erhöhung des Betriebsrisikos je betrieblich-technische Rückfallebene.

8.6 Zusammenfassung des Hauptkapitels

In diesem Hauptkapitel wurde die Systemeffektivität von zwei betrieblich-technischen Rückfallebenen auf Basis der dynamischen Adaption zur Laufzeit anhand eines Anwendungsbeispiels bewertet. Dabei wurde das in Kapitel 7.5 hergeleitete Bewertungsverfahren für Systemeffektivität verwendet.

Bei dem Anwendungsbeispiel handelte es sich um eine infrastrukturseitige Kommunikationsstörung auf einer freien Strecke. Entsprechend des Unterkapitels 6.6.1 kann durch die dynamische Adaption entweder eine Drohne zur Übermittlung von Fahrterlaubnissen im Falle einer infrastrukturseitigen Kommunikationsstörung für ein Ad-Hoc Netzwerk eingebunden werden oder die Züge können über ein Ad-Hoc Netzwerk mit einem Object-Controller die Fahrterlaubnisse einfordern.

Aus dem exemplarischen Vergleich der beiden betrieblich-technischen Rückfallebenen im Falle einer Kommunikationsstörung können folgende Erkenntnisse zusammengefasst werden:

- Die Ressourcen mit niedrigerem Betriebsrisiko und bei gleicher Auswirkung auf die Betriebsqualität – unabhängig von den Lebenszykluskosten – effektiver sind.
- Bei der Bestimmung der Dauer der jeweiligen betrieblich-technischen Rückfallebenen wurde davon ausgegangen, dass die beiden Entdeckerzüge auf der Hälfte der Strecke zum Stehen gekommen sind und dass die Entfernung zu den Drohnen bzw. zu dem nächsten Object-Controller 10 km beträgt. Dieser Fall stellt das Maximum im Betrachtungsraum dar. Es kann aber auch vorkommen, dass die Drohnen ohne Flugzeit und die Entdeckerzüge ohne Zwischenfahrt ein Ad-Hoc-Netzwerk bilden. In hängt die Dauer der jeweiligen betrieblich-technischen Rückfallebenen nur von den verbindungsspezifischen Zeitanteilen ab, die in der Regel ≤ 1 min dauern. Dadurch reduziert sich nicht nur das verursachte Betriebsrisiko je betrieblich-technische Rückfallebene signifikant, sondern aufgrund der Zugfolge-Pufferzeiten zwischen zwei Zügen können dadurch auch Folgeverspätungen vermieden werden.
- Ein Ad-Hoc Netzwerk mit einem Object-Controller kann insgesamt länger dauern als ein Ad-Hoc Netzwerk mit einer Drohne, sofern mehrere Züge pro Richtung von der Kommunikationsstörung betroffen sind. Das liegt daran, dass eine Drohne mehrere Züge gleichzeitig mit den sicherheitsrelevanten und betriebsrelevanten Daten versorgen kann, während jeder Zug mit einem Object-Controller ein Ad-Hoc-Netzwerk bilden muss.
- Wenngleich der Vergleich der Systemeffektivität der beiden betrieblich-technischen Rückfallebenen mit einer manuellen Rückfallebene (Betriebspersonal) nicht explizit erfolgte, kann qualitativ festgehalten werden, dass durch die weitgehend automatisierte Reaktion auf Störungssituationen und durch Einbindung von technischen Systemen als Ressourcen die Sicherheit der Betriebsführung weniger beeinträchtigt werden kann als bei einer menschlichen Beteiligung.

Das in diesem Hauptkapitel vorgestellte Anwendungsbeispiel ist nur exemplarisch erstellt worden. Da die Dauer der jeweiligen betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption anhand der Formeln in den Unterkapiteln 8.4.2 und 8.4.3 bereits vor der Migration ermittelt werden kann, ist es möglich, die Auswirkung von verschiedenen betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb auf die Sicherheit und auf die Betriebsqualität anhand von Simulationen für komplexere Betriebsszenarien vor der Migration zu bestimmen.

Dazu eignet sich beispielsweise die Implementierung der ATO-FMU einschließlich der Datenbank für Services zur Einrichtung von möglichen betrieblich-technischen Rückfallebenen zur Laufzeit das Eisenbahnbetriebsfeld in Darmstadt (EBD). Das EBD ermöglicht komplexe Simulationen mit genauen Zeitvorgaben. Ebenfalls können konkrete Fahrpläne z.B. aus dem EBD zugrunde gelegt werden, um die Auswirkung der jeweiligen Adaptionsart auf die Betriebsqualität zu untersuchen.

9 Zusammenfassung der Arbeit und Ausblick

Wenngleich bereits Forschungsprojekte im Bahnsektor den vollautomatisierten Bahnbetrieb im Visier haben, gibt es noch keine Lösungen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb. In der vorliegenden Dissertation wurden daher betrieblich-technische Rückfallebenen für den Umgang mit Störungssituationen im vollautomatisierten Bahnbetrieb entwickelt und bewertet.

9.1 Zusammenfassung der Vorgehensweise

Auf dem Weg zum digitalen Bahnbetrieb gibt es bereits Bestrebungen, eine europaweit standardisierte Referenzarchitektur für den digitalen Bahnbetrieb zu entwickeln. In den Referenzarchitekturen der RCA und OCORA wurden zwar bereits technische Systeme für den vollautomatisierten Bahnbetrieb spezifiziert, jedoch hat das ATO-System darin die Granularität einer Black-Box und die logischen Beziehungen der technischen Systeme, anhand der eine Zugfahrt beschrieben werden kann, ist nicht vorhanden.

Da Gefährdungen im Bahnbetrieb während einer Zugfahrt auftreten können, war für eine systematische Gefährdungsanalyse zunächst die logische Beziehung der für den vollautomatisierten Bahnbetrieb definierten technischen Systeme zueinander erforderlich. Um zu eruieren, welche gefährliche Betriebssituationen aus den beiden ATO-Teilsystemen im vollautomatisierten Bahnbetrieb verursacht werden können, wurde daher nach einer Anforderungserhebung zunächst in **Hauptkapitel 4** diese logische Beziehung in Form einer funktionalen Systemarchitektur erarbeitet.

Auf Basis der erarbeiteten funktionalen Systemarchitektur wurde dann in **Hauptkapitel 5** eine Gefährdungsanalyse durchgeführt. Bei der Gefährdungsanalyse wurden mögliche Gefährdungsursachen aus den beiden ATO-Teilsystemen während einer Zugfahrt erarbeitet. Da nicht für jede Störungssituation eine betrieblich-technische Rückfallebene erforderlich ist und aus einer Gefährdungsanalyse sehr viele Gefährdungen resultieren können, wurde zunächst ein betrieblicher und umgebungsbedingter Kontext hergeleitet. Damit wurden nur jene Gefährdungsursachen weiter berücksichtigt, bei denen die Weiterfahrt eines Zuges verhindert sein kann oder eine im Vergleich zum Regelbetrieb unsicherere Weiterfahrt eines Zuges vorliegt.

Im Hauptteil der Dissertation **(Hauptkapitel 6)** bestand die Herausforderung darin, für die erarbeiteten gefährlichen Betriebssituationen geeignete betrieblich-technische Rückfallebenen zu entwickeln. Aus dem gegenwärtigen Bahnbetrieb ist bekannt, dass es keinen analytischen Ansatz bei der Entwicklung von betrieblich-technischen Rückfallebenen gibt, dem systematisch gefolgt werden kann.

Betrieblich-technische Rückfallebenen für den vollautomatisierten Bahnbetrieb aus Erfahrungen heraus erst nach unerwünschten Ereignissen zu entwickeln war den gestellten Anforderungen nicht gerecht, weshalb zunächst – unter Berücksichtigung der ständigen technologischen Entwicklungen und der modularen Systemarchitektur des digitalen Bahnbetriebs – ein systematischer Ansatz (dynamische Adaption) zur Entwicklung von betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb hergeleitet wurde. Auf Basis des systematischen Ansatzes wurden dann im selben Hauptkapitel für die zuvor erarbeiteten gefährlichen Betriebssituationen beispielhafte betrieblich-technische Rückfallebenen vorgestellt.

Da der vollautomatisierte Bahnbetrieb noch nicht migriert ist, und die betrieblich-technischen Rückfallebenen auf Basis der dynamischen Adaption Auswirkungen auf die Migration der physikalischen Systemarchitektur des digitalen Bahnbetriebs haben, wurde für eine Migrationsentscheidung in **Hauptkapitel 7** ein Bewertungsverfahren für eine Migrationsentscheidung und zur Auswahl einer betrieblich-technischen Rückfallebenen zur Laufzeit entwickelt.

Schließlich wurde eine beispielhafte betrieblich-technische Rückfallebene auf Basis der dynamischen Adaption anhand eines Anwendungsbeispiels in **Hauptkapitel 8** hinsichtlich der Auswirkung auf die Sicherheit und auf die Betriebsqualität bewertet.

9.2 Zusammenfassung der Ergebnisse und Erkenntnisse

Die funktionale Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt wurde auf einer Hierarchie-Ebene hergeleitet, die für die Durchführung einer Gefährdungsanalyse gemäß der STPA-Methode ausreichend ist. Die in **Hauptkapitel 4** mittels der STPA-Notation hergeleitete funktionale Systemarchitektur führte dazu, dass aus der Interaktion der einzelnen Systemelemente in der funktionalen Systemarchitektur insgesamt vier Regelkreise entstanden sind. Der erste Regelkreis ist der sogenannte ATO-Regelkreis. In dem ATO-Regelkreis sind TMS, ATO-AE, ATO-AT, das Kommunikationssystem, das perzeptuelle Systemelement, das kognitive Systemelement, das Aktor-Systemelement, die Sensoren, das Systemelement ATOM und das Systemelement RMTO enthalten. Der zweite Regelkreis ist die Untersetzung des ersten Regelkreises und stellt den fahrzeugseitigen ATO-Regelkreis dar. Darin sind das perzeptuelle Systemelement, das kognitive Systemelement, das Aktor-Systemelement und die Sensoren enthalten. Der dritte Regelkreis ist der ETCS-Regelkreis. Darin sind neben der Sicherungslogik, die ETCS-Zentrale, die ETCS-OBU, das Kommunikationssystem, Aktor-Systemelement und die Sensoren enthalten. Im vierten Regelkreis, dem fahrzeugseitigen ETCS-Regelkreis sind neben der ETCS-OBU das Aktor-Systemelement und die Sensoren enthalten.

