Deutsches Zentrum für
Schienenverkehrsforschung beim

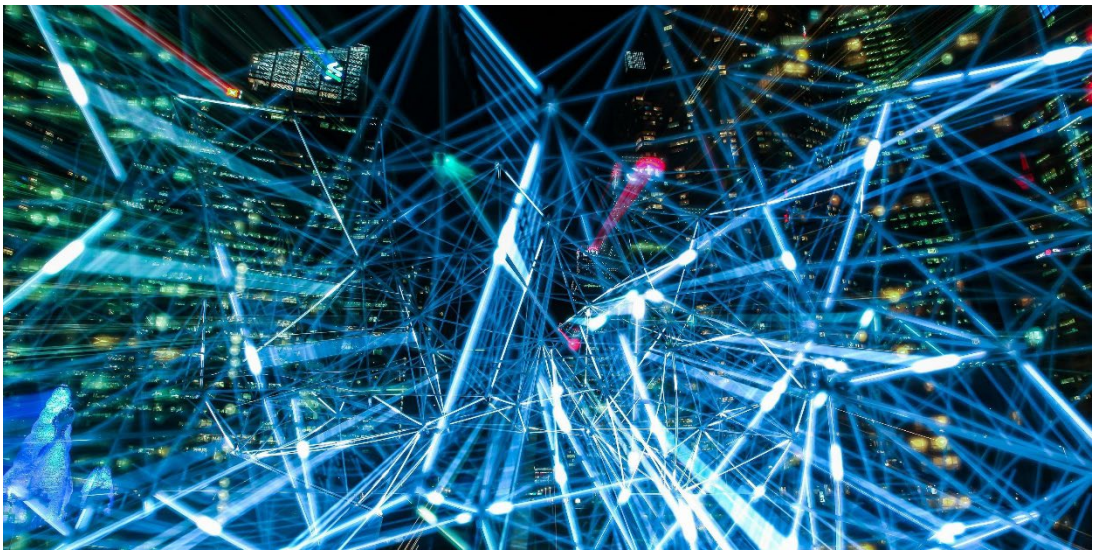
Eisenbahn-Bundesamt

Berichte
des Deutschen Zentrums
für Schienenverkehrsforschung

Bericht 64 (2024)

Sensorbasierte Technologien im Bahnsystem: Markt- und Technologieanalyse

Schlussbericht



Berichte des Deutschen Zentrums
für Schienenverkehrsforschung, Nr. 64 (2024)
Projektnummer 2021-08-D-1202

Sensorbasierte Technologien im Bahnsystem: Markt- und Technologieanalyse

von

Saskia Discher, Dr. Tobias Herrmann, Andreas Schulz
IFB Institut für Bahntechnik GmbH, Berlin

Marco Rehme
Technische Universität Chemnitz, Fakultät für Wirtschaftswissenschaften, Lehrstuhl für Unternehmensrechnung und Controlling (BWL III), Chemnitz

Benjamin Heibutzki, Marco Meinig, Ronny Otto
Fraunhofer ENAS, Abteilung Multi Device Integration, Chemnitz

Prof. Dr. Ina Schiering, Alexander Gabel, Ramona Schmidt
Institut für Information Engineering, Ostfalia Hochschule für angewandte Wissenschaften, Wolfenbüttel

Peter Grenz
POG Consulting, Hamburg

im Auftrag des Deutschen Zentrums für Schienenverkehrsforschung beim Eisenbahn-Bundesamt

Impressum

HERAUSGEBER
Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt

August-Bebel-Straße 10
01219 Dresden

http://www.dzsf.bund.de

DURCHFÜHRUNG DER STUDIE
IFB Institut für Bahntechnik GmbH
Carnotstraße 6
10587 Berlin

ABSCHLUSS DER STUDIE
Juli 2024

REDAKTION
Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt
Dr. Manuela Kauder, Susanne Hillmann, Dr.-Ing. Christian Klotz

BILDNACHWEIS
Pexels, Pixabay 373543

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

ISSN 2629-7973

doi: 10.48755/dzsf.240017.01

Dresden, Dezember 2024

Inhaltsverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface (Anwendungsprogrammierschnittstelle)
ARINC	Aeronautical Radio, Incorporated
AsBo	Assessment Body (Unabhängige Bewertungsstelle)
ASLR	Address Space Layout Randomization
ATEX	Atmosphères Explosives (Explosionsgefährdete Bereiche)
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
AUTOSAR	AUTomotive Open System Architecture
BMDV	Bundesministerium für Digitales und Verkehr
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAN	Controller Area Network
CAN-FD	Controller Area Network Flexible Data Rate
CANopen	CAN - Controller Area Network
CARLO	Occlusion-Aware hieRarchy anomaly detection
CBTC	Communication-Based Train Control
CCN	CANopen Consist Network
CCTV	Closed Circuit Television
CENELEC	Comité Européen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardization; Europäisches Komitee für elektrotechnische Normung)
CIP	Customer Information Platform
CLC	Präfix für CENELEC in Referenznummern von CENELEC-Schriftstücken
CNA	Center for Transportation & Logistics Neuer Adler e. V.
CNN	Convolutional Neural Network
COS	Customer Oriented Services
CRL	Certificate Revocation List
CSM-RA	Common Safety Methods – Risk Assessment (Gemeinsame Sicherheitsmethoden - Risikoanalyse)
CVE	Common Vulnerabilities and Exposures
CYRail	Cybersecurity in the RAILway sector
CYSIS	Arbeitsgruppe Cybersecurity für sicherheitskritische Infrastrukturen
DAK	Digitale Automatische Kupplung
DDos	Distributed Denial of Service
DeBo	Designated Body (Bestimmte Stelle)
DEP	Data Execution Prevention
DIN	Deutsches Institut für Normung
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
DMS	Dehnungsmessstreifen
DNN	Deep Neural Network
EBA	Eisenbahn-Bundesamt
EBO	Eisenbahn-Bau- und Betriebsordnung
ECM	Entity in Charge of Maintenance
ECN	Ethernet Consist Network
EI	Der Eisenbahningenieur
EIGV	Eisenbahn-Inbetriebnahmegenehmigungsverordnung
ENISA	European Network and Information Security Agency
EP	Elektropneumatisch

ERA	Europäische Eisenbahnagentur
ERP	Enterprise-Resource-Planning
ERTMS	European Rail Traffic Management System
ETB	Ethernet Train Backbone
ETB-L	Ethernet Train Backbone Left
ETBN	Ethernet Train Backbone Node
ETB-R	Ethernet Train Backbone Right
ETCS	European Train Control System
EU	Europäische Union
FBOA	Festbremsortungsanlage
FDF	Functional Distribution Framework
FIP	Factory Instrumentation Protocol
FOC	Functional Open Coupling
FTP	File Transfer Protocol
Fz.	Fahrzeug
GNSS	Global Navigation Satellite System (Globales Navigationssatellitensystem)
GPS	Global Positioning System
GSM-R	Global System for Mobile Communications – Rail
HDLC	High-Level Data Link Control
HMAC	Keyed-Hash Message Authentication Code
HOA	Heißläuferortungsanlage
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation and Air Conditioning (Heizung, Lüftung, Klimatechnik)
ICMP	Internet Control Message Protocol
ICS	International Classification for Standards
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IH	Instandhaltung
IKT	Informations- und Kommunikationstechnologie
IMP	Integrated Modular Platform
Infra	Infrastruktur
IO	Input/Output
IoT	Internet of Things
IP	Internet Protocol
IP-Klasse	International Protection-Klasse
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPTCom	IP Train Communications
IR	Infrarot
ISO	Internationale Organisation für Normung
IT	Informationstechnik
ITSS	Industrieplattform für Telematik und Sensorik im Schienengüterverkehr
JSON	JavaScript Object Notation
KI	Künstliche Intelligenz
KV	Kombinierter Verkehr
LiDAR	Light detection and ranging
LonWorks	Local Operatin Network
LTE	Long Term Evolution
MACsec	Media Access Control Security

MCG	Mobile Communication Gateway
MVB	Multifunction Vehicle Bus
NG-TCN	Next-Generation Train Communication Network
NIST	National Institute of Standards and Technology
NNTV/NNTR	Notifizierte nationale technische Vorschrift / Notifizierte nationale technische Regel
NX	Non Executable
OCSP	Online Certificate Status Protocol
OOS	Operator Oriented Services
OPC UA	Open Platform Communications Unified Architecture
OSI	Open Systems Interconnection
PESTEL	Political, Economic, Sociological, Technological, Environmental and Legal Factors-Analysis
PNAC	Port Based Network Access Control
PoW	Proof of Work
REST	Representational state transfer
RFC	Request for Comments
RFID	Radio Frequency Identification
RMR	Railway Mobile Radio
RTU	Remote Terminal Unit (Fernbedienungsterminal)
SAT	Selbstabfertigung Triebfahrzeugführer
SDT	Safe Data Transmission
SGV	Schienengüterverkehr
SIEM	Security Information and Event Management
SIL	Safety Integrity Level (Sicherheits-Integritätslevel)
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SPV	Schienenpersonenverkehr
SSID	Service Set Identifier
SSTF	Seitenselektive Türsteuerung Fernverkehr
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (Modell der IT-Sicherheit)
SVF	Simulation and Virtualization Framework (CONNECTA); Sequential View Fusion (LiDAR)
SWOT	Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen) and Threats (Risiken)-Analysis (Analyse)
SysML	Systems Modeling Language
TAV	Technikbasierte Abfertigungsverfahren
TCMS	Train Control and Monitoring System
TCN	Train Communication Network
TCP	Transmission Control Protocol
TEN	Transeuropäische Netzstrecken
TIS	Technischer Innovationskreis Schienengüterverkehr
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRDP	Train Real Time Data Protocol
TS	Technical Specification (Technische Spezifikation)
TSI	Technical Specifications for Interoperability
TSN	Time Sensitive Networking
TUF	The Update Framework
UDP	User Datagram Protocol
UIC	Union International des Chemins de Fer (Internationaler Eisenbahnverband)

URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall
WLAN	Wireless Local Area Network
WLCN	Wireless Consist Network
WLTB	Wireless Train Backbone
WLTBN	Wireless Train Backbone Node
WPA	Wi-Fi Protected Access
WTB	Wire Train Bus

Kurzbeschreibung/Abstract

Mit dem Forschungsprojekt „Sensorbasierte Technologien im Bahnsystem: Markt- und Technologieanalyse“ wurden wesentliche Grundlagen für den Einsatz von Sensoren im Schienenverkehr untersucht. Neben Recherchen sowie Expertinnen- und Experteninterviews konnte methodisch auch auf die Durchführung von zwei Workshops zurückgegriffen werden, um insbesondere die praxisrelevanten Inhalte und Erfahrungen berücksichtigen zu können.

Insgesamt konnten 43 Anwendungsfälle der Kategorien Herstellung Fahrzeug, Herstellung Infrastruktur, Instandhaltung Fahrzeug, Instandhaltung und Betrieb Infrastruktur sowie Bahnbetrieb herausgearbeitet werden. Diese wurden mithilfe von Expertinnen und Experten hinsichtlich ihres Mehrwertes und ihrer Umsetzbarkeit bewertet, sodass im Rahmen des Projekts sieben Use Cases einer genaueren Analyse unterzogen wurden. Für die Umsetzung von Sensoriklösungen bedarf es zwei Analysen: der Technologie- und der Marktanalyse.

Im Rahmen der Technologieanalyse gilt es zum einen die benötigten Sensoren und Schnittstellen so zu definieren und anzupassen, dass sie der Vielzahl an Anforderungen für einen Einsatz im Schienenverkehr genügen. Hierbei ist es hilfreich, auf bestehende Technologien und Architekturen zurückzugreifen und bereits existierende Patente zu berücksichtigen. Zum anderen muss die Auslegung der Sensorlösungen in jedem Fall sicher erfolgen. Das beinhaltet sowohl die sogenannten Safety-Aspekte als auch die Cybersecurity. Insbesondere bei neuartigen Technologien müssen die Angriffspotenziale so gering wie möglich gehalten werden und beherrschbar sein. Erst wenn alle Anforderungen erfüllt sind, kann das Sensorsystem im Bahnbereich eine Zulassung erhalten und zum Einsatz kommen. Dabei kann es sich, je nach vorgesehenem Sensorsystem, um einen langen Prozess handeln.

Die Marktanalyse beinhaltet ebenfalls mehrere Themen. Zum einen zählt dazu die Stakeholderanalyse. Es wurden 34 Stakeholder-Hauptgruppen als relevant für den Bahnsektor herausgearbeitet. Je nach Anwendungsfall existieren unterschiedliche, teilweise komplexe Beziehungen zwischen den Stakeholdern. Ebenso ließen sich 24 Innovationsbarrieren, eingeordnet in die Kategorien Technologie, Recht, Standardisierung, Geschäftsmodelle und Markt, ableiten, die es vor einem Einsatz des Anwendungsfalls zu beseitigen gilt. Zum anderen umfasst die Marktanalyse Handlungsableitungen und einen Marktausblick. Es ließen sich 36 Maßnahmenvorschläge aus zehn Handlungsfeldern ableiten. Diese konnten den Kategorien Technik und Recht, Markt, Daten- und Informationsmanagement sowie Innovationsförderung zugeordnet werden. Bei der Geschäftsmodellentwicklung konnten die Anwendungsfälle hinsichtlich des größten Veränderungspotenzials und des größten Neuheitscharakters eingeordnet werden, diese Aspekte gilt es auch bei weiteren Use Cases zu beachten. Des Weiteren wurden für den Marktausblick die Marktattraktivität und die Marktreife berücksichtigt.

Die angesprochenen Untersuchungen wurden im Forschungsprojekt insbesondere für sieben ausgewählte Anwendungsfälle durchgeführt, sie lassen sich jedoch auch auf andere Anwendungsfälle übertragen und zeigen die Vielfalt und Komplexität der möglichen Anwendungen. Mit dieser Untersuchung konnte eine Grundlage für den Einsatz von Sensoriksystemen im Schienenverkehr geschaffen werden und auf verschiedene zu berücksichtigende Punkte eingegangen werden. Bis zu einer konkreten Umsetzung von Sensoranwendungen bedarf es allerdings noch einiges an Zeit und tieferen Analysen.

1 Einleitung

Zur Optimierung vielfältiger Abläufe im Betrieb von Bahnen, in der Produktion und Instandhaltung von Schienenfahrzeugen, in der Leit- und Sicherungstechnik sowie in der Logistik im Schienengüterverkehr werden zunehmend digitale Methoden verwendet. Dabei werden durch die Vernetzung von Subsystemen, die Erfassung und Echtzeitauswertung von Sensordaten sowie die Nutzung dieser Daten zur Ableitung von Informationen für verschiedenste Aufgabenbereiche schnellere und effizientere Prozesse unterstützt. Besonders hervorzuheben ist die (teilweise) Automatisierung des Bahnbetriebs, die die Digitalisierung und Vernetzung sämtlicher Teilbereiche voraussetzt. Die für die Umsetzung dieser digitalen Methoden erforderlichen Sensordaten werden auf den Fahrzeugen oder in der Infrastruktur erhoben. Neben betrieblichen Funktionen wie Automatisierung und fahrzeugtechnischen Aspekten wie der effizienten Instandhaltung werden auch Sicherheits- und Komfortaspekte im Fahrgastraum sowie logistische Aspekte des Güterverkehrs berücksichtigt. Einige Sensordaten werden zum Teil bereits auf heutigen Schienenfahrzeugen erfasst (z. B. Geschwindigkeit, Position, Kameraüberwachung). In anderen Fällen befinden sich Sensorsysteme in der Entwicklung, in der Erprobungsphase oder werden in geringem Umfang und ohne Vernetzung im Bahnsystem verwendet (z. B. Ortung von Güterwagen, fahrzeuggestützte Heißläuferdetektion, Bremsdrucküberwachung für die automatische Bremsprobe von Güterzügen). Weitere Sensoren, die für den Einsatz im digitalisierten oder automatisierten Schienenfahrzeug denkbar sind, werden bisher nicht eingesetzt (z. B. Kraft-, Dehnungs-, Spannungssensoren zur Strukturüberwachung).

Zur Umsetzung der Digitalisierung und Automatisierung des Bahnverkehrs werden robuste, zuverlässige, langlebige und präzise Sensoren benötigt sowie die intelligente Analyse und Bewertung der Sensordaten. In komplexen und kostengetriebenen technischen Systemen kann die Anzahl der Sensoren jedoch nicht ohne Nachteile bezüglich Aufwand, Kosten und Zuverlässigkeit beliebig erhöht werden. Die Herausforderung besteht daher darin, aus einer möglichst geringen Anzahl an Sensoren einen maximalen Informationsgehalt für vielfältige Anwendungen zu gewinnen. Dies kann durch Sensordatenfusion, intelligente Datenverarbeitung und automatisierte Entscheidungsfindung erreicht werden. Dazu ist es notwendig, die Sensordaten zwischen den verschiedenen Sensorsystemen, Datenverarbeitungseinheiten, Subsystemen und mit intelligenten Datenplattformen auszutauschen. Dazu sollen Sensorsysteme unterschiedlicher Herkunft und Hersteller beliebig kombiniert werden können und so zu einer Vereinfachung von Ausrüstung und Betrieb beitragen.

Neben funktionaler Sicherheit (Safety) erfordert die Verwendung von vielfältiger Sensorik und Bordnetzen auch Sicherheit gegen Angriffe, da dadurch Angriffspunkte entstehen. Zum einen kann Sensorik selber manipuliert werden, zum anderen werden Sensoren über Netzwerke, insbesondere mobile Netzwerke, angebunden. Besonders bei der Nutzung mobiler Netzwerke bestehen weitere Angriffspotenziale. Neben der Vertraulichkeit und Integrität der gesendeten Daten können durch Angriffe mobile Netzwerke beeinträchtigt werden.

2 Ziel

Um im Zuge der Digitalisierung und Automatisierung des Bahnsystems sichere Sensornetzwerke zu ermöglichen, sollen in diesem Projekt Sensoren, Sensorsysteme und Datenschnittstellen zwischen diesen sowie zu externen Netzwerken untersucht werden. Dabei soll ein zum Erreichen dieses Ziels geeigneter Aufbau der verschiedenen Komponenten ermittelt sowie Komponentenkonzepte recherchiert werden, aus denen ein übergeordnetes Sensorikkonzept ableitbar ist. Dies soll auf Basis des aktuellen Stands der Technik im Bahnsektor und darüber hinaus sowie unter Berücksichtigung der Bedürfnisse der verschiedenen Stakeholder geschehen. Dabei sollen aktuelle und zukünftig denkbare Anwendungsfälle von Sensorik im Bahnsystem sowie die jeweils relevanten Anforderungen an die Komponenten berücksichtigt werden. Um die Anwendbarkeit sicherzustellen, soll dabei auch der bahnspezifische Zulassungsprozess für die Komponenten beachtet werden.

Aus den ermittelten technischen Randbedingungen sollen Handlungsempfehlungen für die Gesamtheit der Stakeholder abgeleitet werden, um zielgerichtete Weiterentwicklungen des Marktes zu ermöglichen. Dabei sollen auch mögliche Nutzengewinne ermittelt werden.

Aufgrund der Risiken bei der Verwendung von digitalen Komponenten und Netzwerken soll im Projekt neben der funktionalen Sicherheit in allen Aspekten auch die Cybersecurity berücksichtigt werden. Dazu werden Angriffspotenziale identifiziert und eine Risikoanalyse durchgeführt.

3 Vorgehen

Das Projekt teilt sich entsprechend der Leistungsbeschreibung in folgende fünf Kapitel auf:

- Bestandsaufnahme Sensormarkt (siehe Kapitel 4)
- Stakeholderanalyse (siehe Kapitel 5)
- Handlungsableitungen und Marktausblick (siehe Kapitel 6)
- Bestandsaufnahme und Patentrecherche – Sensoriksysteme und Teilkomponenten (siehe Kapitel 7)
- Bestandsaufnahme – Datensicherheit und Risikoanalyse, Cybersecurity (siehe Kapitel 8)

Zur Erweiterung der Datenbasis wurden im Projekt zwei Workshops zu unterschiedlichen Zeitpunkten geplant. Der erste Workshop diente der Evaluierung der Use Case Analyse in Kapitel 4. Er war technisch orientiert und sollte dazu dienen, die erarbeiteten Anwendungsfälle von Sensoriklösungen zu filtern und zu bewerten. Dazu wurden 18 Personen aus technischen Bereichen in allen beteiligten Sparten des Bahnsektors (z. B. Fahrzeughersteller, EVU, EIU, Fahrzeughalter, Instandhalter, Logistikunternehmen) sowie Expertinnen und Experten aus der Sensortechnik hinzugezogen. Der erste Workshop wurde zudem dazu genutzt, im Rahmen von Interviews auch Daten für die Kapitel 5 und 6 zu generieren, um auch hier die Analysen auf den empirisch erarbeiteten Bedürfnissen der Stakeholder zu gründen.

Der zweite Workshop fand im Rahmen der Arbeiten an Kapitel 6 statt. Dabei wurden ein qualitativer Marktausblick über wirtschaftliche Marktpotenziale sowie neue Geschäftsfelder und Wertschöpfungsstufen erstellt. Aufgrund der wirtschaftlichen Themen dieses Workshops wurde ein Teilnehmendenkreis von 21 Personen zusammengestellt, um zu vermeiden, dass die Datengenerierung dadurch kompliziert wird, dass Teilnehmende miteinander im direkten Wettbewerb stehen.

4 Bestandsaufnahme Sensormarkt

Zu Beginn erfolgt eine Bestandsaufnahme des Sensormarktes. Ziel ist es, tatsächliche und mögliche Sensoranwendungen im Bahnsystem anhand von konkreten Use Cases zu ermitteln, diese nach ihrer Relevanz zu bewerten sowie im Hinblick auf Anforderungskriterien bezüglich eines Einsatzes im Bahnwesen zu untersuchen. Aufgeteilt ist das Kapitel in drei Unterkapitel.

Im ersten Unterkapitel werden Anwendungsfälle von Sensortechniken herausgearbeitet. Diese werden durch Literaturrecherchen und Expertinnen- und Experteninterviews ermittelt. Es werden sowohl Anwendungsgebiete nach dem Stand der Technik als auch zukünftige Anwendungen berücksichtigt, die aus dem Fahrzeugbereich und der Infrastruktur stammen. Anschließend erfolgten eine Kategorisierung und übersichtliche Darstellung.

Im zweiten Unterkapitel werden die Anwendungsfälle bewertet. Über eine Online-Umfrage und einen Workshop werden die ermittelten Use Cases hinsichtlich ihrer Relevanz und Realisierbarkeit eingeordnet. Das Ergebnis ist eine Liste der relevantesten Anwendungsfälle von Sensorik, die für die weiteren Betrachtungen genutzt werden.

Im dritten Unterkapitel wird eine Anforderungsanalyse durchgeführt. Dazu werden Anforderungen definiert, die an Sensoren im Bahnsystem gestellt werden. Für die relevanten Anwendungsfälle werden die benötigten Komponenten ermittelt. Zudem werden diese Fälle hinsichtlich der Anforderungen bewertet. Zusätzlich wird der Zulassungsprozess von Sensoren im Bahnsystem dargestellt.

4.1 Use Case Analyse

In diesem Unterkapitel sollte eine umfassende Liste von Anwendungsfällen für Sensorik im Bahnwesen erarbeitet werden. Die Liste der Anwendungsfälle soll im weiteren Projektverlauf zur Bewertung nach Relevanz durch Expertinnen und Experten geeignet sein, sodass die relevantesten Anwendungsfälle für Sensorik im Bahnsystem identifiziert werden.

Dazu wurde zunächst eine systematische Literaturrecherche durchgeführt, in der Anwendungsfälle von Sensorik im Bahnbereich sowie die zugehörigen Randbedingungen und Charakteristika (je nach Verfügbarkeit) aufgenommen wurden. Die Verarbeitung der Ergebnisse der Literaturrecherche erfolgte in mehreren Schritten. Zunächst wurden die in der Literatur recherchierten Anwendungsfälle zusammengefasst und vorsortiert. Das Ergebnis dieses Schritts war eine vorläufige Liste der Anwendungsfälle.

Diese Liste wurde für eine Online-Umfrage verwendet, in der Fachleute die Anwendungsfälle hinsichtlich ihrer Relevanz und Umsetzbarkeit bewerteten. Zugleich stellte die Liste die Grundlage für die die Literaturrecherche ergänzenden Expertinnen- und Experteninterviews dar. Die Ergebnisse der Interviews sowie das Feedback des Pretests wurden dann in die Liste eingepflegt, um eine finale Liste der Anwendungsfälle zu erhalten, die in die tatsächliche Umfrage und den darauffolgenden Workshop eingehen konnte. Die Umfrage sowie der Workshop sind Teil des Kapitels 4.2.

Die Details der Recherche und Auswertung werden in den folgenden Kapiteln beschrieben.

4.1.1 Recherche

Die Recherche wurde unter anderem systematisch und chronologisch durchgeführt, um sicher zu stellen, dass keine aktuell diskutierten Anwendungsfälle übersehen werden. Dies bedeutet, dass alle Artikel

aus den ausgewählten Publikationen und Zeiträumen (siehe folgenden Absatz „Publikationen und Untersuchungszeitraum“) gründlich nach dem Thema Sensorik durchsucht wurden, auch wenn der Artikel nicht direkt Sensorik als Thema beinhaltete. Der Grund dafür ist, dass Sensorik heutzutage viel Anwendung findet und häufig thematisch nur nebensächlich ist. Da die Absicht ist, alle Anwendungsfälle abzudecken, werden auch diese Artikel mitbetrachtet.

Publikationen und Untersuchungszeitraum

Bei der Auswahl der Publikationen lag der Fokus auf renommierten Fachzeitschriften in der Bahnbranche. Hier eigneten sich die ZEVrail und der Eisenbahningenieur (EI), da diese gut die neuen technischen Entwicklungen in der deutschen Bahnbrache abdecken. Weitere Fachzeitschriften parallel systematisch zu betrachten, erschien nicht sinnvoll, da diese hauptsächlich dieselben aktuellen Themen abdecken. Abgesehen von der chronologischen Vorgehensweise wurde explizit nach dem Thema Sensorik gesucht, um gegebenenfalls auch Anwendungen zu finden, die nur in anderer Literatur erwähnt werden oder über die länger nicht mehr berichtet wurde. Wenn in Fachzeitschriften bestimmte Sensorsysteme genannt wurden und die Informationen aus dem Artikel nicht ausreichen, wurde die Quellenlage auf Herstellerinformationen, z B. Produktbeschreibungen, erweitert. Dies ermöglichte, weitere Detailinformationen über die Systeme und deren Anwendungen zu finden.

Der Untersuchungszeitraum für die chronologische Vorgehensweise begann mit den aktuellsten Veröffentlichungen und von da aus in die Vergangenheit bis 2020 bzw. 2019. Bei ZEVrail bedeutet das genau: März 2022 bis Mai 2019 inklusive dem Sonderheft Graz von 2019. Beim EI heißt das von Mai 2022 bis April 2021. Die verfügbaren Arbeitsressourcen waren mehr auf die ZEVrail fokussiert, da diese Zeitschrift die beste technische Detailtiefe bietet. Das antichronologische Vorgehen hat den Vorteil, dass zuerst die aktuellsten Artikel über bestimmte Sensorprojekte gefunden werden und dieselben Projekte in älteren Veröffentlichungen vernachlässigt werden können. Dies führt zu einer hohen Aktualität der Rechercheergebnisse. Der Zeitraum wurde als nicht allzu groß gewählt, da schnell der Zeitpunkt eintritt, wo nur wenige neue Anwendungsfälle gefunden werden.

Ein detailliertes Quellenverzeichnis über alle verwendete Literatur befindet sich in Kapitel 6 in der Anlage A.

Recherchetabelle

Die Rechercheergebnisse wurden in einer Tabelle zusammengefasst. Diese Tabelle gliedert sich in drei Abschnitte. Der erste Abschnitt bezieht sich auf den Anwendungsfall, siehe Abbildung 1. Die hier aufgeführten Informationen dienen der allgemeinen Einordnung des Anwendungsfalls aus der jeweiligen Quelle, z. B. hinsichtlich des Realisierungsgrades. Die genauen Bedeutungen der einzelnen Spalten sind in Tabelle 1 genauer erläutert.

	A	B	C	D	E	F
1	Quellen-ID	Use-Case	Betrachtungsgebiet	Status	Zeitraum	Fahrzeug bzw. Infrastruktur
2	Beschreibung	Anwendungsfall auf der höchsten Ebene	Schlagwort	Schlagwort	bitten angeben, wenn nicht bekannt	Liste; bitten angeben, wenn nicht bekannt
3	1	autonomes Fahren	Fahrzeug	Erprobung	seit 2016	Advanced Trainlab (ICE-TD), Combino Straßenbahn Potsdam
4	1	autonomes Fahren	Fahrzeug	Erprobung	seit 2016	Advanced Trainlab (ICE-TD), Combino Straßenbahn Potsdam
5	1	autonomes Fahren	Fahrzeug	Erprobung	seit 2016	Advanced Trainlab (ICE-TD), Combino Straßenbahn Potsdam
6	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
7	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
8	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
9	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
10	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
11	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
12	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
13	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
14	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien
15	2	Immissionsschutz (Schall)	Infra	Betrieb	seit 2021	U-Bahn Wien

Abbildung 1: Auszug aus Recherchetabelle mit dem ersten Abschnitt [IFB GmbH]

Der zweite Abschnitt bezieht sich auf die verwendeten Sensoren, ein Ausschnitt davon ist in Abbildung 2 dargestellt. Die hier aufgeführten Informationen sind für die Beschreibung des Anwendungsfalls nicht erforderlich. Sie dienen als Vorleistung für die in Kapitel 4.3 durchzuführende Analyse der Anwendungsfälle. In Kapitel 4.3 werden die Anwendungsfälle hinsichtlich der benötigten Komponenten untersucht. Da dies eine erneute Konsultation der Quellen erfordern würde, wurden bereits zu diesem Zeitpunkt die entsprechenden Informationen zu den Anwendungsfällen recherchiert und in die Tabelle übernommen.

	H	I	J	K
1	Verwendete Sensoren	physikalisches Wirkprinz	Montageort	Anwendung der Sensoren
2	Schlagwort, 1 Sensor pro Zelle	Schlagwort, 1 Wirkprinzip pro Zelle	Schlagwort, 1 Montageort pro Zelle	Schlagwort, 1 Anwendung pro Zelle
3	Kamera		Fahrzeugfront	Umfelderkennung
4	Lidar		Fahrzeugfront	Umfelderkennung
5	Radar		Fahrzeugfront	Umfelderkennung
6	Beschleunigungssensor		Schiene	
7	Beschleunigungssensor		Schwelle	
8	Beschleunigungssensor		Gleistragplatte	
9	Schwinggeschwindigkeitssensor		Schiene	
10	Schwinggeschwindigkeitssensor		Schwelle	
11	Schwinggeschwindigkeitssensor		Gleistragplatte	
12	Dehnmessstreifen		Schienenfuß	Spannungsanalyse
13	Dehnmessstreifen		Schienenfuß	Geschwindigkeitsermittlung
14	Mikrofon		im Freien	Schallaufzeichnung
15	Wetterstation		im Freien	

Abbildung 2: Auszug aus Recherchetabelle mit dem zweiten Abschnitt [IFB GmbH]

Im dritten Abschnitt werden Informationen über Sensorsysteme gesammelt, falls ein System im Kontext zu einem Anwendungsfall erwähnt wurde. Ein Ausschnitt dazu findet sich in der folgenden Abbildung 3. Auch die hier aufgeführten Informationen sind für die Beschreibung der Anwendungsfälle nicht erforderlich, sondern werden als Vorleistung für die Arbeiten in den Kapiteln 4.3, 7 und 8 aufgenommen.

	L	M	N	O	P
1	Verwendete Sensorsysteme	Anwendung des Systems	Systemkomponenten	Schnittstellen vom Sensorsystem	Kommerziell
2	Schlagwort, 1 Sensorsystem pro Zelle	Schlagwort, 1 Anwendung pro Zelle	Schlagwort	Schlagwort	ja/nein/nicht bekannt
6	Argos OOR (out-of-roundness)	Erkennung geschädigter Räder		Internet	ja
22	Smart Current Collector (SCC)	Überwachung mechanischer Defekte an Oberleitungen	Faseroptische Steckverbindung und Koppler, Lichtquelle, Optisches Spektrometer		nein
25	Siemens Tram Assistant	Kollisionswarnassistenten		Steuergerät zum erzeugen von Kollisionswarn- und Bremssignalen	ja
26	Siemens Mainline Assistant	Kollisionswarnassistenten		Steuergerät zum erzeugen von Kollisionswarn- und Bremssignalen	geplant
29	DafuR von DB Systemtechnik (mit Hegenscheidt ARGUS Komponenten)	Detektion unrunde Räder, Überladungen und Schiefladungen		unbekannt	ja
33	infraView DIANA	Weichendiagnose		Internet	ja

Abbildung 3: Auszug aus Recherchetabelle mit dem dritten Abschnitt [IFB GmbH]

Die vollständige Recherchetabelle aller drei Abschnitte ist in Anlage A zu diesem Zwischenbericht zu finden.

TABELLE 1: ERLÄUTERUNG DER SPALTEN DER RECHERCHETABELLE

Spalte	Spaltenname	Erläuterung
A	Quellen-ID	Verweis auf die Quelle
B	Use Case	Anwendungsfallbenennung auf der obersten Ebene
C	Betrachtungsgebiet	Angabe, ob sich die Anwendung auf Fahrzeug (Fz.) oder Infrastruktur (Infra) bezieht
D	Status	Realisierungsgrad (Anwendung schon in Betrieb, in Forschung oder in Erprobung)
E	Zeitraum	Der Zeitraum des Betriebs oder der Erprobung der Anwendung
F	Fahrzeug bzw. Infrastruktur	Angabe, auf welches Fahrzeug bzw. Fahrzeuggruppe oder Infrastruktur sich die Anwendung bezieht
H	Verwendete Sensoren	Der verwendete Sensor im Anwendungsfall
I	physikalisches Wirkprinzip	Physikalisches Wirkprinzip des Sensors
J	Montageort	Ort der Montage des Sensors
K	Anwendung der Sensoren	Die konkrete Anwendung bzw. der konkrete Nutzen des Sensors
L	Verwendete Sensorsysteme	Name des Sensorsystems
M	Anwendung des Systems	Die konkrete Anwendung bzw. der konkrete Nutzen des Sensorsystems
N	Systemkomponenten	Komponenten des Sensorsystems
O	Schnittstellen vom Sensorsystem	Schnittstellen des Sensorsystems
P	Kommerziell	Angabe, ob es sich dabei um ein kommerziell erwerbliches Sensorsystem handelt

Expertinnen- und Experteninterviews

Um Anwendungsfälle inkl. der entsprechenden Sensoren zu berücksichtigen, über die in den analysierten Veröffentlichungen nicht explizit berichtet wurde, wurden Expertinnen- und Experteninterviews durchgeführt. Damit wurden insbesondere Anwendungsfälle abgedeckt, die im Bahnwesen etabliert sind, die also dem Stand der Technik entsprechen. Es wird vorausgesetzt, dass diese Anwendungsfälle, die im Zuge einer ausgeweiteten Recherche auch der Fachliteratur entnommen werden könnten, langjährigen Fachexpertinnen und -experten der Bahntechnik bekannt sind. Zusätzlich sollten die recherchierten Anwendungsfälle im Rahmen der Interviews hinsichtlich Verständlichkeit, inhaltlichen Ungenauigkeiten und redaktionellen Fehlern geprüft werden. Grundlage der Interviews war jeweils eine vorläufige Liste der Anwendungsfälle, die das Ergebnis der Literaturrecherche abbildet.

Es wurden drei Interviews mit Experten mit langjähriger Erfahrung im Bahnbereich durchgeführt. Zusätzlich wurden Anwendungsfälle und Sensoren aus dem Wissens- bzw. Erfahrungsschatz der Autoren und Autorinnen des Berichts berücksichtigt, die als viertes Interview aufgeführt werden.

Im Folgenden werden Kurzzusammenfassungen der Interviews aufgeführt.

1. Expertinnen- und Experteninterview
    - Brandschutz ist zulassungsrelevant und regulatorisch definiert. Daher ist er als Anwendungsfall von Sensorik nicht zu diskutieren und kann aus der Liste der Anwendungsfälle entfernt werden.
    - Relevanz und Umsetzbarkeit der Anwendungsfälle sind abhängig von den jeweiligen Anforderungen an die Sicherheit (z. B. ist Lokalisierung von Schienenfahrzeugen als Parameter für Zugsicherungssysteme [sicherheitsrelevant] deutlich aufwändiger als für Echtzeit-Fahrplan [nicht sicherheitsrelevant]). Daher müssen verschiedene Anwendungsfälle zur Bewertbarkeit in die Kategorien „sicherheitsrelevant“ und „nicht sicherheitsrelevant“ unterteilt werden.
    - Die Lokalisierung von Fahrzeugen ist in die Kategorien fahrzeug- und streckenseitig zu unterteilen.
    - Ladungsidentifikation ist als Anwendungsfall hinzuzufügen (kombinierbar mit Fahrzeugidentifikation).
2. Expertinnen- und Experteninterview
    - Der Use Case Fahrgastlenkung ist nicht berücksichtigt. Als konkreter Anwendungsfall für Sensorik ergibt sich in dem Zusammenhang die Fahrgastzählung.
3. Expertinnen- und Experteninterview
    - Der Anwendungsfall Umfeldüberwachung bzw. Objekterkennung zur (Teil-)Automatisierung des Bahnbetriebs infrastrukturseitig sollte um die folgenden Sensoren erweitert werden, die z. B. zur Freimeldung von Bahnübergängen verwendet werden:
        - Kamera
        - Infrarot (IR)-Lichtschranke
        - Radarsensor
    - Für die Überwachung des Türenzustands können unter anderem auch Stromsensoren verwendet werden.
    - Die Fahrzeuglokalisierung infrastrukturseitig (sicherheitsrelevant) kann mittels der folgenden Sensoren(-kombinationen) realisiert werden:
        - Balise / Antenne
        - Funkmodul zwischen Bahnsteigtür und Fahrzeug
    - Ladungsidentifikation kann mittels einer Kamera im Gleisbereich realisiert werden.
    - Betriebsstoffüberwachung (Füllstand, Druck) kann mittels eines Wegsensors realisiert werden.
    - Der Anwendungsfall Fahrzeug überwacht Oberleitung kann auch mittels Kameras auf dem Fahrzeugdach oder im Gleisumfeld realisiert werden.
    - Der Anwendungsfall Fahrzeug überwacht Oberbau kann auch mittels Ultraschallsensor realisiert werden.
4. Interview (Autorinnen und Autoren des Berichts)
    - Der Anwendungsfall Infrastruktur überwacht Fahrzeug – sicherheitsrelevant ist um streckenseitige Heißläuferortung (Radsatzlagerzustand) zu ergänzen.
    - Der Anwendungsfall Fahrzeug überwacht Fahrzeug ist um Gleitschutz zu ergänzen.
    - Die Anwendungsfälle Fahrkomfortüberwachung (Beschleunigung) und Fahrzeug überwacht Oberbau (Gleislage) sind um Beschleunigungsmessung mittels Smartphone im Innenraum zu ergänzen.

- Der Anwendungsfall Prüfung der Zugvollständigkeit (Train Integrity Monitoring) ist zu ergänzen. Mögliche Sensoren zur Realisierung sind Funkmodule am Zugende oder Globale Navigationssatellitensysteme (GNSS)-Module an den Zugteilen.

Die Ergebnisse der Interviews wurden mit den Ergebnissen der Literaturrecherche zu einer finalen Liste der Anwendungsfälle von Sensorik im Bahnbereich kombiniert, die im nachfolgenden Kapitel erläutert wird.

4.1.2 Auswertung

Zusammenfassung und Vorsortierung

Die Recherche ergab eine große Anzahl von Anwendungsfällen für Sensorik im Bahnbereich. Die Bewertung sämtlicher Anwendungsfälle durch Expertinnen und Experten im Rahmen einer Online-Umfrage und eines Workshops wäre nicht umsetzbar. Bei einer Umfrage sinkt mit zu großer Länge die Bereitschaft der Teilnehmenden zur vollständigen Beantwortung. Für den Workshop steht nur ein begrenzter Zeitrahmen zur Verfügung (ca. ein Vormittag), sodass die Menge der zu behandelnden Inhalte begrenzt ist. Daher ist eine Reduktion der Anzahl der Anwendungsfälle notwendig. Zunächst wurden die in der Literatur recherchierten Anwendungsfälle zusammengefasst, wobei Mehrfachnennungen gelöscht und sprachliche Variationen vereinheitlicht wurden. Dabei wurden außerdem Anwendungsfälle aussortiert, für die nach Ansicht des Projektteams eines der folgenden Kriterien zutraf:

- Der Anwendungsfall hat keine allgemeine Relevanz:
  Der Anwendungsfall ist eine Nischenlösung (beispielsweise nur für einen kleinen, begrenzten Raum sinnvoll) oder es ist aus anderen Gründen (z. B. ein Anwendungsfall ist regulatorisch definiert) davon auszugehen, dass eine große Mehrzahl der Fachleute den Anwendungsfall als nicht relevant einstuft.
- Der Anwendungsfall ist einfach umsetzbar:
  Die Hürden (z. B. Zulassung, Kosten), die der Realisierung des Anwendungsfalls entgegenstehen, werden als sehr gering eingeschätzt, sodass eine Diskussion mit dem Fachpublikum nicht notwendig ist.
- Der Anwendungsfall berührt das Bahnsystem nur am Rande:
  Die Berührungspunkte mit anderen Branchen (z. B. Bau, Maschinenbau) sind in der Mehrzahl, es handelt sich daher nicht um einen bahnspezifischen Anwendungsfall (z. B. der Einsatz von Sensoren in Maschinen, die zur Fahrzeuginstandhaltung oder zum Gleisbau verwendet werden).

Zudem wurden Anwendungsfälle, die einen ähnlichen Einsatzzweck haben, zusammengefasst. Beispielsweise können aus diversen Gründen verschiedene Zustände der Komponenten des Oberbaus vom Fahrzeug aus überwacht werden. In diesem Fall wurde nicht für jeden Zustand ein Anwendungsfall angelegt, sondern der übergreifende Anwendungsfall „Fahrzeug überwacht Oberbau“ eingeführt. Auf diese Weise wurde auch in anderen Kontexten vorgegangen. Da dieses Vorgehen für einige Anwendungen in hohem Maße und für andere nicht möglich ist, variieren die Anwendungsfälle zwischen hoch aggregierten und einzelnen, sehr spezifischen Fällen, die alleinstehend sind.

Den Anwendungsfällen wurden zur Erläuterung beispielhaft verwendbare Sensoren und die jeweiligen Montageorte zugeordnet. Die Liste dieser Sensoren ist nicht abschließend, sie gibt das Ergebnis von Literaturrecherche und Interviews wieder. Zudem sollte es durch die Angabe der Sensoren und Montageorte für Fachexpertinnen und Fachexperten möglich sein, den Zweck des jeweiligen Anwendungsfalls zu erkennen. Eine ausformulierte Erläuterung der Anwendungsfälle ist daher nicht notwendig. Bei diesem Vorgehen wird davon ausgegangen, dass Fachleute, die anhand der bereitgestellten Informationen nicht in der Lage sind, die Funktionsweise und den Zweck eines Anwendungsfalls zu erkennen, aufgrund mangelnder Vorkenntnisse nicht zur Bewertung des Anwendungsfalls geeignet sind.

Die Anwendungsfälle wurden zudem den in Umfrage und Workshop adressierten Stakeholdergruppen zugeordnet. Die folgenden Gruppen von Stakeholdern innerhalb der Bahnbranche wurden gebildet, um auf Themengebiete spezialisierte Diskussionen im Workshop zu ermöglichen:

- Herstellung Fahrzeug
- Herstellung Infrastruktur
- Instandhaltung Fahrzeug
- Instandhaltung und Betrieb Infrastruktur
- Bahnbetrieb

Mit diesen Gruppen sind die wesentlichen Anwendungsfelder für Sensorik im Bahnbereich abgedeckt. Im Workshop kommen Stakeholder aus diesen Bereichen zusammen, um die jeweiligen Anwendungsfälle zu diskutieren. Dazu wird auch die Vorbewertung in der Umfrage entsprechend dieser Gruppen durchgeführt.

Die Anwendungsfälle wurden daher den Gruppen zugeordnet, wobei jeweils die Installation der Sensoren (z. B. am Fahrzeug -> Gruppe Herstellung Fahrzeug) sowie die Nutzung der entstehenden Daten (z. B. im Bahnbetrieb -> Gruppe Bahnbetrieb) berücksichtigt werden. So wird sichergestellt, dass alle Teilnehmenden an Umfrage und Workshop sich hauptsächlich mit für sie potenziell relevanten Anwendungsfällen befassen.

Feedbackschleifen und Ergebnis

Die durch Zusammenfassung und Vorsortierung der Ergebnisse der Literaturrecherche entstandene Liste wird parallel auf zwei Wegen weiterverarbeitet. Einerseits wird im Rahmen des Kapitels 4.2 der Pretest einer Online-Umfrage erstellt, für den ein vorläufiges Ergebnis ausreichend ist. Andererseits wurde die Liste als Grundlage für die oben beschriebenen Expertinnen- und Experteninterviews verwendet.

Der Pretest der Online-Umfrage wurde von den Bearbeitenden des Projektkonsortiums durchgeführt. Dabei anfallende Anmerkungen zu der Liste der Anwendungsfälle wurden aufgenommen und ggfs. in die Liste eingearbeitet.

Die Liste wurde zudem durch die oben genannten Ergebnisse der Expertinnen- und Experteninterviews ergänzt. Als Ergebnis des Kapitels 4.1 steht die in Tabelle 2 dargestellte, für die Verwendung in Online-Umfrage und Workshop geeignete Liste, aus der auch die Zuordnung zu den Stakeholdergruppen hervorgeht. Demnach konnten 43 Anwendungsfälle identifiziert werden. Für eine bessere Übersicht werden folgende Abkürzungen verwendet: Instandhaltung (IH), Fahrzeug (Fz.) und Infrastruktur (Infra).

TABELLE 2: ANWENDUNGSFÄLLE FÜR SENSORIK IM BAHNBEREICH

Nr.	Anwendungen für Sensorik im Bahnbereich	Beispielhaft verwendete Sensoren	jeweiliger Montageort	Herstellung Fz.	Herstellung Infra	IH Fz.	IH & Betrieb Infra	Bahnbetrieb
1	Umfeldüberwachung bzw. Objekterkennung zur (Teil-) Automatisierung des Bahnbetriebs fahrzeugseitig	(IR-)Kamera, Lidar, Radar, Wärmebildkamera	Fahrzeugfront	x				x
		Beschleunigungssensor	Fahrzeug					

Nr.	Anwendungen für Sensorik im Bahnbereich	Beispielhaft verwendete Sensoren	jeweiliger Montageort	Herstellung Fz.	Herstellung Infra	IH Fz.	IH & Betrieb Infra	Bahnbetrieb
2	Umfeldüberwachung bzw. Objekterkennung zur (Teil-) Automatisierung des Bahnbetriebs infrastrukturseitig	Drucksensor, Kamera, Radar, IR-Lichtschranke	z. B. Bahnübergang		x		x	x
		Aufprallsensoren	Bahnsteig					
3	Fahrzeug überwacht Fahrzeug, z. B.:							
a	Antriebszustand (Diesel)	Temperatursensor	Leistungselektronik, Dieselmotor, Kühlsystem	x		x		
b	Antriebszustand (Elektro)	Stromsensor, piezoelektrischer Wandler, Spannungssensor	elektrischer Antriebsstrang	x		x		
		Temperatursensor	Traktionsbatterie					
c	Rad-Schiene-Kontaktkraft, Heißläufer, Struktur, Fahrdynamik, Gleitschutz	Temperatursensor, Beschleunigungssensor, Drehgeber, Dehnungsmessstreifen (DMS)	Radsatzlagerdeckel	x		x		x
d	Struktur, Neigung, Federung und Dämpfung	Beschleunigungssensor Wegsensor	Wagenkasten und Anbauteile	x		x		
e	Schallemission	Mikrofon	Wagenkasten			x		
f	Türenzustand	DMS, Stromsensor	Türen	x				x
4	Infrastruktur überwacht Fahrzeug – sicherheitsrelevant (z. B. Radlaufflächen, Masse/Überladung, Radsatzlagerzustand)	DMS, Kraftsensor	Schienen		x	x		
		Faseroptischer Sensor, Kamera, Temperatursensor, Laserscanner	Gleisbereich					
5	Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant (z. B. Masse, Schallquellen)	DMS, Kraftsensor	Schienen		x	x		
		Faseroptischer Sensor, Mikrofon	Gleisbereich					
6	Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant (z. B. Zugsicherung)	GNSS (zusätzlich evtl. Drehgeber, Beschleunigungssensor, Kamera, Wirbelstromsensor,	Fahrzeug	x				x

Nr.	Anwendungen für Sensorik im Bahnbereich	Beispielhaft verwendete Sensoren	jeweiliger Montageort	Herstellung Fz.	Herstellung Infra	IH Fz.	IH & Betrieb Infra	Bahnbetrieb
		Ground penetrating RADAR)						
7	Fahrzeuglokalisierung fahrzeugseitig nicht sicherheitsrelevant (z. B. Fahrplan)	GNSS (zusätzlich evtl. Drehgeber, Beschleunigungssensor, Kamera, Wirbelstromsensor, Ground penetrating RADAR)	Fahrzeug	x		x		x
8	Fahrzeuglokalisierung infrastrukturseitig sicherheitsrelevant (z. B. Zugsicherung)	Kamera	z. B. Werkstor		x			x
		Faseroptischer Sensor	Gleisbereich					
		Balise/Antenne	Gleisbereich					
		Funkmodul	Bahnsteigtür (+ Fahrzeug)					
9	Fahrzeuglokalisierung infrastrukturseitig nicht sicherheitsrelevant (z. B. Fahrplan)	Kamera	z. B. Werkstor		x	x		x
		Faseroptischer Sensor	Gleisbereich					
10	Überwachung Bremse (Bremskraft, Temperatur, C-Druck)	Kraftsensor	Bremsge--stänge	x		x		x
		Temperatursensor	Bremssattel					
		Drucksensor	Bremszylinder					
11	Entgleisungsdetektion	Beschleunigungssensor	Drehgestell	x		x		x
12	Fahrzeug-, Ladungsidentifikation	Transponder	Fahrzeug, Ladung			x	x	
		Kamera	Gleisbereich					
13	Betriebsstoffüberwachung (Füllstand, Druck)	Körperschallsensor, Drucksensor, Wegsensor	Tank, Brennstoffzellen	x		x		x
14	Steuerung der Radsatzführung	GNSS-Sensor	Fahrzeug	x		x		
		Wegaufnehmer (Ausdrehung Drehgestell)	Drehgestell					
15	Branddetektion für Löschanlage	Rauchwarnmelder, Feuerwarnmelder	Maschinenraum	x				
16	Energieeinsparung bei Klimatisierung	CO_2-Sensor	Klimaanlage, Innenraum	x				
17	Niveauregulierung des Fahrzeugs zum Bahnsteig	Abstandssensor	Fahrzeug	x				x

Nr.	Anwendungen für Sensorik im Bahnbereich	Beispielhaft verwendete Sensoren	jeweiliger Montageort	Herstellung Fz.	Herstellung Infra	IH Fz.	IH & Betrieb Infra	Bahnbetrieb
	(Erfassung der Bahnsteighöhe)							
18	Steuerung der Bremsverzögerung in Echtzeit	Beschleunigungssensor	Fahrzeug	x				x
19	Ladungsüberwachung (Masse, Vibrationen, Temperatur…) – sicherheitsrelevant (z. B. lastabhängige Bremse)	Magnetsensor, Beschleunigungssensor	Wagenkasten	x				x
		DMS	Drehgestell					
20	Ladungsüberwachung (Masse, Vibrationen, Temperatur…) – nicht sicherheitsrelevant (z. B. Ladungszustand)	Magnetsensor, Beschleunigungssensor	Wagenkasten	x				x
		DMS	Drehgestell					
		Temperatursensor, Feuchtigkeitssensor, Luftdrucksensor	Laderaum					
21	Fahrgastzählung	(IR-)Kamera, Lichtschranke	Türbereich	x				x
		Kraftsensor	Drehgestell/ Fahrwerk, Fahrgastsitze					
22	Fahrkomfortüberwachung (Beschleunigung, Schall Innenraum, Klima Innenraum)	Beschleunigungssensor	Wagenkasten, Sitze, Smartphone im Innenraum			x		x
		Temperatursensor, Hydrometer, Drucksensor, CO_2-Sensor, Mikrofon	Fahrgastraum					
23	Oberleitungsüberwachung	Faseroptischer Sensor, Kraftsensor, Beschleunigungssensor	Stromabnehmer	x	x		x	
		Kamera	Fahrzeugdach, Gleisumfeld					
24	Fahrzeug überwacht Oberbau (z. B. Gleislage, Herzstückzustand, Schwellen, Schiene)	Beschleunigungssensor	Smartphone im Innenraum	x	x		x	
		Beschleunigungssensor, Laser, Gyroskop, Ultraschallsensor, Magnetfeldsensor	Radsatzlager, Fahrwerksbereich					
25	Oberbauüberwachung (z. B. Schienen, Weichen, Schwellen, Gleislage) streckenseitig	Beschleunigungssensor, Drucksensor, Kraftsensor, Wegaufnehmer	Schwelle, Weiche, Schienenfuß		x		x	
		Temperatursensor, Niederschlagssensor, Faseroptischer Sensor	Gleisbereich					
26	Messwagen / Roboter überwacht Infrastruktur (z. B.	Wegsensor, LIDAR, Kamera, Lasersensor	Messwagen, Roboter				x	

Nr.	Anwendungen für Sensorik im Bahnbereich	Beispielhaft verwendete Sensoren	jeweiliger Montageort	Herstellung Fz.	Herstellung Infra	IH Fz.	IH & Betrieb Infra	Bahnbetrieb
	Vegetation, Gleisverschleiß, Tunnelgeometrie, ...)							
27	Fluggerät/Drohne überwacht Infrastruktur (z. B. Vegetation)	Wegsensor, LIDAR, Kamera	Fluggerät/ Drohne				x	
28	Signalüberwachung	Feuchtigkeitssensor, Isolationssensor	Stellwerk		x		x	
29	Unterbauüberwachung	Beschleunigungssensor, Drucksensoren, Feuchtigkeitssensor	Schwelle		x		x	
30	Überwachung von Schallemissionen der Infrastruktur	Beschleunigungssensor, Schwinggeschwindigkeitssensor	Schiene, Schwelle, Gleistragplatte		x		x	
		Mikrofon	Gleisbereich					
31	Weichenferndiagnose	Stromsensoren	Stellwerk		x		x	
32	Überwachung von Brücken und Bauwerken (Kräfte, Druck, Temperatur, Umwelteinwirkungen, Tunnelkonvergenz, ...)	Beschleunigungssensor, Mikrofon, Dehnungssensor, Kraftsensor, Temperatursensor	Tunnel, Brücke, Lärmschutzwand, Bahnhof		x		x	
		Lasersensor	Tunnelwand					
		Neigungssensor, Wegsensor, Windsensor	Fahrleitungsmasten					
33	Diebstahlschutz / Vandalismusüberwachung	Kamera	Fahrzeugtür					x
		Faseroptische Sensoren	Gleis					
		Beschleunigungssensor	Baumaterial					
34	(Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)	Kamera	Werkshalle			x		
35	Prüfung der Zugvollständigkeit (Train Integrity Monitoring)	Funkmodul	Zugende					x
		GNSS-Module	Zugteile					
36	Detektion von Erdrutschen an Böschungen	Neigungssensor	Erdspieß an Böschung		x		x	
37	Auslastung von Park+Ride Parkplätzen ermitteln	GNSS-Sensor	Smartphones von Nutzenden		x		x	
38	Schutz vor Druckschwankungen bei Tunnelfahrt	Drucksensor	Fahrzeugkopf					x

4.2 Workshop zur Bewertung der Use Cases

Ziel des durchgeführten Workshops ist es, die im Ergebnis des Kapitels 4.1 herausgearbeiteten und dort in der vorsortierten Liste zusammengefassten Anwendungsfälle für Sensorik im Bahnsystem durch fachkundige Expertinnen und Experten hinsichtlich ihrer Relevanz bewerten zu lassen und damit eine erste Entscheidungsgrundlage (im Sinne eines Rankings) für die Auswahl einer handhabbaren Menge der „relevantesten“ Use Cases für die Detailanalysen in den weiteren Kapiteln zu schaffen.

Hierfür waren konzeptionelle Arbeiten in einer Vorbereitungsphase erforderlich, in deren Rahmen auch der Relevanzbegriff für die Aufgabenstellung operationalisiert, ein Bewertungsschema erarbeitet und eine Online-Umfrage unter Expertinnen und Experten durchgeführt wurde. Mit den Bewertungsergebnissen wurde ein wichtiges Stimmungsbild zu potenziellen Sensoranwendungen von Branchenexpertinnen und -experten eingeholt. Die Details der Vorbereitungsarbeiten und der Bewertungsergebnisse werden in den folgenden Unterabschnitten beschrieben.

4.2.1 Vorbereitung

Für die gesetzte Aufgabe musste zunächst geklärt werden, was in diesem Kontext unter Relevanz einer Sensoranwendung zu verstehen ist. Dazu wurde, bezogen auf technische Anwendungen im Allgemeinen, eine Schlag- und Stichwortsuche in Literaturdatenbanken und Suchmaschinen (unter Einbeziehung synonymer und ähnlicher Bezeichnungen) vorgenommen. Die Ergebnisse dieser Recherche ließen sich letztlich alle auf zwei Hauptdimensionen einer Relevanz von Anwendungsfällen zurückführen:

1. der (tatsächliche oder erwartbare) **Mehrwert**: konkret für das Projekt die Beantwortung der Frage, welchen Zusatznutzen oder Wertzuwachs ein Sensoreinsatz im jeweiligen Anwendungsfall im Vergleich zum Status Quo bzw. zum Stand der Technik besitzt oder verspricht, und
2. die **Umsetzbarkeit**: konkret für das Projekt die Beantwortung der Frage, wie leicht oder wie schwer der Sensoreinsatz für den jeweiligen Anwendungsfall in der Praxis zu realisieren ist.

Für die beiden Begriffe der Hauptdimensionen wurden im Folgenden mit einer weiteren Schlag- und Stichwortsuche in Literaturdatenbanken bzw. Suchmaschinen gezielt Einzelkriterien für deren Operationalisierung (wieder bezogen auf technische Anwendungen im Allgemeinen) recherchiert, gesammelt, sortiert und diese, in Abstimmung mit ausgewählten Expertinnen und Experten des bestehenden Kontaktnetzwerks, auf die in der nachfolgenden Tabelle 3 aufgeführten Unterpunkte mit Bedeutung für Sensoranwendungen im Bahnsystem aggregiert.

TABELLE 3: EINZELKRITERIEN FÜR MEHRWERT UND UMSETZBARKEIT

Mehrwertkriterien	Umsetzbarkeitskriterien
Minimierung von Instandhaltungskosten	Kosten-Nutzen-Verhältnis
Minimierung sonstiger Betriebskosten	Höhe der Investitionsbedarfe und Finanzierungsquellen
Steigerung der möglichen Streckenkapazitäten oder -geschwindigkeiten	technologischer Reifegrad
Steigerung der Angebotsattraktivität für Bahnkunden	Beherrschbarkeit der Komplexität
Verbesserung von Sicherheitsaspekten	rechtlich-normative Zulässigkeit
Erhöhung der Systemzuverlässigkeit	marktseitige Durchsetzbarkeit
Steigerung von Wettbewerb und Markteffizienz	organisatorische Umsetzbarkeit
Verbesserung der Umweltverträglichkeit	Akzeptanzaussichten

Mehrwertkriterien	Umsetzbarkeitskriterien
Verbesserung der sozialen Nachhaltigkeit	Kompatibilität mit Altsystemen bzw. Aufwand einer Technologiemigration
Vereinfachung und Optimierung von Prozessen	Risiken und Zielkonflikte aus dem Sensoreinsatz
Synergien mit anderen Anwendungen oder Technologien	

Diese recherchierten Grundlagen wurden sodann für die Ableitung eines geeigneten Bewertungsschemas für die Relevanz der Sensoranwendungen genutzt. Aufgrund der Zweidimensionalität und der Überführbarkeit in heruntergebrochene Einzelkriterien bot sich die in der Literatur und Praxis des Strategischen Managements weit verbreitete Portfoliotechnik als nutzbare Methode an. Ein weiteres Argument für diese Methode ist, dass sie die Bewertungsergebnisse mit ihrer einfachen Visualisierung in einer aufgespannten Matrix für die am Workshop teilnehmenden Expertinnen und Experten vergleichsweise einfach und intuitiv erfassbar macht. Das somit entwickelte Mehrwert-Umsetzbarkeit-Portfolio ist in Abbildung 4 dargestellt und weist die nachfolgend beschriebenen Eigenschaften auf.

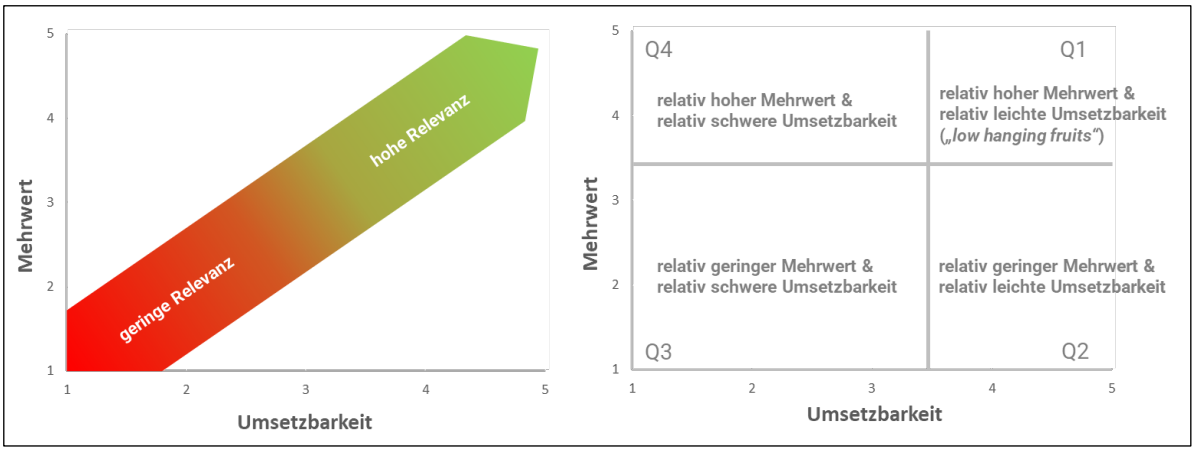


Abbildung 4: Portfolio zur Bewertung der Use Case-Relevanz [TU Chemnitz, BWL III]

Die Ausprägungen der Sensoranwendungen in den beiden Dimensionen Mehrwert und Umsetzbarkeit werden auf einer einheitlichen Skala von 1 (geringster Mehrwert bzw. schwerste Umsetzbarkeit) bis 5 (höchster Mehrwert bzw. leichteste Umsetzbarkeit) bewertet. Grundsätzlich sind eine gewichtete Bewertung und Aggregation der Einzelkriterien umsetzbar. Um die Handhabung des Bewertungsschemas für die eingebundenen Fachexpertinnen und Fachexperten einfach zu halten, wurde jedoch darauf verzichtet. Das heißt, die beiden Hauptdimensionen der Relevanz wurden jeweils gesamthaft zur Bewertung mit 1 bis 5 Punkten gestellt. Die jeweiligen Einzelkriterien wurden dabei nur als ergänzende Information zu den Relevanzdimensionen benannt.

Je weiter rechts oben (in Richtung einer 5-5-Bewertung) eine Sensoranwendung aufgrund ihrer durchschnittlichen Bewertung durch die Expertinnen und Experten im Portfolio positioniert werden kann, umso höher ist ihre Gesamtrelevanz zu interpretieren. Je weiter links unten (in Richtung einer 1-1-Bewertung) sie zu verorten ist, umso geringer ist ihre Gesamtrelevanz einzuschätzen.

Um detailliertere Aussagen zu treffen und eine Clusterung der relevanzbewerteten Sensoranwendungen vornehmen zu können, wurde durch Einzeichnung der Mediane (Zentralwerte) der jeweiligen Dimensionsbewertungen auf den Koordinatenachsen eine 4-Felder-Matrix gebildet. Für die vier Quadranten (Q) dieser Matrix lassen sich, wie in der Literatur des Strategischen Managements üblich, situationsabhängig zu interpretierende Normstrategien mit Empfehlungscharakter ableiten:

- Q1 mit relativ hohem Mehrwert und relativ leichter Umsetzbarkeit (sog. „low hanging fruits“): Empfehlung, die hier eingeordneten Sensoranwendungen in die Praxis umzusetzen;
- Q2 mit relativ geringem Mehrwert und relativ leichter Umsetzbarkeit: Empfehlung zu fallspezifischen Entscheidungen und einer selektiven Umsetzung in die Praxis (z. B. Mitnahme geringer, aber einfach realisierbarer Mehrwerte von Anwendungen, die sich gut in ein strategisches Gesamtgefüge einordnen);
- Q3 mit relativ geringem Mehrwert und relativ schwerer Umsetzbarkeit: Empfehlung, auf eine Umsetzung in die Praxis (zumindest vorerst) zu verzichten;
- Q4 mit relativ hohem Mehrwert und relativ schwerer Umsetzbarkeit: Empfehlung zu fallspezifischen Entscheidungen und einer selektiven Umsetzung in die Praxis (z. B. Arbeit an der Senkung oder Überwindung von Umsetzungshürden für Anwendungen, die sich gut in ein strategisches Gesamtgefüge einordnen).

In einem nächsten Schritt wurde für die Anwendung des soeben dargestellten Bewertungsschemas ein Erhebungsdesign erarbeitet. Da die in Kapitel 4.1 zusammengetragene Gesamtliste von Anwendungsfällen für Sensorik im Bahnsystem mit 43 Eintragungen sehr umfangreich ist, wurde es als unrealistisch eingeschätzt, hierfür die gewünschten Bewertungen im Rahmen eines einzelnen Workshops zu erheben. Deshalb wurde in der Workshopvorbereitungsphase eine Vorabbewertung der Sensoranwendungen unter Rückgriff auf das Bewertungsschema konzipiert, geplant, umgesetzt und ausgewertet. Die Vorabbewertung sollte dabei zwei Zielen dienen: (1) den Workshopteilnehmenden sind sowohl die zu durchdenkenden Use Cases als auch das Bewertungsschema vorab bekannt und (2) im Workshop liegt als Ausgangspunkt bereits ein erstes Stimmungsbild der wesentlichen Stakeholder zur Use Case-Relevanz und zu maßgeblichen Beurteilungskriterien vor.

Zur Umsetzung der Vorabbewertung wurde eine Online-Umfrage entwickelt und in der Software LimeSurvey implementiert. Es wurden bewusst nicht nur die angemeldeten Workshopteilnehmenden gebeten, die Umfrage auszufüllen. Vielmehr wurde die Umfrage an alle 179 Fachexpertinnen und -experten gestreut, die zuvor innerhalb des bestehenden Kontaktnetzwerks des Projektkonsortiums zusammengetragen wurden, um eine möglichst breite Basis der Relevanzbewertungen zu erhalten. Kern der Umfrage waren zwei Tabellen, in welchen für eine Use Case-Liste die beiden Relevanzdimensionen auf der Skala von 1 bis 5 zu bewerten und zusätzlich Beurteilungskriterien für die Relevanz anzugeben waren. Die beiden Kernfragen lauteten diesbezüglich:

- Bewerten Sie aus Ihrer heutigen Sicht den **Mehrwert** der einzelnen Sensoranwendungen im Bahnsystem in der nachfolgenden Auflistung und wählen Sie jeweils das primär ausschlaggebende Kriterium für Ihre Bewertung aus.
- Bewerten Sie nun für die gleiche Auflistung von Sensoranwendungen aus Ihrer heutigen Sicht die **Umsetzbarkeit** der einzelnen Sensoranwendungen und wählen Sie jeweils das primär ausschlaggebende Kriterium für Ihre Bewertung aus.

Für die Beurteilungskriterien wurden in Auswahllisten die recherchierten Kriterien von Tabelle 3 vorgeschlagen und es konnten auch eigene, andere Kriterien benannt werden. Neben den Kernfragen wurden in einem vorangestellten, allgemeinen Teil Fragen zur generellen Einordnung der Antwortenden gestellt. Diese Selbsteinordnung wurde auch für eine Zuordnung zu einer von fünf Stakeholdergruppen genutzt:

a. Herstellung von Schienenfahrzeugen,
b. Instandhaltung von Schienenfahrzeugen,
c. Bahnbetrieb,
d. Herstellung von Schieneninfrastruktur sowie
e. Betrieb und Instandhaltung von Schieneninfrastruktur.

Um die Beantwortungszeit der Umfrage in einem akzeptablen Rahmen zu halten, wurde für jede dieser Gruppen eine gekürzte Version der gesamten Anwendungsliste erzeugt, in welcher nur gruppenrelevante Use Cases auftauchen, und zur Bewertung gestellt. Vor der eigentlichen Umfragedurchführung fand ein Pretest durch alle Konsortiumsmitglieder und ausgewählte Testanwenderinnen und -anwender statt, mit dessen Hilfe verbliebene Unklarheiten und Fehler bereinigt werden konnten. Die Online-Umfrage wurde mit einer Laufzeit von drei Wochen in den Kalenderwochen 27 bis 30 des Jahres 2022 durchgeführt und sie führte zu einem Rücklauf von 29 vollständig ausgefüllten Online-Fragebögen (dies entspricht einer Rücklaufquote von 16 %).

Der zweite Teil des Erhebungsdesigns betraf die Ausgestaltung des Workshops selbst. Nach Abstimmungen zu den organisatorischen Rahmenbedingungen mit dem hierzu betrauten Smart Rail Connectivity Campus (SRCC), stand (nach Abzug der Mittagspause) ein Zeitrahmen von ca. vier Stunden für den Workshop zur Verfügung. Dieser wurde in drei Teile aufgeteilt:

- Teil 1: Vorstellung des Projektes, der Zwischenergebnisse (insbesondere der Ergebnisse der Vorabbewertung der Use Case-Relevanz) und des Vorgehens der Workshoparbeit,
- Teil 2: Moderierte Kleingruppendiskussionen in Orientierung an zuvor hergeleiteten Stakeholdergruppen (Kern der Workshoparbeit) und
- Teil 3: Konsolidierung der Workshopergebnisse und gemeinsame Abschlusspaneldiskussion der Gruppenmoderatoren und Gruppenmoderatorinnen mit dem Publikum.

Für die Workshoparbeit in moderierten Kleingruppen wurden 90 Minuten Zeit angesetzt und zwei Ziele festgelegt: (1) Priorisierung von zwei Sensoranwendungen aus der jeweiligen Liste der Stakeholdergruppe für eine tiefere Auseinandersetzung im Anschluss sowie (2) Diskussion dieser beiden Sensoranwendungen in der Gruppe mit Fokus auf erwartete Mehrwerte und die erwartete Umsetzbarkeit in die Praxis (und damit Einordnung in das zweidimensionale Bewertungsportfolio).

Als methodische Hilfsmittel zur Erreichung dieser Ziele wurden folgende Medien genutzt:

- für die Priorisierung der Anwendungen: gruppenspezifische Bewertungsportfolios aus der Online-Umfrage, deren Ergebnisse die jeweiligen Top-3-Use Cases der Vorabbewertung liefern, sowie an alle teilnehmenden Expertinnen und Experten ausgegebene Klebepunkte (jeweils 3), welche verteilt auf diese oder zwei weitere Use Cases der Gruppenliste den Ausschlag für die Gruppenpriorisierung geben,
- für die Diskussion der Sensoranwendungen: vorbereitete Anwendungssteckbriefe mit vorgegebenen und gemeinsam auszufüllenden Beschreibungsmerkmalen.

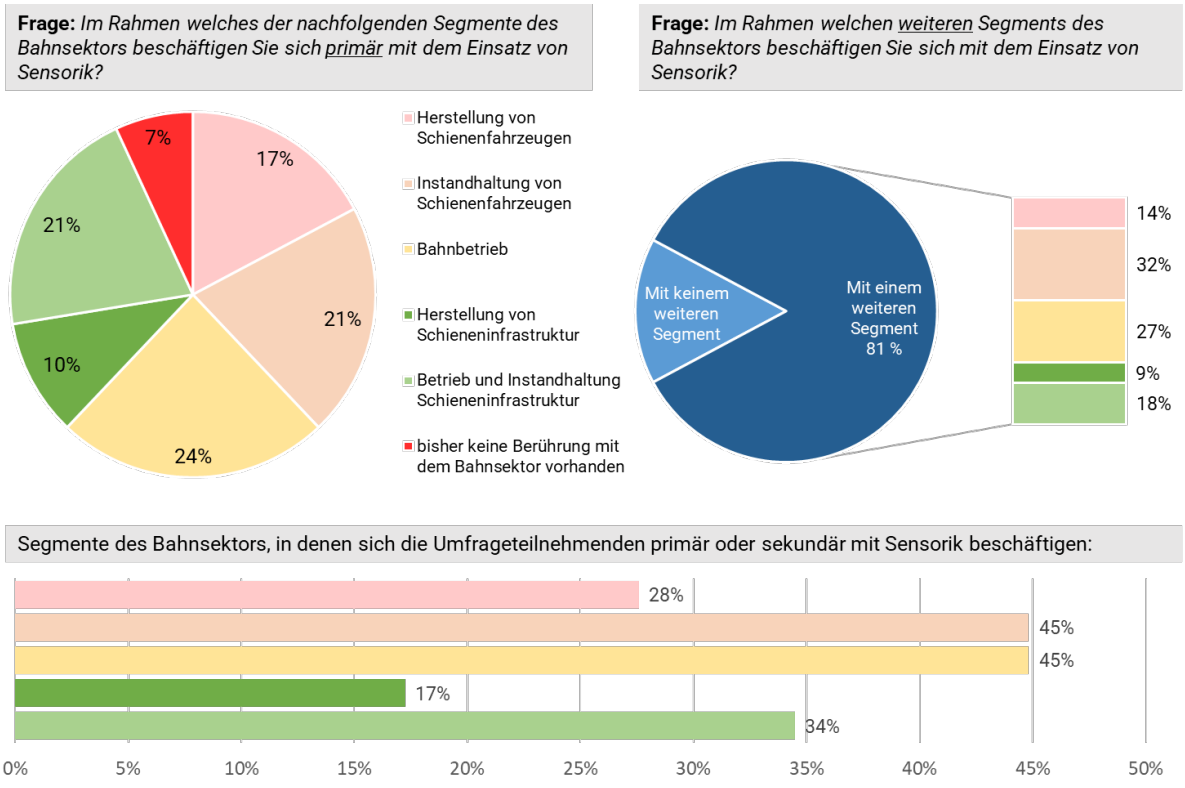
Die gruppenübergreifende Konsolidierung der Workshopergebnisse in Teil 3 des Workshops ermöglichte eine perspektivenübergreifende Einschätzung und Diskussion der insgesamt sechs beleuchteten Use Cases. Für den Workshopabschluss erfolgte nochmals mit Hilfe von Klebepunkten eine Bewertung dieser sechs Use Cases. Dafür hatte jede Experin bzw. jeder Experte einen Klebepunkt für den am einfachsten umzusetzenden Use Case zu verteilen und einen weiteren für den, welcher den größten Mehrwert verspricht.

4.2.2 Ergebnisse

Nachfolgend werden zunächst die Ergebnisse der Vorabbewertung mittels der Online-Umfrage dargelegt. Die Umfrageteilnehmenden repräsentieren 26 Unternehmen und je ein Vertreter aus den Bereichen Behörden/öffentliche Institutionen, Verbände und Interessensgruppen sowie Forschungseinrichtungen. Sie rechnen sich selbst zu 62 % Führungskräften bzw. Referentinnen und Referenten, zu 31 % Spezialistinnen und Spezialisten bzw. Analytikerinnen und Analytikern und zu 7 % Projektleiterinnen

und Projektleitern zu. Branchenseitig ordnen sich 72 % der Kategorie „Bahnindustrie und Eisenbahnunternehmen“ und 38 % der „Bereitstellung von Sensorik und IT“ zu (Mehrfachnennung möglich). Auf die fünf bereits genannten Stakeholdergruppen sind die Umfrageteilnehmenden relativ gleichmäßig verteilt (siehe dazu Abbildung 5). Mit dem Einsatz von Sensorik beschäftigen sich primär 17 % im Rahmen der Herstellung von Schienenfahrzeugen, 21 % im Rahmen der Instandhaltung von Schienenfahrzeugen, 24 % im Rahmen des Bahnbetriebs, 10 % im Rahmen der Herstellung von Schieneninfrastruktur sowie 21 % im Rahmen des Betriebs und der Instandhaltung von Schieneninfrastruktur. Die überwiegende Mehrheit (81 %) beschäftigt sich in mehr als einem dieser Segmente mit dem Einsatz von Sensorik. Davon nennen als weiteres Segment 14 % die Herstellung von Schienenfahrzeugen, 32 % die Instandhaltung von Schienenfahrzeugen, 27 % den Bahnbetrieb, 9 % die Herstellung von Schieneninfrastruktur sowie 18 % den Betrieb und die Instandhaltung von Schieneninfrastruktur. Unter Berücksichtigung dieser Mehrfachnennungen beschäftigen sich 28 % der Umfrageteilnehmenden im Rahmen der Herstellung von Schienenfahrzeugen, je 45 % im Rahmen der Instandhaltung von Schienenfahrzeugen und des Bahnbetriebs, 17 % im Rahmen der Herstellung von Schieneninfrastruktur und 34 % im Rahmen des Betriebs und der Instandhaltung von Schieneninfrastruktur mit dem Einsatz von Sensorik. 7 % der Umfrageteilnehmenden besitzen bisher keine Berührung mit dem Bahnsektor. Bei diesen besteht auch eine Unsicherheit über einen möglichen Einstieg in den Bahnsektor. Als Gründe hierfür wurden die generelle Schwerfälligkeit des Bahnsektors sowie unzureichende eigene Kenntnisse benannt.

Abbildung 5: Selbsteinordnung der Umfrageteilnehmenden [TU Chemnitz, BWL III]



Gefragt nach den ausschlaggebenden Einzelkriterien für den Mehrwert von Sensoranwendungen wurden vor allem die Verbesserung von Sicherheitsaspekten (19 %), die Erhöhung der Systemzuverlässigkeit (16 %), die Minimierung von Instandhaltungskosten (15 %) und die Steigerung der Angebotsattraktivität für Bahnkundinnen und -kunden (10 %) genannt. Antworten auf die Frage nach den ausschlaggebenden Einzelkriterien für die Umsetzbarkeit von Sensoranwendungen im Bahnsektor wurden sehr stark vom Kosten-Nutzen-Verhältnis (29 %) und vom technologischen Reifegrad (26 %) dominiert. Insgesamt ließen sich alle der in Tabelle 3 enthaltenen Kriterien (die an dieser Stelle nicht noch einmal genannten mit

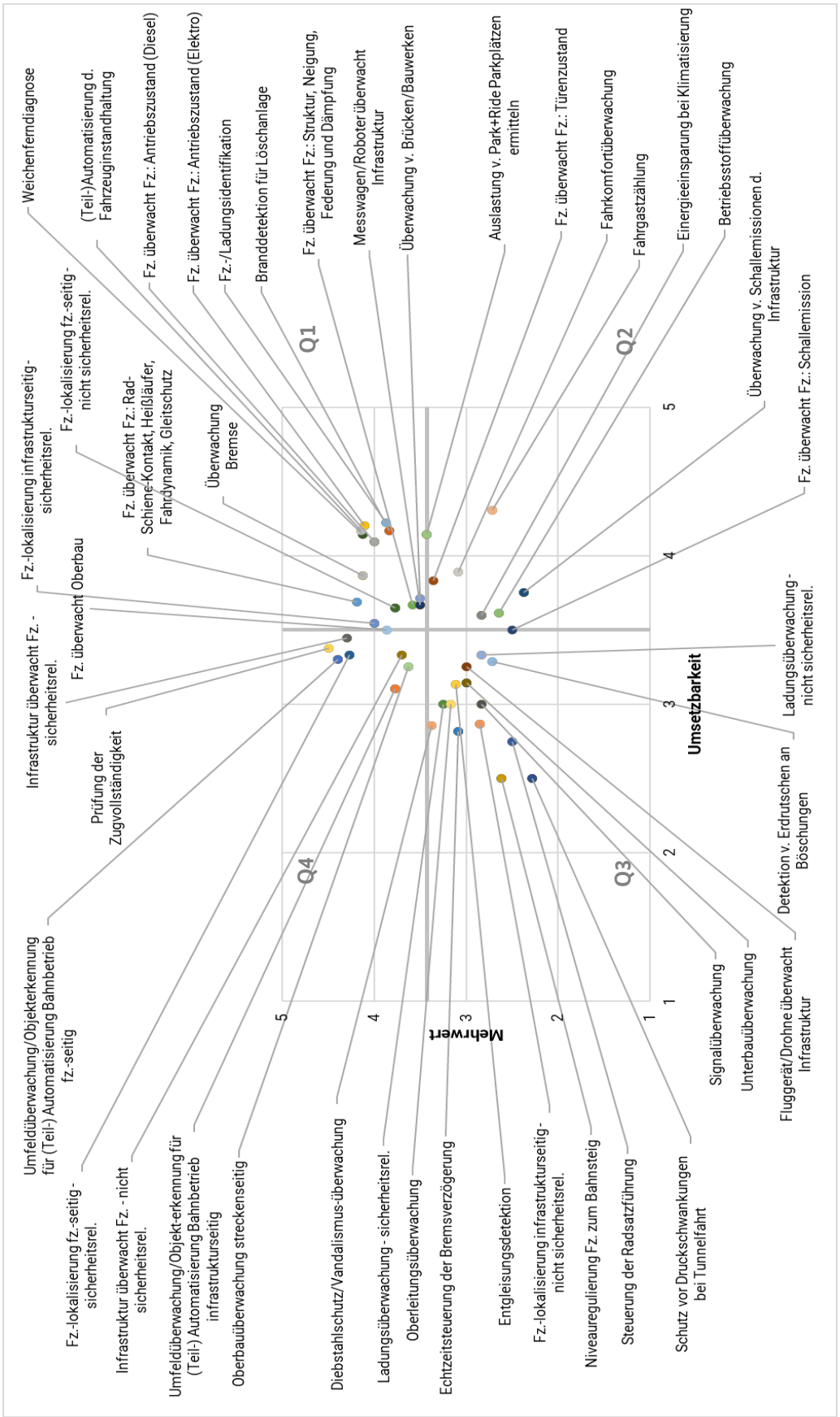
deutlich geringerer Häufigkeit) in den Expertinnen- und Expertenantworten wiederfinden (vgl. Tabelle 4). Knapp 20 % der Umfrageteilnehmenden benannten selbst eigene (nicht zur Auswahl vorgegebene) Relevanzkriterien. Dabei handelte es sich im Wesentlichen aber um Konkretisierungen der zur Auswahl gestellten Kriterien oder um inhaltlich eng verwandte (z. B. die Bahnfestigkeit von Sensoren, die Erfüllung von Sicherheitsnachweisen sowie die Entlastung der Personalbedarfssituation). Insgesamt konnten die Ergebnisse der Literaturrecherche zu Relevanzkriterien mit diesem Teil der Umfrage bestätigt und hinsichtlich der Kriterienbedeutung gewichtet werden.

TABELLE 4: HÄUFIGKEITEN DER NENNUNG AUSSCHLAGGEBENDER RELEVANZKRITERIEN

Mehrwertkriterien		Umsetzbarkeitskriterien	
Minimierung von Instandhaltungskosten	15 %	Kosten-Nutzen-Verhältnis	29 %
Minimierung sonstiger Betriebskosten	5 %	Höhe der Investitionsbedarfe und Finanzierungsquellen	5 %
Steigerung der möglichen Streckenkapazitäten oder -geschwindigkeiten	5 %	technologischer Reifegrad	26 %
Steigerung der Angebotsattraktivität für Bahnkunden	10 %	Beherrschbarkeit der Komplexität	6 %
Verbesserung von Sicherheitsaspekten	19 %	rechtlich-normative Zulässigkeit	5 %
Erhöhung der Systemzuverlässigkeit	16 %	marktseitige Durchsetzbarkeit	2 %
Steigerung von Wettbewerb und Marktefizienz	2 %	organisatorische Umsetzbarkeit	2 %
Verbesserung der Umweltverträglichkeit	2 %	Akzeptanzaussichten	3 %
Verbesserung der sozialen Nachhaltigkeit	1 %	Kompatibilität mit Altsystemen bzw. Aufwand einer Technologiemigration	2 %
Vereinfachung und Optimierung von Prozessen	3 %	Risiken und Zielkonflikte aus dem Sensoreinsatz	2 %
Synergien mit anderen Anwendungen oder Technologien	2 %		

Die Umfrageergebnisse der Relevanzbewertungen aller 43 Sensoranwendungen aus der Gesamtliste hinsichtlich der beiden Dimensionen Mehrwert und Umsetzbarkeit sind in der nachfolgenden Portfoliodarstellung (Abbildung 6) visualisiert. Die meisten Anwendungen haben absolut betrachtet eine positive Bewertung hinsichtlich beider Dimensionen erhalten, erkennbar daran, dass die Mehrheit oberhalb einer 3-3-Bewertung (welche auf einer Skala von 1 bis 5 den Durchschnitt repräsentieren würde) positioniert ist. Das zeigt, dass die befragten Expertinnen und Experten den Großteil der in Kapitel 4.1 recherchierten Anwendungen als bedeutsam ansehen. Mit Hilfe der ermittelten Medianwerte (3,43 für den Mehrwert und 3,50 für die Umsetzbarkeit) konnten die vier zuvor beschriebenen Portfolioquadranten gebildet werden.

Abbildung 6: Umfrageergebnisse zur Use Case-Bewertung [TU Chemnitz, BWL III]



Im hochrelevanten Q1 (relativ hoher Mehrwert & relativ leichte Umsetzbarkeit) lassen sich vor allem sehr viele der fahrzeuginternen Sensoranwendungen zur Zustandsüberwachung von Fahrzeugsubsystemen (*Fahrzeug überwacht Fahrzeug*) finden. Im Q2 (relativ geringer Mehrwert & relativ leichte Umsetzbarkeit) wurden überwiegend „Nice-to-Have"-Anwendungen, wie die Betriebsstoff-, Komfort- und Schallemissionsüberwachung oder eine Fahrgastzählung, eingeordnet. Im etwas weniger attraktiv erscheinenden Q3 (relativ geringer Mehrwert & relativ schwere Umsetzbarkeit) wurden vergleichsweise viele infrastrukturseitige Überwachungsanwendungen (z. B. für Oberleitung, Signale, Unterbau, Böschungen) verortet. Im Q4 (relativ hoher Mehrwert & relativ schwere Umsetzbarkeit) sind vor allem Anwendungen des Bereichs *Infrastruktur überwacht Fahrzeug* und die *Umfeldüberwachung bzw. Objekterkennung für eine (Teil-)Automatisierung des Bahnbetriebs* zu finden. Die nach den einzelnen Stakeholdergruppen gefilterten Varianten des in Abbildung 6 dargestellten Gesamtportfolios ermöglichten einen guten Einstieg in die Workshoparbeit und die damit verbundenen Diskussionen.

Im Rahmen der Online-Umfrage bestand die Möglichkeit weitere Hinweise und Gedanken zu sensorbasierten Technologien und Sensoranwendungen im Bahnsektor mitzuteilen. Die wichtigsten getätigten Aussagen der Umfrageteilnehmenden waren hierbei:

- die Erwartung eines Initialzündungseffekts einer mehrwertgenerierenden Sensorerstanwendung für weitere, folgende Sensoranwendungen, welche dann nur noch überschaubare Mehrkosten verursachen werden;
- die Betonung des Bestehens großer Herausforderungen, insbesondere für Anwendungen der (Teil-)Automatisierung des Bahnbetriebs, z. B. die Reichweiten fahrzeugseitiger Sensoren in Kurven/an Kuppen und ihre Robustheit, die derzeitige Unmöglichkeit bzw. Schwierigkeit der Sicherheitsnachweisführung für bestimmte Sensorsysteme (insbesondere alle, die Machine Learning einsetzen) und in Verbindung mit diesen Herausforderungen und Forschungsbedarfen;
- die Einschätzung, dass eine besser organisierte, eng kooperierende wissenschaftliche Community für die Thematik gebraucht wird (u. a. um offene Standards zu entwickeln und von bzgl. Sensorik weiter entwickelten Branchen zu lernen) und dass die Hürden einer diesbezüglichen Forschungsförderung gesenkt werden müssen.