Eine wesentliche Errungenschaft bei der Herleitung der funktionalen Systemarchitektur zur Beschreibung einer vollautomatisierten Zugfahrt anhand der STPA-Methode war, dass das potenzielle Systemverhalten und Gefährdungen in einem System durch die Analyse der Wechselwirkungen zwischen den darin enthaltenen Systemelementen erarbeitet werden können, anstatt das Systemverhalten in Ereignisketten zu zerlegen.

Bei der Gefährdungsanalyse in **Hauptkapitel 5** hat sich herausgestellt, dass Gefährdungsursachen aus den beiden ATO-Regelkreisen entweder eine Weiterfahrt oder eine im Vergleich zum Regelbetrieb sicherere Weiterfahrt verhindern können. Beim Letzteren können die beiden Schutzziele der LST Kollisionsvermeidung oder Entgleisungsvermeidung verletzt werden.

Eine wesentliche Erkenntnis aus der Gefährdungsanalyse ist, dass die Kommunikationsverbindung zwischen einem Zug und dem TMS oder der ETCS-Zentrale aufgrund der zentralen Betriebsführung für eine sichere Zugfahrt unabdingbar ist. Sofern die Kommunikationsverbindung unterbrochen wird, können weder sicherheitsrelevante noch betriebsrelevante Daten übertragen werden. Von einer Kommunikationsstörung können mehrere Züge gleichzeitig betroffen sein. Da bei fehlender Kommunikationsverbindung die zentrale Betriebsführung vorübergehend unterbrochen wird, kann auch die in der Literatur vorgeschlagene und bereits in Kapitel 2.4 erläuterte Fernsteuerung aus der Betriebszentrale nicht durchgeführt werden.

Eine weitere Erkenntnis aus der Gefährdungsanalyse ist, dass fahrzeugseitige Sensoren – insbesondere für Ortung und Lichtraumüberwachung – kritische technische Systeme im vollautomatisierten Bahnbetrieb darstellen. Im Gegensatz zu traditionellen Softwareanwendungen (mit deterministisches Verhalten) unterliegt das perzeptuelle Systemelement bei der Objekterkennung und Objektklassifizierung stochastischen Unsicherheiten. Daher kann eine vollautomatisierte Zugfahrt entweder aufgrund von Randfällen (Edge-Cases) oder durch Manipulation von außen – wie z.B. durch Adversarial Attacks – beeinträchtigt werden. Unsicherheiten im perzeptuellen Systemelement zur Laufzeit können dann im vollautomatisierten Bahnbetrieb eine Weiterfahrt oder eine im Vergleich zum

Regelbetrieb sicherere Weiterfahrt verhindern. Auch im Falle von Störungen an Sensoren ist eine Fernsteuerung aus der Betriebszentrale nicht möglich.

Die wesentlichen Erkenntnisse aus dem **6. Hauptkapitel** resultieren aus dem entwickelten systematischen Ansatz zur Einrichtung von betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb. Der entwickelte systematische Ansatz sieht eine dynamische Adaption der Systemarchitektur zur Laufzeit vor.

Da im vollautomatisierten Bahnbetrieb Störungen sowohl aus Softwareanwendungen als auch aus Hardwaresystemen verursacht werden können, sind zwei wesentliche Adaptionsarten möglich. Demnach ist es möglich, dass Systemelemente entweder zur Laufzeit ersetzt oder deaktiviert werden können. Bei der Deaktivierung ist eine reine Deaktivierung ohne Funktionsallokation oder mit Funktionsallokation möglich. Beim letzteren wird die betriebliche Funktion des deaktivierten Systemelements auf eine andere Ressource übertragen. Dabei können entweder auf Ressourcen technischer Art oder auf menschliche Ressourcen (z.B. Train-Operator oder Zugpersonal) zurückgegriffen werden. Das Ersetzen eines Systemelements zur Laufzeit ist aufgrund der Anforderung, dass die betrieblich-technischen Rückfallebenen möglichst kurz dauern sollen, nur bei Softwareanwendungen sinnvoll.

Unter der Annahme, dass der vollautomatisierte Bahnbetrieb im Regelbetrieb ausschließlich mit technischen Systemen durchgeführt wird und daher im Falle einer Störungssituation nicht sofort auf manuelle Prozesse zurückfällt, sondern möglichst automatisiert koordiniert und durchgeführt werden kann, wurde im Rahmen dieser Arbeit eine sogenannte ATO Fallback-Management-Unit (ATO-FMU) eingeführt. Die ATO-FMU stellt eine Art Middleware dar und ist sowohl infrastrukturseitig als auch fahrzeugseitig vorhanden. Die ATO-FMU kann unabhängig von den für den Regelbetrieb erforderlichen Systemelementen auf einer sicheren Ebene fungieren und unabhängig von den anderen Systemelementen entwickelt, verändert und bei Bedarf erweitert werden.

Die ATO-FMU umfasst ein Modul zur Störungserkennung, eine Wissensbasis, um die vorliegende Störungssituation dem entsprechenden Schutzziel zuordnen und daraufhin eine geeignete Adaptionsart auswählen zu können und schließlich auch noch die eigentliche Durchführung der dynamischen Adaption, um eine situationsabhängige betrieblich-technische Rückfallebene einzurichten. Dabei werden die entsprechenden Systemelemente in der Systemarchitektur für die Einrichtung einer betrieblich-technischen Rückfallebene koordiniert.

Zur Bewertung der möglichen dynamischen Adaptionsarten hinsichtlich der Auswirkung auf die Sicherheit und auf die Betriebsqualität wurde in **Hauptkapitel 7** ein Bewertungsverfahren für die Auswahl einer betrieblich-technischen Rückfallebene zur Laufzeit und für eine Migrationsentscheidung entwickelt.

Mit dem Bewertungsverfahren kann vor der Migration die Systemeffektivität einer betrieblich-technischen Rückfallebene auf Basis einer dynamischen Adaption bewertet werden. Die Systemeffektivität berücksichtigt die Auswirkung der möglichen dynamischen Adaptionsarten auf die Sicherheit und auf die Betriebsqualität gleichzeitig und setzt diese Auswirkung in das Verhältnis zu den Lebenszykluskosten, die für die ATO-FMU einschließlich der Ressourcen erforderlich sind.

Außerdem kann das Bewertungsverfahren bei dem Bewertungsschritt entsprechend des Ablaufdiagramms in der Abbildung 30 auf der Seite 112 zur Laufzeit herangezogen werden. Die

Auswahl einer betrieblich-technischen Rückfallebene zur Laufzeit erfolgt dann durch eine sequenzielle Bewertung hinsichtlich des Betriebsrisikos und der Auswirkung auf die Betriebsqualität.

Die Systemeffektivität einer betrieblich-technischen Rückfallebene hinsichtlich der Sicherheit der Betriebsführung ist hoch, je kleiner der Risikoindex ist. Beeinflussen lässt sich der Risikoindex dadurch, dass entweder die Anzahl der Störungen an den technischen Systemen durch technische Redundanzen reduziert wird, oder dadurch, dass das Betriebsrisiko in der jeweiligen betrieblich-technischen Rückfallebene möglichst niedrig gehalten wird. Letzteres kann durch den Einsatz von Ressourcen mit niedriger Gefährdungsrate oder durch kurze Dauer der Betriebsführung in der betrieblich-technischen Rückfallebene erreicht werden.

Die Anwendung des Bewertungsverfahrens in **Hauptkapitel 8** anhand eines Anwendungsbeispiels hat gezeigt, dass der wesentliche Vorteil der dynamischen Adaption zur Laufzeit gegenüber den gegenwärtigen betrieblich-technischen Rückfallebenen darin liegt, dass sie weitgehend automatisiert ablaufen und dabei mehrere von einer Störung betroffenen Züge gleichzeitig bedient werden können. Beispielsweise können mit einer Drohne aus dem Unterkapitel 6.6.3 im Falle einer Kommunikationsstörung mehrere Züge gleichzeitig mit den relevanten Fahrterlaubnissen versorgt werden. Es ist auch möglich, dass das Ersetzen einer gestörten Softwareanwendung bei mehreren Zügen gleichzeitig erfolgen kann.

Hinsichtlich der Auswirkung auf die Sicherheit kann schlussgefolgert werden, dass die Einbindung von technischen Systemen, deren Gefährdungsrate niedriger ist als die eines Betriebspersonals, als Ressource einen wesentlichen Vorteil gegenüber den gegenwärtigen betrieblich-technischen Rückfallebenen darstellt. Hinsichtlich der Auswirkung auf die Betriebsqualität spielt die Entfernung der einzubindenden Ressourcen zum gestörten Zug eine wesentliche Rolle. Beispielsweise dauert ein Ad-Hoc Netzwerk mit einem Object-Controller insgesamt länger als ein Ad-Hoc Netzwerk mit einer Drohne, sofern mehrere Züge von der Kommunikationsstörung betroffen sind. Das liegt daran, dass eine Drohne mehrere Züge gleichzeitig mit den sicherheitsrelevanten und betriebsrelevanten Daten versorgen kann, während jeder Zug mit einem Object-Controller ein Ad-Hoc-Netzwerk bilden muss. Zusammengefasst kann festgehalten werden, dass die Systemeffektivität einer betrieblich-technischen Rückfallebene mit niedrigerem Betriebsrisiko und bei gleicher Auswirkung auf die Betriebsqualität – unabhängig von den Lebenszykluskosten – effektiver sind.

Im Weiteren wird auch die Erfüllung der zur Lösung der Aufgabenstellung zusammengestellten Anforderungen zusammenfassend geprüft. Die Anforderungen an die Lösung der Aufgabenstellung wurden von verschiedenen Stakeholdern zusammengestellt und in Anforderungen an die Struktur der Systemarchitektur und Anforderungen an das Systemverhalten in Störungssituationen strukturiert. Um die Vollständigkeit der zusammengestellten Anforderungen möglichst gewährleisten zu können, wurden die Anforderungen mit sogenannten Leitlinien zur Gestaltung von Systemarchitekturen, die sich aus jahrelanger Erfahrung von Experten aus unterschiedlichen Domänen akkumuliert haben und mit Grundsätzen einer guten Prozessgestaltung bottom-up geprüft. In Tabelle 5 erfolgt eine Zusammenstellung der Erfüllung der Anforderungen.

Tabelle 5 Erfüllung der Anforderungen an die Lösung der Aufgabenstellung

Anforderungen an:	Anforderungen	Erfüllt durch:
die Systemstruktur	**Technische Interoperabilität** der betrieblich-technischen Rückfallebenen für den vollautomatisierten Bahnbetrieb	Die entwickelte ATO-FMU kann in die Systemarchitektur der RCA und OCORA **als Middleware eingebettet** werden und fungiert daher mit den technischen Systemen aus der RCA und OCORA. Die technischen Systeme fokussieren sich auf die eigenen betrieblichen Funktionen, in Störungsfall erfolgt die **Koordination über die ATO-FMU**
	Komplexität der Systemarchitektur durch Verwendung von standardisierten Schnittstellen aus RCA und OCORA **minimieren**.	
	Modularität, Austauschbarkeit und **Plug & Play** der technischen Systeme im vollautomatisierten Bahnbetrieb	ATO-FMU kann **unabhängig** von den für den Regelbetrieb erforderlichen Systemelementen **entwickelt, verändert und bei Bedarf erweitert werden**. Das gleiche gilt auch für die anderen Systemelemente.
	Flexibilität der technischen Systeme im vollautomatisierten Bahnbetrieb aufgrund des ständigen Wandels der Technologie	Die ATO-FMU kommuniziert mit anderen Systemelementen über eine standardisierte Kommunikationsschnittstelle und kennt ihre **betrieblichen Funktionen und Fähigkeiten.**
	wirtschaftliche Gestaltung und Durchführung des vollautomatisierten Bahnbetriebs	Durch die **Datenbank für Services der ATO-FMU** müssen die Ressourcen – insbesondere Softwareanwendungen – nicht redundant ausgelegt werden
das Systemverhalten	**Betriebliche Interoperabilität** der betrieblich-technischen Rückfallebenen für den vollautomatisierten Bahnbetrieb	**Keine proprietäre betreiberspezifische Lösungen erforderlich, da die ATO-FMU in jede betreiberspezifische Systemarchitektur eingebettet werden kann** und dadurch betrieblich-technische Rückfallebenen einheitlich aus „einer Hand“ ermöglichen
	Betriebsführung nach dem Prinzip **„Sicherheit vor Pünktlichkeit vor Wirtschaftlichkeit“**	Systemeffektivität je betrieblich-technische Rückfallebene kann anhand des entwickelten Bewertungsverfahrens bewertet werden.
	Möglichst **allgemeingültige** betrieblich-technische Rückfallebenen	Durch den generischen Ablauf der dynamischen Adaption können durch Kenntnis der zu erfüllenden **Schutzziele**

	so wenig wie möglich und **nur so viel wie nötig** betrieblich-technische Rückfallebenen	und der **betrieblichen Funktionen einschließlich der Fähigkeiten** der technischen Systeme **allgemeingültige** betrieblich-technische Rückfallebenen eingerichtet werden
	Flexibilität der Betriebsprozesse für Störungssituationen im vollautomatisierten Bahnbetrieb	Eine vorübergehend neue Systemarchitekturkonfiguration situationsabhängig **durch automatisierte Anpassung der Systemarchitektur zur Laufzeit**

9.3 Nutzen der Dissertation und Ausblick

Die Dissertation bringt insbesondere Nutzen für die europaweit geplanten Forschungsaktivitäten, wie z.B. für das Europes-Rail.

In Europes-Rail ist geplant, die in RCA und OCORA entstandenen Referenzarchitekturen weiter zu detaillieren und darauf basierend Betriebskonzepte für den vollautomatisierten Bahnbetrieb zu entwickeln. Außerdem steht in dem europäischen Forschungsvorhaben ERJU die Entwicklung von Betriebskonzepten sowohl für den Regelbetrieb als auch für Störungssituationen im Fokus. Dazu kann sowohl die im Rahmen der Dissertation entwickelte funktionale Systemarchitektur als auch der systematische Ansatz zur Entwicklung von betrieblich-technischen Rückfallebenen verwendet werden. Um EU weit harmonisierte Betriebsverfahren zu haben, können auf Basis des systematischen Ansatzes (dynamische Adaption) verschiedene physikalische Systemarchitekturen auf ihre Systemeffektivität hin evaluiert werden.

Im Gegensatz zu den gegenwärtigen betrieblich-technischen Rückfallebenen, bei denen die Dauer der betrieblich-technischen Rückfallebenen aufgrund menschlicher Auslastung schwanken kann, erlaubt die dynamische Adaption aus dem Hauptkapitel 6 aufgrund der deterministischen Funktionsweise, die Dauer der jeweiligen betrieblich-technischen Rückfallebene auf Basis der dynamischen Adaption bereits vor der Migration zu ermitteln. Diese Tatsache stellt einen wesentlichen Nutzen hinsichtlich der Bestimmung der voraussichtlich tatsächlichen Beförderungszeit der von einer Störung betroffenen Züge im Betrieb dar. Dadurch ist es möglich, die im Rahmen dieser Dissertation entwickelten beispielhaften betrieblich-technischen Rückfallebenen für den vollautomatisierten Bahnbetrieb in virtuellen Umgebungen zu simulieren und mit dem Bewertungsverfahren aus dem 7. Hauptkapitel zu bewerten, bevor eine Migrationsentscheidung getroffen wird.

Entsprechend der inhaltlichen Eingrenzung aus dem Kapitel 3.5 konnten im Rahmen dieser Arbeit folgende Inhalte nicht behandelt werden, weshalb diesbezüglich noch Forschungsbedarf besteht.

Trotz der erarbeiteten funktionalen Systemarchitektur zur Beschreibung einer Zugfahrt im vollautomatisierten Bahnbetrieb konnten technologische Lösungen, d.h. die Zuordnung der in Hauptkapitel 4 erarbeiteten funktionalen Systemarchitektur auf konkrete Hard- und Software (physikalische Systemarchitektur) nicht behandelt.

Des Weiteren war die Untersuchung von geeigneten Algorithmen für die jeweiligen Systemelemente nicht Gegenstand dieser Arbeit. Daher müssen im nächsten Schritt insbesondere geeignete Algorithmen

für die jeweiligen Systemelemente eruiert werden. Auf Basis der Algorithmen kann die Gefährdungsanalyse gemäß der STPA-Methode auf der nächsten Detaillierungsebene erneut durchgeführt werden.

Bei der Migration der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme, d.h. bei der Umsetzung der physikalischen Systemarchitektur sind technische Redundanzen einzuplanen. Da technologische Lösungen noch nicht vollständig erforscht bzw. entwickelt sind, konnten im Rahmen dieser Arbeit auch keine technischen Redundanzen behandelt werden. Sofern Betreiber konkrete technologische Lösungen festlegen, können in Zukunft auch geeignete technische Redundanzen untersucht und mit dem Bewertungsverfahren aus dem 7. Hauptkapitel bewertet werden.

Des Weiteren ist auf Basis der funktionalen Systemarchitektur aus dem Hauptkapitel 4 eine Risikoanalyse gemäß EN 50126 durchzuführen, um das Risiko der im Rahmen des 5. Hauptkapitels erarbeiteten gefährlichen Betriebssituationen zu bewerten und die tolerierbaren Gefährdungsraten zuzuordnen.

Wenngleich mit der dynamischen Adaption der Systemarchitektur zur Laufzeit die wissenschaftliche Grundlage für eine systematische Bewältigung von Störungssituationen im vollautomatisierten Bahnbetrieb gelegt ist, bedarf es noch an weiterer Forschung hinsichtlich der Detailspezifikation der ATO-FMU. Außerdem ist die ATO-FMU in Zukunft einschließlich der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme – zumindest die Softwareanwendungen – prototypisch zu implementieren und zu testen.

Trotz der exemplarischen Bewertung der Systemeffektivität ausgewählter betrieblich-technischer Rückfallebenen bietet das Bewertungsverfahren die Möglichkeit, die Auswirkung von verschiedenen betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb auf die Sicherheit und auf die Betriebsqualität anhand von Simulationen für komplexere Betriebsszenarien vor der Migration zu bewerten. Simulationen ermöglichen – im Vergleich zu einer exemplarischen Rechnung im Rahmen dieser Arbeit (Hauptkapitel 8) – die genaue Bestimmung der Auswirkung von verschiedenen betrieblich-technischen Rückfallebenen im vollautomatisierten Bahnbetrieb auf die Betriebsqualität. Ebenfalls können konkrete Fahrpläne z.B. aus dem EBD zugrunde gelegt werden, um die Auswirkung der jeweiligen Adaptionsart auf die Betriebsqualität zu untersuchen.

Verzeichnisse

Literaturverzeichnis

(Aebersold und Schubert 2023)	Aebersold, Raphael; Schubert, Max (2023): FRMCS/5G – Wie die Migration effizient gelingen kann. In *Signal + Draht*, (115) Mai 2023, S. 38–46
(Ackermann 1998)	Ackermann, Till (1998): Die Bewertung der Pünktlichkeit als Qualitätsparameter im Schienenpersonenverkehr auf Basis der direkten Nutzenmessung. Stuttgart: Verkehrswiss. Inst. an der Univ (Forschungsarbeiten des Verkehrswissenschaftlichen Instituts an der Universität Stuttgart, Bericht 21).
(Adebahr et al. 2022)	Adebahr, Frederik-Alexander; Milius, Birgit; Naumann, Anja (2023): Flexible Arbeitsumgebungen für die ATO-Rückfallebene. In: Der Eisenbahningenieur 01/23, S. 39–41.
(Alcatel et al. 2005)	Alcatel; Alstom; Ansaldo Signal; Bombardier; Invensys Rail; Siemens (2005): Subset-093 GSM-R Interfaces Class 1 Requirements (v 2.3.0).
(Bazilinskyy et al. 2017)	Bazilinskyy, Pavlo & Petermeijer, Sebastiaan & Petrovych, Veronika & Dodou, Dimitra & de Winter, Joost (2018): Take-over requests in highly automated driving: A crowdsourcing multimedia survey on auditory, vibrotactile, and visual displays. Transportation Research Part F Traffic Psychology and Behaviour. 56. 82-98. 10.1016/j.trf.2018.04.001.
(Becker 2018)	Becker, Torsten (2018): Prozesse in Produktion und Supply Chain optimieren. 3. Auflage 2018. Berlin, Heidelberg: Springer Berlin Heidelberg.
(Bertsche 2009)	Bertsche, Bernd (2009): Zuverlässigkeit mechatronischer Systeme. Berlin, Heidelberg: Springer (VDI-Buch).
(Bilgin und Gungor 2013)	Bilgin, B. E.; Gungor, V. C. (2013): Performance Comparison of IEEE 802.11p and IEEE 802.11b for Vehicle-to-Vehicle Communications in Highway, Rural, and Urban Areas. In: International Journal of Vehicular Technology 2013, S. 1–10. DOI: 10.1155/2013/971684.
(Bundestag 2021)	Bundestag (2021): Gesetzentwurf der Bundesregierung - Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren
(Blanchard et al. 1995)	Blanchard; Verma; Peterson (1995): Maintainability. A key to effective serviceability and maintenance management. New York: John Wiley & Sons.