Im Folgenden werden die Ergebnisse des eigentlichen Workshops zusammengefasst. Ursprünglich war vorgesehen, für jede der fünf Stakeholdergruppen eine eigene Diskussionsgruppe der Expertinnen und Experten im Workshop zu bilden. Aufgrund kurzfristiger Absagen der Teilnahme am Workshop mussten die Stakeholdergruppen weiter zusammengefasst werden, um in jeder Gruppe eine ausreichende Teilnehmendenzahl zu erreichen:

- Gruppe 1 [(a) + (b)]: Herstellung und Instandhaltung von Schienenfahrzeugen, sieben Expertinnen und Experten
- Gruppe 2 [(c)]: Bahnbetrieb, fünf Expertinnen und Experten
- Gruppe 3 [(d) + (e)]: Herstellung, Instandhaltung und Betrieb von Schieneninfrastruktur, sechs Experten und Expertinnen

Bei der Gruppenzusammensetzung wurde darauf geachtet, dass sowohl die potenziellen Sensoranwender des jeweiligen Bahnsegments als auch Bereitsteller von Sensorik und IT repräsentiert sind. Im jeweils ersten Teil der Kleingruppendiskussionen wurden je Gruppe zwei Sensoranwendungen (aus gruppenspezifischen Teillisten) für eine tiefere Auseinandersetzung im Anschluss priorisiert (siehe Abbildung 7).

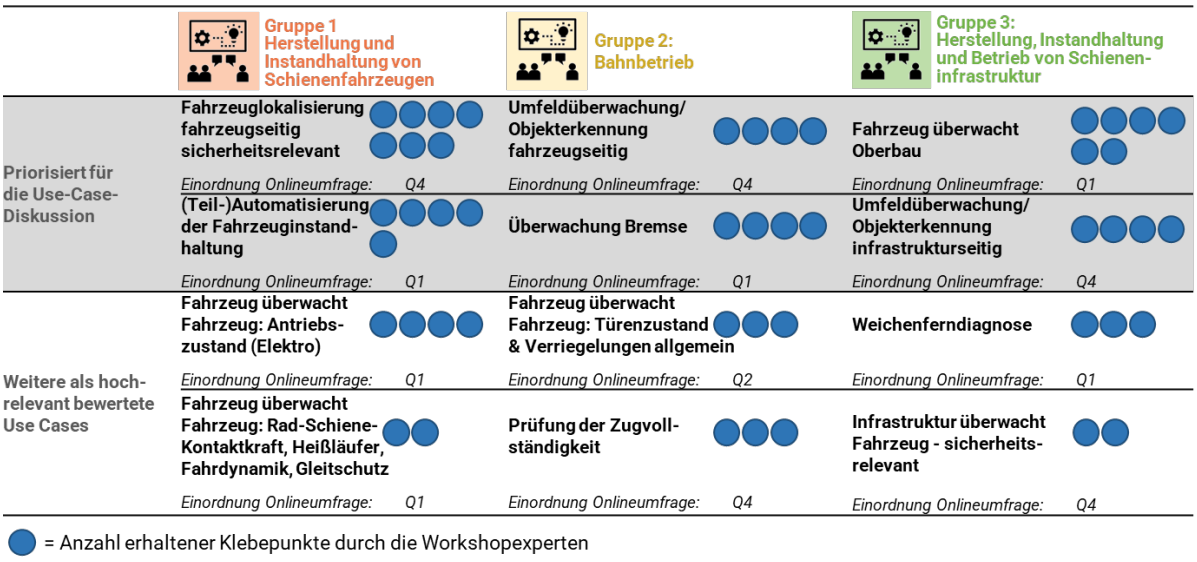


Abbildung 7: Priorisierung von Sensoranwendungen im Workshop [TU Chemnitz, BWL III]

Die für die Diskussion priorisierten Anwendungen sind:

- *Fahrzeuglokalisierung fahrzeugseitig, sicherheitsrelevant* und *(Teil-)Automatisierung der Fahrzeuginstandhaltung* (in Gruppe 1),
- *Umfeldüberwachung/Objekterkennung für (Teil-)Automatisierung des Bahnbetriebs, fahrzeugseitig* und *Überwachung Bremse* (in Gruppe 2) sowie
- *Fahrzeug überwacht Oberbau* und *Umfeldüberwachung/Objekterkennung für (Teil-)Automatisierung des Bahnbetriebs, infrastrukturseitig* (in Gruppe 3).

Sie wurden durch die Online-Umfrage in der Vorabbewertung je zur Hälfte den Quadranten Q1 und Q4 des Portfolios zugeordnet. Dies bestätigt zum einen die mehrwertseitige Relevanzeinschätzung – die Workshopteilnehmenden priorisierten keine Use Cases, welchen vorab nur vergleichsweise geringe Mehrwerte zugestanden wurden. Zum anderen wurde damit deutlich, dass für die Expertinnen und Experten nicht nur leicht umsetzbare Sensoranwendungen von Interesse sind, sondern auch solche, die einen großen Nutzen versprechen, aber noch mit hohen Umsetzungshürden verbunden sind. Gerade bei diesen gilt es, bisher nicht nutzbare Potenziale durch gezielte Maßnahmen erschließbar zu machen. Neben den sechs priorisierten Use Cases sind im unteren Teil von Abbildung 7 auch alle weiteren Sensoranwendungen aufgeführt, die im Rahmen der Relevanzdiskussionen in den Kleingruppen mehr als einen Klebepunkt von den Teilnehmenden erhielten. Hierzu zählen einige Use Cases der Oberkategorie *Fahrzeug überwacht Fahrzeug* sowie die *Weichenferndiagnose*, die *Prüfung der Zugvollständigkeit* und sicherheitsrelevante Anwendungen, in denen die Infrastruktur das Fahrzeug überwacht. Mit einer (nah am Medianwert liegenden) Ausnahme trifft die obige Aussage zur Verortung in den Portfolioquadranten Q1 oder Q4 auch für diese weiteren, im Workshop als relevant bewerteten Use Cases zu.

In den Kleingruppendiskussionen zu den jeweils zwei priorisierten Use Cases kamen die unterschiedlichen Sichtweisen und Wissensstände von potenziellen Sensoranwendern der Bahnindustrie sowie den Bereitstellern von Sensorik und IT zur Sprache. Anhand der vorbereiteten Anwendungssteckbriefe wurden der Hauptzweck bzw. Einsatzszenarien, primäre Teilaufgaben bzw. Teilfunktionen und die beteiligten bzw. einzubindenden Akteure umrissen, ausschlaggebende Mehrwert- und Umsetzbarkeitskriterien identifiziert und für den Use Case bewertet sowie einzusetzende Sensortechnologien, Voraussetzungen, Chancen und Risiken der Anwendung erfasst. Zudem erfolgte auch noch einmal eine Verortung der Use Cases im Bewertungsportfolio. Dabei zeigte sich, dass eine Kriteriengewichtung notwendig ist, um zu

einer konsistenten Gesamtbewertung zu gelangen. Die ausgefüllten Anwendungssteckbriefe sind im Anhang 13.1 zu finden.

Neben den genannten (Pflicht-)Punkten der Anwendungssteckbriefe wurden in den Kleingruppendiskussionen weitere Fragestellungen diskutiert, insbesondere:

- welche Anwendungsvarianten bzw. konkreten Einsatzszenarien bereits gängige Praxis darstellen und wo es Unterschiede zu verwandten Branchen, z. B. Automotive-Industrie und Maschinenbau, gibt;
- welche Herausforderungen und Forschungsbedarfe noch existieren bzw. welche schon als gelöst gelten;
- welche aktuellen Treiber und Trends dazu führen, dass der jeweilige Use Case an Bedeutung gewinnt (z. B. Umgang mit Personalmangel, Bedarf höherer Streckenverfügbarkeiten, datengetriebene Geschäftsmodelle, ETCS-Ausbau, ATO, DAK);
- welche Gemeinsamkeiten und Unterschiede es für ein Personenverkehrs- und für ein Güterverkehrsszenario des jeweiligen Use Cases gibt und
- welche Gemeinsamkeiten und Unterschiede es in verschiedenen geographischen Märkten (innerdeutsch vs. grenzüberschreitend; international) gibt.

Neben der Zuverlässigkeit von Sicherheitsfunktionen (entsprechend der Sicherheitsintegritätslevel) und der Migrationsfähigkeit bestehender Systeme wird vor allem in der Etablierung eines funktionierenden „Business Cases“ für die Sensoranwendungen noch eine häufige Herausforderung gesehen, was die Ergebnisse der Vorfeldrecherchen und der Vorabbewertung mittels Online-Umfrage bestätigt. Dazu gehört zum einen, dass der Sensoreinsatz insgesamt wirtschaftlich sein muss (Kosten-Nutzen-Verhältnis), und zum anderen, dass bei einer Beteiligung unterschiedlicher Stakeholder auch ein ausreichender Anreiz oder Marktmechanismus existiert, der dazu führt, dass Marktakteur A für Marktakteur B eine entsprechende Dienstleistung erbringt (z. B. ein Eisenbahnverkehrsunternehmen überwacht mit seinen Fahrzeugen den Oberbau für Infrastrukturbetreiber).

Nach der Vorstellung aller sechs im Workshop näher betrachteten Use Cases und ihrer Steckbriefinhalte durch die jeweiligen Kleingruppenmoderatorinnen und -moderatoren und der anschließenden gruppenübergreifenden Diskussion im Plenum, erfolgte deren finale Relevanzbewertung durch alle anwesenden Expertinnen und Experten – diesmal getrennt nach den beiden Dimensionen Mehrwert und Umsetzbarkeit (siehe Abbildung 8).

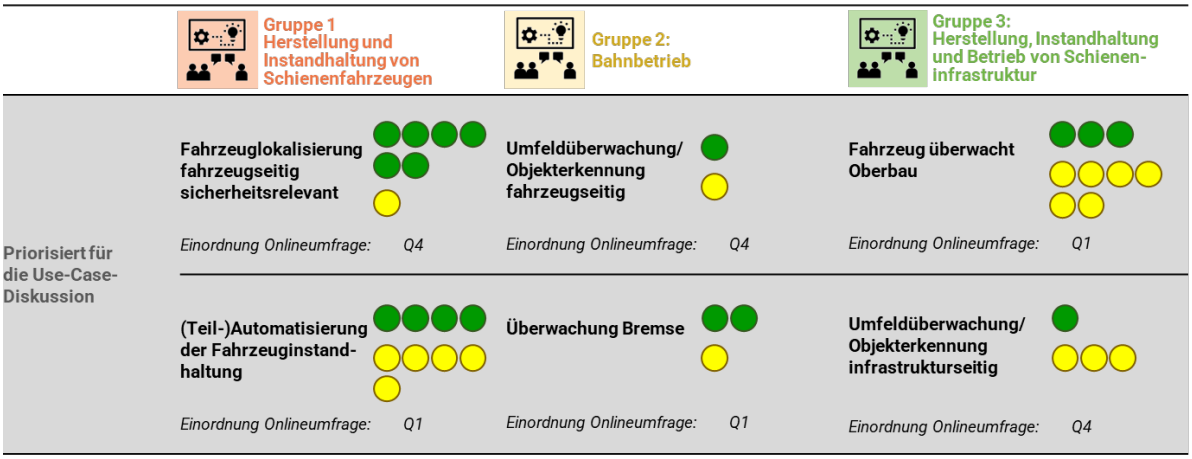


Abbildung 8: Abschließende Bewertung priorisierter Sensoranwendungen im Workshop [TU Chemnitz, BWL III]

Die höchsten Mehrwerte wurden dabei von den Expertinnen und Experten in der *Fahrzeuglokalisierung fahrzeugseitig, sicherheitsrelevant*, in der *(Teil-)Automatisierung der Fahrzeuginstandhaltung* und in der Anwendung *Fahrzeug überwacht Oberbau* gesehen. Bei den beiden letztgenannten wird auch die Umsetzbarkeit als besonders leicht eingeschätzt, was sich mit den Bewertungen der Vorabbewertung (Verortung innerhalb Q1) deckt.

Die Ergebnisse der Vorabbewertung und des Workshops wurden im Nachgang dafür verwendet, mit Blick auf die einzelnen Aufgabenstellungen der weiteren Arbeitsinhalte und in enger Abstimmung mit dem DZSF als Auftraggeber eine Use Case-Auswahl für Detailanalysen zu treffen. Dabei spielte neben der reinen Relevanzeinschätzung auch die Ausgewogenheit der betrachteten Use Cases eine Rolle. In der nachfolgenden Tabelle 5 sind die sieben ausgewählten Use Cases aufgelistet.

TABELLE 5: AUSGEWÄHLTE USE CASES FÜR DETAILANALYSEN

Nr.	Anwendungen für Sensorik im Bahnbereich	Zuordnung der Sensorik zum Teilsystem Bahn	Einschätzung der relativen Umsetzbarkeit (Experten- und Expertinnenumfrage)	Gesamtrelevanzeinschätzung (Umfrage + Workshop (WS))	Priorisierung aus Perspektive der Aufgaben von ... Kapiteln
3b	Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)	Fahrzeug	leicht	B (= im WS hohe Bewertung erhalten)	3
3f	Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen	Fahrzeug	leicht	B (= im WS hohe Bewertung erhalten)	2
5	Infrastruktur überwacht Fahrzeug - nicht sicherheitsrelevant	Infrastruktur	schwer	C (= nur in Umfrage hoch bewertet)	3
6	Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant	Fahrzeug	schwer	A (= im WS für Diskussion priorisiert)	3

Nr.	Anwendungen für Sensorik im Bahnbereich	Zuordnung der Sensorik zum Teilsystem Bahn	Einschätzung der relativen Umsetzbarkeit (Experten- und Expertinnenumfrage)	Gesamtrelevanzeinschätzung (Umfrage + Workshop (WS))	Priorisierung aus Perspektive der Aufgaben von ... Kapiteln
24	Fahrzeug überwacht Oberbau	Fahrzeug	leicht	A (= im WS für Diskussion priorisiert)	4
31	Weichenferndiagnose	Infrastruktur	leicht	B (= im WS hohe Bewertung erhalten)	1
34	(Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)	Infrastruktur	leicht	A (= im WS für Diskussion priorisiert)	2

Darunter finden sich sowohl Sensoranwendungen im Fahrzeug (vier Stück) als auch in der Infrastruktur (drei) sowie voraussichtlich schwer (zwei) und leicht (fünf) umsetzbare. Drei der Use Cases wurden bereits detailliert im Workshop diskutiert und erhielten dort abschließend die besten Bewertungen hinsichtlich des Mehrwertes, drei weitere hatten bei der Use Case-Auswahl im Workshop zumindest ebenfalls eine hohe Relevanzbewertung (drei bis vier Klebepunkte) erhalten und ein weiterer (Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant) wurde in der Vorabbewertung der Online-Umfrage als hochrelevant eingeschätzt. Die getroffene Use Case-Auswahl umfasst Anwendungen, die für alle betrachteten Stakeholdergruppen von Relevanz sind und die sowohl den Personenverkehr als auch den Güterverkehr betreffen.

In der Vorauswahl war auch der Use Case „Überwachung Bremse“ enthalten. Dieser befand sich nach dem ersten durchgeführten Workshop in der engeren Auswahl und wurde daher in der anschließenden Bearbeitung näher betrachtet. Im zweiten Workshop war die Endbewertung allerdings nicht die größte. Des Weiteren sollten die Use Cases möglichst ausgewogen verteilt sein. Daher wurde der Use Case „Überwachung Bremse“ in der Endauswahl nicht berücksichtigt. Da die bis dahin bereits recherchierten Informationen allerdings inhaltlich von Interesse sind, sind sie an vereinzelten Stellen im Bericht zu finden (siehe zum Beispiel Kapitel 7.1.4.2).

4.3 Anforderungsanalyse

Dieses dritte Unterkapitel beschäftigt sich mit einer Anforderungsanalyse. Dazu werden die in Kapitel 4.2 priorisierten Anwendungsfälle zunächst hinsichtlich ihrer benötigten Sensorkomponenten untersucht. Im Anschluss werden Anforderungskriterien definiert, die an Sensoren für einen Einsatz im Bahnsystem gestellt werden. Dadurch können alle Komponenten hinsichtlich der gleichen Anforderungen bewertet werden. Zusätzlich wird der Zulassungsprozess von Sensoren im Bahnwesen dargelegt.

4.3.1 Recherche

Anforderungskriterien

Die Ermittlung der Anforderungskriterien erfolgte über mehrere Schritte. Zunächst wurden über den Erfahrungsschatz der Autorinnen und Autoren dieses Berichts mehrere Anforderungsgruppen definiert, die für Sensoren im Bahnwesen von Relevanz sind. Diese stellen noch nicht die finalen Anforderungsgruppen dar, sondern sind ein erster Aufschlag, der anschließend noch überarbeitet wird:

- Umwelt
- Betriebssicherheit
- Verfügbarkeit
- Wartbarkeit
- Zuverlässigkeit
- IT-Security
- Montage/Anbindung
- Schnittstellen
- Bahnbetrieb
- Störung anderer Komponenten/EMV

Anschließend wurden mehrere Expertinnen- und Experteninterviews mit unterschiedlichen Themenschwerpunkten durchgeführt, um für die Anforderungsgruppen konkrete Anforderungskriterien zu ermitteln. Zusätzlich wurden Regelwerke zu den vorab definierten Anforderungsgruppen und Themenschwerpunkten recherchiert sowie den Expertinnen- und Experteninterviews entnommen und hinsichtlich der Anforderungskriterien analysiert. Des Weiteren wurden auch Informationen aus dem Zulassungsprozess herangezogen.

Die Expertinnen- und Experteninterviews wurden sowohl innerhalb des Projektkonsortiums als auch mit weiteren Expertinnen und Experten durchgeführt. In den Interviews wurde nach Anforderungen zu den vorab definierten Gruppen gefragt. Da nicht jede Expertin und jeder Experte zu allen Gruppen viel beitragen konnte, wurde jede Expertin und jeder Experte anhand ihrer Expertise ausgewählt, sodass jede Gruppe ausreichend vertreten ist. Der Fokus der Interviews lag auf folgenden Themen, mit der Zuordnung zu den jeweiligen Gruppen:

- Bahn allgemein für Gruppe Umwelt, Störung anderer Komponenten/EMV, Schnittstellen sowie grobe Informationen zu den anderen Gruppen
- Bahnbetrieb für Gruppe Bahnbetrieb, Schnittstellen
- Befestigungsart Kleben für Gruppe Montage/Anbindung[1]
- Elektrotechnik für Gruppe Störung anderer Komponenten/EMV
- Security für Gruppe IT-Security
- Safety für die RAMS Prozesse, d. h. Gruppen Verfügbarkeit, Wartbarkeit, Betriebssicherheit, Zuverlässigkeit

Zusätzlich wurden auch Erfahrungen von Sensorherstellern sowie von den Autorinnen und Autoren des Berichts berücksichtigt. Im Folgenden werden Kurzzusammenfassungen der Interviews gegeben.

1. Expertinnen- und Experteninterview zu Bahn allgemein
    - Wichtige Anforderungen ergeben sich aus den Themen Brandschutz und Umwelt sowie aus der Norm DIN EN 50155 für elektrische Betriebsmittel auf Schienenfahrzeugen.
    - Sich durch die Infrastruktur ergebende Anforderungen müssen genauso wie die der Fahrzeuge berücksichtigt werden.

2. Expertinnen- und Experteninterview zu Bahnbetrieb

[1] An dieser Stelle wurde nur eine Befestigungsart betrachtet. In diesem Gespräch kam heraus, dass alles Wichtige in der entsprechenden Norm über Kleben zu finden ist. Darüber hinaus wurden keine Anforderungen genannt. Aufgrund dieser Tatsache wurde auf Experten- und Expertinneninterviews zu anderen Befestigungsarten verzichtet, da an dieser Stelle in die jeweiligen anderen Normen geschaut werden kann.

- Durch den Einsatz von Sensoren darf der Fahrplanbetrieb nicht gestört werden. Die Einsatzdauer der Sensoren muss bestimmt und ggf. ein Dauerbetrieb gewährleistet werden.
- Die Verfügbarkeit der Sensordaten muss hoch sein und die Abtastrate sinnvoll gewählt werden. Dafür sind auch die Daten- und Kommunikationsschnittstellen ausreichend genau zu definieren und hinsichtlich einer sicheren Datenübermittlung auszulegen.

3. Expertinnen- und Experteninterview zu Befestigungsart Kleben
    - Die Befestigungsart, in diesem Fall „Kleben“, darf die Funktionsweise des Sensors nicht beeinflussen. Bspw. wäre ein elastischer Klebstoff für die Messung von präzisen Beschleunigungswerten eher ungeeignet. Es muss allerdings ein geeigneter Kompromiss zwischen Elastizität und Langzeitfestigkeit gefunden werden.
    - Bei der Ausübung von sicherheitsrelevanten Funktionen durch den Sensor sind im Fall einer Klebung einige Nachweise notwendig und die Kohäsion sowie Adhäsion müssten berechnet bzw. getestet werden. Die Norm DIN EN 17460:2022-10 ist für diese Befestigungsart zu berücksichtigen.
4. Expertinnen- und Experteninterview zu Elektrotechnik
    - Elektronische Komponenten müssen allen Witterungsbedingungen Stand halten. Insbesondere das Eindringen von Wasser und Schlamm muss verhindert werden. Dazu sind alle Elemente vor Rost und Korrosion zu schützen.
5. Expertinnen- und Experteninterview zu Security
    - IT-Security ist ein komplexes und umfangreiches Thema. Neben dem Schutz vor Angriffen müssen Recheneinheiten und Softwarelösungen austausch- und updatebar sein. Ebenso sollten gängige Verschlüsselungsstandards eingesetzt werden. Auch das Kontrollsystem zur Zusammenfassung der Signale muss vor Angriffen geschützt sein.
    - Äußere Einwirkungen auf die Sensoreinheit dürfen nicht zu einer Lahmlegung des Zugverkehrs führen. Eine Manipulation der Signale muss ebenfalls ausgeschlossen werden.
6. Expertinnen- und Experteninterview zu Safety
    - Betriebseinschränkungen müssen in jedem Fall ausgeschlossen werden. Dazu sind Analysen, wie die FRACAS-, FMEA- oder FMECA-Analyse, durchzuführen.
    - Eine Bestimmung des Sicherheits-Integritätslevel (SIL)-Levels ist erforderlich. Zusätzlich müssen Gefahrenlogbücher geschrieben und Zuverlässigkeitsdiagramme ermittelt werden.
7. Expertinnen- und Experteninterview der Sensorhersteller
    - Die wichtigste Norm in der Herstellung von Sensoren ist die DIN EN 50155. Weitere Anforderungen werden im Regelfall vom Anwender genannt.
    - Im Bahnbereich sind große Unterschiede in den Betriebsbedingungen, z. B. hinsichtlich Temperatur oder Schock, zu finden.
8. Expertinnen- und Experteninterview zu Bahn allgemein
    - Auf Sensoren wirken vielfältige Umweltbedingungen. In Abhängigkeit der Anwendungsbedingungen müssen die Komponenten gemäß einer bestimmten IP-Klasse ausgelegt werden.
    - Bei einem Fehler des Sensorsystems muss in jedem Fall ein sicherer Zustand gewährleistet werden.

Zulassungsprozess

Bei der Ermittlung des Zulassungsprozesses wurden zum einen Informationen zur Zulassung vom Eisenbahn-Bundesamt (EBA) herangezogen. [1][2] Zum anderen wurden Expertinnen- und Experteninterviews durchgeführt, um von deren Erfahrungen zu profitieren und einen praxisnahen Handlungsleitfaden zu erstellen. Neben dem allgemeinen Vorgehen wurden auch notwendige Nachweise und Regelwerke genannt. Im nachfolgenden werden Kurzzusammenfassungen der Interviews gegeben.

1. Expertinnen- und Experteninterview
    - Die Anforderungen an Sensoreinheiten sind allgemein nur schwer zu definieren und einzugrenzen, da sie sensor- und fahrzeugspezifisch (Einsatzländer, Vollbahnfahrzeuge, Nebenfahrzeuge usw.) sind. Abhängig vom Grad der Sicherheitsrelevanz kann eine erneute Zulassung des Fahrzeugteilsystems erforderlich sein. Für autark funktionierende Sensoreinheiten ist ein Einsatz auf einem Fahrzeug einfacher umsetzbar als für Sensoreinheiten, die in das Fahrzeugsystem eingreifen und ggf. sicherheitsrelevante Tätigkeiten ausüben. Wichtig ist u. a. die Einhaltung der DIN EN 50155 für elektrische Einrichtungen in Schienenfahrzeugen sowie deren funktionalen Anforderungen unter Berücksichtigung der jeweiligen Gefährdungsermittlung.
2. Expertinnen- und Experteninterview
    - Bisher eingesetzte Sensoren bedingen keiner separaten Zulassung oder einer Neuzulassung des Fahrzeugs. Ein Sensor, der dies erfordert, ist nicht bekannt. Denkbar wären Sensoren zur Absicherung von Innovationen bzgl. Leichtbau, z. B. mit Abweichungen in der „DIN EN 12663-1 – Bahnanwendungen – Festigkeitsanforderungen“ o. Ä. Hier könnte ein Sensor Teil der Zulassung sein, da dieser bestimmte Grenzwerte überwacht und gegebenenfalls Aktionen auslöst. Die bisher eingesetzten Sensoren stellen ein Add-on zu bestehenden Betriebs- und Instandhaltungsprozessen dar. Die Anforderungen variieren in Abhängigkeit des Sensors und des Einsatzgebietes. Wichtige Anforderungen sind allgemein u. a. die Themen EMV, Lichtraumprofil, Brandschutz, Explosionsgefährdete Bereiche (ATEX)-Bereiche sowie Montageeigenschaften und Verletzungsrisiko durch Montage und Positionierung des Sensors.
    - In jedem Fall ist eine Signifikanzprüfung durchzuführen. Risikoanalysen (FMEA‘s) sind bei signifikanten Änderungen auszuführen und zu dokumentieren. Es muss sichergestellt werden, dass u. a. durch ein Abfallen des Sensors kein Risiko entsteht und die Befestigung keinen Einfluss auf die Strukturfestigkeit des Fahrzeugs hat. Der Sensor darf zudem das Handling und die Funktionsfähigkeit des Güterwagens nicht beeinträchtigen.
    - Das Gewicht der Sensoreinheit ist ein entscheidender Einfluss bzgl. des Abfallens. Abhängig vom Einbauort können bereits wenige hundert Gramm einen sicherheitsrelevanten Einfluss haben, z. B. hinsichtlich der Personengefährdung durch einen herumfliegenden Sensor. Das Gewicht des Sensors bestimmt ebenfalls über in Frage kommende Montageverfahren (z. B. Kleben, Klemmen, Nieten, Schrauben).
3. Expertinnen- und Experteninterview
    - Die Erstellung einer hochwertigen Systemdefinition (Aufstellung von Schnittstellen, Funktion, Randbedingungen, Systemzugehörigkeit, etc.) in Zusammenarbeit mit verschiedenen Expertinnen und Experten bietet eine solide Grundlage für die Risikoanalyse und die daraus folgenden Systemanforderungen.
    - Weitere Literatur kann aus der CSM-Verordnung und/oder vom Lebenszyklusprozess (V-Modell) der DIN EN 50126 entnommen werden.

Regelwerke

In den Interviews über die Anforderungskriterien und die Zulassung wurden einige Regelwerke genannt, die für Sensorlösungen im Bahnwesen von Bedeutung sind. Da die Vielfalt an Vorschriften groß ist und die Anforderungen in Abhängigkeit des Sensors und des Einsatzgebietes variieren, muss sich auf die wichtigsten Regelwerke konzentriert werden. Daher wurden Regelwerke, die von mehreren Expertinnen und Experten genannt wurden, als besonders relevant eingestuft. Ebenso wurden die von Seiten der Zulassung genannten Vorschriften ebenfalls als notwendig eingestuft. Es wurden insgesamt die in der folgenden Tabelle 6 genannten Regelwerke hinsichtlich darin genannter Anforderungen analysiert. Für eine Risikobewertung sind die SIRF (Sicherheitsrichtlinie Fahrzeug) sowie die Common Safety Methods – Risk Assessment (CSM-RA)-Verordnung 402/2013 heranzuziehen. An dieser Stelle sei angemerkt, dass

die DIN EN 50155 für den Einsatz von Sensorlösungen auf Schienenfahrzeugen eine besondere Bedeutung hat, da sie den Einsatz von Betriebsmitteln auf Schienenfahrzeugen behandelt. Die wichtigsten Inhalte werden im Anschluss an Tabelle 6 näher erläutert.

TABELLE 6: RELEVANTE REGELWERKE FÜR DEN EINSATZ VON SENSOREN IM BAHNWESEN

Nummer	Inhalt
DIN EN 12663	Bahnanwendungen – Festigkeitsanforderungen an Wagenkästen von Schienenfahrzeugen Teil 1 – 2
DIN EN 13749	Bahnanwendungen – Radsätze und Drehgestelle – Festlegungsverfahren für Festigkeitsanforderungen an Drehgestellrahmen
DIN EN 45545	Bahnanwendungen - Brandschutz in Schienenfahrzeugen Teil 1 – 7, insbesondere Teil 2: Anforderungen an das Brandverhalten von Materialien und Komponenten
DIN EN 50121	Bahnanwendungen – Elektromagnetische Verträglichkeit Teil 1 – 5
DIN EN 50125	Bahnanwendungen – Umweltbedingungen für Betriebsmittel Teil 1 – 3
DIN EN 50126	Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) Teil 1 – 2
DIN EN 50128	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme
DIN EN 50129	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – sicherheitsbezogene elektronische Systeme für Signaltechnik
DIN EN 50153	Bahnanwendungen – Fahrzeuge – Schutzmaßnahmen in Bezug auf elektrische Gefahren
DIN EN 50155	Bahnanwendungen – Fahrzeuge – Elektronische Betriebsmittel
DIN EN 50657	Bahnanwendungen – Anwendungen für Schienenfahrzeuge – Software auf Schienenfahrzeugen
DIN EN 61373	Bahnanwendungen – Betriebsmittel von Bahnfahrzeugen – Prüfungen für Schwingen und Schocken
TSI und/oder NNTV/NNTR	Je nach Einsatzgebiet des Fahrzeugs TSI'en und/oder Notifizierte Nationale Technische Vorschriften/Regeln zu entsprechender Fahrzeugkategorie
TR EMV	Technische Regeln zur Elektromagnetischen Verträglichkeit, insbesondere Regelung Nr. 6

Die Norm DIN EN 50155 beschäftigt sich mit dem Einsatz von Betriebsmitteln auf Schienenfahrzeugen, zu denen Sensoren und deren Komponenten gezählt werden. Inhaltlich behandelt sie folgende Themen (in unterschiedlicher Tiefe) und verweist teilweise auch auf die zugehörigen Normen:

- Umweltbedingungen für den Betrieb, mit Verweis auf DIN EN 50125, DIN EN 50121, DIN EN 50124 und DIN EN 61373
- Besondere Betriebsbedingungen
- Elektrische Betriebsbedingungen, mit Verweis auf DIN EN 50121 und DIN EN 50124
- Zuverlässigkeit, Instandhaltbarkeit und zu erwartende Brauchbarkeitsdauer
- Entwicklung/Auslegung, mit Verweis auf DIN EN 50124, DIN EN 50126, DIN EN 50153 und DIN EN 50657
- Elektronische Betriebsmittel, welche nicht für Schienenfahrzeuge entworfen wurden
- Bauelemente
- Konstruktion, mit Verweis auf DIN EN 60529
- Sicherheit, mit Verweis DIN EN 45545 und DIN EN 50153
- Dokumentation, mit Verweis auf DIN EN 50657, DIN EN 61373 und DIN EN 60529
- Prüfung, mit Verweis auf DIN EN 61373 und DIN EN 60529

Zusätzlich erfolgen an Stellen, an denen elektrotechnische Inhalte und Anforderungen an Softwarelösungen behandelt werden, Verweise auf die entsprechenden EN- sowie IEC-Normen. Des Weiteren können zwei Anhänge als relevant eingestuft werden. Der Anhang C behandelt den „Schärfegrad der Betriebsbedingungen an verschiedenen Einbauorten von Schienenfahrzeugen“. Darin werden für verschiedene Einbaubereiche Einsatzbedingungen definiert, die ein gutes Indiz für die Anforderungen an verschiedene Betriebsmittel sind. Der Anhang G erläutert einige Punkte zu „Nicht-bahnspezifisch ausgelegte[n] elektronische[n] Betriebsmittel[n]“, die beim Einsatz solcher Geräte berücksichtigt werden müssen.

4.3.2 Sensorikkomponenten

Bevor es um die erläuterten Anforderungskriterien und den Zulassungsprozess geht, ist es notwendig, die für jeden Use Case benötigten Sensorkomponenten zu erläutern. Diese zeigen, welche Sensoren für den jeweiligen Use Case notwendig und/oder möglich sind. Hier werden jeweils alle möglichen Sensoren aufgeführt. Die genaue Auswahl der einzusetzenden Sensoren muss individuell gewählt werden. Es wird dennoch eine Einschätzung gegeben, was sich als sinnvoll erweist. Für jeden Use Case werden folgende Elemente erläutert:

- Basisinformationen über Ziele, Nutzen, Fahrzeug- und Verkehrsart, etc.
- Informationen zum aktuellen Stand der Forschung
- Tabellarische Übersicht und Abbildung zur Darstellung der Sensoren. Hier wird auch eine Einschätzung von Aufwand zu Nutzen gegeben
- Erläuternder Fließtext zu den Sensoren, der in jedem Fall zusätzliche Informationen beinhaltet

Im Anschluss wird auf die Peripherie eingegangen.

Use Case „Fahrzeug überwacht Oberbau“

Die wichtigsten Informationen des Use Cases „Fahrzeug überwacht Oberbau“ sind in Tabelle 7 aufgeführt. Im Anschluss wird erläutert, in welchen Projekten solche Systeme bereits in Erprobung sind.

TABELLE 7: BASISINFORMATIONEN DES USE CASES „FAHRZEUG ÜBERWACHT OBERBAU“

Ziel		Gewinn von Daten über den Oberbauzustand (z. B. Gleislage, Herzstück- oder Schienenzustand) durch Regelfahrzeuge zur frühzeitigen Erkennung von kritischen Fällen und Trends. Das Ziel ist es, die Oberbauqualität zu verbessern und eine zustandsorientierte Instandhaltung für die Infrastruktur zu ermöglichen, ggf. auch eine Reduktion der Zahl an gesonderten Messfahrten und Messungen. *Mehrwert gegen bestehenden Systemen:* Das Intervall zwischen Messungen wird im Vergleich zum aktuellen Zustand verkürzt und die Anzahl an Messfahrten kann reduziert werden.
Installationsort der Sensoren		Fahrzeug
Nutzen	Primär	EIU
	Sekundär	Fahrzeughalter und/oder ECM, indem außergewöhnliche Belastungen (z. B. Auflaufstöße) bekannt werden und eine Prüfung o. Ä. stattfinden kann.
Fahrzeugart		Alle Fahrzeuge: Reisezug- und Güterwagen, Triebwagen, Lokomotiven (einfachere Realisierbarkeit auf Fahrzeugen mit Stromversorgung)
Verkehrsart		Personen- und Güterverkehr
Sicherheitsrelevanz		Ja, wenn dadurch gesonderte Messungen ersetzt werden.
Umsetzbarkeit (eingeschätzt durch Experten und Expertinnen)		Leicht

Zur Realisierung der Ziele können auf dem Fahrzeug verschiedene Sensoren eingesetzt werden, die bereits in folgenden Projekten in Nutzung oder Erprobung sind:

- Im Projekt Dynotrain wird die Erfassung von Größen, wie die Längshöhe, die Pfeilhöhe, die gegenseitige Höhenlage, die Spurweite und das Schienenquerprofil links/rechts erprobt. Als Abtastrate wurden 16 cm für die ersten drei und 25 cm für die letzten zwei Messgrößen angegeben. [3]

- Im Jahr 2013 wurden im Rahmen eines Innovationsprojekts der DB Systemtechnik im ICE 2 Beschleunigungssensoren als autarkes System eingesetzt. [4] Ebenso werden bei der Schweizerischen Südostbahn (SOB) Beschleunigungssensoren als Probenkörper zur Zustandsaufnahme von u.a. der Gleislängshöhe eingebaut. [5]

- Das CIM-System (Continuous Infrastructure Monitoring) der DB Systemtechnik wird auf Regelzügen verbaut und besteht aus verschiedenen Systemen zur Oberleitungsüberwachung (COLM), der Kraftüberwachung (CFM), der Schienenüberwachung (CTM), der Geometrieüberwachung (CGM) und der Operationsüberwachung (COM). Für die Überwachung der Gleise ist das CTM-System von Bedeutung. [6]

- In mehreren Straßenbahnsystemen wird dieser Use Case ebenfalls erforscht. In der Metro Barcelona werden am Fahrzeug Lasersensoren zur Entfernungsmessung und Beschleunigungssensoren am Achslager zur Bestimmung der Unebenheit der Schiene montiert. [7] In Deutsch-

land gibt es das Forschungsprojekt OnboardEU (Onboard-Daten für die Erkennung von Gleisfehlstellen) des Bundesministeriums für Digitales und Verkehr (BMDV) mit einer Laufzeit von 12/2021 bis 11/2024 unter der Leitung des Instituts für Verkehrssystemtechnik des Deutschen Zentrums für Luft- und Raumfahrt (DLR e. V.) gemeinsam mit dem Austrian Institute of Technology GmbH und i4m technologies GmbH. Ziel ist die kontinuierliche und automatisierte Zustandsüberwachung von Gleisnetzen mit Messsystemen auf Straßenbahnen. Dabei wird insbesondere der Einsatz von Künstlicher Intelligenz zur Detektion von Schäden am Gleis erprobt, indem zwölf Fahrzeuge in verschiedenen Städten mit Messsystemen ausgestattet werden und die Ergebnisse praktisch erprobt und bearbeitet werden. [8] Auch international werden solche Systeme immer mehr in die Forschung einbezogen. [9]

- Grundsätzlich können auch ähnliche Sensoren wie auf Messfahrzeugen eingesetzt werden. Dazu zählen bspw. das Gedo IMS-Scan System von Trimble [10], das RSCM Rail Surface Crack Measurement von Vögel & Plötscher [10] oder das modulare GRP System FX von Amberg Technologies [11].

Unter Zuhilfenahme von Informationen, die in diesen Projekten gewonnen wurden, konnten mögliche Sensoren erarbeitet werden. Die folgende Tabelle 8 und Abbildung 9 zeigen die möglichen Sensoren und werden im Anschluss näher erläutert.

TABELLE 8: MÖGLICHE SENSOREN FÜR DEN USE CASE „FAHRZEUG ÜBERWACHT OBERBAU“

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Beschleunigungssensor 1-axial	Radsatzlager	vertikale Gleislage (Längshöhe)	Nur eine Messrichtung, daher im Nachteil gegen 3-axialem Sensor.
Beschleunigungssensor 3-axial	Radsatzlager	vertikale Gleislage (Längshöhe), horizontale Gleislage, Höhenlage der Schienen	Geeignet.
Linien-Laser-Messsystem	Unterseite Fahrzeug, über dem Gleis	Querprofil der Schiene und Spurweiten	Geeignet.
IMU (3 Beschleunigungssensoren und drei orthogonale Drehraten sensoren (Gyroskop))	Radsatzlager, Drehgestell oder Wagenkasten	Längshöhe, Schienenzustand	Wenn nicht zu teuer, dann geeignet.
Berührungslose Abstandssensoren: Optisch = Lasersensor Induktiv = Wirbelstromsensor Magnetfeldsensor Ultraschallsensor	Radsatzlager, Fahrwerksbereich, Wagenkasten	Längshöhe, Herzstück- und Schienenzustand	Geeignet, wenn wirtschaftlich vertretbar.

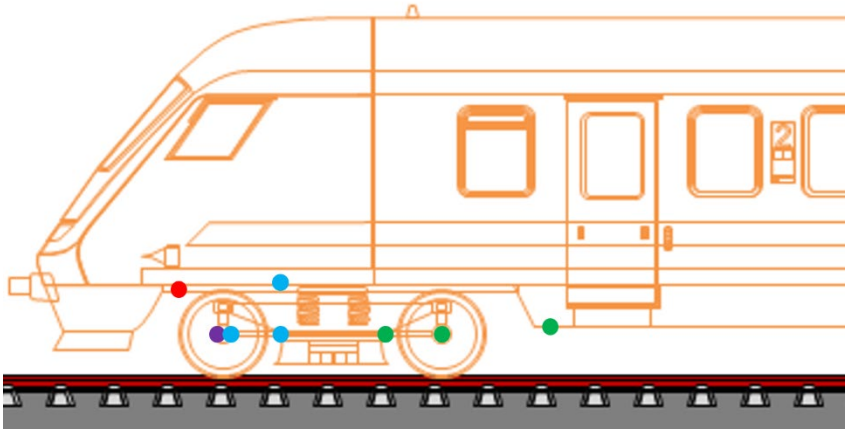


Abbildung 9: Montageorte der Sensoren für den Use Case „Fahrzeug überwacht Oberbau“

Eine einfache Sensorlösung ist die Montage eines Beschleunigungssensors möglichst nah am Rad. Hierfür bietet sich das Radsatzlager an. Dadurch können die Beschleunigungen nah am Rad-Schiene-Kontakt gemessen werden. Je nach Abtastrate des Sensors können auch Vibrationen bestimmt werden. Für die vertikale Gleislage reicht grundsätzlich ein einachsiger Beschleunigungssensor [7][12][13][4], aber mit dreiachsigen Sensoren lassen sich noch weitere Schienenfehler und Gleislageabweichungen (vertikal, horizontal, Höhenlage der Schienen) bestimmen. [14][15]

Die Kopplung aus drei orthogonalen Beschleunigungssensoren und drei orthogonalen Drehratensensoren (Gyroskope) wird als Inertiale Messeinheit (IMU) bezeichnet. Damit kann die Messung der Längshöhe der Schienen sowie die Aufnahme des Schienenzustands bei Montage am Radsatzlager, Drehgestell oder Wagenkasten in Achsnähe ermöglicht werden. Werden die IMUs am Drehgestell oder Wagenkasten montiert, sind noch weitere Sensoren notwendig, um die Position des Sensors relativ zur Schiene zu bestimmen. [16][5]

Für die Bestimmung der Längshöhe können auch berührungslose Abstandssensoren, wie Ultraschallsensoren, Magnetfeldsensoren, Lasersensoren als optisches Messsystem oder Wirbelstromsensoren als induktives Messsystem, eingesetzt werden. Diese können am Radsatzlager oder Fahrwerksbereich montiert werden. Ebenso wird dadurch eine Überwachung des Herzstück- und Schienenzustandes möglich. [16]

Um das Querprofil der Schiene und die Spurweite zu messen, können auch Linien-Laser-Messsysteme installiert werden. Hierbei handelt es sich um ein aufwendigeres und empfindlicheres Messsystem, das an der Unterseite des Fahrzeuges in der Nähe zum Gleis montiert werden muss. Dies kann in abgetrennten Systemen, d. h. dort, wo eine geringere Gefahr für Beschädigungen des Systems besteht, z. B. bei Metrosystemen, als sinnvoll erachtet werden. Insbesondere bei viel Verkehr und engen Bögen erweist sich dieses System als geeignet, da dort häufige Messungen sinnvoll sind, jedoch im Regelbetrieb kaum Zeit für gesonderte Messfahrten zur Verfügung steht. [7]

Use Case „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant“

Die wichtigsten Informationen des Use Cases „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant“ sind in Tabelle 9 aufgeführt. Im Anschluss wird erläutert, in welchen Projekten solche Systeme bereits in Erprobung sind.

TABELLE 9: BASISINFORMATIONEN DES USE CASES „FAHRZEUGLOKALISIERUNG FAHRZEUGSEITIG SICHERHEITSRELEVANT“

Ziel		Ortung und gleisgenaue Lokalisierung von Zügen mit dem Ziel, die Auslastung der Strecke zu optimieren bzw. Moving-Block-Systeme einzusetzen. *Mehrwert gegen bestehenden Systemen:* Es bildet die Grundlage für autonomes Fahren und ermöglicht eine bessere Auslastung der Strecke. Bisher wird so etwas nur in sehr wenigen Systemen (z. B. autonome U-Bahnen) eingesetzt.
Installationsort der Sensoren		Fahrzeug
Nutzen	**Primär**	EVU und EIU zur Steuerung des Verkehrs auf der Strecke
	Sekundär	Fahrzeughalter (als Information für die genaue Position des Fahrzeugs)
Fahrzeugart		Alle Fahrzeuge: Reisezug- und Güterwagen, Triebwagen, Lokomotiven, Messfahrzeuge Eine Lokalisierung pro Zug ist ausreichend, ein geeignetes Betriebskonzept müsste ausgearbeitet werden.
Verkehrsart		Personen- und Güterverkehr, ausgenommen isolierte Streckennetze
Sicherheitsrelevanz		Ja
Umsetzbarkeit (eingeschätzt durch Experten und Expertinnen)		Schwer

Die sicherheitsrelevante Ortung von Fahrzeugen erfolgt bisher infrastrukturseitig. Für die nicht sicherheitsrelevante fahrzeugseitige Ortung von Fahrzeugen sind auf Güterwagen bereits Systeme im Einsatz, mit denen die Position von Güterwagen bestimmt werden kann. Bisher werden dort aber nur Global Positioning System (GPS)-Sensoren mit einer eher geringen Genauigkeit eingesetzt. In Erprobung befinden sich allerdings auch schon GNSS-Sensoren, die eine gleisgenaue Ortung bis zu 2 cm ermöglichen sollen. Eine sicherheitsrelevante Ortung von Fahrzeugen befindet sich in Erprobung bzw. gibt es erste Konzepte, umgesetzt sind diese aber noch nicht.

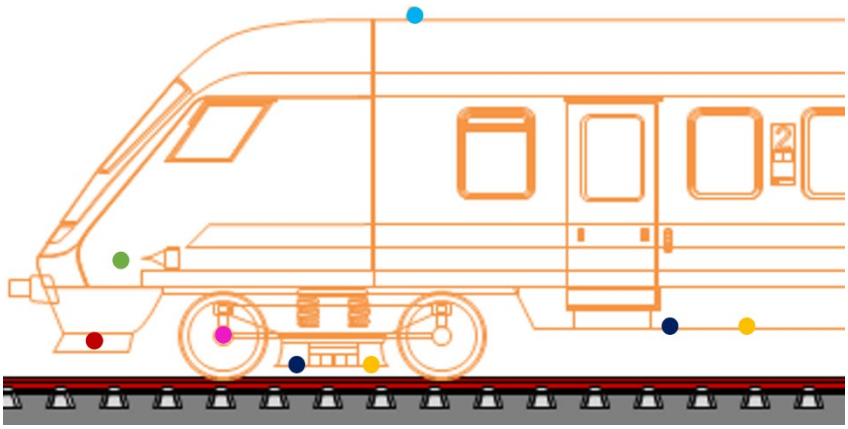


Abbildung 10: Montageorte der Sensoren für Use Case „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant“

Tabelle 10 und Abbildung 10 zeigen mögliche Sensoren, die anschließend näher erläutert werden. Dabei wird insbesondere darauf eingegangen, welche Sensoren kombiniert werden können, damit auch die Sicherheitsrelevanz gewährleistet werden kann.

TABELLE 10: MÖGLICHE SENSOREN DES USE CASES „FAHRZEUGLOKALISIERUNG FAHRZEUGSEITIG SICHERHEITSRELEVANT“

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
GNSS	Fahrzeugdach	Positionskoordinaten	Geeignet.
IMU	Fahrzeug innenliegend	Bewegungsdaten (Geschwindigkeit, Drehraten, Positionsänderung)	In Verbindung mit min. einem weiteren Sensor sinnvoll.
Balisenleser	Unterhalb der Fahrzeugfront	u. a. Positionsdaten	Keine ausschließliche fahrzeugseitige Lösung. Wenn dies kein Problem darstellt, eine geeignete Technologie.
Wegimpulsgeber	Achslager	Bewegungsdaten	In Verbindung mit min. einem weiteren Sensor sinnvoll.
Weitere Geschwindigkeitssensoren (Doppler-Radar, Magnetometer, optisch, ...)	Fahrzeug- bzw. Drehgestellunterseite	Bewegungsdaten	In Verbindung mit min. einem weiteren Sensor möglich, aber seltenere Technologie als IMU oder Wegimpulsgeber.
Ground Penetrating Radar, Magnetfeldsensoren, Wirbelstromsensoren, Bilderkennung	Untergestell, Fahrzeug- bzw. Drehgestellunterseite	Positionsbestimmung	Geeignet, wenn digitale Streckenkarten vorliegen.

Die Fahrzeuglokalisierung kann durch Kombination verschiedener Sensoren erfolgen. Bei Ausfall eines Sensors, bei schlechtem Empfang während einer Tunneldurchfahrt oder anderweitiger Abschattung kann und muss die Lokalisierung dennoch weiterhin ermöglicht werden. Daher bietet sich die Kombination bestimmter Sensoren an. Welche Sensorkombination für eine hochgenaue Fahrzeuglokalisierung am sinnvollsten ist, ist aktuell noch Forschungsbestandteil. Die zwei aktuell näher verfolgten Varianten werden nachfolgend vorgestellt.

Variante 1: Bei Vorhandensein von physischen Balisen, z. B. European Train Control System (ETCS)-Balisen, kann mithilfe von Balisenlesern die aktuelle Position gleisgenau bestimmt werden. Die Genauigkeit hängt hierbei von den Daten der Balise ab. Zusätzlich muss die Position zwischen zwei Einheiten bestimmt werden. Dazu genügt die Information über die zurückgelegte Strecke nach einer Balise. Dies

kann mithilfe üblicher Odometriemethoden erfolgen. [17][18] Die gängigste Variante dafür sind Wegimpulsgeber in Kombination mit mindestens einem weiteren Sensor. [17] Dazu bieten sich inertiale Messeinheiten (IMU, bestehend aus Beschleunigungs- und Drehratensensoren), Doppler-Radar oder auch optische Sensoren und Magnetometer an. [18] Eine große Herausforderung hierbei ist die begrenzte Wetterfestigkeit (Eis & Schnee) einiger Sensoren. Durch die Kombination von Sensoren können Fehler ausgeglichen werden, die beim Gleiten oder Schlupf der Räder auftreten können. Außerdem müssen Ungenauigkeiten durch Raddurchmesserabweichungen bzw. Verschleiß der Räder eliminiert werden.

Wenn eine digitale Streckenkarte existiert und bestimmte physische Eigenschaften der Strecke bekannt sind, lassen sich auch Technologien wie Ground Penetrating Radar, Magnetfeldsensoren, Wirbelstromsensoren oder Bilderkennungsverfahren einsetzen. Diese erkennen spezifische Elemente der Strecke und ermöglichen dadurch eine Zuordnung der genauen Position. [19]

Variante 2: Beim Nichtvorhandensein von physischen Balisen bzw. dem Vorhandensein von virtuellen Balisen ist der Einsatz eines globalen Navigationssatellitensystems (GNSS) notwendig. Bei GNSS können unterschiedliche Satellitensysteme verwendet werden, wie GPS oder auch das sich im Aufbau befindliche Galileo. Dieses System soll zukünftig wesentlich genauer sein als GPS und kann für eine gleisgenaue Ortung ausreichen. [20][18]Um bereits jetzt eine ausreichende Genauigkeit zu erzielen, gibt es die Möglichkeit mit Referenzstationen zu arbeiten. Dieses System nennt sich Differential Global Positioning System. Auch der Einsatz von mehreren unabhängigen Antennen mit gegebenenfalls verschiedenen Montageorten kann nötig sein. Eine Schwierigkeit des GNSS ist der mangelnde Empfang bei Tunneldurchfahrten oder durch Abschattungen von Gebäuden (z. B. Bahnhöfen) und Bergen. Daher ist auch bei der Verwendung von hochgenauen GNSS mindestens ein weiterer Sensortyp notwendig. Dabei können die in Variante 1 genannten Sensoren verwendet werden, z. B. IMU. [20][18] Alternativ können auch spezielle Systeme in Tunneln verbaut werden. Möglich sind bspw. MEMS-Drehratensensoren [21] oder der Einsatz von faseroptischen Sensoren. [19]

Use Case „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“

Die wichtigsten Informationen des Use Cases „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“ sind in Tabelle 11 aufgeführt. Im Anschluss wird erläutert, in welchen Projekten solche Systeme bereits in Erprobung sind.

TABELLE 11: BASISINFORMATIONEN DES USE CASES „FAHRZEUG ÜBERWACHT FAHRZEUG: ZUSTAND VON TÜREN U. A. VERRIEGELUNGEN“

Ziel		Überwachung von Türen u. a. Verriegelungen (wie z. B. Klappen und Hebel am Güterwagen oder Königszapfen im KV) für die Feststellung der Abfahrbereitschaft des Zuges und das Einsparen manueller Vorgänge, Erkennen von ungewöhnlichen Ereignissen während der Zugfahrt sowie Detektion von Verschleißerscheinungen. *Mehrwert gegen bestehenden Systemen:* Der Use Case zielt insbesondere auf den Güterverkehr ab, indem Sensoren dort den Zustand von Verriegelungen und Klappen bestimmen und manuelle Vorgänge eingespart werden können. Im Personenverkehr ist die Zustandsüberwachung bereits vorhanden, eine Verschleißerkennung kann aber noch ergänzt werden.
Installationsort der Sensoren		Fahrzeug
Nutzen	**Primär**	EVU und EIU zur Steuerung des Verkehrs auf der Strecke

	Sekundär	Fahrzeughalter (als Information über Defekte und Verschleiß)
Fahrzeugart		Alle Fahrzeuge: Reisezug- und Güterwagen, Triebwagen, Lokomotiven, Messfahrzeuge
Verkehrsart		Personen- und Güterverkehr
Sicherheitsrelevanz		Ja
Umsetzbarkeit (eingeschätzt durch Experten und Expertinnen)		Schwer

Für den Personenverkehr ist die Technik zur Detektion des Öffnungs-/Verschlusszustandes und zum Einklemmschutz bereits vorhanden. Allerdings ist nicht in jeder Tür eine Verschleißerkennung enthalten. Im Güterwagenbereich sind solche Sensoren allerdings noch nicht verbreitet. Durch die Verwendung geeigneter Sensoren kann bspw. die Wagenvorbereitung wesentlich verkürzt werden. Grundsätzlich gibt es bereits kommerzielle Sensoren, wie den X-Rayl Solar Pointer S3, die AMRA device, den controlguide CTsensor oder auch einen Kingpin-Sensor zur Überwachung des Königszapfens im Kombinierten Verkehr.

Tabelle 12 und Abbildung 11 zeigen mögliche Sensoren. Dabei müssen nicht alle Sensoren gleichzeitig eingesetzt werden. Es ist ausreichend, sich pro Messwert auf eine bestimmte Technologie zu beschränken, sodass alle Funktionen überwacht werden können.

TABELLE 12: MÖGLICHE SENSOREN FÜR DEN USE CASE „FAHRZEUG ÜBERWACHT FAHRZEUG: ZUSTAND VON TÜREN U. A. VERRIEGELUNGEN“

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Radar	Türrahmen	vornehmlich Objekterkennung, aber auch Abstandsmessung	Ein Sensor wäre ausreichend, da sie alle auf dem gleichen Prinzip basieren. Das Lichtgitter liefert die höchste Detektionswahrscheinlichkeit.
Laserscanner (Lidar)	Türrahmen	vornehmlich Objekterkennung, aber auch Abstandsmessung	
Infrarotsensor	Türrahmen	vornehmlich Objekterkennung, aber auch Abstandsmessung	
Lichtgitter	Türrahmen	vornehmlich Objekterkennung, aber auch Abstandsmessung	
Stromsensor	Türrahmen	Geschlossener/Offener Stromkreis	Wird im Automobilbereich bereits eingesetzt, daher geeignet.

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Druckwellenschalter	Türrahmen	Erkennung von Druck und Gegendruck	Wird bereits eingesetzt, daher geeignet.
Magnetischer Sensor	Türrahmen	Abstandsmessung	Ein Sensor wäre ausreichend.
Kontaktsensor	Türrahmen, Verriegelung, Königszapfen	Kontaktdetektion	
Kamera	Decke des Wagenkastens o.Ä.	Bilderfassung des Türbereiches, Abstandsmessung, Objekterkennung	Datenschutz ist schwierig. Zusätzlich müssten die Kameras mit einer Objekterkennung ausgestattet sein, ansonsten würde sich kaum ein Mehrwert bieten.
Körperschallsensor	Türmechanik	Verschleißerkennung	Ein Sensor wäre ausreichend.
Beschleunigungssensor	Türmechanik	Verschleißerkennung	

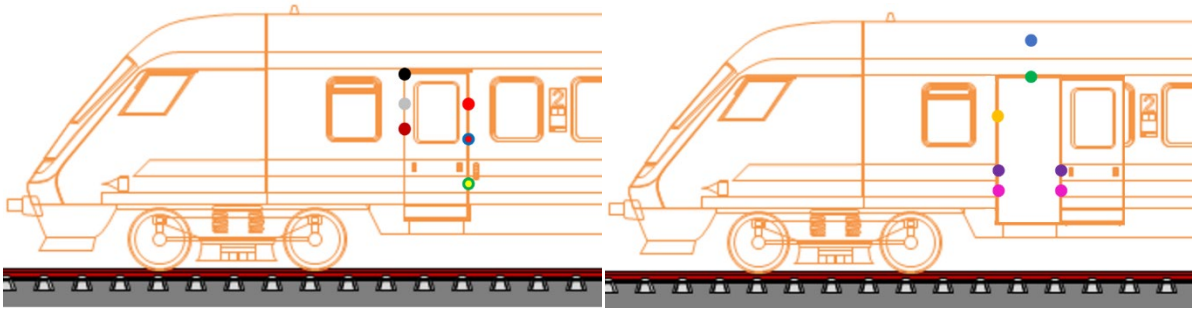


Abbildung 11: Montageorte der Sensoren für Use Case „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“

Die vorhandenen Sensoren können in verschiedene Gruppen eingeteilt werden. Für die Überwachung des Zustandes „geöffnet/verriegelt“ gibt es verschiedene Möglichkeiten, die entsprechend ihrer physikalischen Funktionsweise eingeteilt werden können.

Basierend auf dem Lichtlaufzeitverfahren (Time of Flight, ToF) gibt es Radar, Laserscanner, Infrarotsensor und Lichtgitter. Die Radartechnologie erkennt millimetergenau auf bis zu zwei Meter Entfernung Gegenstände in der Tür. Wenn der vordefinierte Abstand zwischen den zwei Türrahmen kleiner als vorgeschrieben ist, darf die Tür nicht geschlossen werden. Der Laserscanner funktioniert nach dem gleichen Prinzip, nur mit einer anderen Wellenart. Auch hier wird die Distanz zwischen Sender und Empfänger gemessen. Sobald sich etwas dazwischen befindet und der definierte Abstand nicht eingehalten wird, ist das Schließen der Türen nicht möglich. [10] Nach dem gleichen Prinzip funktioniert auch der

Infrarotsensor. Durch den Einsatz mehrerer Sensoren kann auch ein dreidimensionales Bild erzeugt werden. Hierfür gibt es bereits Systeme, die in Türen eingesetzt werden. Dort ist auch eine Unterscheidung von verschiedenen Personen und Gegenständen möglich. [42] Nach einem sehr ähnlichen Prinzip funktioniert das Lichtgitter. Dieses besteht aus mehreren parallelen Lichtschranken. Sobald ein Objekt einen Strahl des Lichtgitters unterbricht, wird dies vom Sensor erkannt und ein Schaltvorgang ausgelöst. [43] Es ist ausreichend, eine dieser Technologien anzuwenden.

Des Weiteren gibt es den Stromsensor, den Druckwellenschalter, den magnetischen Sensor und den Kontaktsensor, die alle über unterschiedliche physikalische Prinzipien einen Kontakt herstellen. Denkbar ist es auch an mehreren Stellen in einer Tür solche Sensoren einzubauen, falls die Tür bzw. Verriegelung schief in ihrer Halterung sitzt. Bei einem Stromsensor wird über das (Nicht-) Vorhandensein eines Stromkreises der Zustand der Tür ermittelt. Beim Zustand „offen“ ist der Stromkreis geschlossen sowie umgekehrt ist der Stromkreis im Zustand „geschlossen“ geöffnet. Bei einem Druckwellenschalter wird vom Signalgeber eine Druckwelle erzeugt, die für eine elektrische Schaltung sorgt. Befinden sich Personen oder Gegenstände im Schließbereich und sorgen für eine Druckänderung, wird eine Tür nicht geschlossen. Bei einem magnetischen Sensor werden in der Tür und im Türrahmen am jeweiligen Berührpunkt ein Sensor und Magnet eingebaut. Wenn die Tür geschlossen ist, befinden sich die beiden Elemente parallel in einem definierten Abstand zueinander. Beim Öffnen der Tür bewegt sich der Magnet vom Sensor weg und die Zustandsveränderung wird erkannt. Ein Kontaktsensor funktioniert auf Basis eines kapazitiven Berührungssensors. Dadurch können Berührungen, Umklammerungen oder Annäherungen erkannt werden.

Ein Sensor, der die Situation visuell darstellt, ist die Kamera. Diese kann Personen oder Gegenstände, wie z. B. Erwachsene, Kinder, Kinderwagen, Rollstuhlfahrer oder Hunde als schematisierte (anonymisierte) Personen erkennen, die sich im Verschlussbereich einer Tür befinden. [22] Möglich ist auch eine Kopplung der Kamera mit dem TOF-Prinzip. Dadurch wäre eine präzisere Darstellung der Situation möglich. Bei dieser Technologie muss die Thematik des Datenschutzes berücksichtigt werden.

Zur Ermittlung des technischen Zustands einer Tür bzw. Verriegelung können Beschleunigungssensoren eingesetzt werden. Dadurch können Schäden, wie bspw. ein defektes Scharnier o. Ä., erkannt werden. Die Montage erfolgt dabei direkt an den zu überwachenden Elementen. Möglich sind hier ein- oder triaxiale Sensoren. [44] Für die gleiche Funktion können auch Körperschallsensoren eingesetzt werden. [23]

Use Case „Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)“

Die wichtigsten Informationen des Use Cases „Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)“ sind in Tabelle 13 aufgeführt. Im Anschluss wird erläutert, in welchen Projekten solche Systeme bereits in Erprobung sind.

TABELLE 13: BASISINFORMATIONEN DES USE CASES „FAHRZEUG ÜBERWACHT FAHRZEUG: ANTRIEBSZUSTAND (ELEKTRO)“

Ziel		Überwachung des Verhaltens der Antriebskomponenten für das frühzeitigere Erkennen möglicher Störungen respektive Schäden im Bereich des Antriebssystems (Elektro). Mithilfe der im Bereich des Antriebsstranges verbauten Sensoren können Daten gewonnen werden, anhand derer bei Auftreten eines Defektes über angemessene Maßnahmen zur Behebung des Defektes entschieden werden kann. Dadurch ist es möglich, während der Fahrt zu ermitteln, ob das Fahrzeug weiterfahren kann oder umgehend gestoppt respektive der Instandhaltung zugeführt werden muss. *Mehrwert gegen bestehenden Systemen:* Die meisten Sensoren sind bereits in den Fahrzeugen verbaut und nehmen Daten auf. Dieser Use Case zielt darauf ab, die Sensordaten explizit für die Diagnose zu nutzen und auf eine zustandsorientierte Instandhaltung umzustellen. Dafür kann es vorteilhaft sein, noch weitere Sensoren einzubauen. Wichtig für diesen Use Case ist vor allem die Betrachtung, wie die Daten genutzt werden können, ohne die Wettbewerbsfähigkeit des Herstellers zu beeinflussen.
Installationsort der Sensoren		Fahrzeug
Nutzen	**Primär**	Fahrzeughalter: Nutzung der Daten zur Detektion möglicher Störungen des Antriebs und Optimierung von Wartungsmaßnahmen respektive Verringerung von Instandhaltungskosten.
	Sekundär	Fahrzeughersteller: die Daten über das Verhalten der Antriebskomponenten im Rahmen des normalen Betriebs kann zur Weiterentwicklung von Antriebssystemen genutzt werden.
Fahrzeugart		Alle elektrisch angetriebenen Fahrzeuge: Lokomotiven, Triebwagen, Messfahrzeuge.
Verkehrsart		Personen- und Güterverkehr (Im Güterverkehr ist dieser Use Case primär nur für die Lokomotivhalter, die mit den Güterwagen fahren, interessant. Die Güterwagenhalter selbst sind hier nur indirekt betroffen, bspw. um den Verbrauch und die Leistung für die Kostenkalkulationen zu berücksichtigen.)
Sicherheitsrelevanz		Nein
Umsetzbarkeit (eingeschätzt durch Experten)		Leicht

Die Überwachung des elektrischen Antriebszustandes ist bereits mit den wichtigsten Sensoren umgesetzt. So befinden sich bereits Strom- und Spannungssensoren am Fahrzeug. Auch Temperatursensoren sind bereits zu finden. Weitere Sensoren können zusätzlich eingebaut werden, um die Genauigkeit zu erhöhen. Die folgende Tabelle 14 und Abbildung 12 zeigen, welche Sensoren insgesamt genutzt werden und notwendig sein können. In folgenden Projekten gibt es bereits Aktivitäten in diese Richtung:

- Im Projekt SensoDIMARIS wurden Körperschallsensoren zur Erkennung von Verschleiß am Fahrzeugantrieb erprobt. Durch die Kopplung von geografischen Koordinaten und Daten verdächtiger Geräusche können die Körperschallsensoren der Infrastruktur oder dem Fahrzeug zugeordnet werden. Ebenso verhält es sich mit Beschleunigungs- und Temperatursensoren. [23]

- In Unterwerken der DB Energie werden Hall-Sensoren zur Messung des Stroms des Antriebs verwendet, was vom Prinzip her auch auf fahrzeugseitige Antriebe übertragen werden kann. [24]

TABELLE 14: MÖGLICHE SENSOREN FÜR DEN USE CASE „FAHRZEUG ÜBERWACHT FAHRZEUG: ANTRIEBSZUSTAND „ELEKTRO“)

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Stromsensor	Versorgungsleitung Traktionsbatterie	Stromversorgung Antrieb	Ist bereits standardmäßig eingebaut.
Spannungssensor	Versorgungsleitung Traktionsbatterie	Spannungsversorgung Antrieb	Ist bereits standardmäßig eingebaut.
Hall-Sensor	Rotorwelle	Motordrehzahl	Ein Sensor wäre vermutlich ausreichend.
Rotorlagesensor	Rotorwelle	Winkellage des Rotors	
Torsionssensor	Rotorwelle	Verwindung der Antriebswelle	
Temperatursensor	Gesamtbereich Antrieb	Temperatur der Antriebskomponenten	Bringt zusätzliche Informationen.
Beschleunigungssensor	Gesamtbereich Antrieb	Detektion schadhafter Vibrationen	Würde für SIL 2 und damit höhere Anforderungen sorgen. Daher nur einsetzen, wenn dies vertretbar ist.
Mikrofon	Gesamtbereich Antrieb	Lärmentwicklung, Störgeräusche	Bringt zusätzliche Informationen.
Drucksensor	Kühlsystem Antrieb	Ermittlung Kühlmitteldruck	Bringt zusätzliche Informationen.

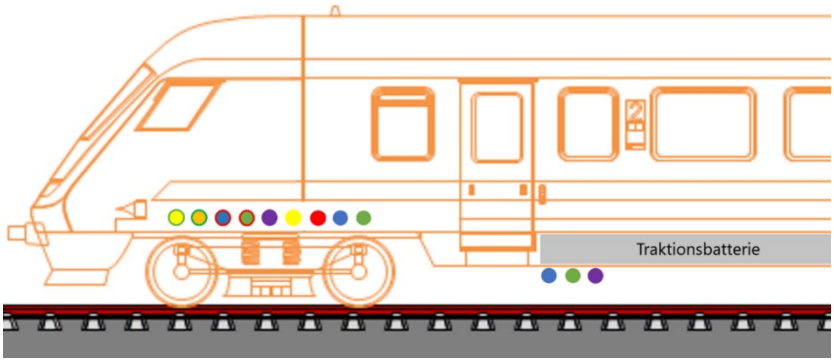


Abbildung 12: Montageorte der Sensoren für Use Case „Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)“

Grundlegende Sensordaten, die im Rahmen des regulären Betriebs an den Antriebskomponenten von Triebfahrzeugen erfasst werden, sind die Versorgungsspannung und die Stromstärke. Die Ermittlung der Spannung wird bereits serienmäßig durch den Oberspannungswandler detektiert, der im speziellen die Fahrdrahtspannung von 15 kV erfasst. Die Betriebsspannung der Fahrmotoren liegt bei 0,5 – 0,6 kV. Um die korrekte Funktion der Fahrmotoren sicherzustellen, kann zudem eine Detektion der Spannung im Bereich der Versorgungsleitung der Fahrmotoren erfolgen. Die Bestimmung der Stromstärke erfolgt ebenfalls im Bereich der Versorgungsleitung des Fahrmotors und kann bspw. durch die Verwendung eines Messwiderstandes realisiert werden. Hinsichtlich des oberleitungslosen Betriebs können zudem im Bereich der Traktionsbatterie Sensoren zur Ermittlung der Spannung sowie der Stromstärke angebracht werden. Die in diesem Zusammenhang gewonnenen Messwerte ermöglichen es, eine Aussage über den aktuellen Zustand der Traktionsbatterie zu treffen und zudem Prognosen bezüglich des Verbrauchs respektive der Reichweite des Triebfahrzeuges bei oberleitungsloser Fahrt zu erstellen. [45][46]

Weitere wichtige Kennwerte, die zur Gewährleistung einer störungsfreien Funktion der elektrischen Antriebskomponenten genutzt werden können, sind das Antriebsmoment und die Motordrehzahl. Die Bestimmung des Antriebsmoments erfolgt dabei im Bereich der Rotorwelle und wird durch die Verwendung eines Drehmoment-Messflansches realisiert. Durch die Ermittlung der Drehmomentwerte kann zu jedem Zeitpunkt nachvollzogen werden, welches Antriebsmoment durch den jeweiligen Fahrmotor zur Verfügung gestellt wird. Die Motordrehzahl kann durch die Verwendung eines Inkrementalgebers (z. B. Hall-Sensor) realisiert werden. Mit Hilfe der detektierten Motordrehzahl wird gewährleistet, dass sich diese während des Betriebs im optimalen respektive unkritischen Bereich befindet. Die Bestimmung der Rotorposition kann dabei über einen Rotorlagesensor erfolgen und eine Effizienzsteigerung ermöglichen. [46][47][48]

Neben den grundsätzlichen Messwerten wie Spannung oder Drehmoment spielen aber auch Faktoren eine signifikante Rolle, die während des Betriebs auf die Komponenten des Antriebssystems einwirken. Diesbezüglich spielt die Temperatur im Bereich der Fahrmotoren sowie an der Traktionsbatterie eine wichtige Rolle, um die korrekte Funktion des Antriebsstranges sicherzustellen. Zur Erfassung der Temperatur werden dabei NTC oder PTC Elemente verwendet. [49]

Zusätzlich können Daten zu Vibrationen oder Störgeräuschen im Bereich der Antriebskomponenten erfasst werden. Durch Flachstellen am Rad oder Defekte an der Motor-, respektive Radsatzlagerung können im Bereich der Fahrmotoren Vibrationen auftreten, die den Antrieb von Triebfahrzeugen beschädigen können. Anhand von Beschleunigungsaufnehmern, die zur Detektion von Vibrationen dienen, kann ermittelt werden, ob eine Beschädigung vorliegt und welche Maßnahmen hinsichtlich der Beschädigung

ergriffen werden müssen. [15] Aber auch durch die Messung von Störgeräuschen, bspw. bei einer erhöhten Geräuschentwicklung im Bereich der Lagerung, lassen sich Defekte frühzeitig erkennen und schwerere Beschädigungen des Gesamtsystems vermeiden.

Use Case „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“

Die wichtigsten Informationen des Use Cases „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“ sind in Tabelle 15 aufgeführt. Im Anschluss wird erläutert, in welchen Projekten solche Systeme bereits in Erprobung sind.

TABELLE 15: BASISINFORMATIONEN DES USE CASES „INFRASTRUKTUR ÜBERWACHT FAHRZEUG – NICHT SICHERHEITSRELEVANT“

Ziel		Ermittlung von Zustandsdaten des Fahrzeugs über infrastrukturseitige Messpunkte zum frühzeitigen Erkennen von kritischen Fällen und Trends zur Vermeidung von schweren Schäden (zustandsorientierte Instandhaltung der Fahrzeuge) *Mehrwert ggn. bestehenden Systemen:* Bestehende Systeme sollen weiträumig umgesetzt werden und ggf. um weitere Komponenten ergänzt werden.
Installationsort der Sensoren		Infrastruktur
Nutzen	**Primär**	Fahrzeughalter und/oder ECM
	Sekundär	EIU (Falls bei einem Messwert immer wieder ein Schwellwert überschritten wird, kann dies auf einen Schaden in der Infrastruktur hindeuten.)
Fahrzeugart		Alle Fahrzeuge (Reisezug- und Güterwagen, Triebwagen, Lokomotiven, Messfahrzeuge).
Verkehrsart		Personen- und Güterverkehr
Sicherheitsrelevanz		Nein
Umsetzbarkeit (eingeschätzt durch Experten und Expertinnen)		Schwer

Für diesen Use Case gibt es eine Vielzahl an möglichen Sensoren. Einige davon, insbesondere solche mit sicherheitsrelevantem Funktionsnutzen, befinden sich bereits lange Jahre im Einsatz. Weitere Komponenten sind seit kürzerer Zeit ebenfalls in Nutzung. Dennoch wäre auch eine Erweiterung um einige Sensoren denkbar. Die folgende Aufzählung erläutert diese Tatsachen:

- Radsensoren, auch bekannt als HOA und FBOA, sind bereits im gesamten Streckennetz in regelmäßigen Abständen verbaut. Ebenfalls können mit den DafuR-Anlagen der DB seit etlichen Jahren auch unrunde Räder, Überladungen und Schiefladungen über Dehnungsmessstreifen

(DMS) und auch faseroptische Sensoren detektiert werden. Möglich ist dadurch auch eine Heißläuferortung und ein Kraftsensor zur dynamischen Radkraftmessung. [25]

- Seit ein paar Jahren gibt es auch einige infrastrukturseitige Anlagen der Firma RailWatch. Diese beinhalten eine Kamera zur Bilderfassung, einen Laserscanner zur Strukturerfassung, ein Mikrofon zur Geräuscherfassung, Radsensoren, und einen thermischen Sensor zur Erfassung der Betriebstemperatur und Wärmeentwicklung. [50][26]

- Seit 2021 ist in Wien das System Argos OOR im Einsatz, das über Beschleunigungssensoren und DMS an der Schiene unrunde Räder, Riffel und Flachstellen erkennen. Oberstes Ziel ist dabei der Immissionsschutz. [27] Gleichzeitig wurde auch das System DMA installiert, das über Beschleunigungs- und Schwinggeschwindigkeitssensoren sowie DMS Geschwindigkeiten misst und Spannungsanalysen durchführt. [28]

- Im Projekt SensoDIMARIS wurden Körperschallsensoren eingebaut, bei denen geografische Koordinaten und Daten verdächtiger Geräusche gekoppelt und dadurch der Infrastruktur oder dem Fahrzeug zugeordnet werden können. Ebenso verhält es sich mit Beschleunigungs- und Temperatursensoren. [23]

- Ein Beschleunigungssensor zur Detektion von Flachstellen befindet sich im Projekt ZF connect@rail in Erprobung. [14]

Die folgende Tabelle 16 und Abbildung 13 geben eine Übersicht über alle möglichen Sensoren und beinhalten für eine bessere Vollständigkeit auch die bereits vorhandenen Sensoren. Um einen besseren Überblick zu erhalten, ist eine Einschätzung zum Aufwand-Nutzen-Verhältnis in der entsprechenden Spalte aufgeführt.

TABELLE 16: MÖGLICHE SENSOREN FÜR DEN USE CASE „INFRASTRUKTUR ÜBERWACHT FAHRZEUG – NICHT SICHERHEITSRELEVANT“

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Beschleunigungssensor	Schiene, Schwelle, Gleistragplatte bzw. Tragwerk	Laufflächenschäden, Radsatzlagerschaden, Federschaden	Nur eine dieser beiden Komponenten sollte eingesetzt werden, ansonsten doppelter Aufwand.
Körperschallsensor	Schiene, Schwelle, Gleistragplatte bzw. Tragwerk	Radunrundheiten, Riffel, Verschleiß an Bauteilen	
DMS	Schiene, Schienenfuß, Schwelle	Radzustandsermittlung, Federbruch, Y und Q am Gleis, Gewichtsmessung	Im Einsatz in DafuR-Anlagen.
Infrarotsensor	Im Gleis	Heißläufer, feste Bremsen	Im Einsatz als standardmäßige sicherheitskritische Komponente.

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Induktiver Näherungssensor	Im Gleis	Detektion herabhängender Teile	Abwägen, wie häufig herabhängende Teile vorkommen und ob sich der Einsatz lohnt.
Radsensor	Im Gleis	Raddurchmesser, Radmittenimpuls, Flachstellen, Radaufprallkräfte	Im Einsatz als standardmäßige sicherheitskritische Komponente.
Faseroptischer Sensor	Nah am Gleis	Raddefekte, Radkraft, Beladungslast, Schäden bzw. Instandhaltungspotenzial	Teure Technologie, u. U. keine eindeutige Zuordnung zu Fahrzeug- oder Infrastrukturkomponente möglich.
Schallpegelmesser	An Halterung neben/über Gleis	Schallquellenortung	Nur eine dieser beiden Komponenten sollte eingesetzt werden, ansonsten doppelter Aufwand.
Akustische Kamera	An Halterung neben/über Gleis	Schallquellenortung	
Infrarottemperatursensor	An Halterung neben/über Gleis	Punktuelle Erfassung von Temperaturen	Nur eine dieser beiden Komponenten sollte eingesetzt werden, ansonsten doppelter Aufwand. Flächendeckende Erfassung vorteilhafter.
Infrarot-/Wärmebild-/ Thermografiekamera	An Halterung neben/über Gleis	Flächendeckende Erfassung von Temperaturen	
Kamera	An Halterung neben/über Gleis	Bildliche Aufnahme eines Wagens	Im Einsatz in infrastrukturseitigen Anlagen.
Laserscanner	An Halterung neben/über Gleis, Schwellenfach	Zustand von Bauteilen durch Abstandsmessung	Aufwand vermutlich zu hoch, da dies nur bei Kenntnis exakter Wagengeometrie Vorteile bringt.

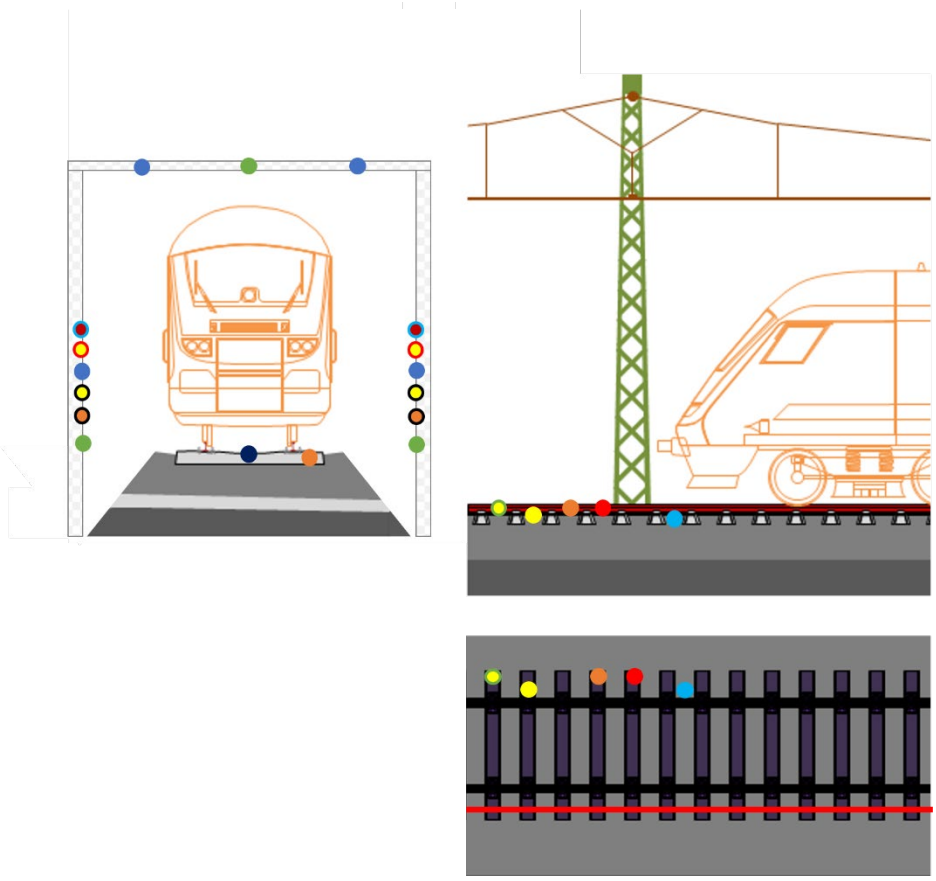


Abbildung 13: Montageorte der Sensoren für Use Case „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“

Grundsätzlich können alle in der Tabelle genannten Sensoren eingebaut werden. Da jedoch einige Sensoren gleiche und/oder ähnliche Komponenten überwachen, ist es ausreichend, die Sensoren auf eine geringere Zahl zu reduzieren. Es bietet sich an solche zu wählen, die bereits weiträumig erprobt sind, ein gutes Kosten-Nutzen-Verhältnis bieten und/oder mehrere Messwerte erfassen können. Darüber hinaus muss erwähnt werden, dass die verwendeten Sensoren meist für sehr vielfältige Bauteile genutzt werden können. Es ist daher davon auszugehen, dass jedem Messwert nicht immer exakt die beschädigte Komponente zugeordnet werden kann. In diesem Fall muss im Anschluss eine genauere Begutachtung des Fahrzeugs stattfinden.

Für eine bessere Übersichtlichkeit lassen sich die Sensoren entsprechend ihrer Einbauorte gliedern. An der Schiene, den Schwellen und teilweise den Gleistragplatten bzw. dem Tragwerk können Beschleunigungssensoren, DMS und Körperschallsensoren montiert werden. Die Beschleunigungssensoren können Laufflächenschäden, wie Radunrundheiten (d. h. Flachstellen, Polygonisierung, Ausbröckelung) und Riffel, Radsatzlagerschäden und Federschäden detektieren. [28] DMS sind häufig in Kraftaufnehmern verbaut und können den Radzustand ermitteln, Federbrüche erkennen, die Kräfte am Gleis bestimmen sowie Gewichtsmessungen durchführen. [51][26][25][29][30][31] Über Körperschallsensoren ist die Erkennung von Verschleiß an Bauteilen (wie Füllzustand Tanks, Türmechanik, Fahrzeugantrieb) sowie Radunrundheiten und Riffel möglich. [23][28]

Im Gleis selbst können Infrarotsensoren, induktive Näherungssensoren und Radsensoren eingebaut werden. Ein Infrarotsensor kann Heißläufer und feste Bremsen erkennen und ist bereits im Einsatz, bekannt als HOA bzw. FBOA. [51] Der induktive Näherungssensor kann vom Fahrzeug herabhängende

Teile detektieren, indem ein induktives Signal bei Näherung eines Bauteils ausgelöst wird. [51] Radsensoren sind ebenfalls bereits im Einsatz und sie können verschiedene Elemente detektieren, wie Raddurchmesser, Radmittenimpuls, Flachstellen und Radaufprallkräfte. [51][32]

Nah am Gleis werden faseroptische Sensoren verbaut. Diese können über Glasfaserkabel Vibrationen und Geräusche erkennen und damit Raddefekte lokalisieren, die Radkraft und Beladungslast ermitteln sowie Schäden bzw. das allgemeine Instandhaltungspotenzial bestimmen. [31]

An Halterungen neben und/oder über dem Gleis können Schallpegelmesser, Infrarottemperatursensoren, Infrarot-/Wärmebild-/Thermografiekameras, Kameras und Laserscanner angebracht werden. Die Schallpegelmesser erfassen Schallquellen, orten diese und detektieren dadurch Radsatzlagerschäden, unübliche Betriebsgeräusche und Flachstellen. [51][26][28][33] Für die Bestimmung von Temperaturzuständen können Infrarottemperatursensoren punktuell bestimmte Temperaturen (z. B. Wärmeentwicklung, thermische Überlastung des Rades) erfassen, während Infrarot-/Wärmebild-/Thermografiekameras flächendeckend Temperaturen erfassen und damit Lagerschäden, thermische Überlastungen des Rades durch Bremsen, feste Bremsen oder überhitzte Ladung detektieren. [51] Die Kamera nimmt ein Bild eines Wagens auf und kann mithilfe von Künstlicher Intelligenz und menschlicher Auswertung eine Detektion von Schäden ermöglichen. [51][26] Der Laserscanner nutzt das Prinzip der Abstandsmessung und kann dadurch den Zustand der Ladung, verschiedener Komponenten oder des Radprofils sowie das Lichtraumprofil erfassen. Zusätzlich lässt sich diese Technologie auch im Schwellenfach montieren, um Unterbodenkomponenten zu überprüfen. [51][34]

Use Case „(Teil-)Automatisierung der Fahrzeuginstandhaltung“

Die wichtigsten Informationen des Use Cases „(Teil-)Automatisierung der Fahrzeuginstandhaltung“ sind in Tabelle 17 aufgeführt. Im Anschluss wird erläutert, in welchen Projekten solche Systeme bereits in Erprobung sind.

TABELLE 17: BASISINFORMATIONEN DES USE CASES „(TEIL-)AUTOMATISIERUNG DER FAHRZEUGINSTANDHALTUNG“

Ziel		Automatisierte Schadenserkennung und Reduzierung von manuellen Tätigkeiten bei der Begutachtung eines Fahrzeuges bei Ankunft an der Werkstatt. Dies führt zu Zeitersparnis, optimierten Arbeitsabläufen, einem Ausgleich des Kapazitäts- und Fachkräftemangels und zu einer höheren Fahrzeugverfügbarkeit. *Mehrwert ggn. bestehenden Systemen:* reduzierte manuelle Tätigkeiten und Personalbelastung (Laufwege), optimierte Arbeitsabläufe, effizientere Planung des Ersatzteilmanagements.
Installationsort der Sensoren		Infrastruktur
Nutzen	**Primär**	ECM
	Sekundär	Fahrzeughalter
Fahrzeugart		Alle Fahrzeuge: Reisezug- und Güterwagen, Triebwagen, Lokomotiven, Messfahrzeuge

Verkehrsart	Personen- und Güterverkehr
Sicherheitsrelevanz	Nein
Umsetzbarkeit (eingeschätzt durch Experten und Expertinnen)	Leicht

Eine automatisierte Schadenserkennung befindet sich bereits im Einsatz in folgenden Anwendungen:

- Die DB verwendet Kamerabrücken mit acht Kameras zur Begutachtung der Wagen, allerdings wird noch keine Unterfluransicht erstellt. Im Projekt „E-Check“ der DB Fernverkehr wird eine Automatisierung der Laufwerkskontrolle (umfasst Untersuchungen im Laufwerksbereich) und der Nachschau (umfasst zusätzlich Untersuchungen an Bremsen, Wagenkasten, Dachausrüstung, Fahrgastraum) angestrebt. Eingesetzt werden sollen dabei Kamerasensortore mit 360° Perspektiven des Bodens, der Seiten, des Daches und der Drehgestelle sowie IT- und Rechnertechnik zur automatisierten Auswertung und Roboter zur zusätzlichen Datenaufnahme und Ver- und Entsorgung von Wasser am Zug. [35]

- Es werden Gleisroboter erprobt, die Entfernungen über Lidar und Kamera messen. Damit lassen sich Unterflurchecks bei stehenden Fahrzeugen realisieren. [36]

- Der Einsatz von Radprofil-Messanlagen ist üblich. Es ist möglich, dieses System mit der automatisierten Schadenserkennung zu koppeln.

Tabelle 18 und Abbildung 14 zeigen die möglichen Sensoren und deren Montageorte.

TABELLE 18: MÖGLICHE SENSOREN DES USE CASES „(TEIL-)AUTOMATISIERUNG DER FAHRZEUGINSTANDHALTUNG (SCHADENSERKENNUNG)“

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Kamera	Halterung neben und/oder über dem Gleis	Bildliche Aufnahme eines Wagens	Befindet sich bereits im Einsatz.
Gefächerte Laser	Im Gleis	Höhenprofile mittels Lichtschnittverfahren	Geeignet für eine Unterbodenbegutachtung.
Lidar	Halterung neben und/oder über dem Gleis	Zustand von Bauteilen durch Abstandsmessung	Nur eine dieser beiden Komponenten sollte eingesetzt werden, ansonsten doppelter Aufwand.
Radar	Halterung neben und/oder über dem Gleis	Zustand von Bauteilen durch Abstandsmessung	
Radprofil-Messanlagen	Im Gleis	Radprofil	Befindet sich bereits im Einsatz.

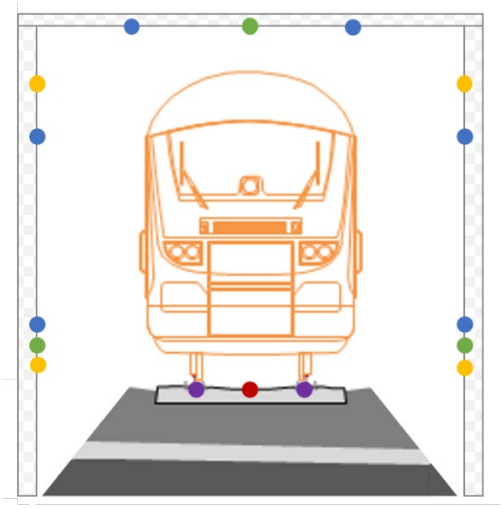


Abbildung 14: Montageorte der Sensoren für Use Case „(Teil-) Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)“

Eine Möglichkeit der Schadenserkennung ergibt sich durch den Einsatz von Kameras. Diese nehmen ein Bild eines Wagens unmittelbar nach der Ankunft an der Werkstatt auf und ermöglichen so, die Schadensaufnahme zu beliebiger Uhrzeit und unabhängig von Witterungseinflüssen durchzuführen. Um die Auswertung der Bilder nicht durch den Menschen vorzunehmen, sollte dies langfristig durch KI Intelligenz realisiert werden. Solche Kamerabrücken sind teilweise schon im Einsatz, allerdings noch ohne eine automatisierte Auswertung. [Workshop 1] [35]

Um genauere Maße eines Fahrzeuges zu erhalten, sind Kameras nur bedingt geeignet. Besser eignen sich dafür u. a. gefächerte Laser. Über Lichtschnittverfahren bestimmen diese Höhenprofile, wie z. B. das Radprofil. Dies ist allerdings nur im Stillstand des Fahrzeugs möglich. [36][37] Ebenso bieten sich Lidar und Radar an. Mittels Abstandsmessung können Zustände spezifischer Bauteile ermittelt werden. [Workshop 1] Hierfür ist allerdings eine genaue Positionskennung der Bauteile notwendig, was auf einfache Weise nur im Stillstand möglich ist oder mit einer sehr hohen Sensorgenauigkeit realisiert werden kann.

Ebenso können die üblichen Radprofil-Messanlagen im Gleis montiert werden und zur standardmäßigen Überprüfung genutzt werden.

Use Case „Weichenferndiagnose“

Die wichtigsten Informationen des Use Cases „Weichenferndiagnose“ sind in Tabelle 19 aufgeführt. Im Anschluss wird erläutert, in welchen Projekten solche Systeme bereits in Erprobung sind.

TABELLE 19: BASISINFORMATIONEN DES USE CASES „WEICHENFERNDIAGNOSE“

Ziel	Gewährleistung der störungsfreien Funktion der Weiche für die sichere Befahrung des Weichenbereiches. Dafür werden Störungen respektive Funktionseinschränkungen ermittelt, die Rückschlüsse auf Reparatur- oder Wartungsmaßnahmen ermöglichen, um die Wartungsintervalle zu optimieren und die Kosten zu reduzieren.

		Mehrwert ggn. bestehenden Systemen: Für eine frühzeitige Prognose können zusätzliche Sensoren eingebaut werden. Der Einbau kann an jeder Weiche realisiert werden.
Installationsort der Sensoren		Infrastruktur
Nutzen	**Primär**	EIU
	Sekundär	EVU: Zustand der Weichen gibt Informationen über eine möglicherweise reduzierte Geschwindigkeit beim Befahren der Weiche
Fahrzeugart		Alle Fahrzeuge (Reisezug- und Güterwagen, Triebwagen, Lokomotiven, Messfahrzeuge)
Verkehrsart		Personen- und Güterverkehr (Als reiner Infrastrukturfall ist dieser Use Case dennoch auch für den Personen- und Güterverkehr interessant, weil der Zustand der Weiche Einfluss auf z. B. die Geschwindigkeit haben kann.)
Sicherheitsrelevanz		Ja
Umsetzbarkeit (eingeschätzt durch Experten und Expertinnen)		Leicht

Bereits im Einsatz bzw. in Erprobung sind die folgenden Systeme:

- Im System infraView DIANA werden bereits seit mehreren Jahren Weichen überwacht, indem defekte Antriebsmotoren von Weichen im Stellwerk erkannt werden. [38]
- Das System VABtrack überwacht Weichenheizungen und -steuerungen und kann Störungszustände erfassen. [39]

In Tabelle 20 und Abbildung 15 werden sämtliche Sensoren und Einbaupositionen aufgeführt, die bzgl. des Use Cases „Weichenferndiagnose“ Verwendung finden.

TABELLE 20: MÖGLICHE SENSOREN DES USE CASES „WEICHENFERNDIAGNOSE“

Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Stromsensor	● Versorgungsleitung Antriebsmotor	Stromverbrauch Antrieb	Ist in den meisten Antrieben standardmäßig eingebaut.
Dehnmessstreifen	● Schiene, Herzbereich Weichenzunge	Belastung Weichensegment Längskräfte im Weichenbereiche	Wird bereits teilweise verwendet, ein Einsatz bietet sich daher an.

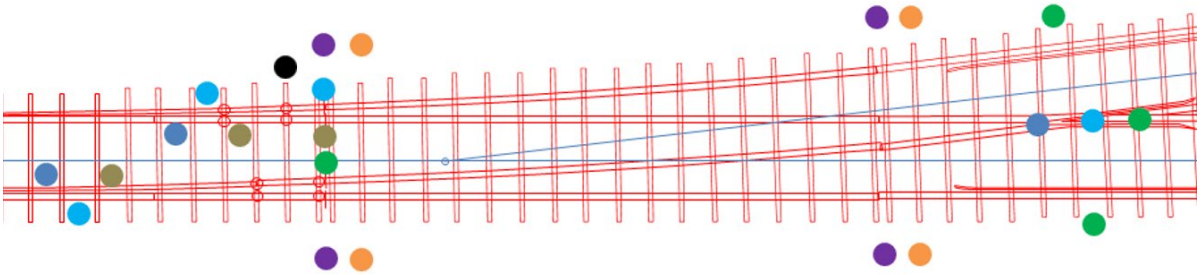
Sensor	Einbauort	Messwert	Einschätzung von Aufwand zu Nutzen
Kraftsensor	● Verschraubungen	Vorspannkraft	Messung der Vorspannkraft bei Weichenverschraubung ist bereits im Einsatz.
Endlageschalter	● Weichenzunge Weichenverschlüsse Übertragungsgestänge	Weichenstellung Stellzeiten Zugriff-, Zeiten	Bietet sich für einen Einsatz an.
Temperatursensor	● Weichenzunge Übertragungsgestänge	Temperatur	Lässt sich „beeinflussungsfrei“ auslegen.
Kamera	● Umfeld Weiche	Weichenstellung Weichenzugriff	Bietet eine übersichtliche und genaue Darstellung der Situation, die Leistungsfähigkeit von Kamerasystemen im Automotivbereich zeigt, dass eine hohe Genauigkeit möglich ist.
Drucksensor	● Umfeld Weiche	Luftdruck (weichennahe Wetterdaten)	Bei zuverlässiger Wettervorhersage nicht notwendig.

Als grundlegend zu erfassende Sensordaten sind die Höhe der Versorgungsspannung und der Stromstärke zu nennen, die dem Weichenantrieb zur Verfügung gestellt werden. Diesbezüglich können entsprechende Sensoren im Bereich der Versorgungsleitungen des Weichenantriebes angebracht werden. Zur Bestimmung der Stromstärke kann einerseits ein Messwiderstand verwendet werden, aber auch die Bestimmung der magnetischen Flussdichte im Bereich der Versorgungsleitung gibt Aufschluss über die Höhe der Stromstärke. [46] [52]

Weitere Messwerte, die für die Sicherstellung der korrekten Funktion der Weiche benötigt werden, sind die Zug- und Druckkräfte, die im Bereich des Übertragungsgestänges, im Bereich der Radsatzführung und an den Weichenzungen auftreten. Dabei lassen sich Zug- und Druckkräfte durch entsprechend ihrer gewünschten Funktion angebrachte Dehnmessstreifen detektieren und geben unter anderem Aufschluss über die Längenänderung im Bereich der Weichenzungen, die aufgrund von Temperaturänderung auftritt.

Weiterhin kann die Temperatur im Bereich der Weiche detektiert werden. Durch die richtige Positionierung von Temperatursensoren im Weichenbereich können Temperaturdaten gesammelt werden, um eine bessere Regelung oder optimierte Anwendung der Weichenheizung zu erzielen. [39]

Abbildung 15: Montageorte der Sensoren für Use Case „Weichenferndiagnose“



Zudem kann die Vorspannkraft der Weichenverschraubung ermittelt werden, um ein unzulässiges Lösen der Verschraubungen im Weichenbereich zu verhindern. In diesem Zusammenhang werden spezielle Kraftsensoren genutzt. Diese Kraftsensoren gleichen in ihrer Dimensionierung einer herkömmlichen Unterlegscheibe und werden zwischen Schiene und Schraubenkopf positioniert. [53][54]

Über Endlageschalter und induktive Sensoren können die korrekte Weichenstellung der Weichenzunge, die Stellzeiten der Weichenverschlüsse und die Zugriffszeiten der Übertragungsgestänge bestimmt werden. [53]

Es ist zu beachten, dass die korrekte Funktion der Weiche einen hohen Stellenwert innerhalb des gesamten Streckennetzes einnimmt. Die Störung respektive Manipulation einer Weiche kann zu schwerwiegenden Störungen im gesamten Streckennetz führen. Dies hat Auswirkungen auf den gesamten Zugverkehr, was Negativeffekte wie Verspätungen oder Zugausfälle hervorruft. Dahingehend bietet die Überwachung des Weichenbereiches durch geeignete Kamerasysteme einen guten Lösungsansatz, um eine Manipulation der Weiche zu unterbinden. Einen zusätzlichen Beitrag zur Gewährleistung einer störungsfreien Funktion der Weiche können Wetterdaten liefern, indem anhand geeigneter Sensoren, beispielsweise der Luftdruck oder die Temperatur ermittelt werden. [40]

Peripherie

Zur Peripherie der Sensorlösungen gehören die Stromversorgung, die Datenübertragung und Kommunikation. Aufgrund der unterschiedlichen Gegebenheiten muss zwischen fahrzeugseitigen Use Cases und infrastrukturseitigen Use Cases unterschieden werden. Bei den fahrzeugseitigen Use Cases bedarf es zudem einer Unterteilung hinsichtlich der Stromversorgung. Diesbezüglich ist zwischen Fahrzeugen mit und ohne Stromversorgung zu unterscheiden.

Peripherie für Fahrzeug Use Cases

Stromversorgung

Alle Sensoren sowie zugehörige Einheiten müssen auf dem Fahrzeug mit Strom versorgt werden. Ein wesentlicher Unterschied ergibt sich hierbei durch die Art der Fahrzeuge. Während Personenwagen, Lokomotiven und Messfahrzeuge über eine bereits bestehende Stromversorgung verfügen, besitzen Güterwagen keine Stromanschlüsse zur Versorgung der Sensoren. Daher muss bei der Betrachtung der Stromversorgung zwischen diesen beiden Fällen unterschieden werden. In beiden Fällen können die Sensoren, wenn sie nicht dauerhaft eingeschaltet sein sollen, über ein GPS-Signal aktiviert werden, indem bei Änderung dieses Signals eine Aktivierung der Sensoren erfolgt.

Für die Fahrzeuge mit Stromversorgung ist der Betrieb der Sensoren auf einfachere Weise zu realisieren. Die Sensoren können an die bestehende Infrastruktur des Fahrzeugs angeschlossen werden. Falls dies aufgrund von schlecht realisierbarer Kabelführung nicht möglich sein sollte oder ein Eingriff in das Fahrzeugsystem vermieden werden soll, sind die Optionen für Fahrzeuge ohne Stromversorgung heranzuziehen.

Bei Fahrzeugen ohne Stromversorgung ist der Betrieb der Sensoren nicht so einfach zu realisieren. Es gibt mehrere Möglichkeiten, die in Tabelle 21, Tabelle 22 und Tabelle 23 beschrieben werden. Für eine genauere Ausarbeitung sei an dieser Stelle auf den DZSF-Forschungsbericht zum Projekt „Mindestausrüstung von Güterwagen“ verwiesen. Drei sinnvolle Möglichkeiten zur Stromerzeugung sind ein Photovoltaik-Modul, ein Achsgenerator oder ein Vibration-Energy-Harvester (VEH). Windgeneratoren und Radio Frequency finden in Schienenfahrzeugen praktisch keine Anwendung. Der erzeugte Strom muss bei allen Varianten in einer Batterie gespeichert werden. Durch diese werden die Sensoren über Kabel mit Strom versorgt. [51] Hinsichtlich des zukünftigen Einsatzes der Digitalen Automatischen Kupplung (DAK) im Güterverkehr ist anzumerken, dass dadurch auch Güterwagen über eine Stromversorgung verfügen würden und somit eine Versorgung der Sensoren am Güterwagen gewährleistet wäre.

TABELLE 21: WICHTIGSTE EIGENSCHAFTEN DES SOLARMODULS [EIGENE DARSTELLUNG NACH [51]]

Option 1: Photovoltaik-Modul	
Funktionsweise	Durch die Sonne erzeugte Energie wird durch das Modul aufgenommen
Montageort	An der Seitenwand des Wagenkastens oder Untergestells
Energieaufnahme	Mittelmäßig, 10 mW/cm²
Vorteile	Bereits erprobte Technologie, viele Produkte sind vorhanden, daher niedrige Investitionskosten
Einschränkung	Funktioniert nur bei Tageslicht und ist anfällig gegenüber Verschmutzung

TABELLE 22: WICHTIGSTE EIGENSCHAFTEN DES ACHSGENERATORS [EIGENE DARSTELLUNG NACH [51]]

Option 2: Achsgenerator	
Funktionsweise	Ein Permanentmagnetrotor ist an der Radachse befestigt und die Spulen als Stator im Gehäusedeckel. Durch die Raddrehung wird Energie erzeugt. Üblicherweise ist ein solcher Generator direkt im Radsatzlager integriert und für eine bestimmte Achsbaugruppe entwickelt. Die erzeugte Leistung ist abhängig von der Baugröße des Generators und der Fahrgeschwindigkeit
Montageort	Achslager
Energieaufnahme	Hoch, 10 – 100 W
Vorteile	Hohe erzeugte Leistung
Einschränkung	Hohe Investitionskosten, Umbau des Achslagers erforderlich, funktioniert nur während der Fahrt und ist abhängig von der Fahrgeschwindigkeit

TABELLE 23: WICHTIGSTE EIGENSCHAFTEN DES VIBRATION-ENERGY-HARVESTER [EIGENE DARSTELLUNG NACH [51]]

Option 3: Vibration-Energy-Harvester (VEH)	
Funktionsweise	Elektromagnetische VEH: zwischen einem Paar Federn ist eine Masse montiert, an der Innenseite der Masse sind hochfeste Magnete angebracht. Eine Induktionsspule ist in der Halterung stationär angebracht, sodass eine Relativbewegung des Magnetfeldes um die Spule herum erreicht wird, wodurch ein Wechselstromausgang entsteht Elektrostatische VEH: Anregung durch Vibrationen durch z. B. Fahrweg Piezoelektrische VEH: bisher nur in Forschungsprojekten untersucht, deutlich geringere Leistung und daher nur Versorgung einzelner Sensoren möglich
Montageort	Achslager oder Drehgestell
Energieaufnahme	Gering, bis 100 mW. Ist abhängig von der Baugröße des VEH, dem Montageort, der Fahrgeschwindigkeit und dem Zustand des überfahrenen Gleises und Oberbaus
Vorteile	Robust und für ungefederte Komponenten geeignet
Einschränkung	Hohe Investitionskosten, funktioniert nur beim Fahren, ist nicht geeignet am Wagenkasten

Datenübertragung und -verarbeitung

Damit die Sensordaten auch genutzt werden können, muss eine Datenübertragung und -verarbeitung stattfinden. Dafür wurden im Güterwagensektor von der Industrieplattform für Telematik und Sensorik im Schienengüterverkehr (ITSS) bereits vier sogenannte ITSS-Schnittstellen bestimmt, die jeweils beschreiben, über welche Wege Daten übertragen werden können. Die ersten beiden sind bereits ausreichend spezifiziert. Die folgenden vier Schnittstellen gibt es [51] [55]:

- ITSS 1: Server Telematikanbieter zu (Kunden-)Server
- ITSS 2: Sensoren zu Telematiksystem
- ITSS 3: Telematiksystem zu mobilem Endgerät
- ITSS 4: Intrazug-Kommunikation Wagen zu Wagen zu Lok

Denkbar sind dabei verschiedene Kopplungen der Schnittstellen [51]:

- ITSS 1 und 2 (On-Board online): Hierbei werden Sensordaten permanent am Wagen aufgezeichnet. Dort werden die Rohdaten in einem Telematiksystem o. Ä. gespeichert, in lokaler Echtzeit verarbeitet und mit geringer Latenz per Mobilfunk (LTE/5G) aktiv zunächst an den Server des Telematikanbieters und von dort zum (Kunden-)Server übertragen. Es kann also stets der aktuelle Stand abgerufen werden.
- ITSS 2 und 3 (On-Board offline): Die Sensordaten werden am Wagen aufgezeichnet und lokal mit geringem Energiebedarf in Zwischenspeichern gespeichert. Das Auslesen der Daten für die Auswertung und Analyse erfolgt anschließend manuell über eine physische Schnittstelle (z. B. NFC, durch Anschließen eines Gerätes, Kurzstreckenfunk, o. Ä.).
- ITSS 1 (Flottenmanagement/Telematik): Die Aufzeichnung von Daten und die Übertragung der Daten erfolgt mehrmals am Tag per Mobilfunk (3G/LTE). Dazu werden die Daten zunächst an den Server des Geräteherstellers und anschließend an den Wagenhalter übermittelt. Der Unterschied zum System „On-Board online“ besteht darin, dass keine zusätzlichen Sensoren am Wagen verbaut sind, sondern ausschließlich in der Telematikbox. Diese dient zur Positionsbestimmung, um das Flottenmanagement zu realisieren. Heutzutage ist in vielen Fällen ein zusätzlicher Beschleunigungssensor zur Bestimmung harter Auflaufstöße installiert.
- Für den Personenverkehr und nach Einsatz der DAK ITSS 2 und 4, ggf. 1 (Option): Die Sensordaten können über ITSS 2 an das Telematiksystem eines Wagens übertragen werden. Bei vorhandener Busleitung im Zug kann über ITSS 4 die Intrazugkommunikation realisiert werden. Die Daten können auf der Lokomotive für den Triebfahrzeugführer sichtbar sein und, wenn gewünscht, von dort über ITSS 1 an die Server übermittelt werden.

Die heutzutage gängige Variante im Güterverkehr ist das Flottenmanagement bzw. die Telematik mit ITSS 1. Dabei gibt es auf dem Fahrzeug ein Telematikgerät. Das Telematikgerät nimmt die Daten der Sensoren auf, verarbeitet sie und überträgt sie per Langstreckenkommunikation (über Mobilfunk) an einen Server. Im Regelfall handelt es sich hierbei um den Server des Telematikanbieters, von dem die Daten an den Server des Kunden übertragen werden können. Auf den Telematikgeräten ist zudem eine Ortung installiert. Im Personenverkehr können die Daten bereits über ein Bussystem innerhalb des Fahrzeugs übermittelt werden, sodass die Daten vom Triebfahrzeug an den Kunden gesendet werden können. [Workshop 2]

Die externe Datenverarbeitung muss in jedem Fall ein Benutzersystem einschließlich Datenbank, Benutzeroberfläche und Datenverarbeitung besitzen. Die anschließende Auswertung der Daten kann manuell, automatisiert oder auf Basis von Künstlicher Intelligenz erfolgen. Konkret ist damit Folgendes gemeint:

- Manuell: Die Daten werden an eine Stelle gesendet, bei der ein Mensch die Daten manuell auswertet.
- Automatisiert: Die Daten gelangen an eine Stelle, bei der die Daten ein bekanntes Programm durchlaufen und somit automatisiert ausgewertet werden. Die Informationen können nur so ausgewertet werden, wie es im Vorhinein programmiert wurde.
- Auf Basis Künstlicher Intelligenz: Die Daten werden mittels Künstlicher Intelligenz ausgewertet, indem diese immer weiter lernt, bis die Fähigkeiten eines Menschen erreicht sind.

Fahrzeugortung

Neben den reinen Daten muss auch die Position des Fahrzeuges erfasst werden. Möglich sind die folgenden Varianten:

- GNSS: Das Fahrzeug sendet seinen Standort.
- GNSS in Kombination mit Streckenkarten: Das Fahrzeug sendet seinen Standort. Dieser wird mit den Streckenkarten abgeglichen, um das Fahrzeug einem genauen Gleis zuzuordnen.
- GPS in Kombination mit Geofencing: Die Strecke ist in verschiedene Gebiete eingeteilt. Jeder Wagen ist mit GPS ausgestattet. Durch Abgleich dieser Daten kann markiert werden, in welchem Gebiet sich ein Wagen befindet und eine Benachrichtigung erfolgen.
- Balisen zur punktuellen Positionsbestimmung in Kombination mit einem Achsgenerator bzw. Weg-/Radimpulsgeber zur Ermittlung des Positionsfortschrittes zwischen den Balisen.
- Faseroptische Sensoren im Abgleich mit Fahrplandaten: Die Überfahrt eines Zuges erzeugt ein Signal, das mit dem Abgleich der Fahrplandaten den genauen Zug bzw. Wagen angibt.

Die meisten Telematiksysteme enthalten bereits standardmäßig einen GPS-/GNSS-Sensor. Dies ist im Vergleich von Nutzen zu Aufwand/Kosten die beste Variante. Dennoch muss in jedem Fall zwischen der Genauigkeit und den Kosten abgewogen werden. Dies ist individuell für jeden Anwendungsfall zu bestimmen. Ebenso muss bestimmt werden, ob die Ortung ausschließlich fahrzeugseitig erfolgen soll, in Kombination oder eigenständig mit infrastrukturseitigen Varianten. Damit dies möglich ist, wird hier kurz auf alle Varianten eingegangen.

Wenn eine auf mehrere Meter genaue Position ausreicht, genügt der Einsatz eines GNSS-Sensors, wobei sich die Genauigkeit immer weiter erhöhen wird. Die Kombination aus GNSS und Streckenkarten ist sinnvoll, wenn die Position eines Wagens gleis- bzw. zentimetergenau gewünscht wird, andernfalls kann darauf verzichtet werden. Die Kombination von GNSS mit Geofencing ist nur vorteilhaft, wenn ausschließlich eine Information von Interesse ist, sobald ein Fahrzeug ein definiertes Gebiet befahren hat, andernfalls wäre es mehr Aufwand für die gleichen Informationen im Vergleich zum reinen GNSS. Beim Einsatz von Balisen könnten bestehende Systeme genutzt werden. Allerdings wäre an jedem Zug bzw. Fahrzeug der Einbau eines Achsgenerators notwendig. Da nicht jeder Wagen mit einem Balisenleser ausgestattet ist, müsste in jedem Fall bekannt sein, welche Wagenreihung vorliegt und aus dieser auf die Fahrzeugposition geschlossen werden. Der Einsatz faseroptischer Sensoren wäre eine neue Technologie, bei der mit hohen Kosten zu rechnen ist, wenn jedes Gleis mit einer solchen Technologie ausgerüstet werden soll. Ebenso wäre der Aufwand für den Abgleich mit den Fahrplandaten erheblich.

Peripherie für Infrastruktur Use Cases

Stromversorgung

Die Stromversorgung wird über das öffentliche Stromnetz realisiert, indem sich an der Strecke ein Systemschrank befindet, der mit dem Stromnetz verbunden ist und alle Sensoren, Rechner, etc. mit Energie versorgt. Sollen die Sensoren nicht dauerhaft eingeschaltet werden, ist es möglich diese über Radsensoren zu aktivieren, indem an jeder Messstelle solche Einrichtungen montiert werden, die bei Überfahrt eine Einschaltung der Sensoren auslösen. [51][31][41]

Datenübertragung und -verarbeitung

Damit die Sensordaten auch genutzt werden können, muss eine Datenübertragung und -verarbeitung gewährleistet werden. Die nachfolgend erläuterte und in Abbildung 16 dargestellte Struktur gibt diesbezüglich eine grobe Übersicht.

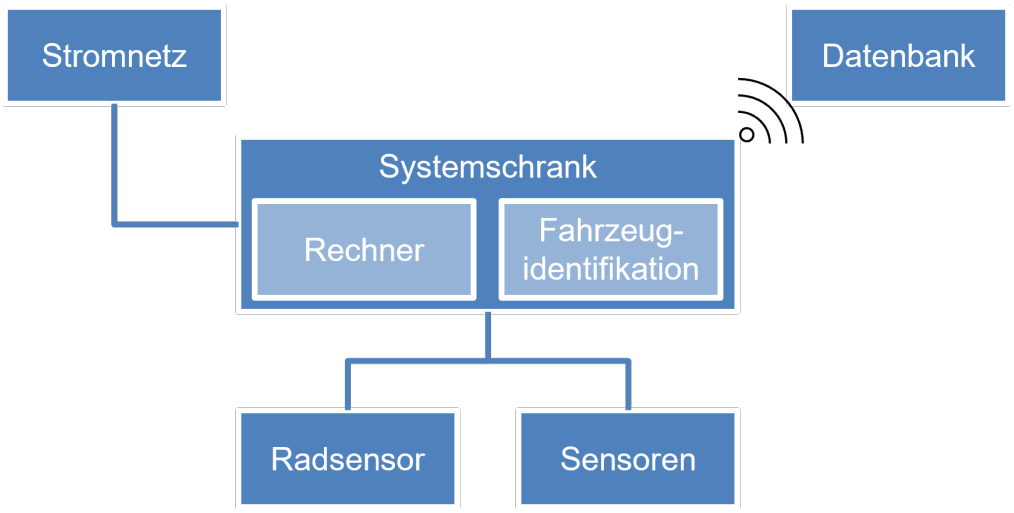


Abbildung 16: Datenübertragung der Infrastruktur Use Cases

Der Systemschrank bildet das zentrale Element. Dieser ist an der Strecke alleinstehend, an einem Mast oder an einer Wand montiert und an die Energieversorgung, d. h. das Stromnetz, angeschlossen. Zusätzlich enthält er einen Rechner zur Steuerung und Datenverarbeitung sowie ein System zur Fahrzeugidentifikation. Der Systemschrank ist darüber hinaus mit einem oder mehreren Sensoren verbunden. Die Sensoren werden über diese Leitungen auch mit Energie versorgt. Ebenso sind Radsensoren bzw. Achszähler mit dem Systemschrank verbunden. Diese detektieren die Überfahrt eines Zuges und sind zu installieren, um die Sensoren zu aktivieren und die Fahrtrichtung des Zuges zu erfassen. Zusätzlich ist der Systemschrank über eine Langstreckenkommunikation mit der externen Datenverarbeitung, z. B. einer Datenbank, verbunden.

Die Kurzstreckenkommunikation zwischen Sensoren bzw. Radsensor/Achszähler und Systemschrank wird durch die Verwendung von Kabeln realisiert. Im Systemschrank erfolgt dann die erste Rohdatenverarbeitung. Dabei werden die Sensormesswerte in analoge, elektrische Signale umgewandelt. Anschließend werden über Analog-/Digital-Signalwandler digitale Signale erstellt und an die Auswerteelektronik gesendet, was über Optokoppler- und Relais-Schnittstellen erfolgen kann. Die Datenübertragung an die Datenbank erfolgt als Langstreckenkommunikation über (Mobil-)Funk, eine Ethernet-/Wireless-Verbindung (LTE/5G) oder GSM. Der Datenbankserver ist in einem lokalen Netzwerk oder einer Cloud (unter Nutzung von 5G) abgelegt. [31][41][34][Workshop 1]

Die konkrete Datenauswertung kann sowohl vor Ort als auch in der Zentrale durchgeführt werden. Wie bei den Fahrzeug Use Cases sind dabei drei Varianten möglich [26]:

- Manuell: Die Daten werden an eine Stelle gesendet, bei der ein Mensch die Daten manuell auswertet.
- Automatisiert: Die Daten gelangen an eine Stelle, bei der die Daten ein bekanntes Programm durchlaufen und somit automatisiert ausgewertet werden. Die Informationen können nur so ausgewertet werden, wie es im Vorhinein programmiert wurde.
- Auf Basis Künstlicher Intelligenz: Die Daten werden mittels Künstlicher Intelligenz ausgewertet, indem diese immer weiter lernt, bis die Fähigkeiten eines Menschen erreicht sind.

Fahrzeugidentifikation

Bei den Infrastruktur Use Cases ist eine sichere Fahrzeugidentifikation notwendig, um die Daten dem jeweiligen Fahrzeug zuzuordnen. Daher muss der Systemschrank mit einem Fahrzeugerkennungssystem ausgestattet sein. Möglich sind folgende Varianten [26][28][Workshop 1]:

- Detektion der Wagennummer über ein Kamerasystem
- RFID-Transponder am Fahrzeug und eine Auswerteeinheit (d. h. hier am Systemschrank) an der Messstelle ermöglicht eine achsgenaue Ortung
- Abgleich des Zeitstempels des Sensors mit den Fahrplandaten des EIUs bzgl. der Transportwege zur Bestimmung des EVUs/Wagenhalters. Zusätzlich Nutzung von Achszählern oder Glasfaserkabeln zur Bestimmung der Achszahl und Abgleich mit der Wagenreihung für die Bestimmung der Achse bzw. des Wagens

In heutigen Systemen werden bereits Kamerasysteme oder RFID-Transponder eingesetzt. Bei Kamerasystemen darf die Wagennummer nicht zu stark verschmutzt sein, es ist jedoch keine Aufrüstung der Wagen erforderlich. Dies ist bei den RFID-Transpondern erforderlich, ansonsten handelt es sich dabei auch um ein sicheres, funktionsfähiges System. Die Nutzung von Fahrplandaten und Achszählern oder Glasfaserkabel sorgt ebenfalls für ein sicheres System, benötigt aber genaue Fahrplandaten und eine erneute Kommunikationsschnittstelle, die für einen erschwerten Prozess sorgt. Der zusätzliche Einsatz von Achszählern wäre einfacher bzw. kostengünstiger als Glasfaserkabel realisierbar.

4.3.3 Anforderungskriterien

Die Recherche führte zu einer großen Zahl an relevanten Anforderungen. Damit die Menge an Kriterien handhabbar ist und sich ein geeigneter Handlungsleitfaden ergibt, ist eine Reduktion der Anforderungen erforderlich. Zunächst wurden Mehrfachnennungen gelöscht und sprachliche Variationen vereinheitlicht. Anschließend wurden einige Elemente aussortiert bzw. angepasst, die nach Ansicht des Projektteams kombiniert werden können. Einige Anforderungen hängen eng zusammen und gehen teilweise sehr tief ins Detail, sodass die Möglichkeit besteht, diese unter einem Oberbegriff zusammenzufassen. Bspw. wurden die Kriterien „Beständigkeit gegenüber unterschiedlichen Umgebungsdrücken“ und „Beständigkeit gegenüber Höhenlage“ aus der Gruppe Umwelt zum Kriterium „Beständigkeit gegenüber unterschiedlichen Umgebungsdrücken durch Höhenlage“ zusammengefasst oder spezifische Kriterien zur Stromversorgung durch das Kriterium „Einhaltung der Anforderungen zur Stromversorgung gemäß DIN EN 50155, z. B. zu Themen wie Spannungs- und Stromversorgung, Schutzeinrichtungen“ ersetzt. So kann der wesentliche Nutzen der Anforderungsliste erhalten bleiben und der Fokus auf die im Bahnwesen für möglichst alle Sensoreinheiten geltenden Anforderungen beibehalten werden.

Nach Durchführung der Recherche sowie der Anpassung der Anforderungskriterien bot sich eine geringfügige Anpassung der Anforderungsgruppen an. Es wurden folgende Gruppen festgelegt:

1. Betriebsbedingungen
2. Umwelt
3. Schnittstellen
    a. Allgemein
    b. Elektro
    c. Daten
    d. Kommunikation
4. Montage
5. Störung anderer Systeme/EMV
6. Betriebssicherheit und Zuverlässigkeit
7. Verfügbarkeit
8. Instandhaltung
9. Security
10. Safety

Zu jeder Gruppe gibt es mehrere Kriterien. Die Liste aller Anforderungen umfasst insgesamt 130 Elemente und befindet sich im Anhang in Kapitel 13.2.1.

Die Anforderungskriterien werden nun noch auf jeden Use Case angewendet, indem beurteilt wird, ob die Anforderung für den Use Case von Relevanz ist, ggf. auch mit einer genaueren Angabe. Diese Ergebnisse sind im Anhang in Kapitel 13.2.2 zu finden. Eine detaillierte Betrachtung für jeden einzelnen Sensor ist im Rahmen dieses Projektes nicht möglich. An einigen Stellen werden aber, sofern notwendig, Hinweise zu Unterschieden zwischen Sensoren gegeben.

4.3.4 Zulassungsprozess

Der Zulassungsprozess muss aufgrund der als relevant ausgewählten Use Cases sowohl für Sensoren am Fahrzeug als auch in der Infrastruktur betrachtet werden. Seit dem 4. Eisenbahnpaket erfolgt die Zulassung nach der Eisenbahn-Inbetriebnahmegenehmigungsverordnung (EIGV). Darin sind „die Bedingungen für das Inverkehrbringen und für die Inbetriebnahme von Bestandteilen des Eisenbahnsystems“ [47] geregelt. In § 9 und § 10 wird beschrieben, wann eine Genehmigung erforderlich ist.

Die Zulassung von Fahrzeugen kann durch die Europäische Eisenbahnagentur (ERA) oder das EBA erfolgen. Erfolgt der Einsatz der Fahrzeuge ausschließlich in Deutschland, entscheidet der Antragsteller, ob die ERA oder das EBA das Fahrzeug zulassen soll. Bei einem Einsatz der Fahrzeuge in mehreren Ländern, ist in jedem Fall die ERA zuständig. Zusätzlich muss bestimmt werden, ob es sich um ein einzelnes Fahrzeug oder einen Fahrzeugtyp handelt. Für eine Zulassung oder erneute Genehmigung müssen die benötigten Nachweise gemäß Artikel 28 der Durchführungsverordnung 2018/545 erbracht werden. Dazu gehören EG-Prüferklärungen. In diesen bestätigt der Antragsteller die Übereinstimmung mit den entsprechenden Vorschriften, was durch die zugehörigen Stellen bestätigt wird. Die „Benannte Stelle“ (NoBo) prüft die Konformität mit den Technical Specifications for Interoperability (TSI)-Richtlinien, die „Bestimmte Stelle“ (DeBo) die Konformität mit den nationalen Vorschriften NNTV/NNTR und die „Unabhängige Bewertungsstelle (AsBo)“ die ordnungsgemäße Anwendung des Risikomanagementverfahrens, falls dies erforderlich ist. [1]

Für die Zulassung von Infrastruktur ist das EBA zuständig. Bei einer erstmaligen Inbetriebnahme wird ein Antrag auf Inbetriebnahmegenehmigung gestellt. Handelt es sich nicht um die erstmalige Inbetriebnahme, muss geprüft werden, ob es sich um eine Instandhaltung oder darüberhinausgehende Tätigkeiten handelt. Ob eine über die Instandhaltung hinausgehende Tätigkeit eine genehmigungspflichtige Änderung ist, kann der Anlage 4 der EIGV entnommen werden. Anschließend muss eine Aufrüstung angezeigt werden, die durch das EBA geprüft wird. [2]

Um die Komplexität dieses Projektes in einem vertretbaren Rahmen zu halten und im Anschluss einen praxisnahen Handlungsleitfaden für eine Umsetzung zu erhalten, wird der Einsatz der Fahrzeuge nur deutschlandweit betrachtet. Damit allerdings beurteilt werden kann, ob es sich bei den hier vorliegenden Sensorlösungen um genehmigungspflichtige Änderungen im Sinne der EIGV handelt, sind verschiedenste Schritte zu durchlaufen, eine pauschale Aussage kann vorab nicht getroffen werden. Dafür kann sich am Lebenszyklusmodell der DIN EN 50126 orientiert werden. Demnach müssen folgende Schritte durchlaufen werden, bevor ein Sensorsystem am Fahrzeug oder in der Infrastruktur in Betrieb genommen werden kann:

1. Konzept
2. Systemdefinition und Anwendungsbedingungen
3. Risikoanalyse, ggf. Anpassung und Wiederholung
4. Systemanforderungen
5. Zuteilung der Systemanforderungen
6. Entwicklung/Konstruktion und Implementierung

7. Fertigung
8. Installation/Montage
9. System-Validierung (einschließlich Sicherheits-Abnahme und Inbetriebsetzung)
10. Systemabnahme
11. Betrieb und Instandhaltung, dann Erfassung der Leistungsfähigkeit sowie Änderungen und Nachrüstung und anschließender Wiederbeginn des Lebenszyklus
12. (Stilllegung und Entsorgung)

Es müssen auch für alle hier vorliegenden Use Cases alle Schritte durchlaufen werden. In Schritt 9 und 10 (System-Validierung und Systemabnahme) kann unter Umständen die erneute Inbetriebnahme erforderlich werden. Nach der Aussage von Expertinnen und Experten liegen ab SIL 2 höhere Anforderungen vor, was bereits ab dem Einsatz von Vibrations- und Schwingungsmessungen der Fall ist. Im Rahmen der Risikoanalyse müssen zahlreiche Regelwerke geprüft werden. Dazu zählen die im Abschnitt

Regelwerke genannten Elemente in Kapitel 4.3.1. Diese Normen beinhalten teilweise auch Informationen, wie mit neuen, noch nicht im Bahnsystem zugelassenen Systemen umzugehen ist.

Für die sichere Entwicklung eines neuen Systems sollte der Prozess unter Einbeziehung verschiedener Expertinnen und Experten durchgeführt werden. Ebenso bietet es sich an, direkt mit den zuständigen Stellen in Kontakt zu stehen (d. h. NoBo, DeBo, AsBo). Dies bietet eine gute Grundlage, damit alle Inhalte und Aspekte berücksichtigt werden, u. a. für die Risikoanalyse und die daraus folgenden Systemanforderungen. Weitere Informationen zur Risikoanalyse können der CSM-Verordnung entnommen werden.

Im Rahmen der Systemdefinition müssen Informationen zum Sensorsystem und dem Fahrzeug bzw. der Infrastruktur bestimmt werden. Nachfolgend sind einige Beispiele aufgelistet, um was für Informationen es sich dabei handelt. Es handelt sich hierbei nicht um eine vollständige Liste:

- Zweckbestimmung/Verwendung
- Einbauort (Fahrzeug/Infrastruktur)
- Sicherheitsrelevanz (ja/nein)
- Autarkes Sensorsystem/Abgriff von Daten des bestehenden Fahrzeug-/Infrastruktursystems/Steuerung des bestehenden Fahrzeug-/Infrastruktursystems
- Bestandteile und deren Funktionen
- Gewicht
- Schnittstellen
- Systemumgebung

Die Fahrzeuginformationen umfassen z. B.:

- Fahrzeugart (Lokomotive, Triebwagen, Reisezugwagen, oder anderes)
- Einsatzort (Europa/Deutschland/Insellösung)
- Fahrzeug-Baureihe
- Max. betriebliche Höchstgeschwindigkeit, max. betrieblicher Überhöhungsfehlbetrag
- Betriebliche Zugkonfigurationen, z. B. Mehrfachtraktion
- Traktionsausrüstung
- Bremsausrüstung
- Zugbeeinflussung
- Funkausrüstung
- Betriebliche Besonderheiten

Bei der Infrastruktur sind bspw. folgende Informationen relevant:

- Einsatzort (öffentliche Infrastruktur, Werksbahn, Industriebahn o. Ä.)
- Art der Schienen, Schwellen, Unterbau
- Lage bzw. Zugänglichkeit der Infrastruktur
- Häufigkeit der Überfahrten

Da eine genaue Systemdefinition im Rahmen dieses Projektes nicht möglich ist, kann nur eine Einschätzung gegeben werden, ob eine erneute Inbetriebnahmegenehmigung erforderlich sein wird oder nicht. Dazu werden einige der wichtigsten Merkmale der Use Cases bestimmt, zu denen Folgende zählen:

- Der Einbauort des Sensorsystems (Fahrzeug oder Infrastruktur)
- Die Sicherheitsrelevanz (d. h. die Beantwortung der Frage, ob das Sensorsystem sicherheitsrelevante Funktionen überwacht/ausübt oder nicht?)
- Handelt es sich um ein autark funktionierendes Sensorsystem, greift das Sensorsystem Daten des bestehenden Fahrzeug-/Infrastruktursystems ab oder greift das Sensorsystem Daten ab und steuert das Fahrzeug-/Infrastruktursystem?

Die Einschätzung der Use Cases zu diesen Themen sowie eine anschließende Tendenz zur Notwendigkeit werden nun für jeden Use Case erläutert. An dieser Stelle wird noch einmal darauf hingewiesen, dass – unabhängig zur Notwendigkeit einer erneuten Inbetriebnahmegenehmigung nach EIGV – in jedem Fall die zu Beginn dieses Kapitels erläuterten Schritte zu durchlaufen sind, d. h. immer auch eine Risikoanalyse durchzuführen ist.

Use Case „Fahrzeug überwacht Oberbau“:

- Einbauort: Fahrzeug
- Sicherheitsrelevanz: ja, wenn gesonderte Messfahrten dadurch ersetzt werden
- Autark funktionierendes System. Je nach Fahrzeug ggf. Stromabgriff
- ➔ Eine erneute Inbetriebnahme kann notwendig sein, dies hängt u. a. von den genau eingesetzten Sensoren und deren Montageorten, der umgesetzten Stromversorgung und den SIL-Leveln ab. Es kann u. U. eine Anpassung des Regelwerkes bzgl. der Messfahrten erforderlich sein.

Use Case „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant“:

- Einbauort: Fahrzeug
- Sicherheitsrelevanz: ja
- Abgriff von Daten und u. U. Steuerung des Systems
- ➔ Eine erneute Inbetriebnahme wird notwendig sein aufgrund des Einflusses in das System und der Änderung der sicherheitsrelevanten Fahrzeugortung. Eine Änderung des entsprechenden Regelwerkes wird notwendig sein.

Use Case „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“:

- Einbauort: Fahrzeug
- Sicherheitsrelevanz: ja
- Abgriff von Daten
- ➔ Eine erneute Inbetriebnahme kann in Abhängigkeit des konkreten Anwendungsfalls notwendig sein. Werden dadurch manuelle Tätigkeiten ersetzt und wird die Abfahrbereitschaft des Zuges festgestellt, ist voraussichtlich eine erneute Inbetriebnahmegenehmigung und Änderung des entsprechenden Regelwerkes erforderlich. Wird nur der Verschleißzustand überwacht und eine

zustandsorientierte Instandhaltung angestrebt, ist nicht unbedingt eine erneute Inbetriebnahme notwendig.

Use Case „Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)“:

- Einbauort: Fahrzeug
- Sicherheitsrelevanz: nein
- Stromversorgung über das Fahrzeug. Zusätzlich je nach Sensor, Abgriff von Daten oder autark funktionierendes System

➔ Eine erneute Inbetriebnahme kann u. U., je nach Sensor, erforderlich sein. Werden nur wenige autark funktionierende Sensoren eingebaut, ist voraussichtlich keine Inbetriebnahme notwendig. Insgesamt hängt dies aber vom Ergebnis der Risikoanalyse ab.

Use Case „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“:

- Einbauort: Infrastruktur
- Sicherheitsrelevanz: nein
- Autark funktionierendes System

➔ Eine erneute Inbetriebnahme ist voraussichtlich nicht erforderlich.

Use Case „(Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)“:

- Einbauort: Infrastruktur
- Sicherheitsrelevanz: nein
- Autark funktionierendes System

➔ Eine erneute Inbetriebnahme ist vermutlich nicht erforderlich.

Use Case „Weichenferndiagnose“:

- Einbauort: Infrastruktur
- Sicherheitsrelevanz: ja
- Abgriff von Daten

➔ Die Notwendigkeit hängt u. a. von den tatsächlich eingesetzten Sensoren sowie deren Funktionen und Einbauorten ab. In Abhängigkeit davon kann eine Inbetriebnahmegenehmigung erforderlich sein.

Abschließend kann festgehalten werden, dass es sich beim Thema Zulassung um einen komplexen Prozess handelt. Für jeden Anwendungsfall sind eine Reihe von Untersuchungen notwendig, bevor dieser überhaupt zum Einsatz kommen kann. Je nach Komplexitätsgrad der Lösung kann durchaus eine erneute Inbetriebnahme des Fahrzeugs oder der Infrastruktur erforderlich werden. In diesem Fall gestaltet sich der Prozess weitaus komplexer und umfangreicher, bevor ein Sensorsystem zum Einsatz kommen kann. Daher müssen die Use Cases gewissenhaft ausgewählt und die Sensorik auf das notwendige Minimum reduziert werden. Zudem empfiehlt es sich, bezüglich der Use Cases auf eine gute Umsetzbarkeit zu achten.

5 Stakeholderanalyse

Dieses Kapitel widmet sich aufbauend auf den Use Case-Analysen den verschiedenen an Sensoranwendungen im Bahnsystem beteiligten Anspruchs- bzw. Interessengruppen. Dazu gehört zum einen eine entsprechende Identifikation und Abgrenzung von grundsätzlich existierenden Stakeholdern. Zum anderen sind die zum Teil unterschiedlichen Sichtweisen von Stakeholdern auf infrage kommende Sensoranwendungen zu untersuchen und Abhängigkeiten bzw. Wechselbeziehungen aus der Verflechtung der Stakeholder miteinander herauszuarbeiten. Auf diese Weise können Grundlagen für das sich anschließende Kapitel erarbeitet werden, welches sich der Marktseite und bestehenden Handlungsbedarfen widmet. In den nachfolgenden Unterabschnitten werden das Vorgehen und die Ergebnisse der entsprechenden Unterkapitel dargestellt.

5.1 Umfeld und Stakeholder

Ziel dieses Unterkapitels ist es, dass allen Konsortialpartnern für ihre weiteren Analysen das relevante Umfeld der Einflussfaktoren und insbesondere die in diesem Umfeld (inter-)agierenden und voneinander abgegrenzten Stakeholder bekannt sind. Stakeholder sind Anspruchs- bzw. Interessengruppen, die – bezogen auf den Untersuchungsgegenstand – mit ihren Entscheidungen und mit dem von ihnen ausgeübten Einfluss maßgeblich mitbestimmen, welche Sensoranwendungen in welcher Form und mit welchen Konsequenzen im zukünftigen Bahnsystem verwirklicht werden.

Zu Projektbeginn wurde zunächst in gemeinsamen Abstimmungen des Projektkonsortiums das relevante und zu betrachtende Umfeld definiert. In Anlehnung an eine PESTEL-Analyse (Political, Economic, Sociological, Technological, Environmental and Legal Factors) wurden dabei auf Basis der vorhandenen Expertise Makrofaktoren identifiziert und in die folgenden vier (nicht immer trennscharf voneinander abgrenzbaren) Bereiche eingeordnet:

1) Technik:
   Funktionalität und Leistungsfähigkeit existierender Sensoren; technologische Reife neuartiger Sensortechnologien; alternative Wirkprinzipien/konkurrierende Sensortechnologien; einsetzbare Methoden der Sensordatenfusion; verfügbare sowie heutige eingesetzte Informations- und Kommunikationstechnologien im Bahnsystem und deren Migrationsfähigkeit; State-of-the-Art-Bahntechnik für potenzielle Sensoranwendungen (als „zu übertreffende“ Vergleichsbasis)
2) Markt:
   Marktverfügbarkeit und aktuelle Verbreitung von Sensorsystemen; Kosten von Sensorsystemen (Beschaffung und laufender Betrieb); Anbieterstruktur des Sensormarktes (inkl. Marktmacht, geographische Verteilung und Lieferketten); Marktstruktur potenzieller Sensoranwender im Bahnsektor; (Sensor-)Datenmarktplätze; zu berücksichtigende Marktregulierungen
3) Recht:
   Zulassungsfähigkeit von Sensorsystemen im Bahnsektor (inkl. zusätzlicher Anforderungen bei Personenbeförderung); Realisierbarkeit, Aufwand und Kosten von Sicherheitsnachweisführungen; von der Sensoranwendung tangierte eisenbahnrechtliche Vorschriften (z. B. Eisenbahn-Bau- und Betriebsordnung (EBO), Europäische Union (EU)-Richtlinien/Eisenbahnpakete); datenschutzrechtliche Bestimmungen; haftungsrechtliche Regelungen (insb. bei Einsatz von Software und Maschinellem Lernen); gewerbliche Schutzrechte; Technische Normen und Standards; betrieblich-technische Regelwerke

4) Gesellschaft:
   Gesellschaftlicher und politischer Druck für nachhaltigere Mobilitätslösungen allgemein und speziell für einen leistungsstärkeren, zuverlässigeren und klimaschonenderen Schienenverkehr; zunehmende Herausforderung der Verfügbarkeit qualifizierter Fachkräfte, insbesondere im Bahnsektor; Förderlandschaft für Bahninnovationen; Technologieakzeptanz der Sensoranwendungen (z. B. ATO) durch Personal und Kundinnen und Kunden

In diesem durch die vier Bereiche abgebildeten Umfeld agieren relevante Akteure unterschiedlichster Art. Um zu einem Stakeholder-Gesamtbild zu gelangen, wurde folgendermaßen vorgegangen: Zunächst wurden Schlag- und Stichwortsuchen in Literaturdatenbanken und Suchmaschinen (EBSCO, ScienceDirect, Sciencegate, ResearchGate, Google Scholar) – unter Einbeziehung der Schlagworte „Stakeholder", „Marktrolle" oder „(Markt-)Akteur" in Kombination mit „Sensor*" und/oder „Bahn*" (sowie synonymer und ähnlicher Bezeichnungen, insbesondere englischsprachiger Pendants) – vorgenommen. Dabei konnte kein bereits existierendes Gesamtbild gefunden werden, welches die Akteure des Untersuchungsgegenstands hinreichend und vollständig abbildet. Vielmehr musste die Struktur der Sensorindustrie und die des Bahnsektors – zunächst getrennt voneinander betrachtet – erfasst werden. Grundlagen hierfür bildeten neben einigen wissenschaftlichen Quellen [56][57][58][59] vor allem Übersichten aus Branchenkatalogen (u. a. von Verbänden wie AMA und Rail.S), aus Fachportalen, aus Publikationen von Marktforschungs- und Beratungsunternehmen sowie aus Verzeichnissen relevanter Messen und Ausstellungen (z. B. Railway Forum, InnoTrans). Dort aufgeführte Marktrollen und ergänzende Akteurinnen und Akteure in unterschiedlichen Detaillierungsgraden wurden dann – mit den oben genannten Makrofaktoren des Umfeldes sowie den in Kapitel 4.1 identifizierten Use Cases mit jeweiligen „Nutznießern" und „Ermöglichern" im Hinterkopf – neu sortiert und gruppiert. Das dabei entstandene Gesamtbild wurde im Entwurf schließlich in mehreren Iterationsstufen mit ausgewählten Expertinnen und Experten sowie innerhalb des Projektkonsortiums diskutiert, validiert und auf Basis des erhaltenen Feedbacks überarbeitet bzw. verbessert. Dabei waren insbesondere die ausgeprägten Marktkenntnisse des Fraunhofer ENAS über die Sensorindustrie und die des IFB Institut für Bahntechnik GmbH über den Bahnsektor von Nutzen.

Das im Ergebnis entstandene Gesamtbild der relevanten Stakeholder ist in der nachfolgenden Abbildung 17 mit Vierecken für jede Stakeholderhauptgruppe dargestellt. Aufgrund der Komplexität der Realität waren in diesem modellhaften Abbild Vereinfachungen erforderlich. So sind bspw. diverse relevante Untergruppen einer übergeordneten Stakeholdergruppe durch drei kleine Kästchen innerhalb des jeweiligen Vierecks angedeutet. Des Weiteren sind nur die wichtigsten Stakeholderbeziehungen mit schwarzen Verbindungslinien visualisiert oder im Sinne einer besseren Übersichtlichkeit mit Fußnoten (a bis c) gekennzeichnet. In der Realität existieren noch weitaus mehr.

Die aufgeführten Stakeholdergruppen sind als relevante, grundlegende Marktrollen für den Sensoreinsatz im Bahnwesen zu verstehen. Mehrere dieser Rollen können in der Praxis auch auf ein und denselben Marktakteur im Sinne eines Unternehmens bzw. einer Institution zusammenfallen. Sie werden in der Stakeholderanalyse dennoch getrennt betrachtet, da mit jeder Rolle spezifische, voneinander abgrenzbare Marktfunktionen verbunden sind, die einen eigenen Blick auf den Nutzen, die Chancen und die Risiken von Sensoranwendungen werfen. Im Anhang 13.3 ist ein Glossar mit detaillierteren und im Weiteren genutzten Arbeitsdefinitionen für jede Stakeholdergruppe zu finden. Nachfolgend soll daher nicht auf jede einzelne Gruppe, sondern nur auf übergreifende Zusammenhänge eingegangen werden.

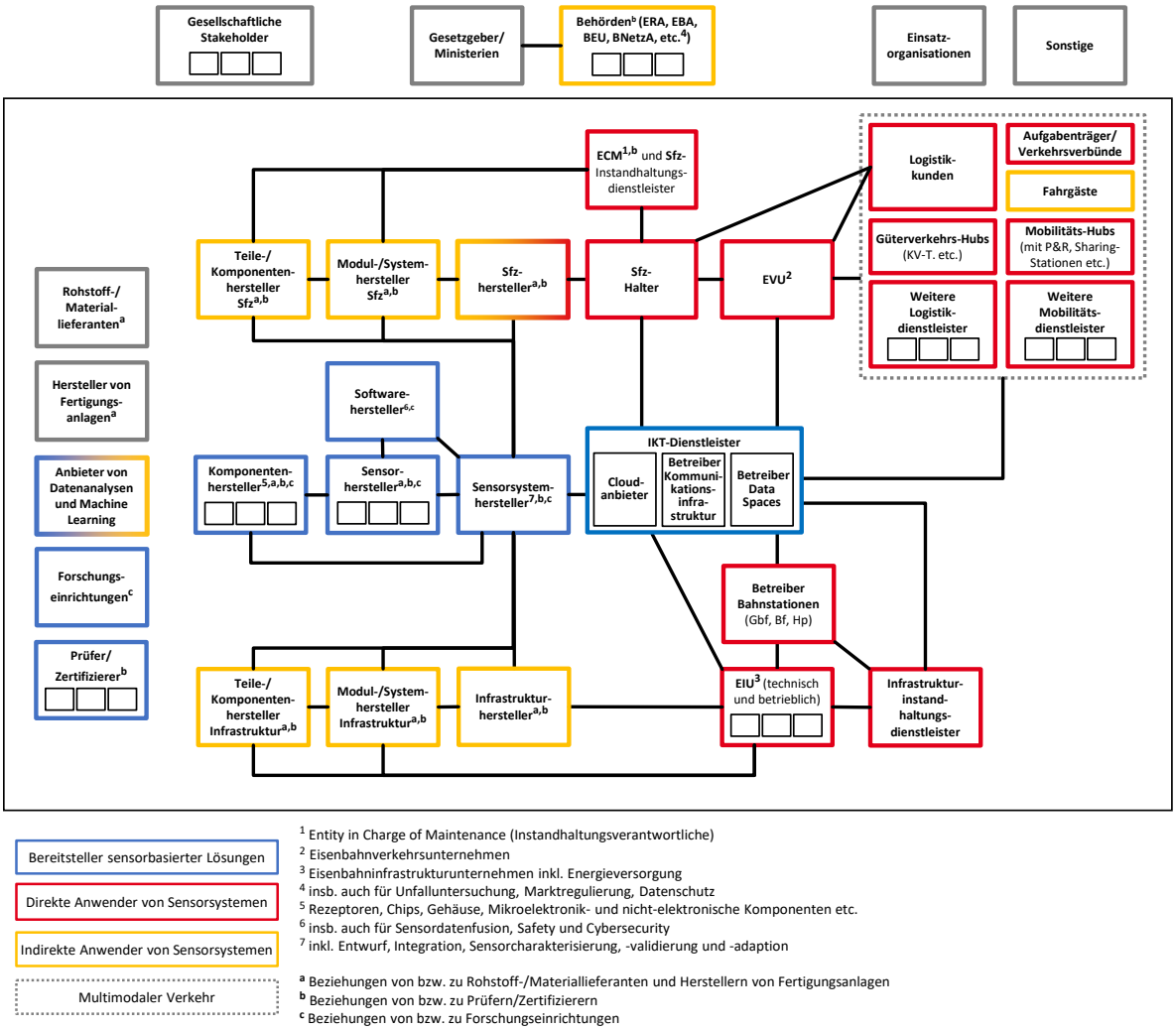


Abbildung 17: Gesamtbild relevanter Stakeholder [TU Chemnitz, BWL III]

Mit Bezug auf das Untersuchungsobjekt lassen sich grob drei Kategorien von Stakeholdern unterscheiden.

Unter *Bereitstellern sensorbasierter Lösungen* (in Abbildung 17 blau umrahmt) sollen alle Wertschöpfungspartner verstanden werden, die am Generieren, Zurverfügungstellen und Nutzbarmachen von Sensordaten beteiligt sind. Dies umfasst primär die verschiedenen Akteure der Sensorherstellung (in der entsprechenden Wertschöpfungskette von den Sensorikkomponenten bis zum Sensorsystem), aber auch verschiedene Informations- und Kommunikationstechnologie (IKT)-Dienstleister, Anbieter von Datenanalysen und Machine Learning, unterschiedliche Prüfer/Zertifizierer sowie Forschungseinrichtungen. IKT-Dienstleister nehmen eine zentrale Schlüsselposition zwischen den Herstellern und Anwenderinnen und Anwendern sensorbasierter Lösungen ein. Ihre bereits im Rahmen der Erstellung des Gesamtbildes der Stakeholder erwartete hohe Bedeutung wurde in den beiden durchgeführten Workshops sowie in den getätigten Expertinnen- und Experteninterviews bestätigt. Dabei kristallisierten sich hauptsächlich drei besonders wichtige Untergruppen heraus:

1. *Cloudanbieter*, welche über Anwendungsprogrammierschnittstellen (API) das vereinfachte und ressourcensparende Sammeln, Speichern, Verarbeiten sowie das Bereitstellen sensorbasierter Daten auf verschiedenen Hardwareplattformen ermöglichen,

2. *Betreiber von Kommunikationsinfrastrukturen*, mit deren Hilfe Sensordaten bzw. sensorbasierte Daten drahtgebunden oder drahtlos zwischen verschiedenen Gesamtsystemelementen oder zwischen unterschiedlichen Stakeholdern übertragen werden sowie
3. *Betreiber von Datenräumen (Data Spaces)*, welche auf einer sicheren Plattform ein vertrauenswürdiges Teilen sensorbasierter Daten sowie eine souveräne Bewirtschaftung von (sensorbasierten) Datengütern ermöglichen, indem sie sicherstellen, dass Daten bis zu ihrer gewünschten kostenlosen oder entgeltlichen Bereitstellung im Einflussbereich des Urhebers verbleiben.

Unter *direkten Anwendern von Sensorsystemen* (in Abbildung 17 rot umrahmt) sollen solche verstanden werden, die primär selbst mit den durch bahnspezifische Sensorsysteme generierten Daten interagieren bzw. einen Daten-/Informationsoutput für indirekte Anwenderinnen und Anwender generieren.

Unter *indirekten Anwendern von Sensorsystemen* (in Abbildung 17 gelb umrahmt) sollen solche verstanden werden, die primär einen Nutzen aus durch bahnspezifische Sensorsysteme generierten Daten (oder daraus abgeleiteten, angereicherten, höherwertigen Informationen) ziehen, ohne jedoch selbst direkt mit diesen Daten zu interagieren. Die Grenzen zwischen direkten und indirekten Anwenderinnen und Anwendern sind fließend.

Grau gestrichelt umrahmt sind die neben den Eisenbahnverkehrsunternehmen bzw. Schienenfahrzeughaltern an einem (grundsätzlich multimodal[2] erfolgenden) Verkehr beteiligten Akteure. Dies sind zum einen die Kundinnen und Kunden von Personenverkehrs- und Güterverkehrsleistungen (bei ersteren zudem die verantwortlichen Aufgabenträger), zum anderen aber auch weitere Logistik- bzw. Mobilitätsdienstleister außerhalb des Systems Bahn (z. B. Speditionen, Reedereien, Bus- und Taxiunternehmen) sowie die Betreiber der entsprechenden Umstiegs- bzw. Umschlagseinrichtungen („Hubs“).

Durchgehend grau umrahmt sind Stakeholder, die selbst weder Sensoranwender noch Bereitsteller von Sensorlösungen sind, aber wichtige vorgelagerte, den Rahmen setzende oder direkt und indirekt eingreifende Funktionen repräsentieren. Dabei handelt es sich bspw. um Lieferanten von Rohstoffen, Materialien und Produktionstechnik, den Gesetzgeber und gesellschaftliche Interessengruppen sowie gewollt oder ungewollt mit Sensordaten in Berührung kommende Dritte.

In Abbildung 17 wurde die Positionierung der Stakeholdergruppen so gewählt, dass im unteren Teil der Teilstrang der Eisenbahninfrastruktur, im oberen Teil der Teilstrang des Schienenfahrzeugs (bis hin zur Nutzung von Eisenbahnverkehrsleistungen rechts) und dazwischen die in beide Stränge hineinwirkende Sensorindustrie verortet sind. Die aufgrund ihrer Verflechtungen bzw. ihres übergeordneten Charakters nicht übersichtlich in diese Grundstruktur einfügbaren Stakeholder wurden am linken bzw. oberen Rand positioniert, je nachdem, ob es sich bei ihnen um Wertschöpfungspartner oder um einflussnehmende Institutionen bzw. Gruppen handelt.

Die eigentlichen Stakeholderanalysen (Abschnitt 5.2), unter Einbeziehung der sieben für die Detailbetrachtungen ausgewählten Use Cases (vgl. Tabelle 5), werden anhand des durch Abbildung 17 vorgegebenen Rasters der 34 Stakeholder-Hauptgruppen erfolgen. Das heißt für jeden detaillierter untersuchten Use Case werden zunächst – im Sinne eines Ausschnittes aus dem Gesamtbild – diejenigen Hauptgruppen von Stakeholdern identifiziert, die bei dieser Sensoranwendung relevant sind. Anschließend erfolgt – bei Bedarf – ein Herunterbrechen von diesen auf relevante Untergruppen von Stakeholdern oder

[2] Multimodaler Verkehr meint die Nutzung unterschiedlicher Verkehrsmodi (hier: Eisenbahn kombiniert mit weiteren) innerhalb eines Zeitraumes. Einen Sonderfall stellt der intermodale Verkehr dar, bei welchem Verkehrsmittelwechsel auf einem Weg von A nach B stattfinden [56]. Multimodalität erlaubt es, Stärken unterschiedlicher Fortbewegungsmittel zu verbinden, sodass im Gesamtgefüge Emissions- und Staureduzierungen, wirtschaftlichere und sozial förderliche Mobilitätsoptionen sowie nachhaltigere Flächen- und Ressourcennutzungen realisiert werden. Im Güterverkehr wird bei intermodalen Wegeketten vom Kombinierten Verkehr (KV) gesprochen.

auch auf funktionale Rollen (z. B. Triebfahrzeugführer, Wagenmeister, Fahrdienstleiter) einer Stakeholdergruppe.

Für die Workshopdurchführung sowie die Stakeholderanalysen wurde eine Beteiligung von fachkundigen Expertinnen und Experten angestrebt, deren Zusammensetzung die Breite des erarbeiteten Gesamtbildes relevanter Stakeholder widerspiegelt. Für die Zwecke der Expertinnen- und Experteneinbindung war jedoch auch eine Verdichtung des sehr feingliedrigen Stakeholdergesamtbildes erforderlich. In Abstimmung mit der Use Case-Analyse in Kapitel 4.1, die auch eine Zuordnung von Sensoranwendungen zu primären Anwenderinnen und Anwendern umfasste, wurden deshalb die folgenden sechs übergeordneten Stakeholdergruppen abgegrenzt (siehe Abbildung 18). Fünf dieser Gruppen sind anwenderseitig.

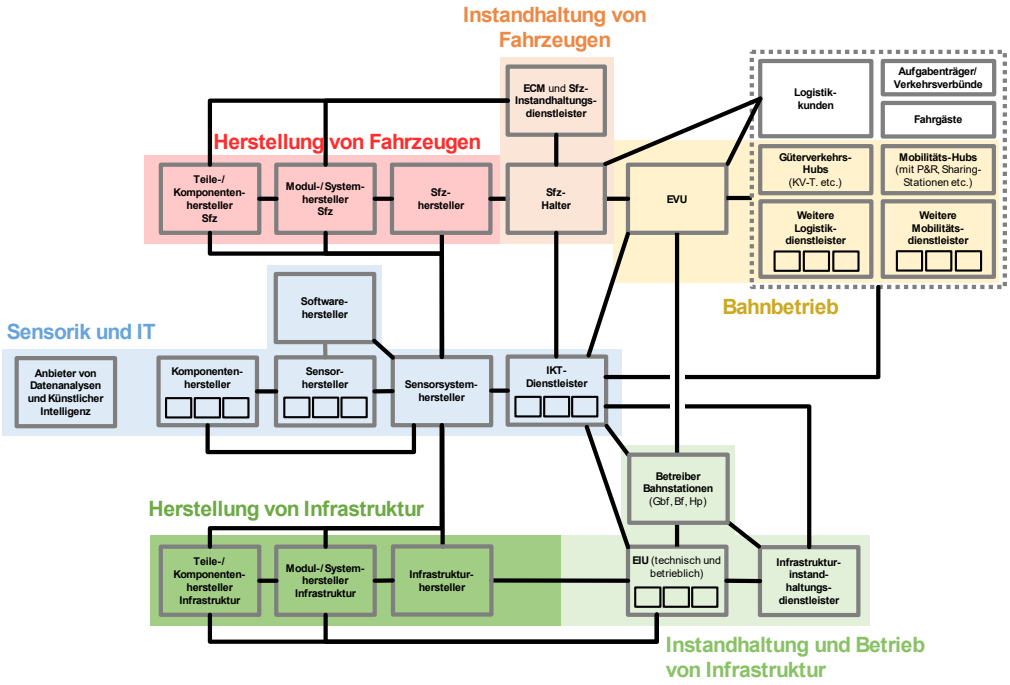


Abbildung 18: Übergeordnete Stakeholdergruppen [TU Chemnitz, BWL III]

Die Expertinnen- und Experteneinbindung konzentrierte sich primär darauf, Vertreter über alle sechs übergeordneten Felder in die Analysen einzubeziehen. Auch einige der Stakeholdergruppen des Gesamtbildes von Abbildung 17, die bei dieser Verdichtung herausgefallen sind, können im Rahmen von ergänzenden bzw. vertiefenden Einzelinterviews wichtige Erkenntnisse liefern, weshalb sie nicht ausgeschlossen werden sollen. Hierbei ist insbesondere an Behörden wie das EBA und die Bundesstelle für Eisenbahnunfalluntersuchung, an Prüfer/Zertifizierer, an Vertreter von Kundinnen und Kunden bzw. Kundenverbänden sowie an Forschungseinrichtungen zu denken. Wie in Abschnitt 4.2.2 erläutert, mussten für den Workshop zur Use Case-Bewertung die fünf anwenderseitigen, übergeordneten Stakeholdergruppen aufgrund kurzfristiger Absagen zu drei Gruppen zusammengefasst werden.

Im Rahmen dieses Kapitels erfolgte neben der Erarbeitung des vorgestellten Stakeholder-Gesamtbildes und der definitorischen Abgrenzung der einzelnen Stakeholdergruppen voneinander (siehe Anhang 13.3) auch eine Sammlung und Zuordnung von Unternehmen und Institutionen, die in den Kontaktnetzwerken der Konsortiumspartner bekannt sind, als Vertreter dieser Gruppen (inklusive dort vorhandener Ansprechpartnerinnen und -partnern). Die entsprechende Stakeholder-Kontaktliste umfasst ca. 180 Eintragungen und wurde für die Workshopeinladungen und die durchgeführte Online-Umfrage genutzt.

5.2 Konzeption und Durchführung Stakeholderanalyse

Die in Kapitel 5.1 identifizierten Makrofaktoren des relevanten Umfelds und die dort abgegrenzten Stakeholdergruppen wurden im Rahmen der eigentlichen Stakeholderanalyse genutzt, um Erkenntnisse über bestehende wirtschaftliche Leistungsverflechtungen, (vertrags-)rechtliche Verflechtungen, stakeholderspezifische Ziele und Interessen sowie gegenseitige Einflüsse zu generieren. Die zugrundeliegende Fragestellung lautet, welche System- und Wertschöpfungspartner in welcher Weise zusammenarbeiten müssen, um sinnvolle und Mehrwert versprechende Sensoranwendungen tatsächlich in die Bahnpraxis überführen zu können. Dabei dienten die sieben für die Detailbetrachtungen ausgewählten Use Cases (vgl. Tabelle 5) als Fallstudien, um zu generalisierenden Schlussfolgerungen zu gelangen.

Methodisch erfolgten im Rahmen dieses Kapitels hierfür:

- eine analytische Auseinandersetzung mit den Stakeholderbeziehungen in den betrachteten Use Cases unter Rückgriff auf vorhandene Fachliteratur und Studien;
- die Durchführung leitfadengestützter und strukturierter Interviews mit ausgewählten Expertinnen und Experten sowie deren anschließende Auswertung und
- die Zusammenführung der Erkenntnisse als Basis für das Kapitel 6.

In enger Abstimmung mit allen Konsortialpartnern sowie in Validierungsgesprächen mit ausgewählten Expertinnen und Experten des Kontaktnetzwerks (z. B. Udo Wehner, Zentrum für Wissens- und Technologietransfer der TU Chemnitz; Rachel Hegemann, DB Systel) wurde zunächst der in Abbildung 19 dargestellte Untersuchungsansatz für die Stakeholderanalyse entwickelt, um ein gemeinsames Grundverständnis der bestehenden Zusammenhänge festzuhalten.

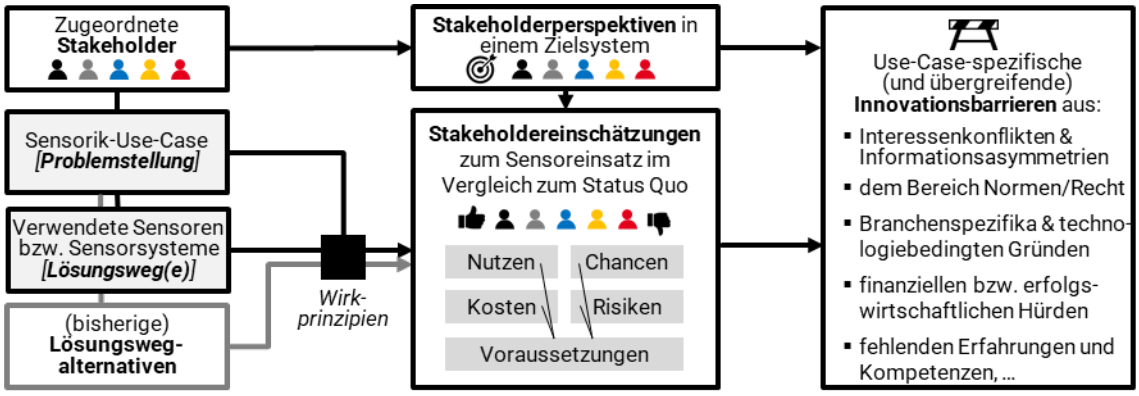


Abbildung 19: Untersuchungsansatz für die Stakeholderanalyse [TU Chemnitz, BWL III]

Den Sensorik Use Cases im Bahnsystem liegt jeweils eine spezifische *Problemstellung* zugrunde, bei der aus Sicht eines oder mehrerer Stakeholder ein bestimmtes Ziel erreicht bzw. eine spezifische Funktion erfüllt werden soll (z. B. der sichere Betrieb einer bestimmten Bahnsystemkomponente bzw. entsprechende Überprüfungen). Für dieses Ziel bzw. diese Funktion existieren in der Regel (sofern es sich nicht um völlig neue Anwendungskontexte handelt) bisherige *Lösungsalternativen*, die im Status Quo entweder noch ohne Sensorik auskommen (z. B. visuelle und manuelle Überprüfungen durch Menschen) oder schon auf einem gewissen Stand etablierter Sensortechnik beruhen. Untersuchungsgegenstand ist immer eine Problem-Lösungs-Kombination. Das heißt, für jeden Use Case werden konkrete technologie- und ggf. herstellerspezifische Sensoren bzw. Sensorsysteme als *Lösungsweg* betrachtet. Diese führen (genauso wie die Lösungsalternativen) über die jeweils zum Einsatz kommenden Wirkprinzipien oder

Wirkungsgefüge zu bestimmten Ergebnissen. Dabei ist nicht nur allein an technische Wirkprinzipien von Sensoren, sondern auch an Ursache-Wirkungs-Verflechtungen in den sozio-technischen Systemen (also z. B. auch an zur Wirkung kommende Marktmechanismen und rechtliche Zusammenhänge wie Haftungsfragen und Verpflichtungen) zu denken. Werden die Ergebnisse des innovativen Sensoreinsatzes mit denen des Status Quo verglichen, so lassen sich Einschätzungen über seine Vorteilhaftigkeit gewinnen. Diese sind aber perspektivenspezifisch in Abhängigkeit von dem verfolgten Zielsystem eines Stakeholders. Solche Stakeholdereinschätzungen betreffen den Nutzen, die Kosten, die Chancen und Risiken sowie die Voraussetzungen des Sensoreinsatzes. Sie sind im Rahmen der Stakeholderanalyse zu eruieren. Aus einer vergleichenden Gegenüberstellung dieser *Stakeholderperspektiven und -einschätzungen* können schließlich Use Case spezifische und Use Case übergreifende, den Sensoreinsatz hemmende *Innovationsbarrieren* abgeleitet werden, welche eine Grundlage für die Ableitung von Handlungsfeldern (siehe Kapitel 6) bilden. Solche Barrieren können grundsätzlich unterschiedlichen Bereichen entstammen [60]. Beim vorliegenden Untersuchungsgegenstand ist hier insbesondere mit Interessenkonflikten, Macht- und Informationsasymmetrien zwischen den Stakeholdern, mit Hürden aus dem Bereich Normen und Recht, mit besonderen Spezifika der hiesigen Bahnbranche (sowohl Schwächen als auch Stärken) und Defiziten existierender Sensortechnologien, mit wirtschaftlichen Barrieren sowie unzureichenden bisherigen Erfahrungen und Kompetenzen zu rechnen, die es in systematischer Weise herauszuarbeiten gilt.

Basierend auf einer durchgeführten Literaturanalyse zu Stakeholdertheorien und dem Stakeholdermanagement wurde, ausgehend von dem Untersuchungsansatz und in Anlehnung an [61], das nachfolgende Vorgehen für die Durchführung der Stakeholderanalyse konzipiert:

1. Identifikation der relevanten Stakeholder in den jeweiligen Use Cases und ihr Herunterbrechen auf die erforderliche Tiefe (ggf. auf funktionale Rollen)
   (*Methode: analytische Ableitung und Validierung in Expertinnen- und Experteninterviews*)
2. Herausarbeitung und Gegenüberstellung der Ziele und Interessen dieser Stakeholder mit Fokus auf den jeweils konkreten Use Case
   (*Methode: Erhebung in Expertinnen- und Experteninterviews sowie analytische Ableitung einer Basislösung für Vergleichszwecke*)
3. Bestimmung der Stakeholdereinschätzungen des Sensoreinsatzes im jeweiligen Use Case: Nutzen, Kosten, Chancen, Risiken, damit im Zusammenhang stehende Voraussetzungen und gesehene Innovationsbarrieren (*Methode: Erhebung in Expertinnen- und Experteninterviews)*
4. Bewertung der Stakeholder und ihrer Positionierung zum Use Case, insb. hinsichtlich ihrer Befürwortung der Anwendung, ihrer Bedeutung für einen Erfolg, ihres Engagements, bestehender Zielkongruenzen und -konflikte
   (*Methode: analytische Ableitung aus den Antworten der Expertinnen- und Experteninterviews)*
5. Stakeholder und Use Case übergreifende Auswertung hinsichtlich benötigter Kooperationen und Leistungsverflechtungen samt potenzieller Marktakteure sowie potenzieller Handlungsfelder

Nachfolgend werden die Ergebnisse für die sieben untersuchten Fallstudien Use Cases dargestellt. Darin sind die Einschätzungen von Expertinnen und Experten und eventuelle Rückmeldungen zu analytisch hergeleiteten Basislösungen bereits eingearbeitet. Die Innovationsbarrieren werden strukturiert und Use Case übergreifend in Abschnitt 5.3 dargestellt. Auf eine Use Case spezifische Zuordnung in der Ergebnisdarstellung wurde aus Gründen der Übersichtlichkeit (Vermeidung von Wiederholungen in lediglich anderen Formulierungen) verzichtet.

Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)

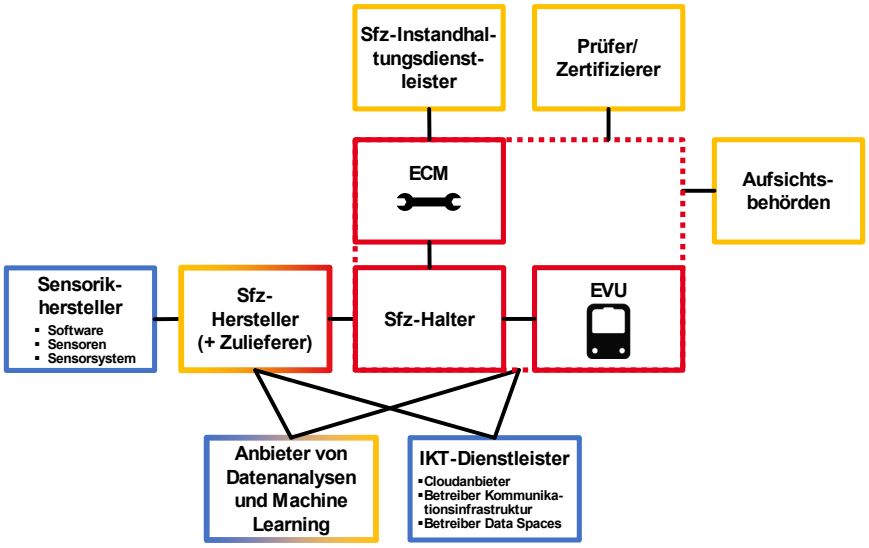


Abbildung 20: Involvierte Stakeholder im Use Case *Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)* [TU Chemnitz, BWL III]

Im Zentrum dieser sensorbasierten Anwendung stehen die Betreiber elektrisch angetriebener Schienenfahrzeuge, insbesondere von Elektrolokomotiven und Elektrotriebwagen. Zur Vereinfachung und aufgrund weitgehend übereinstimmender Interessen werden für die Analyse dieses Anwendungsfalls die drei Stakeholderrollen Sfz-Halter, EVU und ECM zusammengefasst (in Abbildung 20 gekennzeichnet durch die gestrichelte Linie). Auch die Schienenfahrzeughersteller (sowie dem elektrischen Antriebssystem zuordenbare Zulieferer) können zumindest indirekte (ggf. auch direkte) Anwender dieser Sensorlösung darstellen, wenn sie im Fahrzeugbetrieb erhobene Sensordaten zur Produktverbesserung bzw. -weiterentwicklung nutzen. Die Sensorikhersteller (im Sinne der Sensorsystemhersteller und der dahinterliegenden Wertschöpfungskette) beliefern in diesem Use Case die Fahrzeughersteller mit der Sensortechnik zur Überwachung von Antriebskomponenten. Als weitere Enabler der tatsächlichen Nutzbarkeit dieser Sensorlösung agieren zum einen verschiedene IKT-Dienstleister, welche das Übertragen und Bereitstellen von Sensordaten aus dem Fahrzeug heraus an Fahrzeugbetreiber (Halter/EVU/ECM) bzw. Fahrzeughersteller ermöglichen und zum anderen Anbieter von Datenanalysen und Machine Learning, durch deren Produkte und Leistungen die große Menge und Vielfalt gesammelter Sensor(roh)daten erst interpretier- und verstehbar wird. Für die Verwertung sensorbasierter Erkenntnisse im Rahmen der Fahrzeuginstandhaltung ist nicht nur die ECM selbst als direkter Anwender zu sehen, sondern auch ggf. für spezifische Instandhaltungsarbeiten am Antriebssystem eingebundene Instandhaltungsdienstleister als indirekte Anwender. Schließlich sind mittelbar von diesem Use Case auch die Aufsichtsbehörden (insbesondere das EBA) sowie akkreditierte, unabhängige Prüfer und Zertifizierer von Relevanz, wenn es um die Überwachung der Fahrzeuginstandhaltung und der Betriebsabläufe in EVUs (hier speziell: Entscheidungen auf Basis von Sensordaten) sowie die Überprüfung von Instandhaltungsbetrieben und EVUs hinsichtlich der Einhaltung erforderlicher Standards geht.

In Tabelle 24 sind die Ergebnisse hinsichtlich der von den primär relevanten Stakeholdern mit dem Use Case verfolgten Ziele und Interessen sowie bezüglich ihrer Einschätzungen zu Nutzen, Kosten, Chancen, Risiken des Use Case in komprimierter Form übersichtlich dargestellt.

TABELLE 24: STAKEHOLDERANALYSE *FAHRZEUG ÜBERWACHT FAHRZEUG: ANTRIEBSZUSTAND (ELEKTRO)*

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
Sfz-Halter/ EVU/ECM	▪ Wirtschaftlicher Betrieb des Sfz ▪ Vermeidung von Betriebsstörungen ▪ Optimierte Fahrzeuginstandhaltung	▪ Minimierung von Ausfallzeiten durch Früherkennung und gezieltere Instandhaltungsmaßnahmen ▪ Minimierung der Betriebskosten des Sfz durch bessere Zuverlässigkeit und Vermeidung von Folgeschäden	▪ Kosten des Zugangs zu Sensordaten (z. B. nur beim Hersteller verfügbar) ▪ Aufwand und Schwierigkeit eigener Datenauswertungen (u. a. Schulungskosten) ▪ Kosten von Datenauswertungen durch Dritte (Spezialisten)	▪ Künftige Schadensvermeidung durch besseres Verständnis der Anzeichen/Ursachen ▪ Kosteneinsparungen durch Umstellung von planmäßiger Instandhaltung auf Condition-Based (CBM)/Predictive Maintenance (PM)	▪ Unzureichende finanzielle und personelle (Qualifikation) Ressourcen für die Anwendung ▪ Unzureichendes Kosten-Nutzen-Verhältnis der analysierten Datenbasis ▪ Regulatorische Zulässigkeit von CBM/PM fraglich
Sfz-Hersteller (+ Zulieferer)	▪ Wettbewerbsvorteile beim Absatz von Sfz bzw. Antrieben (Steigerung der Produktzuverlässigkeit) ▪ Diversifizierung des Produktportfolios mit ergänzenden oder zusätzlichen Leistungen ▪ Vermeidung von evtl. Gewährleistungsansprüchen	▪ Verbesserung des Produktdesigns künftiger Antriebe/Sfz auf Basis von Daten aus dem Betrieb ▪ Kundenbindung durch Qualitätsverbesserungen und Unterstützung bei der Sfz-Wartung ▪ Überwachungs- Diagnose- und Prädiktionsleistungen als Komplementärprodukt zum Sfz ▪ ggf. direkte Monetarisierung eigener Sensordaten	▪ Entwicklungs-, Beschaffungs- und Implementierungskosten für die Sensorintegration ▪ Qualifikations-/ Personalkosten für eigene Auswertungen bzw. Kosten von Datenauswertungen durch Dritte (Spezialisten) ▪ Bei eigenen Überwachungs- Diagnose- und Prädiktionsprodukten: Systementwicklungs- und Systembetreuungskosten	▪ Abgrenzung von Wettbewerbern durch Qualitätsvorteile und neue Leistungsbündel ▪ Erschließung zusätzlicher Erlösquellen aus den Ergänzungsleistungen	▪ Unerwünschter Abfluss sensibler Sfz-bezogener Unternehmensdaten durch den Datenaustausch ▪ Unzureichende Vermarktbarkeit eigener Überwachungs- Diagnose- und Prädiktionsleistungen (Kompetenzvorsprung bei Datenanalysten oder zu geringe Zahlungsbereitschaft bei Halter/EVU/ECM)
Sensorikhersteller	▪ Erreichen bzw. Bewahren von Innovationskraft und Technologieführerschaft ▪ Etablierte Bahnzulieferer: Sicherung bzw. Steigerung des Absatzes eigener Sensorprodukte ▪ Neueinsteiger: Erschließung des Geschäftsfeldes Bahn	▪ Weiterentwicklung/Verbesserung der Sensorik für die spezifische Anwendung ▪ Gewinnung von Marktanteilen und Kundenbindung als Lieferant im Oligopol der Sfz-Hersteller	▪ F&E-Kosten neuartiger Sensoren/Sensorsysteme (ggf. über viele, auch bahnferne Anwendungen amortisierbar) ▪ Fertigungskosten bahnfester Sensoren/Sensorsysteme (dürfen nicht zu hoch für bahntypische Stückzahlen sein)	▪ Wachsende Produktnachfrage, insb. durch zunehmende Verbreitung von Batterietriebzügen ▪ Auf-/Ausbau von Markteintrittsbarrieren und Stärkung der Marktposition als etablierter Lieferant der Sfz-Hersteller (Know-How-Vorsprung)	▪ Etablierte Bahnzulieferer: Preisdruck durch Konkurrenten, da bereits etablierte Sensorik in Elektroantrieben ▪ Neueinsteiger: Entwicklungsaufwand bahnfester Sensorik ggf. nicht lohnend ▪ Ggf. Produkthaftungsrisiken für fehlerhaft funktionierende Sensorsysteme
IKT-Dienstleister	▪ Etablierung als zuverlässige Anbieter für die sichere Übertragung und Bereitstellung sensorbasierter Daten im Bahnsektor ▪ Erlösgenerierung durch verstärkten Datenaustausch (z. B. zwischen	▪ Gesteigerte Datenkommunikation und Cloudnutzung bzw. mehr Plattformnutzer oder Transaktionen gegen entsprechende Entgelte ▪ Ggf. Verbesserung eigener Systeme	▪ Kosten für den Aufbau und Betrieb der IKT-Infrastrukturen i. e. S. (Datenübertragung und -speicherung) ▪ Kosten für die Datensicherheit (Schutz sensibler	▪ Diversifikation: Referenzen für bahnspezifische Produktlösungen ▪ Etablierung langfristiger Partnerschaften und neuer Kooperationen zu Betreibern/Herstellern von Sfz	▪ Reputationsschäden, ggf. rechtlichen Konsequenzen bei unzureichender Datensicherheit ▪ Schnelllebigkeit von Technologien und hohe Wettbewerbsintensität im IKT-Sektor

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	Herstellern und Betreibern von Sfz)	hinsichtlich bahnspezifischer Anforderungen	Daten vor unbefugten Zugriffen und Verfälschung), insb. Entwicklung und laufende Aktualisierung von Schutzsystemen	▪ Beitrag zur Entstehung neuer Angebote und Geschäftsmodelle basierend auf dem Sensordatenaustausch	▪ Hohe Abhängigkeit von relativ wenigen Kunden (EVU und Sfz-Hersteller)
Anbieter von Datenanalysen/Machine Learning	▪ Entwicklung und Verkauf von Analyse-, Diagnose- und Vorhersagetools an Sfz-Halter/EVU/ ECM oder Sfz-Hersteller ▪ Verkauf von Schulungen oder Beratungsleistungen im Bereich der Fahrzeugdiagnose und -wartung	▪ Entwicklung/ Optimierung funktionsfähiger und nutzenstiftender Modelle/Algorithmen durch Füttern mit realen Betriebsdaten von Sfz-Elektroantrieben ▪ Kenntnisgewinn über Informationsbedarfe bei Betreibern/Herstellern von Sfz	▪ Technologie(weiterentwicklungs) kosten ▪ Qualifizierungs- und Personalkosten spezialisierter Mitarbeiter mit zumindest grundlegenden Bahnkenntnissen	▪ Kompetenzgewinn bei der Muster- und Anomalieerkennung für Elektroantriebe ▪ Übertragung von Kompetenzgewinnen und Produktlösungen auf andere sensorbasierte Anwendungen im Bahnsektor und darüber hinaus	▪ Fehlende Abschätzbarkeit des Geldwertes der Nutzenpotenziale bei den Anwendern ▪ Damit vorab Unsicherheit, wie lohnend die Entwicklung derart spezifischer Lösungen ist
Sfz-Instandhaltungsdienstleister	▪ Verkauf von Instandhaltungsdienstleistungen an die ECM ▪ Effiziente Erledigung eigener Instandhaltungsarbeiten (Vermeidung unnötiger und unnötig langer Arbeiten, z. B. für Fehlersuche)	▪ Gezieltere und schnellere Erledigung der Arbeiten durch präzisere Diagnosedaten von Antriebsproblemen ▪ Lerneffekte und Qualitätsverbesserungen bei den eigenen Instandhaltungsarbeiten	▪ Weiterbildungs- bzw. Schulungskosten für die richtige Dateninterpretation durch eigene Mitarbeiterinnen und Mitarbeiter ▪ Ggf. Investitionsbedarf in technische Schnittstellen zur Datenübermittlung	▪ Ggf. Vermarktung präventiver Instandhaltungsarbeiten auf Basis von Sensordaten als neues Angebot	▪ Verlust menschlicher Diagnosekompetenzen durch zu starkes Verlassen auf Analysetools ▪ Ggf. Risiko, dass ECM durch Analyse-, Diagnose- und Vorhersagetools auf die eigenen spezifischen Kompetenzen verzichten kann
Aufsichtsbehörden	▪ Verbesserung des Sicherheitsniveaus im Eisenbahnbetrieb ▪ Effizienzsteigerungen Bahnbetrieb und -instandhaltung ▪ Förderung elektrischer Antriebe	▪ Weniger Betriebsstörungen ▪ Ggf. bessere Kenntnisse über Zustände/Probleme der Sfz-Instandhaltung im Markt	▪ Ggf. Kosten einer Daten- und Systemintegration aus verschiedenen Quellen für ein umfassendes Gesamtbild ▪ Kosten einer Datenökonomie für den Markt (und Verteilungsfrage)	▪ Ggf. verbesserte Überwachung von ECM und Instandhaltungsdienstleistern auf Basis aggregierter Zustandsdaten	▪ Ermöglichung neuer Angriffspotenziale im Bereich sensibler Fahrzeugdaten
Prüfer/ Zertifizierer	▪ Verkauf von Prüfungs- und Zertifizierungsleistungen ▪ Gewährleistung der Sicherheit, Qualität, Konformität von Produkten und Prozessen	▪ Größere und objektivere Datengrundlage bei der Durchführung von Prüfungen und Zertifizierungen ▪ Eigene Erkenntnisgewinne	▪ Ggf. Investitionsbedarf in technische Schnittstellen ▪ Schulungskosten für eigene Mitarbeiter bzgl. Sensoranwendungen	▪ Ggf. neue Marktsegmente für Prüfdienstleistungen ▪ Mitwirkung an der Entwicklung neuer Standards	▪ Haftungsrisiken im Zusammenhang mit der Dateninterpretation ▪ Unsichere Entwicklung bzgl. Standards und Vorschriften

Zusammenfassend lassen sich folgende Schlussfolgerungen aus der anwendungsspezifischen Stakeholderanalyse ableiten:

- Es bestehen stakeholderübergreifende **Zielkongruenzen** bei dem Use Case hinsichtlich einer grundlegenden Stärkung des Systems Bahn insgesamt im Sinne von mehr Sicherheit, Effizienz und einer Störungsvermeidung.
- **Potenzielle Interessenkonflikte** zwischen den Stakeholdern bestehen hinsichtlich der Offenlegung von Sfz-Daten (Sfz-Hersteller wollen dies vermeiden) sowie bezüglich der Bedarfe nach eigenen Wertschöpfungsbeiträgen und der zugehörigen Preise. ECM haben hier Interesse an der Erbringung von profitablen planmäßigen und außerplanmäßigen Instandhaltungsleistungen. Anbieter von Datenanalysen haben hier Interesse an der Erbringung von profitablen Analyseleistungen. EVU bzw. Sfz-Halter möchten insgesamt möglichst wenig für Instandhaltungs- und Analyseleistungen ausgeben.
- **Größter Nutznießer** des Use Cases ist das EVU bzw. der Sfz-Halter.
- Die **wichtigsten Wertschöpfungspartner** des Use Cases sind der Sfz-Hersteller, die Anbieter von Datenanalysen und die ECM bzw. die Instandhaltungsdienstleister.