(Blazhko et al. 2017)	Blazhko, V., Kalinovsky, A., Kovalev, V. (2017): Unmanned Aerial Vehicle (UAV): Back to Base Without Satellite Navigation. In: Krasnoproshin, V., Ablameyko, S. (eds) Pattern Recognition and Information Processing. PRIP 2016. Communications in Computer and Information Science, vol 673. Springer, Cham. https://doi.org/10.1007/978-3-319-54220-1_15
(Bosse 2010)	Bosse, Gunnar (2010): Grundlagen für ein generisches Referenzsystem für die Betriebsverfahren spurgeführter Verkehrssysteme. Online verfügbar unter: https://nbn-resolving.org/urn:nbn:de:gbv:084-11032810363.
(Braband 2019)	Braband, Jens (2019): Funktionale Sicherheit. In: Lothar Fendrich und Wolfgang Fengler (Hg.): Handbuch Eisenbahninfrastruktur. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 583–638.
(Braband et al. 2022)	Braband, Jens; Evers, Bernhard; Rexin, Franziska; Lindner, Luisa; Kinas, Marco; Milius, Birgit; Adebahr, Frederik; Schäbe, Hendrik (2022): ATO-RISK. Abschlusspräsentation.
(Brandau 2011)	Brandau, Jochen (2011): Rückfallkonzept für den GSM-R-Zugfunk. In: *Deine Bahn*, S. 46–51.
(Brandenburger et al. 2016)	Brandenburger, Niels; Naumann, Anja; Jipp, Meike (2016): Die Entwicklung der Aufgaben des Triebfahrzeugführers in der Zukunft In: *Signal + Draht*, (108) März 2016, S. 37–42.
(Brandenburger et al. 2017)	Brandenburger, Niels; Hörmann, Hans-Jürgen; Stelling, Dirk; Naumann, Anja (2017): Der Train Operator. In: *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit* 231 (10), S. 1115–1122. DOI: 10.1177/0954409716676509.
(Brandenburger et al. 2018a)	Brandenburger, Niels; Naumann, Anja (2018a): Towards remote supervision and recovery of automated railway systems: The staff's changing contribution to system resilience. In: *International Conference on Intelligent Rail Transportation (ICIRT)*, S. 1–5. DOI: 10.1109/ICIRT.2018.8641576.
(Brandenburger et al. 2018b)	Brandenburger, Niels; Naumann, Anja (2018b): Menschliche Problemlösung macht automatisierten Bahnverkehr erfolgreich. In: *Signal + Draht*, S. 6–13.
(Bundesamt für Justiz, 2019)	Bundesamt für Justiz (01.08.2019): Eisenbahn-Bau- und Betriebsordnung (EBO).
(Bundesamt für Justiz, 2021)	Bundesamt für Justiz (15.09.2021): Allgemeine Eisenbahngesetz (AEG).

(Cellarius et al. 2021)	Cellarius, Bastian; Fritsche, Richard; Lohmar, Thorsten; Kuo, Fang-Chun (2021): Design of an FRMCS 5G E2E System for Future Rail Operation. Ericsson, Digitale Schiene Deutschland und DB Netze.
(Cheok et al. 1998a)	Cheok, M. C., Parry, G. W., & Sherry, R. R. (1998a): Response to 'Supplemental viewpoints on the use of importance measures in risk- informed regulatory applications'. Reliability Engineering & System Safety, 60(3), 261.
(Cheok et al. 1998b)	Cheok, M. C., Parry, G. W., & Sherry, R. R. (1998b): Use of importance measures in risk-informed regulatory applications. Reliability Engineering & System Safety, 60(3), 213-226
(Crespo 2020)	Crespo, Arturo (2020): Dynamisches und intermodales Störfallmanagement für S-Bahn Systeme. Dissertation. TU Darmstadt, Darmstadt.
(DB Fernverkehr AG 2010)	DB Fernverkehr AG (2010): Richtlinie 418.10-90 „Triebfahrzeugführerheft für Triebfahrzeugführer der EFF Klassen 2 und 3“.
(DB Netz AG 2014)	DB Netz AG (2014): Risikoanalyse zu ETCS Baseline 3, Gefährdungsidentifikation. v. 5.5. München.
(DB Netz AG 2016)	DB Netz AG (2016): Fahrdienstvorschrift. Richtlinie 408.
(DB Netz AG 2017)	DB Netz AG (2017): Richtlinie (Ril) 420 - Betriebszentralen DB Netz AG.
(DB Netz AG 2018)	DB Netz AG (2018): Grundsätze zur Erstellung der Entwurfsplanung zur Ausrüstung von Strecken mit ETCS Level 2. Richtlinie 819.1343, S. 6.
(DB Netz AG 2020)	DB Netz AG (2020): Richtlinie 413.0301 Streckenstandards.
(DB Netz AG 2022)	DB Netz AG (2022): Richtlinie 405 Fahrwegkapazität.
(DB Sicherheit, o.D.)	DB Sicherheit (o.D.): Kompetenzcenter Multicopter, Beratung, Planung und Durchführung von Multicoptereinsätzen im DB-Konzern und für Dritte. Online verfügbar unter https://www1.deutschebahn.com/dbsicherheit-de/Unsere_Leistungen/Weitere-Leistungen/02_Multicopter-7749316, zuletzt geprüft am, 09.04.2023
(Destatis 2021)	Statistisches Bundesamt: Betriebsdaten des Schienenverkehrs Fachserie 8 Reihe 2.1 - 2017, 2018
(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 50126-2:2017)	DIN EN 50126-1:2017, Oktober 2018: Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS), Teil 2: Systembezogene Sicherheitsmethodik.
(DIN EN 50128:2011)	DIN EN 50128:2011, März 2012: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme
(DIN EN 50129:2018)	DIN EN 50129:2018, Juni 2019: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsbezogene elektronische Systeme für Signaltechnik
(DIN VDE V 0831-103:2020)	DIN VDE V 0831-103:2020: Elektrische Bahn-Signalanlagen Teil 103: Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik
(Düpmeier 2022)	Düpmeier, Frederik (2022): Smarte Sicherungslogik für das Stellwerk der nächsten Generation. Dissertation. TU Darmstadt, Darmstadt.
(earthofdrones 2022)	earthofdrones (2022): RTH function (return to home) - important notes. Online verfügbar unter https://earthofdrones.com/rth-function-return-to-home-important-notes/, zuletzt geprüft am, 14.03.2023
(EBA 2012)	EBA (2012): Sicherheitsrichtlinie Fahrzeug Ausführungsbestimmungen (SIRF 400), Hg. v. EBA (Rev 2), S. 4.
(Ehrmanntraut 2010)	Ehrmanntraut, R. (2010): FULL AUTOMATION OF AIR TRAFFIC MANAGEMENT IN HIGH COMPLEXITY AIRSPACE. Dissertation. Universitätsbibliothek Dresden
(Emery 2017)	Emery, Daniel (2017): Towards automatic train operation in long distance service: State-of-the-art and challenges. In: *17 th Swiss Transport Research Conference*.
(ERA 2005)	ERA (2005): ERTMS/ETCS Subset-093 GSM-R Interfaces Class 1 Requirements. Hg. v. ERA (v 2.3.0).
(ERA 2016a)	ERA (2016a): ERTMS/ETCS Subset-026 System Requirements Specification Chapter 3 Principles. Hg. v. ERA (v 3.6.0).
(ERA 2016b)	ERA (2016b): ERTMS/ETCS Subset-026 System Requirements Specification Chapter 4 Modes and Transitions. Hg. v. ERA (v 3.6.0).
(ERA 2016c)	ERA (2016c): ERTMS/ETCS Subset-026 System Requirements Specification Chapter 5 Procedures. Hg. v. ERA (v 3.6.0).

(ERA 2018) European Railway Agency (ERA) (2018): ATO over ETCS - System Requirements Specification. REF: SUBSET 125 (Issue 0.1.0).

(Essid et al. 2020) Essid, Amin; Klaus, Christian; Üyümez, Bilal (2020): Alternative Communication Paths in Disrupted Automated Railway Operations. In: Eisenbahntechnischer Rundschau Science (10), S. 11-15.

(EUG 2020a) EUG & EULYNX (2020a): RCA - Architectural Approach and Systems of Systems Perspective. RCA.Doc. 13 (Gamma. 1).

(EUG 2020b) EUG & EULYNX (2020b): RCA - Concept Degraded Modes in RCA. RCA.Doc 32 (Gamma 1).

(EUG 2022) EUG & EULYNX (2022): ATO - Concept. RCA.Doc 72.

(Eurail Press 2022) Eurail Press (2022): Kurzberichte. In: *Signal + Draht* (1+2), S. 60–63.

(Europäische Union 2012a) Europäische Union (14.11.2012): Technische Spezifikation für die Interoperabilität des Teilsystems "Verkehrsbetrieb und Verkehrssteuerung" des Eisenbahnsystems in der Europäischen Union und zur Änderung der Entscheidung 2007/756/EGeuropäischen Eisenbahnraums. Rechtsvorschrift 2012/757/EU.

(Europäische Union 2012b) Europäische Union (21.11.2012): RICHTLINIE (EU) 2012/32 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums. EU-Richtlinie 2012/34.

(Europäische Union 2016) Europäische Union (11.05.2016): RICHTLINIE (EU) 2016/797 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 11. Mai 2016 über die Interoperabilität des Eisenbahnsystems in der Europäischen Union (Neufassung). EU-Richtlinie 2016/797.

(Fabbian 2006) Fabbian, F. (2006): Converting existing service to fully automatic operation. In: *WIT Press Computers in Railways X* (88), S. 373–379. DOI: 10.2495/CR060371.

(Fassel 2008) Fassel, Michael (2008): Bereitstellung bei der Deutschen Bahn AG, Ein Blick hinter die Kulissen der Zugfahrt [PowerPoint Folien].

(Fischer 2020) Fischer, Markus (2020): Smartrail 4.0: Utopie und Realität – BAV pfeift Bahnen zurück. Online verfügbar unter https://sev-online.ch/de/aktuell/kontakt.sev/2020/utopie-und-realitt-202019-35343/ , zuletzt geprüft am, 08.04.2023

(Frtunikj et al. 2014) Frtunikj, J., Rupanov, V., Armbruster, M., Knoll, A. (2014): Adaptive Error and Sensor Management for Autonomous Vehicles: Model-Based Approach and Run-Time System. In: Ortmeier, F.,

Rauzy, A. (eds) Model-Based Safety and Assessment. IMBSA 2014. Lecture Notes in Computer Science, vol 8822. Springer, Cham. https://doi.org/10.1007/978-3-319-12214-4_13

(Gold et al. 2013) Gold C., Damböck D., Lorenz L., Bengler K. (2013): Take over! How long does it take to get the driver back into the loop? [Conference session]. Proceedings of the Human Factors and Ergonomics Society 57th Annual Meeting (pp. 1938–1942)

(Goll und Dausmann 2013) Goll, Joachim; Dausmann, Manfred (2013): Architektur- und Entwurfsmuster der Softwaretechnik. Wiesbaden: Springer Fachmedien Wiesbaden.