Fahrzeug überwacht Fahrzeug: Zustand von Türen und anderen Verriegelungen

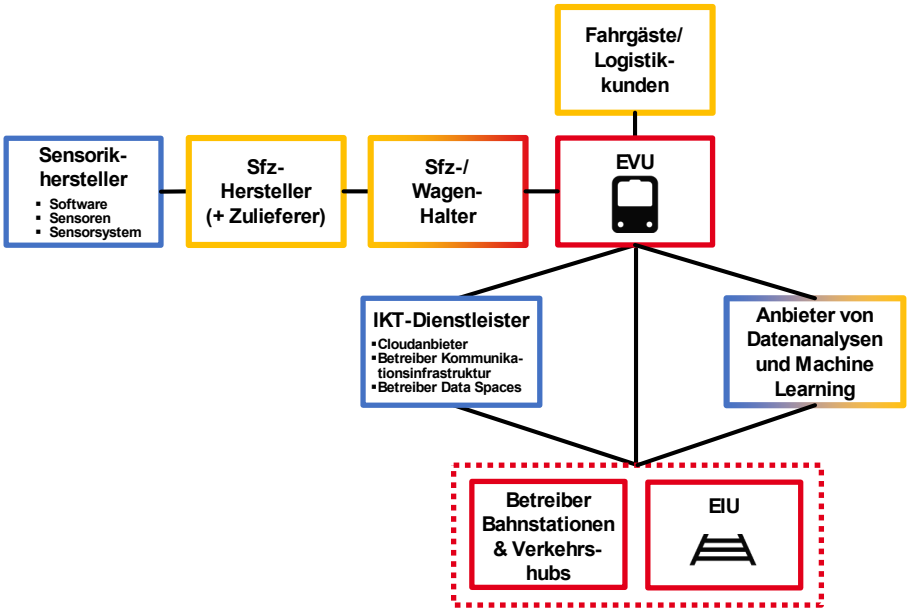


Abbildung 21: Involvierte Stakeholder im Use Case *Fahrzeug überwacht Fahrzeug: Zustand von Türen/Verriegelungen* [TU Chemnitz, BWL III]

Im Zentrum dieser sensorbasierten Anwendung stehen die Betreiber von Schienenfahrzeugen, sowohl des Personennah- und Fernverkehrs (Sicherheitsverriegelungen von Ein- und Ausstiegstüren) als auch des Güterverkehrs (Verschlüsse/Verriegelungen für die Ladungssicherung und den Verbund von Güterwagen), sowie als Pendant auf der Infrastrukturseite die Betreiber von entsprechenden Bahnstationen und Verkehrshubs (Personen-, Rangier- und Güterbahnhöfe, Kombinierter Verkehr (KV)-Terminals, Mobilitätsstationen etc.). Hierfür wurden in der Analyse die korrespondierenden Stakeholderrollen EVU sowie – in Abbildung 21 mit gestrichelter Linie zu einer zweiten Analyseeinheit zusammengefasst – die Betreiber von Bahnstationen, Verkehrshubs und EIU angesetzt. Einen weiteren wichtigen und im Falle des Güterverkehrs regelmäßig separat vom EVU zu betrachtenden Anwender stellen die Sfz- bzw. Wagenhalter (Logistikunternehmen, Vermietungs- und Leasinggesellschaften von Güterwagen) dar. Indirekte Anwender dieser Sensoranwendung sind die Fahrgäste und Logistikkunden als die im Transportprozess

betroffenen Endkunden sowie die Schienenfahrzeughersteller (sowie den Verrieglungssystemen zuordenbare Zulieferer) als Umsetzer von Produktverbesserungsmöglichkeiten basierend auf im Betrieb erhobenen Daten. Die Sensorikhersteller (im Sinne der Sensorsystemhersteller und der dahinterliegenden Wertschöpfungskette) beliefern in diesem Use Case die Fahrzeughersteller mit der Sensortechnik zur Überwachung der jeweiligen personen- oder güterverkehrsseitigen Verriegelungssysteme. Als weitere Enabler der tatsächlichen Nutzbarkeit dieser Sensorlösung agieren zum einen verschiedene IKT-Dienstleister, welche das Übertragen und Bereitstellen von Sensordaten der Verriegelungen an relevante Adressaten (z. B. an das Lade-, Sicherheits- und Rangierpersonal von Bahnstationen und Verkehrshubs oder an EVU und Wagenhalter) ermöglichen und zum anderen Anbieter von Datenanalysen und Machine Learning, durch deren Produkte und Leistungen eine große Menge entsprechend gesammelter Sensor(roh)daten für weitergehende Interpretationen und Optimierungen genutzt werden kann.

In Tabelle 25 sind die Ergebnisse hinsichtlich der von den primär relevanten Stakeholdern mit dem Use Case verfolgten Ziele und Interessen sowie bezüglich ihrer Einschätzungen zu Nutzen, Kosten, Chancen, Risiken des Use Case in komprimierter Form übersichtlich dargestellt.

TABELLE 25: STAKEHOLDERANALYSE FAHRZEUG ÜBERWACHT FAHRZEUG – ZUSTAND VON TÜREN UND ANDEREN VERRIEGELUNGEN

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
EVU	▪ Sicherer Betrieb des Sfz bzw. Wagens ▪ Vermeidung von Betriebsstörungen und Einhaltung der Fahrpläne	▪ Schnellere Zugabfertigung im Güterverkehr und an Haltepunkten im Personenverkehr (Kundenzufriedenheit, Effizienz) ▪ Sinnvollerer Personaleinsatz im Güterverkehr (manuelle Tätigkeiten ersetzen)	▪ Gestiegene Komplexität der Instandhaltung der Komponenten (Mitarbeiterschulungen) ▪ Kosten der Sensorwartung	▪ Ggf. Zusatznutzen (z. B. Fahrgastzählung) ▪ Imageverbesserungen durch pünktlichere Zugfahrten	▪ Datenschutzprobleme ▪ Negative Auswirkungen auf Fahrplan und Kundenvertrauen bei Fehlern oder Manipulationen der Sensorlösung
Sfz-/Wagen-Halter	▪ Sicherheit des Sfz/ Wagens bzw. transportierter Güter und Fahrgäste	▪ Vermeidung von Schäden und Folgekosten durch menschliche Fehler	▪ Investitionskosten für Nachrüstlösungen ▪ Kosten der Sensorwartung	▪ Kosten- und Zeitersparnisse durch effizientere Abfertigung ▪ Vertrauensstärkung gegenüber Logistikkunden	▪ Evtl. Zusatzkosten durch Sensorfehlfunktionen ▪ Ggf. unzureichendes Kosten-Nutzen-Verhältnis
Sfz-Hersteller (+ Zulieferer)	▪ Kundenbindung und Wettbewerbsvorteile durch Innovations- und Zuverlässigkeitsvorsprung der Systeme (positive Wirkung auf Sfz-Absatz)	▪ Verbesserung der Systemzuverlässigkeit auf Basis von Daten aus dem Betrieb ▪ Ggf. Realisierung von Synergien mit anderen Sensoranwendungen	▪ (Weiter-)Entwicklungs-, Beschaffungs- und Implementierungskosten für die Sensorlösung	▪ Komplementäre Anwendungen auf Basis der verbauten Sensorik ▪ Verbesserung der Zuverlässigkeit/ Lebensdauer der Türen/Verriegelungen auf Basis der Sensordaten	▪ Gewährleistungsrisiken und Imageschäden bei Fehlfunktionen oder Unzuverlässigkeit der Systeme
Sensorikhersteller	▪ Weiterentwicklung bzw. Erweiterung des Produktprogramms für neue Sensoranwendungen ▪ Etablierte Bahnzulieferer: Umsatzsteigerungen für eigene Sensorprodukte	▪ Verbesserung der Zuverlässigkeit der Sensorik für die spezifische Anwendung ▪ Etablierung als renommierter Lieferant für sichere und zuverlässige Sensorlösungen gegenüber den Sfz-Herstellern	▪ F&E-Kosten neuartiger Sensoren/Sensorsysteme ▪ Fertigungskosten bahnfester Sensoren/Sensorsysteme (dürfen nicht zu hoch für bahntypische Stückzahlen sein)	▪ Wachsende Nachfrage nach Sensorüberwachung insb. im Güterwagenbereich ▪ Diversifikation des Produktportfolios mit neuen Sensoranwendungen im Bahnsektor	▪ Hohe Entwicklungskosten für spezialisierte Bahnanwendungen ggf. nicht rentabel ▪ Leichte Substituierbarkeit durch billigere, alternative Sensortechnologien zu erwarten

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	▪ Neueinsteiger: Erschließung des Geschäftsfeldes Bahn				▪ Reputationsrisiken bei fehlerhaften Neuentwicklungen
Betreiber Bahnstationen & Verkehrshubs, EIU	▪ Effiziente und sichere Abwicklung des Zugverkehrs ▪ Reduzierung von Störungen und Verzögerungen durch Probleme an Türen/Verriegelungen	▪ Steigerung der Verfügbarkeit eigener Infrastrukturen für Kunden ▪ Sinnvollerer Einsatz des eigenen Servicepersonals	▪ Kosten der Umstellung betrieblicher Abläufe ▪ Ggf. Investitions- und Betriebskosten für Schnittstellen zur Datenübertragung und -verarbeitung	▪ Verbesserte Kundenzufriedenheit durch reibungslose Zugabwicklung ▪ Ggf. Einsparung von bzw. geringere Anforderungen an Servicepersonal	▪ Fehlerhafte Verriegelungssensorik als neue Störungsquelle ▪ Manipulationsmöglichkeiten ▪ Ggf. datenschutzrechtliche Missbrauchsmöglichkeiten
Fahrgäste, Logistikkunden	▪ Personen- und Frachtsicherheit ▪ Pünktlichkeit und Zuverlässigkeit ▪ reibungsloser Ein-/ Ausstieg bzw. effiziente Verladung	▪ Verringerung des Risikos von Verspätungen ▪ Verringerung von Sicherheitsrisiken	▪ Keine direkten Kosten ▪ Ggf. Weitergabe von Zusatzkosten der Sensorik an Ticketpreise/ Transportentgelte	▪ Besseres Fahrgasterlebnis ▪ Effizienzsteigerungen in der Logistikkette	▪ Tracking- und Tracing-Risiken ▪ Unnötige Störungen durch Fehlalarme der Sensorik
IKT-Dienstleister	▪ Etablierung als zuverlässige Anbieter für die sichere Bereitstellung sensorbasierter Daten im Bahnsektor ▪ Weiterentwicklung und Demonstration eigener Technologiekompetenz	▪ Weiterentwicklung eigener Plattformen zu bahnkonformen Lösungen ▪ Umsatzsteigerungen durch Datenkommunikation, Cloud- bzw. Plattformnutzung	▪ Kosten für Aufbau, Implementierung und Betrieb der IKT-Infrastrukturen ▪ Kosten für die Datensicherheit (laufende Aktualisierung von Schutzsystemen)	▪ Diversifikation: Referenzen für bahnspezifische Produktlösungen ▪ Weiterentwicklung zu domänenübergreifenden Angeboten/Geschäftsmodellen (Verkehrssektor und darüber hinaus)	▪ Reputationsschäden, ggf. rechtlichen Konsequenzen bei unzureichender Datensicherheit ▪ Schnelllebigkeit von Technologien und hohe Wettbewerbsintensität im IKT-Sektor
Anbieter von Datenanalysen/Machine Learning	▪ Erschließung des Geschäftsfelds Bahn mit neuen Analyseprodukten ▪ Zugriff auf Realdaten zur Produktentwicklung	Entwicklungsmöglichkeiten für Analysealgorithmen und ML-Modelle: ▪ Verriegelungen ▪ komplementäre Anwendungen	▪ F&E-Kosten der Entwicklung neuer Algorithmen/Modelle ▪ Personalbeschaffungs- und Qualifizierungskosten (Bahnkenntnisse)	▪ Erhöhung der Wettbewerbsfähigkeit durch verbesserte Datenmodelle ▪ Reputationsgewinn mit Referenzen für spezifische Bahnlösungen	▪ Reputationsrisiken bei unzureichender Analysegüte ▪ Fehlende Abschätzbarkeit tatsächlich möglicher Mehrwerte von Analyseprodukten

Zusammenfassend lassen sich folgende Schlussfolgerungen aus der anwendungsspezifischen Stakeholderanalyse ableiten:

- Es bestehen stakeholderübergreifende **Zielkongruenzen** bei dem Use Case hinsichtlich einer gewünschten Beschleunigung der Zugabfertigung (durch Einsparungen manueller Vorgänge und eine bessere Behebung von Verzögerungsursachen) bei gleichzeitiger Unfallvermeidung (sowohl durch Störfälle bei Ein- und Ausstieg bzw. Verladung als auch während der Fahrt)
- **Potenzielle Interessenkonflikte** zwischen den Stakeholdern bestehen hinsichtlich des Preisniveaus und der Zuverlässigkeit der verwendeten Sensorlösungen. Anbieter möchten möglichst hohe Umsätze bei überschaubaren Entwicklungs- und Fertigungskosten generieren, während die Anwender aufgrund der sehr hohen Zahl von Türen bzw. Verriegelungen im Rollmaterial sehr stark auf Kosteneffizienz und eine hohe Zuverlässigkeit getrimmt sind. Weitere Interessenkonflikte betreffen wahrgenommene Tracking- und Tracing-Risiken von Seiten der Fahrgäste und Logistikkunden.
- **Größter Nutznießer** des Use Cases ist das EVU bzw. der Sfz-/Wagenhalter.

- Die **wichtigsten Wertschöpfungspartner** des Use Cases sind die Sensorsystemhersteller sowie die Sfz-/Wagenhersteller. Ihnen obliegt es, wirtschaftliche Sensorlösungen für die Zustandserkennung von Türen und Verriegelungen mit einem adäquaten Kosten-Nutzen-Verhältnis in das entsprechende Rollmaterial zu integrieren. Anbieter von Datenanalysen/Machine Learning spielen bei dieser Anwendung eine vergleichsweise untergeordnete Rolle, sofern es um die reine Zustandserkennung von Türen und Verriegelungen und nicht um weiterreichende Detektionsanwendungen geht.

Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant

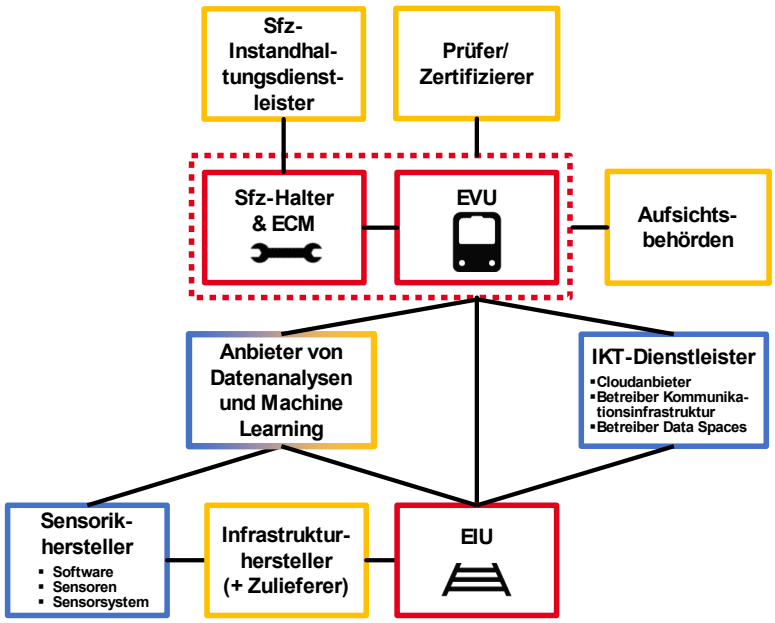


Abbildung 22: Involvierte Stakeholder im Use Case *Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant* [TU Chemnitz, BWL III]

Die zentralen Stakeholder dieser sensorbasierten Anwendung sind zum einen die Betreiber von Schienenfahrzeugen, für welche Fahrzeugzustandsdaten erfasst und bereitgestellt werden, und zum anderen die EIU, auf deren Anlagen mit entsprechenden Sensorsystemen diese Zustandsdatenerfassung erfolgt. Bei ersteren werden für die Analyse dieses Anwendungsfalls zur Vereinfachung und aufgrund der zusammenhängenden Interessen die Stakeholderrollen EVU, Sfz-Halter und ECM zusammengefasst (in Abbildung 22 gekennzeichnet durch die gestrichelte Linie). Ein primärer Anwendungszweck ist im vorliegenden Fall die zustandsorientierte Fahrzeuginstandhaltung. Für eine solche kommen neben der direkten Anwenderrolle der ECM auch diverse weitere Sfz-Instandhaltungsdienstleister (z. B. mit spezialisierten Leistungen für Fahrwerke, Karosserien oder Scheiben) als indirekte Anwender in Betracht. Auch wenn im untersuchten Use Case nicht-sicherheitsrelevante Fahrzeugeigenschaften im Fokus stehen, so sind dennoch (auch im Sinne der Vollständigkeit) die Aufsichtsbehörden (insbesondere das EBA) sowie akkreditierte, unabhängige Prüfer und Zertifizierer von grundsätzlicher Relevanz, wenn es um die Überwachung der Fahrzeuginstandhaltung und der Betriebsabläufe in EVUs (hier speziell: Entscheidungen auf Basis von Sensordaten) sowie die Überprüfung von Instandhaltungsbetrieben und EVUs hinsichtlich der Einhaltung erforderlicher Standards geht. Die Sensorikhersteller (im Sinne der Sensorsystemhersteller und der dahinterliegenden Wertschöpfungskette) beliefern in diesem Use Case die Infrastrukturhersteller (bzw. Zulieferer entsprechender Infrastrukturkomponenten wie Schwellen oder Kamerabrücken) mit der in die Infrastruktur der EIU zu integrierenden streckenseitigen Sensortechnik. Als wichtige Enabler der tatsächlichen Nutzbarkeit dieser Sensorlösung agieren wieder verschiedene IKT-Dienstleister, welche das Übertragen und Bereitstellen von infrastrukturseitig erhobenen Sensordaten über den Fahrzeugzustand an die Fahrzeugbetreiber (EVU/Halter/ECM) und ggf. weitere Adressaten ermöglichen

sowie Anbieter von Datenanalysen und Machine Learning, durch deren Produkte und Leistungen die im vorliegenden Anwendungsfall besonders große Menge und Vielfalt gesammelter Sensor(roh)daten erst interpretier- und verstehbar wird.

In Tabelle 26 sind die Ergebnisse hinsichtlich der von den primär relevanten Stakeholdern mit dem Use Case verfolgten Ziele und Interessen sowie bezüglich ihrer Einschätzungen zu Nutzen, Kosten, Chancen, Risiken des Use Case in komprimierter Form übersichtlich dargestellt.

TABELLE 26: STAKEHOLDERANALYSE INFRASTRUKTUR ÜBERWACHT FAHRZEUG – NICHT SICHERHEITSRELEVANT

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene ...				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
EVU/ Sfz-Halter & ECM	▪ Sicherer und wirtschaftlicher Betrieb des Sfz ▪ Vermeidung von Betriebsstörungen ▪ Optimierte Fahrzeuginstandhaltung	▪ Minimierung von Ausfallzeiten mit Früherkennung und zustandsbasierter Instandhaltung ▪ Vermeidung von Folgeschäden ▪ Nutzung sensorbasierter Detektion ohne eigene Investitionen in Sensortechnik	▪ An EIU zu zahlende Entgelte für Sfz-Zustandsdetektion ▪ Kosten für richtige Interpretation der Sensordaten: ▪ Mitarbeiterschulungen ▪ Leistungen von Datenanalysten	▪ Kosteneinsparungen durch teilweise Umstellung auf Condition-Based (CBM)/Predictive Maintenance (PM) ▪ Wirtschaftliche Vorteile streckenseitiger Detektion ▪ Reputationsverbesserungen mit mangelärmeren Zügen	▪ Fehlendes oder zu teures Angebot von Seiten der EIU ▪ Ungewollter Datenabfluss über eigene Sfz-Flotten ▪ Neue Abhängigkeiten durch fehlende eigene Kompetenzen und Sensortechnik ▪ Regulatorische Zulässigkeit von CBM/PM fraglich
EIU	▪ Sicherheit und Zuverlässigkeit der Infrastruktur ▪ Vermeidung von Betriebsstörungen auf eigenen Strecken	▪ Kein direkter bzw. unmittelbarer Nutzen! ▪ Möglichkeit der Erweiterung des bestehenden Geschäftsfeldes/ neue Erlösquellen	▪ Investitionskosten in die gesamte Sensortechnik ▪ Betriebskosten der Sensortechnik ▪ Kosten der Qualifizierung eigenen Personals bzw. Kosten von Datenauswertungen durch Dritte	▪ Kompetenzgewinn ▪ Aufbau eines profitablen neuen Geschäftsfeldes gegenüber den EVU ▪ Vermeidung des übermäßigen Verschleißes eigener Schieneninfrastruktur durch mangelhafte Sfz	▪ Risiko versunkener Kosten in Sensortechnik bei ausbleibender Nachfrage von Seiten der EVU bzw. der Unwirtschaftlichkeit des Geschäftsmodells ▪ Haftungsrisiken bezüglich Abfluss schützenswerter Unternehmensdaten der EVU
Infrastruktur-hersteller (+ Zulieferer)	▪ Vermarktung höherwertigerer und teurerer Infrastrukturen ▪ Erweiterung des Produktportfolios	▪ Zusatzerlöse durch Integration von Sensortechnik bzw. Verkauf entsprechender Komplettlösungen ▪ Kundenbindung von EIU für entsprechende Speziallösungen	▪ Beschaffungs- und Implementierungskosten für die Sensorintegration ▪ Bei eigenen Überwachungs-, Diagnose- und Prädiktionsprodukten: Systementwicklungs- und Systembetreuungskosten	▪ Abgrenzung von Wettbewerbern durch Produktinnovationen ▪ Profitabler Absatz integrierter Sensorlösungen ▪ Profitable Wartungsleistungen für die Sensorik	▪ Risiko versunkener Entwicklungskosten in nicht nachgefragte Produkte ▪ Gewährleistungsrisiken und Imageschäden bei Fehlfunktionen oder Unzuverlässigkeit der Systeme
Sensorikhersteller	▪ Weiterentwicklung bzw. Erweiterung des Produktprogramms für neue stationäre Sensoranwendungen	▪ Funktions- und Qualitätsverbesserung der eigenen Sensor- und Datenfusionslösungen mit Sfz-Flottendaten aus dem Betrieb	▪ F&E-Kosten neuartiger Sensoren/Sensorsysteme ▪ Fertigungskosten bahnfester Sensoren/Sensorsysteme	▪ Diversifikation des Produktportfolios mit nachgefragten neuen Sensoranwendungen im Bahnsektor	▪ Hohe Entwicklungskosten für spezialisierte Bahnanwendungen bei Unklarheit über tatsächliche Nachfrage

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	▪ Etablierte Bahnzulieferer: Umsatzsteigerungen für eigene Sensorprodukte ▪ Neueinsteiger: Erschließung des Geschäftsfeldes Bahn	▪ Etablierung als renommierter Lieferant für stationäre Sensorlösungen gegenüber den Infrastrukturherstellern und EIU		▪ Erreichen von Technologieführerschaft ▪ Ggf. wirtschaftlich vorteilhaftes Alternativangebot zu fahrzeugseitiger Sensordetektion	▪ Reputationsrisiken bei fehlerhaften Neuentwicklungen
IKT-Dienstleister	▪ Etablierung als zuverlässige Anbieter für die sichere, stakeholderübergreifende Bereitstellung sensorbasierter Daten im Bahnsektor ▪ Weiterentwicklung und Demonstration eigener Technologiekompetenz	▪ Weiterentwicklung von Cloud-Plattformen und Data Spaces für bahnkonforme Lösungen ▪ Umsatzsteigerungen durch Datenkommunikation, Cloud- bzw. Plattformnutzung	▪ Kosten für Weiterentwicklung, Aufbau, Implementierung und Betrieb der IKT-Infrastrukturen ▪ Kosten für die Datensicherheit (laufende Aktualisierung von Schutzsystemen)	▪ Bildung strategischer Partnerschaften mit EIU und EVU ▪ Absatz ergänzender Beratungsleistungen ▪ Weiterentwicklung zu domänenübergreifenden Angeboten/Geschäftsmodellen	▪ Reputationsschäden, ggf. rechtlichen Konsequenzen bei unzureichender Datensicherheit ▪ Schnelllebigkeit von Technologien und hohe Wettbewerbsintensität im IKT-Sektor
Anbieter von Datenanalysen/Machine Learning	▪ Erschließung des Geschäftsfelds Bahn mit neuen Analyseprodukten ▪ Zugriff auf Realdaten zur Produktentwicklung ▪ Ausbau technologischer Kompetenz	Entwicklungsmöglichkeiten für Analysealgorithmen und ML-Modelle: ▪ Güte der Zustandserkennung ▪ Verbesserung der Prädiktion ▪ Instandhaltungsempfehlungen	▪ F&E-Kosten der Entwicklung neuer Algorithmen/Modelle ▪ Personalbeschaffungskosten- und Qualifizierungskosten (Bahnkenntnisse)	▪ Bildung strategischer Partnerschaften mit EVU, EIU und Infrastrukturherstellern ▪ Reputationsgewinn mit funktionierenden PM-Referenzen für Sfz	▪ Reputationsrisiken bei unzureichender Güte der Fehlerdetektion und Prädiktion ▪ Fehlende Abschätzbarkeit der Mehrwerte von Analyseprodukten
Sfz-Instandhaltungsdienstleister	▪ Verkauf von Instandhaltungsdienstleistungen an die ECM ▪ Effiziente Erledigung eigener Instandhaltungsarbeiten (Vermeidung unnötiger und unnötig langer Arbeiten, z. B. für Fehlersuche)	▪ Gezieltere und schnellere Erledigung der Arbeiten durch präzisere Diagnosedaten von Fahrzeugmängeln ▪ Lerneffekte und Qualitätsverbesserungen bei den eigenen Instandhaltungsarbeiten	▪ Weiterbildungs- bzw. Schulungskosten für die richtige Dateninterpretation durch eigene Mitarbeiter ▪ Ggf. Investitionsbedarf in technische Schnittstellen zur Datenübermittlung	▪ Ggf. Vermarktung eigener präventiver Instandhaltungsarbeiten auf Basis von Sensordaten als neues Angebot	▪ Verlust menschlicher Diagnosekompetenzen durch zu starkes Verlassen auf Analysetools ▪ Ggf. Risiko, dass ECM durch Analyse-, Diagnose- und Vorhersagetools auf die eigenen spezifischen Kompetenzen verzichten kann
Aufsichtsbehörden	▪ Verbesserung des Sicherheitsniveaus im Eisenbahnbetrieb ▪ Effizienzsteigerungen Bahnbetrieb und -instandhaltung ▪ Innovations- und Wettbewerbsförderung	▪ Weniger Betriebsstörungen ▪ Ggf. bessere Kenntnisse über Zustände/Probleme der Sfz-Instandhaltung im Markt	▪ Ggf. Kosten einer Datenintegration aus verschiedenen Quellen für ein umfassendes Gesamtbild ▪ Kosten einer Datenökonomie für den Markt (und Verteilungsfrage) ▪ Ggf. Schließen marktseitiger Finanzierungslücken	▪ Ggf. verbesserte Überwachung von ECM und Instandhaltungsdienstleistern auf Basis aggregierter Zustandsdaten ▪ Diskriminierungsfreie Zusammenarbeit zwischen EIU und EVU	▪ Ermöglichung neuer Angriffspotenziale im Bereich sensibler Fahrzeugdaten ▪ Marktversagen (Nichtzustandekommen kooperativer Geschäftsmodelle) ▪ Marktverzerrungen durch Datenlecks
Prüfer/ Zertifizierer	▪ Verkauf von Prüfungs- und Zertifizierungsleistungen ▪ Gewährleistung der Sicherheit,	▪ Größere und objektivere Datengrundlage bei der Durchführung von Prüfungen und Zertifizierungen	▪ Ggf. Investitionsbedarf in technische Schnittstellen	▪ Ggf. neue Marktsegmente für Prüfdienstleistungen ▪ Mitwirkung an der Entwicklung neuer Standards	▪ Haftungsrisiken im Zusammenhang mit der Dateninterpretation ▪ Unsichere Entwicklung bzgl.

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene ...				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	Qualität, Konformität von Produkten und Prozessen	▪ Eigene Erkenntnisgewinne	▪ Schulungskosten für eigene Mitarbeiter bzgl. Sensoranwendungen		Standards und Vorschriften

Zusammenfassend lassen sich folgende Schlussfolgerungen aus der anwendungsspezifischen Stakeholderanalyse ableiten:

- Es bestehen stakeholderübergreifende **Zielkongruenzen** bei dem Use Case hinsichtlich der Vermeidung von Betriebsstörungen im Gesamtsystem Bahn und des übermäßigen Verschleißes der Sfz und der Schieneninfrastruktur
- **Potenzielle Interessenkonflikte** zwischen den Stakeholdern bestehen vor allem zwischen EVU und EIU hinsichtlich der Offenlegung bzw. Nutzung von Sfz-Daten für eigene Optimierungen sowie bezüglich der zu zahlenden Preise für die Sfz-Zustandsdetektion. Zudem haben Anbieter von Datenanalysen Interesse an der Erbringung von profitablen Analyseleistungen. EVU bzw. Sfz-Halter & ECM möchten insgesamt möglichst wenig für Instandhaltungs- und Analyseleistungen ausgeben.
- **Größter Nutznießer** des Use Cases ist das EVU bzw. der Sfz-/Wagenhalter.
- Die **wichtigsten Wertschöpfungspartner** des Use Cases sind die EIU, die Anbieter von Datenanalysen und die Betreiber von Data Spaces. Ohne den Willen und die aktive Beteiligung der EIU an einer Angebotserbringung ist der Use Case nicht umsetzbar. Anbieter von Datenanalysen werden eine wichtige Rolle spielen, da die Zusammenführung unterschiedlichster streckenseitiger Sensordaten zu einem realitätsnahen Zustandsbild der vorbeifahrenden Sfz keine triviale Aufgabe ist und spezifische Kenntnisse und Tools erfordert. Data Spaces erscheinen unabdingbar, um sicherstellen, dass sfz- bzw. flottenbezogene Sensordaten eines oder mehrerer EVU nicht in den falschen Händen (z. B. von Konkurrenten) landen.

Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant

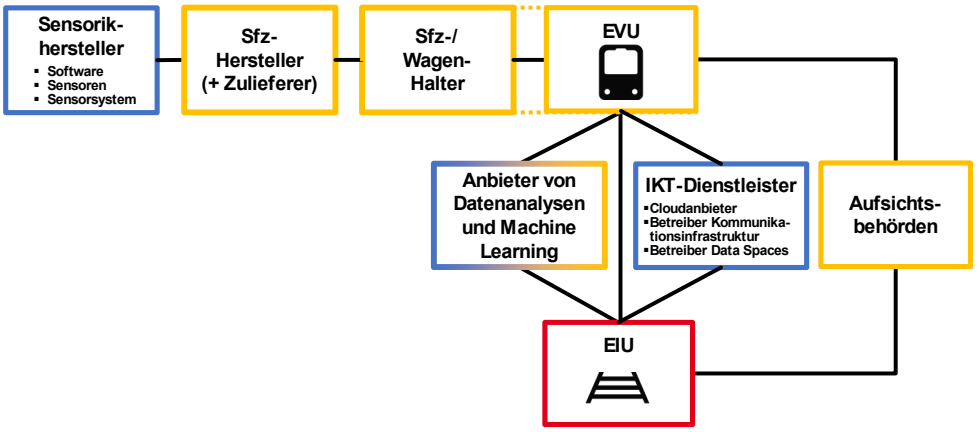


Abbildung 23: Involvierte Stakeholder im Use Case *Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant* [TU Chemnitz, BWL III]

Die zentralen Stakeholder dieser sensorbasierten Anwendung sind die EIU als Betreiber der Leit- und Sicherungstechnik sowie die EVU, die für die Analyse dieses Anwendungsfalls zur Vereinfachung und aufgrund der zusammenhängenden Interessen mit der Rolle der Sfz- bzw. Wagen-Halter zusammengefasst wurden (in Abbildung 23 gekennzeichnet durch die gestrichelte Linie). Die Sensorikhersteller (im Sinne der Sensorsystemhersteller und der dahinterliegenden Wertschöpfungskette) beliefern in diesem Use Case die Sfz-Hersteller mit der Sensortechnik zur Fahrzeuglokalisierung. Als weitere Enabler der tatsächlichen Nutzbarkeit dieser Sensorlösung agieren zum einen verschiedene IKT-Dienstleister, wel-

che das Übertragen und Bereitstellen von Lokalisierungsdaten aus dem Fahrzeug heraus an die Zentralen der EIU und der EVU ermöglichen, und zum anderen Anbieter von Datenanalysen und Machine Learning, deren Produkte und Leistungen bezüglich der Fahrzeuglokalisierung Präzisionssteigerungen, Fehlerkorrekturen, die Erkennung von Anomalien sowie Prozessautomatisierungen für weitergehende Anwendungen erlauben. Da im untersuchten Use Case die sicherheitsrelevante Fahrzeuglokalisierung im Fokus steht zählen hier auch die Aufsichtsbehörden (insbesondere das EBA) zu den primär relevanten Stakeholdern.

In Tabelle 27 sind die Ergebnisse hinsichtlich der von den primär relevanten Stakeholdern mit dem Use Case verfolgten Ziele und Interessen sowie bezüglich ihrer Einschätzungen zu Nutzen, Kosten, Chancen, Risiken des Use Case in komprimierter Form übersichtlich dargestellt.

TABELLE 27: STAKEHOLDERANALYSE FAHRZEUGLOKALISIERUNG FAHRZEUGSEITIG SICHERHEITSRELEVANT

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
EIU	▪ Verbesserung der Sicherheit auf den eigenen Strecken ▪ Minimierung von Zugverspätungen und Betriebsstörungen ▪ Künftig ggf. fortschrittliche Folgeanwendungen wie ATO	▪ Echtzeit-Überwachung von Zügen und präzisere Lokalisierung auf der Strecke ▪ Frühere Erkennung von Problemen und Störungen und Verbesserte Reaktionsfähigkeit	▪ Ggf. Implementierungskosten neuer fahrzeugseitiger Lokalisierungssysteme beim EIU ▪ Kosten für IKT-Leistungen im Betrieb ▪ Kosten für Schulung des Personals	▪ Kosteneinsparungen durch Verzicht auf streckenseitige Sensorik ▪ Steigerung der möglichen Kapazitätsauslastung der Strecken ▪ Erlössteigerung durch Möglichkeit kürzerer Streckenblöcke	▪ Unzureichende Zuverlässigkeit und Verfügbarkeit der Lokalisierung (Erfordernis von Redundanzen) ▪ Regulatorische Zulässigkeit ggf. fraglich (in Abhängigkeit von jeweiligen SIL-Anforderungen) ▪ Manipulationsmöglichkeiten
EVU, Sfz-/ Wagen-Halter	▪ Effiziente Fahrzeugdisposition und -kontrolle ▪ Sicherstellung von Pünktlichkeit und Sicherheit der Sfz ▪ Künftig ggf. fortschrittliche Folgeanwendungen wie ATO	▪ Echtzeit-Überwachung eigener Züge und präzisere Lokalisierung ▪ Bessere Planung und Optimierung des Fahrzeugeinsatzes	▪ Investitionskosten der Lokalisierungstechnik ▪ Wartung der Lokalisierungstechnik (inkl. Personalschulungen) ▪ Kosten für IKT-Leistungen im Betrieb	▪ Steigerung der Kundenzufriedenheit durch pünktliche und zuverlässige Zugdienste ▪ Wirtschaftliche Vorteile aus Folgeanwendungen wie ATO	▪ Technische Störungen oder Ausfälle der Lokalisierungssysteme ▪ Regulatorische Zulässigkeit ggf. fraglich (in Abhängigkeit von jeweiligen SIL-Anforderungen) ▪ Manipulationsmöglichkeiten
Sfz-Hersteller (+ Zulieferer)	▪ Erfüllung neuer Kundenanforderungen und -erwartungen ▪ Innovationsbedingte Wettbewerbsvorteile beim Absatz der eigenen Sfz	▪ Integration von Lokalisierungssystemen als Mehrwert für eigene Fahrzeuge ▪ Ggf. weitere Mehrwerte der Fahrzeuge durch Nutzung für komplementäre Anwendungen	▪ Beschaffungs- und Implementierungskosten für die Sensorintegration in die Sfz, inkl. Kompatibilitätssicherung mit vorhandenen Systemen ▪ Zertifizierung und Tests der neuen Technologie	▪ Abgrenzung von Wettbewerbern durch Produktinnovationen ▪ Verbesserung der Kundenbindung und langfristigen Geschäftsbeziehungen ▪ Ggf. neue Erlösquellen (Ergänzungsleistungen)	▪ Technische Herausforderungen bei der Integration ins Sfz ▪ Unsicherheit über Marktakzeptanz und Kundenbereitschaft für den Einsatz der Technologie (vs. Entwicklungsaufwand)
Sensorikhersteller	▪ Reputationsaufbau als zuverlässiger Anbieter von Lokalisierungslösungen ▪ Etablierte Bahnzulieferer: Umsatzsteigerungen für	▪ Umsatzsteigerung durch den Produktverkauf an Sfz-Hersteller ▪ Technologische Weiterentwicklung eigener Lokalisierungslösungen	▪ F&E-Kosten neuartiger Lokalisierungstechnologien ▪ Fertigungskosten bahnfester Sensoren/Sensorsysteme	▪ Steigende Nachfrage nach Lokalisierungssensoren in der Bahnindustrie (neuer Wachstumsmarkt) ▪ Möglichkeit der Technologie- o-	▪ Zu erwartende hohe Konkurrenz durch andere Sensorhersteller und möglicher Preisdruck ▪ Unsicherheit über die Zulässigkeit, Akzeptanz und

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	eigene Lokalisierungslösungen ▪ Neueinsteiger: Erschließung des Geschäftsfeldes Bahn		▪ Zertifizierung und Konformitätsbewertung der Sensoren nach den Bahnstandards	der der Kostenführerschaft bei Lokalisierungslösungen	Nachfrage nach neuen Lokalisierungssensoren in der Bahnindustrie
IKT-Dienstleister	▪ Etablierung als zuverlässige Anbieter für die sichere Übertragung und Bereitstellung von Lokalisierungsdaten ▪ Weiterentwicklung und Demonstration eigener Technologiekompetenz	▪ Weiterentwicklung eigener Plattformen und Technologien für eine bahnkonforme Übertragung sicherheitsrelevanter Lokalisierungsdaten ▪ Umsatzsteigerungen durch Datenkommunikation, Cloud- bzw. Plattformnutzung	▪ Kosten für Weiterentwicklung, Aufbau, Implementierung und Betrieb der an die Bahnwelt angepassten IKT-Infrastrukturen ▪ Kosten für die Datensicherheit (laufende Aktualisierung von Schutzsystemen)	▪ Markt- und Umsatzwachstum für Lokalisierungslösungen im Bahnsektor ▪ Weiterentwicklung der Plattformen zu verkehrssektorübergreifenden Angeboten ▪ IKT-Umsatzpotenziale für Wartung, Support und Beratung	▪ Hohe Wettbewerbsintensität im IKT-Sektor ▪ Erfüllbarkeit der SIL-Anforderungen bei der Übertragung von Lokalisierungsdaten ▪ Reputationsschäden, ggf. rechtlichen Konsequenzen bei unzureichender Datensicherheit
Anbieter von Datenanalysen/Machine Learning	▪ Erschließung des Geschäftsfelds Bahn mit neuen Analyseprodukten, insb. mit komplexeren Folgeanwendungen ▪ Zugriff auf Realdaten zur Produktentwicklung	▪ Umsatzsteigerung durch Verkauf von Datenanalyse-Dienstleistungen ▪ Weiterentwicklung von ML-Algorithmen auf Basis bahnspezifischer Anwendungen	▪ F&E-Kosten der Entwicklung neuer Algorithmen/Modelle ▪ Personalbeschaffungskosten- und Qualifizierungskosten (Bahnkenntnisse)	▪ Wachsender Markt für weitergehende datenbasierte Lösungen im Bahnsektor ▪ Aufbau strategischer Partnerschaften mit EIU und EVU	▪ Fehlende Abschätzbarkeit der Mehrwerte von Analyseprodukten für die Lokalisierung ▪ Reputationsrisiken bei unzureichender Güte der Analysen
Aufsichtsbehörden	▪ Verbesserung des Sicherheitsniveaus im Eisenbahnbetrieb ▪ Effizienzsteigerungen Bahnbetrieb (insb. höhere Streckenkapazitäten) ▪ Innovations- und Wettbewerbsförderung	▪ Verbesserung der Sicherheit und Verfügbarkeit des Bahnbetriebs durch präzise Lokalisierungsdaten ▪ Förderung von auf Lokalisierung aufbauenden Folgeanwendungen mit hohen gesellschaftlichen Mehrwerten	▪ Überprüfung und Zulassung neuer Lokalisierungssysteme nach den gesetzlichen Vorgaben ▪ Schulung und Qualifizierung des Personals hierfür ▪ Ggf. Schließen marktseitiger Finanzierungslücken	▪ Verbesserung der Sicherheit und Effizienz des Systems Bahn insgesamt ▪ Eröffnung von Innovationspotenzialen diverser, weiterer Folgeanwendungen	▪ Ermöglichung neuer Angriffspotenziale im sicherheitsrelevanten Bereich ▪ Unzureichende Beurteilbarkeit der Einhaltung von Sicherheitsanforderungen ▪ Ungewisser Ausgang von Zulassungsprozessen

Zusammenfassend lassen sich folgende Schlussfolgerungen aus der anwendungsspezifischen Stakeholderanalyse ableiten:

- Es bestehen stakeholderübergreifende **Zielkongruenzen** bei dem Use Case hinsichtlich eines gemeinsam verfolgten Innovationsschubs für das System Bahn insgesamt. Die sicherheitsrelevante Fahrzeuglokalisierung stellt hierbei eine wichtige Basisanwendung für viele weitere neuartige Use Cases, insbesondere im Bereich der Automatic Train Operation (ATO) dar.
- **Potenzielle Interessenkonflikte** zwischen den Stakeholdern bestehen vor allem hinsichtlich der Frage, welcher bzw. welche Stakeholder die Implementierungskosten der Fahrzeuglokalisierungssysteme in welchem Umfang zu tragen haben sowie bezüglich der gegebenenfalls notwendig werdenden Regulierungsbedarfe.
- **Größter Nutznießer** des Use Cases ist das EIU.
- Die **wichtigsten Wertschöpfungspartner** des Use Cases sind die Sensorsystemhersteller der Lokalisierungslösungen, die Betreiber der Kommunikationsinfrastrukturen, über welche Lokalisie-

rungsdaten übertragen werden, die EVU, deren Fahrzeuge lokalisiert werden, und die Aufsichtsbehörden, welche die Rahmenbedingungen für die Nutzbarkeit neuartiger fahrzeugseitiger Lokalisierungssysteme setzen.

Fahrzeug überwacht Oberbau

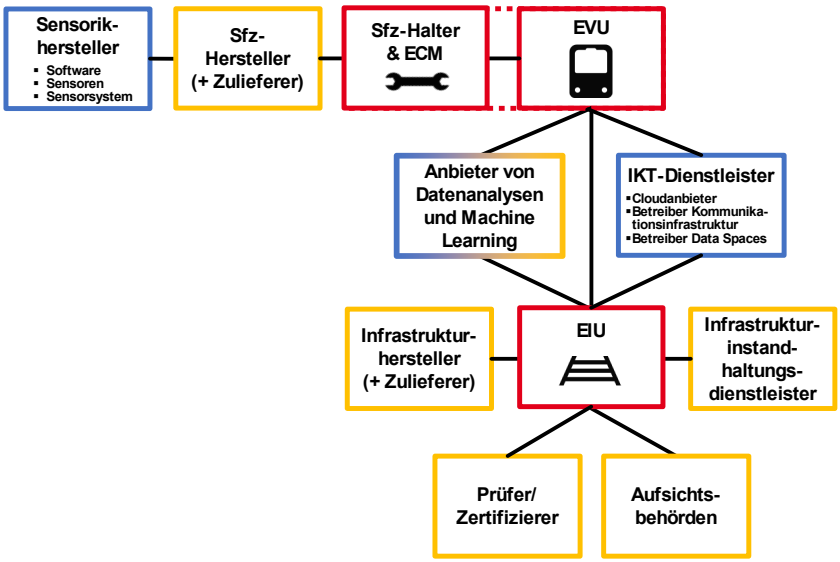


Abbildung 24: Involvierte Stakeholder im Use Case *Fahrzeug überwacht Oberbau* [TU Chemnitz, BWL III]

Die zentralen Stakeholder dieser sensorbasierten Anwendung sind zum einen die EIU, deren Gleiskörper auf ihren Bahnstrecken hinsichtlich des Infrastrukturzustandes untersucht werden, und zum anderen die Betreiber von Schienenfahrzeugen, welche die Zustandsdaten des Oberbaus beim Befahren erfassen und anschließend den EIU bereitstellen. Bei letzteren werden für die Analyse dieses Anwendungsfalls zur Vereinfachung und aufgrund der zusammenhängenden Interessen die Stakeholderrollen EVU, Sfz-Halter und ECM zusammengefasst (in Abbildung 24 gekennzeichnet durch die gestrichelte Linie). Ein primärer Anwendungszweck ist im vorliegenden Fall die zustandsorientierte Instandhaltung von Komponenten des Gleiskörpers (Schienen, Schwellen, Bettung etc.). Für eine solche spielen neben der direkten Anwenderrolle des EIU auch weitere Infrastrukturinstandhaltungsdienstleister, die Infrastrukturhersteller (bzw. Zulieferer entsprechender Infrastrukturkomponenten), die Aufsichtsbehörden (insbesondere das EBA) sowie akkreditierte, unabhängige Prüferinnen und Prüfer und Zertifiziererinnen und Zertifizierer eine wesentliche Rolle als indirekte Anwenderinnen und Anwender dieser Sensoranwendung. Die Sensorikhersteller (im Sinne der Sensorsystemhersteller und der dahinterliegenden Wertschöpfungskette) beliefern in diesem Use Case die Sfz-Hersteller (bzw. Zulieferer entsprechender Fahrzeugkomponenten wie Fahrwerk und Radsätze) mit der fahrzeugseitig zu integrierenden Sensortechnik. Als wichtige Enabler der tatsächlichen Nutzbarkeit dieser Sensorlösung agieren wieder verschiedene IKT-Dienstleister, welche das Übertragen und Bereitstellen von fahrzeugseitig erhobenen Sensordaten über den Infrastrukturzustand an die EIU und ggf. weitere Adressaten ermöglichen sowie Anbieter von Datenanalysen und Machine Learning, durch deren Produkte und Leistungen die große Menge und Vielfalt gesammelter Sensor(roh)daten erst interpretier- und verstehbar wird.

In Tabelle 28 sind die Ergebnisse hinsichtlich der von den primär relevanten Stakeholdern mit dem Use Case verfolgten Ziele und Interessen sowie bezüglich ihrer Einschätzungen zu Nutzen, Kosten, Chancen, Risiken des Use Case in komprimierter Form übersichtlich dargestellt.

TABELLE 28: STAKEHOLDERANALYSE FAHRZEUG ÜBERWACHT OBERBAU

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene ...				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
EIU	▪ Gewährleistung der Sicherheit und Zuverlässigkeit des Bahnbetriebs ▪ Frühzeitige Erkennung von Schäden und Verschleiß im Schienenoberbau ▪ Optimierung der Instandhaltungsprozesse und Reduzierung von Ausfallzeiten	▪ Minimierung von Ausfallzeiten und Reduzierung von Instandhaltungskosten mit Früherkennung und zustandsbasierter Instandhaltung ▪ Vermeidung von Folgeschäden ▪ Nutzung sensorbasierter Detektion ohne eigene Investitionen in Sensortechnik	▪ An EVU zu zahlender Entgelte für Zustandsdetektion des Oberbaus ▪ Kosten für richtige Interpretation der Sensordaten: ▪ Mitarbeiterschulungen ▪ Leistungen von Datenanalysten	▪ Kontinuierliche Überwachung des Oberbaus mit schnelleren Reaktionsmöglichkeiten ▪ Wirtschaftliche Vorteile fahrzeugseitiger Detektion (Verzicht auf Streckensensorik) ▪ teilweise Umstellung auf Condition-Based (CBM) /Predictive Maintenance (PM)	▪ Fehlende/zu teure Angebote von Seiten der EVU ▪ Ungewollter Datenabfluss über eigene Infrastrukturzustand ▪ Neue Abhängigkeiten durch fehlende eigene Kompetenzen und Sensortechnik ▪ Regulatorische Zulässigkeit von CBM/PM fraglich
EVU, Sfz-/ Halter & ECM	▪ Gewährleistung der Sicherheit und Zuverlässigkeit des Bahnbetriebs ▪ Reduzierung von Schäden an Sfz und Verlängerung ihrer Lebensdauer ▪ Minimierung von Betriebsstörungen und Ausfallzeiten	▪ Kein direkter Nutzen! ▪ Ggf. indirekter Nutzen durch Vermeidung von Sfz-Schäden durch Oberbauschäden ▪ Möglichkeit der Erweiterung des bestehenden Geschäftsfeldes/ neue Erlösquellen	▪ Investitionskosten in die gesamte Sensortechnik ▪ Betriebskosten der Sensortechnik ▪ Kosten der Qualifizierung eigenen Personals bzw. Kosten von Datenauswertungen durch Dritte	▪ Kompetenzgewinn ▪ Aufbau eines profitablen neuen Geschäftsfeldes gegenüber den EIU ▪ Nutzung von ggf. ohnehin für eigene Anwendungen vorgehaltener Fahrzeugsensorik	▪ Technische Herausforderungen bei der Interpretation der Infrastrukturdaten ▪ Unklarheit über tatsächliche Nachfrage von Seiten der EIU
Sfz-Hersteller (+ Zulieferer)	▪ Innovationsbedingte Wettbewerbsvorteile beim Absatz der eigenen Sfz ▪ Vermarktung höherwertigerer und teurerer Sfz	▪ Zusatzerlöse durch Integration von Sensortechnik ▪ Ggf. zusätzliche Mehrwerte eigener Sfz durch Nutzbarkeit für fahrzeugseitige Anwendungen	▪ Beschaffungs-/ Implementierungskosten für die Sensorintegration in die Sfz ▪ Zertifizierung und Tests der neuen Technologien ▪ Bei eigenen Diagnose- und Prädiktionsprodukten: Systementwicklungs- und Systembetreuungskosten	▪ Abgrenzung von Wettbewerbern durch Produktinnovationen ▪ Profitabler Absatz integrierter Sensorlösungen ▪ Ggf. profitable Wartungsleistungen für die Sensorik	▪ Risiko versunkener Entwicklungskosten in nicht nachgefragte Produkte ▪ Gewährleistungsrisiken und Imageschäden bei Fehlfunktionen oder Unzuverlässigkeit der Systeme
Sensorikhersteller	▪ Weiterentwicklung bzw. Erweiterung des Produktprogramms für neue fahrzeugseitige Sensoranwendungen ▪ Etablierte Bahnzulieferer: Umsatzsteigerungen für eigene Sensorprodukte ▪ Neueinsteiger: Erschließung des Geschäftsfeldes Bahn	▪ Funktions- und Qualitätsverbesserung der eigenen Sensor- und Datenfusionslösungen mit Daten aus dem Betrieb ▪ Etablierung als renommierter Lieferant für fahrzeugseitige Sensorlösungen gegenüber den Sfz-Herstellern und EVU	▪ F&E-Kosten neuartiger Sensoren/Sensorsysteme ▪ Fertigungskosten bahnfester Sensoren/Sensorsysteme	▪ Diversifikation des Produktportfolios mit stakeholderübergreifenden Sensoranwendungen im Bahnsektor ▪ Erreichen von Technologieführerschaft ▪ Ggf. wirtschaftlich vorteilhaftes Alternativangebot zu streckenseitiger Detektion	▪ Hohe Entwicklungskosten für spezialisierte Bahnanwendungen bei Unklarheit über tatsächliche Nachfrage ▪ Reputationsrisiken bei fehlerhaften Neuentwicklungen
IKT-Dienstleister	▪ Etablierung als zuverlässige Anbieter für die sichere,	▪ Weiterentwicklung von Cloud-Plattformen und Data Spaces für	▪ Kosten für Weiterentwicklung, Aufbau, Implementierung und	▪ Bildung strategischer Partnerschaften mit EIU und EVU	▪ Reputationsschäden, ggf. rechtlichen Konsequen-

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	stakeholderübergreifende Bereitstellung sensorbasierter Daten im Bahnsektor ▪ Weiterentwicklung und Demonstration eigener Technologiekompetenz	bahnkonforme Lösungen ▪ Umsatzsteigerungen durch Datenkommunikation, Cloud- bzw. Plattformnutzung	Betrieb der IKT-Infrastrukturen ▪ Kosten für die Datensicherheit (laufende Aktualisierung von Schutzsystemen)	▪ Absatz ergänzender Beratungsleistungen ▪ Weiterentwicklung zu domänenübergreifenden Angeboten/Geschäftsmodellen	zen bei unzureichender Datensicherheit ▪ Schnelllebigkeit von Technologien und hohe Wettbewerbsintensität im IKT-Sektor
Anbieter von Datenanalysen/Machine Learning	▪ Erschließung des Geschäftsfelds Bahn mit neuen stakeholderübergreifenden Analyseprodukten ▪ Zugriff auf Realdaten zur Produktentwicklung ▪ Ausbau technologischer Kompetenz	Entwicklungsmöglichkeiten für Analysealgorithmen und ML-Modelle: ▪ Güte der Zustandserkennung ▪ Verbesserung der Prädiktion ▪ Instandhaltungsempfehlungen für EIU	▪ F&E-Kosten der Entwicklung neuer Algorithmen/Modelle ▪ Personalbeschaffungskosten- und Qualifizierungskosten (Bahnkenntnisse)	▪ Bildung strategischer Partnerschaften mit EVU, EIU und Sfz-Herstellern ▪ Reputationsgewinn mit funktionierenden PM-Referenzen für den Oberbau	▪ Reputationsrisiken bei unzureichender Güte der Fehlerdetektion und Prädiktion ▪ Fehlende Abschätzbarkeit der tatsächlichen Mehrwerte von Analyseprodukten
Infrastrukturhersteller (+ Zulieferer)	▪ Absatz von Infrastrukturprodukten für den Oberbau an die EIU ▪ Erfüllung neuer Kundenanforderungen und -erwartungen	▪ Kein direkter Nutzen! ▪ Kundenbindung von EIU durch Mitwirkung an innovativen Instandhaltungsprozessen	▪ Keine direkten Kosten ▪ Ggf. Investitionsbedarf in technische Schnittstellen	▪ Erkenntnisgewinne für die Verbesserung der eigenen Infrastrukturprodukte	▪ Risiko der teilweisen Substitution des Bestandsgeschäftes durch zustandsbasierte Instandhaltung ▪ Risiko des besseren Erkennens systematischer Mängel eigener Produkte
Infrastrukturinstandhaltungsdienstleister	▪ Verkauf von Instandhaltungsdienstleistungen für den Oberbau an die EIU ▪ Erfüllung neuer Kundenanforderungen und -erwartungen	▪ Gezieltere und schnellere Erledigung der Arbeiten durch präzisere Diagnosedaten über Oberbaumängel ▪ Lerneffekte und Qualitätsverbesserungen bei den eigenen Instandhaltungsarbeiten	▪ Weiterbildungs- bzw. Schulungskosten für die richtige Dateninterpretation durch eigene Mitarbeiterinnen und Mitarbeiter ▪ Ggf. Investitionsbedarf in technische Schnittstellen zur Datenübermittlung	▪ Ggf. Vermarktung eigener präventiver Instandhaltungsarbeiten auf Basis von Sensordaten als neues Angebot	▪ Ggf. Verlust menschlicher Diagnosekompetenzen durch zu starkes Verlassen auf Analysetools ▪ Ggf. Substitutionsrisiko eigener Leistungen, wenn EIU Analyse- und Vorhersagetools nutzt
Prüfer/ Zertifizierer	▪ Verkauf von Prüfungs- und Zertifizierungsleistungen ▪ Gewährleistung der Sicherheit, Qualität, Konformität von Produkten und Prozessen	▪ Größere und objektivere Datengrundlage bei der Durchführung von Prüfungen und Zertifizierungen ▪ Eigene Erkenntnisgewinne	▪ Ggf. Investitionsbedarf in technische Schnittstellen ▪ Schulungskosten für eigene Mitarbeiterinnen und Mitarbeiter bzgl. Sensoranwendungen	▪ Ggf. neue Marktsegmente für Prüfdienstleistungen ▪ Mitwirkung an der Entwicklung neuer Standards	▪ Haftungsrisiken im Zusammenhang mit der Dateninterpretation ▪ Unsichere Entwicklung bzgl. Standards und Vorschriften
Aufsichtsbehörden	▪ Verbesserung des Sicherheitsniveaus im Eisenbahnbetrieb ▪ Effizienzsteigerungen Bahnbetrieb und -instandhaltung ▪ Innovations- und Wettbewerbsförderung	▪ Weniger Betriebsstörungen durch Infrastrukturmängel ▪ Ggf. bessere Kenntnisse über Zustände/Probleme der Oberbau-Instandhaltung im Markt	▪ Ggf. Kosten einer Datenintegration aus verschiedenen Quellen für ein umfassendes Gesamtbild ▪ Kosten einer Datenökonomie für den Markt (und Verteilungsfrage)	▪ Ggf. verbesserte Überwachung von EIU und Instandhaltungsdienstleistern auf Basis aggregierter Zustandsdaten ▪ Diskriminierungsfreie Zusammenarbeit zwischen EIU und EVU	▪ Marktversagen (Nichtzustandekommen kooperativer Geschäftsmodelle) ▪ Marktverzerrungen durch Datenlecks

Zusammenfassend lassen sich folgende Schlussfolgerungen aus der anwendungsspezifischen Stakeholderanalyse ableiten:

- Es bestehen stakeholderübergreifende **Zielkongruenzen** bei dem Use Case hinsichtlich der Erhöhung der Betriebssicherheit und der effizienteren Instandhaltung der Bahnstrecken.
- **Potenzielle Interessenkonflikte** zwischen den Stakeholdern bestehen vor allem zwischen EIU und EVU hinsichtlich der Preise der Überwachungsleistung. Zudem haben Anbieter von Datenanalysen Interesse an der Erbringung von profitablen Analyseleistungen. EIU möchten insgesamt möglichst wenig für Instandhaltungs- und Analyseleistungen ausgeben.
- **Größter Nutznießer** des Use Cases ist das EIU.
- Die **wichtigsten Wertschöpfungspartner** des Use Cases sind die EVU, die Sensorsystemhersteller bzw. Sfz-Hersteller, die Anbieter von Datenanalysen und die Betreiber von Data Spaces. Ohne den Willen und die aktive Beteiligung der EVU an einer Angebotserbringung ist der Use Case nicht umsetzbar. Auch die Sensorsystem- und Sfz-Hersteller müssen an der Entwicklung und Implementierung entsprechender fahrzeugseitiger Systeme aktiv mitwirken. Anbieter von Datenanalysen werden eine wichtige Rolle spielen, da die Zusammenführung unterschiedlichster fahrzeugseitiger Sensordaten zu einem realitätsnahen Zustandsbild des Oberbaus der befahrenen Bahnstrecken keine triviale Aufgabe ist und spezifische Kenntnisse und Tools erfordert. Data Spaces erscheinen unabdingbar, um sicherstellen, dass infrastrukturbezogene Sensordaten eines oder mehrerer EIU nicht in den falschen Händen (z. B. von potenziellen Angreiferinnen oder Angreifern auf kritische Infrastrukturen) landen.

Weichenferndiagnose

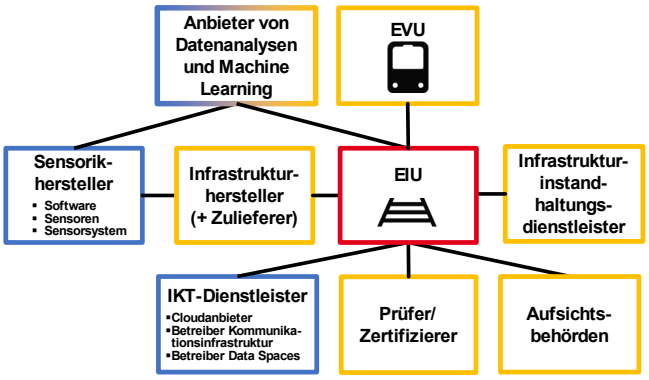


Abbildung 25: Involvierte Stakeholder im Use Case *Weichenferndiagnose* [TU Chemnitz, BWL III]

Zentraler Stakeholder dieser sensorbasierten Anwendung ist das EIU, dessen Weichen hinsichtlich ihres Zustandes und möglicherweise bestehender Instandhaltungsbedarfe untersucht werden. Sekundäre Nutznießer können die EVU sein, wenn sie bspw. Informationen über reduzierte zulässige Geschwindigkeiten an wartungsbedürftigen Weichen erhalten. Für die auf Basis der Sensordaten ausgelösten Instandhaltungsprozesse sind neben den EIU als direkte Anwender auch ggf. in Anspruch genommene weitere Infrastrukturinstandhaltungsdienstleister, die Infrastrukturhersteller (hier konkret Weichenhersteller und Zulieferer entsprechender Weichenkomponenten), die Aufsichtsbehörden (insbesondere das EBA) sowie akkreditierte, unabhängige Prüferinnen und Prüfer sowie Zertifiziererinnen und Zertifizierer als indirekte Anwenderinnen und Anwender von Bedeutung. Die Sensorikhersteller (im Sinne der Sensorsystemhersteller und der dahinterliegenden Wertschöpfungskette) beliefern in diesem Use Case die Weichen- bzw. Weichenkomponentenhersteller mit der zu integrierenden Sensortechnik. Als wichtige Enabler der tatsächlichen Nutzbarkeit dieser Sensorlösung agieren wieder verschiedene IKT-Dienstleister, welche das Übertragen und Bereitstellen von infrastrukturseitig erhobenen Sensordaten über den

Weichenzustand an die EIU (und ggf. weitere Adressaten) ermöglichen sowie Anbieter von Datenanalysen und Machine Learning, durch deren Produkte und Leistungen die Menge und Vielfalt gesammelter Sensor(roh)daten erst interpretier- und verstehbar wird.

In Tabelle 29 sind die Ergebnisse hinsichtlich der von den primär relevanten Stakeholdern mit dem Use Case verfolgten Ziele und Interessen sowie bezüglich ihrer Einschätzungen zu Nutzen, Kosten, Chancen, Risiken des Use Case in komprimierter Form übersichtlich dargestellt.

TABELLE 29: STAKEHOLDERANALYSE WEICHENFERNDIAGNOSE

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
EIU	▪ Gewährleistung der Sicherheit und Zuverlässigkeit des Bahnbetriebs ▪ Frühzeitige Erkennung von Schäden und Verschleiß an Weichen ▪ Optimierung der Instandhaltungsprozesse und Reduzierung von Ausfallzeiten	▪ Minimierung von Ausfallzeiten und Reduzierung von Instandhaltungskosten mit Früherkennung und zustandsbasierter Instandhaltung ▪ Vermeidung von Folgeschäden	▪ Investitionskosten der Sensortechnik ▪ Betriebskosten der Sensortechnik ▪ Kosten der Qualifizierung eigenen Personals bzw. Kosten von Datenauswertungen durch Dritte	▪ Kontinuierliche Überwachung der Weichen mit schnelleren Reaktionsmöglichkeiten ▪ Teilweise Umstellung auf Condition-Based (CBM) /Predictive Maintenance (PM)	▪ Manipulationsmöglichkeiten durch Angreifer ▪ Möglicherweise fehlende Wirtschaftlichkeit des Sensoreinsatzes ▪ Regulatorische Zulässigkeit von CBM/PM fraglich
EVU	▪ Gewährleistung der Sicherheit und Zuverlässigkeit des Bahnbetriebs ▪ Reduzierung von Schäden an Sfz	▪ Kein direkter bzw. unmittelbarer Nutzen! ▪ Ggf. Vorabinformationen über den Zustand befahrener Weichen	▪ Keine direkten Kosten ▪ Ggf. Kostenweitergabe an EVU über Trassenpreise	▪ Ggf. Vermeidung von Unfällen aufgrund schadhafter Weichen	▪ Keine unmittelbaren Risiken
Infrastrukturhersteller (+ Zulieferer)	▪ Vermarktung höherwertigerer und teurerer Infrastrukturprodukte für Weichen an die EIU ▪ Produktverbesserung der Weichen	▪ Zusatzerlöse durch Integration von Sensortechnik bzw. Verkauf entsprechender Komplettlösungen ▪ Kundenbindung von EIU für entsprechende Spezialösungen ▪	▪ Beschaffungs- und Implementierungskosten für die Sensorintegration ▪ Bei eigenen Überwachungs-, Diagnose- und Prädiktionsprodukten: Systementwicklungs- und Systembetreuungskosten	▪ Abgrenzung von Wettbewerbern durch Produktinnovationen ▪ Profitabler Absatz integrierter Sensorlösungen ▪ Ggf. profitable Wartungsleistungen für Sensorik ▪ Nutzung von Sensordaten zur Qualitätsverbesserung der Weichen	▪ Risiko der teilweisen Substitution des Bestandsgeschäftes durch zustandsbasierte Instandhaltung ▪ Risiko des besseren Erkennens systematischer Mängel eigener Produkte
Sensorikhersteller	▪ Weiterentwicklung bzw. Erweiterung des Produktprogramms für neue stationäre Sensoranwendungen ▪ Etablierte Bahnzulieferer: Umsatzsteigerungen für eigene Sensorprodukte ▪ Neueinsteiger: Erschließung des Geschäftsfeldes Bahn	▪ Funktions- und Qualitätsverbesserung der eigenen Sensor- und Datenfusionslösungen mit Daten aus dem Betrieb ▪ Etablierung als renommierter Lieferant für stationäre Sensorlösungen gegenüber den Infrastrukturherstellern und EIU	▪ F&E-Kosten neuartiger Sensoren/Sensorsysteme ▪ Fertigungskosten bahnfester Sensoren/Sensorsysteme	▪ Diversifikation des Produktportfolios mit nachgefragten neuen Sensoranwendungen im Bahnsektor ▪ Erreichen von Technologie- oder Kostenführerschaft	▪ Hohe Entwicklungskosten für spezialisierte Bahnanwendungen bei Unklarheit über tatsächliche Nachfrage ▪ Reputationsrisiken bei fehlerhaften Neuentwicklungen
IKT-Dienstleister	▪ Etablierung als zuverlässige Anbieter für die sichere Übertragung und	▪ Weiterentwicklung von Cloud-Plattformen und Data Spaces für	▪ Kosten für Weiterentwicklung, Aufbau, Implementierung und	▪ Bildung strategischer Partnerschaften mit EIU	▪ Reputationsschäden, ggf. rechtlichen Konsequen-

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	Bereitstellung sensorbasierter Daten im Bahnsektor ▪ Weiterentwicklung und Demonstration eigener Technologiekompetenz	bahnkonforme Lösungen ▪ Umsatzsteigerungen durch Datenkommunikation, Cloud- bzw. Plattformnutzung	Betrieb der IKT-Infrastrukturen ▪ Kosten für die Datensicherheit (laufende Aktualisierung von Schutzsystemen)	▪ Weiterentwicklung zu domänenübergreifenden Angeboten/Geschäftsmodellen	zen bei unzureichender Datensicherheit ▪ Hohe Wettbewerbsintensität im IKT-Sektor
Anbieter von Datenanalysen/Machine Learning	▪ Erschließung des Geschäftsfelds Bahn mit neuen Analyseprodukten ▪ Zugriff auf Realdaten zur Produktentwicklung ▪ Ausbau technologischer Kompetenz	Entwicklungsmöglichkeiten für Analysealgorithmen und ML-Modelle: ▪ Güte der Zustandserkennung ▪ Verbesserung der Prädiktion ▪ Instandhaltungsempfehlungen	▪ F&E-Kosten der Entwicklung neuer Algorithmen/Modelle ▪ Personalbeschaffungskosten- und Qualifizierungskosten (Bahnkenntnisse)	▪ Bildung strategischer Partnerschaften mit EIU und Infrastrukturherstellern ▪ Reputationsgewinn mit funktionierenden PM-Referenzen für Weichen	▪ Reputationsrisiken bei unzureichender Güte der Fehlerdetektion und Prädiktion ▪ Fehlende Abschätzbarkeit der Mehrwerte von Analyseprodukten
Infrastrukturinstandhaltungsdienstleister	▪ Verkauf von Instandhaltungsdienstleistungen für Weichen an die EIU ▪ Erfüllung neuer Kundenanforderungen und -erwartungen	▪ Gezieltere und schnellere Erledigung der Arbeiten durch präzise Weichendiagnosedaten ▪ Lerneffekte und Qualitätsverbesserungen	▪ Schulungskosten für die richtige Dateninterpretation durch eigene Mitarbeiterinnen und Mitarbeiter ▪ Ggf. Investitionsbedarf in technische Schnittstellen zur Datenübermittlung	▪ Ggf. Vermarktung eigener präventiver Instandhaltungsarbeiten auf Basis von Sensordaten als neues Angebot	▪ Ggf. Verlust menschlicher Diagnosekompetenzen ▪ Ggf. Substitutionsrisiko eigener Leistungen, wenn EIU Analyse- und Vorhersagetools nutzt
Prüfer/ Zertifizierer	▪ Verkauf von Prüfungs- und Zertifizierungsleistungen ▪ Gewährleistung der Sicherheit, Qualität, Konformität von Produkten und Prozessen	▪ Bessere Datengrundlage bei der Durchführung von Prüfungen und Zertifizierungen ▪ Eigene Erkenntnisgewinne	▪ Ggf. Investitionsbedarf in technische Schnittstellen ▪ Schulungskosten für eigene Mitarbeiter bzgl. Sensoranwendungen	▪ Ggf. neue Marktsegmente für Prüfdienstleistungen ▪ Mitwirkung an der Entwicklung neuer Standards	▪ Haftungsrisiken im Zusammenhang mit der Dateninterpretation ▪ Unsichere Entwicklung bzgl. Standards und Vorschriften
Aufsichtsbehörden	▪ Verbesserung des Sicherheitsniveaus im Eisenbahnbetrieb ▪ Effizienzsteigerungen Bahnbetrieb und -instandhaltung	▪ Weniger Betriebsstörungen durch frühzeitige Problemerkennung ▪ Datenbasis für Entscheidungen zur Infrastrukturverbesserung	▪ Kosten einer Datenökonomie für den Markt (und Verteilungsfrage)	▪ Ggf. verbesserte Überwachung von EIU und Instandhaltungsdienstleistern	▪ Ermöglichung neuer Angriffspotenziale im Bereich sensibler Infrastrukturelemente

Zusammenfassend lassen sich folgende Schlussfolgerungen aus der anwendungsspezifischen Stakeholderanalyse ableiten:

- Es bestehen stakeholderübergreifende **Zielkongruenzen** bei dem Use Case hinsichtlich der Erhöhung der Betriebssicherheit und einer besseren Instandhaltungsplanung und -durchführung für Weichen.
- **Potenzielle Interessenkonflikte** zwischen den Stakeholdern bestehen vor allem zwischen EIU und Infrastrukturherstellern (bzw. auch Sensorikherstellern und Anbietern von Datenanalysen/Machine Learning) hinsichtlich der Preise von Ferndiagnosesystemen und ergänzender Dienstleistungen sowie zwischen EIU und Infrastrukturherstellern bezüglich des Anstrebens planmäßig-vorbeugender Instandhaltung. EIU möchten mit prädiktiven Instandhaltungsstrategien Kosten sparen, wohingegen Infrastrukturhersteller Interesse an einer zeitbezogenen Instandhaltung im Sinne eines planbaren und regelmäßig wiederkehrenden Produktabsatzes haben.
- **Größter Nutznießer** des Use Cases ist das EIU.

- Die **wichtigsten Wertschöpfungspartner** des Use Cases sind die Sensorsystemhersteller, die Weichenhersteller und die Anbieter von Datenanalysen.

(Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)

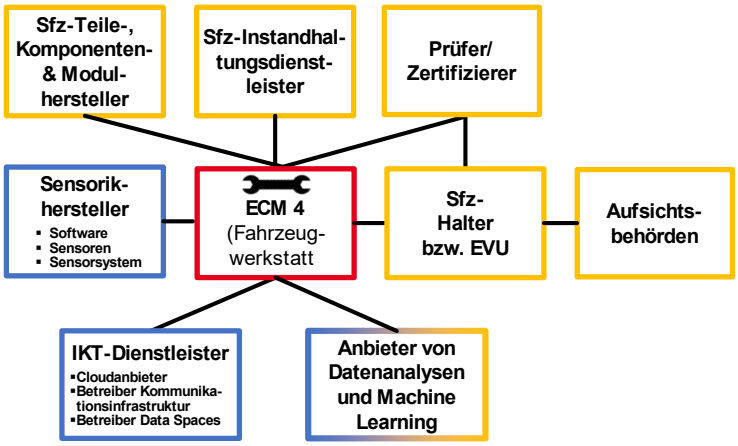


Abbildung 26: Involvierte Stakeholder im Use Case *(Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)* [TU Chemnitz, BWL III]

Zentraler Stakeholder dieser sensorbasierten Anwendung ist die Fahrzeugwerkstatt in der ECM4-Rolle, welche für die Erbringung der Instandhaltungsleistungen inklusive Befundung und Dokumentation verantwortlich ist. Sie wird in diesem Use Case von den Sensorikherstellern (im Sinne der Sensorsystemhersteller und der dahinterliegenden Wertschöpfungskette) mit der stationär zu integrierenden Sensortechnik ausgestattet. Die Sfz-Halter bzw. EVU als Kunden der ECM profitieren indirekt von der automatisierten Schadenerkennung. Weitere indirekte Anwenderinnen und Anwender dieser Sensoranwendung sind die im Zuge der ausgelösten Instandhaltungsprozesse involvierten Teile-, Komponenten- und Modulhersteller von Schienenfahrzeugen (als Lieferanten von Ersatzteilen), ggf. in Anspruch genommene Sfz-Instandhaltungsdienstleister (z. B. mit spezialisierten Leistungen für Fahrwerke, Karosserien oder Scheiben), die Aufsichtsbehörden (insbesondere das EBA) sowie akkreditierte, unabhängige Prüferinnen und Prüfer und Zertifiziererinnen und Zertifizierer. Als wichtige Enabler der tatsächlichen Nutzbarkeit dieser Sensorlösung agieren wieder verschiedene IKT-Dienstleister, welche das Übertragen und Bereitstellen der erhobenen Sensordaten über den Fahrzeugzustand an die ECM (und ggf. weitere Adressaten) ermöglichen sowie Anbieter von Datenanalysen und Machine Learning, durch deren Produkte und Leistungen die große Menge und Vielfalt gesammelter Sensor(roh)daten erst interpretier- und verstehbar wird.

In Tabelle 30 sind die Ergebnisse hinsichtlich der von den primär relevanten Stakeholdern mit dem Use Case verfolgten Ziele und Interessen sowie bezüglich ihrer Einschätzungen zu Nutzen, Kosten, Chancen, Risiken des Use Case in komprimierter Form übersichtlich dargestellt.

TABELLE 30: STAKEHOLDERANALYSE (TEIL-)AUTOMATISIERUNG DER FAHRZEUGINSTANDHALTUNG (SCHADENSERKENNUNG)

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
ECM 4 (Fahrzeug-werkstatt)	▪ Effiziente Ausführung von Instandhaltungsarbeiten, insb. bezüglich des Personaleinsatzes ▪ Wirtschaftlichkeit/ Profitabilität der	▪ Beschleunigung der Schadensbefundung → Kapazitätssteigerung	▪ Investitionskosten der Sensortechnik ▪ Betriebs- und Wartungskosten der Sensortechnik	▪ Kosteneinsparungen durch weniger manuelle Befundungsarbeit ▪ Qualitätsverbesserung der Inspektionen	▪ Verlust menschlicher Diagnosekompetenzen durch zu starkes Verlassen auf Detektionstools

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	Bearbeitung von Instandhaltungsaufträgen	▪ Transparenzerhöhung durch standardisierte Erfassung ▪ Optimierung und Teilautomatisierung von Folgearbeitsprozessen	▪ Kosten der Qualifizierung eigenen Personals bzw. Kosten von Datenauswertungen durch Dritte	▪ Erringen der Kosten- und Qualitätsführerschaft für Werkstattleistungen	▪ Akzeptanzprobleme der eigenen Mitarbeiter ▪ Ggf. Akzeptanzprobleme der EVU-Kunden
Sfz-Halter/ EVU	▪ Wirtschaftlicher Betrieb der Sfz ▪ Optimierte Fahrzeuginstandhaltung	▪ Präzisere Erkennung von Sfz-Mängeln und Vermeidung von Folgeschäden ▪ Kürzere Werkstattverweilzeiten/Erhöhung der Fahrzeugverfügbarkeit	▪ Keine direkten Kosten ▪ Ggf. Kostenweitergabe über Werkstattpreise ▪ Ggf. Investitionsbedarf in technische Schnittstellen für eigene Auswertungen	▪ Ggf. Weitergabe von resultierenden Preisvorteilen der Werkstatt an Sfz-Halter/EVU	▪ Risiko des Abflusses sensibler Sfz-Flottendaten des EVU ▪ Risiko unerkannter Mängel durch zu starkes Verlassen auf Detektionstools
Sensorikhersteller	▪ Weiterentwicklung bzw. Erweiterung des Produktprogramms für neue stationäre Sensoranwendungen ▪ Etablierte Bahnzulieferer: Umsatzsteigerungen für eigene Sensorprodukte ▪ Neueinsteiger: Erschließung des Geschäftsfeldes Bahn	▪ Funktions- und Qualitätsverbesserung der eigenen Sensor- und Datenfusionslösungen mit Daten aus dem Werkstattbetrieb ▪ Etablierung als renommierter Lieferant für stationäre Sensorlösungen gegenüber den ECM bzw. EVU	▪ F&E-Kosten neuartiger Sensoren/Sensorsysteme ▪ Fertigungskosten bahnfester Sensoren/Sensorsysteme	▪ Diversifikation des Produktportfolios mit neuen Sensoranwendungen im Bahnsektor ▪ Technologieführerschaft im Werkstattsegment ▪ Übertragbarkeit von Produktverbesserungen auf bahnfremde Branchen	▪ Hohe Entwicklungskosten für spezialisierte Bahnanwendungen bei Unklarheit über tatsächliche Nachfrage ▪ Reputationsrisiken bei fehlerhaften oder unzuverlässigen Neuentwicklungen
IKT-Dienstleister	▪ Etablierung als zuverlässige Anbieter für die sichere, stakeholderübergreifende Bereitstellung sensorbasierter Daten im Bahnsektor ▪ Weiterentwicklung und Demonstration eigener Technologiekompetenz	▪ Weiterentwicklung von Cloud-Plattformen und Data Spaces für bahnkonforme Lösungen ▪ Umsatzsteigerungen durch Datenkommunikation, Cloud- bzw. Plattformnutzung	▪ Kosten für Weiterentwicklung, Aufbau, Implementierung und Betrieb der IKT-Infrastrukturen ▪ Kosten für die Datensicherheit (laufende Aktualisierung von Schutzsystemen)	▪ Diversifikation: Referenzen für bahnspezifische Produktlösungen ▪ Etablierung langfristiger neuer Kooperationen ▪ Beitrag zur Entstehung neuer Geschäftsmodelle basierend auf dem Sensordatenaustausch	▪ Reputationsschäden, ggf. rechtlichen Konsequenzen bei unzureichender Datensicherheit ▪ Schnelllebigkeit von Technologien und hohe Wettbewerbsintensität im IKT-Sektor
Anbieter von Datenanalysen/Machine Learning	▪ Erschließung des Geschäftsfelds Bahn mit neuen Analyseprodukten ▪ Zugriff auf Realdaten zur Produktentwicklung ▪ Ausbau technologischer Kompetenz	Entwicklungsmöglichkeiten für Analysealgorithmen und ML-Modelle: ▪ Güte der Zustandserkennung ▪ Verbesserung der Prädiktion ▪ Instandhaltungsempfehlungen	▪ F&E-Kosten der Entwicklung neuer Algorithmen/Modelle ▪ Personalbeschaffungskosten- und Qualifizierungskosten (Bahnkenntnisse)	▪ Bildung strategischer Partnerschaften mit ECM ▪ Reputationsgewinn mit funktionierenden Referenzen für die automatisierte Schadenserkennung an Sfz	▪ Reputationsrisiken bei unzureichender Güte der Fehlerdetektion und Prädiktion ▪ Fehlende Abschätzbarkeit der Mehrwerte von Analyseprodukten
Sfz-Teile, Komponenten- & -Modulhersteller	▪ Absatz von Ersatzteilprodukten für Sfz ▪ Qualitäts-/Produktverbesserungen an den hergestellten Teilen	▪ Kein direkter Nutzen!	▪ Keine direkten Kosten ▪ Ggf. Investitionsbedarf in technische Schnittstellen	▪ Möglichkeit der sensordatenbasierten Produktverbesserung sofern Zugang zu (anonymisierten) Daten möglich ist	▪ Risiko des besseren Erkennens systematischer Mängel eigener Produkte
Sfz-Instandhaltungsdienstleister	▪ Verkauf von Instandhaltungsdienstleistungen an die ECM	▪ Gezieltere und schnellere Erledigung der Arbeiten	▪ Schulungskosten für die richtige Dateninterpretation durch eigene	▪ Ggf. Vermarktung präventiver Instandhaltungsarbeiten auf Basis	▪ Ggf. Risiko, dass ECM durch Analyse-, Diagnose-

Stakeholder	Mit dem Use Case verfolgte bzw. verbundene …				
	Ziele/Interessen	Nutzen	Kosten	Chancen	Risiken
	▪ Effiziente Erledigung eigener Instandhaltungsarbeiten	durch präzisere Diagnosedaten n ▪ Lerneffekte und Qualitätsverbesserungen	Mitarbeiterinnen und Mitarbeiter ▪ Ggf. Investitionsbedarf in technische Schnittstellen	von Sensordaten als neues Angebot	und Vorhersagetools auf die eigenen spezifischen Kompetenzen verzichten kann
Prüfer/ Zertifizierer	▪ Verkauf von Prüfungs- und Zertifizierungsleistungen ▪ Gewährleistung der Sicherheit, Qualität, Konformität von Produkten und Prozessen	▪ Bessere Datengrundlage bei der Durchführung von Prüfungen und Zertifizierungen ▪ Eigene Erkenntnisgewinne	▪ Ggf. Investitionsbedarf in technische Schnittstellen ▪ Schulungskosten für eigene Mitarbeiterinnen und Mitarbeiter bzgl. Sensoranwendungen	▪ Ggf. neue Marktsegmente für Prüfdienstleistungen ▪ Mitwirkung an der Entwicklung neuer Standards	▪ Haftungsrisiken im Zusammenhang mit der Dateninterpretation ▪ Unsichere Entwicklung bzgl. Standards und Vorschriften
Aufsichtsbehörden	▪ Verbesserung des Sicherheitsniveaus von Sfz ▪ Effizienzsteigerungen in der Sfz-Instandhaltung ▪ Einhaltung geltender Vorschriften und Standards der Sfz-Instandhaltung	▪ genauere und frühzeitigere Erkennung von Sfz-Schäden ▪ Ggf. bessere Kenntnisse über Zustände/Probleme der Sfz-Instandhaltung im Markt	▪ Kosten einer Datenökonomie für den Markt (und Verteilungsfrage)	▪ Ggf. verbesserte Überwachung von ECM und Instandhaltungsdienstleistern auf Basis der Sensordaten	▪ Akzeptanz- und Vertrauensprobleme einer teilautomatisierten Schadensbefundung ▪ Marktverzerrungen durch Datenlecks

Zusammenfassend lassen sich folgende Schlussfolgerungen aus der anwendungsspezifischen Stakeholderanalyse ableiten:

- Es bestehen stakeholderübergreifende **Zielkongruenzen** bei dem Use Case hinsichtlich der gewünschten schnelleren und effizienteren Durchführung von Instandhaltungsarbeiten und des effektiveren Personaleinsatzes hierbei.
- **Potenzielle Interessenkonflikte** zwischen den Stakeholdern bestehen vor allem zwischen der Sfz-Werkstatt und den EVU/Sfz-Haltern bezüglich des Wertes der abrechenbaren Diagnose- und Befundungsleistungen sowie bezüglich der Offenlegung von (auch historischen) Sfz- und Sfz-Komponenten-Daten. Darüber hinaus bestehen voraussichtlich Interessenkonflikte innerhalb der Sfz-Werkstatt zwischen den Fertigungsmitarbeitern und dem Management hinsichtlich der potenziellen Änderung von Arbeitsabläufen und der Sicherung bestimmter Arten von Arbeitsplätzen im Bereich der Fahrzeugbefundung.
- **Größter Nutznießer** des Use Cases ist die ECM.
- Die **wichtigsten Wertschöpfungspartner** des Use Cases sind die Sensorsystemhersteller, die Anbieter von Datenanalysen, die Sfz-Halter (als Kunden) und Cloudanbieter.