(Grey 2018) Grey, Eva (2018): Around the world: 1,000km of fully automated metros. Online verfügbar unter https://www.railway-technology.com/features/around-world-driverless-metro-lines/, zuletzt geprüft am, 08.04.2023

(Gunther 2007) Gunther, Brux (2007): Automatischer Betrieb Projekt RUBIN - U-Bahn Nürnberg. In: *Das Eisenbahn Ingenieur Kompendium*.

(Haas 2015) Haas, Jürgen (2015): Rückfallebenen für Streckenausrüstung ETCS Level 2 ohne Signale. In: *Signal + Draht S.* 6-10 (107).

(Hansen und Pachl 2014) Hansen, Ingo A.; Pachl, Jörn (Hg.) (2014): Railway Timetabling & Operations. Analysis, modelling, optimisation, simulation, performance evaluation. Unter Mitarbeit von Thomas Albrecht. 2. rev. and extended ed. [Erscheinungsort nicht ermittelbar]: Eurailpress in DVV Media Group.

(Hirshorn 2007) Hirshorn, Steven R. (2007): NASA Systems Engineering Handbook.

(Huang 2020) Huang, Po-Chi (2020): Risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten des Bahnbetriebs. Dissertation. Universitätsbibliothek Braunschweig.

(IEC 62267:2009) IEC 62267, Juli 2009: Railway applications – Automated urban guided transport (AUGT) – Safety requirements

(IEEE 2003) IEEE (2003): IEEE Standard for User Interface Requirements in Communications-Based Train Control (CBTC) Systems. IEEE Std 1474.2-2003. New York, N.Y: Institute of Electrical and Electronics Engineers.

(IEEE 2005) IEEE (2005): IEEE standard for communications-based train control (CBTC) performance and functional requirements. IEEE Std 1474.1-2003. New York, N.Y: Institute of Electrical and Electronics Engineers. Online verfügbar unter http://ieeexplore.ieee.org/servlet/opac?punumber=9643.

(Jacob 2022) Jacob, Baseliyos (2022): ATO Betuweroute. DZSF Workshop.

(Jurtz 2019) Untersuchung zur Einführung von ETCS im Kernnetz der S-Bahn Stuttgart. Abschlussbericht. Online verfügbar unter https://vm.baden-wuerttemberg.de/fileadmin/redaktion/m-mvi/intern/Dateien/PDF/Abschlussbericht_Untersuchung_ETCS_Stuttgart.pdf, zuletzt geprüft am 13.03.2023

(Kämmerer 2017) Kämmerer, Florian Rudolf (2017): Entwicklung eines Kennzahlensystems für Effektivität des Bahnbetriebs bei Abweichungen vom Regelbetrieb. Masterarbeit, TU Darmstadt

(Khan et al. 2017) Khan, Muhammad & Qureshi, Ijaz & Safi, Engr & Khan, Inam. (2017): Flying Ad-Hoc Networks (FANETs): A Review of Communication architectures, and Routing protocols. 10.1109/INTELLECT.2017.8277614.

(Kossiakoff et al. 2011) Alexander, Kossiakoff; William, N. Sweet; Samuel, J. Seymour; Steven, M. Biemer (2011): Systems engineering. Principles and practice (op. 2011). 2nd ed. Hoboken, N.J.: Wiley-Interscience (Wiley series in systems engineering and management, 67).

(Lindner 2012) Lindner, Tobias (2012): Entwicklung einer Methode zur Bewertung unterschiedlicher Rückfallebenen. In: *Signal + Draht* (104), S. 37–39.

(Lindner et al. 2014) Lindner, Tobias; Milius, Birgit; Arenius, Marcus; Schwencke, Daniel; Grippenkoven, Jan; Sträter, Oliver (2014): Betrachtungen zur Zuverlässigkeit des Triebfahrzeugführers, Erfassung sicherheitsbeeinflussender Faktoren und ihrer Bedeutung auf Basis von Ereignisdaten. In: *Eisenbahningenieur*, Januar 2014 S. 10–16.

(Leveson 2012) Leveson, Nancy (2012): Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, © Massachusetts Institute of Technology

(Leveson und Thomas 2018) Leveson, Nancy; Thomas, John P. (2018): STPA Handbook. Online verfügbar unter https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf, zuletzt geprüft am 13.03.2023

(Mahboob und Zio 2018) Mahboob, Qamar; Zio, Enrico (Hg.) (2018): Handbook of RAMS in railway systems. Boca Raton: Taylor & Francis CRC Press.

(Maier und Eberhardt 2000) Maier, Mark W.; Rechtin, Eberhardt (2000): The art of systems architecting. 2nd ed. Boca Raton: CRC Press.

(Martin 2014) Martin, Ullrich (2014): Performance Evaluation. In: Ingo A. Hansen und Jörn Pachl (Hg.): Railway timetabling & operations. Analysis, modelling, optimisation, simulation, performance

	evaluation. Unter Mitarbeit von Thomas Albrecht. 2. rev. and extended ed. Hamburg: Eurailpress, S. 275–290.
(Martin und Li 2014)	Martin, Ullrich; Li, Xiaojun (2014): Entwicklung einer simulationsbasierten Methodik zur ursachenbezogenen Engpassbewertung komplexer Gleisstrukturen in spurgeführten Verkehrssystemen unter Berücksichtigung stochastischer Bedingungen. DFG Forschungsprojekt (2326/10-1). Stuttgart, 2014.
(Maschek 2015)	Maschek, Ulrich (2015): Sicherung des Schienenverkehrs. Wiesbaden: Springer Fachmedien Wiesbaden.
(Meyer zu Hörste 2017)	Meyer zu Hörste, Michael (2017): Fully automatic railway operation: technical, operational and legal requirements.
(Milius und Huang 2017)	Milius, Birgit; Huang, Po-Chi (2017): Sichere Rückfallebenen in Zeiten der Rail-IT-Automation. In: Der Eisenbahningenieur 11/17, S. 36–39.
(Morant 2017)	Morant, Sue (2017): Automation spurs operational rethink in Barcelona. Online verfügbar unter https://www.railjournal.com/in_depth/automation-spurs-operational-rethink/, zuletzt geprüft am, 25.07.2023
(Morast und Nießen 2020)	Morast, Albrecht; Nießen, Nils (2020): Regelwerke und Gesetze in Bezug auf den fahrerlosen Betrieb. In: *Deine Bahn*, S. 18–21.
(Naeem 2017)	Naeem, Ali (2017): 7 Key CBTC Functions Transit Operators. Achieve Operational Efficiency, Recover Faster from Service Disruptions & Increase Ridership Satisfaction. CBTC Solutions Inc.
(Nagaraju und Fiondella 2018)	Vidhyashree Nagaraju and Lance Fiondella (2018): Software Reliability in RAMS Management. In Mahboob, Qamar; Zio, Enrico (Hg.) (2018): Handbook of RAMS in railway systems. Boca Raton: Taylor & Francis CRC Press.
NFON 2023	NFON (2023): Fallbacklösungen in der Telekommunikationstechnik. Online verfügbar unter https://www.nfon.com/de/los-gehts/cloud-telephonie/lexikon/knowledgebase-detail/fallback#c717, zuletzt geprüft am 09.04.2023
(Nießen et al. 2017)	Nießen, Nils; Schindler, Christian; Valée, Dirk (2017): Assistierter, automatischer oder autonomer Betrieb - Potentiale für den Schienenverkehr. In: *Eisenbahntechnischer Rundschau* (4).
(OCORA 2022a)	OCORA (2022a): Stakeholder Requirements. OCORA-TWS05-020 (Version 2.1).

(OCORA 2022b) OCORA (2022b): OCORA - CCS On-Board (CCS-OB) Architecture. OCORA-TWS01-035.

(Pachl 2007) Pachl, Jörn (2007): Kommunikation im Bahnbetrieb. In: *Deine Bahn*, S. 35–40.

(Pachl 2011) Pachl, Jörn (2011): Systemtechnik des Schienenverkehrs. Bahnbetrieb planen, steuern und sichern. 6., überarbeitete Auflage. Wiesbaden: Vieweg+Teubner (Studium).

(Pachl 2017) Pachl, Jörn (2017): Betriebliche Randbedingungen für autonomes Fahren auf der Schiene. In: *Deine Bahn*, S. 11–19.

(PAS 1883:2020) PAS 1883:2020, August 2020: Operational design domain (ODD) taxonomy for an automated driving system (ADS). Specification. The British Standards Institution 2020

(Rumsey 2010) Rumsey, Alan (2010): Semi-automatic, driverless and unattended operation of trains. In: *Signal + Draht* (102).

(Schawel 2011) Schawel, Christian (2011): Top 100 Management Tools. Das wichtigste Buch eines Managers. 3., überarbeitete Auflage. Wiesbaden: Gabler Verlag / Springer Fachmedien Wiesbaden GmbH, Wiesbaden.

(Schnieder 2019) Schnieder, Lars (2019): Eine Einführung in das European Train Control System (ETCS). Das einheitliche europäische Zugsteuerungs- und Zugsicherungssystem. 1st ed. 2019. Wiesbaden: Springer Fachmedien Wiesbaden; Springer Vieweg (essentials).

(Schröder et al. 2021) Schröder, Jan; Alpoim, Christoph Goncalves; Dickgießer, Boris; Knollmann, Volker (2021): Digital S-Bahn Hamburg - Erstmalige Realisierung von „ATO over ETCS“ in Deutschland. In: *Signal+Draht* (113), S. 52–59.

(Schwanhäußer 1974) Schwanhäusser, Wulf (1974): Die Bemessung der Pufferzeiten im Fahrplangefüge der Eisenbahn. Dissertation. Rheinisch-Westfälischen Technischen Hochschule Aachen, Aachen

(Skybrary, o.D.) Skybrary (o.D.): Quick Reference Handbook (QRH). Online verfügbar unter https://www.skybrary.aero/articles/quick-reference-handbook-qrh, zuletzt geprüft am 09.04.2023.

(Slamal et al. 2022) Slamal, Sofia; Wala, Jens; Üyümez, Bilal (2022): Fahren auf elektronische Sicht im vollautomatisierten Betrieb – mögliche Gestaltungsvarianten. In: *Eisenbahntechnischer Rundschau* (11), S. 28–31.

(Smith and Simpson 2011) Smith, David J; Simpson, Kenneth GL (2011): Safety Critical Systems Handbook: A Straightfoward Guide to Functional Safety,

IEC 61508 (2010 Edition) and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 AND ISO 13849, Third Edition

(Smith 2019) Smith, Kevin (2019): Rise of the machines: Rio Tinto breaks new ground with AutoHaul. IRJ - International Railway Journal (08/2919). Online verfügbar unter https://www.railjournal.com/in_depth/rise-machines-rio-tinto-autohaul/, zuletzt geprüft am 09.03.2023.

(Tanenbaum und Van Steen 2007) Tanenbaum, Andrew S.; Van Stehen, Maarten (2007): Distributed Systems: Principles and Paradigms, Pearson Prentice Hall , Upper Saddle River, NJ, Second Edition

(Trinckauf 2013) Trinckauf, Jochen (2013): Visionen und Aussichten in der Bahnsicherungstechnik. In: *Deine Bahn*, S. 7–10.

(Trinckauf et al. 2020) Trinckauf, Jochen; Maschek, Ulrich; Kahl, Richard; Krahl, Claudia (2020): ETCS in Deutschland 2020. 1. Aufl. Leverkusen: PMC Media House GmbH.

(UIC 1998) UIC (1998): ERTMS/ETCS RAMS Requirements Specification - Chapter 2 – RAM (Version 6).

(UIC 2018) UIC (2018): Future Railway Mobile Communication System - User Requirements Specification (Version 3.0.0).

(Üyümez und Oetting 2019) Üyümez, Bilal; Oetting, Andreas (2020): Integration of Humans in the Fallback Process by a Machine in Fully Automated Railway Operation. In: Tareq Ahram, Waldemar Karwowski, Alberto Vergnano, Francesco Leali und Redha Taiar (Hg.): Intelligent Human Systems Integration 2020, Bd. 1131. Cham: Springer International Publishing (Advances in Intelligent Systems and Computing), S. 992–998.

(Üyümez 2019) Üyümez, Bilal (2019): Potenziale einer Mensch-Maschine Kooperation bei Störungen im automatisierten Betrieb. In: Eisenbahntechnischer Rundschau (10), S. 18-24.

(Vakhtel 2002) Vakhtel, Sergey (2002): Rechnerunterstützte analytische Ermittlung der Kapazität von Eisenbahnnetzen. Dissertation. RWTH Aachen, Aachen.

(Völp und Esteves-Verissimo 2018) Voelp, Marcus; Esteves-Verissimo, Paulo (2018): Intrusion-Tolerant Autonomous Driving. In: 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC). 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC). Singapore, 29.05.2018 - 31.05.2018: IEEE, S. 130–133.

(Weiss et al. 2020)	Philipp Weiss, Andreas Weichslgartner, Felix Reimann, and Sebastian Steinhorst (2020): Fail-operational automotive software design using agent-based graceful degradation. In Proceedings of the 23rd Conference on Design, Automation and Test in Europe (DATE '20). EDA Consortium, San Jose, CA, USA, 1169–1174.
(Wende 2003)	Wende, Dietrich (2003): Fahrdynamik des Schienenverkehrs. 1. Auflage. Wiesbaden: Vieweg+Teubner (Studium).
(Winner et al. 2015)	Winner, Hermann; Hakuli, Stephan; Lotz, Felix; Singer, Christina (Hg.) (2015): Handbuch Fahrerassistenzsysteme. Wiesbaden: Springer Fachmedien Wiesbaden.
(Winzer 2013)	Winzer, Petra (2013): Generic Systems Engineering. Berlin, Heidelberg: Springer Berlin Heidelberg.
(Wolf und Langer 2022)	Wolf, Richard; Langer, Georg (2022): GoA4-Readiness – Herausforderungen für zukünftige Fahrzeuggenerationen. In: *ZEVrail*, S. 4–9.
(Xue et al. 2018)	Xue, W., Yang, B., Kaizuka, T., & Nakano, K. (2018): A Fallback Approach for an Automated Vehicle Encountering Sensor Failure in Monitoring Environment. 2018 IEEE Intelligent Vehicles Symposium (IV), 1807-1812.
(Zimmermann und Hommel 2003)	Zimmermann, A., Hommel, G. (2003): A train control system case study in model-based real time system design. In: International Parallel and Distributed Processing Symposium. IEEE, pp. 118–126.

Abkürzungsverzeichnis

Abzw.	Abzweigstelle
AEG	Allgemeines Eisenbahngesetz
AFB	Automatische Fahr- und Bremssteuerung
AS	automatische Stromabnehmersenkeinrichtung
ATO	Automatic Train Operation (automatisierter Bahnbetrieb)
ATO-AE	Automatic Train Operation Execution
ATO-AT	Automatic Train Operation Transactor
ATOM	Automatic Train Operation Monitoring
ATO-OBU	Automatic Train Operation Onboard Unit
ATO-TS	Automatic Train Operation Trackside System
BCM	Business Continuity Management, Betriebskontinuitätsmanagement
Bf.	Bahnhof
Bü	Bahnübergang
CBTC	Communication-Based-Train Control System
CCU	Command and Control Computing Unit (Safe Computing Plattform, sichere Rechenplattform)
Digital ATO	Digital and Automated Train Operation
DIN	Deutsches Institut für Normung
DLR	Deutschen Zentrum für Luft- und Raumfahrt
DSD	Digitale Schiene Deutschland
DSRC	Dedicated Short Range Communication, zweckgebundene Nahbereichskommunikation
DSTW	Digitales Stellwerk
DTO	driverless train operation
EBD	Eisenbahnbetriebsfeld in Darmstadt
EBO	Eisenbahnbau- und Betriebsordnung
ECAM	Electronic Centralized Aircraft Monitor
ECU	Electronic Control Unit

EIU	Eisenbahninfrastrukturunternehmen
EN	Europäische Norm
ERA	European Railway Agency
ERJU	Europes-Rail Joint Undertaking
ETCS	European Train Control System
ETCS L2 oS	ETCS Level 2 ohne Signale
EUG	Vereinigung europäischer Bahnbetreiber (ERTMS Users Group)
EVU	Eisenbahnverkehrsunternehmen
FBQ	Fallback Benefit Quotient
FFFIS	Form Fit Function Interface Specification
FMU	Fallback Management Unit
FNC	Fallback Normal Costs
FOB	Fallback Operational Benefit
FRMCS	Future Rail Mobile Communication System
FS	Full-Supervision (vollüberwachter Fahrmodus beim ETCS-System)
GAMAB	Globalement au moins aussi bon, Generell mindestens so gut
GoA	Grade of Automation, Automatisierungsgrad der Zugfahrten
GSM-R	Global System for Mobile – Rail
Hp	Haltepunkt
Hst	Haltestelle
IEEE	Institute of Electrical and Electronics Engineers
IP	Innovation-Pillar
ITS	Intelligent Transport Systems
JP	Journey-Profiles
LCC	Life Cycle Costs, Lebenszykluskosten
LEU	Lineside Electronic Unit
LST	Leit- und Sicherungstechnik
LZB	Linienförmige Zugbeeinflussung
MA	Movement Authority

MP	Movement Permission, Fahrterlaubnisanfrage
MTBF	Mean-Time-Between-Failures
NTC	National Train Control
OC	Object-Controller
OCORA	Open CCS On-board Reference Architecture
OS	On-Sight (Fahren auf Sicht beim ETCS-System)
PFH	Probability of Failure per Hour, Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde
PMNO	Public Mobile Network Operator
PSs	Perception System
PZB	Punktförmige Zugbeeinflussung
QRH	Quick Reference Handbook
RAP	Redundanz-Allokation-Problem
RAMS	Reliability, Availability, Maintainability und Safety
RAW	Risk-Achievement-Worth, Risikoleistungswert
RBC	Radio Block Center, ETCS-Zentrale
RCA	Open CCS Reference Architecture
Ril	Richtlinie
RMTO	Remote Manual Train Operation
RTH	Return-to-Home
SGV	Schienengüterverkehr
SIL	Safety Integrity Level
SP	Segment-Profiles
SysP	System-Pillar
SPFV	Schienenpersonenfernverkehrszüge
SPNV	Schienenpersonennahverkehrszüge
SR	Staff Responsible (ein Fahrmodus beim ETCS-System)
STPA	System-Theoretic Process Analysis
Tf	Triebfahrzeugführer

THR	Tolerable-Hazard-Rate (tolerierbare Gefährdungsrate)
TMS	Traffic Management System
TO	Train-Operator
TRDP	Train Real Time Data Protocol
TSI	Technische Spezifikation der Interoperabilität
Überleitst	Überleitstelle
UIC	International Union of Railways, Internationaler Eisenbahnverband
UITP	International Association of Public Transport
UTO	Unattended train operation
UVCCB	Universal Vehicle Command and Control Bus
VDE	Verband der Elektrotechnik Elektronik Informationstechnik
VLS	Vehicle Localization System
VS	Vehicle Supervisor
Zs1	Zusatzsignal (Ersatzsignal)
Zs7	Zusatzsignal (Vorsichtssignal)

Variablenverzeichnis

$\sum t_{Wa,zul}$	zulässige Summe der außerplanmäßigen Wartezeit in einem Betriebsprogramm
$\sum t_{Wa}$	tatsächliche Summe der außerplanmäßigen Wartezeit in einem Betriebsprogramm
$\sum BR$	Summe des Betriebsrisikos über die Lebensdauer eines technischen Systems
$P_0(p_i, t)$	Wahrscheinlichkeit für das Top-Ereignis (betriebliche Funktion wird nicht erfüllt), wenn ein Systemelement deaktiviert ist (p_i =1)
$P_0(t)$	Wahrscheinlichkeit für das Top-Ereignis aus dem Regelbetrieb.
Q_0	festgelegte Betriebsqualität im Regelbetrieb (z.B. wirtschaftlich optimaler Bereich, $Q_0 = 0{,}5 - 1{,}2$)
ΔQ_0	Abweichung von der vereinbarten Betriebsqualität aus dem Regelbetrieb
R_{Grenz}	Risikogrenzwert auf einem Netzelement mit einem bestimmten Streckenstandard
S_i	Schadensausmaß, das sich im Falle von einem unerwünschten Ereignis während der jeweiligen betrieblich-technischen Rückfallebene ergibt
$T_{sys,i}$	Lebensdauer eines technischen Systems
f_{SIL}	Faktor, der sich durch die Abstufung des SIL ergibt.
n_{Kombi}	Kombinierte Betrachtung der möglichen Gefährdungsursachen unter Vernachlässigung der Reihenfolge
$n_{Störung,i}$	Häufigkeit einer Störungssituation im Systemelement i
p_R	Ausfall- bzw. Versagenswahrscheinlichkeit der eingebundenen Ressource
p_i	Ausfallwahrscheinlichkeit eines Systemelements aus der Systemarchitektur
$t_{RFE,D,i}$	Dauer der betrieblich-technischen Rückfallebene auf Basis der jeweiligen Adaptionsart
$\lambda_{D,i}$	Gefährdungsrate, die aus der jeweiligen dynamischen Adaption resultiert
$\lambda_{D,oFa}$	Geänderte Gefährdungsrate aufgrund der Deaktivierung eines gestörten Systemelements ohne Funktionsallokation
λ_E	Geänderte Gefährdungsrate aufgrund des Ersetzens zur Laufzeit
λ_{RB}	Gefährdungsrate des ersetzten Systemelements im Regelbetrieb
LCC_{rel}	Prozentuale Änderung der Lebenszykluskosten im Vergleich zu den Basiskosten aufgrund der technischen Redundanzen und der dynamischen