Anwendungsübergreifende Auswertung

Bei allen sieben näher untersuchten Sensoranwendungen liegen insgesamt recht komplexe Wertschöpfungsverflechtungen und damit gegenseitige Abhängigkeiten, Einflüsse und Einflussmöglichkeiten der Stakeholder vor. Es ist davon auszugehen, dass dies auch auf die weiteren 36 Sensoranwendungen aus der Gesamtliste dieser Studie (vgl. Tabelle 2) zutrifft. Die Verflechtungen sind bereits hoch, wenn der Sensoreinsatz innerhalb einer der Anwendungsdomänen – Fahrzeug bzw. Infrastruktur – stattfindet (z. B. nur fahrzeuginterne Fahrzeugüberwachungssysteme), wenn vergleichsweise einfach und eindeutig diagnostizierbare technische Zustände erfasst und ausgewertet werden und wenn lediglich Komfort- oder Effizienzaspekte von der Anwendung berührt werden. Sie gewinnen noch einmal an Bedeutung, wenn zwischen den Domänen Fahrzeug und Infrastruktur ein Austausch (z. B. von sensorbasierten Da-

ten oder darauf aufbauenden Produkten) erfolgt, wenn anspruchsvollere und fortschrittlichere Folgeanwendungen mit den erhobenen Daten realisiert werden sollen (z. B. Fahrzeug- und diverse Prozessautomatisierungen) und wenn Sicherheitsaspekte von der Sensoranwendung berührt werden.

Infolge dieser starken Verflechtungen werden sich neue, innovative Sensoranwendungen im Bahnsystem künftig nur durchsetzen können, wenn sie aus Perspektive der verschiedenen involvierten Stakeholder (auch der rahmensetzenden wie z. B. Aufsichtsbehörden und der mittelbar betroffenen wie Fahrgäste sowie Passantinnen und Passanten) hinsichtlich der individuell wahrgenommenen Chancen und Risiken Erfolg versprechend und vertretbar sind. Für die beteiligten Marktakteure gilt zudem konkret, dass ihr Anteil an der Realisierung einer Sensoranwendung sich wirtschaftlich rechnen muss. Die Unsicherheit darüber kann einen Markteintritt und damit die Einführung einer im Grunde sinnvollen Anwendung verhindern. Basisvoraussetzungen sind insgesamt ausreichende Mehrwerte bei den Nutznießern der Anwendung, welche die Kosten des Einsatzes sensorbasierter Technologien übersteigen, sowie funktionierende Verteilungsmechanismen für die anfallenden Nutzen und Kosten zum Vorteil aller Beteiligten. In vielen Fällen müssen hierfür erst neue Geschäftsmodelle entwickelt werden.

Zielkongruenzen des Sensoreinsatzes zwischen den verschiedenen Stakeholdern bestehen in der Regel im gemeinsamen Grundinteresse, das System Bahn in seiner Gesamtheit zuverlässiger, effizienter, noch sicherer und kundenseitig attraktiver als das heutige zu gestalten. Zugleich versprechen sich die Stakeholder von bestimmten Schlüsselanwendungen wie der Fahrzeuglokalisierung Innovationsschübe für völlig neue Produkte und Geschäftsfelder, z. B. für einen künftigen automatisierten Fahrbetrieb. Interessenkonflikte betreffen meist zwei Bereiche: zum einen die Preisfindung und angestrebte bzw. zu meidende Abhängigkeiten in den Anbieter-Abnehmer-Beziehungen (bezogen auf diverse Produkte und sensorbasierte Leistungen in der Gesamtwertschöpfungskette) und zum anderen die Offenlegung eigener Daten, aus der unerwünschte Folgen resultieren können. In manchen Fällen führt der Sensoreinsatz potenziell auch zu einer – zumindest teilweisen – Substituierbarkeit der klassischen Geschäftsmodelle von Stakeholdern, z. B. im Bereich der planmäßigen, zeitorientierten Instandhaltung. Die größten direkten Nutznießer der untersuchten Sensoranwendungen wären die Eisenbahnverkehrs- und die Eisenbahninfrastrukturunternehmen. Die Bereitsteller sensorbasierter Lösungen profitieren vor allem durch Umsatzsteigerungen, den Ausbau der eigenen Produktpalette und Kompetenzgewinne. Die wichtigsten Wertschöpfungspartner variieren stark je nach Anwendung. Schlüsselrollen kommen dabei aber immer wieder den Sensorsystemherstellern, den Anbietern von Datenanalysen und den Betreibern von Data Spaces zu.

Die mit den Nutzen, Kosten, Chancen und Risiken von Sensoranwendungen im Zusammenhang stehenden Voraussetzungen für deren Umsetzbarkeit sind letztlich an die Überwindung bzw. Bewältigung von grundlegenden Innovationsbarrieren geknüpft. Diese werden im nachfolgenden Abschnitt vorgestellt.

5.3 Innovationsbarrieren

Aus der analytischen Auseinandersetzung mit den Stakeholderbeziehungen und den geführten Stakeholderinterviews (sowie den Diskussionsbeiträgen in den durchgeführten Workshops) konnte letztlich eine anwendungsübergreifende Liste von Innovationsbarrieren für Sensoranwendungen im Bahnsystem erstellt werden. In dieser findet sich auch ein großer Teil der Schlüsselherausforderungen wieder, welche eine umfassende, aktuelle Literaturstudie zu Schienenverkehrsinnovationen und Forschungen im Umfeld des Internet of Things (IoT) benennt [61]. Die Liste von Innovationsbarrieren wurde auch als Ausgangspunkt für die Ableitung von Handlungsfeldern und Maßnahmenvorschlägen in Kapitel 6.1 weitergenutzt. Der Entwurf der Liste wurde in mehreren Iterationsschritten durch das erhaltene Feedback innerhalb Projektkonsortiums und von ausgewählten Expertinnen und Experten verfeinert.

Die in Summe 24 identifizierten Innovationsbarrieren wurden folgendermaßen klassifiziert:

- sieben Barrieren wurden der Kategorie „Technologie“ zugeordnet: T1 bis T7
- vier Barrieren wurden der Kategorie „Recht“ zugeordnet: R1 bis R4
- drei Barrieren wurden der Kategorie „Standardisierung“ zugeordnet: S1 bis S3
- fünf Barrieren wurden der Kategorie „Geschäftsmodelle“ zugeordnet: G1 bis G5
- fünf Barrieren wurden der Kategorie „Markt“ zugeordnet: M1 bis M5

Diese Kategorisierung folgt in etwa der Einteilung der Umfeldbereiche in Abschnitt 5.1. Sie unterscheidet sich von dieser aber dahingehend, dass die Standardisierung als eigene Kategorie aus dem übergreifenden Feld „Recht“ und die Geschäftsmodelle als eigenständige Kategorie aus dem übergreifenden Feld „Markt“ ausgegliedert wurde. Zudem wurde den der gesellschaftlichen Sphäre zuordenbaren Barrieren keine eigene Kategorie gewidmet, da die Anzahl hierfür nicht ausreichend war und es sich im Wesentlichen um den Fachkräftemangel handelte, der schließlich der Kategorie Markt zugeordnet wurde. Im Folgenden werden die einzelnen Innovationsbarrieren kurz und knapp vorgestellt.

T1 Kompatibilität und Interoperabilität in heterogenen Bahnsystemen
Die starke Heterogenität von Bahnsystemen stellt eine Herausforderung für den Sensoreinsatz hinsichtlich der Kompatibilität und Interoperabilität dar. Die Heterogenität zeigt sich in vielen Facetten, bspw. in unterschiedlichen technischen Spezifikationen von Bahninfrastruktur, unterschiedlichen Fahrzeugtypen und Antriebsarten, unterschiedlicher Leit- und Sicherheitstechnik, verschiedenen Betreibermodellen und Tarifsystemen.

T2 Herausforderungen steigender Systemkomplexität für die Bahntauglichkeit
Das System Bahn ist ohnehin bereits sehr komplex und unterliegt einer Vielzahl von Regelwerken und Vorschriften. Mit einem verstärkten Einsatz von Sensorlösungen steigt diese Komplexität weiter, sowohl was die technischen Schnittstellen angeht als auch die Verflechtungen von Stakeholdern über verschiedene Wertschöpfungsprozesse. Darunter können wichtige Leistungsparameter wie die Instandhaltbarkeit und die Skalierbarkeit leiden.

T3 Kurze Innovationszyklen von Digitaltechnologien/lange Lebenszyklen der Bahntechnik
Bahntechnik weist typischerweise sehr lange Lebenszyklen und auch vergleichsweise größere Wartungszyklen (besonders im Güterverkehr) auf, sowohl im Bereich der Infrastruktur als auch dem der Fahrzeuge. Die sehr kurzen Innovationszyklen von Digitaltechnologien können damit unter Umständen organisatorisch-wirtschaftlich nur schwer vereinbar sein. Ihr Austausch nach bereits vergleichsweise kurzen Zeiträumen kann zu aufwendig oder zu teuer sein. Andererseits ist die Dauer des Supports bei den Versionen bzw. Generationen von Digitaltechnologien recht kurz.

T4 Technologischer Aufwand zur Wahrung von Datensicherheit und Datenschutz
Der Einsatz sensorbasierter Technologien erhöht den Aufwand, um die Datensicherheit und den Datenschutz sicherzustellen, da neue Schnittstellen und Datenflüsse hervorgerufen werden.

T5 Fehlende massenmarkttauglichen Commercial-off-the-Shelf-Produkte (COTS)
Für viele der diskutierten oder in Aussicht gestellten Sensoranwendungen im Bahnsystem existiert derzeit noch keine Standard-Hardware und -Software, die mit einer entsprechenden Massenproduktion bzw. einem entsprechend großen Absatz zu marktverträglichen Preisen angeboten werden kann. Stattdessen gibt es meist nur sehr teure Pilotumsetzungen, was einen Markthochlauf hemmt.

T6 Teilweise noch unzureichender Entwicklungsstand der Technologie
Technologien für Sensorlösungen haben in einigen speziellen Bereichen noch einen unzureichenden Entwicklungsstand. Dies betriff v. a. die Performanz, den Stromverbrauch und die Zuverlässigkeit von spezifischen Systemkomponenten und Datenaustauschschnittstellen. Gesamthaft betrachtet ist die

technologische Reife für Sensoranwendungen im Bahnsystem aber recht hoch und nicht als primäres Hindernis für die Verbreitung entsprechender Innovationen anzusehen.

T7 Teilweise noch unzureichende bzw. unzureichend identifizierte sensorbasierte Trainingsdaten
Für maschinelle Auswertungen und Interpretationen großer Datensätze in Bahnanwendungen werden ausreichend Trainingsdaten benötigt. Diese müssen häufig entweder noch erfasst bzw. erhoben werden oder sie existieren schon, aber wurden bisher nicht als solche identifiziert. Technologien für das maschinelle Lernen an sich sind zumeist vorhanden und hinreichend erprobt.

R1 Zeit- und Kostenaufwand der Bahnzulassung bzw. -zertifizierung
Die Dauer von Bahnzulassungsprozessen und die dabei anfallenden Kosten (insbesondere für Sicherheitsnachweise) stellen eine große Hürde, insbesondere für kleinere und bisher nicht im Bahnsektor aktive Unternehmen, dar.

R2 Fehlende Zulassungsfähigkeit bzw. die Ungewissheit über eine solche
Vor Beendigung des Zulassungsprozesses ist häufig nicht klar, ob die Zulassung überhaupt erfolgreich sein wird. Das Risiko der Nichtzulassung schreckt viele Unternehmen vor den erforderlichen Anstrengungen ab. Zudem gibt es Sensoranwendungen, insbesondere solche, bei denen maschinelles Lernen oder verteilte Systeme (Cloudlösungen) zur Anwendung kommen, die nach heutiger Rechtslage nicht zulassungsfähig sind.

R3 Einhaltung von Datenschutzvorschriften
Der Einsatz sensorbasierter Systeme eröffnet neue Potenziale zur beabsichtigten oder unbeabsichtigten Verletzung von Datenschutzvorschriften. Demzufolge sind verstärkte Anstrengungen zur Einhaltung der Vorschriften erforderlich.

R4 Haftungsrisiken aus Fehlfunktionen/Ausfällen
Aus Fehlfunktionen oder Ausfällen sensorbasierter Technologien können Haftungsrisiken resultieren. Eine noch nicht ausreichende Systemzuverlässigkeit oder die subjektive Wahrnehmung einer solchen kann daher als Innovationbarriere wirken.

S1 Fehlende oder konkurrierende Standards
Das Fehlen etablierter Standards, insbesondere in den Bereichen der Sensorsystemimplementierung und des Datenaustauschs, behindert Innovationen. Auch wenn konkurrierende Standards nebeneinander existieren und nicht klar ist, welcher sich am Ende durchsetzen wird, wirkt dies innovationshemmend.

S2 Dauer und Kosten der Standardisierung
Wie Zulassungsprozesse sind auch Standardisierungsprozesse häufig sehr langwierig und werden nicht selten vom technologischen Fortschritt überholt. Sie sind auch mit hohen Kosten verbunden, sodass sich meist nur große Marktplayer daran beteiligen können. Das kann dazu führen, dass viele Stakeholderinteressen beim fertigen Standard unberücksichtigt bleiben.

S3 Unzureichende Implementierbarkeit existierender Standards
Ein weiteres Problem im Bereich der Standardisierung ist, dass im Ergebnis oftmals Standards festgeschrieben werden, die an der Praxis vorbei entwickelt wurden und eine zu hohe Komplexität aufweisen, als dass sie noch implementierbar sind.

G1 Hohe Investitionsbedarfe bei schwer zu bewertender Rentabilität
Für die Umsetzung von sensorbasierten Anwendungen im Bahnsystem sind meist sehr hohe Investitionen für IT-Infrastrukturen, harmonisierte Schnittstellen, Software und Schulungen erforderlich. Hinzu kommen auch laufende Aufwendungen für die Wartung und Erneuerung der Systeme. Demgegenüber

stehen jedoch zugleich auch noch große Unsicherheiten über die generierbaren Erlöse und damit über die Rentabilität der Investitionen. Das liegt darin begründet, dass Zahlungsbereitschaften für neuartige Sensoranwendungen im Bahnsystem noch weitgehend unbekannt und schwer zu schätzen sind.

G2 Anfall von Kosten und Nutzen des Sensoreinsatzes bei unterschiedlichen Stakeholdern
Wenn die Kosten und die Nutzen des Sensoreinsatzes bei unterschiedlichen Stakeholdern anfallen und keine Klarheit darüber herrscht, dass eine entsprechende Leistung (deutlich) gewinnbringend an den Nutznießer vermarktet werden kann, so sind die Chancen des Angebots einer solchen Leistung sehr gering. Bspw. riskieren EVU eine erneute Fahrzeugzulassung, wenn sie in Sensorik zur Überwachung des Oberbaus investieren würden, ohne zu wissen, ob EIU diese Leistung überhaupt (in ausreichendem Maße) nachfragen würden.

G3 Konflikte um Verfügungsrechte an Daten
Um die Verfügungsrechte an Daten können Konflikte ausbrechen, welche Innovationen hemmen. Da im deutschen Recht kein traditionelles Eigentum an Daten existiert, sind viele Stakeholder darauf bedacht, Wissensvorsprünge und Datenzugänge mit behelfsweisen Rechtskonstruktionen zu schützen.

G4 Befürchtung des ungewünschten Abflusses sensibler oder werthaltiger Daten
Viele Unternehmen scheuen berechtigter- oder unberechtigterweise das Teilen von Daten (damit auch von sensorbasierten Daten), weil sie einen Abfluss sensibler oder werthaltiger Daten befürchten. Auch wenn sie diese Daten ggf. bisher selbst gar nicht verwerten, kann mit dem Teilen an eine evtl. sogar unbestimmte Menge an Adressaten ein empfundener Bedeutungsverlust einhergehen. Zudem wird oft eine Beeinträchtigung des bisherigen Geschäftsmodells gefürchtet.

G5 Nichtexistenz bzw. Unwirtschaftlichkeit von Migrationsstrategien
Wenn keine durchdachten und praktikablen Umsetzungsstrategien für eine Migration von Alttechnologien zu neuen sensorbasierten Technologien existieren oder wenn eine solche Migration voraussichtlich nicht wirtschaftlich ist, dann werden sich entsprechende Innovationen nicht durchsetzen.

M1 Mangel an qualifizierten Fachkräften
Der Mangel an qualifiziertem Personal, insbesondere in den Bereichen Bahntechnik, Data Sciences und speziell an der Schnittstelle zwischen beiden hemmt Innovationen. Sowohl potenziellen Anwendern als auch Anbietern sensorbasierter Bahnanwendungen fehlt es häufig an ausreichend qualifizierten Köpfen, um Innovationen voranzutreiben bzw. zu nutzen.

M2 Intra- und interorganisationale Widerstände
Widerstände innerhalb und zwischen Organisationen hemmen oftmals Innovationen, so auch im Fall sensorbasierter Technologien für das Bahnsystem. Dabei geht es zum einen um eine eher innovationsfeindliche Organisationskultur oder unzureichende Mitarbeiterakzeptanz für Veränderungen, zum anderen um negative Einstellungen zu Kooperationen und einem entsprechend ausgeprägten Marktverhalten.

M3 Wirtschaftliche Interessenkonflikte
Auch objektive wirtschaftliche Interessenkonflikte, losgelöst von den Einstellungen der Entscheidungsträger von Marktteilnehmern, können einem verstärkten Einsatz sensorbasierter Lösungen im Bahnsystem entgegenstehen. Bspw. besitzen Hersteller von Komponenten, Modulen und Systemen ein Interesse an starren Wartungsplänen, weil dies ihren Produktabsatz sichert. Auch haben Hersteller generell ein Interesse an proprietären Systemen, weil sie die Abhängigkeit ihrer Kundinnen und Kunden sichern. Bei der Frage nach Wayside- vs. On-Board-Sensorlösungen können sich die Interessen von EIU (Erzielung hoher Trassenpreise) und von Sfz-Herstellern (Erzielung hoher Fahrzeugpreise) gegenüberstehen.

M4 Oligopolistische Marktstrukturen und Marktmacht,
Insbesondere im Bereich der Herstellung von Schienenfahrzeugen und von Bahninfrastruktur existieren nur sehr wenige Anbieter mit hoher Marktmacht. Dies erschwert die Verhandlungspositionen von Zulieferern mit innovativen Produktlösungen und kann innovationshemmend wirken.

M5 Hoher Kostendruck auf potenzielle Sensoranwender
Die potenziellen Sensoranwender, vor allem die EVU, stehen häufig unter einem enormen Kostendruck. Gleichzeitig besteht eine Abhängigkeit von wenigen spezialisierten und zugelassenen Sensorsystemherstellern im Bahnsektor, da hohe Markteintrittsbarrieren existieren. Dadurch können sich kostengünstige Innovationen nur schwer durchsetzen. Im Zweifel werden EVU nur die Minimalanforderungen von Aufgabenträgern erfüllen und haben keinen Spielraum für innovative Fahrzeugausstattungen.

6 Handlungsableitungen und Marktausblick

Ziel der Arbeiten in diesem Kapitel ist, aufbauend auf der Stakeholderanalyse (und unter Berücksichtigung der Erkenntnisse der weiteren Kapitel) Handlungsbedarfe für einen verstärkten Einsatz von Sensorik im Bahnsystem (dort wo dieser sinn- und vorteilhaft erscheint) abzuleiten sowie einen Ausblick auf zukünftige Marktentwicklungen und Geschäftsmodelle für Sensoranwendungen im Bahnkontext zu wagen. In den nachfolgenden Unterabschnitten werden das Vorgehen und die Ergebnisse der entsprechenden Unterkapitel dargestellt.

6.1 Handlungsfelder

Ziel dieses Unterkapitels war die Ableitung und Aufbereitung verständlicher Handlungsfelder für eine zukünftig stärkere Integration von Sensoren und Sensorsystemen in Erfolg versprechenden Anwendungsbereichen im Bahnsektor. Dabei sollte ein Augenmerk auch auf Möglichkeiten einer aktiven Anreizgestaltung liegen. Den hergeleiteten Handlungsfeldern sollten auch jeweils konkrete Maßnahmenvorschläge, die Zielgruppen entsprechender Maßnahmen und Maßnahmenverantwortliche zugeordnet und voneinander abgegrenzt werden.

6.1.1 Vorgehen und Gesamtübersicht

Als Grundlage für die Entwicklung der Handlungsfelder dienten neben literaturbasierten Recherchen und einigen Erkenntnissen des Kapitels 4 (hier insbesondere die Ergebnisse der Relevanzkriterien bei den Use Case Bewertungen und die Ergebnisse der Anforderungsanalyse) schwerpunktmäßig die durchgeführten Stakeholderanalysen des Kapitels 5 und die in diesem Zusammenhang aus der analytischen Auseinandersetzung sowie den geführten Expertinnen- und Experteninterviews abgeleiteten Innovationsbarrieren.

Mit Hilfe literaturbasierter Recherchen wurden in einem ersten Schritt potenzielle Handlungsfelder aus einer Analogie zu themenverwandten Innovationsfeldern des Mobilitätssektors allgemein abgeleitet. Unter dem Schlagwort der Mobilitätswende vollzieht sich seit den letzten zehn bis fünfzehn Jahren eine allmähliche und zugleich facettenreiche Transformation von Technologien, Geschäftsmodellen und Wertschöpfungsketten, die immer wieder ähnliche Handlungsbedarfe nach sich zieht. Deshalb wurde hierzu eine Schlag- und Stichwortsuche in Literaturdatenbanken und Suchmaschinen hinsichtlich mobilitätsbezogener Forschungs- und Innovationsthemen der letzten Jahre und diese Themen repräsentierende Projekte unternommen. Die betrachteten Forschungs- und Innovationsthemen waren (unter Einbeziehung synonymer und ähnlicher Bezeichnungen):

- Elektromobilität
- Automatisiertes bzw. Autonomes Fahren
- Vernetzte Mobilität
- Shared Mobility bzw. Mobility-as-a-Service
- Seamless Mobility bzw. intermodale Reiseketten
- Intelligente Verkehrssysteme
- Stärkung des Schienenverkehrs bzw. des Umweltverbunds
- Smart Cities bzw. nachhaltige Stadtentwicklung

Diese thematischen Suchbegriffe wurden jeweils kombiniert mit den Schlagworten „Aktionsfeld“, „Aufgabenfeld“, „Handlungsfeld“, „Handlungsempfehlungen“ oder „Maßnahmenbereich“. Obwohl sich die vorgeschlagenen Einzelmaßnahmen erwartungsgemäß je nach Thema mehr oder weniger stark voneinander unterscheiden, konnten dennoch aus dieser Recherche immer wiederkehrende und übergreifende Bereiche mit Handlungsbedarfen identifiziert werden. Dies waren in aggregierter Form:

- Handlungsbedarfe im Verkehrsrecht, z. B. die Fahrzeugzulassung betreffend
- Handlungsbedarfe im Informationstechnologierecht, z. B. den Datenschutz betreffend
- Bedarfe nach Normung und Standardisierung
- Erfordernisse des stakeholderübergreifenden Teilens von Daten (entgeltlich oder unentgeltlich)
- Bedarfe an Neu- und Weiterentwicklungen von Geschäftsmodellen, z. B. die Monetarisierung von Daten betreffend
- Technische Maßnahmen zur Sicherstellung von Zuverlässigkeit, Verfügbarkeit und Sicherheit
- Kooperationsbedarfe zwischen Marktteilnehmenden
- Disziplin- und branchenübergreifender Wissenstransfer
- Wettbewerbs- bzw. marktstimulierende Maßnahmen, z. B. durch Marktregulierungen
- Finanzielle Förderungen von (Erst-)Investitionen
- Weitere Forschungs- und Erprobungsaktivitäten
- Transformationskonzepte für Technologiemigrationen
- Volkswirtschaftliche Analysen zum gesellschaftlichen Nutzen von Innovationen
- Technikfolgenabschätzungen von Innovationen

Auf Grundlage dieser übergreifenden und für Mobilitätsinnovationen typischen Handlungsbedarfsbereiche entstand durch eine Adaption auf den vorliegenden Untersuchungsgegenstand sensorbasierter Technologien im Bahnsystem und nach Abstimmungen mit den Konsortialpartnern und ausgewählten Expertinnen und Experten ein Grundraster sortierter und zueinander in Beziehung gesetzter Handlungsfelder. Der Erstentwurf dieser Handlungsfeldübersicht wurde schrittweise überarbeitet, neu angeordnet, ergänzt bzw. zusammengefasst und zeitlich parallel dazu mit Inhalten, also mit konkreten Maßnahmenvorschlägen, untersetzt. Dabei flossen nacheinander die folgenden Erkenntnisse in die Bearbeitungsschritte ein:

1. Erkenntnisse der analytischen Auseinandersetzung mit den Stakeholderbeziehungen sowie aus den diese begleitenden Expertinnen- und Experteninterviews, insbesondere hinsichtlich existierender Interessenkonflikte
2. Erkenntnisse aus den im Ergebnis der Stakeholderanalyse und den Expertinnen- und Experteninterviews abgeleiteten Innovationsbarrieren
3. Erkenntnisse des zweiten Expertinnen- und Experten-Workshops zu den Geschäftsmodellen und zum Marktausblick, insbesondere hinsichtlich der Schlüsselfaktoren für einen Geschäftsmodellerfolg und der unterdurchschnittlich bewerteten Kriterien für Marktattraktivität und Marktreife

In der nachfolgenden Abbildung 27 ist die Gesamtübersicht der strukturierten Handlungsfelder in ihrer finalen Fassung dargestellt.

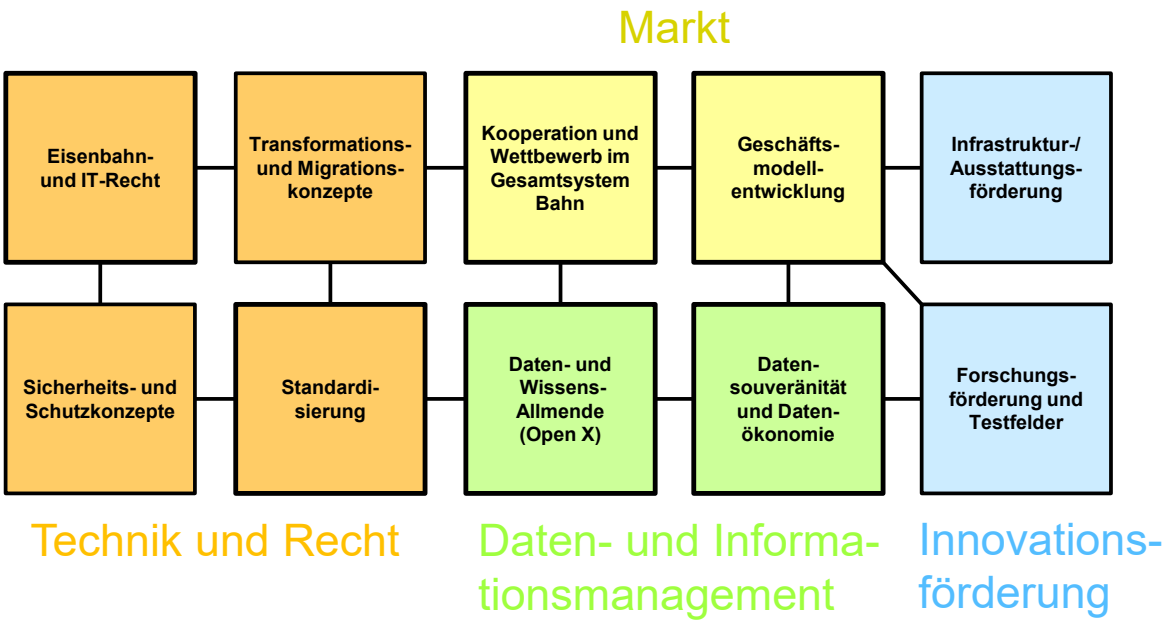


Abbildung 27: Gesamtübersicht der Handlungsfelder [TU Chemnitz, BWL III]

Es wurden insgesamt zehn Handlungsfelder identifiziert, die wiederum vier übergeordneten Kategorien zuordenbar sind. Bei Letzteren handelt es sich um:

- den Bereich **Technik und Recht**, der sich mit der Wechselwirkung zwischen technologischen Neu- und Weiterentwicklungen und rechtlichen bzw. normativen Rahmenbedingungen beschäftigt,
- den Bereich **Markt**, der sich mit den wirtschaftlichen Voraussetzungen von langfristigen Innovationserfolgen beschäftigt,
- den Bereich **Daten- und Informationsmanagement**, der sich im Rahmen des Projektes als äußerst wichtiger Engpass für die Durchsetzung sensorbasierter Lösungen im Bahnsystem herauskristallisierte und deshalb als eigenständige Kategorie berücksichtigt wird, auch wenn hier wieder technische, rechtliche und wirtschaftliche Faktoren zum Tragen kommen und
- den Bereich der **Innovationsförderung** durch staatliche bzw. öffentliche Institutionen.

Bei den Handlungsfeldern handelt es sich im Einzelnen um:

- das **Eisenbahn- und IT-Recht** mit Herausforderungen und gesetzlichen Novellierungs- oder Klarstellungsbedarfen, insbesondere bei Zulassungsprozessen und Zertifizierungsverfahren sowie bei Datensicherheits- und Datenschutzanforderungen,
- die technischen **Sicherheits- und Schutzkonzepte** zur adäquaten Umsetzung rechtlich geforderter und sachlich gebotener Schutzhandlungen,
- das in großer Nähe zu den ersten beiden stehende und oft als Bindeglied zwischen Recht und Technik wirkende Aufgabenfeld der **Standardisierung** sensorbezogener Lösungen im Mobilitätssektor (technische Spezifikationen und gemeinsame Regeln zur Gewährleistung von Interoperabilität, Kompatibilität und Produktqualität),
- **Transformations- und Migrationskonzepte** für einen reibungslosen und geordneten Übergang von bestehenden Technologie(plattforme)n zu neuen Lösungen,

- die Förderung von **Kooperation und Wettbewerb im Gesamtsystem Bahn** (über alle Teilbereiche hinweg) und darüber hinaus, um funktionierende Wertschöpfungsketten und bestreitbare Märkte für sensorbasierte Mobilitätslösungen zu schaffen,
- die eng damit im Zusammenhang stehende Aufgabe der **Geschäftsmodellentwicklung**, um für sinnvolle Sensoranwendungen eine langfristige wirtschaftliche Basis zu haben,
- die **Daten- und Wissensallmende** als gemeinschaftlicher und offener Zugang zu Daten, Informationen und Wissen im Sinne eines öffentlichen Gutes (umgesetzt über verschiedene Open-X-Formate),
- die **Datensouveränität und Datenökonomie**, welche mit der Kontrolle, Hoheit und Verfügungsgewalt über eigene Daten sowie mit wirtschaftlichen Verwertungskonzepten für diese erst die Voraussetzungen für datenbasierte Geschäftsmodelle schaffen,
- die **Infrastruktur- und Ausstattungsförderung**, mit welcher der Staat bzw. die öffentliche Hand als maßgeblicher Stakeholder finanzielle und risikobezogene Barrieren hinsichtlich der Erstinvestitionen aber auch des Betriebs reduzieren kann und
- die **Forschungsförderung und Testfelder**, mit denen der Staat noch bestehende Hürden auf Seiten der Technologie bzw. bezüglich ihres Transfers in marktfähige Produkte und Dienstleistungen verringern kann.

Die Anordnung der zehn Felder wurde so gewählt, dass mit den in Abbildung 27 eingezeichneten Verbindungslinien die primären Zusammenhänge zu benachbarten Handlungsfeldern am besten deutlich werden. So bestehen bspw. starke Abhängigkeiten bei der Entwicklung Erfolg versprechender Geschäftsmodelle zu gelungenen Kooperationen, zu einer funktionierenden Datenökonomie sowie zu Forschungs- und Ausstattungsförderungen. Nichtdestotrotz lassen sich auf diese Weise nicht alle existierenden Wechselwirkungen zwischen den Handlungsfeldern übersichtlich darstellen – es gibt also noch weitaus mehr. Zugleich sind die Einzelmaßnahmen auch nicht immer überschneidungsfrei nur genau einem Handlungsfeld zuordenbar. In Zweifelsfällen wurden sie der Einfachheit halber dem Handlungsfeld zugeordnet, welches ihnen die größte Abgrenzbarkeit gegenüber verwandten Maßnahmen bietet.

Alle zehn Handlungsfelder sind auf Basis der durchgeführten Analysen und Interviews als „wichtig“ zu betrachten. Dennoch wurde in Abbildung 27 mit der unterschiedlichen Rahmendicke der Felder eine gewisse Prioritätseinschätzung visualisiert. Diese Einschätzung basiert auf der wahrgenommenen Häufigkeit des Auftauchens zugehöriger Themen- und Fragenkomplexe in den durchgeführten Recherchen, Interviews und den Diskussionen der beiden Workshops. Einen besonders hohen Handlungsdruck weisen demzufolge die Bereiche „Kooperation und Wettbewerb im Gesamtsystem Bahn“, „Geschäftsmodellentwicklung“, „Datensouveränität und Datenökonomie“ sowie „Standardisierung“ auf.

Insgesamt wurden 36 Maßnahmenvorschläge – pro Handlungsfeld jeweils drei bis fünf – erarbeitet, die in den nachfolgenden Abschnitten dargestellt werden. Grundsätzlich ist ein weiteres Herunterbrechen auf noch spezifischere und besser operationalisierbare Einzelmaßnahmen möglich. Da es sich hier um eine Grundlagenarbeit handelt, wurde dies aber nur an wenigen Stellen mit Aufzählungen angedeutet, wenn mehrere verschiedene Umsetzungspfade augenscheinlich waren. Es wird empfohlen, in Folgeaktivitäten die Maßnahmenvorschläge dieser Untersuchung gemeinsam mit den Stakeholdern zu validieren und bei Bedarf zu konkretisieren.

6.1.2 Eisenbahn- und IT-Recht

In der nachfolgenden Tabelle 31 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Eisenbahn- und IT-Recht, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 31: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *EISENBAHN- UND IT-RECHT*

Maßnahmenvorschlag	**Zielgruppen**	**Maßnahmen-verantwortliche**
Erleichterung des Zulassungsprozesses für neue Sensorlösungen: ▪ Transparente Zulassungsrichtlinien ▪ Mentoring-Programme für Neueinsteiger in den Bahnsektor ▪ Ggf. vereinfachte/beschleunigte Antrags-/Prüfverfahren oder die Schaffung von Experimentierklauseln	Sensorsystemhersteller, IKT-Dienstleister, Fahrzeug- und Infrastruktur-hersteller	EBA, ERA, Gesetzgeber/Ministerien, Verbände
Einrichtung von **Expertengremien für die Novellierung von Zulassungsprozessen** vor dem Hintergrund neuer Digitaltechnologien (insbesondere das maschinelle Lernen betreffend)	Fachexpertinnen und -experten aus Wissenschaft und Praxis (IKT & Prüfung)	EBA, ERA, Gesetzgeber/Ministerien
Erprobung und Etablierung neuer Test- und Zertifizierungsverfahren für Sensorlösungen im Bahnbereich	Prüferinnen und Prüfer/Zertifiziererinnen und Zertifizierer	EBA, ERA, Forschungseinrichtungen
Einrichtung von **Arbeitsgruppen zur Erarbeitung von Datensicherheits- und Datenschutzrichtlinien** (bei Bedarf: von Anpassungsvorschlägen des IT-Rechts) für den verstärkten Einsatz von Sensorlösungen im Bahnsektor	Fachexpertinnen und -experten IT-Recht EVU, IKT-Dienstleister	Datenschutzbehörden, Gesetzgeber/Ministerien, Industrieverbände, BSI

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Herausforderungen steigender Systemkomplexität für die Bahntauglichkeit, insbesondere für Wartbarkeit und Skalierbarkeit
- Technologischer Aufwand zur Wahrung von Datensicherheit und Datenschutz
- Zeit- und Kostenaufwand der Bahnzulassung bzw. -zertifizierung (insbesonere Sicherheitsnachweise)
- Fehlende Zulassungsfähigkeit bzw. die Ungewissheit über eine solche vor Beendigung des Zulassungsprozesses, insbesondere KI-gestützter und verteilter Systeme (Cloudlösungen)
- Einhaltung von Datenschutzvorschriften

Ein Großteil der Maßnahmen in diesem Feld betrifft die Zulassung. Wie in Abschnitt 4.3.4 dargestellt, sind die zu durchlaufenden Zulassungsprozesse sehr komplex und es sind zahlreiche Regelwerke zu prüfen. Dies ist umso aufwendiger und herausfordernder, je mehr die Sicherheitsrelevanz von der jeweiligen Sensoranwendung betroffen ist. Gerade für KMU und Neueinsteiger in die Bahnbranche von Seiten der Sensor(system)hersteller und beteiligter IKT-Dienstleister stellt dies eine beträchtliche Umsetzungshürde dar. Es fehlt häufig an Vorwissen, Ressourcen und einer klaren Aussicht auf einen Zulassungserfolg am Ende der langwierigen Prozesse.

Deshalb sind hier Erleichterungen zu schaffen, welche entsprechende Einstiegshürden senken können. Solche Erleichterungen können darin bestehen, die Richtlinien für die Zulassung von Sensorsystemen im Bahnsektor transparenter und nachvollziehbarer zu gestalten, z. B. in Form von einfachen und kurzen Zulassungsleitfäden, welche den konsequenten Weg von der Anwendungsidee bis hin zur bahnzugelassenen Sensorlösung im Wust der zu berücksichtigenden technischen Regelwerke aufzeigen. Dies könnte auch von Informationskampagnen begleitet werden. Auch könnten bestehende Regelwerke auf ihre

Verständlichkeit hin sowie den Bezug und die Anwendbarkeit auf infrage kommende Sensoranwendungen geprüft und ggf. ergänzt oder angepasst werden. Eine weitere Möglichkeit besteht darin, potenzielle Einsteiger in die Bahnbranche mit Mentoringprogrammen zu unterstützen und sie mit der Begleitung eines ersten Zulassungsprozesses dazu zu befähigen, dies künftig mit den gewonnenen Kompetenzen selbstständig zu bewältigen. Gegebenenfalls besteht auch die Möglichkeit zur Durchsetzung vereinfachter und beschleunigter Antrags- und Prüfverfahren oder zur Schaffung von Experimentierklauseln, welche zeitlich, räumlich und/oder situativ beschränkte Zulassungen unter vereinfachten Anforderungen ermöglichen, um Erfahrungen zu sammeln und Lernprozesse zu ermöglichen. Dies wird aber stark von den jeweils relevanten Sicherheitsanforderungsstufen abhängen.

Die bisherigen Maßnahmenvorschläge betrafen den Status Quo des Bahnzulassungsrechts. Es wird aber voraussichtlich unabdingbar sein, im Zuge der technologischen Fortschritte auch das bestehende Recht und die darin vorgesehenen Zulassungsverfahren zu novellieren, weiterzuentwickeln und geforderte Nachweisverfahren zu verändern. Sonst werden einzelne sinnvolle sensorbasierte Anwendungen, basierend auf (hinsichtlich des Stands der Technik) veralteten Zulassungsverfahren, nie zulassungsfähig werden. Dies betrifft insbesondere Gesamtlösungen, bei denen maschinelles Lernen zum Einsatz kommt, welches in den existierenden Normen für System- und Softwareentwicklungsprozesse noch nicht berücksichtigt wird. Hier ergeben sich insbesondere zulassungsrechtliche Handlungsbedarfe in Bezug auf den Nachweis funktionaler Sicherheit bei einer (noch) unzureichenden Erklärbarkeit von Künstliche Intelligenz (KI)-Entscheidungen [63]. Es wird vorgeschlagen, vor diesem Hintergrund Gremien aus Fachexpertinnen und -experten einzurichten, welche sich mit den Fragen beschäftigen, an welchen Stellen des Zulassungsrechts Novellierungen erforderlich sind und wie diese ausgestaltet werden können und sollten.

Werden bestehende Test- und Zertifizierungsverfahren für neue Sensorlösungen angepasst oder neue eingeführt, so sollte dies vor der flächenmäßigen Durchsetzung und Etablierung mit einer Erprobungsphase durch die Expertinnen und Experten, also die Prüferinnen und Prüfer sowie Zertifiziererinnen und Zertifizierer, bei ausgewählten Herstellern bzw. Anwendern geschehen. Dies ermöglicht es, noch Anpassungen für die praktische Durchführbarkeit basierend auf den probeweisen gewonnenen Erfahrungen vorzunehmen.

Bezogen auf das Informationstechnologierecht sollten sich ebenfalls Fachexpertinnen und -experten in Arbeitsgruppen zusammenfinden, um gemeinsam mit den an Sensorlösungen für das Bahnsystem beteiligten IKT-Dienstleistern bestehende Datensicherheits- und Datenschutzrichtlinien hinsichtlich ihrer Passfähigkeit, Praktikabilität und Vollständigkeit zu prüfen und bei Bedarf auch Anpassungsvorschläge für das existierende Informationstechnologierecht zu erarbeiten, um den verstärkten Einsatz bei Bahnanwendungen zu fördern.

6.1.3 Sicherheits- und Schutzkonzepte

In der nachfolgenden Tabelle 32 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Sicherheits- und Schutzkonzepte, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 32: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *SICHERHEITS- UND SCHUTZKONZEPTE*

Maßnahmenvorschlag	Zielgruppen	Maßnahmenverantwortliche
Pragmatische Weiterentwicklung existierender Sicherheits- und Schutzkonzepte auf Basis realistischer und aktueller Risikobewertungen (und des Status Quo als Benchmark für das Sicherheitsniveau) →*„Vorbeugen“*	Anbieter und Anwender von Sensorlösungen	EBA, ERA, Forschungs-einrichtungen, IT-Fachexpertinnen und -experten, Anbieter und Anwender von Sensorlösungen
Sicherheitsaudits und Sicherheitsmonitoring auf Basis aktueller Sicherheits- und Schutzkonzepte →*„Erkennen“*	Anwender von Sensorlösungen	Prüferinnen und Prüfer/Zertifiziererinnen und Zertifizierer, Anwender von Sensorlösungen
Vorhaltung und Umsetzung von Abhilfemaßnahmen zur Bewältigung von Störfällen und Krisensituationen →*„Reagieren und Wiederherstellen“*	Anwender von Sensorlösungen und betroffene Dritte (z. B. Fahrgäste)	Anwender von Sensorlösungen

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Kompatibilität und Interoperabilität in heterogenen Bahnsystemen
- Herausforderungen steigender Systemkomplexität für die Bahntauglichkeit, insbesondere für Wartbarkeit und Skalierbarkeit
- Technologischer Aufwand zur Wahrung von Datensicherheit und Datenschutz

Die technischen Sicherheits- und Schutzkonzepte dienen der adäquaten Umsetzung rechtlich geforderter und sachlich gebotener Schutzmaßnahmen gegen Gefährdungen, Bedrohungen und Angriffsszenarien (hinsichtlich der Cybersecurity-Bedrohungen siehe auch Kapitel 8). Sie sind grob in die Aufgabenbereiche „Vorbeugen“, „Erkennen“ sowie „Reagieren und Wiederherstellen“ kategorisierbar. Daran orientieren sich die Maßnahmenvorschläge in diesem Feld.

Es wird im Bereich „Vorbeugen“ zunächst darauf ankommen, bestehende Konzepte pragmatisch weiterzuentwickeln. Dazu gehört es, realistische und aktuelle (hinsichtlich der Kenntnis von technischen Schwachstellen und Bedrohungslagen) Risikobewertungen zugrunde zu legen. Zugleich besteht die Gefahr, unbeabsichtigt neue Innovationshürden zu schaffen, indem mit der Einführung neuer sensorbasierter Technologien in den überabeiteten Sicherheits- und Schutzkonzepten (bzw. auch im Zulassungsrecht, siehe Abschnitt 6.1.2) letztlich höhere Anforderungen an das Sicherheitsniveau gestellt werden, als es im Status Quo des Bahnsystems erreicht wird. Auch wenn weitere Sicherheitsverbesserungen ein wichtiges Mehrwertkriterium für den Einsatz sensorbasierter Technologien im Bahnsystem darstellen (siehe Abschnitt 4.2.1 und Tabelle 4) und daher berechtigterweise entsprechende Erwartungen der Stakeholder existieren, so ist grundsätzlich davon auszugehen, dass das heutige Bahnsystem „sicher genug“

ist, um seinen Betrieb zu verantworten. Daher sollte der Status Quo des erreichten Sicherheitsniveaus auch als Benchmark für den Einsatz neuer Sensoranwendungen dienen, insbesondere wenn diese mit weiteren Mehrwerten verbunden sind.

Die jeweils aktuell gültigen Sicherheits- und Schutzkonzepte sind schließlich auch im Sinne des „Erkennens“ von Gefährdungen und Bedrohungen praktisch anzuwenden. Das heißt, ein laufendes Sicherheitsmonitoring und wiederkehrende Sicherheitsaudits sind durchzuführen. Dies dient zum einen dazu, sich entwickelnde, bestehende oder plötzlich auftretende Gefährdungen und Bedrohungen an sich rechtzeitig zu erkennen, um darauf reagieren zu können. Zum anderen dient es auch dazu, eine unzureichende Vorbereitung durch eine mangelhafte Implementierung der Sicherheits- und Schutzkonzepte zu erkennen und abzustellen, bevor Gefährdungen und Bedrohungen eintreten.

Im Falle des Eintritts von Störfällen und Krisensituationen sind die richtigen Abhilfemaßnahmen zu deren Bewältigung umzusetzen und das betroffene Segment des Gesamtsystems Bahn muss wieder möglichst schnell in einen funktionsfähigen und sicheren Zustand zurückversetzt werden („Reagieren und Wiederherstellen“). Dies setzt voraus, dass die richtigen Abhilfemaßnahmen als Notfallpläne vorgehalten werden und dass auf sie zeitnah zugegriffen werden kann.

6.1.4 Transformations- und Migrationskonzepte

In der nachfolgenden Tabelle 33 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Transformations- und Migrationskonzepte, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 33: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *TRANSFORMATIONS- UND MIGRATIONSKONZEPTE*

Maßnahmenvorschlag	**Zielgruppen**	**Maßnahmen-verantwortliche**
Erstellung von **Roadmaps** und **Technologiemigrationsplänen** für die schrittweise Implementierung neuer Sensorlösungen (basierend auf einer klaren Langfristvision und Wirtschaftlichkeitsbewertungen sowie priorisiert nach Marktsegmenten, Einsatzfeldern etc.)	EVU, EIU, IKT-Dienstleister (Infrastruktur-betreiber)	EBA, ERA, Forschungseinrichtungen, EVU, EIU, Verbände
Planung/Durchführung von **Schulungs- und Qualifizierungsmaßnahmen für die Technologiemigration**	EVU, EIU, Instandhalter, Infrastruktur- und Sfz-Hersteller	IKT-Dienstleister, Sensorsystemhersteller, Bildungseinrichtungen
Pilothafte Umsetzungen, deren Evaluierung und schließlich flächendeckender **Rollout neuartiger Sensorlösungen**	EVU, EIU	Infrastruktur- und Sfz-Hersteller
Planungs- und ausführungsseitige Sicherstellung von **Modularität, Flexibilität und Upgradefähigkeit von Bahntechnik** für zukünftige Technologiemigrationen	EVU, EIU	Aufgabenträger, Infrastruktur- und Sfz-Hersteller

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Kurze Innovationszyklen von Digitaltechnologien organisatorisch-wirtschaftlich nur schwer mit langen Lebens-/Wartungszyklen der Bahntechnik (Infrastruktur und Sfz) vereinbar
- Nichtexistenz bzw. Unwirtschaftlichkeit von Migrationsstrategien

Der Einsatz sensordatenbasierter Systeme geht in vielen Fällen mit einem recht weitreichenden Übergang von bestehenden Technologieplattformen oder Grundtechnologien auf neue einher. Denn viele Sensoranwendungen können ihre Potenziale und Mehrwerte erst richtig entfalten, wenn sie großflächig skaliert im Bahnsystem zum Einsatz kommen. Um einen solchen Übergang reibungslos und geordnet zu gestalten bzw. ihn überhaupt erst zu ermöglichen, braucht es gut vorbereiteter und durchdachter Konzepte und Maßnahmen.

Zunächst ist es wichtig, eine klare Vorstellung und Langfristvision davon zu besitzen, was man mit welchem Zeithorizont durch eine flächendeckende Einführung bestimmter Sensoranwendungen erreichen möchte. Dazu gehört es auch, eventuelle Synergien zwischen verschiedenen sensortechnischen Ausrüstungen in Fahrzeugen und der Infrastruktur sowie zwischen verschiedenen Sensoranwendungen zu berücksichtigen. Auch fundierte wirtschaftliche Einschätzungen zu den Kosten und Nutzen der hochskalierten Anwendungen und der damit verbundenen Umstellungen werden benötigt. Es ist durchaus denkbar, dass ein Umstieg von Legacy-Technologien trotz vielfältiger monetärer Mehrwerte nicht wirtschaftlich ist, weil die Alttechnologien eine so hohe Verbreitung und eine so tiefe Integration in die Prozesse und Systeme von Infrastrukturen und Organisationen besitzen, dass die erforderlichen Investitionen, Schulungen und weiteren Anpassungsmaßnahmen einfach zu hoch bzw. zu umfangreich sind. Daher sind die ökonomischen Auswirkungen vorab im Einzelfall zu bewerten. Auf Basis einer begründeten Langfristvision können und sollten dann mit Priorisierungen für Marktsegmente und Einsatzfelder konkrete Roadmaps und Technologiemigrationspläne entwickelt werden, aus denen hervorgeht, bis wann und wo im Gesamtsystem eine Technologiemigration umgesetzt werden soll und wie die dafür benötigten Finanzmittel zur Verfügung gestellt werden sollen.

Da es sich bei einer Technologiemigration meist um ein großes Unterfangen handelt, welches tief in die bestehenden Geschäftsprozesse beteiligter Stakeholder (bis hin zu den Instandhaltern) eingreift, werden oft auch sehr umfangreiche Schulungs- und Qualifizierungsmaßnahmen für sie benötigt. Diese werden in vielen Fällen auch eine gewisse Zeit in Anspruch nehmen bzw. ist mit Engpässen von Seiten der internen oder externen Bildungsanbieter zu rechnen. Deshalb stellt auch die vorausschauende Planung und konsequente Durchführung von Schulungs- und Qualifizierungsmaßnahmen einen bedeutsamen Handlungsbedarf dar. Gegebenenfalls können hierbei auch verschiedene Stakeholdergruppen von Seiten der Sensorlösungsanbieter und Anwender miteinander kooperieren.

Neben vorbereitenden planenden und qualifizierenden Aktivitäten ist der tatsächliche physische Rollout neuartiger Sensorlösungen in der Fläche schließlich auch mit Nachdruck umzusetzen. Dies geschieht im Idealfall, nachdem in ersten pilothaften Umsetzungen noch Erfahrungen gesammelt werden konnten und eine Evaluierung der ursprünglichen Umsetzungsplanung erfolgte, die ggf. noch zu Nachjustierungen der Roadmaps und Technologiemigrationspläne führen. Die Umsetzung wird zudem enge Kooperationen zwischen den beteiligten Stakeholdern voraussetzen.

Zuletzt ist auch vorausschauend an zukünftige und heute noch nicht anwendungs- und technologieseitig bestimmbare Systemtransformationen und Technologiemigrationen zu denken. Hierfür ist es sinnvoll, in der Planung von Bahnsystemen und bei der Ausführung von Bau- und Fertigungsleistungen auf eine möglichst hohe Modularität, Flexibilität und Upgradefähigkeit zu achten, die einen zukünftigen

Technikwechsel nicht unnötig erschwert. Im Speziellen ist dies von Relevanz hinsichtlich der Möglichkeiten, vergleichsweise kurzlebige Digitaltechnologien in langlebigen Schienenfahrzeugen und Schieneninfrastrukturen überhaupt erst oder einfacher durch aktuellere ersetzen zu können.

6.1.5 Standardisierung

In der nachfolgenden Tabelle 34 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Standardisierung, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 34: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *STANDARDISIERUNG*

Maßnahmenvorschlag	Zielgruppen	Maßnahmen-verantwortliche
Entwicklung verkehrsträgerübergreifender und EU-weit bzw. international **harmonisierter Standards** für die Sensorsystemimplementierung und den Datenaustausch	EVU, EIU, Sensorhersteller, IKT-Dienstleister, EBA, ERA	Standardisierungsgremien, Fachverbände, Forschungseinrichtungen
Einrichtung von **Arbeitsgruppen zur Sicherstellung der Implementierbarkeit von Standards**, insbesondere in bestehende Prozesse im Bahnbereich	Standardisierungsgremien	Fachexpertinnen und -experten aus Wissenschaft und Praxis
Förderung von KMU und gesellschaftlichen Stakeholdern bei Standardisierungsprozessen (hinsichtlich Beteiligung und Interessenvertretung)	Anbieter von Sensorlösungen, gesellschaftliche Stakeholder	Gesetzgeber/Ministerien, Verbände

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Kompatibilität und Interoperabilität in heterogenen Bahnsystemen
- Fehlende oder konkurrierende Standards der Sensorsystemimplementierung, des Datenaustauschs
- Dauer und Kosten der Standardisierung (nur große Player können mitwirken)
- Unzureichende Implementierbarkeit existierender Standards (zu hohe Komplexität, an Praxis vorbei)

Die Standardisierung gehört zu den wichtigsten Handlungsfeldern in Bezug auf einen stärkeren Einsatz sinnvoller Sensoranwendungen im Bahnsystem. Sie stellte bereits bei den Innovationsbarrieren eine eigene Kategorie dar. Dabei wurde deutlich, dass es nicht nur um die Existenz hersteller- und länderübergreifender Standards an sich geht, sondern auch um weitere Begleitaspekte von Standardisierungsprozessen.

Der erste Maßnahmenvorschlag betrifft die Entwicklung benötigter Standards, vor allem in den Bereichen des Datenaustausches und der Sensorsystemimplementierung bzw. für hierfür benötigte Systemarchitekturen. Neben einer EU-weiten oder internationalen Harmonisierung ist dabei auch von besonderer Wichtigkeit, dass die Welt der Vollbahnen nicht isoliert, sondern als Teil der Mobilitätswelt als Ganzes betrachtet wird, in welcher die Verkehrsteilnehmenden in zunehmendem Maße auch multi- und intermodal unterwegs sind. Heutige Standards unterscheiden sich häufig schon zwischen den Domänen

der Eisenbahn und der Straßenbahn. Dies erschwert es, übergreifende Systemlösungen zu implementieren. Zukünftige Standards, insbesondere den Datenaustausch betreffend, sollten verkehrsträgerübergreifend ausgestaltet werden. Für den Fall, dass zwei oder mehr neue Standards miteinander konkurrieren und noch nicht absehbar ist, welcher sich schlussendlich am Markt durchsetzen wird, bleibt meist nur die Möglichkeit des Abwartens und Beobachtens oder die Arbeit an Flexibilitäts- und Interoperabilitätsoptionen. Gegebenenfalls können Proofs-of-Concepts nachweisen, welcher Standard technisch vorteilhaft ist.

Ein weiterer Maßnahmenvorschlag betrifft die Problematik der Existenz von in der Praxis ungenutzten Standards. Es ist leider häufig der Fall, dass Standards entwickelt und festgeschrieben werden, die im Laufe des Standardisierungsprozesses übermäßig komplex, aufwendig und umfangreich wurden, sodass sie für die tatsächlichen Marktteilnehmenden nicht mehr implementierbar sind. Spezielle Arbeitsgruppen könnten sich gezielt damit befassen, auf welche Weise solche Situationen vorab verhindert werden können bzw. wie die Implementierbarkeit speziell in die bereits existierenden Prozesse des Bahnsystems sichergestellt werden kann.

Ein letzter Maßnahmenvorschlag in diesem Feld ist die Förderung der Beteiligung von KMU und gesellschaftlichen Stakeholdern bei Standardisierungsprozessen. Aufgrund der hohen Dauer und Kosten von Standardisierungsprozessen sind in diese meist nur sehr große Marktteilnehmenden involviert. Dies kann negative Auswirkungen haben, weil nicht die Interessen der ganzen Breite an Stakeholdern berücksichtigt werden.

6.1.6 Kooperation und Wettbewerb im Gesamtsystem Bahn

In der nachfolgenden Tabelle 35 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Kooperation und Wettbewerb im Gesamtsystem Bahn, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 35: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *KOOPERATION UND WETTBEWERB IM GESAMTSYSTEM BAHN*

Maßnahmenvorschlag	**Zielgruppen**	**Maßnahmen-verantwortliche**
Förderung der Stakeholderkommunikation, insbesondere zwischen Anbietern, Anwendern und Prüferinnen und Prüfern/Zertifiziererinnen und Zertifizierern von Sensorlösungen **über geeignete Plattformen und Formate** ▪ Ideen-/Erfahrungsaustausch (Best Practices, Lessons Learnt) ▪ Formulierung gemeinsamer Forderungen an die Politik	Alle relevanten Stakeholder	Industrieverbände (Bahn + Sensorik), Gesetzgeber/Ministerien, Behörden
Einrichtung von Fokusgruppen für einen **Wissens- und Erfahrungstransfer aus anderen Anwendungsdomänen** (Automobilindustrie, Industrieproduktion & -logistik, Luft- und Raumfahrt, Energie- und Umwelttechnik, Montanindustrie)	Anbieter und Anwender von Sensorlösungen (Bahn + Nicht-Bahn)	Industrieverbände, Gesetzgeber/Ministerien, EBA, ERA

Förderung des Innovations- und Kooperationswettbewerbs durch Wettbewerbsregulierung und Senkung von Eintrittsbarrieren	Infrastruktur- und Sfz-Hersteller, Sensorsystemhersteller	BNetzA, EBA, ERA, Gesetzgeber/Ministerien, Verbände

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Intra- und interorganisationale Widerstände
- Wirtschaftliche Interessenkonflikte
- Oligopolistische Marktstrukturen und Marktmacht, insbesondere im Bereich der Herstellung von Sfz und Bahninfrastruktur
- Hoher Kostendruck auf potenzielle Sensoranwender (insbesondere EVU) bei gleichzeitiger Abhängigkeit von wenigen spezialisierten Sensorsystemherstellern im Bahnsektor

Die Förderung eines stärkeren themenbezogenen Austausches zwischen den beteiligten Stakeholdern gehört zweifelsohne zu den wichtigsten Handlungsempfehlungen, die im Ergebnis des vorliegenden Vorhabens entstanden sind. Sie wurde hier der Handlungsfeldkategorie „Markt“ zugeordnet, könnte aber auch als ein übergreifender Maßnahmenvorschlag für alle Handlungsfelder und Innovationsbarrieren angesehen werden. Hier sind die öffentliche Seite, aber auch die Industrieverbände von Bahn- und Sensorik- bzw. IKT-Sektor gefragt, Initiative zu übernehmen und Plattformen bzw. Austauschformate zu schaffen, in denen alle relevanten Stakeholder, insbesondere die (potenziellen) Anbieter und Anwender von Sensorlösungen sowie die Prüferinnen und Prüfer und Zertifiziererinnen und Zertifizierer, wiederkehrend für einen konstruktiven Dialog zusammentreffen und gemeinsam an den bestehenden Herausforderungen arbeiten. Ein solcher Dialog kann zum einen dazu dienen, bestehende Erfahrungen und künftige Ideen auszutauschen, zum anderen auch dazu, gemeinsame Forderungen an den Gesetzgeber zu formulieren, um den Einsatz sinnvoller Sensoranwendungen im Bahnsystem zu forcieren. Ein enger Austausch zwischen den Stakeholdern ermöglicht es, dass sich bewährte Best Practices aus der praktischen Anwendung einzelner Unternehmen in der Branche verbreiten, und dass auch andere aus individuellen Fehlschlägen und Erfolgen der Vergangenheit bezüglich des Einsatzes sensorbasierter Technologien lernen können.

Ein weiterer Ansatzpunkt ist das Lernen von anderen Anwendungsdomänen, in denen sensorbasierte Systeme und Lösungen schon deutlich weiter verbreitet sind, als dies im Bahnsystem heute der Fall ist. Hier kann man, neben der Automobilindustrie, in der Sensorik für die zunehmende Fahrzeugvernetzung und -automatisierung bzw. für intelligente Straßenverkehrssysteme bereits seit langem ein Brennpunktthema ist, auch an die Bereiche industrielle Produktion und Logistik, Luft- und Raumfahrt, Energie- und Umwelttechnik sowie Montanindustrie denken. Es wird vorgeschlagen, Fokusgruppen für einen entsprechenden Wissens- und Erfahrungstransfer in die Bahnindustrie hinein einzurichten. Diese Gruppen könnten in gemeinsamen Strategiepapieren konkretere Transfervorschläge erarbeiten.

Ein weiterer wichtiger marktseitiger Maßnahmenvorschlag ist die Förderung des Innovations- und Kooperationswettbewerbs. Wie bei den Innovationsbarrieren bereits dargelegt, bestehen große Abhängigkeiten von einer vergleichsweise geringen Anzahl von Marktteilnehmern – sowohl in der klassischen Bahnindustrie von wenigen Infrastruktur- und Fahrzeugherstellern als auch Abhängigkeiten von wenigen stark spezialisierten Sensorsystemherstellern. Hier sind Anreize zur Senkung von Markteintrittsbarrieren und gegebenenfalls spezifische Eingriffe von Seiten der Wettbewerbsregulierung gefragt. Ziel solcher Maßnahmen sollte es sein, das Ringen von verschiedenen Unternehmen um die besten Produkt-, Prozess- oder Geschäftsmodellinnovationen zu fördern und zugleich Raum dafür zu schaffen, dass auch Wettbewerber in einer kooperativen Art und Weise zusammenarbeiten können, um gemeinsame Innovationsziele zu erreichen.

6.1.7 Geschäftsmodellentwicklung

In der nachfolgenden Tabelle 36 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Geschäftsmodellentwicklung, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 36: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *GESCHÄFTSMODELLENTWICKLUNG*

Maßnahmenvorschlag	Zielgruppen	Maßnahmenverantwortliche
Schaffung von Anreizen für strategische Partnerschaften und kooperative Geschäftsmodelle bei stakeholderübergreifenden Sensoranwendungen (Auseinanderfallen von Kosten und Nutzen des Sensoreinsatzes)	EVU, EIU	Gesetzgeber/Ministerien, EBA, ERA, Verbände
Durchführung von perspektivenübergreifenden Wirtschaftlichkeitsanalysen für alternative Geschäftsmodelloptionen von Sensoranwendungen	Anbieter und Anwender	Anbieter und Anwender
Öffentlich-privaten Partnerschaften (ÖPP) zur Teilung von Kosten und Risiken, wenn besonders hohe Investitionsbedarfe und Unsicherheiten zusammenfallen	EVU, EIU, Infrastruktur-, Sfz.-Hersteller, IKT-Dienstleister	Gesetzgeber/Ministerien, Aufgabenträger
Gezielte Verbesserung der benötigten Berufsqualifikationen durch (Weiter-)Bildungsförderung, Sensibilisierung und Ermutigung, transparente Kommunikation bzw. Öffentlichkeitsarbeit, attraktive Arbeitsbedingungen und internationalen Austausch	Fachkräfte (Bahnsektor, Data Sciences und MINT-Berufe allgemein)	Gesetzgeber/ Ministerien, Verbände, Anbieter und Anwender von Sensor-lösungen

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Mangel an qualifizierten Fachkräften, insbesondere in den Bereichen Bahn, Data Science und speziell an deren Schnittstelle
- Fehlende Zulassungsfähigkeit bzw. die Ungewissheit über eine solche vor Beendigung des Zulassungsprozesses
- Haftungsrisiken aus Fehlfunktionen/Ausfällen
- Hohe Investitionsbedarfe bei noch schwer zu bewertender Rentabilität
- Anfall von Kosten und Nutzen des Sensoreinsatzes bei unterschiedlichen Stakeholdern
- Befürchtung des ungewünschten Abflusses sensibler oder werthaltiger Daten

Auch das Handlungsfelder der Geschäftsmodelle bzw. ihrer Neu- und Weiterentwicklung ist von primärer Bedeutung. Für einen Großteil der betrachteten Sensoranwendungen ist nicht eine unzureichende Technologieentwicklung ein Problem, sondern das bisherige Fehlen funktionsfähiger Geschäftsmodelle.

Ein erster wichtiger Ansatz in diesem Feld ist es, strategische Partnerschaften und kooperative Geschäftsmodelle zwischen Stakeholdern zu fördern, die bei bestimmten Sensoranwendungen zusammenarbeiten müssen, obwohl die Kosten und der Nutzen des Sensoreinsatzes beim jeweils anderen anfallen. Solche Use Cases waren z. B. „Fahrzeug überwacht Oberbau“ und „Infrastruktur überwacht Fahrzeug“. Dies kann geschehen, indem übergreifende und bisher nicht realisierte gemeinsame Nutzen identifiziert werden, indem faire Verteilungsmodelle für die anfallenden Kosten bzw. die verlangten Preise gefunden werden oder indem ein neutraler Vermittler zwischengeschaltet wird.

Um der großen Unsicherheit über die Vorteilhaftigkeit von Investitionen zu begegnen, sollten Wirtschaftlichkeitsanalysen für alternative Geschäftsmodelloptionen durchgeführt werden, die gezielt auch die Perspektiven der eigenen Geschäftspartner und der wichtigsten anderen Beteiligten entlang der Wertschöpfungskette berücksichtigen. Auf diese Weise kann ein klareres Bild von den Erfolgsvoraussetzungen eines angedachten Geschäftsmodells oder von den entscheidenden Einflussfaktoren gewonnen werden.

Nicht immer führen solche Wirtschaftlichkeitsbewertungen zu einem hinsichtlich des Risikos befriedigenden Ergebnis. Das heißt Eingangsgrößen der Bewertung für ein an sich vorteilhaft bewertetes Geschäftsmodell können so risikobehaftet sein, dass von einer Investition durch private Unternehmen oder auch Industriekonsortien abgesehen wird. In diesem Fall – also, wenn besonders hohe Investitionsbedarfe und Unsicherheiten zusammenfallen – können gegebenenfalls öffentlich-privaten Partnerschaften (ÖPP) zur Teilung der zu tragenden Kosten und Risiken und damit zu einer Umsetzung der sensordatenbasierten Geschäftsmodelle beitragen.

Eine weitere wichtige Hürde für die Realisierung neuer Geschäftsmodelle mit Sensorlösungen im Bahnsystem stellt der Mangel an qualifizierten Fachkräften dar. Dies betrifft auch die Herausforderung weniger digitalaffine Menschen beim Wandel der anfallenden Arbeitsaufgaben mitzunehmen. Der daraus abgeleitete Maßnahmenvorschlag ist die gezielte Verbesserung der benötigten Berufsqualifikationen. Dies kann durch die inner- oder außerbetriebliche Förderung der (Weiter-)Bildung in den benötigten Wissensdomänen geschehen, durch eine Sensibilisierung und Ermutigung von potenziellen Auszubildenden und bestehenden Mitarbeiterinnen und Mitarbeitern (die auf die Wichtigkeit der Qualifikation und ihre beruflichen Chancen hinweist), durch eine transparente Kommunikation bzw. Öffentlichkeitsarbeit, durch attraktive Arbeitsbedingungen sowie einen internationalen Austausch von Fachkräften.

6.1.8 Daten- und Wissens-Allmende (Open X)

In der nachfolgenden Tabelle 37 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Daten- und Wissens-Allmende (Open X), zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 37: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *DATEN- UND WISSENS-ALLMENDE (OPEN X)*

Maßnahmenvorschlag	**Zielgruppen**	**Maßnahmen-verantwortliche**
Förderung des freien Teilens sensorbasierter Daten im Bahnsektor (**Open Data**), z. B. durch ▪ Anreize oder Verpflichtungen zur Datenfreigabe	Anwender von Sensorlösungen, Betreiber Data Spaces, Cloudanbieter	Gesetzgeber/Ministerien, Projektträger, Standardisierungsgremien

▪ Entwicklung funktionierender Lizenzmodelle und Data-Sharing-Verträge ▪ Etablierung offener Datenstandards ▪ Unterstützung der Schaffung und des Betriebs hierfür benötigter technischer Infrastrukturen		
Förderung von Open-Source-Projekten für Sensorlösungen im Bahnsektor: Software mit öffentlichem Quelltext oder Hardware nach freien Bauplänen	Softwarehersteller, Sensorsystemhersteller	Gesetzgeber/Ministerien, Projektträger, Verbände
Förderung einer transparenten, offenen und frei zugänglichen Wissenschaftspraxis und Wissensvermittlung für Sensoranwendungen im Bahnsektor (**Open Science, Open Access, Open Education**)	Anbieter und Anwender von Sensorlösungen	Forschungseinrichtungen, Gesetzgeber/Ministerien

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Teilweise noch unzureichender Entwicklungsstand der Technologie
- Teilweise noch unzureichende bzw. unzureichend identifizierte sensorbasierte Trainingsdaten für maschinelle Auswertungen/Interpretationen großer Datensätze in Bahnanwendungen
- Konflikte um Verfügungsrechte an Daten
- Mangel an qualifizierten Fachkräften, insbesondere in den Bereichen Bahn, Data Science und speziell an deren Schnittstelle

Die Zugänglichkeit zu sensorbasierten Daten ist von entscheidender Bedeutung für die Realisierung darauf aufbauender Anwendungen und für den Umfang der mit diesen erzielbaren Mehrwerten. In vielen Fällen existiert bereits eine entsprechende Datenbasis, zumindest in Gestalt unverarbeiteter Rohdaten, bei einzelnen Stakeholdern (z. B. Fahrzeugherstellern), doch sie ist nicht oder nur zu nicht vertretbaren Preisen zugänglich für die potenziellen Nutzerinnen und Nutzer, da Bedenken von Seiten der Dateninhaber herrschen, diese herauszugeben.

Die Förderung des freien Teilens sensorbasierter Daten im Bahnsektor (bzw. im Mobilitätssektor allgemein) im Sinne des Open-Data-Gedankens stellt deshalb einen abgeleiteten Maßnahmenvorschlag dar. Eine Umsetzung dieser Förderung ist auf verschiedenen Wegen möglich. Der Gesetzgeber kann Anreize oder auch Verpflichtungen für das freie Teilen sensorbasierter Daten schaffen. Das Gesetz für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz) zur Umsetzung der Richtlinie 2003/98/EG (PSI-Richtlinie) oder die Novellierung des Personenbeförderungsgesetzes (PBefG) zur Umsetzung der Richtlinie 2010/40/EU (IVS-Richtlinie) sind Beispiele für derartige Regelungen. Ein weiterer wichtiger Ansatzpunkt ist die Entwicklung funktionierender Standard-Lizenzmodelle für Daten bzw. Data-Sharing-Verträge in Analogie zu den Creative-Commons-Lizenzen für urheberrechtlich schützbare Werke bzw. Medien. Eine Förderung offener Datenstandards erleichtert das Teilen von Daten zwischen den Stakeholdern, sofern sich diese Standards durchsetzen. Zudem kann die finanzielle und nicht-finanzielle Unterstützung der Schaffung und des Betriebs von technischen Infrastrukturen für den Datenaustausch eine geeignete Maßnahme sein.

Ein zweiter Maßnahmenvorschlag betrifft nicht die Daten an sich, sondern die Förderung von Open-Source-Projekten für Sensorlösungen im Bahnsektor. Unter den Begriff Open Source fällt zum einen Software mit öffentlichem Quelltext und zum anderen Hardware nach freien Bauplänen. Open-Source-Konzepte wirken innovationsfördernd, da eine breitere weltweite Gemeinschaft an der Weiterentwicklung von Hard- und Software arbeiten kann.

Ein letzter Maßnahmenvorschlag in diesem Feld betrifft die Förderung einer transparenten, offenen und frei zugänglichen Wissenschaftspraxis und Wissensvermittlung für Sensoranwendungen im Bahnsektor. Unter den Schlagworten Open Science, Open Access und Open Education existieren bewährte Konzepte, die hierfür zur Anwendung kommen können.

6.1.9 Datensouveränität und Datenökonomie

In der nachfolgenden Tabelle 38 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Datensouveränität und Datenökonomie, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 38: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *DATENSOUVERÄNITÄT UND DATENÖKONOMIE*

Maßnahmenvorschlag	Zielgruppen	Maßnahmen-verantwortliche
Unterstützung bei der Datenmonetarisierung, z. B. bei der Identifikation und Akquise potenzieller Kundinnen und Kunden, der Preisfindung, der Festlegung von Nutzungsberechtigungen und Haftungsfragen in Verträgen	Inhaber sensorbasierter Daten	Forschungseinrichtungen, Verbände, Beraterinnen und Berater
Förderung von **Pilotprojekten und Testumgebungen bei denen Data Spaces** für Sensoranwendungen im Bahnsystem **genutzt werden**	Bereitsteller und Nutzer von Sensordaten (anwendungsspezifisch)	Betreiber Data Spaces, EBA, ERA, Projektträger
Förderung des Aufbaus, des Betriebs und der Weiterentwicklung von Data Spaces für Bahnanwendungen sowie der Interoperabilität mit anderen Datenräumen	Betreiber Data Spaces	Gesetzgeber/Ministerien, Projektträger
Analyse & Klassifizierung der Sensibilität und des Werts eigener Daten; **Überwachung & Auditierung von Datenflüssen**	Inhaber sensorbasierter Daten	Inhaber sensorbasierter Daten, ggf. Beraterinnen und Berater
Verbesserung der Datenqualität (genau, vollständig, konsistent, aktuell); **Einsatz fortschrittlicher Analyse-/Interpretationstechniken**	Inhaber sensorbasierter Daten	Anbieter von Daten-analysen und Machine Learning, Sensorsystem-hersteller

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Technologischer Aufwand zur Wahrung von Datensicherheit und Datenschutz
- Teilweise noch unzureichende bzw. unzureichend identifizierte sensorbasierte Trainingsdaten für maschinelle Auswertungen/Interpretationen großer Datensätze in Bahnanwendungen
- Konflikte um Verfügungsrechte an Daten
- Befürchtung des ungewünschten Abflusses sensibler oder werthaltiger Daten
- Intra- und interorganisationale Widerstände

Das Handlungsfeld Datensouveränität und Datenökonomie gehört zu den wichtigsten Bereichen mit einem Handlungsbedarf. Es betrifft die wirtschaftliche Verwertbarkeit von sensorbasierten Daten und steht damit in einem engen Zusammenhang zum Handlungsfeld der Geschäftsmodellentwicklung. Wie bereits im Zusammenhang mit dem Handlungsfeld Daten- und Wissens-Allmende erwähnt, ist eine Datenbasis, die für in diesem Projekt untersuchte Sensoranwendungen genutzt werden kann, in vielen Fällen „irgendwo“ und bisher ungenutzt bereits vorhanden. Oftmals sind gesammelten sensorbasierten Daten auch prinzipiell zugänglich, weil sie sich im eigenen Einflussbereich, z. B. dem des Sfz-Herstellers oder der ECM, befinden. Das Problem besteht dann vielmehr darin, überhaupt erst zu erkennen, was man mit diesen Daten anfangen und wie man sie einer wirtschaftlichen Verwertung (im eigenen Unternehmen oder als kommerzielles Produkt für andere Marktteilnehmende) zuführen kann.

Ein erster Maßnahmenvorschlag greift diese Problematik auf und zielt auf die beratende Unterstützung von Inhabern sensorbasierter Daten bei ihrer Datenmonetarisierung. Hier gilt es z. B. – eine externe Verwertung betreffend – Hilfen bei der Identifikation und Akquise potenzieller Kundinnen und Kunden, bei der Preisfindung, bei der Festlegung von beidseitig fairen Nutzungsbedingungen und bei Haftungsfragen in Verträgen zu leisten. Auch bei einer unternehmensinternen Verwertung können entsprechende Hilfestellungen zum Auffinden interner Verwertungsmöglichkeiten oder zur Kosten-Nutzen-Abschätzung nützlich sein.

Ein zentrales Problem, welches die Datenverwertung über Stakeholdergrenzen hinweg behindert, sind Befürchtungen des ungewünschten Abflusses sensibler oder werthaltiger Daten. Dabei geht es darum, die Kontrolle, Hoheit und Verfügungsgewalt über eigene Daten nicht ungewollt zu verlieren. In den letzten fünf bis zehn Jahren wurden erste Umsetzungen des Konzeptes sog. Data Spaces (Datenräume) realisiert. Data Spaces ermöglichen in einer sicheren virtuellen Umgebung ein vertrauenswürdiges Teilen von (sensorbasierten) Daten aus verschiedenen Quellen sowie eine souveräne Bewirtschaftung von (sensorbasierten) Datengütern. Das bedeutet, sie stellen sicher, dass Daten bis zu ihrer gewünschten entgeltlichen oder kostenlosen Bereitstellung im Einflussbereich ihres Urhebers bzw. Besitzers verbleiben und dass nur berechtigte Adressaten unter den vereinbarten Nutzungskonditionen auf sie zugreifen können. Im Kontext von Mobilität existieren, neben anderen, zwei in Deutschland besonders bedeutsame und bekannte Data Spaces, die auf Initiative und mit Förderung des Bundesministeriums für Verkehr und digitale Infrastruktur entstanden. Dies ist zum einen der von DRM Datenraum Mobilität GmbH (DRM) betriebene Mobility Data Space als Datenaustauschplattform für neue Geschäftsmodelle und Services und zum anderen die von der Bundesanstalt für Straßenwesen (BASt) betriebene Mobilithek als Nationaler Zugangspunkt für Mobilitätsdaten gemäß IVS-Richtlinie & PBefG (siehe Abschnitt 6.1.8).

Um sensordatenbasierte Anwendungsfälle in der Bahnpraxis voranzubringen, sollten diese bestehenden Infrastrukturen von Data Spaces genutzt und auf diese zurückgreifenden Pilotprojekte und Testumgebungen für Bahnanwendungen gefördert werden. Zudem erscheint es sinnvoll, den Aufbau und Betrieb, vor allem aber die funktionale Weiterentwicklung solcher Data Spaces sowie ihre Interoperabilität mit anderen Datenräumen zu fördern. In diesem Zusammenhang können auch neue Funktionsmodule oder Tools entstehen, die eine ökonomische Verwertung sensorbasierter Mobilitätsdaten im gesamten Mobilitätsökosystem vereinfachen.

Weitere Maßnahmenvorschläge dieses Handlungsfeldes fallen eher in den Aufgabenbereich der Inhaber sensorbasierter Daten selbst. Nichtdestotrotz kann öffentlichen Aufgabenträgern oder Verbänden die Rolle zukommen, diese dafür zu sensibilisieren. Der Wert und die Sensibilität eigener Daten sind zu prüfen und zu klassifizieren, um darauf aufbauend Entscheidungen über deren Schutz und Verwertung treffen zu können. Datenflüsse aus der eigenen Organisation sind entsprechend der Einschätzungen ihres Schutzbedürfnisses zu überwachen und zu auditieren. Wo notwendig und sinnvoll für erfolgreiche Verwertungen, ist die Qualität der Datenbasis hinsichtlich Genauigkeit, Vollständigkeit, Konsistenz und Aktualität zu verbessern. Zudem sind fortschrittliche Analyse- und Interpretationstechniken für die sensorbasierten Daten anzuwenden, um zu zufriedenstellenden Ergebnissen zu gelangen.

6.1.10 Infrastruktur-/Ausstattungsförderung

In der nachfolgenden Tabelle 39 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Infrastruktur-/Ausstattungsförderung, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 39: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *INFRASTRUKTUR-/AUSSTATTUNGSFÖRDERUNG*

Maßnahmenvorschlag	Zielgruppen	Maßnahmen-verantwortliche
(Direkte) **finanzielle Förderung von Investitionen** in bestimmte Sensorlösungen über Finanzierungsmodelle und Förderprogramme	EVU, EIU, Betreiber Kommunikationsinfrastruktur	Gesetzgeber/Ministerien, Projektträger, Finanz-institutionen
Forderung von Sensorlösungen im Rahmen von **Ausschreibungs- und Vergabeverfahren** für Verkehrsverträge und Infrastrukturprojekte	EVU, EIU	Aufgabenträger/ Verkehrsverbünde
Schaffung nachhaltiger **Finanzierungsmöglichkeiten für den laufenden Betrieb** der Sensordatenerfassung und -verarbeitung, inkl. der Instandhaltung von Sensortechnik	EVU, EIU	Gesetzgeber/Ministerien, Aufgabenträger
Setzen nichtfinanzieller, rechtlicher Anreize für Investitionen in Sensorlösungen, z. B. Anpassung von Netzzugangs-/Zulassungskriterien	EVU, EIU, Infrastruktur- und Sfz-Hersteller	Gesetzgeber/Ministerien, EBA, ERA

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Oft noch keine massenmarkttauglichen Commercial-off-the-Shelf-Produkte (COTS) verfügbar, sondern nur teure Pilotumsetzungen
- Hohe Investitionsbedarfe (IT-Infrastruktur, harmonisierte Schnittstellen, Software, Schulungen) bei noch schwer zu bewertender Rentabilität
- Intra- und interorganisationale Widerstände

Wie bereits im Zusammenhang mit den Transformations- und Migrationskonzepten (vgl. Abschnitt 6.1.4) und der Geschäftsmodellentwicklung (vgl. Abschnitt 6.1.7) angeklungen, stellt die Wirtschaftlichkeit bzw. die Unsicherheit über ein ausreichendes betriebswirtschaftliches Kosten-Nutzen-Verhältnis oft einen innovationshemmenden Faktor dar. Es kann daher sein, dass gesellschaftlich gewünschte oder volkswirtschaftlich sinnvolle Investitionen in Ausrüstungen und Infrastrukturen für Sensoranwendungen im Bahnsystem ohne staatliche Unterstützung unterbleiben.

Ein erster Maßnahmenvorschlag beinhaltet daher die direkte finanzielle Förderung von Investitionen in bestimmte Sensorlösungen über Förderprogramme oder sonstige Finanzierungsmodelle. Hier ist sorgfältig abzuwägen, welche Sensoranwendungen aus öffentlicher Perspektive wirklich gebraucht werden und ob diese sich nicht auch ohne finanzielle Förderungen vom Staat in einem akzeptablen Zeithorizont durchsetzen würden. Mit der Förderung besteht aber auch die Möglichkeit einer Markterweiterung, indem auch KMU, die innovative Sensorlösungen anbieten, einen Marktzugang erhalten.

Eine weitere Möglichkeit bei der Erneuerung von Infrastrukturen und Fahrzeugflotten besteht darin, dass die zuständigen Aufgabenträger bei den Ausschreibungs- und Vergabeverfahren für öffentliche Verkehrsverträge und Infrastrukturprojekte bestimmte Sensorausstattungen bzw. Sensorlösungen fordern. Dies hat den Vorteil gegenüber dem ersten Vorschlag, dass im Vergabeverfahren das wirtschaftlichste Angebot zum Tragen kommt und damit die Gefahr, dass zu große bzw. unnötige Investitionszuschüsse gewährt werden, stark sinkt.

Zu beachten ist aber auch, dass eine reine Fokussierung auf Anfangsinvestitionen in vielen Fällen nicht ausreichend sein wird, damit bestimmte wünschenswerte Sensoranwendungen nachhaltig (über Experimentier- und Pilotphasen hinaus) realisiert werden können. Auch Ersatzinvestitionen von Sensortechnik sowie der laufende Betrieb der Sensordatenerfassung und -verarbeitung (mit Wartung von Hard- und Softwaresystemen) verursacht Kosten, die unter Umständen nicht ohne staatliche Kofinanzierung auskommen. Daher bildet die Schaffung nachhaltiger Finanzierungsmöglichkeiten für den laufenden Betrieb einen weiteren Maßnahmenvorschlag.

Zuletzt sind auch nichtfinanzielle, rechtliche Anreize von Seiten des Staates ein möglicher Ansatz, um Investitionen in Sensorlösungen zu forcieren. Hierbei kann bspw. an Anpassungen von Netzzugangs- bzw. Zulassungskriterien gedacht werden. Diese werden sich aber mittelbar auch in gestiegenen Preisen (oder erhöhten Subventionsbedarfen) von Bahnleistungen widerspiegeln.

6.1.11 Forschungsförderung und Testfelder

In der nachfolgenden Tabelle 40 sind die entwickelten Maßnahmenvorschläge für das Handlungsfeld Forschungsförderung und Testfelder, zusammen mit den Zielgruppen, auf welche die jeweilige Maßnahme gerichtet ist, und den Verantwortlichen für deren Umsetzung im Überblick aufgeführt.

TABELLE 40: MAßNAHMENVORSCHLÄGE FÜR DAS HANDLUNGSFELD *FORSCHUNGSFÖRDERUNG UND TESTFELDER*

Maßnahmenvorschlag	**Zielgruppen**	**Maßnahmen-verantwortliche**
Schaffung von Reallaboren/Testfeldern für die praktische Erprobung Erfolg versprechender Sensoranwendungen und zugehöriger Geschäftsmodelle	Anwender & Entwickler von Sensorlösungen	Gesetzgeber/Ministerien, Projektträger, Verbände
Gezielte **F&E-Förderung bzgl. technologieseitiger Verbesserungspotenziale** (z. B. Performanz, Stromverbrauch, Zuverlässigkeit von Komponenten)	Forschungseinrichtungen, Komponenten-, Software-, Sensorhersteller, IKT-Dienstleister	Gesetzgeber/Ministerien, Projektträger
Förderung wissenschaftlicher Begleitforschung, insb. von Analysen des volkswirtschaftlichen und nachhaltigkeitsbezogenen Nutzens von Sensor-anwendungen sowie der sozioökonomischen Folgen ihres Einsatzes	Forschungseinrichtungen	Gesetzgeber/Ministerien, Projektträger

In die inhaltliche Ausarbeitung der Maßnahmenvorschläge dieses Handlungsfeldes sind als eine Grundlage die folgenden Innovationsbarrieren eingeflossen:

- Herausforderungen steigender Systemkomplexität für die Bahntauglichkeit, insbesondere für Wartbarkeit und Skalierbarkeit
- Teilweise noch unzureichender Entwicklungsstand der Technologie
- Teilweise noch unzureichende bzw. unzureichend identifizierte sensorbasierte Trainingsdaten für maschinelle Auswertungen/Interpretationen großer Datensätze in Bahnanwendungen
- Haftungsrisiken aus Fehlfunktionen/Ausfällen
- Hohe Investitionsbedarfe bei noch schwer zu bewertender Rentabilität

Auch wenn im Entwicklungsstand und Reifegrad der Sensortechnologien und der Technologien zur effektiven und effizienten Auswertung sensorbasierter Daten nicht die größten Herausforderungen für einen verstärkten Einsatz von Sensorlösungen im Bahnsystem liegen, so gibt es doch den Bedarf nach weiteren technologischen Verbesserungen und Herausforderungen beim Transfer in marktfähige Produkte und Dienstleistungen.