	Adaption (ATO-FMU) einschließlich der erforderlichen Ressourcen für die betrieblich-technischen Rückfallebenen
$BR_{D,i}$	Betriebsrisiko der jeweiligen dynamischen Adaption mit unterschiedlicher Gefährdungsrate
$BR_{D,i}$	Betriebsrisiko der jeweiligen dynamischen Adaption
C	Fähigkeit des betrachteten Systems, seine beabsichtigte Aufgabe in einer bestimmten Zeit bei einer bestimmten Auslastung zu erfüllen
LCC_{Basis}	Basiskosten der für den vollautomatisierten Bahnbetrieb erforderlichen technischen Systeme
$LCC_{D,i}$	Zusatzkosten für die dynamische Adaption (ATO-FMU) einschließlich der erforderlichen Ressourcen für die betrieblich-technischen Rückfallebenen
LCC_{Gesamt}	gesamte Lebenszykluskosten aus der Summe der Basiskosten für die Migration des vollautomatisierten Bahnbetriebs und der Kosten für die technischen Redundanzen sowie für die dynamische Adaption (ATO-FMU)
$LCC_{Redundanz}$	Zusatzkosten für die technischen Redundanzen
LCC	Lebenszykluskosten des betrachteten Systems
$MTBF_{sys,i}$	Mittlere Zeit bis zum Ausfall eines technischen Systems
RI_{dyn}	Erwarteter Risikoindex der jeweiligen dynamischen Adaption über die Lebensdauer
$RAW_{mFa}(i \mid t)$	Risikoleistungswert, wenn ein Systemelement i aus der Systemarchitektur mit Funktionsallokation zum Zeitpunkt t deaktiviert wird
$RAW_{oFa}(i \mid t)$	Risikoleistungswert, wenn ein Systemelement i aus der Systemarchitektur ohne Funktionsallokation zum Zeitpunkt t deaktiviert wird
RAM	RAM-Werte repräsentieren dabei die Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit des betrachteten Systems
SE	Effektivität des betrachteten Systems
i	Systemelement i aus der Systemarchitektur
t	Zeit
$t_{Wa,Z1}$	außerplanmäßige Wartezeit des Entdeckerzuges
$t_{Bef,ist}$	tatsächliche Beförderungszeit des Entdeckerzuges
$t_{Bef,plan}$	planmäßige Beförderungszeit des Entdeckerzuges
$t_{VF,ij}$	Folgeverspätung des nachfolgenden Zuges aufgrund der außerplanmäßigen Wartezeit des Entdeckerzuges
t_{Pij}	Pufferzeit zwischen zwei Zügen

t_{Vei}	Einbruchsverspätung des Entdeckerzuges,
t_{Vej}	Einbruchsverspätung der nachfolgenden Züge.
$n_{betroffen}$	Anzahl der von der Störungssituation betroffenen Züge

Abbildungsverzeichnis

Tabellenverzeichnis

Anlagen

Anlage 1: Das Kommunikationsdiagramm der Mensch-Maschine Kooperation mit einem Train-Operator und einem Zugpersonal

Einbindung eines Zugpersonals zur ersatzweisen Übernahme der Geschwindigkeitsregelung

Bei GoA3 geführten Personenzügen ist es auch denkbar, das Zugpersonal vorübergehend zu beauftragen, die Geschwindigkeitsregelung für eine Weiterfahrt in Störungssituation zu übernehmen. Damit in der Mensch-Maschine Kooperation das eingebundene Zugpersonal in Störungssituation aufgrund der begrenzten Zeit nicht zu viele maschinelle Daten verarbeiten muss, wäre es sinnvoll, das Zugpersonal mit dem Train-Operator kooperieren zu lassen. Das eingebundene Zugpersonal kann verbale Anweisungen von dem Train-Operator empfangen, um die Geschwindigkeitsregelung ersatzweise zu übernehmen. Das Zugpersonal kann während der Geschwindigkeitsregelung gleichzeitig die Lichtraumüberwachung übernehmen und dabei das Freisein des vorausliegenden Streckenabschnitts an den Train-Operator verbal melden. Ein Zugpersonal kann auch lediglich als visueller Informationskanal für den Train-Operator wirken, ohne dabei die Geschwindigkeitsregelung zu übernehmen. Das Kommunikationsdiagramm dazu ist wie folgt:

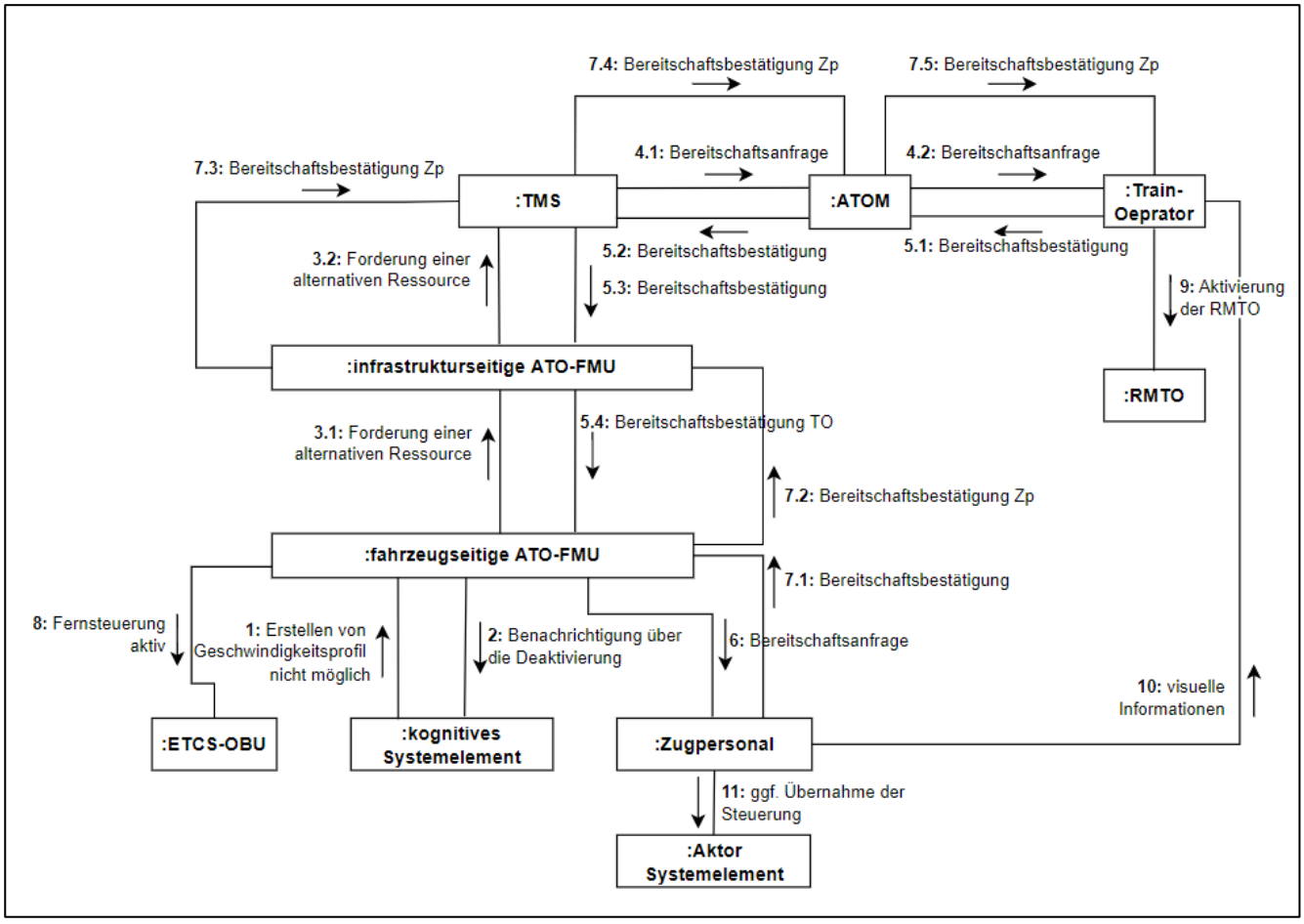

Abbildung 50 Kommunikationsdiagramm, das die Koordination während der Deaktivierung einer gestörten Kamera bzw. eines gestörten kognitiven Systemelements (mit Funktionsallokation auf Zugpersonal für eine Mensch-Maschine Kooperation) darstellt

Die folgende Tabelle enthält die kurze Erläuterung der einzelnen Schritte innerhalb des Kommunikationsdiagramms.

Tabelle 6 Tabelle mit kurzer Erläuterung der einzelnen Schritte innerhalb des Kommunikationsdiagramms.