Als wichtigste Maßnahme in diesem Bereich wurde von den befragten Expertinnen und Experten die Schaffung von Reallaboren und Testfeldern für die praktische Erprobung Erfolg versprechender Sensoranwendungen, aber auch für die zugehörigen Geschäftsmodelle angesehen. Auf diese Weise kann, bei Bedarf wissenschaftlich begleitet, nicht nur die technische Funktions- und Leistungsfähigkeit von Sensorlösungen in der realen Bahnwelt geprüft und validiert, sondern auch die betrieblich-organisatorische Umsetzbarkeit und die wirtschaftliche Tragfähigkeit untersucht werden. Mit den gewonnenen Erkenntnissen aus solchen Reallaboren können Optimierungen an der Technologie, aber auch am konzipierten Geschäftsmodell vorgenommen werden.

Dort, wo es in der Tat noch bedeutsame technologieseitige Verbesserungspotenziale gibt, sollte eine gezielte F&E-Förderung ansetzen. Dies betrifft nach den Analyse- und Interviewergebnissen dieses Projektes insbesondere die Performanz, den Stromverbrauch und die Zuverlässigkeit von einzelnen Elektronikkomponenten im Gesamtsystem einer Sensorlösung. Es erscheint ratsam, mit Hilfe weiterer Studien oder Voruntersuchungen die technologischen F&E-Bedarfe genauer zu spezifizieren, bevor bestimmte F&E-Aktivitäten gezielt gefördert werden.

Zuletzt scheint es ratsam, auch eine wissenschaftliche Begleitforschung zu fördern, um Fortschritte, Auswirkungen und die Effektivität eines verstärkten Sensoreinsatzes im Bahnsystem zu beobachten, zu bewerten und zu analysieren. Hinsichtlich der Auswirkungen sind insbesondere Analysen des volkswirtschaftlichen und nachhaltigkeitsbezogenen Nutzens (ökonomische, ökologische und soziale Verbesserungen) von Sensoranwendungen sowie Analysen der sozioökonomischen Folgen ihres Einsatzes von Interesse.

Das nachfolgende Kapitel befasst sich im Rahmen des entsprechenden Unterkapitels genauer mit den Geschäftsmodellen und einem Ausblick auf die zukünftigen Märkte für Sensoranwendungen im Bahnsystem (Handlungsfeldkategorie Markt). Es hat aber nicht das Ziel (genauere) Handlungsempfehlungen abzuleiten, sondern Einschätzungen zu den im Detail untersuchten Use Cases sowie zu verallgemeinerbaren Einfluss- und Erfolgsfaktoren zu erlangen.

6.2 Marktausblick und Geschäftsmodelle

Dieses Unterkapitel beschäftigt sich mit einer wirtschaftlichen Betrachtung von Sensorlösungen im Bahnsektor. Dies beinhaltet zum einen die Analyse neuer bzw. veränderter Geschäftsmodelle mit den zugehörigen Wertschöpfungsstufen und Marktrollen und zum anderen die – primär qualitative – Beurteilung von Marktpotenzialen und Marktaussichten („Marktausblick“). Als Grundlage für diese Arbeiten

dienen vor allem die Erkenntnisse des Kapitels 5 und der dort vorgenommenen Analyse von Stakeholderbeziehungen. Methodische Basis war ein zweiter Expertinnen- und Experten-Workshop, welcher wieder Vertreterinnen und Vertreter der beiden Hauptgruppen der Bereitsteller sensorbasierter Lösungen sowie der Bahnanwender (Hersteller, Betreiber und Instandhalter von Schienenfahrzeugen und -infrastruktur) zusammenbrachte und gemeinsam diskutieren ließ.

Für die wirtschaftlichen Untersuchungen und die Workshopkonzeption wurde wieder auf die sieben in Kapitel 4 festgelegten Use Cases für Detailanalysen zurückgegriffen. In den nachfolgenden Unterabschnitten werden die konzeptionellen Vorbereitungen und die Ergebnisse vorgestellt.

6.2.1 Vorbereitung

Für die beiden Aufgabenbereiche – Geschäftsmodellbetrachtung und Marktausblick – wurde jeweils ein Workshoptag mit einer Gesamtdauer von je knapp sechs Stunden und einer effektiven Gruppenarbeitszeit von 120 bzw. 150 Minuten im Rahmen eines zweitägigen Workshops mit technologischem Rahmenprogramm (optionale Bahnfahrt auf dem Digitalen Testfeld Erzgebirge) vorgesehen. Die in den Kleingruppen erarbeiteten Ergebnisse zu beiden Aufgabenbereichen wurden am Ende wieder gruppenübergreifend diskutiert und Use Cases übergreifend konsolidiert.

Analog zum ersten Workshop wurden für die Aufgabenbearbeitung und Gruppendiskussionen wieder drei moderierte Kleingruppen gebildet, in denen die Geschäftsmodelle bzw. die Marktpotenziale für jeweils zwei Sensoranwendungen einer genaueren Betrachtung unterzogen wurden. Die eingeladenen Expertinnen und Experten konnten dabei vorab ihre Präferenzen für die sieben zur Auswahl gestandenen Detailanalyse-Use Cases mit einer Priorität von 1 (= höchste Präferenz) bis 4 kundtun. Die Zuordnung der Use Cases und der Expertinnen und Experten zu den drei Gruppen erfolgte dann derart, dass den individuell geäußerten Präferenzen bestmöglich entsprochen werden konnte. In der folgenden Tabelle sind neben den entsprechenden Zuordnungen auch Indikatoren für das Interesse an den Use Cases sowie die letztliche Anzahl der teilnehmenden Expertinnen und Experten je Gruppe ersichtlich. Insgesamt nahmen 21 Expertinnen und Experten am zweiten Workshop teil.

TABELLE 41: KLEINGRUPPENZUORDNUNG WORKSHOP 2

Use Case	Infra überwacht Fzg. nicht sicherheitsrelevant	Fzg. überwacht Fzg.: Zustand Türen u. a. Verriegelungen	(Teil-)Automatisierung der Fahrzeuginstandhaltung	Fzg. überwacht Fzg. Antriebszustand (Elektro)	Fzg. überwacht Oberbau	Fzg.-Lokalisierung fahrzeugseitig sicherheitsrelevant	Weichenferndiagnose
Anzahl der Nennungen bei der Priorisierung	**16**	**11**	**17**	**8**	**11**	**21**	**8**
Durchschnittliche Priorität	**2,4**	**2,5**	**2,4**	**2,9**	**2,4**	**2,3**	**3,1**
Erfolgte Diskussion bereits in WS 1?			**X**		**X**	**X**	
	Gruppe A (4 Expertinnen und Experten)		**Gruppe B (7 Expertinnen und Experten)**		**Gruppe C (10 Expertinnen und Experten)**		

Das größte Interesse der Expertinnen und Expertien bestand an der Sensoranwendung Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant (21 Nennungen). Die Durchschnittsprioritäten für die Use Cases lagen grundsätzlich nah beieinander (im Bereich um den Wert 2,4). Nur die beiden Use Cases Fahrzeug überwacht Fahrzeug Antriebszustand (Elektro) und Weichenferndiagnose stießen auf geringeres Interesse, was auch an den geringeren Nennungen bei der Priorisierung erkennbar ist. Letzterer Use

Case (mit der geringsten Durchschnittspriorität) fiel aus der Berücksichtigung im Workshop heraus, da in den drei Gruppen nur insgesamt sechs Sensoranwendungen betrachtet werden konnten.

Nachfolgend werden die konzeptionellen und methodischen Vorarbeiten und damit das Vorgehen des zweiten Workshops getrennt nach den beiden Aufgabenbereichen des Kapitels dargestellt.

Aufgabenbereich Geschäftsmodellbetrachtung

Für die Geschäftsmodellbetrachtung wurde in Anlehnung an [64] das nachfolgende Begriffsverständnis genutzt: Ein Geschäftsmodell beschreibt, wie ein Unternehmen Werte schafft (*Leistungserbringung*), diese an Kundinnen und Kunden bzw. Partnerinnen und Partner überträgt (*Leistungsbereitstellung*) sowie für sich selbst vereinnahmt (*Gewinnerzeugung*) und wie es sein *Leistungsangebot kommuniziert* (vgl. Abbildung 28).

Abbildung 28: Bestandteile von Geschäftsmodellen [Eigene Darstellung nach [64]]

In der Abbildung sind die Inhalte der vier genannten Geschäftsmodell-Dimensionen jeweils mit zwei W-Fragen weiter untersetzt. Im Rahmen des Workshops konnten und sollten nicht alle Geschäftsmodell-Dimensionen detailliert für die sechs betrachteten Use Cases erarbeitet werden. Vielmehr wurde sich auf eine Betrachtung des Leistungsangebots als Kerns eines jeden Geschäftsmodells konzentriert.

Das Leistungsangebot eines Geschäftsmodells ergibt sich aus seinen zentralen Wert- bzw. Nutzenversprechen gegenüber den Kundinnen und Kunden. Als methodisches Hilfsmittel für die Herleitung des

Leistungsangebots aus vorhandenen Kundenbedürfnissen wurde die *Value Proposition Canvas* von Osterwalder et al. ausgewählt. Diese Methode weist neben ihrer ausgeprägten Markt- und Kundenorientierung die Vorteile einer vergleichsweise einfachen Systematik und intuitiv nachvollziehbaren Vorgehensweise und damit einer hohen Eignung für Workshoparbeit auf. Die übersichtliche Canvas (deutsch: Leinwand) besteht aus zwei Bereichen, welche die Kundenseite und die Anbieterseite repräsentieren, mit jeweils drei Feldern. Eine erklärende Darstellung der Value Proposition Canvas zeigt, adaptiert auf das hier im Fokus stehende Untersuchungsobjekt der Sensorlösungen, die Abbildung 29.

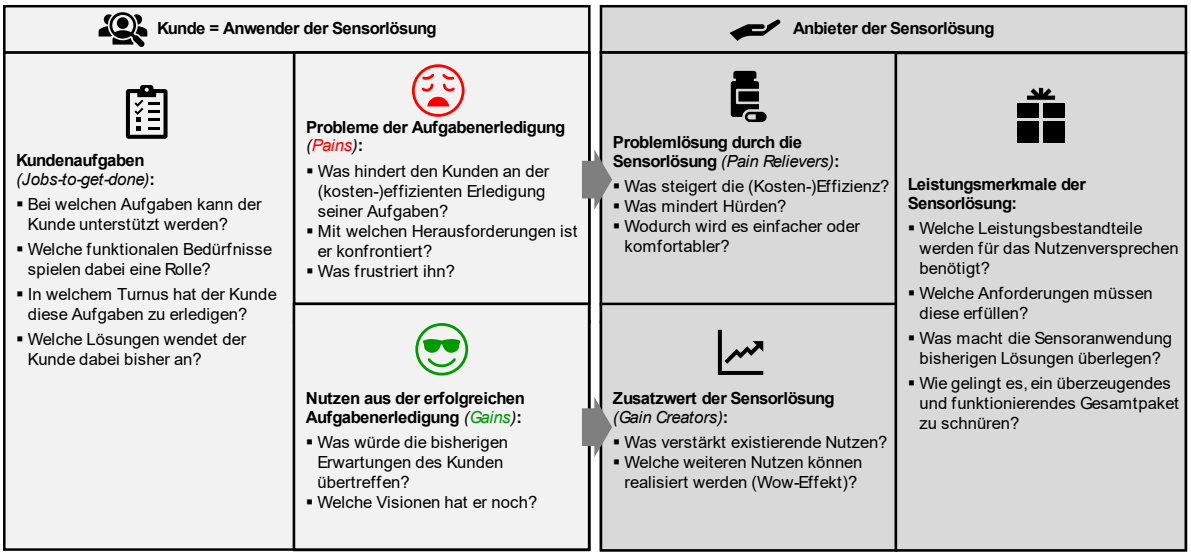


Abbildung 29: Value Proposition Canvas zur Herleitung des Wertversprechens eines Geschäftsmodells [TU Chemnitz, BWL III]

Die Felder der Canvas werden in der Gruppendiskussion von links nach rechts durchlaufen und ausgefüllt. Ausgangspunkt ist die Einnahme der Perspektive potenzieller Anwender von Sensorlösungen und die Überlegung, welche Aufgaben und Teilaufgaben zu ihrer typischen Geschäftstätigkeit gehören (die sog. *Jobs-to-get-done*). Zur Auseinandersetzung mit den Kundenaufgaben gehören auch Antworten auf die Fragen, welche Bedürfnisse, Anforderungen und Rahmenbedingungen dabei jeweils eine Rolle spielen und welche Lösungen (mit oder ohne Sensorik) bisher zu Anwendung kommen. Ausgehend von den Kundenaufgaben werden dann in den beiden benachbarten Feldern der Canvas die bisherigen Probleme bei der Aufgabenerfüllung (sog. *Pains*) und die sich aus einer erfolgreichen Aufgabenerfüllung ergebenden Nutzen (sog. *Gains*) genauer betrachtet und spezifiziert. Um mit dem Einsatz einer neuen Sensorlösung einen Mehrwert generieren und ein entsprechendes Wertversprechen formulieren zu können, müssen genau diese Probleme oder Nutzen angesprochen werden. Dies geschieht entweder dadurch, dass existierende Probleme bei der Aufgabenerledigung durch den Einsatz der Sensorlösung reduziert, gelindert oder beseitigt werden (sog. *Pain Relievers*) oder dass mit dem Einsatz der Sensorlösung ein größerer oder zusätzlicher Nutzen aus der Aufgabenerfüllung erlangt werden kann (sog. *Gain Creators*). Für die Betrachtung dieser beiden Wege und die Herleitung entsprechender Ansatzpunkte werden die beiden benachbarten Canvas-Felder genutzt, welche nun der Kundenperspektive spiegelbildlich die Anbieterperspektive gegenüberstellen. In einem letzten Schritt werden schließlich aus den identifizierten Pain Relievers und Gain Creators die korrespondierenden Produkt- bzw. Dienstleistungsbestandteile der Sensorlösung aus Anbietersicht mit entsprechenden Leistungsmerkmalen charakterisiert. Das gesuchte Wertversprechen gegenüber der Kundin oder dem Kunden manifestiert sich letztlich in den Vorteilen dieser Leistungsmerkmale gegenüber denen der bisher bei der Kundin oder beim Kunden eingesetzten Produkte bzw. Dienstleistungen.

Die Kleingruppendiskussion zur Geschäftsmodellbetrachtung am ersten Workshoptag wurde hinsichtlich des Arbeitsablaufs in drei Teile gegliedert, die jeweils für beide der einer Gruppe zugeordneten Sensoranwendungen durchlaufen wurden:

1. Zunächst erfolgte eine Kurzvorstellung des Use Cases (durch Gruppenmoderatorinnen und -moderatoren) anhand des visualisierten Einsatzszenarios und einer Übersicht der involvierten Stakeholder (Arbeitsergebnis aus Kapitel 5.2). Dies diente dazu, ein gemeinsames Verständnis aller Gruppenmitglieder zu schaffen, und es bestand die Möglichkeit, das vorgeschlagene Stakeholderbild anzupassen.

2. Anschließend wurde die Kundenseite der Value Proposition Canvas betrachtet, indem (a) das Kundensegment (= potenzielle Anwender der Sensorlösung) konkretisiert wurde, dessen Perspektive eingenommen werden soll, (b) die Gruppenteilnehmer zunächst jeder für sich – mithilfe beschreibbarer Kärtchen – Einschätzungen zur Kundenaufgabe, zu den Pains und zu den Gains abgaben und (c) schließlich in der gemeinsamen Diskussion die Ergebnisse für diese drei Felder konsolidiert wurden.
3. Zuletzt wurde sich in einer gemeinsamen Diskussion der Anbieterseite der Value Proposition Canvas gewidmet, dabei die potenziellen Anbieter einer zugehörigen Sensorlösung konkretisiert und die drei Canvas-Felder als Spiegelbild der Kundenperspektive ausgefüllt.

Als ergänzende Aufgabe zur Geschäftsmodellbetrachtung wurden die Expertinnen und Experten zu Beginn des zweiten Workshoptages nach der kleingruppenübergreifenden Vorstellung und Diskussion der Ergebnisse des Vortages (Inhalte der jeweiligen Value Proposition Canvas) gebeten, Einschätzungen hinsichtlich des **Veränderungspotenzials bzw. Neuheitscharakters der Geschäftsmodelle** abzugeben. Hierfür wurden jeder Expertin bzw. jedem Experten

- zwei blaue Klebepunkte zur Markierung von Sensoranwendungen, die zu stark veränderter Geschäftsmodellen (mit ggf. veränderten Wertschöpfungsstrukturen) führen, und
- zwei gelbe Klebepunkte zur Markierung von Sensoranwendungen, die zu völlig neuen Geschäftsmodellen (mit ggf. auch neuartigen Wertschöpfungsstrukturen) führen

ausgehändigt. Diese konnten frei auf die sechs im Workshop betrachteten Use Cases verteilt werden.

Aufgabenbereich Marktausblick

Für den Marktausblick der Use Cases stellten die ausgefüllten Felder der Value Proposition Canvas die Grundlage hinsichtlich der zu bewertenden Geschäftsmodelle dar. Für eine entsprechende Marktbewertung im Rahmen des Workshops wurde – wieder unter Nutzung der Portfoliotechnik des Strategischen Managements – ein eigenes **Bewertungsportfolio** konzipiert. Auf Basis von Vorgesprächen und eigener existierender Vorarbeiten zu Marktbewertungsportfolios (in anderen Anwendungskontexten) wurden die folgenden beiden primär relevanten Dimensionen, heruntergebrochen auf jeweils vier Bewertungskriterien, identifiziert und genutzt:

1. die **Marktattraktivität** aus Sicht der Anbieter von Sensorlösungen mit der dahinterliegenden Frage, wie lohnenswert eine Markterschließung ist, und den Kriterien
    a. **erwartetes Marktpotenzial** (künftiges Marktvolumen und Marktwachstum dahin)
    b. **erwartete Rentabilität** (Gewinnaussichten im Verhältnis zum eingesetzten Kapital)
    c. **Umfeldbedingungen des Marktes** (positive oder negative Einflüsse von Seiten Recht, Politik und öffentliche Meinung)
    d. **Potenziale der Sensorprodukte** (Möglichkeiten zur technologischen Weiterentwicklung oder zur Nutzbarmachung von Synergien im Produktportfolio des Anbieters)
2. die **Marktreife** der Sensorlösung mit der dahinterliegenden Frage, wie nah sie an einem Zustand ist, in dem sie am Markt verkauft und von den Anwendern sinnvoll genutzt werden kann, und den Kriterien
    a. **Verfügbarkeit der Sensorlösung** (tatsächliche Möglichkeit eines Erwerbs zu marktgerechten Preisen gegenüber einem Prototypenstatus und evtl. weiterem F&E-Bedarf)
    b. **Zulassungsfähigkeit der Sensorlösung** (gemäß geltender Regularien im Bahnsystem)
    c. **Know-how der potenziellen Sensoranwender** (Fähigkeit, gewonnene Sensordaten oder daraus abgeleitete Informationen auszuwerten und sinnvoll zu nutzen)
    d. **Strategische Ausgereiftheit der Geschäftsmodelle & -beziehungen** (Klarheit und Stabilität der ggf. völlig neuartigen Geschäftsmodelle, insbesondere der Rollenverteilungen und Erlösmodelle)

Die Ausprägungen der jeweils vier Einzelkriterien in den beiden Dimensionen Marktattraktivität und Marktreife waren von den Expertinnen und Experten auf einer einheitlichen Skala von 1 (= ungenügend) bis 5 (= sehr gut) zu bewerten. Für die Auswertung wurden durchschnittliche Expertinnen- und Expertenbewertungen (arithmetisches Mittel) und deren Streuung (empirische Standardabweichung) für die Einzelkriterien berechnet und die Bewertungen für die Dimensionen (unter Annahme einer Gleichgewichtung der jeweiligen Kriterien) zusammengefasst. Als grafisches Bewertungsergebnis resultiert daraus eine Position in der in den Wertebereichen 1 bis 5 aufgespannten Matrix, siehe Abbildung 30.

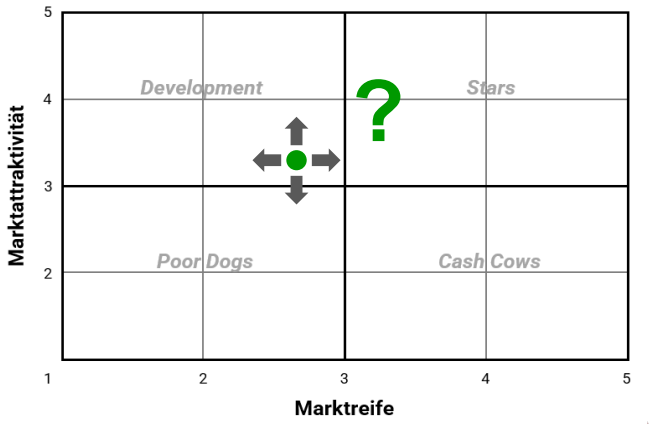


Abbildung 30: Marktbewertungsportfolio für die Geschäftsmodelle von Sensoranwendungen [TU Chemnitz, BWL III]

Je weiter rechts oben (in Richtung einer 5-5-Bewertung) eine Sensoranwendung bzw. ihr Geschäftsmodell aufgrund ihrer Durchschnittsbewertung im Portfolio liegt, umso wahrscheinlicher ist die praktische Umsetzung in absehbarer Zeit. In Anlehnung an das sehr bekannte und in der Praxis häufig genutzte Portfolio der Boston Consulting Group, welches auf den Konzepten des Produktlebenszyklus und der Erfahrungskurve fußt, wurde die Matrix in vier Felder mit den nachfolgenden Bezeichnungen und Interpretationen eingeteilt:

- „Poor Dogs“: mit relativ geringer Marktattraktivität und relativ geringer Marktreife: eine Markterschließung neuer Anwendungen in diesem Bereich durch Anbieter von Sensorlösungen ist kaum zu erwarten; sofern Anbieter bereits Forschung und Entwicklung für solche Use Cases betrieben, ist eher mit einem Zurückstellen oder Ausstieg aus diesen Aktivitäten zu rechnen
- „Cash Cows“: mit relativ geringer Marktattraktivität und relativ hoher Marktreife: Anbieter, die bereits über marktreife bzw. marktnahe Produkte verfügen, werden diese im Sinne einer Mitnahmestrategie vermarkten und verwerten, aber kaum weitere Investitionen dafür tätigen; mit einem Markteintritt von Neueinsteigern ist eher nicht zu rechnen
- „Development“: mit relativ hoher Marktattraktivität und relativ geringer Marktreife: hier ist mit verstärkten Entwicklungsaktivitäten bzw. -bedarfen für Produkte und Systemlösungen von potenziellen Anbietern zu rechnen, um diese zu einer Marktreife zu führen und künftig entsprechende (neue) Märkte im Bahnsektor zu erschließen; in diesem Feld befinden sich die relevantesten Use Cases für die Ableitung von Handlungsempfehlungen zur Überwindung bestehender Innovationsbarrieren, insbesondere mit Blick auf das Bewertungskriterium 1c (Umfeldbedingungen des Marktes)
- „Stars“: mit relativ hoher Marktattraktivität und relativ hoher Marktreife: hier ist – sofern nicht bereits geschehen – zeitnah mit Markteintritten von Anbietern von Sensorlösungen mit entsprechenden Produkten und Dienstleistungen zu rechnen, in diesem Feld befinden sich die zeitlich relevantesten Use Cases für das Erscheinen neuer oder veränderter Geschäftsmodelle

Für das methodische **Vorgehen** im Workshopteil der Marktbewertung wurde ein Ablauf in mehreren Schritten in Anlehnung an die Delphi-Methode gewählt. Bei der Delphi-Methode wird eine schriftliche Befragung mehrerer Einzelpersonen mit Fachexpertise mehrfach wiederholt, wobei ab der zweiten Runde ein Feedback in anonymisierter Form gegeben wird, wie die anderen Expertinnen und Experten geantwortet haben, und dabei ggf. eine Präzisierung des Untersuchungsobjekts erfolgt. Vorteile dieses Vorgehens sind ein Entgegenwirken der üblichen Gruppendynamik mit sehr dominanten Personen und die Möglichkeit, eigene Ersteinschätzungen in einem Prozess der Meinungsbildung auf Basis des erhaltenen Feedbacks und eigener Reflexionen zu überdenken und ggf. zu korrigieren. Dies kann sowohl zu einer Konsensbildung in der Gruppe als auch zur Schärfung konkurrierender Hauptmeinungsbilder führen. Der konzipierte und durchgeführte Ablauf im Workshop war wie folgt:

1. Erläuterung, Kurzdiskussion und Klärung von Verständnisfragen zu den zwei Dimensionen und je vier Kriterien des Bewertungsportfolios (durch Gruppenmoderatorin oder -moderator)
2. Individuelles Ausfüllen des tabellarischen Bewertungsbogens (Werte im Bereich 1 bis 5 für jedes Einzelkriterium) für die betrachtete Sensoranwendung durch jedes Kleingruppenmitglied als Erstbewertung
3. Auswertung der Erstbewertungen (Mittelwertberechnung und grafische Darstellung der Position im Portfolio) sowie gemeinsame Gruppendiskussion zu den Kriterieneinschätzungen beider Dimensionen und zugehörigen Begründungen auf dieser Basis
4. Erneutes individuelles Ausfüllen des tabellarischen Bewertungsbogens (Werte im Bereich 1 bis 5 für jedes Einzelkriterium) für die betrachtete Sensoranwendung durch jedes Kleingruppenmitglied als Zweitbewertung nach der Diskussion
5. Auswertung der Zweitbewertungen (Mittelwertberechnung und grafische Darstellung der Position im Portfolio) sowie abschließende Gruppendiskussion der resultierenden (Neu-)Positionierung im Marktbewertungsportfolio mit Möglichkeit einer finalen Anpassung (z. B. Einzeichnen eines breiteren Unschärfebereichs der Bewertung)

Die Schritte 2 bis 5 wurden nach der Bearbeitung für die erste einer Gruppe zugeordnete Sensoranwendung für die zweite Anwendung wiederholt.

Als ergänzende Aufgabe zum Marktausblick sollten die Expertinnen und Experten Überlegungen zum potenziellen Marktvolumen für zur jeweiligen Sensorlösung gehörende Produkte im Sinne einer Umsatzpotenzialanalyse anstellen – was einer Konkretisierung des Marktbewertungskriteriums 1a (erwartetes Marktpotenzial) entspricht. Dabei sollten die relevanten Bezugsgrößen für die Mengen- und Preiskomponenten potenzieller Umsatzvolumen durchdacht und diskutiert werden (z. B. Preise bezogen auf Sensorstückzahlen, auf Datenmengen oder auf die Anzahl von erbrachten Leistungsvorgängen; Absatzmengen abgeleitet aus Flottengrößen von Schienenfahrzeugen oder aus der Länge des Streckennetzes) und dort, wo möglich, auch Größenordnungen abgeschätzt werden. Das Format für diese Aufgabe war eine offene Gruppendiskussion. Als methodisches Hilfsmittel und grober Diskussionsleitfaden wurde das in Abbildung 31 dargestellte tabellarische Analyseschema konzipiert und zur Verfügung gestellt.

	Kundenbasis		Mengenkomponente (Absatz)			Preiskomponente		Umsatz-potenziale (Schätzung)
Sensorlösung, genauer spezifiziert	**Räumlicher Bezug**, z. B. D, EU, Welt	**Zahl potenzieller Kunden** (Schätzung)	**geeignete Bezugs-größe**, z. B. Anzahl Sfz./ Sfz.-Kompo-nenten, Strecken-netzlängen	**Wert der Bezugs-größe** (Schätzung)	**Bemer-kungen**	**geeignete Bezugsgröße**, z. B. Vorgänge, Datenmengen, Sensorzahl	**im Markt realisierbare Preise** (Schätzung)	

Abbildung 31: Analyseschema für Umsatzpotenziale [TU Chemnitz, BWL III]

Zunächst sollte die Sensorlösung im Sinne eines konkreten Produkts (z. B. Kamera- oder Lidarsensor) oder einer Dienstleistung (z. B. Sensordatenanalyse) spezifiziert werden, dann die Kundenbasis bezogen auf einen geographischen Raum hinsichtlich ihrer Zahl geschätzt werden, bevor die Mengen- und Preiskomponenten von Umsatzpotenzialen genauer diskutiert werden.

6.2.2 Ergebnisse

Nachfolgend werden die Workshopergebnisse getrennt nach den beiden Aufgabenbereichen des Kapitels dargestellt.

Aufgabenbereich Geschäftsmodellbetrachtung

An dieser Stelle werden zunächst die Ergebnisse der Erarbeitung des Wert- und Nutzenversprechens bzw. Leistungsangebotes der Geschäftsmodelle mit Hilfe der Value Proposition Canvas für die sechs betrachteten Use Cases dargestellt. Nach Darstellung der ausgefüllten Canvas werden jeweils die wesentlichsten Diskussionserkenntnisse hinsichtlich der Schlüsselfaktoren für den Erfolg des Geschäftsmodells beschrieben.

Use Case: Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant

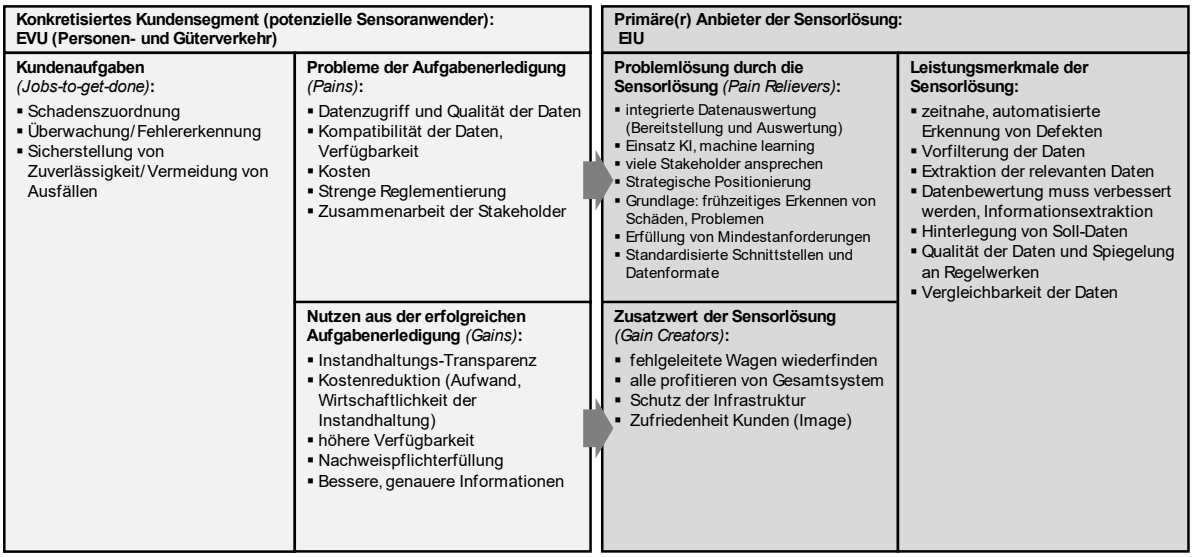


Abbildung 32: Value Proposition Canvas für den Use Case „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“ [TU Chemnitz, BWL III]

Für das potenzielle Geschäftsmodell des Use Cases „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“ (siehe Abbildung 32) ist es von entscheidender Bedeutung, dass eine Motivation der Eisenbahninfrastrukturunternehmen existiert, ein entsprechendes Leistungsangebot für Eisenbahnverkehrsunternehmen überhaupt erst am Markt zu etablieren (sofern es sich nicht um Unternehmen handelt, die in einer Doppelrolle eigene Fahrzeuge auf eigenen Bahnstrecken überwachen). Dabei kommt es auf die faire Verteilung der anfallenden Kosten der Sensorlösung (Anfall erstmal beim EIU) und den resultierenden Nutzen aus ihr (hauptsächlich beim EVU) zwischen Anbieter und Nachfrager über festgelegte Preise an. Wenn der Nutzen des EVU aus den gewonnenen Sensordaten den vom EIU verlangten (bzw. zur Kostendeckung benötigten) Preis nicht hinreichend übersteigt, hat das Geschäftsmodell keine Basis. Als eine wesentliche Kernleistung des Geschäftsmodells wird neben der Erfassung/Bereitstellung von Sensordaten eine möglichst weitgehend automatisierte und prozessintegrierte Auswertung dieser Daten gesehen. Eine Automatisierung der Auswertungsprozesse dient der erforderlichen Kosteneffizienz und eine hohe Prozessintegration (v. a. auch kundenseitig in die (Instandhaltungs-)Prozesse des EVU) dient dazu, dass mit den gewonnenen Daten überhaupt erst sinnvoll etwas angefangen werden kann, ohne dass jeweils arbeits- und kostenintensive manuelle Tätigkeiten ausgeführt werden müssen. Als weiterer wichtiger Schlüsselfaktor, auch in Richtung einer Automatisierung und Prozessintegration, wurde in der Geschäftsmodelldiskussion auf die Bedeutung der Standardisierung von Datenformaten und Datenschnittstellen hingewiesen.

Use Case: Fahrzeug überwacht Fahrzeug – Zustand von Türen und anderen Verriegelungen

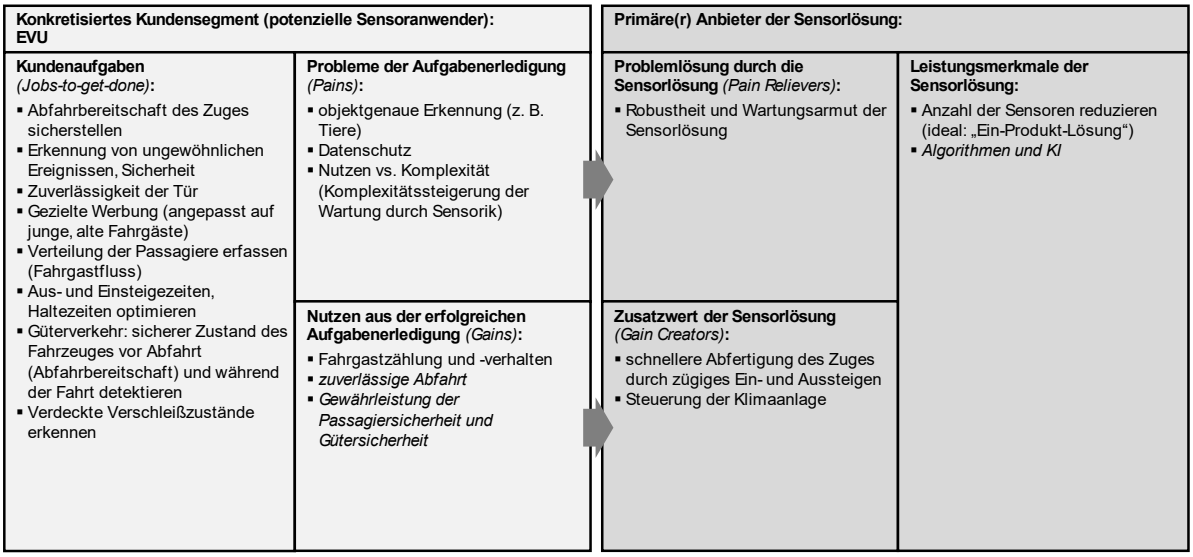


Abbildung 33: Value Proposition Canvas für den Use Case „Fahrzeug überwacht Fahrzeug – Zustand von Türen und anderen Verriegelungen“ [TU Chemnitz, BWL III]

Für das Geschäftsmodell des Use Cases „Fahrzeug überwacht Fahrzeug – Zustand von Türen und anderen Verriegelungen“ (siehe Abbildung 33) wurde die Komplexitätsreduktion und das Kosten-Nutzen-Verhältnis der eingesetzten Sensortechnik als wichtigster Schlüsselfaktor gesehen. Nur wenn mit kostengünstiger Standardsensorik die hohe Zahl an Türen und Verriegelungen von Wagons und Fahrzeugen überwacht werden kann, rechnet sich der Sensoreinsatz. Besondere Herausforderungen werden im Personenverkehrsszenario (z. B. detektierte Türstörungen an Haltepunkten durch Fahrgäste oder sonstige Einflüsse) aufgrund der dort vorherrschenden Komplexität des Anwendungsfalls gesehen. Z. B. sind hier Herausforderungen des Datenschutzes (mögliche Identifikation von Personen) und die oft nur eingeschränkten Behebungsmöglichkeiten einer detektierten Störung zu berücksichtigen.

Use Case: (Teil-)Automatisierung der Fahrzeuginstandhaltung

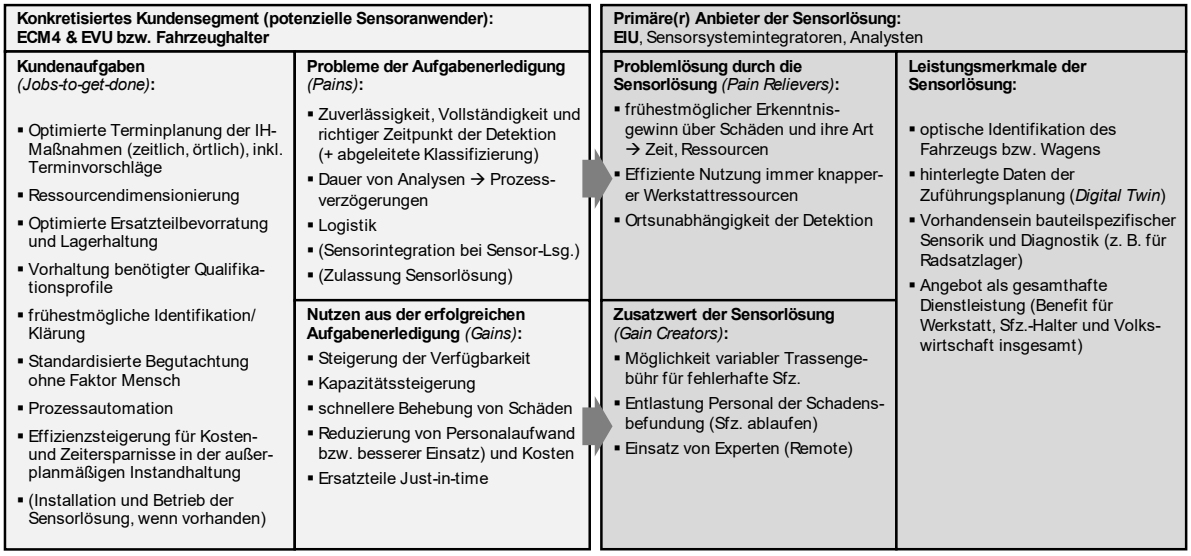


Abbildung 34: Value Proposition Canvas für den Use Case „(Teil-)Automatisierung der Fahrzeuginstandhaltung“ [TU Chemnitz, BWL III]

Für das Geschäftsmodell des Use Cases „(Teil-)Automatisierung der Fahrzeuginstandhaltung“ (siehe Abbildung 34) wurde wieder eine möglichst weitgehend automatisierte und prozessintegrierte Auswertung der erhobenen Sensordaten als eine wesentliche Kernleistung angesehen. Dies ist zum einen wichtig, damit die Fahrzeugwerkstatt in der ECM4-Rolle kosteneffizient und weitgehend naht- und friktionslos aus den mit Hilfe von Sensorik miterhobenen Fahrzeugbefundungsdaten die erforderlichen außerplanmäßigen Instandhaltungsmaßnahmen, inklusive ggf. erforderlicher Bestellprozesse, in die Wege leiten kann. Zum anderen betrifft die Prozessintegration auch den stakeholder- und akteursübergreifenden Datenaustausch zwischen Fahrzeugwerkstatt, Fahrzeughalter und ggf. involvierten Prüfungsdienstleistern unter Wahrung sensibler und schutzwürdiger Daten.

Use Case: Fahrzeug überwacht Fahrzeug – Antriebszustand (Elektro)

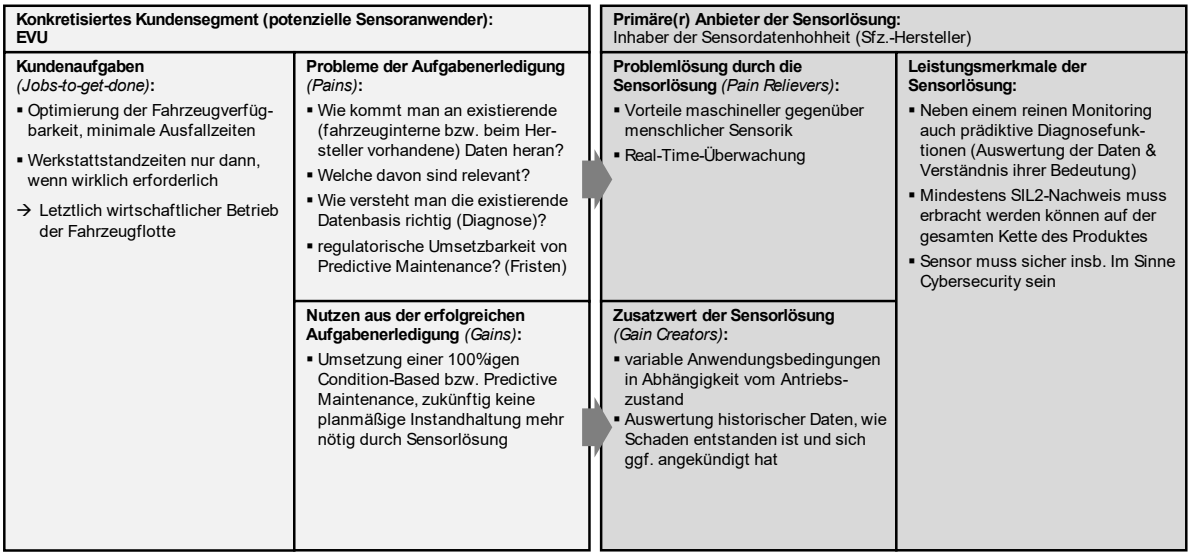


Abbildung 35: Value Proposition Canvas für den Use Case „Fahrzeug überwacht Fahrzeug – Antriebszustand (Elektro)“ [TU Chemnitz, BWL III]

Für das Geschäftsmodell des Use Cases „Fahrzeug überwacht Fahrzeug – Antriebszustand (Elektro)“ (siehe Abbildung 35) wurde ebenfalls eine möglichst weitgehend automatisierte und prozessintegrierte Auswertung der Sensordaten als wichtige Kernleistung identifiziert. Ein Mehrwert entsteht für das EVU als Nutzer erst aus der richtigen Interpretation komplexer Antriebszustandsdaten. Diskutiert wurde zudem die Abhängigkeit des Geschäftsmodells vom Willen des Inhabers der Sensordatenhoheit in Verbindung mit evtl. vorhandener Markt- und Preissetzungsmacht. In vielen Fällen sind und bleiben – je nach Vertragskonstellation mit dem Fahrzeugkäufer – die Schienenfahrzeughersteller Inhaber der Hoheit über (zumindest einen großen Teil der) Antriebszustandsdaten. Befürchtungen von Schienenfahrzeug- bzw. Antriebsherstellern, dass sensible Daten über ihre Technologien (bzw. damit im Zusammenhang stehende Wettbewerbsvorteile oder Schwachstellen) in die falschen Hände abfließen, könnten dem betrachteten Geschäftsmodell entgegenstehen und dafür sorgen, dass Hersteller die Daten nur intern auswerten, anstatt sie mit den EVU zu teilen. Auch für diesen Use Case wurde wieder auf die hohe Bedeutung der Standardisierung von Datenformaten und Datenschnittstellen hingewiesen.

Use Case: Fahrzeug überwacht Oberbau

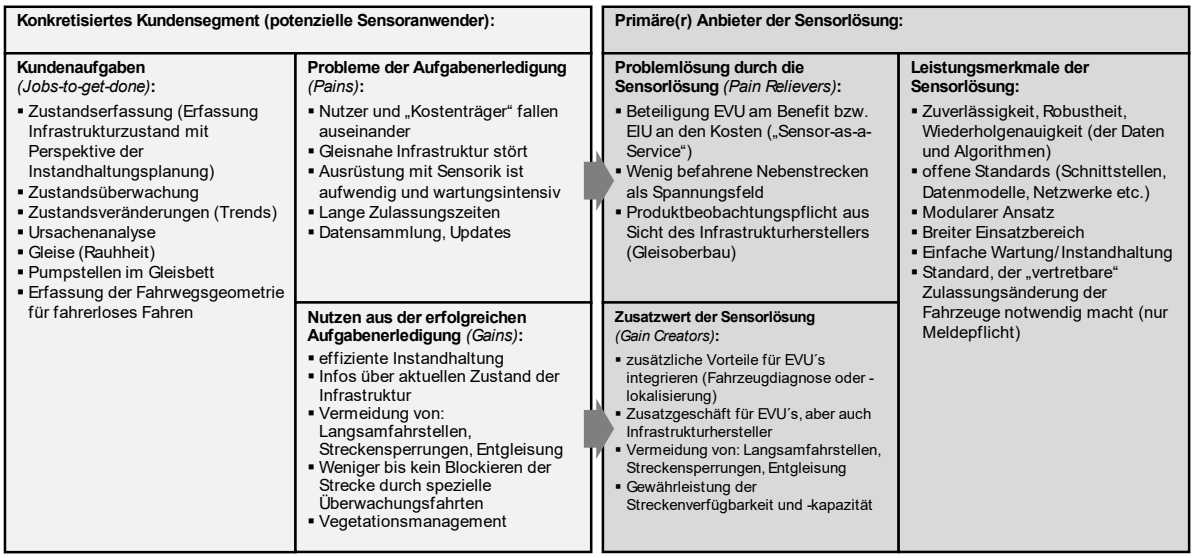


Abbildung 36: Value Proposition Canvas für den Use Case „Fahrzeug überwacht Oberbau“ [TU Chemnitz, BWL III]

Für das Geschäftsmodell des Use Cases „Fahrzeug überwacht Oberbau“ (siehe Abbildung 36) wurde analog zum umgekehrten Anwendungsfall „Infrastruktur überwacht Fahrzeug“ die Motivation der Eisenbahnverkehrsunternehmen entsprechende Leistungsangebote für Eisenbahninfrastrukturunternehmen überhaupt erst am Markt anzubieten als ein wesentlicher Schlüsselfaktor gesehen. Auch hier geht es um eine faire Verteilung der aus dem Sensoreinsatz resultierenden Kosten (Anfall erstmal beim EVU) und Nutzen, wobei zu beachten ist, dass die bei diesem Use Case erhobenen Sensordaten sekundär auch dem EVU bzw. Fahrzeughalter dienen können bzw. dass die dabei im Fahrzeug zum Einsatz kommenden Sensoren in den meisten Fällen zugleich auch anderen Anwendungen dienen, aus denen das EVU selbst den primären Nutzen zieht. Wenn der (Zusatz-)Nutzen des EIU aus den gewonnenen Sensordaten zum Zustand des Oberbaus den vom EVU verlangten Preis nicht hinreichend übersteigt bzw. im Vergleich zu klassischen Alternativen (Fahrten mit Prüffahrzeugen) zu gering ist, hat das Geschäftsmodell keine Basis. Unklarheit herrschte bei diesem Geschäftsmodell darüber, welchem Stakeholder die Aufgabe der Sensordatenauswertung für die richtige Interpretation zuzuordnen ist – eher dem EVU oder dem EIU oder gar einem dritten Datendienstleister. Die Standardisierung von Datenformaten und Datenschnittstellen wurde auch hier wieder als ein Schlüsselfaktor gesehen. Zudem wurde diskutiert, dass für einen hinreichenden Streckendurchsatz (und damit für das Funktionieren des Geschäftsmodells) ein noch zu bestimmender Mindestanteil mit entsprechender Sensorik ausgerüsteter Fahrzeugflotten erforderlich sein wird.

Use Case: Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant

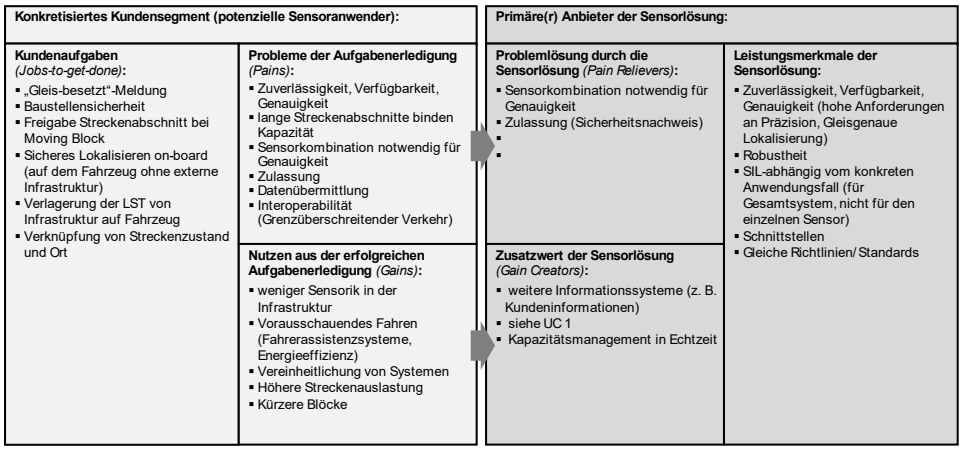


Abbildung 37: Value Proposition Canvas für den Use Case „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant" [TU Chemnitz, BWL III]

Für das Geschäftsmodell des Use Cases „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant" (siehe Abbildung 37) wurde das Vorhandensein umsetzbarer Konzepte für die Systemmigration, ausgehend vom Status Quo, als ein Schlüsselfaktor diskutiert. Ein vollumfänglicher Nutzen dieser Basisanwendung und darauf aufbauender Anwendungen (z. B. im Bereich der Fahrzeugautomatisierung) ist erst bei einer Komplettausrüstung der Fahrzeugflotten gegeben. Demensprechend werden hier gesetzliche Regelungsbedarfe zur Ausschöpfung der Gesamtpotenziale gesehen. Zudem wurde wieder auf die hohe Bedeutung der Standardisierung von Datenformaten und Datenschnittstellen hingewiesen.

Einschätzung des Veränderungspotenzials bzw. Neuheitscharakters der Geschäftsmodelle

In Abbildung 38 sind die Ergebnisse der Klebepunktbewertungen durch die Expertinnen und Experten hinsichtlich des Veränderungsgrades bzw. der Neuartigkeit der Geschäftsmodelle visualisiert.

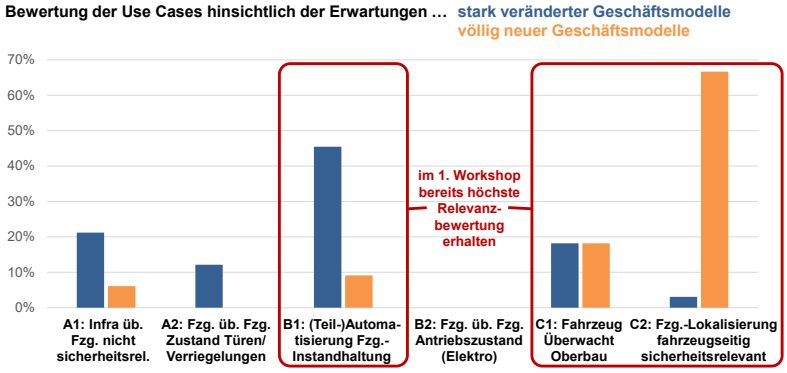


Abbildung 38: Bewertung des Veränderungspotenzials bzw. Neuheitscharakters der Geschäftsmodelle [TU Chemnitz, BWL III]

Die drei Use Cases mit den höchsten Bewertungsergebnissen in diesen beiden Kategorien erhielten bereits im ersten Workshop die höchste Relevanzbewertung (vgl. Abbildung 7 und Abbildung 8). Das heißt, dass bei hinsichtlich der erwarteten Mehrwerte und der erwarteten Umsetzbarkeit bedeutsamen Sensoranwendungen zugleich mit Weiterentwicklungen oder Umbrüchen der Grundmechanismen der Geschäftstätigkeit zu rechnen ist. Das größte Veränderungspotenzial der existierenden Geschäftsmodelle wird beim Use Case „(Teil-)Automatisierung der Fahrzeuginstandhaltung" gesehen. Der höchste Neu-

heitscharakter im Vergleich zu bestehenden Geschäftsmodellen wird beim Use Case „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant“ erwartet. Mit dem Use Case „Fahrzeug überwacht Fahrzeug – Antriebszustand (Elektro)“ werden keine veränderten oder neuen Geschäftsmodelle erwartet. Entsprechende Antriebszustandsdaten werden zum Teil bereits heute verwertet und ergänzen lediglich die Prozesse in weiter fortbestehenden Geschäftsmodellen.

Aufgabenbereich Marktausblick

An dieser Stelle werden zunächst die Einordnungen der Use Cases bzw. ihrer Geschäftsmodelle in das zuvor beschriebene Marktbewertungsportfolio präsentiert, bevor die Ergebnisse der Kriterienbewertungen je Use Case und die jeweils wichtigsten Diskussionspunkte der Workshoparbeit dargestellt werden.

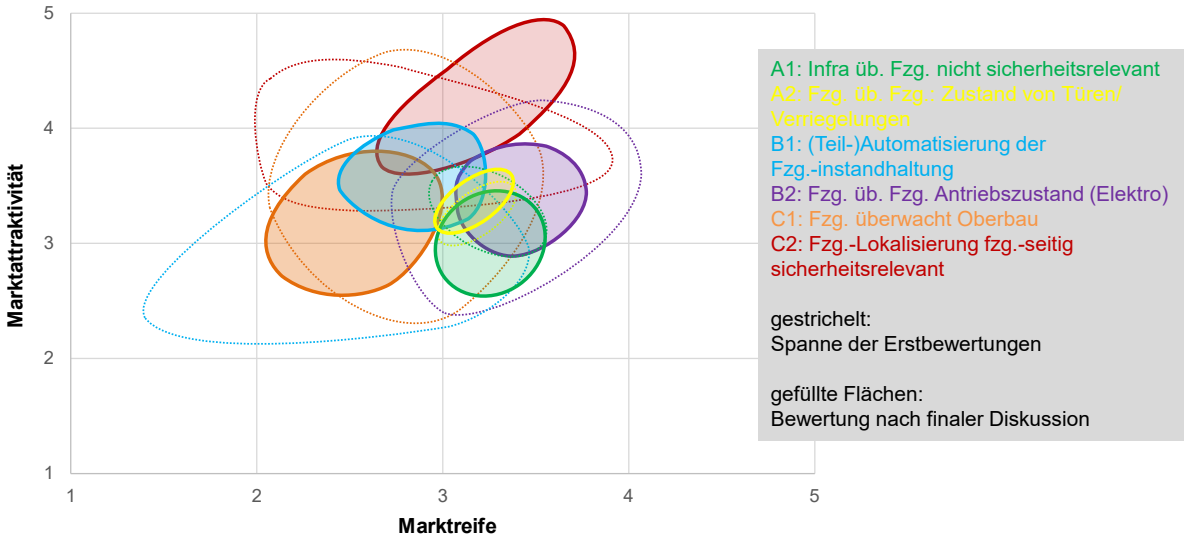


Abbildung 39: Marktbewertungsportfolio mit Verortung aller betrachteter Use Cases gemäß der Expertinnen- und Experteneinschätzungen im Workshop [TU Chemnitz, BWL III]

Als eine grundlegende Tendenz ist aus Abbildung 39 abzulesen, dass es nach den gemeinsamen Kleingruppendiskussionen zu einer Annäherung der Spannweite der Expertinnen- und Expertenmeinungen kam, was so auch zu erwarten war. Die gestrichelt umrahmten Flächen repräsentieren die Ränder der Punktwolken der Einzelmeinungen vor der Diskussion (noch unbeeindruckt von den folgenden Diskussionsinhalten und deren nochmalige Reflexion). Sie sind in den meisten Fällen größer als die farblich korrespondierenden gefüllten Flächen, welche die jeweilige Bewertung nach finaler Diskussion (als im Konsens festgelegter Unschärfebereich auf Basis der Zweitbewertungen) repräsentieren. Sie umrahmen aber meist nicht (zumindest nicht vollständig) die gefüllten Flächen. Dies bedeutet, dass es im Ergebnis der Gruppendiskussion nicht nur zu einer Annäherung der Meinungen, sondern auch zu leichten Verschiebungen im Vergleich zu den Erstbewertungen in die ein oder andere Richtung kam.

Alle sechs Use Cases sind eher in der oberen Hälfte des Portfolios positioniert, das heißt ihre Marktattraktivität wird als vergleichsweise hoch eingeschätzt. Dies deckt sich mit den Erwartungen aus der vorangegangenen Use Case Auswahl für die Detailanalysen, in der gezielt zuvor als relevant (insbesondere im Sinne erwarteter Mehrwerte) eingeschätzte Sensoranwendungen herausgegriffen wurden.

Bei vier der sechs Use Cases wird die Marktreife in der finalen Bewertung bereits überwiegend oberhalb des mittleren Wertes der Skala 1 bis 5 gesehen. Die beiden Use Cases „(Teil-)Automatisierung der Fahrzeuginstandhaltung“ und „Fahrzeug überwacht Oberbau“ weisen hingegen eine Einordnung überwiegend unterhalb dieses mittleren Wertes auf. Die mit Abstand höchste Marktattraktivität wird für den Use Case „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant“ gesehen. Relativ zu den anderen ist

die Einschätzung der Marktattraktivität bei den beiden Use Cases „Fahrzeug überwacht Oberbau“ und „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“ am geringsten.

Nachfolgend wird näher auf die Ergebnisse der einzelnen Use Cases eingegangen. Dabei werden zu Beginn immer tabellarisch die Durchschnittsbewertungen und deren Streuung (als empirische Standardabweichung) in beiden Bewertungsrunden für alle acht Einzelkriterien dargestellt. Besonders niedrige Durchschnittsbewertungen kleiner als 2,5 sind dabei farblich rot und besonders hohe (größer als 3,5) farblich grün hervorgehoben. Streuungen größer 1 sind farblich rot (und kleiner 1 farblich grün) hervorgehoben.

Use Case: Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant

TABELLE 42: MARKTBEWERTUNG USE CASE „INFRASTRUKTUR ÜBERWACHT FAHRZEUG – NICHT SICHERHEITSRELEVANT“ [TU CHEMNITZ, BWL III]

I. Marktattraktivität (Sicht der Anbieter von Sensorlösungen)					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung**	
		Erst-	Zweit-	*Erst-*	*Zweit-*
I.a	**erwartetes Marktpotenzial** (Größe & Wachstum)	**3,3**	**2,7**	*0,6*	*0,6*
I.b	**erwartete Rentabilität**	**3,0**	**2,3**	*0,0*	*0,6*
I.c	**Umfeldbedingungen des Marktes** (Recht, Politik, öffentliche Meinung)	**2,3**	**2,0**	*0,6*	*1,0*
I.d	**Potenziale der Sensorprodukte** (Weiterentwicklung & Synergien)	**4,3**	**4,7**	*0,6*	*0,6*

II. Marktreife					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung**	
		Erst-	Zweit-	*Erst-*	*Zweit-*
II.a	**Verfügbarkeit der Sensorlösung zu marktgerechten Preisen** (versus weiterer F&E-Bedarf)	**4,0**	**3,5**	*0,0*	*0,7*
II.b	**Zulassungsfähigkeit der Sensorlösung im Bahnsystem**	**4,0**	**3,0**	*1,4*	*2,0*
II.c	**Know-how der potenziellen Sensoranwender**	**3,3**	**3,3**	*0,6*	*0,6*
II.d	**Strategische Ausgereiftheit der Geschäftsmodelle & -beziehungen**	**2,3**	**2,3**	*0,6*	*0,6*

* arithmetisches Mittel; Bewertung auf der Skala von 1 (= ungenügend) bis 5 (= sehr gut) ** empirische Standardabweichung

Beim Use Case „Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant“ werden trotz der grundsätzlich als hoch eingeschätzten Potenziale entsprechender Sensorprodukte vor allem die derzeitigen Umfeldbedingungen des Marktes und nach der Diskussion auch die erwartete Rentabilität als kritisch gesehen (siehe Tabelle 42). Hinsichtlich der Marktreife mangelt es nach Meinung der Expertinnen und Experten vor allem an der strategischen Ausgereiftheit der Geschäftsmodelle und -beziehungen, was sich mit den aufgeworfenen Fragen in der vorangegangenen Geschäftsmodelldiskussion (Kosten-Nutzenteilung zwischen EVU und EIU, fehlende Marktanreize, First-Mover-Risiko) deckt. Hinsichtlich der Zulassungsfähigkeit der Sensorlösung im Bahnsystem schwanken die Meinungen der Expertinnen und Experten sehr stark. In der Diskussion zur Marktbewertung wurden zudem die stringenten Reglementierungen im Bahnsektor als ein Hemmnis (insbesondere für den ergänzenden Einsatz von KI-Technologien) sowie das erwartete begrenzte Marktvolumen (nur wenig Systeme im gesamten Streckennetz benötigt) angesprochen.

Use Case: Fahrzeug überwacht Fahrzeug – Zustand von Türen und anderen Verriegelungen

TABELLE 43: MARKTBEWERTUNG USE CASE „FAHRZEUG ÜBERWACHT FAHRZEUG – ZUSTAND VON TÜREN UND ANDEREN VERRIEGELUNGEN“ [TU CHEMNITZ, BWL III]

I. Marktattraktivität (Sicht der Anbieter von Sensorlösungen)					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung***	
		Erst-	Zweit-	*Erst-*	*Zweit-*
I.a	**erwartetes Marktpotenzial** (Größe & Wachstum)	**2,7**	**3,3**	*0,6*	*0,6*
I.b	**erwartete Rentabilität**	**3,0**	**3,0**	*1,0*	*0,0*
I.c	**Umfeldbedingungen des Marktes** (Recht, Politik, öffentliche Meinung)	**3,0**	**2,7**	*1,0*	*1,2*
I.d	**Potenziale der Sensorprodukte** (Weiterentwicklung & Synergien)	**4,0**	**4,3**	*1,0*	*0,6*

II. Marktreife					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung***	
		Erst-	Zweit-	*Erst-*	*Zweit-*
II.a	**Verfügbarkeit der Sensorlösung zu marktgerechten Preisen** (versus weiterer F&E-Bedarf)	**3,5**	**3,0**	*0,7*	*0,0*
II.b	**Zulassungsfähigkeit der Sensorlösung im Bahnsystem**	**3,0**	**2,3**	*1,4*	*0,6*
II.c	**Know-how der potenziellen Sensoranwender**	**3,3**	**3,7**	*0,6*	*0,6*
II.d	**Strategische Ausgereiftheit der Geschäftsmodelle & -beziehungen**	**2,7**	**3,7**	*0,6*	*0,6*

* arithmetisches Mittel; Bewertung auf der Skala von 1 (= ungenügend) bis 5 (= sehr gut) ** empirische Standardabweichung

Beim Use Case „Fahrzeug überwacht Fahrzeug – Zustand von Türen und anderen Verriegelungen“ werden ebenfalls sehr hohe Potenziale der Sensorprodukte gesehen (siehe Tabelle 43). Die restlichen Kriterien der Marktattraktivität erhielten eine mittlere Bewertung. Die Marktreife wird insbesondere hinsichtlich des Know-hows der Sensoranwender und der Ausgereiftheit der Geschäftsmodelle als hoch angesehen. Die Zulassungsfähigkeit der Sensorlösung im Bahnsystem wird nach der gemeinsamen Diskussion hingegen als kritisch beurteilt. In der zugehörigen Diskussion wurde dieser Use Case als ein Wachstumsmarkt bezeichnet, der jedoch wenig innovationsgetrieben ist und bei dem es eher um die Weiterentwicklung existierender Technik geht. Als wichtiges Problem wurde die unzureichende, aber auch unattraktive Standardisierung genannt. Aufgrund der sehr kurze Innovationszyklen von Digital- und Sensortechnologien ist eine Standardisierung für die langen Lebenszyklen von Schienenfahrzeugen häufig wenig sinnvoll.

Use Case: (Teil-)Automatisierung der Fahrzeuginstandhaltung

TABELLE 44: MARKTBEWERTUNG USE CASE „(TEIL-)AUTOMATISIERUNG DER FAHRZEUGINSTANDHALTUNG“ [TU CHEMNITZ, BWL III]

I. Marktattraktivität (Sicht der Anbieter von Sensorlösungen)					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung**	
		Erst-	Zweit-	*Erst-*	*Zweit-*
I.a	**erwartetes Marktpotenzial** (Größe & Wachstum)	**3,3**	**4,1**	*1,2*	*0,6*
I.b	**erwartete Rentabilität**	**2,6**	**3,5**	*0,7*	*0,8*
I.c	**Umfeldbedingungen des Marktes** (Recht, Politik, öffentliche Meinung)	**2,7**	**2,7**	*1,0*	*0,5*
I.d	**Potenziale der Sensorprodukte** (Weiterentwicklung & Synergien)	**3,3**	**3,9**	*1,2*	*0,6*

II. Marktreife					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung**	
		Erst-	Zweit-	*Erst-*	*Zweit-*
II.a	**Verfügbarkeit der Sensorlösung zu marktgerechten Preisen** (versus weiterer F&E-Bedarf)	**2,6**	**2,8**	*0,9*	*1,0*
II.b	**Zulassungsfähigkeit der Sensorlösung im Bahnsystem**	**3,1**	**2,9**	*1,0*	*1,2*
II.c	**Know-how der potenziellen Sensoranwender**	**2,5**	**3,1**	*1,1*	*0,6*
II.d	**Strategische Ausgereiftheit der Geschäftsmodelle & -beziehungen**	**2,0**	**2,5**	*0,5*	*0,8*

* arithmetisches Mittel; Bewertung auf der Skala von 1 (= ungenügend) bis 5 (= sehr gut) ** empirische Standardabweichung

Beim Use Case „(Teil-)Automatisierung der Fahrzeuginstandhaltung“ wurden nach der gemeinsamen Diskussion insbesondere das erwartete Marktpotenzial und die Potenziale der Sensorprodukte (für Weiterentwicklungen und Synergien) als sehr hoch eingeschätzt (siehe Tabelle 44). Hinsichtlich der Marktattraktivität näherten sich die Meinungen der Expertinnen und Experten bezüglich der einzelnen Kriterien einander an (abnehmende Streuung). Eher kritisch wurde die strategische Ausgereiftheit der Geschäftsmodelle und -beziehungen gesehen, insbesondere bei der Erstbewertung. In der zugehörigen Diskussion wurde darauf verwiesen, dass derzeit noch kein wirklich vermarktbares Produkt existiert, weil für die Interpretation der Masse an anfallenden Daten und für die Zuverlässigkeit der zugehörigen Schadensklassifizierung erst noch praktische Erfahrungen gesammelt werden müssen. Auch die Auditierbarkeit bzw. Zertifizierbarkeit entsprechender Systeme sei momentan noch schwierig. Herausforderungen bestehen darüber hinaus darin, Verfügbarkeitssteigerungen von Schienenfahrzeugen auf Basis frühzeitig erkannter Schäden in wirtschaftliche Potenziale umzurechnen und dann den Beitrag der Sensorlösung daran zu eruieren.

Use Case: Fahrzeug überwacht Fahrzeug – Antriebszustand (Elektro)

TABELLE 45: MARKTBEWERTUNG USE CASE „FAHRZEUG ÜBERWACHT FAHRZEUG – ANTRIEBSZUSTAND (ELEKTRO)“ [TU CHEMNITZ, BWL III]

I. Marktattraktivität (Sicht der Anbieter von Sensorlösungen)					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung**	
		Erst-	Zweit-	*Erst-*	*Zweit-*
I.a	**erwartetes Marktpotenzial** (Größe & Wachstum)	**3,3**	**3,8**	*1,0*	*0,5*
I.b	**erwartete Rentabilität**	**3,4**	**3,5**	*0,8*	*0,5*
I.c	**Umfeldbedingungen des Marktes** (Recht, Politik, öffentliche Meinung)	**2,9**	**3,7**	*0,9*	*1,0*
I.d	**Potenziale der Sensorprodukte** (Weiterentwicklung & Synergien)	**4,1**	**3,5**	*0,6*	*1,2*

II. Marktreife					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung**	
		Erst-	Zweit-	*Erst-*	*Zweit-*
II.a	**Verfügbarkeit der Sensorlösung zu marktgerechten Preisen** (versus weiterer F&E-Bedarf)	**3,9**	**3,5**	*0,6*	*0,9*
II.b	**Zulassungsfähigkeit der Sensorlösung im Bahnsystem**	**4,0**	**4,0**	*0,5*	*0,8*
II.c	**Know-how der potenziellen Sensoranwender**	**3,5**	**2,9**	*1,2*	*0,8*
II.d	**Strategische Ausgereiftheit der Geschäftsmodelle & -beziehungen**	**2,5**	**2,6**	*0,9*	*0,9*

* arithmetisches Mittel; Bewertung auf der Skala von 1 (= ungenügend) bis 5 (= sehr gut) ** empirische Standardabweichung

Beim Use Case „Fahrzeug überwacht Fahrzeug – Antriebszustand (Elektro)“ wurden nach der Diskussion vor allem das erwartete Marktpotenzial und die Umfeldbedingungen des Marktes als sehr gut bewertet (siehe Tabelle 45). Auch die Zulassungsfähigkeit der Sensorlösung im Bahnsystem wurde als sehr hoch eingeschätzt, da es sich um Anwendungen handelt, die zu Teilen bereits eingesetzt werden. Vergleichsweise hoch ist auch die Verfügbarkeit der Sensorlösung, zumindest was die Datenerfassung angeht. In der zugehörigen Diskussion wurde darauf verwiesen, dass das Know-How der Anwender sich noch am Anfang der Lernkurve befindet. Zudem wurde diskutiert, dass das Bewusstsein beim potenziellen Kunden, dass mit entsprechenden Datenauswertungen hohe Potenziale zur Senkung von Instandhaltungskosten bestehen, erst geweckt werden muss. Außerdem wurde auf einen hersteller- und adressatenübergreifenden Standardisierungsbedarf hingewiesen.

Use Case: Fahrzeug überwacht Oberbau

TABELLE 46: MARKTBEWERTUNG USE CASE „FAHRZEUG ÜBERWACHT OBERBAU“ [TU CHEMNITZ, BWL III]

I. Marktattraktivität (Sicht der Anbieter von Sensorlösungen)					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung***	
		Erst-	Zweit-	*Erst-*	*Zweit-*
I.a	**erwartetes Marktpotenzial** (Größe & Wachstum)	**3,6**	**3,7**	*1,3*	*1,2*
I.b	**erwartete Rentabilität**	**2,9**	**2,9**	*0,9*	*0,8*
I.c	**Umfeldbedingungen des Marktes** (Recht, Politik, öffentliche Meinung)	**2,8**	**2,4**	*1,5*	*1,1*
I.d	**Potenziale der Sensorprodukte** (Weiterentwicklung & Synergien)	**4,2**	**4,2**	*0,8*	*0,7*

II. Marktreife					
Kriterium		Durchschnittliche Expertenbewertung*		*Streuung der Expertenbewertung***	
		Erst-	Zweit-	*Erst-*	*Zweit-*
II.a	**Verfügbarkeit der Sensorlösung zu marktgerechten Preisen** (versus weiterer F&E-Bedarf)	**3,1**	**3,1**	*1,2*	*0,9*
II.b	**Zulassungsfähigkeit der Sensorlösung im Bahnsystem**	**3,2**	**3,4**	*1,1*	*1,0*
II.c	**Know-how der potenziellen Sensoranwender**	**3,3**	**2,9**	*1,1*	*0,9*
II.d	**Strategische Ausgereiftheit der Geschäftsmodelle & -beziehungen**	**1,7**	**1,6**	*0,7*	*0,5*

* arithmetisches Mittel; Bewertung auf der Skala von 1 (= ungenügend) bis 5 (= sehr gut) ** empirische Standardabweichung

Beim Use Case „Fahrzeug überwacht Oberbau“ wurden das erwartete Marktpotenzial und die Potenziale der Sensorprodukte (für Weiterentwicklungen und Synergien) als sehr hoch eingeschätzt (siehe Tabelle 46). Kritisch hingegen werden nach der Diskussion vor allem die Umfeldbedingungen des Marktes gesehen. Zudem mangelt es bei diesem Use Case laut Meinung der Expertinnen und Experten besonders an der strategischen Ausgereiftheit der Geschäftsmodelle. In der zugehörigen Gruppendiskussion wurde vor allem auf die schwierige Anbieter-Nachfrager-Konstellation von EVU und EIU und das schwierige Umfeld, das sich aus der Einordnung des Schienenoberbaus als kritische Infrastruktur ergibt, verwiesen. Die Expertinnen und Experten können sich grundsätzlich das Anbieten entsprechender Sensorlösungen als ein völlig neues Geschäftsfeld losgelöst vom bisherigen Markt vorstellen und haben die Bedeutung von Datenmarktplätzen hierfür betont.

Use Case: Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant

TABELLE 47: MARKTBEWERTUNG USE CASE „FAHRZEUGLOKALISIERUNG FAHRZEUGSEITIG SICHERHEITSRELEVANT“ [TU CHEMNITZ, BWL III]

I. Marktattraktivität (Sicht der Anbieter von Sensorlösungen)					
Kriterium		Durchschnittliche Expertenbewertung*		Streuung der Expertenbewertung**	
		Erst-	Zweit-	Erst-	Zweit-
I.a	**erwartetes Marktpotenzial** (Größe & Wachstum)	4,4	4,4	*0,7*	*0,7*
I.b	**erwartete Rentabilität**	3,9	3,7	*0,9*	*0,7*
I.c	**Umfeldbedingungen des Marktes** (Recht, Politik, öffentliche Meinung)	3,3	3,6	*1,0*	*0,9*
I.d	**Potenziale der Sensorprodukte** (Weiterentwicklung & Synergien)	4,0	4,6	*0,9*	*0,5*

II. Marktreife					
Kriterium		Durchschnittliche Expertenbewertung*		Streuung der Expertenbewertung**	
		Erst-	Zweit-	Erst-	Zweit-
II.a	**Verfügbarkeit der Sensorlösung zu marktgerechten Preisen** (versus weiterer F&E-Bedarf)	3,0	3,6	*1,2*	*0,7*
II.b	**Zulassungsfähigkeit der Sensorlösung im Bahnsystem**	2,4	2,6	*1,2*	*0,7*
II.c	**Know-how der potenziellen Sensoranwender**	3,6	3,9	*0,7*	*0,8*
II.d	**Strategische Ausgereiftheit der Geschäftsmodelle & -beziehungen**	2,6	2,9	*0,9*	*0,8*

* arithmetisches Mittel; Bewertung auf der Skala von 1 (= ungenügend) bis 5 (= sehr gut) ** empirische Standardabweichung

Der Use Case „Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant“ erhielt bei allen Kriterien der Marktattraktivität sehr hohe Bewertungen (siehe Tabelle 47). Bei der Marktreife wurden die Verfügbarkeit der Sensorlösung sowie das Know-how der potenziellen Sensoranwender als hoch eingeschätzt. Etwas kritischer beurteilen die Expertinnen und Experten momentan noch die Zulassungsfähigkeit der Sensorlösung im Bahnsystem. Hierzu wurde in der Diskussion darauf verwiesen, dass die Sicherheitsrelevanz in diesem Use Case einen starken Einfluss auf die Marktreife hat. Insbesondere erfordere eine Zulassung als Gesamtlösung eine redundante Auslegung. Außerdem sei die strategische Ausgereiftheit der Geschäftsmodelle noch nicht sehr ausgeprägt. Es sei momentan noch weitgehend unklar, welcher Akteur die Finanzierung der entsprechenden Sensorausstattung der Fahrzeugflotten tragen wirf. Diskutiert wurde auch, ob eine entsprechende Ausstattung künftig in bestimmten Streckennetzen ein Netzzugangskriterium werden könnte.

7 Bestandsaufnahme und Patentrecherche – Sensoriksysteme und Teilkomponenten

In diesem Kapitel wurde eine Bestandsaufnahme zu Sensoriksystemen und Teilkomponenten durchgeführt. Die Recherche fokussierte sich auf digitale Systeme und Datenschnittstellen. Es wurde eine Übersicht zu Systemarchitekturen, Softwaretechnologien und Gestaltungsprinzipien erarbeitet. Neben der Bahnbranche wurden vor allem die Automatisierungstechnik und das IoT in verschiedenen Anwendungsbereichen betrachtet. Anhand des vom DZSF vorgeschlagenen Leitbildes konnte eine Auswahl aus den Rechercheergebnissen abgeleitet werden. Diese wurde hinsichtlich ihrer Eigenschaften, sowie Vor- und Nachteile analysiert und klassifiziert. Abschließend wurde für diese Ergebnisteilmenge eine Prüfung der Schutzrechtssituation durchgeführt und Barrieren für die industrielle Anwendung ermittelt.

Die Abschnitte des Kapitels sind wie folgt gegliedert: Abschnitt 7.1 beschreibt die Rechercheergebnisse zu sensorbasierten Technologien. Die Recherche hatte das Ziel einen umfassenden Überblick zum Stand der Technik sensorbasierter Technologien zu ermitteln. Abschnitt 7.2 beschreibt die Analyse, Klassifizierung und Eignungsprüfung der recherchierten Inhalte. Es fand eine Auswahl für das System Bahn geeigneter Technologien statt. Zu diesen wurden weitere technologische Details ermittelt, um Fragen der Anwendbarkeit und des Nutzens für den Bahnbereich beantworten zu können. Abschnitt 7.3 beschreibt die Recherche der Patent- und Lizensierungssituation für die ausgewählten Technologien.

7.1 Bestandsaufnahme

7.1.1 Vorgehensweise und Methodik

Mit einer Internetrecherche über gebräuchliche, freie Suchmaschinen wie z. B. Google oder Microsoft Bing wurde zunächst eine Übersicht über Hersteller, Informationsportale und Literaturquellen erstellt. Diese diente als Grundlage für die Auswahl und Durchführung von insgesamt zehn Experteninterviews. In diesen wurden vor allem Technologien, Architekturen sowie Projektvorhaben aus der Bahnbranche diskutiert. Auf der Grundlage dieser Gespräche wurde eine spezifische Recherche zu Fachliteratur, Veröffentlichungen, Datenblättern und Produktinformationen ausgeführt. Dazu wurden spezielle Suchmaschinen für wissenschaftliche Literatur wie z. B. Scopus[3] und Google Scholar[4] genutzt sowie die Internetseiten der jeweiligen Anbieter von Produkten und Technologien. Die Vorgehensweise zur Bestandsaufnahme im Kapitel 7.1 folgt dem Schema in Abbildung 40.

[3] https://www.scopus.com

[4] https://scholar.google.com

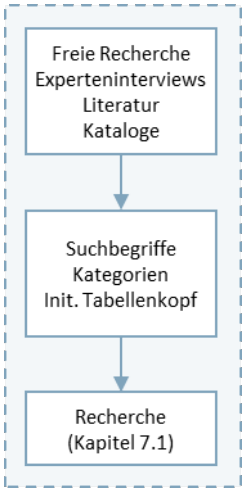


Abbildung 40: Vorgehensweise im Kapitel 7.1 Bestandsaufnahme

Es wurden Informationen aus den folgenden dreizehn Kategorien aufgenommen: Systemarchitekturen, Zugbeeinflussungssysteme, Türsteuerungen, Funksysteme, Netzwerkprotokolle, Feldbusse, Kommunikationsstandards, Auszeichnungssprachen, Modellierungssprachen, Datenformate, Semantik, Ontologien und Hardwarekomponenten. Die Recherchetabelle umfasst 121 Ergebnisse. Für jede Position wurden Informationen zu Recherchegegenstand und Anwendung, Entwicklungsstadium, Einsatzgebiet, wirtschaftliche Aspekte und den genutzten Informationsquellen dokumentiert.

7.1.2 Sensorbasierte Technologien

7.1.2.1 Rechercheziele des Abschnittes

Sensoren sind die Sinne technischer Systeme. Als Bauteil erfassen sie bestimmte Eigenschaften ihrer Umgebung und wandeln diese in verarbeitbare, meist elektrische Signale. Sensorbasierte Technologien umfassen neben den Sensoren, weitere Hardware- und Softwarekomponenten sowie Subsysteme für deren Betrieb und für die Erfassung, Verarbeitung, Übertragung und Speicherung von Sensordaten.

Sensorbasierte Technologien werden für die Überwachung und Automatisierung technischer Vorgänge und Prozesse benötigt. Sie sind wesentlicher Bestandteil der Mess-, Steuerungs- und Regelungstechnik und liefern wertvolle Daten oder Informationen für die Wartung, Optimierung oder Effizienzsteigerung von Komponenten und Anlagen. Sensorbasierte Technologien ermöglichen viele Zukunftsanwendungen im Bereich der Digitalisierung und Automatisierung. Dies ist ein branchenunabhängiger Trend mit stark zunehmender Bedeutung für den Bahnsektor. Sensordaten unterstützen bei der Realisierung automatischer Fahrfunktionen, bei der Ladungsüberwachung, -verfolgung und -ortung oder bei der zustandsbasierten und prädiktiven Instandhaltung.

Sensorbasierte Technologien nach dem Stand der Technik sind heterogen. Zu den Stakeholdern gehören u. a. Forschung und Entwicklung, Komponenten- und Systemhersteller, Distributoren, IT-Dienstleister, Anwendungsentwickler, Service- und Supportanbieter sowie das große Feld der Anwender. Daraus hat sich eine riesige Produktvielfalt entwickelt. In einer branchenunabhängigen Darstellung werden in diesem Abschnitt wichtige Bestandteile sensorbasierter Technologien recherchiert und vorgestellt. Das Ziel besteht darin ein aktuelles Bild vom Stand der Technik zu entwickeln. Zwischen einzelnen Technologien bestehen zudem Übergangsbereiche, die eine genaue Zuordnung erschweren. Das betrifft z. B. die Abgrenzung von Sensoren und Sensorsystemen oder von smarten Sensoren und smarten Syste-

men. Neue technologische Möglichkeiten erlauben die Miniaturisierung von Komponenten und Systemen und in der Folge eine höhere Integrationsdichte von Funktionen. Der Bereich zwischen Komponenten und Systemen verschwimmt zunehmend. Recherchiert wurde insbesondere auch der Stand der Technik in Bezug auf die Interoperabilität von Hardware und Software bei sensorbasierten Technologien. Eine wesentliche Voraussetzung für den nahtlosen Datenaustausch in heterogenen Systemen.

Das Kapitel beginnt mit einer einführenden Darstellung der Komponenten von Sensorsystemen. Dabei wird eine Begriffsklärung und die Abgrenzung von Sensorelement, Sensor und Sensorsystem durchgeführt. Anschließend beginnt die Darstellung der Rechercheinhalte mit den wichtigsten Hardwareschnittstellen. Dem Abschnitt folgen die Entwicklungsstufen von Sensoren bis zum smarten Sensor. Es wird eine Unterscheidung von smarten Sensoren und smarten Systemen vorgenommen. Netzwerke und Sensornetzwerke sind Voraussetzung für Konnektivität im IoT. Dieser Abschnitt stellt die wichtigsten Netzwerkprotokolle dar. Für einen nahtlosen Datenaustausch sind neben den Hardwareschnittstellen offene Protokolle, Datenstrukturen und eine gemeinsame Semantik erforderlich. In den letzten beiden Unterabschnitten werden die Rechercheergebnisse zu Datenverarbeitung, Modellierung und Austausch vorgestellt. Die beschriebenen Informationen haben sowohl grundlegenden (Allgemeinwissen im Fachgebiet) als auch spezifischen Charakter. Das Allgemeinwissen des Fachgebietes wird im Wesentlichen nicht anhand von Literaturstellen zitiert.

7.1.2.2 Komponenten eines Sensorsystems

Sensoren und Sensorsysteme sind wichtige Grundbausteine einer jeden sensorbasierten Anwendung. In diesem Abschnitt werden die wesentlichen Komponenten eines Sensorsystems vorgestellt. Die DIN 1319 „Grundlagen der Messtechnik“ ist Ausgangspunkt der Diskussion. In dieser sind wichtige Grundbegriffe wie Messgerät, Messeinrichtung, Messkette und (Messgrößen-) Aufnehmer definiert. Eine typische Messkette besteht beispielsweise aus Aufnehmer, Messumformer oder Messverstärker, Analog-Digital-Umsetzer, Mikrorechner mit Anzeige oder Ausgabe und einem Hilfsgerät zur Energieversorgung. Eine solche Messkette ist schematisch in Abbildung 41 aufgezeigt.

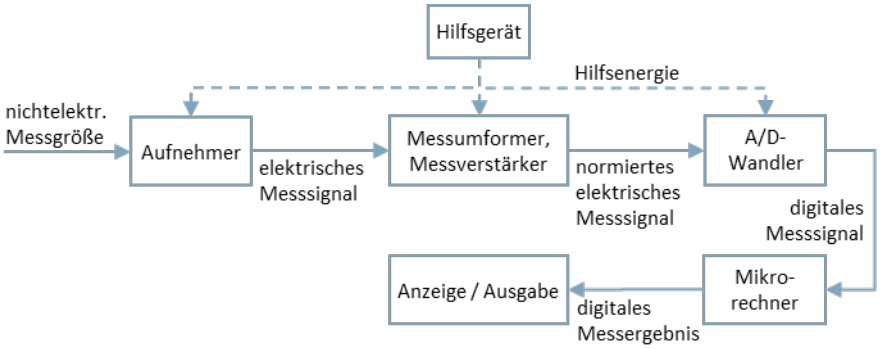


Abbildung 41: Typische Anordnung der Komponenten in einer Messkette [Eigene Darstellung nach [66]]

Aufnehmer oder Messgrößenaufnehmer werden üblicherweise als Sensoren bezeichnet. Sie wandeln nichtelektrische Signale z. B. von physikalischen oder chemischen Messgrößen in elektrische Signale um. Sensoren sind wesentliche Bestandteile von Messgeräten und Messketten.

Im industriellen Kontext wird die Kombination aus Sensor und Auswerteeinheit als Sensorsystem bezeichnet. Vor allem durch die fortschreitenden Möglichkeiten der Mikro- und Nanotechnologie besteht der Trend die Auswerteelektronik ebenfalls in den Sensor zu integrieren (siehe auch Abschnitt Smarte Sensoren und Systeme). In Abbildung 42 sind die Komponenten eines Sensorsystems schematisch dargestellt.

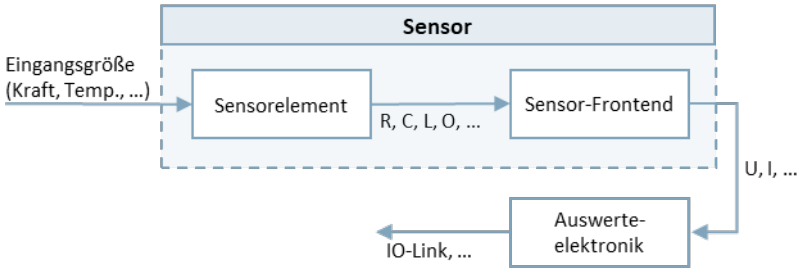


Abbildung 42: Komponenten eines Sensorsystems [Fraunhofer ENAS]

Das Kernelement eines jeden Sensors ist das Sensorelement. Dieses wandelt eine Eingangsgröße oder Messgröße in eine elektrisch messbare Größe um. Das kann z. B. ein Dehnungsmesstreifen sein, welcher in Anhängigkeit von der Dehnung seinen elektrischen Widerstand ändert oder ein mikro-elektro-mechanisches System (MEMS), welches Beschleunigungen, Vibrationen oder Drehraten in die Änderung einer elektrischen Kapazität umsetzt. Bei komplexen Sensorelementen wird meist in unmittelbarer Nähe ein Sensor-Frontend eingesetzt. Dieses wandelt das Ausgangssignal des Sensorelementes in ein elektrisches Signal um. Sensorelement und Sensor-Frontend sind in einem Gehäuse integriert und werden als Sensor bezeichnet. Sensoren gibt es in den unterschiedlichsten Ausführungsformen (Größe, Gehäuseform, elektrische Schnittstellen, Befestigungsmöglichkeiten). Die Anpassung eines Sensors an die jeweilige Anwendung erfolgt durch eine spezifische Auswerteelektronik und das nachgeordnete Automatisierungssystem.

Durch hochintegrierte Halbleiterschaltungen können zunehmend immer mehr Funktionen der Auswerteelektronik sowie nachgeordneter Signal- und Datenverarbeitungssysteme in den Sensor integriert werden. Dadurch verschwimmt die Grenze zwischen Sensor und Sensorsystem. Es entstehen smarte Sensoren mit teilweise umfangreichen Fähigkeiten zur Konfiguration, Selbstüberwachung, Adaption und Datenverarbeitung (siehe Abschnitt Technologische Entwicklungsstufen).

Sensoren und Sensorsysteme haben meist spezifische Gehäuse und damit verbundene Befestigungsmöglichkeiten. Sind diese nicht standardisiert, kann ein Austausch im Reparaturfall bei gleichzeitigem Wechsel des Modells oder des Herstellers erhebliche Probleme bereiten.

Sensoren für die Produktentwicklung oder Forschung können von Elektronikdistributoren, wie z. B. Farnell [88] oder Digikey [89] bezogen werden. Industrielle Sensoren zur direkten Montage an Anlagen oder Infrastrukturkomponenten werden von einer Vielzahl von Sensorherstellern angeboten, wie z. B. Pepperl+Fuchs [90], Lenord+Bauer [91] und SICK [92].

7.1.2.3 Schnittstellen von Sensoren und Sensorsystemen

Wie Hüning [93] darstellt, können Sensorsysteme nicht isoliert betrachtet werden. Es findet vielmehr eine Interaktion mit ihrer Umgebung und mit anderen Systemen statt. Sensoren bspw. messen ihre Umgebung, andere Systeme oder das eigene technische Subsystem. Die entstandenen Messdaten müssen an informationsverarbeitende Systeme weitergegeben werden. Dies geschieht über Sensorschnittstellen, Datenbusse und Netzwerke. Schnittstellen sind eine wesentliche Eigenschaft von Sensoren oder Sensorsystemen. Sensoren sind oft mit einer Auswerteelektronik oder mit einem Steuerungs- bzw. Automatisierungssystem verbunden. Die Sensorschnittstellen bestimmen dabei die Art und den Umfang der übertragenen Daten. [93]

Es existiert eine große Anzahl an unterschiedlichen Sensorschnittstellen. Viele marktgängige Sensoren sind derzeit allerdings noch mit einer analogen Schnittstelle (z. B. Temperatursensoren, Kraftsensoren, Neigungssensoren) oder einer einfachen digitalen Schnittstelle (z. B. induktive und kapazitive Sensoren,

Ultraschallsensoren, Magnetfeldsensoren) ausgestattet. Mit diesen Schnittstellen ist nur eine unidirektionelle Übertragung der Sensorsignale vom Sensor zum übergeordneten System möglich. Sensoren mit analogen Schnittstellen werden aufgrund ihrer Robustheit nach wie vor gern in Industrieanwendungen eingesetzt.

Analoge Gleichspannungssignale für Regel- und Steueranlagen sind in der DIN IEC 60381 Blatt 2 genormt und liegen im Bereich zwischen -10 V und +10 V. Analoge Gleichstromsignale sind in der gleichen Norm im Blatt 1 beschrieben und liegen zwischen 0 mA (oder 4 mA) und 20 mA. Häufig wird ein versetzter Nullpunkt verwendet, um defekte Signalleitungen erkennen zu können. Die Verwendung von Einheitssignalen erleichtert die Austauschbarkeit der Sensoren in einem Automatisierungssystem im Reparaturfall. Analoge Signale sind im Allgemeinen robust gegenüber Störungen und sind sowohl wert- als auch zeitkontinuierlich. Sie können bei Bedarf eine große Signalbandbreite übertragen, wie sie bspw. bei Beschleunigungs- und Vibrationssensoren erforderlich ist. Analoge Sensoren bestehen aus einem oder mehreren Sensorelementen und einem analogen Vorverstärker. Bei komplexeren Sensorelementen wird meist ein Analog-Frontend eingesetzt. In Abbildung 43 ist der schematische Aufbau eines Sensors mit analoger Schnittstelle dargestellt.

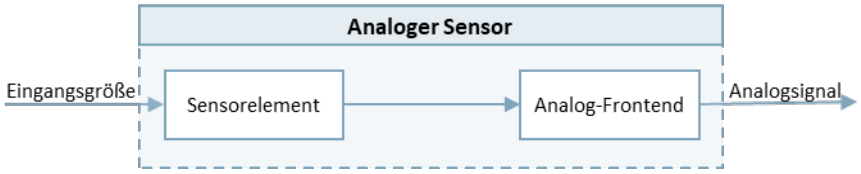


Abbildung 43: Schematische Darstellung eines Sensors mit analoger Schnittstelle [Fraunhofer ENAS]

In der Automatisierungstechnik werden Sensoren sehr häufig für Positionieraufgaben, als Endlagenschalter oder für Zählaufgaben eingesetzt. Diese Sensoren haben meist einen oder mehrere Schaltausgänge. Die Ausgangssignale sind wertdiskret (z. B. 1 V oder 5 V) jedoch zeitkontinuierlich. Die eingesetzten Sensorprinzipien sind vielfältig und können je nach Messaufgabe bspw. induktiv, kapazitiv, optisch oder auf Ultraschall basieren.

Neben analogen Schnittstellen und Schaltausgängen haben sich bei Sensoren und Sensorsystemen digitale Schnittstellen etabliert. Digitale Signale sind wert- und zeitdiskret. Sie werden im Sensor durch Abtastung und Analog-Digital-Wandlung der analogen Messwerte erzeugt. Digitale Signale können über große Entfernungen unverfälscht übertragen werden. Sie sind weniger empfindlich gegenüber Rauschen, können jedoch ebenso gestört werden. Speicherung und Weiterverarbeitung sind im Vergleich zu analogen Signalen leichter möglich. Ein digitaler Sensor besteht genau wie ein analoger Sensor aus einem oder mehreren Sensorelementen und einem Sensor-Frontend. Dieses muss neben einem analogen Schaltungsteil Analog-Digital-Wandler und einen digitalen Schaltungsteil enthalten. Dieser kann weitere Funktionen zur digitalen Signalverarbeitung, Datenverarbeitung und Übertragung bereitstellen. Ein digitaler Sensor ist schematisch in Abbildung 44 aufgezeigt.

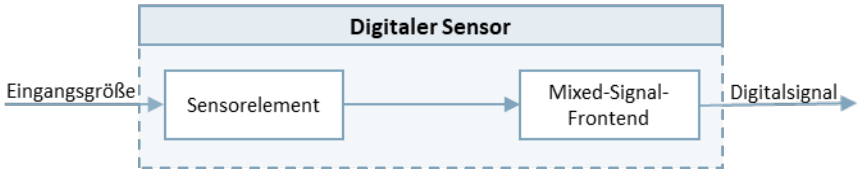


Abbildung 44: Schematische Darstellung eines Sensors mit digitaler Schnittstelle [Fraunhofer ENAS]

Die Vielzahl der digitalen Schnittstellen ist historischen Ursprungs und aus den jeweiligen Anwendungsfällen hervorgegangen. Neben Schnittstellen für Punkt-zu-Punkt-Verbindungen wie RS 232 haben sich vor allem Bussysteme (siehe Tabelle 48) etabliert. Vorteilhaft dabei ist, dass mehrere Sensoren an den

gleichen elektrischen Leitungen (dem Bus) angeschlossen sind und durch eine Auswerteeinheit ausgelesen werden können. Die Auswahl des jeweils auszulesenden Sensors erfolgt entweder über eine digitale Adresse oder über zusätzliche Steuerleitungen wie z. B. Chip- oder Sensor-Select). Im industriellen Umfeld haben sich robuste Feldbussysteme durchgesetzt. Diese zeichnen sich gegenüber normalen Bussystemen durch eine höhere Festigkeit gegenüber elektromagnetischen Störungen aus. Gegenwärtig erfolgt der Übergang von Feldbussen zu Ethernet-basierten Feldbussen, welche auch als Industrial Ethernet bezeichnet werden. Ziel ist es den Ethernet-Standard in der industriellen Fertigung nutzbar zu machen und damit ein einheitliches Kommunikationssystem zwischen der Leitungsebene, der Steuerungsebene und der Sensorebene zu etablieren (siehe Abschnitt 7.1.3). In Abbildung 45 sind gegenwärtig häufig verwendete Sensorschnittstellen zusammengestellt.

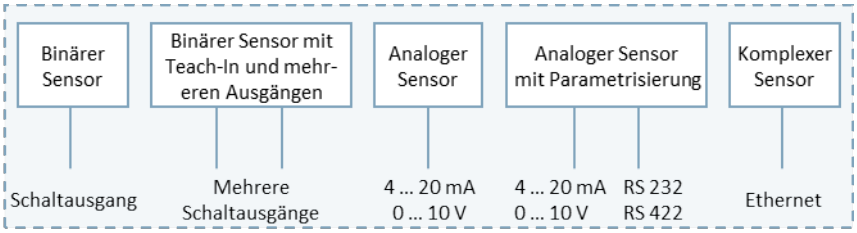


Abbildung 45: Gegenwärtig häufig verwendete Sensorschnittstellen [Eigene Darstellung nach [67]]

Die meisten Sensoren sind auch heute noch mit einer einfachen analogen oder digitalen Schnittstelle ausgestattet und an eine Auswerteeinheit oder ein übergeordnetes System angebunden. Feldbusse und Industrial Ethernet werden erst ab der Systemebene eingesetzt. Eine Auswahl gebräuchlicher Schnittstellen von Sensoren und Sensorsystemen ist in Tabelle 48 aufgelistet.

TABELLE 48: AUSWAHL GEBRÄUCHLICHER SCHNITTSTELLEN VON SENSOREN UND SENSORSYSTEMEN

Abkürzung	Bezeichnung	Quelle/Referenz
Analoge Schnittstellen		
U	Spannungsausgang	[67]
I	Stromausgang	[67]
PWM	Frequenzausgang und Pulsweitenmodulation	[68]
Digitale Schnittstellen		
I/O	Schaltausgang	[67]
A/B/Z	Inkrementalgeber	[69]
RS 232	Recommended Standard 232	[70]
RS 422	Recommended Standard 422	[71]
RS 485	Recommended Standard 485	[72]
SSI	Synchron-Serielle Schnittstelle	[73]
BiSS Interface	BiSS Interface	[69]

SENT	Single Edge Nibble Transmission	[74]
PSI5	Peripheral Sensor Interface 5	[75]
Busse und Feldbusse		
I2C	Inter-Integrated Circuit	[76]
SPI	Serial Peripheral Interface	[77]
IO-Link	IO-Link	IEC 61131-9 [94]
AS-Interface	Actuator-Sensor-Interface	[78]
CAN/CANopen	Controller Area Network	[79] [80]
LON	Local Operating Network	[81]
HART	Highway Addressable Remote Transducer	[82]
CC-Link	Control and Communications Link	[83]
ControlNet	ControlNet	[84]
DeviceNet	DeviceNet	[85]
M-Bus	Meter-Bus	[86]
Modbus RTU	Modbus Remote Terminal Unit	[87]
PROFIBUS	PROFIBUS	[94]
Netzwerke		
Ethernet	siehe Abschnitt Netzwerke und Sensornetzwerke	Kapitel 7.1.2.6
Industrial Ethernet	siehe Abschnitt Netzwerke und Sensornetzwerke	Kapitel 7.1.2.6
Wireless	siehe Abschnitt Netzwerke und Sensornetzwerke	Kapitel 7.1.2.6

Sensor und Auswerteeinheit sind häufig über eine einfache analoge oder digitale Punkt-zu-Punkt-Verbindung verbunden. Bussysteme erweitern die Möglichkeiten und erlauben bei gleicher Leitungsanzahl die Adressierung von mehreren Sensoren durch eine Auswerteeinheit. Folgende Verbindungen zwischen Sensor und Auswerteeinheit werden eingesetzt:

- Punkt-zu-Punkt-Verbindungen: sehr häufig verwendet
- Datenbus-Verbindung: zunehmend bedeutsamer
- Netzwerk-Verbindung (geschaltet): zurzeit selten eingesetzt

Sensorsysteme sind in Bezug auf die Schnittstelle weniger limitiert. Ab der Auswerteeinheit oder einem Gateway sind prinzipiell alle Schnittstellen möglich. In den einzelnen Branchen und Anwendungen haben sich jedoch bestimmte Schnittstellen etabliert und werden vorrangig eingesetzt, so z. B. Controller Area Network (CAN) im Automobilbereich oder EtherCAT in der Automatisierungstechnik (siehe Abschnitt Netzwerke und Sensornetzwerke). Je nach Komplexität der Schnittstelle muss neben der Hardwareebene auch die Datenübertragungsebene spezifiziert sein. Hardwareschnittstellen spezifizieren die mechanische Ausführung der Steckverbinder und Kontakte sowie die erlaubten Signalpegel. Diese können analoge oder digitale Signale transportieren. Eine Sonderform sind die binären Signale. Diese stehen für Schaltausgänge und liefern zeitkontinuierliche jedoch wertediskrete Signale.

Wie in [67] diskutiert, ist eine Konsolidierung der Sensorschnittstellen sinnvoll. Des Weiteren ist eine bidirektionale Kommunikation zwischen Auswerteeinheit und Sensor wünschenswert. Ein solcher Kommunikationskanal ermöglicht die Übertragung von Konfigurationsparametern und erlaubt die gezielte Abfrage von Statusinformationen. Eine Initiative besteht in der Entwicklung der Input/Output (IO)-Link-Technologie. Wie von [94] berichtet, handelt es sich dabei um eine in IEC 61131-9 weltweit standardisierte IO-Technologie. Diese kann für die leistungsfähige Kommunikation mit Sensoren als auch Aktoren in einer Punkt-zu-Punkt-Verbindung eingesetzt werden. Ohne zusätzliche Anforderungen kann der geläufige 3-Leiter Sensor und Aktor Anschluss genutzt werden. [94] hebt hervor, dass es sich nicht um einen Feldbus handelt, sondern vielmehr um eine Weiterentwicklung bisheriger Anschlusstechnik. Die Konsolidierung der Sensorschnittstellen am Beispiel von IO-Link ist in Abbildung 46 schematisch aufgezeigt.

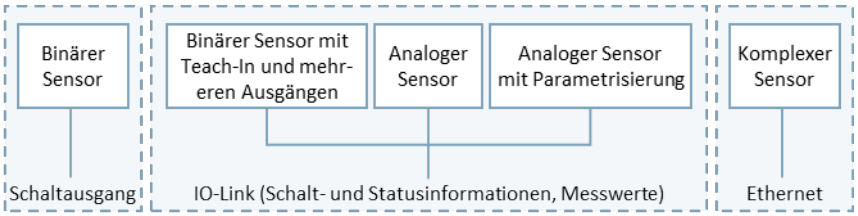


Abbildung 46: Konsolidierung der Sensorschnittstellen am Beispiel von IO-Link [Eigene Darstellung nach [67]]

7.1.2.4 Technologische Entwicklungsstufen von Sensoren

Ein Sensor wandelt eine physikalische oder chemische Messgröße in eine für den Menschen oder für ein elektronisches System lesbares Messsignal um. In seiner einfachsten Ausführungsform kann dies die mechanische Wandlung einer Größe z. B. eines Druckes, einer Kraft oder einer Temperatur in eine entsprechende Skalenanzeige sein (Sensor 1.0). Durch Fortschritte in der Elektrotechnik und nachfolgend vor allem in der Elektronik und Mikroelektronik, konnten immer mehr Funktionen in einem Gehäuse in unmittelbarer Nähe des Sensorelementes integriert werden. Die Fähigkeiten der Sensoren, aber auch ihre Komplexität nahmen zu. In Anlehnung an [95] und [96] ist die Evolution des Sensores vom einfachen mechansichen Transducer (Sensor 1.0) bis zum smarten Sensor (Sensor 4.0) in Abbildung 47 dargestellt.

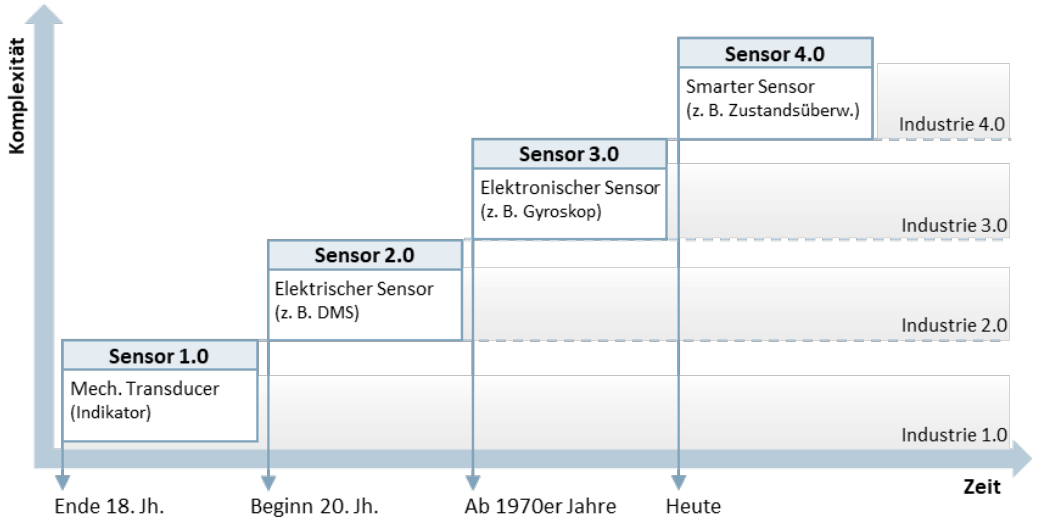


Abbildung 47: Evolution des Sensors [Eigene Darstellung nach [95] und [96]]

Sensoren wurden dadurch leistungsfähiger, störsicherer, vielseitiger und anwenderfreundlicher. Derzeit findet der Übergang vom elektronischen Sensor (Sensor 3.0) zum smarten Sensor (Sensor 4.0) statt. Damit einher geht nicht nur die Verbesserung der Datenauswertung im Sensor, sondern auch die Integration von komplexeren Schnittstellen zur Datenübertragung. Entsprechende Rechenleistung vorausgesetzt, ist eine Anbindung von Sensoren über Standard-Ethernet oder Industrial Ethernet möglich. Dies erlaubt die direkte und schnelle Übertragung von Sensordaten in einem Netzwerk ohne den Umweg über Auswerteeinheiten, Gateways oder die Prozesssteuerung eines Automatisierungssystems. Unter dem Begriff Self-X wird eine ganze Reihe von Funktionen smarter Sensoren zusammengefasst, wie beispielsweise Selbstidentifikation, Selbstdiagnose, Selbstkonfiguration, Kalibrierung und Reparatur [96].

Darüber hinaus wird durch immer leistungsfähigere Mikroprozessoren eine Bewertung der Messdaten im Sensor möglich. Dies kann die zu übertragenden Daten erheblich reduzieren und auf Statussignale, Statusupdates sowie Warn- oder Alarmmeldungen reduzieren. Durch die dezentrale Verknüpfung von Sensoren und Aktoren in einem Automatisierungssystem im Kontext von Industrie 4.0 und dem Industrial Internet of Things (IIoT) wird die Latenz der Datenübertragung sehr stark verringert und eine Reaktion in „Echtzeit“ auf Alarmmeldungen möglich.

7.1.2.5 Smarte Sensoren und Systeme

Mikrocontroller haben mittlerweile bei akzeptabler Größe und moderatem bis niedrigem Energieverbrauch eine ausreichende Leistungsfähigkeit erreicht, um direkt im Sensor neben Sensorelement und Mixed-Signal-Frontend integriert zu werden. Die Datenauswertung wird dadurch von der Auswerteeinheit oder einem übergeordneten Automatisierungsssystem in den Sensor verlagert. Das vereinfacht die Installation und ermöglicht einen Sensoreinsatz an bisher aus technischen oder wirtschaftlichen Gründen unzugänglichen Messstellen. Ziel der Integration ist es, den ursprünglichen Sensor hinsichtlich Größe und Gewicht zu erhalten oder sogar stärker zu miniaturisieren. Dabei soll der Preis für die neuen Funktionalitäten und die Einsparung von Auswerte- und Steuergeräten angemessen bleiben oder sogar sinken. In Abbildung 48 ist die schematische Darstellung eines smarten Sensors abgebildet.

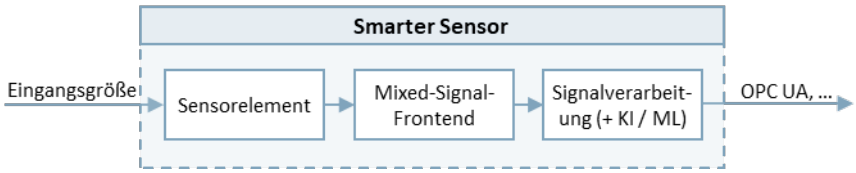


Abbildung 48: Schematische Darstellung eines smarten Sensors [Fraunhofer ENAS]

Der zunehmende Einsatz von Sensoren und von Sensoren mit einer großen Signalbandbreite erhöht die zu verarbeitende, zu übertragende und zu speichernde Datenmenge signifikant. Es ist daher wünschenswert die Daten bereits im Sensor zu verarbeiten und nur noch Statusmeldungen, Warnmeldungen oder wesentliche Prozesskenngrößen zu übertragen. Dies erfordert eine fortgeschrittene Signalverarbeitung entweder in der Nähe des Sensors oder integriert in diesen. Aktuelle Mikrokontroller können zudem komplexe Datenübertragungsprotokolle bedienen und somit Daten in Netzwerken übertragen.

Smarte Systeme erweitern die Funktionalität smarter Sensoren darüber hinaus vor allem in Richtung Aktorik. Ziel ist es aus den erfassten Sensorsignalen unmittelbar und dezentral im Sensorsysteme eine Handlungsanweisung abzuleiten. Dazu sind eine umfangreiche Auswertung und Analyse der Sensordaten notwendig, welche aus den Grundbausteinen Datenverarbeitung, Wissensdatenbank und künstliche Intelligenz besteht. Zu einem smarten System gehören weiterhin Komponenten zur Datenkommunikation und zur Energieversorgung. Eine schematische Darstellung der wesentlichen Komponenten eines smarten Systems ist in Abbildung 49 abgebildet.

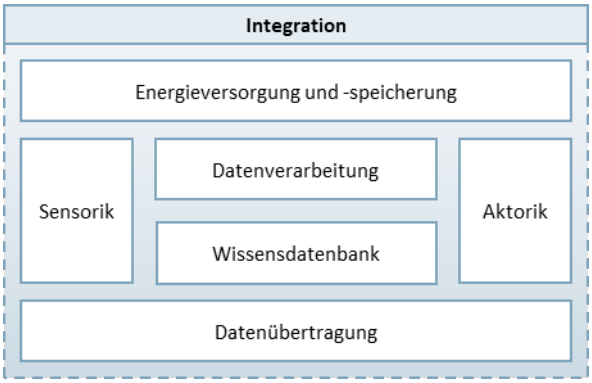


Abbildung 49: Komponenten eines smarten Systems [Eigene Darstellung nach [97]]

Aktuelle Forschungs- und Entwicklungsarbeiten zu smarten Systemen beschäftigen sich darüber hinaus mit ihrer Auslegung als autonome Systeme, welche über einen langen Zeitraum autark Messdaten sammeln können. Die Datenübertragung findet über Funknetzwerke statt und die Energiegewinnung durch Batterien oder Energie Harvesting. Diese Systeme müssen sehr energieeffizient und sparsam arbeiten.

7.1.2.6 Netzwerke und Sensornetzwerke

Die Kommunikation zwischen Sensor, Auswerteeinheit, Steuergerät, Gateway sowie einem Steuerungs- und Automatisierungssystem wird durch Hardware- und Softwareschnittstellen ermöglicht. Die Komponenten können dabei über eine Punkt-zu-Punkt-Verbindung, ein Bussystem oder ein Netzwerk angeschlossen werden. Kommunikationsnetze werden anhand von verschiedenen Netzwerktopologien aufgebaut. Abbildung 50 zeigt schematisch einige häufig eingesetzte Netzwerktopologien.

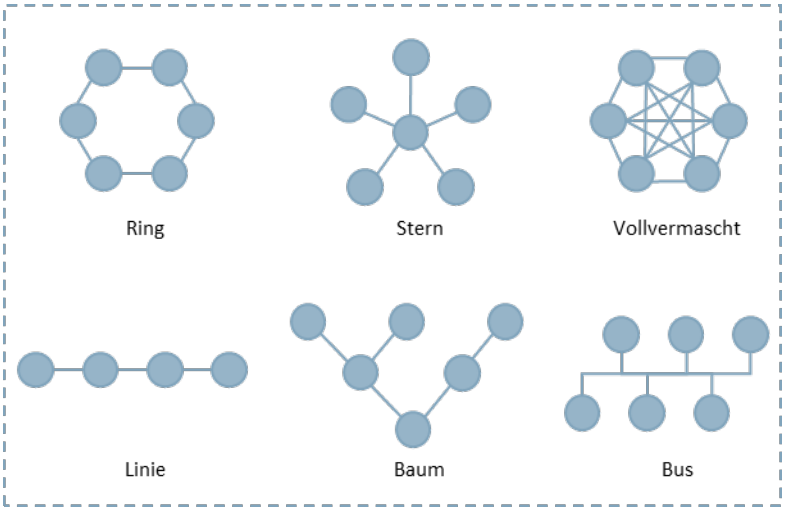


Abbildung 50: Ausgewählte Netzwerktopologien [Eigene Darstellung nach [98]]

Historisch begann die Vernetzung von Komponenten zunächst mit Punkt-zu-Punkt-Verbindungen. Diese Architektur ist bei steigender Sensoranzahl jedoch nur mit großem Aufwand skalierbar. Jeder Sensor muss einzeln verkabelt werden und am Steuergerät eine entsprechende Anzahl an freien Schnittstellen verfügbar sein. Sehr viel effizienter ist die Anordnung von Sensoren entlang eines Datenbusses. Daraus haben sich die Bustopologie, die Linientopologie und die Ringtopologie entwickelt. Da die gesamte Kommunikation aller Teilnehmenden über einen Bus abläuft, kommt auch diese Architektur irgendwann an ihre Grenzen. Eine gute Alternative bieten die sternförmige und die baumförmige Topologie.

Eine Auswahl an gängigen Feldbussystemen wurde im Abschnitt Schnittstellen von Sensoren und Sensorsystemen in Tabelle 48 vorgestellt.

Wie in [99] dargestellt, wurde Industrial Ethernet mit dem Ziel einer Vereinheitlichung der Kommunikationsinfrastruktur eingeführt. Im Bereich der Feldbusse war eine große Heterogenität entstanden, welche den Datenaustausch zwischen den Systemen erheblich erschwerte. Ethernet Netzwerke boten die Chance einer einheitlichen Infrastruktur von der Führungsebene bis zur Feldebene. [99] hebt hervor, dass mittlerweile mehr Ethernet-basierte Lösungen existieren, als ursprünglich Feldbusse. Es sei also genau ein gegenteiliger Effekt eingetreten. Die Situation sei vor allem für den Anwender schwierig, da er die Systeme nicht miteinander vergleichen kann.

Um den Datenverkehr in Ethernet-basierten Netzwerken weiter zu begrenzen, wurden an den zentralen Knoten Netzwerkswitches eingesetzt. Diese leiten die Datenpakete sehr gezielt nur über den Datenbus vom Sender zum Empfänger und verringern dadurch das Datenaufkommen bei allen anderen Netzwerkteilnehmern. Je nach Anwendungsfall und den Anforderungen an Zuverlässigkeit, Übertragungsgeschwindigkeit, Latenz und Anzahl der möglichen Netzwerkteilnehmenden haben sich unterschiedliche Spezifikationen für Datenbusse und Datennetzwerke herausgebildet. Eine Auflistung wesentlicher Ethernet-basierter Feldbusse wurde in Tabelle 49 erstellt.

TABELLE 49: AUFLISTUNG GÄNGIGER ETHERNET-BASIERTER FELDBUSSE (INDUSTRIAL ETHERNET)

Abkürzung	Bezeichnung	Quelle/Referenz
BACnet/IP	Building Automation and Control Network	[100]
CC-Link IE Field	CC-Link IE Field Network	[101]
CC-Link IE TSN	CC-Link IE Field Network TSN	[102]
EtherCat	Ethernet for Control Automation Technology	[103]
EtherNet/IP	EtherNet Industrial Protocol	[104]
Modbus TCP	Modbus TCP	[105]
Powerlink	Ethernet POWERLINK	[106]
PROFINET	Process Field Network	[107]
SERCOS III	Serial Realtime Communication System	[108]
Lon(Works)	Local Operating Network	[81]
WorldFIP	Flux Information Processus	[109]

Weit verbreitete Umsetzungen von echtzeitfähigem Ethernet können bereits Buszyklen von rund 100 µs erreichen. Dies sind unter anderem: EtherNet/IP, Profinet, Ethernet Powerlink, SERCOS III, EtherCAT, VARAN, SafetyNET p und, TSN.

In Tabelle 50 sind gängige Funkkommunikationstechnologien aufgelistet.

TABELLE 50: AUFLISTUNG GÄNGIGER FUNKKOMMUNIKATIONSTECHNOLOGIEN

Abkürzung	Bezeichnung	Quelle/Referenz
GSM(-R)	Global System for Mobile Communications Railway (früher Groupe Spécial Mobile)	[110]
LTE	Long Term Evolution	[111]
5G	Fifth-generation technology standard for cellular networks	[112]
FRMCS	Future Railway Mobile Communication System	[113]
RMR	Railway Mobile Radio	[218]
Bluetooth und BLE	Bluetooth und Bluerooth Low Energy	[114]
LoRa	Long Range	[115]
Wi-Fi (WLAN)		
Zigbee	Zigbee	[116]
Z-Wave	Z-Wave	[117]
6LoWPAN	IPv6 over Low power Wireless Personal Area Network	[118]
RFID	Radio-frequency identification	[119]
NB-IOT	Narrowband IoT	[120]
NFC	Near Field Communication	[121]

Die große Vielfalt an Spezifikationen und Kommunikationssystemen erschwert den Datenaustausch zwischen diesen erheblich. Das Open Systems Interconnection (OSI)-Referenzmodell beschreibt aus diesem Grund Kommunikation über unterschiedliche technische Systeme hinweg und versucht die Weiterentwicklung zu vereinfachen. Die Schichten des OSI-Modells sind in Abbildung 51 dargestellt.

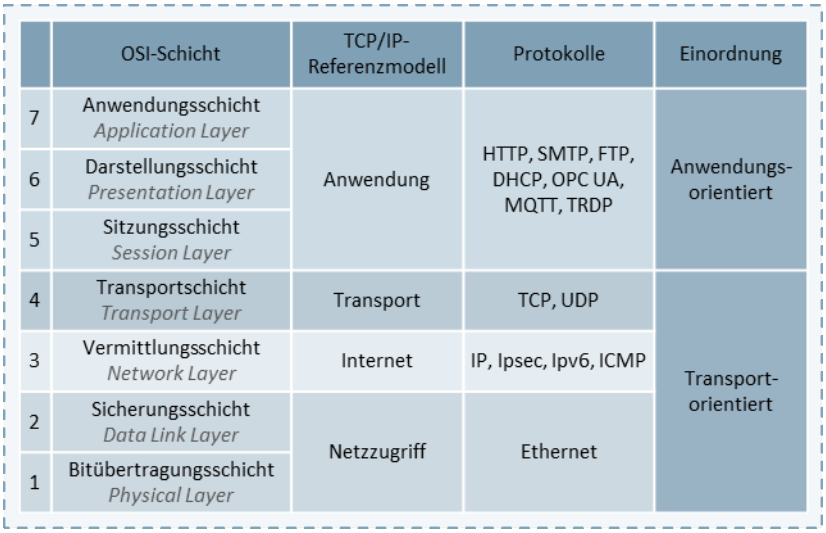


Abbildung 51: ISO/OSI-Referenzmodell für Netzwerkprotokolle als Schichtarchitektur [Eigene Darstellung nach ITU-T X.200 (07/1994) [122] und [123]]

Die Datenpakete bilden dabei ein Schalenmodel und werden mit jeder hinzukommenden OSI-Schicht um die zugehörenden Informationen ergänzt.

Die Datenübertragung wird über Netzwerkprotokolle geregelt. In Tabelle 51 ist eine Auswahl gängiger Protokolle aufgeführt.

TABELLE 51: ÜBERSICHT GÄNGIGER NETZWERKPROTOKOLLE

Abkürzung	Bezeichnung	OSI-Schicht	Quelle / Referenz
MQTT	Message Queuing Telemetry Transport	5 bis 7	[124]
UDP	User Datagram Protocol	4	[122][123]
TCP	Transmission Control Protocol	4	[122][123]
IP	Internet Protocol	3	[122][123]
TRDP	Train Real Time Data Protocol	4	[263]
CIP	Common Industrial Protocol	5 bis 7	[290]
IPTCom	IPTCom	4	[125]
DNP	Decentral Network Protocol	N/A	[126]
HDLC	High-Level Data Link Control	2	[127]
AMQP	Advanced Message Queuing Protocol	5 bis 7	[128]
CoAP	Constrained Application Protocol	5 bis 7	[129]
DDS	Data Distribution Service	5 bis 7	[130]
LoRaWAN	LoRaWAN	2 und 3	[131]

Abkürzung	Bezeichnung	OSI-Schicht	Quelle / Referenz
LWM2M	Lightweight M2M	5 bis 7	[132]
XMPP	Extensible Messaging and Presence Protocol	5 bis 7	[133]

7.1.2.7 Prozessschritte der Datenerfassung und -verarbeitung

Im Folgenden sollen von Sensoren aufgenommene Daten betrachtet werden. Sensoren wandeln eine physikalische oder chemische Messgröße in ein elektrisches Signal um, welches von einem elektronischen System weiterverarbeitet werden kann. Direkt nach der Datenaufnahme findet die Signalkonditionierung statt. Anschließend folgt die Analog-zu-Digital-Wandlung mit der Übertragung an einen Computer oder ein Mikrokontroller-basiertes System. Ein Datenerfassungssystem ist beispielhaft in Abbildung 52 aufgezeigt.

Abbildung 52: Prozessschritte der Datenerfassung [Eigene Darstellung nach [134]]

Sind die Daten einmal von einem elektronischen System erfasst worden, durchlaufen sie im Allgemeinen die Prozessschritte der Datenverarbeitung (siehe Abbildung 53).

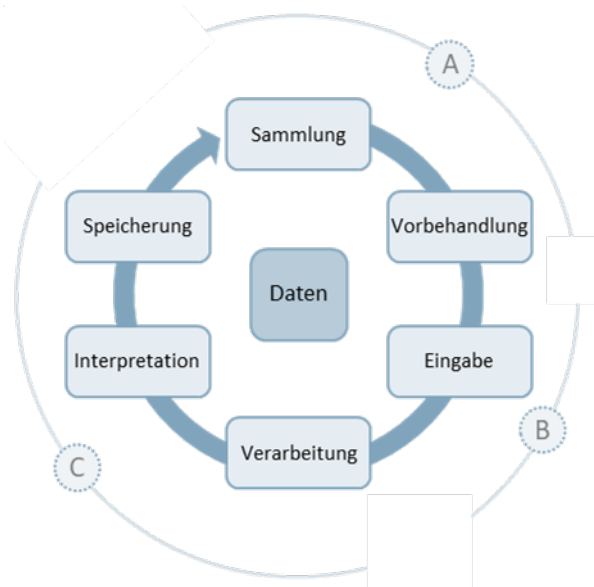


Abbildung 53: Prozessschritte der Datenverarbeitung [Eigene Darstellung nach [135]]

Der Datenverarbeitungszyklus beginnt mit der Datenerfassung. Das kann ein Sensorsystem sein oder ein Data Lake. Anschließend folgt die Datenaufbereitung. Dabei werden die Daten vorverarbeitet und bereinigt. Es folgt die Eingabe der Daten in das Zielsystem. Das kann z. B. ein Data Warehouse sein. Im nächsten Schritt werden die Daten verarbeitet. Das kann mit konventionellen Algorithmen erfolgen oder

mit maschinellem Lernen. Danach werden die Ergebnisse aufbereitet und meist visualisiert. Die Ergebnisse werden anschließend gespeichert. Dabei sind alle gesetzlichen Vorschriften zu beachten.

Um eine Einordnung von Technologien (siehe Abschnitt 7.2.4) in die Prozessschritte der Datenerfassung zu ermöglichen, wurden die Teilsegmente A, B und C in der Abbildung gekennzeichnet. Der Bereich A steht für Datenerfassung, wie sie in Abbildung 52 dargestellt ist. Der Bereich B steht für Datenschnittstellen und für manuelle Dateneingabe z. B. über eine Tastatur. Der Bereich C bezeichnet das Rechenzentrum oder die Cloud.

7.1.2.8 Modellierung und Datenaustausch

Hardware, Software und Daten müssen zusammenarbeiten, damit Datenaustausch und Auswertung zu den gewünschten Resultaten führen. Im Folgenden werden damit verbundene Begriffe kurz vorgestellt.

Systemarchitektur

- Das Layout, die Struktur, das Verhalten und das Zusammenwirken der Komponenten eines Systems. Kann Hardware und Software umfassen.
- Beschreibt Erfassung, Verarbeitung, Übertragung und Speicherung der Messdaten eines Sensorsystems.
- Ausarbeitung häufig unter Nutzung von UML (Unified Modelling Language) und Derivaten, wie z. B. Systems Modeling Language (SysML) oder SensorML.

Datenmodell [144]

- Beschreibt die aktuellen oder zukünftigen Datenstrukturen eines Anwendungsbereiches. Dieser kann fachlicher (z. B. Geschäftsprozess, Organisationseinheit, Business Service) und/oder technischer Natur (z. B. Smartphone App, IT-Plattform, Web-Service) sein.
- Ausarbeitung häufig unter Nutzung einer Modellierungssprache.
- Datenmodelltypen: konzeptionelles/semantisches Datenmodell, logisches Datenmodell oder physisches/technisches Datenmodell.

Datenformat [139]

- Ein Begriff aus der Datenverarbeitung, der festlegt, wie Daten strukturiert und dargestellt werden und wie sie bei ihrer Verarbeitung zu interpretieren sind.
- Die Syntax und die Semantik der Daten innerhalb einer Datei, eines Programmes oder einer Datenübertragung.

Austauschformat [145]

- Ein Begriff aus der elektronischen Datenverarbeitung (EDV) und bezeichnet meist ein Dateiformat, welches mit vielen verschiedenen Anwendungen auf fast jedem Betriebssystem kompatibel ist.

Datenschnittstelle

- Legt fest, welche Daten bzw. Datenformate eine Software/Firmware (z. B. eines Sensorsystems) einlesen oder ausgeben kann.

Semantik [146]

- Beschreibt die Bedeutung eines Wortes oder einer Phrase. Wenn zwei unterschiedliche Worte, dasselbe meinen, dann sind diese semantisch gleich.

Ontologie [146]

- Beschreibt die Wissensrepräsentation in strukturierter Form. Hier geht es darum, Informationen in einen gemeinsamen Kontext zu bringen.

Die vorangegangenen Abschnitte haben Sensoren, Sensorsysteme und deren Vernetzung untereinander und mit übergeordneten Automatisierungssystemen aufgezeigt. Dabei ist sichtbar geworden, dass im Bereich der Schnittstellen, der Feldbusse und des Industrial Ethernet eine große Vielfalt an Produkten existiert. Die Heterogenität erschwert die Interoperabilität der Systeme und die Zusammenführung in einem einzigen großen Netzwerk. Doch nicht nur die Hardware ist heterogen. Die von den Sensoren erzeugten, in den Netzwerken übertragenen und auf in den Automatisierungssystemen gespeicherten Daten folgen ebenfalls keinem einheitlichen Standard. Es gibt eine große Vielfalt an Datenformaten, Kommunikationsprotokollen und Datenmodellen. In diesem Abschnitt wurden daher zunächst nach Semantiken, Ontologien, Modellierungssprachen, Auszeichnungssprachen und Datenformaten recherchiert. Um einen Überblick über die vorhandenen Möglichkeiten zu erhalten.

In Tabelle 52 und Tabelle 53 sind ausgewählte, aktuell häufig verwendete Semantiken, Ontologien und Sprachen aufgeführt.

TABELLE 52: SEMANTIK UND DIE ZUGEHÖRIGEN SPRACHEN

Abkürzung	Bezeichnung	Quelle/Referenz
SPRINT	Semantics for PerfoRmant and scalable INteropera-bility of multimodal Transport	[147]
Semantic Web	Semantic Web	[148]

TABELLE 53: ONTOLOGIE UND DIE ZUGEHÖRIGEN SPRACHEN

Abkürzung	Bezeichnung	Quelle/Referenz
RDF-Schema	Resource Description Framework Schema	[149]
DAML+OIL	DARPA Agent Markup Language Ontology Inference Layer	[150]
F-Logic	Frame Logic	[151]
OWL	Web Ontology Language	[152]
WSML	Web Service Modeling Language	[153]

Die Encyclopedia Britannica [136] definiert eine Auszeichnungssprache als ein Standard-Textkodierungssystem. Dieses besteht aus einer Anzahl von Symbolen zur Steuerung von Struktur, Formatierung oder der Beziehung zwischen seinen Teilen. Wenn ein Dokument gedruckt oder auf einem Bildschirm angezeigt wird, werden die Markup-Symbole vom entsprechenden Gerät (Computer, Drucker, Browser usw.) interpretiert und steuern damit das Aussehen des Dokumentes. Ein auf diese Weise markiertes Dokument enthält neben dem anzuzeigenden Text ebenso die Symbole der Auszeichnungssprache. Die am häufigsten verwendeten Auszeichnungssprachen sind SGML (Standard Generalized Markup Language), HTML (Hypertext Markup Language) und XML (Extensible Markup Language). [136]

Eine Auswahl häufig eingesetzter Auszeichnungssprachen ist in Tabelle 54 aufgelistet.

TABELLE 54: AUSWAHL HÄUFIG EINGESETZTER AUSZEICHNUNGSSPRACHEN

Abkürzung	Bezeichnung	Quelle/Referenz
SGML	Standard Generalized Markup Language	[154]
HTML	Hypertext Markup Language	[155]
PS	PostScript	[156]
RTF	Rich Text Format	[157]
TeX/LaTeX	TeX/LaTeX	[158]
XML	Extensible Markup Language	[159]
YAML	Yet Another Markup Language	[160]
SVG	Scalable Vector Graphics	[161]

Fleischmann [137] beschreibt den Begriff Modellierungssprache. Modellierungssprachen stellen das Vokabular und die Grammatik zur Verfügung, die benötigt werden, um Sachverhalte der menschlich wahrgenommenen Realität in Modellen abbilden zu können. Die Sprachen sind künstlich definiert. Sie schaffen für alle Akteurinnen und Akteure einen definierten Ausgangspunkt für die Modellbildung. Dies trifft sowohl auf Akteurinnen und Akteure als Personen zu, als auch auf Computersysteme. Die standardisierte UML (engl. Unified Modeling Language) ist die am weitesten verbreitete Modellierungssprache. Hingegen sind Programmablaufpläne die älteste bis heute gebräuchliche Repräsentationsform von Modellen des Kontrollflusses in einem Computerprogramm. [138]

Modellierungssprachen weisen neben einer definierten Syntax darüber hinaus eine Semantik auf. Es kann zwischen formalen und informalen Modellierungssprachen unterschieden werden. Die Semantik wird in formalen Modellierungssprachen (die oft auch als Spezifikationssprachen bezeichnet werden) genau festgelegt. In den Sprachdefinitionen informeller Modellierungssprachen wird die Semantik ausschließlich umgangssprachlich definiert. [138]

In Tabelle 55 sind beispielhaft verschiedene Modellierungssprachen abgebildet.

TABELLE 55: MODELLIERUNGSSPRACHEN

Abkürzung	Bezeichnung	Quelle/Referenz
Programmablaufplan	Programmablaufplan	[162]
Petri-Netze	Petri-Netze	[163]
UML	Unified Modeling Language	[298]
SysML	Systems Modeling Language	[300]
SensorML	Sensor Model Language	[252]

Abkürzung	Bezeichnung	Quelle/Referenz
SDL	Spezifikations- und Beschreibungssprache	[164]

Der Begriff „Datenformat“ stammt aus der Datenverarbeitung. Er definiert die Struktur und Darstellung von Daten sowie deren Interpretation während der Verarbeitung. In dieser Hinsicht ist das Datenformat dem Ausdruck „Datentyp“ sehr ähnlich, kann ihn ergänzen oder als Synonym verwendet werden. [139]

Einige wesentliche Datenformate sind in Tabelle 56 aufgeführt.

TABELLE 56: DATEIFORMATE/DATENFORMAT

Abkürzung	Bezeichnung	Quelle/Referenz
JSON	JavaScript Object Notation	[295]
BSON	Binary JSON	[165]
ProtoBuf	Protocol Buffers	[166]

Plattformunabhängigkeit ist für vernetzte Systeme von großer Bedeutung. Für den Austausch von Daten zwischen internetbasierten Systemen ist JavaScript Object Notation (JSON) ein leichtgewichtiges Datenformat. Es kann sowohl von Menschen als auch von Maschinen gelesen werden. [140] Es ist ein eigenständiges Datenformat ohne Verknüpfung mit der JavaScript-Sprache. Gleichzeitig eignet es sich aufgrund seiner unkomplizierten Struktur und der Kodierung im Unicode-Zeichensatz für den Datenaustausch zwischen verschiedensten Systemen. [140] Das JSON-Format verbreitet sich in der Industrie. Dies wird in erster Linie durch die zunehmende Verknüpfung von Informationstechnologien mit Maschinen und Geräten der Feldebene vorangetrieben. JSON ist bereits weit verbreitet, da es u. a. in Feldgeräten und Softwaresystemen mit Representational state transfer (REST)-Schnittstellen verwendet wird. Sensoren und Geräte können über MQTT integriert werden. Wie in [140] ausgeführt wird derzeit häufig NoSQL verwendet. Der zunehmende Trend zu maschinellem Lernen und künstlicher Intelligenz macht JSON zu einem einfachen, aber flexiblen Datenformat. [140]

7.1.2.9 Internet of Things

Die Empfehlung ITU-T Y.2060 [141] gibt einen Überblick über das IoT. Sie beschreibt dieses als eine globale Infrastruktur für die Informationsgesellschaft. Als Grundlage sind interoperable Informations- und Kommunikationstechnologien notwendig. Diese bestehen zum Teil bereits oder müssen entwickelt werden. Über diese Infrastruktur können sowohl physische als auch virtuelle Dinge miteinander verbunden werden. In der Folge sind verschiedene neue und fortschrittliche Dienste möglich, wie z. B. Datenerfassung, Verarbeitung, Identifikation und Kommunikation. Hinzu kommen Aspekte der Datensicherheit und des Datenschutzes.

Nach der Empfehlung ITU-T Y.2060 muss jedes IoT-Gerät die Fähigkeit zur Kommunikation aufweisen. Optional und im Wesentlichen abhängig vom Anwendungszweck, ist die Ausstattung mit Sensoren und Aktoren sowie Fähigkeiten zur Datenerfassung, Datenspeicherung und Datenverarbeitung.

Die Empfehlung ITU-T Y.2060 definiert ein IoT-Referenzmodell. Dieses besteht aus den vier Ebenen application layer, service support and application support layer, network layer und device layer. Die Abbildung 54 zeigt eine schematische Darstellung des IoT Referenzmodells mit allen Ebenen.

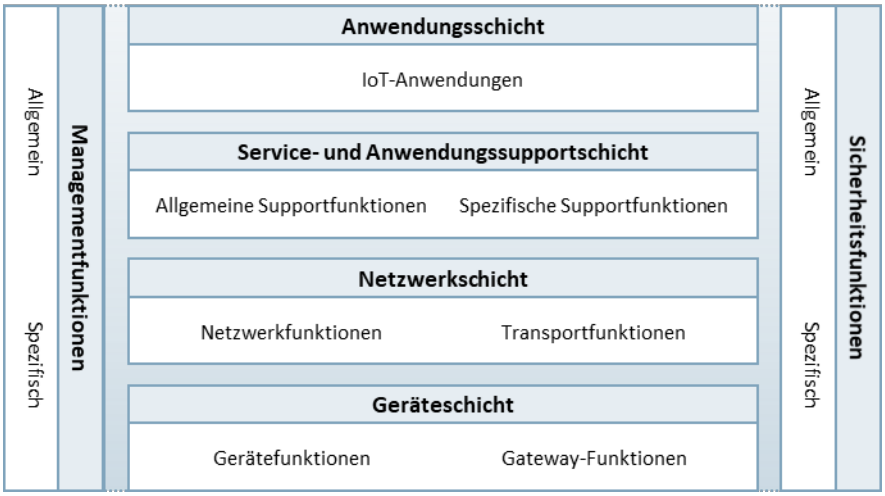


Abbildung 54: IoT-Referenzmodell [Eigene Darstellung nach der Empfehlung ITU-T Y.2060 [141]]

Es findet eine zunehmende Vermischung von digitaler und physischer Welt statt, wie in [142] ausgeführt. Dabei werden Komponenten, Module und Systeme „smart“ und beinhalten zunehmend Sensoren, Aktoren und leistungsfähige Datenverarbeitung. Die Vernetzung der Dinge schafft einen Mehrwert indem Sensordaten und Informationen über das Gerät oder die Maschine hinaus verfügbar werden. So kann ein Getränkeautomat bspw. Informationen zur Anzahl der vorhandenen Getränke bereitstellen. Die Anwendungsgebiete für IoT sind vielfältig und sehr heterogen. Sie reichen von der Medizin, über die Landwirtschaft bis hin zur industriellen Fertigung. IoT-Geräte variieren daher in ihrer Komplexität sehr stark in Abhängigkeit vom Anwendungsfall. Das IoT ist mit seinen vernetzten Sensoren und Aktoren ein wesentlicher Baustein der vierten industriellen Revolution, welche auch als Industrie 4.0 bezeichnet wird. [142]

7.1.2.10 Zusammenfassung des Abschnittes

Ziel des Abschnittes 7.1.2 war es, einen branchenunabhängigen Überblick über den Stand der Technik bei sensorbasierten Technologien zu ermitteln. Aufgrund des großen Umfanges dieses Themas wurde für diesen Bericht zunächst eine Begriffsklärung vorgenommen. Die Recherche verfolgte besonders das Ziel die Interoperabilität der Technologien hinsichtlich Hardware und Software aufzuzeigen. Zu jeder Technologie wurde eine allgemeine Definition recherchiert. Danach wurde die technologische Vielfalt in Bezug auf Schnittstellen und Kommunikationsprotokolle ermittelt sowie ihre Popularität in der Anwendung.

Der Abschnitt Technologische Entwicklungsstufen beschreibt den Wandeln in der Sensortechnik vom einfachen Transducer bis hin zum smarten Sensor. Ermöglicht wird dieser Wandel durch Entwicklungsfortschritte in den Schlüsseltechnologien Mikroelektronik, Materialforschung, Integrationstechnologien, Siliziumtechnologie, Mikrorechentechnik, Schaltungstechnik, Informationstechnik, Algorithmen usw. Kleine, leistungsfähige Sensorsysteme treffen auf einen wachsenden Bedarf in der Automatisierung nach besserer und engmaschigerer Überwachung von Anlagen zum Zwecke der Prozessoptimierung, Zustandsüberwachung und vorausschauenden Wartung.

Bei industriellen Sensoren haben sich zahlreiche Standardschnittstellen etabliert. Diese reichen von einfachen Schaltausgängen, über analoge Einheitssignale bis hin zu einfachen digitalen Schnittstellen. Es gibt einen Trend zu bidirektionalen digitalen Schnittstellen zum Austausch von Daten und Konfigurationsparametern (z. B. IO-Link, AS-Interface). Diese Schnittstellen sind nicht netzwerkfähig und die Da-

ten werden nicht anhand einer Semantik oder Ontologie codiert. Einzelne besonders komplexe Sensoren besitzen bereits Bus- oder Ethernet-Schnittstellen. Sensorsysteme aus der IoT-Welt sind meist netzwerkfähig und nutzen Protokolle für den Datenaustausch.

Es besteht ein großer Unterschied zwischen konventionellen Sensorsystemen und IoT-basierten Sensorsystemen. Konventionelle Sensorsysteme sind Bestandteil eines Automatisierungssystems. Sensoren mit Standardschnittstellen können gut ausgetauscht werden, wenn es sich nicht um Spezialanfertigungen (Form, Befestigung, Messparameter usw.) handelt. Für die am meisten verwendeten industriellen Sensoren gibt es eine große Auswahl.

7.1.3 Sensorbasierte Technologien in der Automatisierung

7.1.3.1 Rechercheziele des Abschnittes

Die Automatisierungsbranche ist ein intensiver Anwender von verschiedenen sensorbasierten Technologien. Automatisierungs- und Regelungssysteme benötigen Sensoren, um Informationen über Prozesse und Vorgänge zu erhalten. Es gibt daher einen hohen Grad an Systematisierung. Kerngebiete der Automatisierung sind die Überwachung, Steuerung und Regelung von Prozessen. In der Automatisierung spielen sensorbasierte Technologien eine große Rolle.

In diesem Abschnitt wird die Anwendung sensorbasierter Technologien in der (industriellen) Automatisierung recherchiert und vorgestellt. Klassische Automatisierungssysteme sind meist nach der Automatisierungspyramide aufgebaut. Das IoT ist eine Technologie, die für die industrielle Automatisierung eine wachsende Bedeutung erlangt. Die Recherche fokussiert weniger auf einzelne Komponenten, sondern auf Systeme und Architekturen. Betrachtet wird vor allem auch der durch Digitalisierung und IoT stattfindende Wandel in der Automatisierung.

Ausgehend von der Automatisierungspyramide wird zunächst die Leittechnik betrachtet. Gezeigt wird ein typisches System und der Weg der Daten von der Prozess- bis zur Unternehmensebene. Danach erfolgt eine Betrachtung der Digitalisierung und des IoT. Der Einfluss und die Veränderungen auf die Leittechnik werden dargestellt. Es wird gezeigt, dass sich die klassische Automatisierungspyramide verändert und eine stärkere Vernetzung aller Systeme stattfindet.

7.1.3.2 Betriebstechnologie und Automatisierungspyramide

Die Automatisierungspyramide gibt nach Kleinemeier [167] mit ihrem hierarchischen Charakter die Struktur der Leittechnik in der automatisierten Fabrik vor. Durch Elektronik und Informationstechnologien findet seit der dritten industriellen Revolution eine fortschreitende Automatisierung der Fabriken statt. Die Automatisierungspyramide veranschaulicht die Verteilung der Komponenten und System auf den einzelnen Ebenen vom Prozess bis zum Enterprise-Resource-Planning (ERP). Es gibt eine große Vielzahl an unterschiedlichen Darstellungen wie Meudt et al. [168] beschreiben. Die klassische Darstellung nutzt eine Unterscheidung von sechs Ebenen. Eine schematische Darstellung der Pyramide zusammen mit den Ebenen der Leittechnik zeigt Abbildung 55.

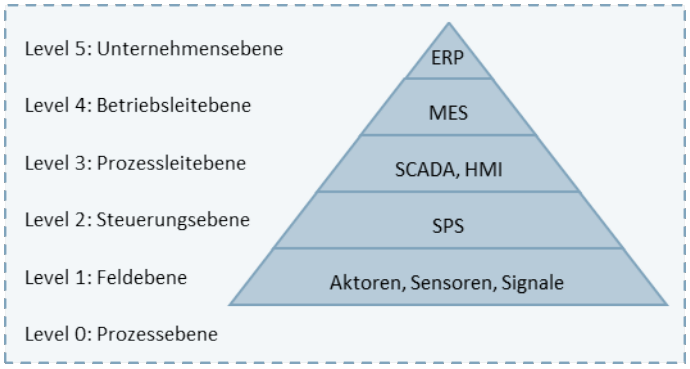


Abbildung 55: Automatisierungspyramide und Level [Eigene Darstellung nach [168], [169] und [170]]

Die Funktion der einzelnen Ebenen wird in Meudt et al. [168] beschrieben. Auf der Prozessebene (Level 0) findet die Fertigung und der Produktionsprozess statt. Darauf folgt die Feldebene (Level 1), auch Shopfloor genannt. Diese wird durch Sensoren und Aktoren gebildet. Es findet die Verarbeitung produktionsrelevanter Informationen statt. Darüber liegt die Steuerungsebene (Level 2). Über SPS wird eine meist dezentrale Steuerung und Regelung der Maschinen und Anlagen durchgeführt. In der Steuerungsebene werden die Sensordaten verarbeitet und als Ergebnisdaten zurückgegeben. Die Darstellung der Steuerung über Bedien- und Beobachtungssysteme findet in der Leitebene (Level 3) statt. Hier sind die Prozessleitsysteme und die Mensch-Maschine-Schnittstellen angeordnet. Für die Produktionsfeinplanung ist die Betriebsebene (Level 4) vorgesehen. Von dieser Ebene aus wird die Produktion gesteuert, gelenkt und kontrolliert. Dazu werden Betriebs-, Maschinen und Personaldaten genutzt. Auf der Unternehmensebene (Level 5), auch als Topfloor bezeichnet, findet die Produktionsgrobplanung und die Bestellabwicklung der industriellen Fertigung statt. [168]

In Abbildung 56 ist als Anwendungsbeispiel eine Fabrikautomatisierung mit mehreren Sensoren und Aktoren sowie Steuerungs- und Leitebenen bis zum ERP dargestellt.

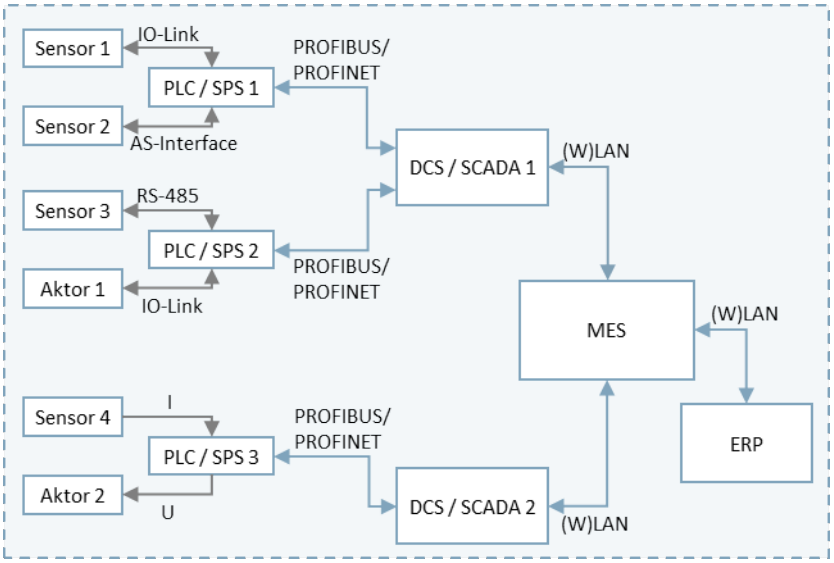


Abbildung 56: Anwendungsbeispiel Fabrikautomation [Fraunhofer ENAS]

Die Ebenen der Automatisierungspyramide finden sich im Anwendungsbeispiel in der Abbildung 56 wieder. Dabei muss nicht jedes Automatisierungssystem alle Ebenen aufweisen. Je komplexer es ist, desto mehr Ebenen sind jedoch notwendig. In den höheren Ebenen steigt die Menge der zu übertragenden

Daten. Demgegenüber nimmt die Übertragungsgeschwindigkeit ab. Eine kurze Latenzzeit ist in den höheren Ebenen von geringerer Bedeutung. Wichtig ist, dass zu jeder Zeit eine zuverlässige und sichere Kommunikation gegeben ist. In der Feld- und Steuerungsebene ist in vielen Fällen Echtzeitfähigkeit notwendig, damit Regelkreise schnell genug auf Prozessgrößen reagieren können. Die Automatisierungspyramide ist ein strukturierter Ansatz zur Verwaltung von Automatisierungssystemen und zur Optimierung der Produktionseffizienz.

7.1.3.3 Digitalisierung und Industrie 4.0

Industrie 4.0

Für die intelligente Vernetzung von Industriemaschinen und -prozessen unter Verwendung von Informations- und Kommunikationstechnologie steht der Begriff „Industrie 4.0“. Unternehmen können intelligente Vernetzung auf vielfältige Weise einsetzen. Dazu zählen bspw.: flexible Produktion, wandelbare Fabrik, kundenzentrierte Lösungen, optimierte Logistik, Einsatz von Daten und ressourcenschonende Kreislaufwirtschaft. [143]

Die Informationstechnologie hat sich seit den 70er Jahren in den Firmen ausgebreitet. Erste computergestützte Automatisierungen, die Verwendung von Informationstechnik in den Büros sowie Desktop-PCs führten zu einer Revolution in der Industrie. Die Haupttechnologie für Industrie 4.0 ist das Internet und nicht mehr der Computer. Die Digitalisierung der Produktion erhält durch die globale Vernetzung über Unternehmens- oder Ländergrenzen hinweg eine neue Qualität: Die vierte industrielle Revolution, Industrie 4.0, wird durch das IoT, Maschine-zu-Maschine-Kommunikation und Produktionsstätten, die immer intelligenter werden, eingeläutet. [143]

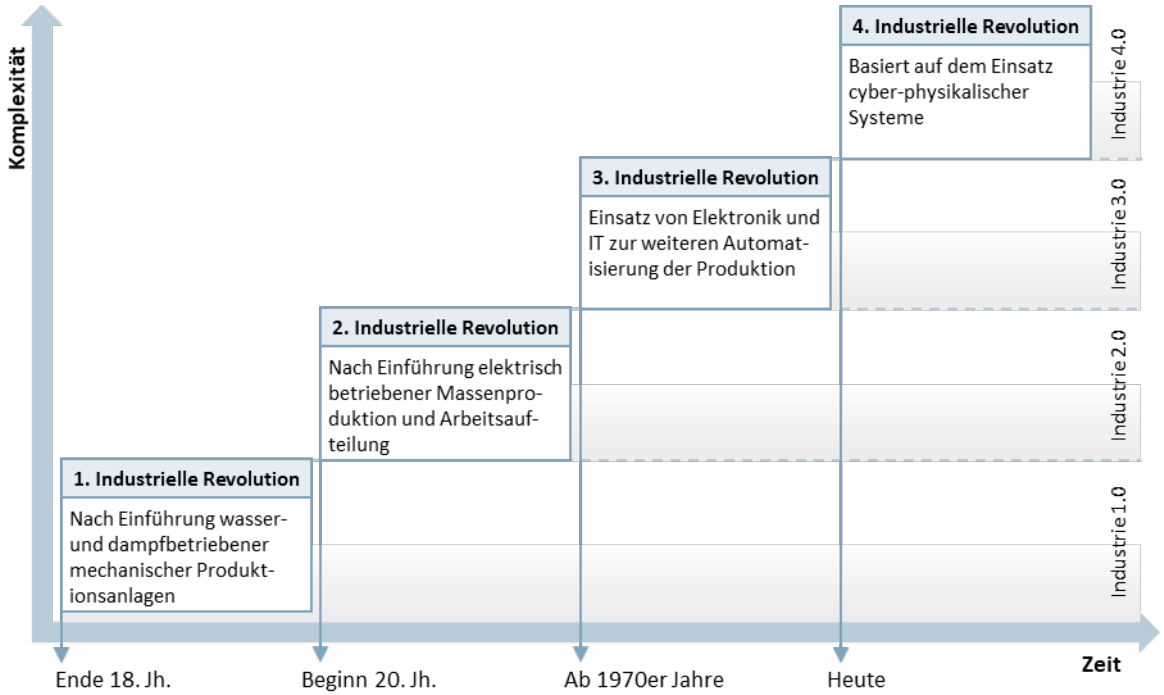


Abbildung 57: Die vier Stufen der industriellen Revolution [Eigene Darstellung nach [171]]

Industrie 4.0 bezeichnet einen fundamentalen Prozess der Wertschöpfung durch Innovation und Transformation in der Industrie. Neue Möglichkeiten für Wirtschaft und Arbeit in weltumspannenden, digitalen Ökosystemen sind das Hauptthema dieser Veränderung: Flexible, hochdynamische und weltweit

vernetzte Wertschöpfungsnetzwerke mit neuen Kooperationsformen ersetzen die derzeit festen und unbeweglichen Wertschöpfungsketten. Durch diese Daten ermöglichte Geschäftsmodelle legen den Fokus auf den Nutzen der Kundinnen und Kunden und die Ausrichtung auf Lösungen und ersetzen die Produktzentrierung als gängiges Modell der Wertschöpfung in der Industrie. In der vernetzten Wirtschaft spielen Verfügbarkeit, Transparenz und Zugang zu Daten eine entscheidende Rolle für den Erfolg und bestimmen wesentlich die Wettbewerbsfähigkeit. [173]

Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0)

Das Referenzarchitekturmodell (IEC PAS 63088) [172] kombiniert die wesentlichen Bestandteile von Industrie 4.0 in drei Dimensionen. Dadurch wird sichergestellt, dass alle Beteiligten an Industrie 4.0 eine gemeinsame Sichtweise vertreten und ein gemeinsames Verständnis entwickeln. [174]

Das Referenzarchitekturmodell kann genutzt werden, um Anwendungsfälle für Industrie 4.0 zu identifizieren und die erforderlichen Standards für diese Anwendungsfälle zu ermitteln. Dabei erfolgt eine Überprüfung der Eignung von Konzepten und Methoden in den einschlägigen Normen für die Anwendung im Industrie-4.0-Umfeld. Daraufhin werden ausdrücklich die geeignetsten Normen empfohlen, um eine vollständige Interoperabilität sicherzustellen. [175]

Es werden sechs Architekturschichten (siehe Abbildung 58) in Bezug auf Eigenschaften und Systemstrukturen beschrieben, die jeweils Funktionen und funktionsspezifische Daten aufweisen. [175]

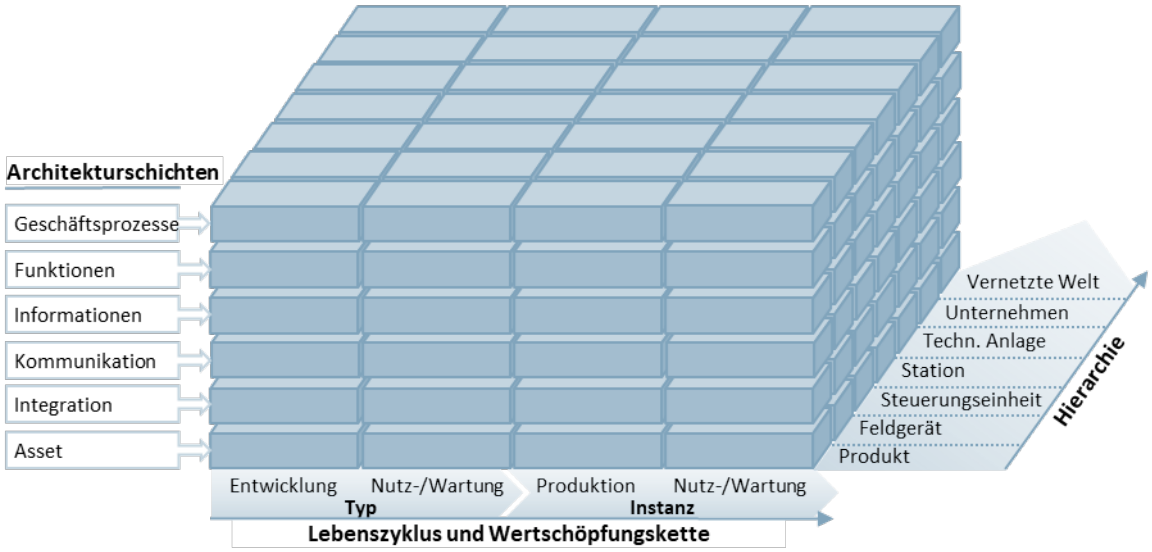


Abbildung 58: Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) [Eigene Darstellung nach [176]]

Assets in der Wertschöpfungskette werden in „Lebenszyklus und Wertschöpfung“ beschrieben. Dies umfasst Idee, Entwicklung und Instandhaltung einer Asset-Art sowie die Produktion, Nutzung und Instandhaltung spezifischer Instanzen dieser. Assets beziehen sich auf Gegenstände, die für ein Unternehmen von Nutzen sind. [175]

Die funktionale Hierarchie einer Fabrik wird durch die Hierarchieebenen beschrieben, die in die Wertschöpfungsprozesse integriert sind. Sie wird durch die Wertschöpfungsprozesse des Produkts innerhalb und außerhalb der Fabrik sowie durch die Verbindung zu unternehmensübergreifenden Wertschöpfungsprozessen erweitert. [175]

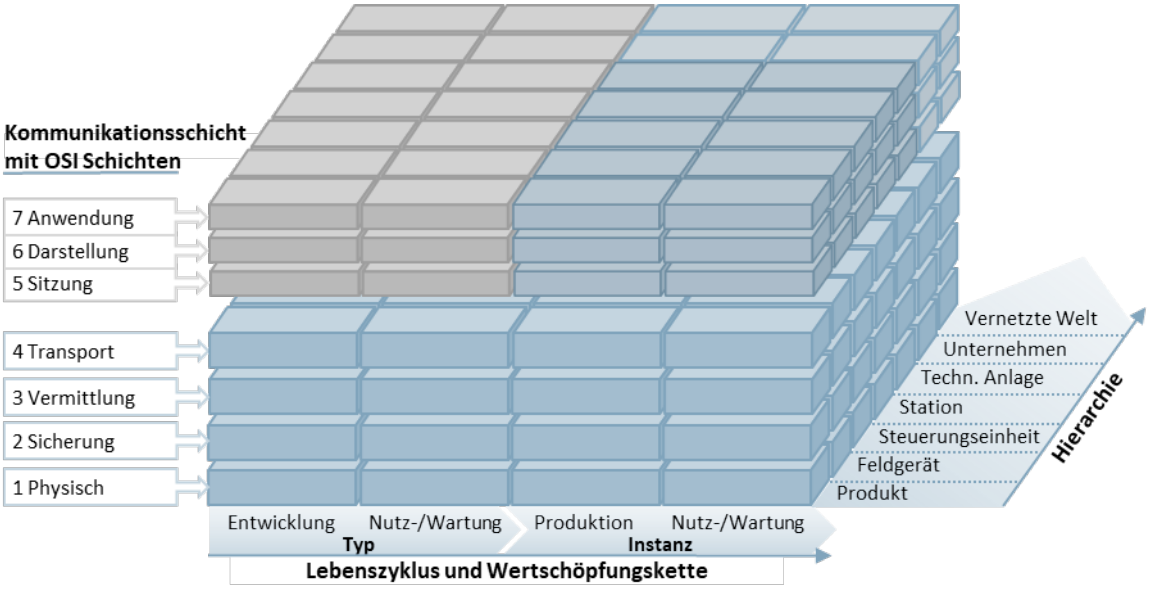


Abbildung 59: RAMI 4.0 – Kommunikationsschicht [Eigene Darstellung nach [174]]

Industrie 4.0-Objekte sind weltweit eindeutig identifizierbar und besitzen Fähigkeiten zur Kommunikation. Die Verwaltungsschale und das Asset bilden ihre Komponenten. Die Verwaltungsschale beinhaltet wichtige Angaben zur Verwaltung des Assets und zu seinen technischen Funktionen. [175]

Leitbild für Industrie 4.0

Das Leitbild 2030 zeigt einen ganzheitlichen Lösungsansatz zur Gestaltung digitaler Ökosysteme. Damit soll die Grundlage für eine zukünftige Datenökonomie geschaffen werden, die den Erfordernissen einer sozialen Marktwirtschaft entspricht: Offene Ökosysteme, die Vielfalt und Pluralität betonen und den Wettbewerb aller Marktteilnehmenden fördern. Drei strategische Handlungsbereiche und deren enge Verknüpfung sind im folgenden Sinne entscheidend für eine erfolgreiche Umsetzung von Industrie 4.0: Souveränität, Interoperabilität und Nachhaltigkeit. [177]

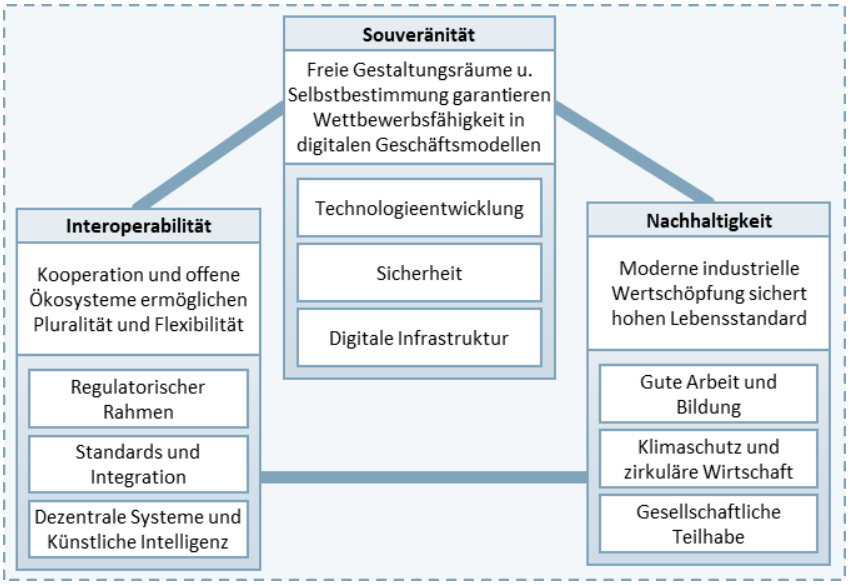


Abbildung 60: Leitbild 2030 für Industrie 4.0 [177]

Interoperabilität

In der Industrie 4.0 ist die flexible Vernetzung der verschiedenen Teilnehmenden zu agilen Wertschöpfungsnetzen ein wesentlicher Bestandteil digitaler Geschäftsprozesse. Die Interoperabilität aller Beteiligten ist für die Entwicklung solcher komplexen, dezentralen Strukturen von entscheidender strategischer Bedeutung. Die direkte operative und prozessuale Vernetzung über Unternehmens- und Branchengrenzen hinweg wird nur durch ein hohes Maß an Interoperabilität sichergestellt, zu dem sich alle Partner eines Ökosystems bekennen und gleichermaßen beitragen. Im Gegensatz dazu erlauben interoperable Strukturen und Schnittstellen Herstellern und Kundinnen und Kunden, sich uneingeschränkt an digitalen Wertschöpfungsnetzen zu beteiligen, was letztendlich zur Entwicklung neuer Geschäftsmodelle beitragen kann. So fördert die Interoperabilität auch die Souveränität. [177]

Als die drei wichtigsten Bausteine werden angesehen:

- Standards und Integration,
- regulatorischer Rahmen und
- dezentrale Systeme und KI. [177]

Verwaltungsschale

In der Verwaltungsschale wird der digitale Zwilling für Industrie 4.0 umgesetzt. Es handelt sich beim Digitalen Zwilling um eine digitale Darstellung, die den Anforderungen verschiedener Anwendungsfälle genügt. [178]

Die Verwaltungsschale kann Interoperabilität zwischen verschiedenen Herstellern ermöglichen. Sie steht für intelligente und nicht-intelligente Produkte zur Verfügung und repräsentiert den vollständigen Lebenszyklus von Maschinen, Anlagen, Geräten und Produkten. Durch die Verwaltungsschale können geordnete Wertschöpfungsketten geschaffen werden. Die digitale Basis für autonome Systeme und KI kann die Verwaltungsschale bilden. [178]

Der Gegenstand wird durch die Verwaltungsschale in die Industrie 4.0-Kommunikation integriert. Sie ist im Internet erreichbar und kann das Asset eindeutig identifizieren. Sie verfügt über eine standardisierte und sichere Kommunikationsschnittstelle und kann intelligente und nicht-intelligente („passive“) Assets (ohne Kommunikationsschnittstelle) einbinden. Dies geschieht bspw. über Bar- oder QR-Codes. Die Verwaltungsschale bildet den gesamten Produktlebenszyklus ab. [178]

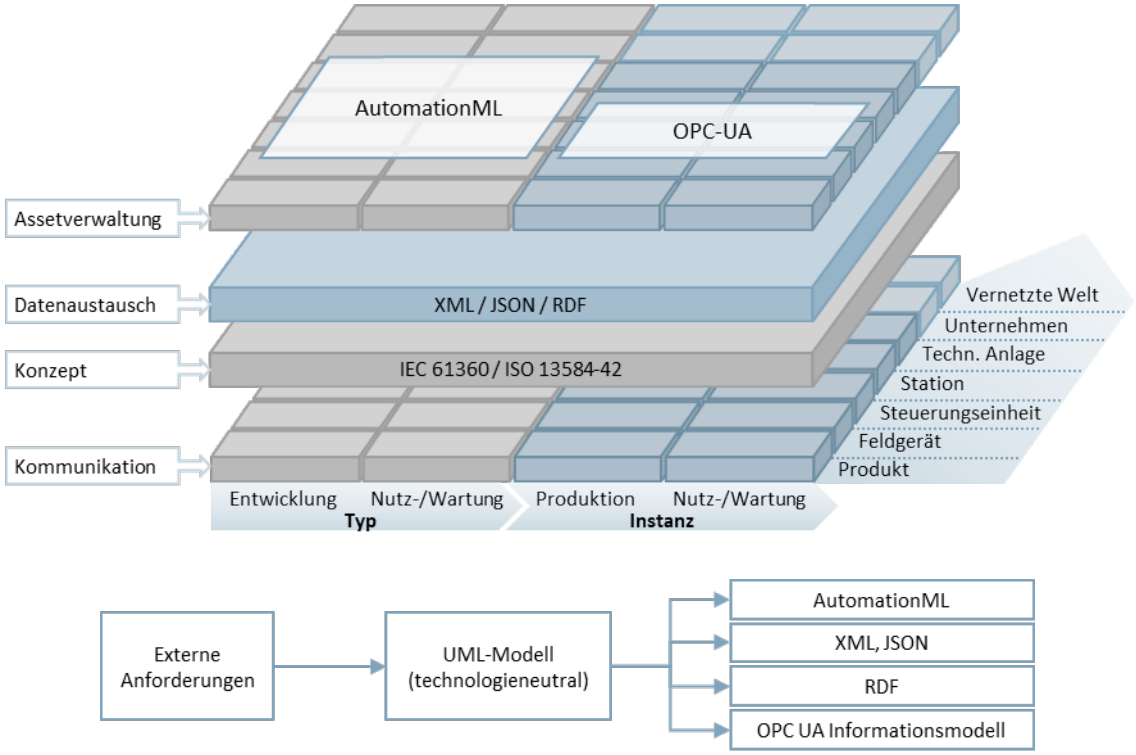


Abbildung 61: Die Verwaltungsschale im Überblick [Eigene Darstellung nach [178]]

7.1.3.4 Industrial Internet of Things

Es existieren mehrere IoT-Definitionen. Die für den industriellen Gebrauch relevanten beschreiben explizit die Arten intelligenter Komponenten, die in herkömmliche Objekte integriert sind. Dadurch ist es möglich, dass diese Gegenstände als IoT-Geräte betrachtet werden und Teil von Cyber-Physical Systems (CPS) sein können. [179]

Um den gesamten Produktionswert zu optimieren, handelt es sich um ein System, das vernetzte intelligente Objekte, cyberphysische Anlagen, zugehörige generische Informationstechnologien und optionale Cloud- oder Edge-Computing-Plattformen umfasst. Diese ermöglichen den intelligenten und autonomen Echtzeitzugang, die Erfassung, Analyse, Kommunikation und den Austausch von Prozess-, Produkt- und/oder Serviceinformationen in der Industrie. Dieser Wert kann sich auf: Verbesserte Lieferung von Waren oder Dienstleistungen, Produktivitätssteigerung, Arbeitskosteneinsparung, Energieeinsparung und Verkürzung des Build-to-Order-Zyklus. [179]

Folgende Protokolle werden laut Boyes et al. [179] zum Aufbau und zur Verwaltung von Verbindungen sowie zur Übermittlung von Informationen verwendet. Sie können in drei Klassen eingeteilt werden:

- Infrastruktur (IPv4, IPv6, 6LoWPAN, UDP),
- Erkennung (mDNS, HyperCat, UPnP) und
- Datenprotokolle (MQTT, XMPP, LLAP, REST, SOAP). [179]

TABELLE 57: AUSGEWÄHLTE KOMMUNIKATIONSSTANDARDS FÜR DAS IIOT

Abkürzung	Bezeichnung	Quelle/Referenz
OPC UA	OPC Unified Architecture	[180][181]
MQTT + Sparkplug	Message Queuing Telem-etry Transport	[124][182]
mioty	Mioty	[183][184]
IO-Link	IO-Link	[94]
USB	Universal Serial Bus	[301]

Im Folgenden werden ausgewählte Kommunikationsprotokolle und Standards kurz vorgestellt.

OPC UA

Für den sicheren und verlässlichen Datenaustausch in der industriellen Automatisierung sowie in anderen Branchen ist laut [180] OPC der geeignete Interoperabilitätsstandard. Es ist unabhängig von der Plattform und sorgt für einen reibungslosen Informationsaustausch zwischen den Geräten unterschiedlicher Anbieter. Die OPC Foundation hat die Verantwortung für die Ausarbeitung und Wartung dieses Standards. [180]

Der OPC-Standard besteht aus verschiedenen Spezifikationen, die von Softwareentwicklern, Endbenutzern und Branchenanbietern erarbeitet wurden. Diese Anforderungen legen die Verbindung zwischen Clients und Servern sowie zwischen Servern und Servern fest. Dazu gehören der Zugang zu Echtzeitdaten, die Überwachung von Alarmen und Ereignissen, der Zugang zu historischen Daten sowie weitere Anwendungen. [180]

Eine plattformunabhängige serviceorientierte Architektur namens OPC Unified Architecture (UA) wurde 2008 veröffentlicht. Sie integriert alle Funktionen der einzelnen OPC Classic-Spezifikationen in einem erweiterbaren Framework. Mit diesem mehrstufigen Ansatz werden die ursprünglichen Ziele der Design-Spezifikation erreicht: [181]

- *Funktionale Äquivalenz:* alle COM OPC Classic-Spezifikationen werden auf UA abgebildet,
- *Plattformunabhängigkeit:* vom eingebetteten Mikrocontroller bis zur cloudbasierten Infrastruktur,
- *sicher:* Verschlüsselung, Authentifizierung und Prüfung,
- *erweiterbar:* Möglichkeit, neue Funktionen hinzuzufügen, ohne bestehende Anwendungen zu beeinträchtigen und
- *umfassende Informationsmodellierung:* zur Definition komplexer Informationen. [181]

MQTT und Sparkplug

Sparkplug wird von der Eclipse Foundation betrieben und ist eine Open-Source-Spezifikation. Sie bietet MQTT Nutzern ein Framework, mit dem sie Daten aus ihren Anwendungen, Sensoren, Geräten und Gateways nahtlos in die MQTT-Infrastruktur integrieren können. Es wird auf GitHub veröffentlicht. Die Entwicklung von Sparkplug unterliegt dem Eclipse Foundation Specification Process (EFSP). Die Spezifikationsdokumente können von jedem für jeden Zweck kopiert und weitergegeben werden, ohne Kosten oder Lizenzgebühren. [182]

Die Sparkplug-Spezifikation zielt darauf ab, einen MQTT-Topic-Namespace, Payload und Session-State-Management festzulegen, der im Allgemeinen für den gesamten IIoT-Markt geeignet ist, aber insbesondere den Anforderungen von Echtzeit-SCADA/Control-HMI-Lösungen entspricht. MQTT-basierte Infrastrukturen können wertvollere Echtzeitinformationen auch für die Anforderungen von Line-of-Business- und MES-Lösungen liefern, wenn die betrieblichen Anforderungen dieser Systeme erfüllt werden. [182]

Mioty

Für die Übermittlung von Sensordaten und Information zur Steuerung in Netzwerken kommen robuste Funktechnologien zum Einsatz. In der Ära des IoT werden Menschen und Objekte auf intelligente Weise miteinander vernetzt. Dies führt zu Neuerungen z. B. in den Bereichen Smart City und Industrie 4.0. [183][184]

Das IoT-Protokoll mioty, welches vom Fraunhofer IIS entwickelt wurde, stellt in Bezug auf Skalierbarkeit, Kosteneffizienz, Reichweite, Übertragungssicherheit und Batterielebensdauer neue Möglichkeiten für die drahtlose Datenübertragung zu Verfügung. Ein asymmetrisches Übertragungsverfahren, das Telegramsplitting genannt wird, umfasst zahlreiche einfache IoT-Endgeräte und zentrale Basisstationen. Die stabile Übertragung von Daten kann bereits über eine Basisstation gewährleistet werden. Mioty erreicht eine Reichweite von zahlreichen Kilometern und ist bekannt für seine Energieeffizienz, wobei die Batterielebensdauer bis zu 20 Jahre beträgt. [183][184]

IO-Link

Der IO-Link Master kann wie in Abbildung 62 dargestellt als Gateway zu Ethernet-basierten Datennetzen fungieren.

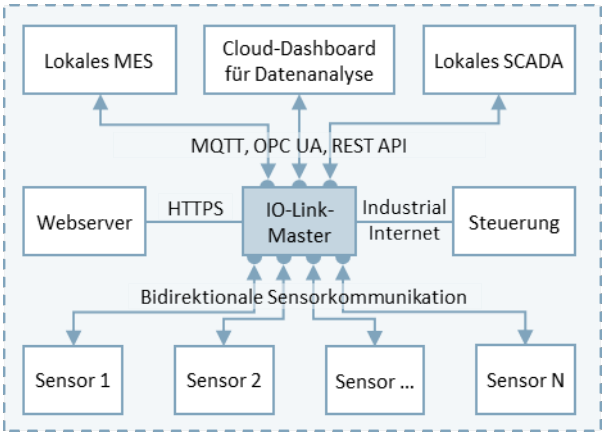


Abbildung 62: Verbindungsmöglichkeiten und gängige Schnittstellen an Auswerteeinheit oder Gateway [Eigene Darstellung nach [185]]

Die Ausstattung der Daten mit einer entsprechenden Semantik (siehe Abschnitt Modellierung und Datenaustausch) müsste für diesen Fall im IO-Link-Master stattfinden.

7.1.3.5 Betriebstechnologie im Wandel durch Industrie 4.0

Die Automatisierungspyramide wurde lange Zeit als Bezugspunkt und bedeutende Leitlinie für Projekte im Bereich der Automatisierung betrachtet. Andere Darstellungen treten heutzutage zunehmend auf und werden als aktueller Ansatz verbreitet. [Q48] Die Pyramide ist im Hinblick auf Digitalisierung und IIoT aus den folgenden Gründen unzureichend geworden:

1. Alleinstellungsmerkmale und in der Pyramide dargestellte Strategie sind nicht mehr uneingeschränkt gültig. [186]
2. Smart Factory besteht nicht nur aus Maschinen und einem ERP. Es gibt unterschiedliche Schnittstellen auch außerhalb der Pyramide (Condition Monitoring, fahrerlose Transportsysteme). [186]
3. Der Fokus auf ein ERP als alleinigen Endpunkt der Pyramide ist nicht mehr ausreichend. Die Daten werden mit unterschiedlichen Systemen und Technologien erhoben. [186]
4. Digitale Vernetzung ist viel mehr als das Fortführen der Automatisierung. [186]
5. Es gibt den einen Weg via MES heute oft nicht mehr. Es werden verschiedene Technologien für die Datenübertragung parallel genutzt. Beispiele hierfür sind LPWAN, UWB, OPC UA, MQTT oder Node-Red. [186]

Es ist erkennbar, dass die Daten, die in der Fertigung von Smart Factories gesammelt und dort verwendet werden, aus sehr verschiedenen Quellen stammen. Eines haben diese anderen Technologien und Elemente gemeinsam: Sie sind in der Regel nicht direkt mit der jeweiligen Anlage verbunden, sondern integrieren sich auf andere Weise in die Datenlandschaft. Deshalb ist eine Ergänzung der Pyramide um weitere Quellen, Datenströme und Anwendungen erforderlich. Die Anwendungen arbeiten außerdem mit verschiedenen Technologien und Schnittstellen zusammen. [186]

Diese Einflüsse werden in einer veränderten Pyramide, wie in Abbildung 63 dargestellt, berücksichtigt.