Schritt im Kommunikationsdiagramm	Kurze Erläuterung des Schritts
1	Von dem kognitiven Systemelement wird die Störung gemeldet, dass kein Geschwindigkeitsprofil erstellt werden kann
2	Die fahrzeugseitige ATO-FMU benachrichtigt das kognitive Systemelement, dass es deaktiviert wird
3.1	Die fahrzeugseitige ATO-FMU fordert von der infrastrukturseitigen ATO-FMU eine alternative Ressource für die Erstellung eines Geschwindigkeitsprofils, da durch Deaktivierung ohne Funktionsallokation keine Weiterfahrt möglich ist
3.2	Die infrastrukturseitige ATO-FMU leitet die Anfrage an das TMS weiter
4 (4.1 – 4.2)	Das TMS fragt über das Systemelement ATOM die Bereitschaft eines Train-Operators an
5 (5.1 – 5.4)	Sofern ein Train-Operator bereit ist, wird die Bereitschaft bestätigt und an die fahrzeugseitige ATO-FMU übermittelt
6.1	Danach fragt die fahrzeugseitige ATO-FMU die Bereitschaft eines Zugpersonals an
7 (7-1 – 7.5)	Sofern ein Zugpersonal bereit ist, wird die Bereitschaft bestätigt und an den Train-Operator übermittelt
8	Sofern eine Fernsteuerung durch den eingebundenen Train-Operator erfolgen soll, wird die ETCS-OBU von der fahrzeugseitigen ATO-FMU darüber benachrichtigt
9	Train-Operator aktiviert die Fernsteuerung
10	Das eingebundene Zugpersonal übermittelt verbal das Freisein des vorausliegenden Streckenabschnitts an den Train-Operator
11	Ggf. kann das Zugpersonal von dem Train-Operator beauftragt werden, die Geschwindigkeitsregelung zu übernehmen

Anlage 2: Berechnung der Mindestzugfolgezeit und der mittleren Mindestzugfolgezeit aus dem festgelegten Betriebsprogramm sowie der zulässigen außerplanmäßigen Wartezeit

Zur Berechnung der Mindestzugfolgezeit und der mittleren Mindestzugfolgezeit aus dem festgelegten Betriebsprogramm ist das Betriebsprogramm aus dem Unterkapitel 8.3.2 erforderlich.

Tabelle 7 Betriebsprogramm für das Anwendungsbeispiel

Betriebsprogramm für M160					
Modellzüge	SPFV: ICE	SPNV-S: RE	SPNV-L: RB	SGV-S	SGV-L
Höchstgeschwindigkeit der Modellzüge	250 km/h	160 km/h	120 km/h	100 km/h	80 km/h
Anzahl der Modellzüge / Richtung und 1 h	4	2	1	2	1

Da die Berechnung mit Hilfe von Matlab durchgeführt wurde, sind die Ergebnisse der Mindestzugfolgezeiten und der mittleren Mindestzugfolgezeit in der Tabelle 8 zusammengestellt.

Tabelle 8 Tabelle der Mindestzugfolgezeiten der Modellzüge aus dem Betriebsprogramm

z_{ij} in **s**	SPFV: ICE	SPNV	SGV-S	SGV-L
SPFV	169.13	144.95	169.00	121.00
SPNV	226.19	177.74	193.42	145.42
SGV-S	322.19	273.74	238.00	190.00
SGV-L	532.19	483.74	447.99	287.99
$\bar{z}$ **in s**	$\mathbf{164,4}\ \boldsymbol{s}$			

Tabelle 9 Tabelle der Fahr- und Beförderungszeiten der Modellzüge im Betrachtungsraum. Regelzuschlag in Anlehnung an DB Ril 402.0301 3 % für Personenzüge und 4 % für Güterzüge

	SPFV	SPNV	SGV-S	SGV-L
Fahrzeit der Modellzüge im Betrachtungsraum in **min**	7,76 min	8,87 min	10,35 min	13,8 min
Beförderungszeit der Modellzüge im Betrachtungsraum mit Regelzuschlag in **min**	8 min	9,14 min	10,76 min	14,35 min

Zur Berechnung der zulässigen Summe der außerplanmäßigen Wartezeit in dem festgelegten Betriebsprogramm kann das Mittelwertverfahren nach *Schwanhäußer (1974)* verwendet werden. Die Formel dazu ist wie folgt:

$$E(t_{Wa}) = \left(p_{v,ein} - \frac{p_{v,ein}^2}{2}\right) * \frac{\bar{t}_{v,ein}{}^2}{\bar{t}_P + \bar{t}_{v,ein} * \left(1 - e^{-\frac{\bar{z}}{\bar{t}_{v,ein}}}\right)} * \left[p_g * \left(1 - e^{-\frac{t_{Z_{gm}}}{\bar{t}_{v,ein}}}\right)^2 + (1 - p_g)\frac{t_{Z_{vm}}}{\bar{t}_{v,ein}} * \left(1 - e^{-\frac{2*t_{Z_{vm}}}{\bar{t}_{v,ein}}}\right) + \frac{\bar{z}}{\bar{t}_P} * \left(1 - e^{-\frac{\bar{z}}{\bar{t}_{v,ein}}}\right)^2\right] \quad A1$$

$p_{v,ein}$ = Wahrscheinlichkeit für das Auftreten einer Einbruchsverspätung (gemittelt über alle Modellzüge),

$\bar{t}_{v,ein}$ = mittlere Einbruchsverspätung der verspäteten Züge (gemittelt über alle Modellzüge),

$\bar{z}$ = mittlere Mindestzugfolgezeit = **164,4 s = 2,74 min (Tabelle 8 Anhang 2)**,

$\bar{t}_P$ = mittlere Zugfolge-Pufferzeit = **1 min (Tabelle 6 in Ril 405.0103A02)**,

p_g = Wahrscheinlichkeit für das Auftreten von gleichrangigen Zugfolgefällen

$t_{Z_{vm}}$ = mittlere maßgebende Mindestzugfolgezeit der rangunterschiedlichen Zugfolgefälle

$t_{Z_{gm}}$ = mittlere maßgebende Mindestzugfolgezeit der gleichrangigen Zugfolgefälle

Die Werte für die Einbruchsverspätung der verspäteten Züge und der Wahrscheinlichkeit für das Auftreten einer Einbruchsverspätung wurden aus der Tabelle 2 in **405.0204A03** entnommen und in der folgenden Tabelle festgehalten:

	$p_{v,ein}$	$\bar{t}_{v,ein}$
SPFV	0,5	5 min
SPNV	0,6	4,5 min
SGV	0,6	10 min

Die resultierende mittlere Einbruchsverspätung der verspäteten Züge, gemittelt über alle Modellzüge, beträgt dann $\bar{\boldsymbol{t}}_{\boldsymbol{v,ein}} = \mathbf{11,2}\ \boldsymbol{min}$**.** Die Berechnung wurde mit Hilfe von Matlab duchgeführt.

Die Wahrscheinlichkeit für das Auftreten von gleichrangigen Zugfolgefällen ergibt sich aus der Anzahl der Personenzüge in dem Betriebsprogramm dividiert durch die Gesamtanzahl der Züge und beträgt bei dem festgelegten Betriebsprogramm $\boldsymbol{p_g = 0,7}$**.**

Die Berechnung der mittleren maßgebenden Mindestzugfolgezeit der rangunterschiedlichen und gleichrangigen Zugfolgefälle wurde mit Hilfe von Matlab durchgeführt. Die Ergebnisse sind wie folgt:

$$\boldsymbol{t_{Z_{vm}} = 104,75\ s}$$

$$\boldsymbol{t_{Z_{gm}} = 87,59\ s}$$

Durch Einsetzen dieser Werte in die Formel A1 ergibt sich der Erwartungswert der Folgeverspätungen, gewichtet über alle Modellzüge entsprechend ihrer Auftretenshäufigkeiten $\boldsymbol{E(t_{Wa}) = 4,43\ min}$**.** Dieser Wert gilt für einen Zug im Betriebsprogramm. Um die Summe der zulässigen Folgeverspätungen während eines bestimmten Untersuchungszeitraums bestimmen zu können, ist der Wert mit der Anzahl

der Züge in dem Untersuchungszeitraum zu multiplizieren. Bei dem festgelegten Betriebsprogramm (Tabelle 8 Anhang 2) sind 10 Züge pro Stunde und Richtung vorhanden. Die Summe der zulässigen Folgeverspätungen in dem Betriebsprogramm über eine Stunde beträgt dann

$$\sum \boldsymbol{t_{Wa,zul} = 10 * 4,43\ min = 44,3\ min}.$$

Anlage 3: Herleitung der Flugzeit einer Drohne zu den von der Kommunikationsstörung betroffenen Zügen

Für die Ermittlung der Flugzeit der Drohne zum Zug ist zunächst der Ort des Zuges und der Ort der gefundenen und aktivierten Drohne erforderlich. Unter der Annahme, dass die Ortsangaben als GPS-Koordinaten vorliegen, kann die Berechnung der Flugstrecke (Luftlinie) mit Hilfe der Berechnung von Orthodromen erfolgen. Die Luftlinie beträgt demnach

$$L_{luft} = R_{Erde} * \arccos(x) \qquad A2$$

mit

$$x = \sin(\theta_A) * \sin(\theta_B) + \cos(\theta_A) * \cos(\theta_A) * \cos(\lambda_B - \lambda_A)$$

wobei

R_{Erde}= Radius der Erde (6378,137 km)

θ_A=geografische Breiteangabe der Drohne,

θ_B=geografische Breiteangabe des Zuges,

λ_A= geografische Längenangabe der Drohne und

λ_B= geografische Längenangabe des Zuges sind.

Die Flugstrecke der Drohne enthält die Komponenten **Steigflug, Geradeausflug und Sinkflug.**

Für die **Steigzeit** auf die maximale Steighöhe h_{max} (von Boden aus $h_0 = 0\,m$) ergibt sich mit der Steigrate (Geschwindigkeit v_{steig})

$$t_{steig} = \frac{2 * h_{max}}{v_{steig}} \qquad A3$$

Für die **Zeit des Geradesausflugs** ergibt sich dann mit der Luftgeschwindigkeit (True Air Speed v_{TAS})

$$t_G = \frac{L_{Luft}}{v_{TAS}} \qquad A4$$

Für den Sinkflug auf die gewünschte Höhe h_{soll} (z.B. Höhe der Oberleitung + Sicherheitsabstand) lässt sich die **Sinkzeit** mit der Sinkgeschwindigkeit (Sinkrate v_{sink}) mit

$$t_{sink} = \frac{2 * (h_{max} - h_{soll})}{v_{sink}} \qquad A5$$

bestimmen.

Die gesamte Flugzeit der Drohne zum Zug ergibt sich dann aus der Summe der Steigzeit, der Zeit für den Geradeausflug und der Sinkzeit und kann mit

$$\boldsymbol{t_{Flug,Drohne} = \sum t_i = t_{steig} + t_G + t_{sink}} \qquad A6$$

bestimmt werden.

Eine vereinfachte Rechnung mit Excel ergibt für eine Flugzeit einer Drohne zum Entdeckerzug im Funkloch folgendes Ergebnis:

Flugzeit einer Drohne zum Entdeckerzug zum Aufbau eines Ad-Hoc Netzwerks	
Entfernung (Luftlinie)	10 km
Steigrate/Sinkrate der Drohne	25 m/s
Maximale Steighöhe	70 m
Luftgeschwindigkeit	50 km/h
Steigzeit	5,6 s
Zeit für Geradeausflug	720 s
Sinkzeit	5,6 s
Flugzeit einer Drohne zum Entdeckerzug	**731,2 s (12,19 min)**