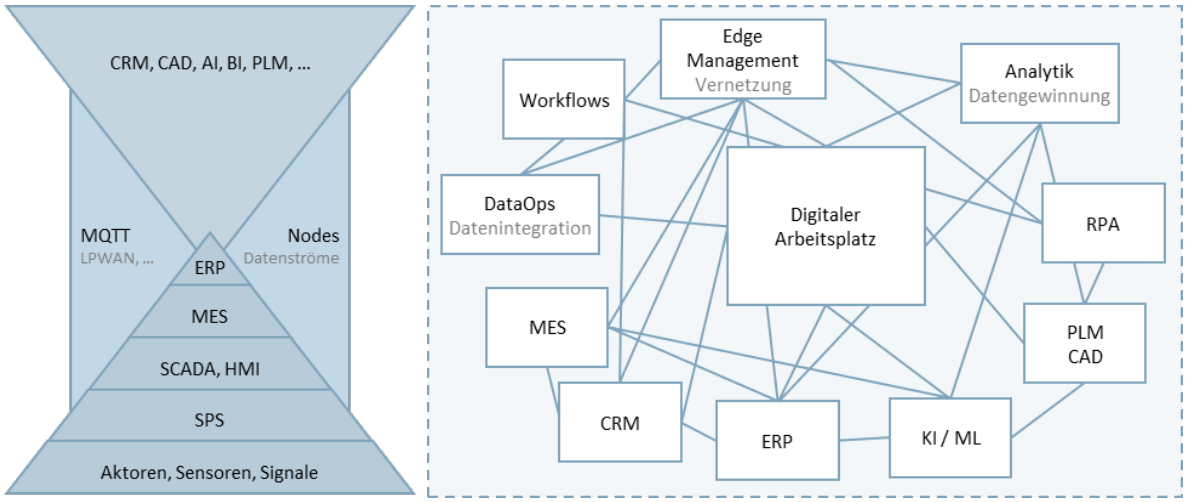


Abbildung 63: veränderte Automatisierungspyramide als Pyramidenstruktur (links) und als Netzwerkstruktur (rechts) [Eigene Darstellung nach [186] und [188]]

Die Gedanken des IIOT werden die Pyramide zukünftig noch stärker verändern, sodass die in Abbildung 63 (rechts) gezeigte netzwerkartige Abbildung die heutige Situation und auch den Blick in die kommenden Jahre bisher am besten darstellt. [186]

Die aufgezeigten Veränderungen lassen sich ebenfalls am gezeigten Beispiel erkennen. Durch neue Netzwerkkomponenten und Kommunikationsprotokolle, sowie netzwerkfähige Sensoren und Aktoren oder Sensornetzwerke werden neue Kommunikationsverbindungen möglich. Diese können sowohl in der traditionellen Form der Automatisierungspyramide existieren, als auch als Erweiterung mit direktem Zugang zu übergeordneten Ebenen. Beispielhaft ist dies in Abbildung 64 wiederum am Beispiel der Fabrikautomation aufgezeigt.

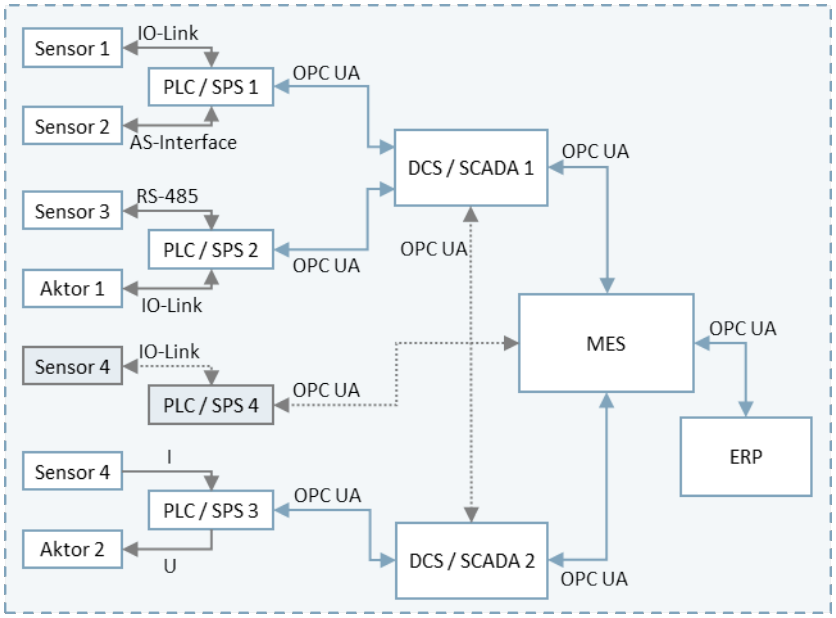


Abbildung 64: Veränderungen in der Fabrikautomation durch IIoT-Technologien [Fraunhofer ENAS]

Die durch Digitalisierung, IoT und Industrie 4.0 ausgelösten Veränderungen gehen weit über eine Erweiterung der Automatisierungspyramide und Digitalisierung der einzelnen Komponenten hinaus. Daten werden aus den unterschiedlichsten Quellen geliefert. Die Komponenten und Systeme sind vernetzt und können miteinander kommunizieren. Dabei werden aktuell die verschiedensten Kommunikationstechnologien eingesetzt. Dies führt zu einer zunehmenden Heterogenität der Automatisierungssysteme, zu Kompatibilitätsproblemen und zu steigender Komplexität der Datenauswertung. Aus diesem Grund wird im Rahmen des IIoT verstärkt an der Entwicklung und Etablierung von Kommunikationsstandards gearbeitet.

7.1.3.6 Zusammenfassung des Abschnittes

Ziel des Abschnittes 7.1.3 war es, einen umfassenden Überblick über den Einsatz von sensorbasierten Technologien in der industriellen Automatisierung zu erlangen. Durch den in den siebziger Jahren beginnenden Einsatz von Elektronik und Informationstechnologien zur Automatisierung der Produktion ist heute bereits ein hoher Grad an Digitalisierung im industriellen Umfeld vorhanden. Die vierte industrielle Revolution treibt die Vernetzung der Produktionssysteme weiter voran und stellt eine Verbindung zwischen realen Objekten und virtuellen Prozessen her.

Die Recherche begann mit der klassischen Betriebstechnologie und der Automatisierungspyramide. Auf dieser Grundlage werden seit vielen Jahren Automatisierungssysteme im industriellen Umfeld entwickelt. Anschließend wurde das Konzept von Industrie 4.0 betrachtet. Das Leitbild für Industrie 4.0 mit Souveränität, Nachhaltigkeit und Interoperabilität wurde als Lösungsansatz zur Gestaltung digitaler Ökosysteme aufgenommen. Abschließend wurde das Konzept der Verwaltungsschale für die Umsetzung des digitalen Zwillings für Industrie 4.0 recherchiert.

In der industriellen Automatisierung gibt es gefestigte Strukturen, die auf etablierten Konzepten und Technologien beruhen. Derzeit findet der Übergang von Industrie 3.0 zu Industrie 4.0 statt. Dabei verändert die voranschreitende Vernetzung der Produktionssysteme die etablierten Strukturen. Die Interoperabilität der Systeme und Technologien wird als bedeutsamer Schritt gesehen, vor allem vor dem Hintergrund einer historisch gewachsenen großen Heterogenität der Technologien.

Barrieren gibt es auf verschiedenen Ebenen, wie z. B. unterschiedliche Systeme, Fragen der IT-Sicherheit, Mangel an qualifizierten Mitarbeiterinnen und Mitarbeitern, hohe Investitionskosten, Angst vor Veränderungen oder mangelnde Infrastruktur.

Die Zukunftsvision wird durch das Leitbild von Industrie 4.0 gezeichnet: Souveränität, Interoperabilität und Nachhaltigkeit. Es gibt einen großen Bedarf nach einem offenen, standardisierten Kommunikationsstandard, welcher den Datenaustausch zwischen den Systemen verbessert. Durch den Bedarf der industriellen Automatisierung werden Kommunikationsprotokolle wie MQTT und Open Platform Communications Unified Architecture (OPC UA) vorangetrieben und zunehmend standardisiert.

7.1.4 Sensorbasierte Technologien im Bahnsystem

7.1.4.1 Rechercheziele des Abschnittes

Im Abschnitt 7.1.4 wurden sensorbasierte Technologien im Bahnsystem betrachtet. Der Abschnitt gliedert sich neben dieser Einleitung und einer Zusammenfassung in vier weitere Abschnitte zu Personenverkehr, Güterverkehr, Infrastruktur und Systemarchitekturen. Ziel war es, einen umfassenden Überblick über den Stand der Technik zur Vernetzung von Systemen und Komponenten sowie zur Datenkommunikation im Bahnsystem zu erhalten. Darüber hinaus wurden aktuelle Forschungsergebnisse aus verschiedenen Shift2Rail-Projekten, wie z. B. Connecta und Safe4Rail einbezogen. Begonnen wurde mit einer Recherche über gängige Suchmaschinen und in frei zugänglichen Dokumenten der Shift2Rail-Projekte. Detaillierte Informationen zu einzelnen Technologien wurden darüber hinaus in wissenschaftlichen Veröffentlichungen recherchiert.

Leistungsfähige Netzwerke und Protokolle zur Datenkommunikation sind Voraussetzung für die Etablierung von sensorbasierten Technologien, wie sie bspw. in den in diesem Projekt erarbeiteten Use Cases (siehe Abschnitt 4.2.2) beschrieben wurden. In Abschnitt 7.2 werden die Ergebnisse der Recherche daher klassifiziert, analysiert und an beispielhaften Use Cases dargestellt.

7.1.4.2 Personenverkehr

Zug-Kommunikationsnetzwerke

In der folgenden Tabelle 58 sind die wichtigsten Zug-Kommunikationsnetze aufgeführt. Sie werden im weiteren Verlauf detaillierter beschrieben.

TABELLE 58: ÜBERSICHT ZUG-KOMMUNIKATIONSNETZWERKE

Abkürzung	Bezeichnung	Quelle/Referenz
TCN	Train Communication Network	[187], [263]
NG-TCN	Next Generation TCN	[194]
WTB	Wire Train Bus	[190], [191]
MVB	Multifunction Vehicle Bus	[191]
CANopen	Controller Area Network open	[80]
ETB	Ethernet train backbone	[194]

Abkürzung	Bezeichnung	Quelle/Referenz
ECN	Ethernet consist network	[195]
WLTB	Wireless Train Backbone	[194]
TRDP	Train Real Time Data Protocol	[263], [269], [265]

TCN – Train Communication Network

Das Train Communication Network besteht in seiner Struktur aus zwei Stufen. Die erste Stufe besteht aus einem Zugbus, dem Wire Train Bus (WTB) und die zweite Stufe aus einem Fahrzeugbus, dem Multifunction Vehicle Bus (MVB) [189]. Für die Kommunikation sind im Train Communication Network (TCN) zwei unterschiedliche Datenarten definiert. Der Wire Train Bus kann sowohl elektrisch als auch optisch übertragen werden. Für die elektrische Übertragung kommen sogenannte Twisted Pair Kabel zum Einsatz und bei optischer Übertragung Glasfaser. Im Physical Layer wird eine RS-485 Schnittstelle mit einer digitalen Übertragungsrate von 1 Mbit/s verwendet. Der Multifunction Vehicle Bus wird hingegen als echter Datenbus nach dem Prinzip Single Master – Multi Slave ausgeführt. Die Signalpegel auf der Datenleitung werden differentiell nach dem Industriestandard RS-485 mit einer Brutto-Übertragungsrate von 1,5 Mbits/s übertragen [190].

Seit etwa 1995 kommt bei Eisenbahnfahrzeugen der folgende Hersteller für den Feldbus MVB zum Einsatz: Siemens, AEG/ABB/Adtranz und Bombardier. Hingegen sind mit TCN die nachfolgenden Triebzüge der Deutschen Bahn ausgestattet: InterCityExpress ICE T, ICE TD und ICE 3. [192]

Union International des Chemins de Fer (UIC)-Kabel bestehen dabei aus mehreren Adern, die je nach UIC-Standard verschiedene Belegungen aufweisen. 1996 noch 18-adrig, führte der Wechsel von WTB (Wire Train Bus) zu Ethernet Train Backbone (ETB) und ab 2017 zu 24 Adern. UIC-Standards definieren Funktionalitäten wie die Notbremsüberbrückung oder Statusübermittlungen („Notbremse gezogen“). [193]

ETB – Ethernet Train Backbone und WLTB – Wireless Train Backbone

Das Wireless Train Backbone (WLTB) ist die Weiterentwicklung des ETB [194], wobei die Verwendung von Funktechnologie für die Kommunikation zugelassen wird. Technisch basiert WLTB auf Long Term Evolution (LTE). Da LTE-Funkressourcenplanung bietet, kann eine skalierbare und zuverlässige Kommunikation zwischen zwei gekoppelten Zügen aufgesetzt werden. Im Gegensatz zu 802.11-basierten Funkanwendungen (Wireless Local Area Networks (WLAN)) bietet LTE eine Zugriffsplanung, wodurch Kollisionen im Netzwerk vermieden werden. Im Gegensatz zu WLTB ist ETB ein zugweites Kommunikationsnetzwerk, welches auf der Ethernet-Technologie basiert und mit IEC-61375-2-5 standardisiert ist.

TCMS – Train Control and Monitoring System

Das Train Control and Monitoring System (TCMS) ist ein Bordsystem für Züge, das mit dem Einsatzzweck gebaut wurde, eine ganze Reihe von Zugausrüstungen und deren funktionalen Prozessen zu steuern und zu überwachen. TCMS zentralisiert alle Informationen zu Betriebszuständen der gesamten sogenannten „intelligenten“ Zugausrüstung, basierend auf einer Steuerungs- und Überwachungsarchitektur. [198]

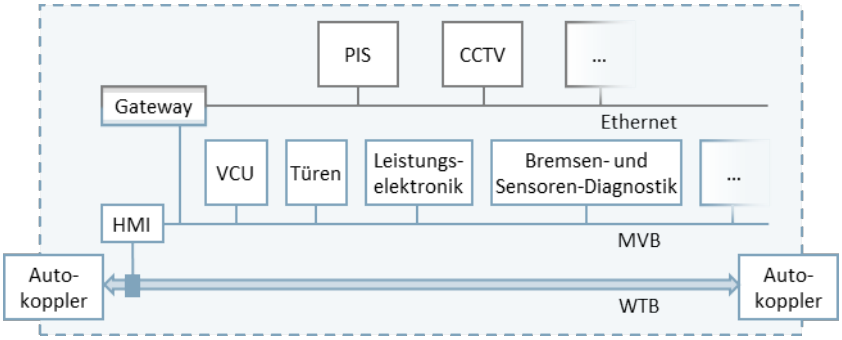


Abbildung 65: TCMS Architektur [Eigene Darstellung nach [197]]

In den Shift2Rail-Projekten CONNECTA und Safe4Rail wird an Technologien für eine Weiterentwicklung des TCMS gearbeitet [259].

NG-TCN Next Generation of Train Communication Network

Das Next-Generation Train Communication Network (NG-TCN) fungiert als Subsystem des TCMS und definiert den Teil der Architektur, der die Infrastruktur für die Kommunikation von Endgeräten innerhalb des Zuges verwendet. Das Subsystem besteht insgesamt aus dem NG-TCN Netzwerk, seinen Funktionen und dem Service auf den Endgeräten, der für Nutzanwendungen bereitgestellt wird. Das NG-TCN wird durch die folgenden zwei Betriebsschnittstellen begrenzt: 1) Schnittstellen zwischen dem NG-TCN und den Endgeräten (innerhalb eines Zuges), 2) Schnittstellen zwischen Zügen, um eine Zugin-teroperabilität herzustellen, wenn während des Betriebes Züge miteinander verbunden werden. Bei NG-TCN können die Endgeräte sowohl sicherheitsrelevante Anwendungen als auch nicht sicherheitsrelevante Anwendungen umsetzen. Da das NG-TCN ein nicht vertrauenswürdiges Netzwerk ist, müssen technische Lösungen implementiert werden, um das entsprechende Sicherheitsniveau auf Anwendungsebene zu erreichen. Dabei wird die EN 50159 Serie als Referenz verwendet. [196]

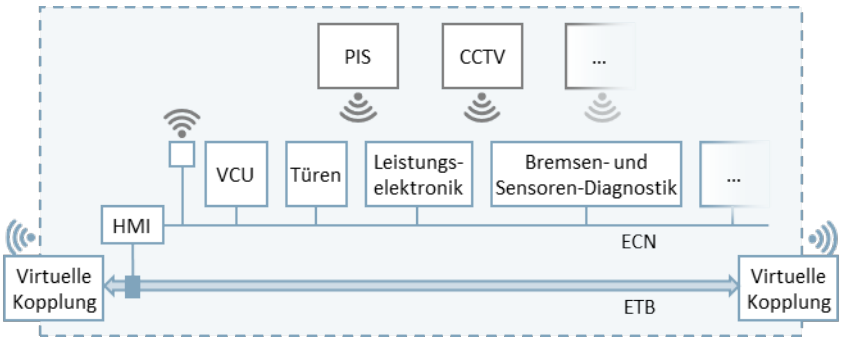


Abbildung 66: NG-TCMS Architektur [Eigene Darstellung nach [197]]

Aus diesem Grund sollen künftige TCN auf den Ethernet-Standards Time-Sensitive Networking (TSN) basieren, die Echtzeitfähigkeit bieten. Die OCORA-Initiative (Open CCS On-board Reference Architecture) der europäischen Bahnunternehmen Deutsche Bahn, NS (Niederlande), SNCF (Frankreich), die Österreichischen Bundesbahnen (ÖBB) oder die Schweizerischen Bundesbahnen (SBB) beschäftigt sich derzeit intensiv mit der konkreten Gestaltung dieser NG-TCN (Next-Generation TCN). [269]

Recherche für den Use Case „Überwachung Bremse“

Im Kapitel 4 Bestandsaufnahme Sensormarkt wurde im Abschnitt 4.1 eine Use Case Analyse durchgeführt. Diese ergab eine Tabelle mit 38 möglichen Anwendungen von Sensorsystemen im Bahnsystem.

Der Use Case „Überwachung Bremse“ war in dieser Liste enthalten. Die Ergebnisliste wurde durch eine Online-Umfrage und einen ersten Workshop bewertet. Die Bewertung führte zu einer Aufnahme des Use Cases „Überwachung Bremse“ in die Auswahlliste. Diese war unter anderem Ausgangspunkt für die Recherchearbeiten in diesem Kapitel. In der weiteren Analyse und Diskussion innerhalb des Konsortiums und im zweiten Workshop wurde dieser Use Case in der Priorisierungsliste weiter nach hinten gestellt (siehe Abschnitt 4.2.2) und fiel dadurch aus der Auswahlliste heraus. Die Ergebnisse der Recherche sollten allerdings im Bericht verbleiben und sind daher an verschiedenen Stellen zu finden.

Der erste Use Case zu dem spezifisch recherchiert wurde, war der Use Case „Überwachung Bremse“ (Bremskraft, Temperatur, C-Druck). Es wurde zu Bremssystemen und zur Elektropneumatisch (EP)-Leitung eine Bestandsaufnahme durchgeführt.

Elektropneumatische Bremse EP-Leitung

Die im Bahnsystem eingesetzte elektropneumatische Bremse verlangsamt das Fahrzeug per Druckluft, indem eine elektrische Übermittlung notwendiger Signale an beteiligten Druckluftventilen stattfindet. [199] Im Triebwagen der Bahn existiert ein Steuergerät zur entsprechenden Signalgebung. Die Übermittlung erfolgt dabei über WTB für die ganze Zuglänge oder über MVB innerhalb eines Fahrzeugs. Zur Funktionalität ist eine automatische Kupplung notwendig, weswegen die EP-Bremse bei Güterzügen nicht zum Einsatz kommt. Die Übertragung und Überwachung der Steuerbefehle können mit einer EP-Leitung oder UIC-Kabeln stattfinden.

Recherche für den Use Case „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“

Dieser Use Case war ebenfalls in der Ergebnisliste von Kapitel 4 enthalten und wurde in einer Online-Umfrage und im ersten Workshop bewertet. Der Use Case wurde hoch bewertet und insgesamt mit einer guten Umsetzbarkeit eingeschätzt. Zudem ergab die Analyse eine hohe Relevanz für die nachfolgenden Arbeitspakete. Im zweiten Workshop wurde der Use Case mit mittleren Werten für die Marktreife und -attraktivität bewertet. Er wurde im Abschnitt 7.2.6.3 zur Ergebnisdarstellung genutzt und im Abschnitt 8.2.1 zur Risikoanalyse der Datensicherheit und Cybersecurity.

Startpunkt zu dieser Use Case-spezifischen Recherche war eine allgemeine Recherche zur Systemarchitektur Tür. Hierbei wurden sowohl zugweite Türsystem-Architekturen als auch lokale Architektur-systeme innerhalb der Tür selbst einbezogen.

TABELLE 59: ÜBERSICHT TÜRSTEUERSYSTEME

Abkürzung	Bezeichnung	Quelle/Referenz
DS	Dezentrale Türsteuerung	[200]
ZS	Zentrale Türsteuerung	[201]
DSM	Dezentrale Türsteuerung mit Master	[202]
ZMSS	Zentrales Master/Slave Türsteuersystem	[203]
SIDOOR	SIDOOR Siemens	[204], [205]
Bircher PSC	Bircher PSC	[206]
Griessbach	Griessbach Türsteuerung	[207]

Türsteuerung und Türsensorik

Seit 1972 ist es bereits erforderlich, dass die Türen fernschließbar sind. [208] Dafür sind Adern im UIC-Kabel (Union Internationale des Chemins de Fer) reserviert. Schon seit 1980 (allerdings erst seit 2000 international) sind sogenannte Türblockiereinrichtungen verpflichtend. [209] Sie sollen die Türöffnung unter bestimmten Bedingungen verhindern. So definiert „TB5“ eine Blockade ab 5 km/h, „TB0“ gar eine manuelle Blockade zur Beseitigung der Schließlücke (Zeit zwischen Anfahrt und Erreichen der 5 km/h). [210] Seitenselektive Türsteuerung Fernverkehr (SSTF) erlaubt zusätzlich die namensgebende Auswahl der Türen. [211] Türsteuerungen wie Selbstabfertigung Triebfahrzeugführer (SAT) und (Technikbasierte Abfertigungsverfahren) TAV erweitern die Funktionalität um Schließbarkeit durch die Fahrzeugführerin oder den Fahrzeugführer (statt Fahreugbegleiterin oder Zugbegleiter) bzw. bei TAV automatisiert und Signalgebung über die Zustände der Türen. [210] Eine automatisierte Schließung der Türen wie bei TAV erfordert den Einsatz von Sicherheitsmechanismen um Einklemmungen zu verhindern oder zu erkennen. [212]

Hier hat die Recherche verschiedene Sensorsysteme identifiziert. Einfache Lichtschranken erlaubten eine Umgehung des überwachten Bereiches, wenn sie bspw. nur den Boden überwachten, weswegen moderne Systeme Lichtgitter nutzen, um mehr Bereiche abzudecken. Druckplatten im Fußbereich und Druckwellenschalter in Türen, genauer deren Dichtungsgummi, können auf physische Einflüsse reagieren. In der klassischen Leittechnik werden die Sensoren mit dem nächsten, übergeordneten Steuergerät verbunden (siehe Kapitel 7.1.3.2). Bei einem dezentralen Konzept ist es das Steuergerät der jeweiligen Tür. Bei einem zentralen Konzept ist es das zentrale Steuergerät im Wagon oder Triebfahrzeug.

Recherchen einer Risikoanalyse zeigten weitere Möglichkeiten auf, welche Sensorik Blockaden detektieren könnte: Optoelektronik in den Dichtungsgummis (Detektion auf Raumverengung mittels gepulstem Infrarotlicht), Motorstromüberwachung (Vergleich Stromkurven bei vergangenen Öffnungen und Schließungen), Weg-Zeit-Geber (Abweichungen zu vergangenen Vorgängen), Widerstandsmessung einer in die Türgummilippen integrierten elektrischen Schaltleiste bei Verformung und abschließend der Einsatz von Überwachungskameras. [210]

Allen Sensorsystemen gemein ist, dass eine Reversierung bei Hinderniserkennung stattfinden muss, d. h. die Tür geht wieder auf. Weiterhin sollte ein optionales erzwungenes (und langsames) Schließen trotz Hindernis möglich sein. Die Prüfung der Fehlerfreiheit erfolgt durch Schließkraftmessung, bei der Messkeulen auftretende Kräfte beim Schließvorgang erfassen. [213]

Dezentrale Türsteuerung

Bei der dezentralen Steuerung wird pro Tür ein Steuergerät verbaut, welches ausschließlich diese Tür steuert. Jedes Türsteuergerät besitzt eine eigene Anbindung zum Fahrzeugbus. Bei diesem Konzept lassen sich kurze Leitungen zwischen Steuergerät und Tür realisieren. Es eignet sich daher besonders gut bei Türantrieben mit Elektromotor. [200]

Zentrale Türsteuerung

Im Gegensatz zur dezentralen Steuerung ist bei der zentralen Steuerung nur ein Steuergerät verbaut. Dieses steuert alle Türen des Fahrzeugs und ist zentrales Bindeglied zum Fahrzeugbus. Bei diesem Aufbau entstehen verhältnismäßig lange Leitungen zwischen Steuergerät und Tür. Es eignet sich daher eher für pneumatische Türantriebe. Das Steuergerät lässt sich dabei konfigurieren und nach Anzahl und Art der Tür anpassen. [201]

Dezentrale Türsteuerung mit Master

Dieses Prinzip ist ähnlich aufgebaut wie die dezentrale Steuerung. Jede Tür verfügt über ein eigenes Steuergerät. Die verbauten Steuergeräte sind über ein Bussystem, z. B. RS-485 oder CAN, an eine zentrale Mastersteuerung angeschlossen. Der Master übermittelt so die Steuersignale an die jeweiligen dezentralen Türsteuergeräte und verfügt über einen zentralen Diagnosespeicher. An das Fahrzeug ist der Master wieder über den Fahrzeugbus angeschlossen. [202]

Zentrales Master/Slave Türsteuersystem

Auch dieses System verfügt über ein zentrales Mastergerät, welches mit den jeweiligen Türsteuergeräten über ein Bussystem verbunden ist. Die Türsteuergeräte sind bei diesem Prinzip als Slavegeräte ausgeführt. Sie arbeiten Steuerbefehle selbstständig ab und sind in der Lage dem Master Zustandsinformationen zu übermitteln. Die Anbindung an den Fahrzeugbus erfolgt auch hier durch den Master, der wiederrum über einen zentralen Diagnosespeicher verfügt. [203]

SIDOOR Siemens

Siemens bietet mit SIDOOR ein Türmanagementsystem, welches sich herstellerunabhängig für alle Türen eignet. „Die im Betrieb anfallenden Daten lassen sich lokal oder global auslesen und auswerten, um unnötige Wartungsarbeiten ebenso zu vermeiden wie Ausfallzeiten. Entsprechende Kommunikationsschnittstellen können dank der Unabhängigkeit vom Türsystem einfach ergänzt werden.“ [204] Das System steuert stets die Tür gemäß der Normen und errechnet automatisch das optimale Fahrverhalten der Tür. Es besteht aus einem Netzteil, welches das Türsteuergerät, den Türantrieb sowie die Tür versorgt. Das Türsteuergerät verfügt dabei über digitale Eingänge wie bspw. Lichtschranken oder Türtaster. Zudem verfügt es über digitale Ausgänge, um Zustände, wie offen oder geschlossen, anzuzeigen. Das Türsteuergerät ist außerdem für eine Systemanbindung mit verschiedenen Kommunikationsschnittstellen ausgerüstet. Dies umfasst: PROFINET, PROFIBUS, CANopen und Relais-Modul. SIDOOR kann dem Konzept der dezentralen Türsteuerung zugeordnet werden. [204][205]

Bircher PSC

Die BBC Bircher Automation AG entwickelte einen Kommunikationsserver (PSC), als Bindeglied zwischen Bahnsteig und Kontrollsystem, für ein Bahnsteigtürsystem. Der Kommunikationsserver enthält dabei verschiedene Schnittstellen (CAN Bus, Input/Output (sogennate IOs), Modbus TCP, Modbus RTU, RS-485, OPC UA, Universal Serial Bus (USB) und File Transfer Protocol (FTP)) für verschiedene Anwendungen. Die Aufgabe des Kommunikationsservers besteht in der „... Erfassung des aktuellen Zustands

des Türsystems sowie die Meldung aller kritischen Zustände als Alarme ans stationsübergreifende Kontrollsystem“. [206] Bircher gibt folgende Funktionen des PSCs an:

- „Überwachung der Türen per CAN
- Zeitsynchronisierung der Türen per CAN
- Überwachung der Passagiererkennung per CAN
- Überwachung des Bahnsteigtürsystems per digitale Inputs
- Einlesen der Daten vom Zugkontrollsystem
- Lokale Anzeige der Zustände in der externen Visualisierung per OPC UA
- Stationsübergreifende Anzeige der Zustände im externen Leitsystem per Modbus
- Aufzeichnung der Daten im remanenten Speicher
- Aufzeichnung der Daten in Dateien
- Bereitstellung der Dateien per USB und FTP
- Lokale Anzeige der Zustände mit Lampen an digitale Outputs
- Schnittstelle zum externen Wartungsprogramm per OPC UA
- Firmware Update der Türen über Zentralen Software Download“ [206]

Griessbach Innentürsteuerung

Griessbach bietet eine Innentürsteuerung für automatische WC-Türen, Innentüren und Übergangstüren an. Eine integrierte Neigungssensorik passt dabei die Türautomatik der Fahrzeugneigung z. B. in Kurvenfahrten oder bei Gleisüberhöhung an. Klemm- und Quetschgefahren werden durch die Reversierfunktion mit leichtgängiger Antriebsumkehr ausgeschlossen. Durch die Firmware stehen Einstellungsoptionen zur Anpassung auf einzelne Türeigenschaften wie Flügelzahl, Türgewicht, Öffnungsweite und -geschwindigkeit zur Verfügung. Mit dieser Innentürsteuerung lassen sich Gleichstrom- als auch Drehstrommotoren ansteuern. Die Standardausführung umfasst zwei CAN-Schnittstellen. Eine CAN-Schnittstelle dient dabei zur Einbindung in das Zug-Bussystem. Es lassen sich aber auch Schnittstellen für Ethernet, Profinet oder TCP/IP integrieren. Für Parametrierung, Servicefunktionen und Firmware-updates sind zwei USB-Anschlüsse enthalten. [207]

7.1.4.3 Güterverkehr

Güterwagen verfügen in der Regel über keine elektrischen Bauteile und Infrastruktur. In den vergangenen Jahren wurde dies durch die Ausstattung einzelner Güterwagen mit autonomen Energiesystemen zur Verfolgung von Fahrzeugen und zur Überwachung des Zustands verändert. Normalerweise sind die Geräte mit einem GPS-Empfänger (Global Positioning System) ausgestattet, der die Position und den Kilometerstand dokumentiert. Die Mobilfunkverbindung ermöglicht es, Positions- und weitere Sensordaten an den Server oder in die Cloud zu übertragen. Die Anzahl der Systeme steigt aufgrund der Digitalisierungsoffensive der großen Güterwagenbetreiber stark an. Forschungsprojekte untersuchen eine stärkere Automatisierung von Güterzügen sowie eine verbesserte logistische Einbindung. [214]

Industrieplattform für Telematik und Sensorik im Schienengüterverkehr (TISS)

Im Dezember 2014 schlossen sich die Telematiksystemanbieter in der ITSS Practise Group zusammen, um bessere Voraussetzungen für den Einsatz von Telematiksystemen im Schienengüterverkehr zu schaffen. Ziel war dabei die Erstellung eines einheitlichen, offenen und kostenlosen Standards für den Austausch von Daten im Schienengüterverkehr mit den Eigenschaften: anbieterneutral, zukunftsfähig, modular, flexibel erweiterbar; Europa- und weltweit einsetzbar; geringer Implementierungsaufwand auf

Anbieter- und Nutzerseite; keine Vorschriften zu übergreifenden Prozessen; nicht wettbewerbsbeschränkend; Möglichkeit für kundenseitige oder anbieterseitige Erweiterungen; sowie Differenzierungen vom Wettbewerb. [223]

Die Anwendungsmöglichkeiten von Telematikdaten sind: Flottensteuerung, Ladungsinformation, Transportprozess (Zugbetrieb), Unterstützungsprozess/Instandhaltung und Unterstützungsprozess/Sonstige. [223]

Die Systemschnittstellen sind wie in Abbildung 67 dargestellt aufgebaut.

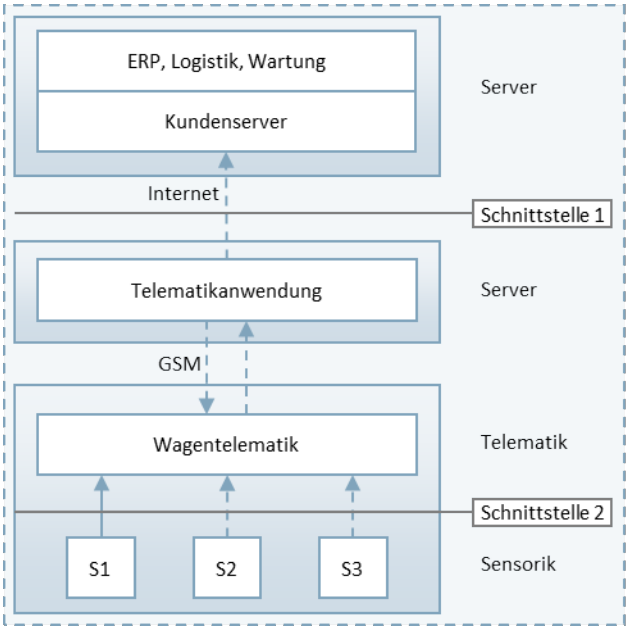


Abbildung 67: Schematische Darstellung eines Telematiksystems [Eigene Darstellung nach [223]]

Es werden zwei standardisierte Schnittstellen geschaffen, über welche Datenaustausch zwischen a) dem Telematiksystem der Anbieter und den EDV-Systemen der Kunden und b) dem Telematikgerät und der am Wagen befindlichen Sensorik stattfinden kann. Dabei können Sensoren über Kabel- oder Funkverbindung an das Telematikgerät angeschlossen werden. Daten können über die Schnittstelle 1 im JSON Datenformat abgerufen werden. [223]

Digitale Automatische Kupplung

Güterwagen werden mit einer Digitalen Automatischen Kupplung (DAK) automatisch verbunden. Die mechanische Verbindung zwischen den Wagen wird dabei ohne die Hilfe des Rangierpersonals hergestellt. Die DAK kuppelt sowohl die Luftleitung für die Bremse als auch eine Strom- und Datenbusleitung, wobei auch diese automatisch erfolgt. [225] In der Spezifikation und Erprobung ist die mechanische Kupplung zwar schon weit fortgeschritten, aber sie ist noch nicht für die elektrischen Verbindungen und Datenverbindungen geeignet. In Abbildung 68 ist eine schematische Darstellung der Verbindungen aufgezeigt.

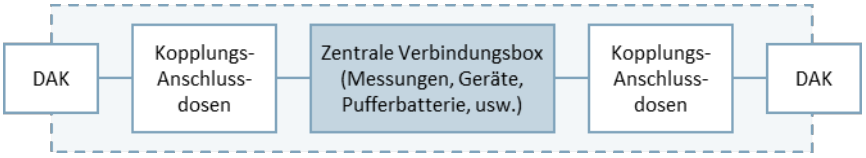


Abbildung 68: Schematische Darstellung der elektrischen Verbindungen und der Datenverbindungen bei DAC [Eigene Darstellung nach [224]]

7.1.4.4 Infrastruktur

DIANA-Plattform

Die IoT-Plattform ermöglicht die Überwachung, Steuerung und Diagnose von Fahrzeugen und verteilten Infrastrukturanlagen: [226]

- Geomonitoring: Geomonitoring unterstützt die Bauüberwachung. Vor und während der Bauzeit erhalten die Kräfte vor Ort Echtzeitdaten zum Einfluss der durchgeführten Maßnahmen. [226]
- Daten in Echtzeit: Dashboards helfen dabei, sich einen Überblick der aktuellen Daten im Feld zu verschaffen und somit das Gesamtsystem zu bewerten. Explorativ kann auf individuelle Anwendungsfälle eingegangen werden, um Informationen in Entscheidungsprozessen zu nutzen. [226]
- Präventive Instandhaltung: Durch Interpretation von Sensorinformationen zu definierten Referenzwerten wird eine frühzeitige Beurteilung möglich. Instandhaltungsarbeiten lassen sich zielgerichtet steuern und Ausfälle von Anlagen in der Infrastruktur vermeiden. [226]
- Dokumentation und Analyse: Instandhaltungsmaßnahmen werden dokumentiert und erneut auftretende Probleme registriert. Dadurch werden wiederkehrende Fehler aufgedeckt, die sich mit Prozessänderungen reduzieren lassen. [226]

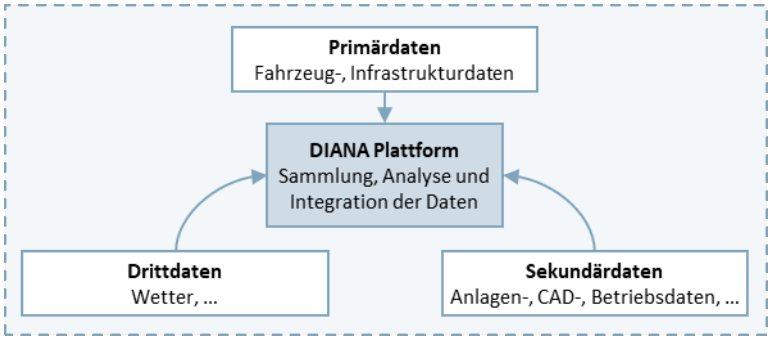


Abbildung 69: Schematische Darstellung des DIANA Systems [Eigene Darstellung nach [226]]

KONUX

KONUX bietet Lösungen für die Planung von Eisenbahninfrastruktur-Management sowie für vorausschauende Instandhaltung, Netzwerkauslastungs- und Verkehrs-Monitoring. [227]

Bestandteile der KONUX-Lösung:

- KONUX Switch: In einem ökonomisch optimalen Modell setzt eine Lösung zur vorausschauenden Instandhaltung von Weichen auf maschinelles Lernen und IIoT, um defekte Weichen als Verspätungsgrund auszuschalten. [227]

- KONUX Network: Ein detaillierteres Bild des Verkehrs im Streckennetz und dessen Auswirkungen auf die gesamte Infrastruktur wird durch eine Lösung zur Nutzungsüberwachung und Inspektionsplanung vermittelt. [227]
- KONUX Traffic: Die Lösung für die Optimierung der Fahrpläne und die Verringerung der Verspätungen hilft Planern, Disponenten und Fahrdienstleitern dabei, Kapazitätsengpässe zu beheben und ihnen bei der Planung zu helfen. [227]

Railigent X

Die Förderung nachhaltiger Mobilität beinhaltet die digitale Erhöhung der Kapazität von Bahnsystemen – wobei weniger Ressourcen benötigt werden. Die Railigent X Anwendungssuite unterstützt dies. Sie ermöglicht es Bahnbetreibern, Instandhaltern und Asset-Inhabern Daten besser zu interpretieren, Assets zu analysieren und Handlungen zu entwickeln. Auf diese Weise können Betrieb und Wartung verbessert werden, um eine Systemverfügbarkeit von bis zu 100 % zu erreichen. [228]

Railigent X unterstützt bei der Entscheidungsfindung und automatisiert Abläufe für:

- die Betriebsoptimierung,
- die präventive und vorausschauende Instandhaltung und
- das Lebenszyklus-Management der Komponenten („Assets“) und des gesamten Bahnsystems. [228]

7.1.4.5 Systemarchitekturen

Zugbeeinflussungssysteme

In der folgenden Tabelle 60 sind gängige nationale und internationale Zugbeeinflussungssysteme aufgeführt. Eine Auswahl wird im Weiteren kurz beschrieben.

TABELLE 60: ZUGBEEINFLUSSUNGSSYSTEME

Abkürzung	Bezeichnung	Quelle/Referenz
LZB	Linienförmige Zugbeeinflussung	[229]
PZB	Punktförmige Zugbeeinflussung	[229]
ETCS	European Train Control System	[229]
CBTC	Communication-Based Train Control	[216], [217]
PTC	Positive Train Control	[230]
ATACS	Advanced Train Administration and Communications System	[231]
SELCAB	SELCAB	[232]
ZUB 123	ZUB 123	[232]
EBICAB	EBICAB	[232]
BACC	Blocco automatico a correnti codificate	[232]

Abkürzung	Bezeichnung	Quelle/Referenz
KLUB-U/P	Комплексное локомотивное устройство безопасности	[233]
ASFA	Anuncio de Señales y Frenado Automático	[232]

ETCS – European Train Control System

„Das ETCS ist ein System, mit dem die Zugfahrten auf dem Streckennetz kontrolliert und beeinflusst werden können. ETCS überwacht z. B., ob ein Zug einen Gleisabschnitt befahren darf sowie die Geschwindigkeit. „...Technisch handelt es sich bei ETCS um ein rechnergestütztes System, das je nach Funktionsstufe (Level) in unterschiedlicher Weise das Zusammenspiel von Zugfahrt und Fahrterlaubnis kontrolliert." [234] Es wird in vier verschiedene ETCS-Level unterschieden [214]:

- Level 0: Dieses Level unterstützt keine Zugbeeinflussung durch ETCS, es werden nur Balisen gelesen und eine Verbindung zur Streckenzentrale aufgebaut.
- Level 1: Die klassischen Signale werden durch den Zugführer an der Strecke beobachtet. Es findet aber eine punktuelle Datenübertragung statt, von den Streckensignalen hin zum Fahrzeug.
- Level 2: In dieser Ausführungsform werden keine konventionellen Signalanlagen an der Strecke benötigt. Diese werden durch virtuelle Streckensignale, die im Voraus am Führerstand angezeigt werden, ersetzt. Die Datenübertragung findet kontinuierlich in beide Richtungen über Global System for Mobile Communications - Rail (GSM-R) Kommunikation statt. [215]
- Level 3: Dieses ist derzeit noch nicht verfügbar, wird aber mit weiteren Optimierungen entwickelt. Die Ortung des Fahrzeugs erfolgt hier nur noch auf dem Zug selbst und die Abstände zwischen den Fahrzeugen erkennt das System ebenfalls selbst, als so genannte „Moving Blocks". Dadurch können die Züge in kurzen Abständen hintereinanderfahren und die Streckenkapazität wird erhöht. [234]

CBTC – Communication-Based Train Control

Ein Communication-Based Train Control (CBTC)-System ist ein kontinuierliches, automatisches Zugsteuerungssystem, das eine hochauflösende Zugstandortbestimmung nutzt, unabhängig von Gleisstromkreisen. Es findet eine kontinuierliche, bidirektionale Datenkommunikation über Funk (je nach Region) im 2.4, 5.8 bzw. 5.9 GHz-Band vom Zug zur Infrastruktur am Streckenrand statt. Die Streckenüberwachung versorgt dabei das Fahrzeug mit Führungsdaten. Nach der Norm IEEE 1474 können die zug- und streckenseitigen Prozessoren die folgenden Stufen implementieren [216][217]:

- ATP (Automatic Train Protection) Zugbeeinflussung
- ATO (Automatic Train Operation) Vollautomatischer Zugbetrieb
- ATS (Automatic Train Supervision) Zugleitsystem

Anwendungsbeispiele von CBTC sind die U-Bahn New York, Metro Madrid, S-Bahn Kopenhagen und ein Pilotprojekt bei der U-Bahn München.

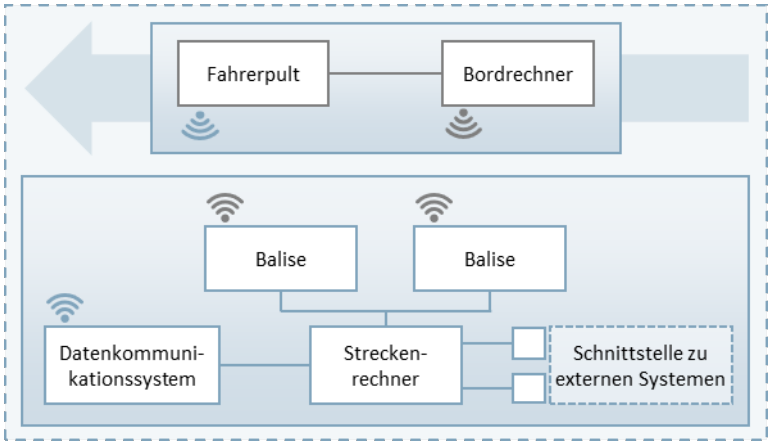


Abbildung 70: CBTC Architektur [Eigene Darstellung nach [216][217]]

Übergeordnete Systemarchitekturen

ETCS und European Rail Traffic Management System (ERTMS), sowie Übersicht aus anderen Ländern.

TABELLE 61: SYSTEMARCHITEKTUREN

Abkürzung	Bezeichnung	Quelle/Referenz
ETCS	European Train Control System	[214][215]
ERTMS	European Rail Traffic Management System	[218]

ERTMS – European Rail Traffic Management System

Das ERTMS ist ein Zugleitsystem und besteht aus dem ETCS (European Train Control System) als Zugbeeinflussungssystem sowie dem GSM-R (Global System for Mobile Communications-Rail) als Kommunikationssystem [218][219]. Nach Beschluss der europäischen Kommission vom 28.09.2021 werden das GSM-R und FRMCS (Future Railway Mobile Communication System) als Railway Mobile Radio (RMR) zusammengefasst. [220] Außerdem umfasst ERTMS u. a. die Regelwerk TSI CCS und OPE (Technical Specifications for Interoperability – Command, Control and Signaling und OPE als Subsystem for Operation and Trafficmanagement). Mit der im Jahr 2022 vorgestellten Version der TSI ZZS (ZZS: Zugsteuerung, Zugsicherung und Signalgebung) ist der automatisierte Fahrbetrieb (ATO – Automatic Train Operation) hinzugekommen. [218] Die TSI ZZS soll genutzt werden, um regelmäßige Verbesserung in Form von Innovationen und Rechtsfortentwicklungen voranzubringen. Derzeit befindet es sich im Ausbau und in der Einführung und soll zukünftig auf den neun europäischen Güterverkehrskorridoren eingeführt werden. [218]

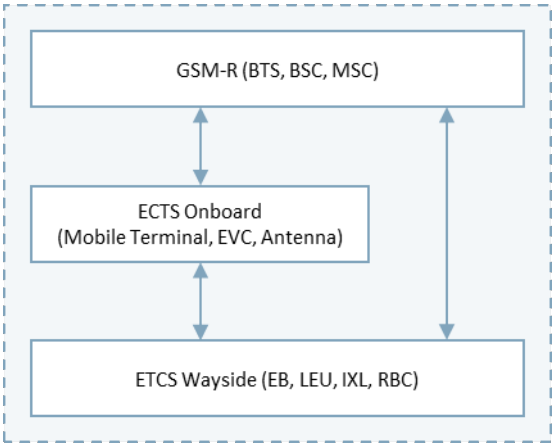


Abbildung 71: ERTMS Architektur [Eigene Darstellung nach [219]]

Wendezugsteuerung und sonstiges

Wendezugsteuerung

Die Fernsteuerung eines Triebfahrzeugs, die Wendezugsteuerung oder in der Schweiz die sogenannte Vielfachsteuerung, sind notwendig, um einen Wendezug (Pendelzug) zu betreiben. In der Regel wird sie im Personenverkehr und in wenigen Fällen auch in Güterzügen eingesetzt. Die Triebfahrzeugführerin oder -führer hat die Möglichkeit, den Zug von dem Triebfahrzeug oder dem Steuerwagen aus zu führen. Dabei kann das „ferngesteuerte“ Triebfahrzeug, das vom Steuerwagen aus stammt, den Zug „schieben“. Bei Fahrtrichtungswechseln ist es daher nicht mehr nötig, das Triebfahrzeug an das andere Zugende zu übertragen. In Wendezugsteuerungen gibt es einen Unterschied zwischen der Datenübertragung in paralleler und in serieller Form. [235]

Integriertes Bordinformationssystem (IBIS) – ÖPNV-Systeme

Das IBIS eines Fahrzeuges setzt sich aus dem Zentralgerät zusammen, welches die verbundenen Peripheriegeräte über einen Wagenbus ansteuert. Alle Daten, die für den Betrieb erforderlich sind, werden im IBIS abgelegt. Daher funktioniert das System selbstständig, auch wenn es keine Funkversorgung gibt. Wenn das Fahrzeug über die entsprechenden Schnittstellen verfügt, unterstützen neue IBIS-Geräte auch das Blindeninformationssystem BLIS und können mit einer Vielzahl weiterer Daten versorgt werden, die an die BLS übermittelt werden. Dazu zählen z. B. die Position des Fahrzeugs, das Ziel der Fahrt, die Besetzung und die momentane Geschwindigkeit. Umgekehrt ist es der BLS möglich, akustische oder visuelle Signale direkt in ein bestimmtes Fahrzeug oder in alle Fahrzeuge auf einer Linie zu übertragen, etwa Fahrplanabweichungen, Betriebsanweisungen und Informationen über technische Störung. [236]

7.1.4.6 Zusammenfassung des Abschnittes

Im Kapitel 7.1.4 wurden sensorbasierte Technologien im Bahnsystem untersucht. Ziel der Recherche war es, den Stand der Technik zur Vernetzung von Systemen und Komponenten sowie zur Datenkommunikation im Bahnsystem zu erhalten. Des Weiteren waren Entwicklungsprojekte mit einer Ausrichtung auf die Weiterentwicklung dieser Technologien Bestandteil der Recherche.

Im Bahnsystem haben sich verschiedene Systemarchitekturen etabliert. Im Wesentlichen sind das:

- Zugbeeinflussungssysteme (z. B. PZB, LZB, ETCS),
- Zug-Kommunikationsnetzwerke (z. B. TCN, WTB, MVB, ETB, ECN),

- Telematiksysteme (z. B. TIS/ITSS),
- Infrastrukturüberwachung (z. B. DIANA, KONUX, Railigent X),
- Wendezugsteuerungssysteme (z. B. ZWS, ZDS, ZMS, FMZ) und
- Systemarchitekturen (TCMS, ETCS, ERTMS).

Das Bahnsystem ist auf Sicherheit und Zuverlässigkeit ausgelegt. Neue Technologien werden daher besonders intensiven Prüfungen unterzogen, bevor diese eingesetzt werden. Zudem müssen viele Systeme unter rauen Einsatzbedingungen über Jahrzehnte zuverlässig und sicher funktionieren. Diese Voraussetzungen führen sicherlich zu einem zögerlicheren Einsatz neuer Technologien, jedoch nicht zu einem Verzicht.

Die Recherche zeigt eine historisch gewachsene, heterogene Welt. Im Bahnsystem ist alles spezifiziert und nach strengen Anforderungen getestet. Was die hohe Sicherheit bei der Bahn gewährleistet, erschwert gleichzeitig neuen Marktteilnehmern eigene Komponenten zu etablieren. Es ist eine Frage der Verfügbarkeit von Energie und Datenleitungen, welche Kommunikationsprotokolle letztendlich eingesetzt werden können. Und es ist eine Frage der Update- und Erneuerungsfähigkeit der eingesetzten Systeme.

Die Ergebnisse der Recherche wurden in Abschnitt 7.2 klassifiziert, analysiert und an beispielhaften Use Cases dargestellt. Interessant für sensorbasierte Anwendungen sind vor allem die Bestrebungen Ethernet-basierte Datennetze in Schienenfahrzeugen zu installieren. Diese öffnen das Bahnsystem für zahlreiche etablierte Informationstechnologien (siehe Abschnitt 7.1.2) und Entwicklungen aus anderen Branchen, wie der industriellen Automatisierung (siehe Abschnitt 7.1.3).

7.1.5 Zusammenfassung und Fazit

Es wurden Informationen aus den folgenden dreizehn Kategorien aufgenommen: Systemarchitekturen, Zugbeeinflussungssysteme, Türsteuerungen, Funksysteme, Netzwerkprotokolle, Feldbusse, Kommunikationsstandards, Auszeichnungssprachen, Modellierungssprachen, Datenformate, Semantik, Ontologien und Hardwarekomponenten. Die Recherchetabelle umfasst 121 Ergebnisse. Für jede Position wurden Informationen zu Recherchegegenstand und Anwendung, Entwicklungsstadium, Einsatzgebiet, wirtschaftliche Aspekte und den genutzten Informationsquellen dokumentiert.

Die Ergebnisse der Recherche wurden in den Abschnitt 7.1 eingearbeitet (siehe Tabelle 48 bis Tabelle 61). Eine vollständige Ergebnisliste befindet sich zudem im Anhang dieses Berichtes zusammen mit einer kurzen Erläuterung der Handhabung.

Fazit

- Vielfältige Protokolllandschaft bestehend aus mehreren Schichten.
- Eine Anwendung erfordert die Nutzung mehrerer Protokolle die kompatibel zueinander sein müssen.
- Proprietäre Protokolle erschweren die Kompatibilität und den Datenaustausch.
- Daher benennen die meisten Anwender die Interoperabilität als Hemmnis bei der Digitalisierung.

Die neuen Möglichkeiten sensorbasierter Systeme werden vielfältig getestet, um einen Eindruck über deren Zuverlässigkeit, Langlebigkeit und die Qualität der damit gewonnenen Daten zu bekommen. Vielfach können durch neue Sensorsysteme und Kommunikationsnetzwerke lange bestehende Probleme gelöst werden. An anderen Stellen ist der zusätzliche Einsatz von Sensorik nicht sofort als wirtschaftlicher Erfolg sichtbar.

Es findet eine Entwicklung statt, bei der Sensoren mit immer mehr Funktionen und einer verbesserten Datenverarbeitung ausgestattet werden. Sensoren liefern nicht nur Daten, sondern können aus den Daten bereits Informationen extrahieren. Die Menge der übertragenen Daten kann dadurch reduziert werden. Durch leistungsfähigere Datenverarbeitung und Rechentechnik können Subsysteme immer mehr Aufgaben übernehmen und unabhängig vom übergeordneten Steuerungssystem agieren. Es findet eine Neuverteilung der Datenverarbeitung zwischen Cloud und Edge statt. Subsystem können durch eine verbesserte Datenverarbeitung zudem intelligenter agieren. Viele Aufgaben, die bisher zwangsläufig ein Mensch ausführen musste, können auf Maschinen übertragen werden.

Die Abkehr von hochspezialisierten Feldbussen zu Kommunikationsnetzwerken erfordert die Ergänzung der Kommunikationsnetze um spezielle Funktionen der Echtzeitfähigkeit und der Sicherheit der Kommunikation. In Reglungsprozessen dürfen keine Datenpakete verspätet übertragen werden oder verloren gehen. Es muss gewährleistet sein, dass die Daten unverfälscht beim Empfänger ankommen und ebenfalls nicht abgehört werden.

Es entstehen neue Herausforderungen bzgl. der Nachvollziehbarkeit der eingesetzten Algorithmen und der Datensicherheit.

7.2 Analyse, Klassifizierung und Eignung

7.2.1 Vorgehensweise und Methodik

Aus den Ergebnissen der Bestandsaufnahme wurden anhand des Leitbildes 17 Technologien für die weitere Analyse und Klassifizierung ausgewählt. Diese wurden in die fünf Kategorien Personenverkehr, Güterverkehr, Betriebstechnologie, Informationstechnologie und Konvergenz von Betriebs- und Informationstechnologie eingeteilt. Es wurden die Prozessschritte der Datenverarbeitung benannt und deren Abdeckung für die Auswahl aufgezeigt. Die Vorgehensweise in Kapitel 7.2 folgt in Abbildung 72.

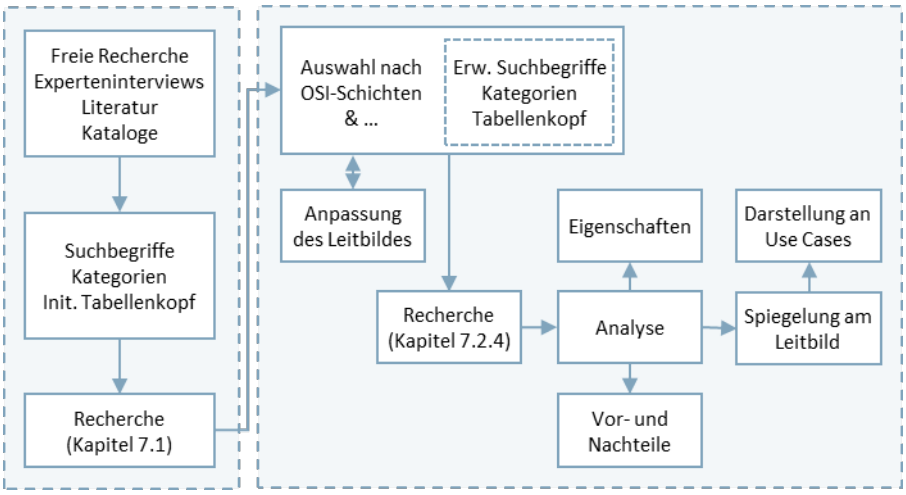


Abbildung 72: Vorgehensweise im Kapitel 7.2 Analyse, Klassifizierung und Eignung

Die Eigenschaften, sowie Vor- und Nachteile wurden benannt und daraus Anforderungen an Systemarchitekturen, Datenschnittstellen und Gestaltungsprinzipien abgeleitet. Es wurden die Veränderungen und Auswirkungen durch die Digitalisierung und das IoT auf existierende Architekturen diskutiert. Dabei wurde besonders auf die Schlüsselfaktoren von kombinierten OT (Operational Technology) und IT (Information Technology) Architekturen eingegangen.

7.2.2 Leitbild für Sensoriksysteme und Komponenten

Im Projekt wurde ein Leitbild für Sensoriksysteme und Komponenten zur Bewertung der Ergebnisse eingesetzt. Das Leitbild wurde vom DZSF initiiert und während der Projektlaufzeit entsprechend des Erkenntnisgewinnes aktualisiert und angepasst.

Die Inhalte des Leitbildes bezogen auf Sensoriksysteme und Komponenten werden in der folgenden Aufzählung kurz zusammengefasst.

- Voraussetzung für die Digitalisierung und Automatisierung ist die Ausstattung von Schienenverkehrssystemen mit Datennetzen.
- Wichtiger Anwendungszweck ist die Einbindung von Sensoren, sowie die Datenerfassung und Datenverarbeitung.
- Anforderungen an Sensoriksysteme im Schienenverkehr:
    - Flexibilität als Antwort auf Heterogenität und Variabilität
        - Plug & Play, sowie Herstellerunabhängigkeit durch einheitliche und offene Schnittstellen
        - Dokumentiert und „weitgehend“ schutzrechtsfrei
    - Service-orientierte, modellbasierte Architektur
        - Abwärts- und Aufwärtskompatibilität
    - Sicherheit
        - Verankerung von Sicherheitsmechanismen in der Systemarchitektur
        - Zugriffskontrolle, Rollenmodelle und Authentifizierung
        - Selektive Bereitstellung und Trennung von Informationen, z. B. konzeptuelle Trennung (Sensor, Sensorsignal, Datenverarbeitung, Messdaten)
    - Robust und verfügbar
        - Priorisierung und Verschlüsselung
        - Redundanzen und Unterscheidung von einfachen und sicherheitsrelevanten Systemen

7.2.3 Klassifizierung und Auswahl

Die Klassifizierung wurde zu verschiedenen Zeitpunkten im Projekt durchgeführt. Die Klassen sind in der Tabelle „Analysetabelle Teil 1 bis 3“ im Anhang C aufgeführt. Die Vorgehensweise zeigt Abbildung 72.

7.2.4 Analyse ausgewählter Technologien

Im Kapitel 7.1.2 wurden sensorbasierte Technologien recherchiert und beschrieben. Die dazugehörigen Kommunikations- und Datennetze bestehen aus Hardware- und Softwarekomponenten. Die Hardware sorgt für die physikalische Verbindung der Komponenten über Schnittstellen, Kabel oder Funkverbindungen. Über dieser physikalischen Ebene existieren weitere Ebenen die über Softwareprotokolle den Verbindungsaufbau und Datenaustausch regulieren und überwachen. Ein weitverbreitetes Modell ist das OSI-Modell, welches im Abschnitt 7.1.2.6 Netzwerke und Sensornetzwerke beschrieben wurde. Anhand dieses Modells lassen sich die Hardware- und Softwarekomponenten im IoT einordnen. Die folgende Grafik gibt einen Überblick über gängige Komponenten der IoT-Protokolllandschaft. Ein Kommunikationsstandard kann durch Kombination von kompatiblen Komponenten bedarfsgerecht zusammengesetzt werden. Wichtig ist nur, dass Sender und Empfänger die gleiche IoT-Sprache sprechen.

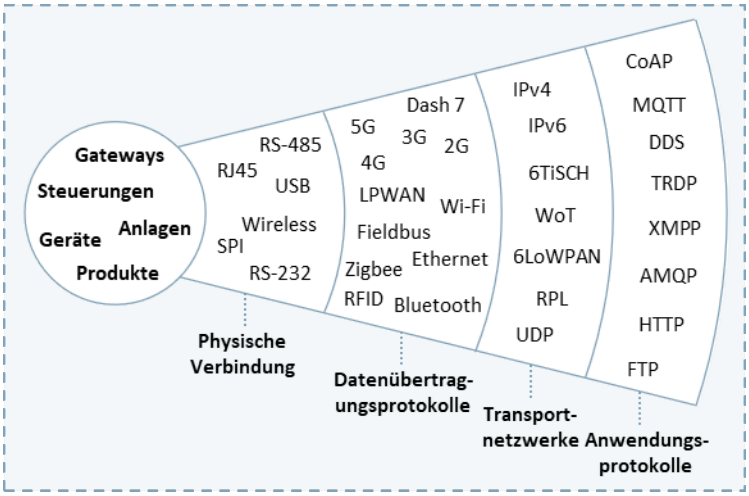


Abbildung 73: Die IoT Protokolllandschaft [Eigene Darstellung nach [237]]

Aus dieser vielfältigen Protokolllandschaft wurden 17 Komponenten für die weitere, detaillierte Analyse und Klassifizierung ausgewählt. Die Auswahl fand zum einen nach Vorgabe der Leistungsbeschreibung statt. Darin bestand die Forderung nur Komponenten ab einem OSI-Level von 5 und höher (in Ausnahmefällen auch 4 und höher) zu betrachten.

7.2.4.1 Personenverkehr

TCN – Train Communication Network

Das TCN vereint eine Reihe eisenbahnspezifischer Bussysteme und Netzwerke sowie Kommunikations- und Anwendungsprofile. Das TCN wird derzeit als IEC-Standard entwickelt und ist als europäische Normenreihe in verschiedenen nationalen Normen verfügbar, z. B. DIN EN 61375. Der TCN-Standard wird mit Unterstützung mehrerer Forschungsprojekte weiterentwickelt.

Allgemeine Datenklassen von Netzwerken: Aus einer anderen Perspektive können Daten und Datenströme über Bussysteme und Switch-Netzwerke übertragen werden. Zur Unterscheidung und Klassifizierung der Datenübertragung werden fünf Hauptdatenklassen nach IEC 61375-1 verwendet: Prozessdaten (PD), Nachrichtendaten (MD), Überwachungsdaten, Stromdaten und Best-Effort-Daten.

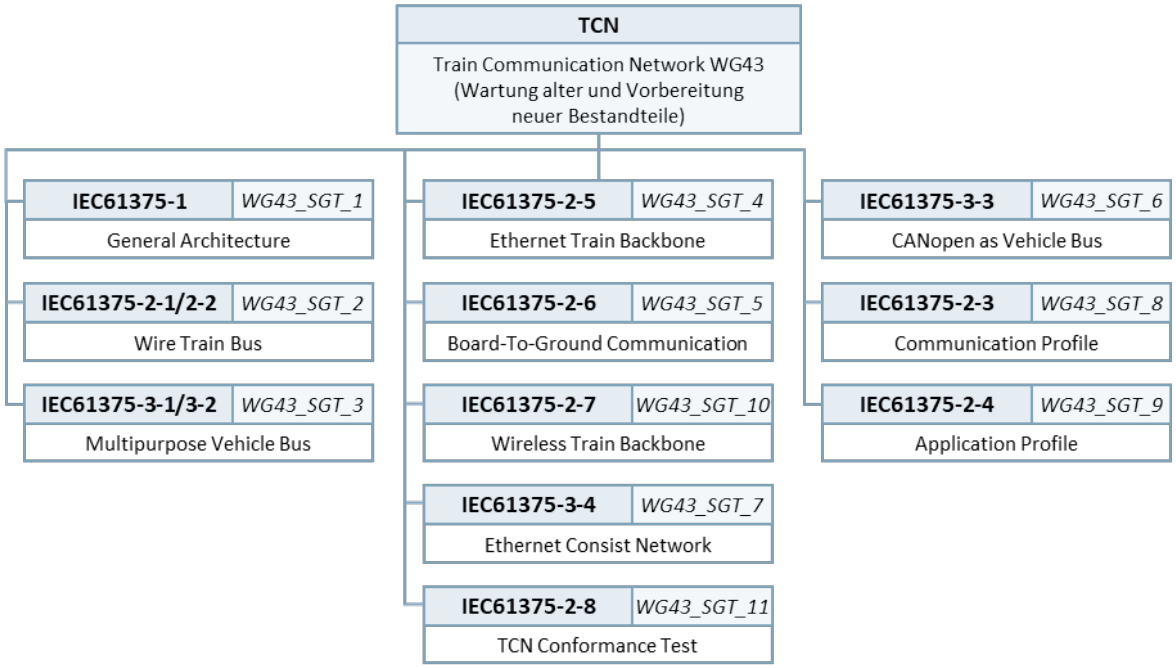


Abbildung 74: Evolution der TCN-Standard Serie [Eigene Darstellung nach [238]]

Insbesondere für Bahnen müssen verschiedene Anforderungen berücksichtigt werden, wie z. B. Umgebungsbedingungen und Robustheitsanforderungen, aber auch eine hochverfügbare, sichere und echtzeitfähige Kommunikation bahnspezifischer Daten. [214]

Vorteile

Eine Besonderheit des TCN ist die Fähigkeit, die Topologie des Backbones selbst zu bestimmen. [214]

Dieser im Train Communication Network vorkommende Standard ermöglicht eine weltweite Interoperabilität von Schienenfahrzeugen. Das Train Communication Network sorgt auch dafür, dass die Ausrüstung ausgetauscht werden kann, was wiederum die Kosteneffizienz der Technologie verdeutlicht. Die Besonderheit des Zugbusses, der zu den beiden Feldbussen gehört, besteht darin, dass er in der Lage ist, eine Konfiguration bei jeder Änderung der Zugzusammenstellung vorzunehmen, um die Position eines Fahrzeugs und dessen Eigenschaften automatisch zu erkennen und weiterzugeben. [239]

Nachteile

Es lässt sich feststellen, dass TCN und die übrigen Feldbusse an ihre Bandbreitengrenze stoßen. Die Forderung nach leistungsfähigen standardisierten Transportprotokollen wie TCP/IP oder UDP/IP kommt aufgrund von Preis- und Bandbreitenproblemen zustande. [240]

Die Hauptschwächen der heutigen Netzwerkarchitektur sind in Tabelle 7 von CONNECTA „D3.2 – Drive-by-Data Technology Evaluation Report“ aufgeführt [241].

Eine Vielzahl von Kommunikationsprotokollen und Datenbussen, darunter PROFIBUS, CAN, MVB, PROFINET, Ethernet/IP, CIP und IEC 61375, bilden die Grundlage von Bahnnetzen. Dadurch entstehen Schwierigkeiten hinsichtlich Interoperabilität, Komplexität und Verwaltbarkeit. Zudem steigen die Ausgaben für Design, Integration, Wiederverwendung, Zertifizierung (Homologation) und Instandhaltung. Die ETB- bzw. Ethernet Consist Network (ECN)-Netze, wie sie in IEC 61375 beschrieben sind, verwenden Ethernet mit Virtual Local Area Network (VLAN) (IEEE 802.1Q). Sie unterstützen nur eingeschränkt

die Gestaltung von deterministischen und skalierbaren Systemarchitekturen für Anwendungen wie TCMS der nächsten Generation oder SIL2. [242]

NG-TCN – Next Generation Train Communication Network

Die Weiterentwicklung des TCN zum Next Generation TCN zeigt Abbildung 66 in Kapitel 7.1.4.2. Diese befindet sich derzeit in der Forschung und Entwicklung.

Die Forschung des TCMS der neuen Generation (NG TCMS) begann mit dem EU-Joint Undertaking Shift2Rail-Leuchtturmprojekt Roll2Rail und wird in den Projekten CONNECTA und Safe4RAIL fortgeführt.

Das NG TCMS verbindet alle Bordgeräte (TCMS, Signalisierung, betreiber- und kundenorientierte Dienste) und kann mit anderen Zügen und Bodennetzen verbunden werden.

Erschwinglichkeit, Komplexität, modulare Zertifizierung, häufige dynamische Neukonfiguration und die Möglichkeit, verteilte sicherheitskritische Funktionen zu hosten, sind die größten Herausforderungen im TCMS der nächsten Generation. [242]

Besondere Vorteile

Die nächste Generation von TCMS-Architekturen bietet die Möglichkeit, alle Hard-RT-, Echtzeit- und Soft-Time-Funktionen zu integrieren und unterstützt unterschiedliche Berechnungs- und Kommunikationsmodelle für verschiedene Anwendungsanforderungen. [242]

Spezieller Nachteil

NG-TCN befindet sich derzeit in Entwicklung.

Die Vorteile und Nachteile aus der Analyse sind in Tabelle 62 und Tabelle 69 gegenübergestellt.

TABELLE 62: ANALYSEERGEBNISSE VON TRDP UND RMR

Begriff	TRDP	RMR
Recherchegegenstand und Anwendung		
Name	Train Real Time Data Protocol	Railway Mobile Radio (GSM-R + FRMCS)
Kategorie	Netzwerkprotokoll	Zugkommunikationsnetz
Anwendungsfeld	Datentransportprotokoll	Datenübertragung
Plattformunabhängigkeit	ja	eigene Plattform
OSI-Modell		
OSI-Schicht	5	ab 5
Untere OSI-Schicht vorgegeben	ja, UDP/TCP	
Prozessschritte der Datenverarbeitung	B	B

Begriff	TRDP	RMR
Entwicklungsstadium		
im Einsatz	ja (2015)	ja (GSM-R)
in Entwicklung	nein	ja
Sensoranbindung		
Einsatzgebiete	In Zügen, Übertragung Prozessdaten	Schienenfahrzeug, Zugfunk
Plug and Play	nein	(nein)
Offene Schnittstellen	Publisher-Subscriber-Modell	(nein)
Daten		
Erweiterbarkeit	-	ja
Security-Mechanismen	eigene Safety-Layer-Implementation	
Robustheit	CRC-Prüfsumme	
Verfügbarkeit	-	
selbstbeschreibende Daten	nein	
Datenpriorisierung	nein	
Verschlüsselung	nein	RMR

7.2.4.2 Güterverkehr

Im Eisenbahngüterverkehr gab es in den letzten Jahrzehnten keine einheitlichen Normen für Telematik-Systeme und Sensorik. Das Resultat waren eine Vielzahl von Einzellösungen, die die weitere Verbreitung von Telematik- und Sensoriksystemen auf dem Markt behinderten. Mit der Standardisierung von Schnittstellen strebt die Technischer Innovationskreis Schienengüterverkehr (TIS) als Practice Group des Sektors danach, die Integrationsfähigkeit der Telematik-Systeme und Sensorik verschiedener Anbieter zu verbessern. Um die Innovationskraft des Schienengüterverkehrs zu stärken und die Wachstumschancen zu erhöhen, soll dies eine größere Investitionssicherheit und günstige Rahmenbedingungen für einen flächendeckenden Einsatz von Telematik und Sensorik auf der Betreiberseite schaffen. [243]

Die Vorteile und Nachteile aus der Analyse sind in Tabelle 63 und Tabelle 69 gegenübergestellt.

TABELLE 63: ANALYSEERGEBNISSE VON TIS/ITSS

Begriff	TIS/ITSS
Recherchegegenstand und Anwendung	
Name	Industrieplattform für Telematik und Sensorik im Schienengüterverkehr
Kategorie	Systemarchitektur
Anwendungsfeld	Schienengüterverkehr
Plattformunabhängigkeit	eigene Plattform

Begriff	TIS/ITSS
OSI-Modell	
OSI-Schicht	
Untere OSI-Schicht vorgegeben	
Prozessschritte der Datenverarbeitung	B, C
Entwicklungsstadium	
im Einsatz	
in Entwicklung	Ja
Sensoranbindung	
Einsatzgebiete	Güterwagen
Plug and Play	-
Offene Schnittstellen	ja, offene Standards
Daten	
Erweiterbarkeit	ja
Security-Mechanismen	
Robustheit	-
Verfügbarkeit	-
selbstbeschreibende Daten	nein
Datenpriorisierung	nein
Verschlüsselung	nein

7.2.4.3 Betriebstechnologie

Das Konzept der Automatisierungspyramide stellt die Hierarchie der Leit- und Automatisierungsebene in einer deutlich strukturierten Pyramide dar. [254]

Der Übergang von der Maschine oder Anlage zum ERP wird durch die Automatisierungspyramide beschrieben. Die Datenreise vom Ort des Geschehens, also der Fertigung, zum Waren- und Wirtschaftssystem, wo die Planung stattfindet, ist gemeint. Auf diese Weise ist es möglich, die geplante Leistung zu jeder Zeit mit der tatsächlich erbrachten Leistung zu vergleichen. Es ist ein bedeutender Schritt in Richtung einer transparenten Fabrik. Darüber hinaus ist es möglich, der Maschine Produkte, Aufträge, Programme und gegebenenfalls auch Material zuzuordnen und zu senden. Die Vorzüge, die durch den Weg, der in der Pyramide beschrieben wird, erzielt werden können, sind nach wie vor unbestritten und relevant. [186]

Die Vorteile und Nachteile aus der Analyse sind in Tabelle 64 und Tabelle 69 gegenübergestellt.

TABELLE 64: ANALYSEERGEBNISSE VON IO-LINK, CIP UND LON(WORKS)

Begriff	IO-Link	CIP	Lon(Works)
Recherchegegenstand und Anwendung			
Name	Single-drop digital communication interface for small sensors and actuators	Common Industrial Protocol	Local Operating Network
Kategorie	automatisiertes Kommunikationssystem	Kommunikationsprotokoll	Feldbus
Anwendungsfeld	Datenübertragung (Punkt-zu-Punkt)	Datentransportprotokoll	Gebäudeautomatisierung
Plattformunabhängigkeit	ja	ja	ja
OSI-Modell			
OSI-Schicht	1 bis 5	5 bis 7	1 bis 7
Untere OSI-Schicht vorgegeben	ja (3-Leiter, Funk)		ja (Kupferkabel, Glasfaser, Funk)
Prozessschritte der Datenverarbeitung	B	B	B
Entwicklungsstadium			
im Einsatz	ja	ja	ja (~1990)
in Entwicklung	wird weiter entwickelt	nein	wird weiter entwickelt
Sensoranbindung			
Einsatzgebiete	Sensoren, Aktoren, Industrieanlagen, Gebäude	Industrieautomation	dezentrale Automatisierung (Gebäude-, Indutrie- und Prozessautomatisierung)
Plug and Play	teilweise (Austausch von defekten Sensoren 1 zu 1 Plug and Play möglich)	-	teilweise (bei vorkonfigurierten Knoten)
Offene Schnittstellen	Master-Slave-Prinzip	Peer-to-Peer	ja, Bussystem (Domain, Subnet und Knoten)
Daten			
Erweiterbarkeit	ja	-	ja bis 127 Knoten pro Subnetz
Security-Mechanismen	eigene Safety-Layer-Implementation	CLIP-Safety Protokoll	eindeutige IDs, Authentifizierung des Senders
Robustheit	CRC Signatur über Prozessdaten und Sicherungscode	CRC-Prüfsumme	CRC-Prüfsumme, Acknowledged verschiedene Bustopologien

Begriff	IO-Link	CIP	Lon(Works)
Verfügbarkeit	ja (Diagnose) Geräte-zustand Betriebszustand	-	garantierte Reaktionszeit
selbstbeschreibende Daten	nein	nein	nein
Datenprioriserung	nein	ja in Verbindung mit CAN	ja Priority Slots
Verschlüsselung	nein	nein	ja (Mancherster-Code)

7.2.4.4 Informationstechnologie und IoT

Die folgenden neun Technologien aus der Analysetabelle konnten dem Bereich der Informationstechnologie und IoT zugeordnet werden: XML, JSON, SSN, USB, User Datagram Protocol (UDP), TCP/IP, UML, SysML und SensorML. Aufgrund der Vielzahl wurden sie für eine übersichtlichere Darstellung auf drei Tabellen aufgeteilt.

Die Vorteile und Nachteile aus der Analyse sind in Tabelle 65 und Tabelle 69 gegenübergestellt.

TABELLE 65: ANALYSEERGEBNISSE VON XML, JSON UND SSN

Begriff	XML	JSON	SSN
Recherchegegenstand und Anwendung			
Name	Extensible Markup Language	JavaScript Object Notation	Semantic Sensor Network Ontology
Kategorie	Auszeichnungssprache	Datenformat	Modellierungssprache
Anwendungsfeld	Definition und Austasch von Datenstrukturen	Definition und Austasch von Datenstrukturen	Sensormodellsprache
Plattformunabhängigkeit	ja	ja	ja
OSI-Modell			
OSI-Schicht	5 bis 7	5 bis 7	ab 5
Untere OSI-Schicht vorgegeben			
Prozessschritte der Datenverarbeitung	B, C	B, C	C
Entwicklungsstadium			
im Einsatz	ja (1998)	ja (1997)	ja (2017)
in Entwicklung	nein (letzte Aktualsierung 2008)	nein (letzte Aktualisierung 2017)	
Sensoranbindung			
Einsatzgebiete	Datenaustausch, Webservices	Datenübertragung	Sensoren
Plug and Play	-	-	-

Begriff	XML	JSON	SSN
Offene Schnittstellen	-	-	-
Daten			
Erweiterbarkeit	ja	ja	ja
Security-Mechanismen	nein	nein	nein
Robustheit	-	-	-
Verfügbarkeit	-	-	-
selbstbeschreibende Daten	ja	ja	ja
Datenprioriserung	-	-	-
Verschlüsselung	nein	nein	nein

Semantic Sensor Network Ontology

Die Semantic Sensor Network (SSN) Ontologie beschreibt Sensoren und ihre Messdaten, Verfahren, untersuchte Merkmale, Proben, die dafür verwendet werden und Eigenschaften. Außerdem können auch Aktoren beschrieben werden. SSN verwendet für seine grundlegenden Klassen und Merkmale eine einfache, aber eigenständige Kernontologie namens SOSA (Sensor, Observation, Sample und Actuator), die in seine horizontale und vertikale Modularisierungsarchitektur integriert ist. Satellitenbilder, groß angelegte wissenschaftliche Überwachung, Industrie- und Haushaltsinfrastrukturen, soziale Sensorik, Bürgerwissenschaft und beobachtungsgesteuerte Ontologien sowie das IoT sind Beispiele für ihre unterschiedlichen Anwendungs- und Anwendungsfälle. [253]

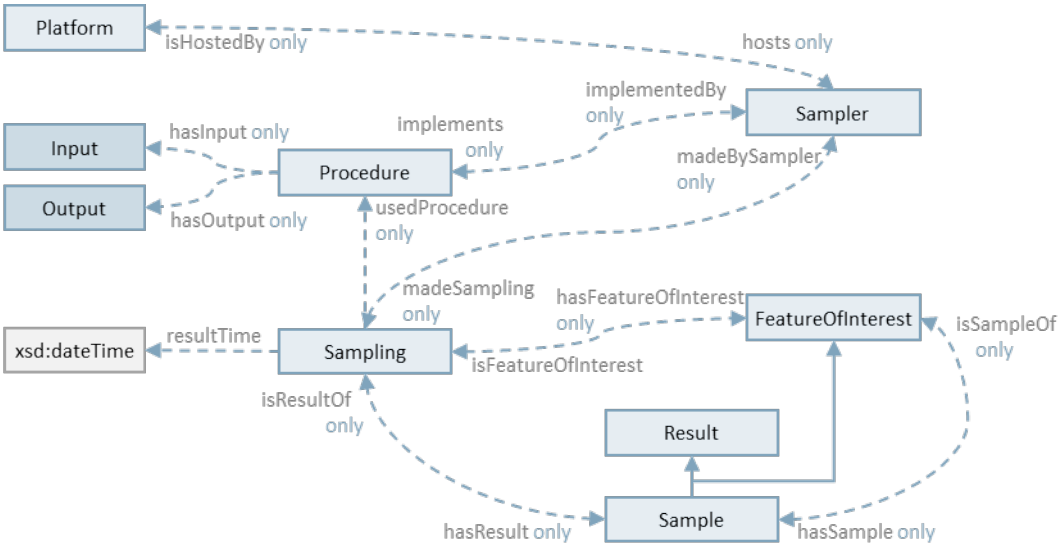


Abbildung 75: An der Datenaufnahme beteiligte Klassen und Beziehungen (SOSA/SSN) [Eigene Darstellung nach [253]]

Die Vorteile und Nachteile aus der Analyse sind in Tabelle 66 und Tabelle 69 gegen-übergestellt.

TABELLE 66: ANALYSEERGEBNISSE VON USB, UDP UND TCP/IP

Begriff	USB	UDP	TCP/IP
Recherchegegenstand und Anwendung			
Name	Universal Serial Bus	User Datagram Protocol	Transmission Control Protocol/Internet Proto-col
Kategorie	Datenübertragungs-system	Netzwerkprotokoll	Gruppe von Netzwerk-protokollen
Anwendungsfeld	Datenübertragung	Datentransportprotokoll	Datentransportprotokoll
Plattformunabhäng-igkeit	ja	ja	ja
OSI-Modell			
OSI-Schicht	1 bis 7	4	4 / 3
Untere OSI-Schicht vorgegeben	ja		
Prozessschritte der Datenverarbeitung	B	B	B
Entwicklungsstadium			
im Einsatz	ja (1996)	ja	ja
in Entwicklung	wird weiter entwickelt	nein	nein
Sensoranbindung			
Einsatzgebiete	Datenübertragung, Datenschnittstelle, Span-nungsquelle	Datenübertragung bei vielen Clients	Datenübertragung
Plug and Play	ja, teilweise	-	-
Offene Schnittstellen	ja, Host-Device-Prinzip	-	ja
Daten			
Erweiterbarkeit	ja	-	-
Security-Mechanismen	nein	nein	nein
Robustheit	CRC-Prüfsumme, Acknowledged, Bitüber-tragung	CRC-Prüfsumme	CRC-Prüfsumme (TCP)
Verfügbarkeit	garantierte Übertra-gungsraten	-	-
selbstbeschreibende Daten	teilweise (durch Treiber)	nein	nein
Datenprioriserung	nein	nein	nein
Verschlüsselung	nein	nein	nein

Die Vorteile und Nachteile aus der Analyse sind in Tabelle 67 und Tabelle 69 gegenübergestellt.

TABELLE 67: ANALYSEERGEBNISSE VON UML, SYSML UND SENSORML

Begriff	UML	SysML	SensorML
Recherchegegenstand und Anwendung			
Name	Unified Modeling Language	Systems Modeling Language	Sensor Model Language
Kategorie	Modellierungssprache	Modellierungssprache	Modellierungssprache
Anwendungsfeld	Softwaremodellierung	Systemmodellierung	Sensormodellsprache
Plattformunabhängigkeit	ja	ja	ja
OSI-Modell			
OSI-Schicht	5 bis 7	5 bis 7	5 bis 7
Untere OSI-Schicht vorgegeben			
Prozessschritte der Datenverarbeitung	C	C	C
Entwicklungsstadium			
im Einsatz	ja (1996)	ja (2007)	ja (2009)
in Entwicklung	nein (letzte Aktualisierung 2017)	wird weiter entwickelt	wird weiter entwickelt
Sensoranbindung			
Einsatzgebiete	Softwarespezifikation	Systementwurf	Beschreibung von Sensoren und Messprozessen
Plug and Play	-	-	-
Offene Schnittstellen	-	-	-
Daten			
Erweiterbarkeit	ja	ja	ja
Security-Mechanismen	nein	nein	nein
Robustheit	-	-	-
Verfügbarkeit	-	-	-
selbstbeschreibende Daten	ja		ja
Datenprioriserung	-	-	-
Verschlüsselung	nein	nein	nein

SensorML

SensorML ist ein vom Open Geospatial Consortium anerkannter Standard und eine XML-Kodierung, mit der Sensoren und Messprozesse beschrieben werden können. SensorML ermöglicht die Beschreibung einer Vielzahl von Sensoren, einschließlich stationärer und dynamischer Plattformen sowie In-situ- und

Remote-Sensoren. Es stellt Standardmodelle sowie eine XML-Kodierung zur Verfügung, die es verwenden kann, um sämtliche Abläufe zu beschreiben. Dazu gehören der Prozess der Sensormessung sowie Anweisungen, um Informationen auf höherer Ebene aus Beobachtungen abzuleiten. Die Informationen in einem Sensornetz werden durch Beobachtungen und Messungen, die eine benutzerzentrierte Ansicht bieten, anbieterzentriert dargestellt. Sensorerkennung, Sensorlokalisierung, Sensordatenverarbeitung, Sensorprogrammierungsmechanismus und Abonnement für Sensorwarnungen sind einige der unterstützten Funktionen. [251][252]

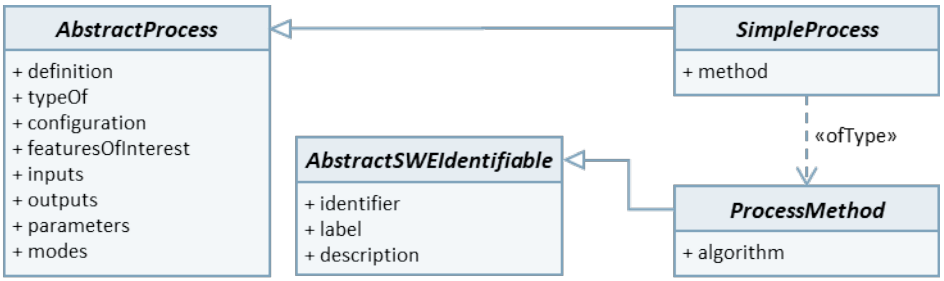


Abbildung 76: SensorML Anwendungsbeispiel [Eigene Darstellung nach [251]]

Die Sensor Model Language (SensorML) konzentriert sich hauptsächlich darauf, Prozesse und Verarbeitungskomponenten zu definieren, die mit der Messung und der Umwandlung von Messdaten in Verbindung stehen und robust und semantisch sind. [252]

7.2.4.5 Konvergenz von Betriebs- und Informationstechnologie

Ursprünglich bezieht sich der Begriff „IT“ oder „Informationstechnologie“ auf den Gebrauch von Computern zur Verarbeitung und Verwaltung von Daten. Normalerweise bezieht sich der Ausdruck OT oder Betriebstechnologie (engl. Operational Technology) auf die Hardware und die Maschinen, die für die physischen Abläufe eines Unternehmens zuständig sind. Im Kontext der Digitalisierung und von Konzepten wie Industrie 4.0 verschwimmt die Grenze zwischen IT und OT jedoch immer stärker. Das Konzept der OT/IT-Konvergenz ermöglicht den Unternehmen im Zuge der technologischen Entwicklung eine hohe Flexibilität und Leistungsfähigkeit. Dieses Konzept umfasst die Verknüpfung von Informationstechnologie- und Betriebstechnologiesystemen. [256]

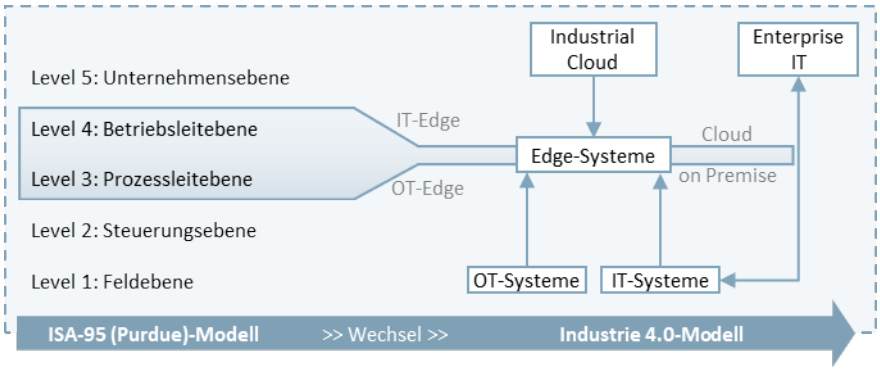


Abbildung 77: OT-IT-Konvergenz: Zwei Welten zusammenbringen [Eigene Darstellung nach [257]]

Die Vorteile und Nachteile aus der Analyse sind in Tabelle 68 und Tabelle 69 gegen-übergestellt.

TABELLE 68: ANALYSEERGEBNISSE VON OPC UA UND MQTT

Begriff	OPC UA	MQTT
Recherchegegenstand und Anwendung		
Name	Open Platform Communications Unified Architecture	Message Queuing Telemetry Transport
Kategorie	Datenmodell	(Nachrichten)Protokoll
Anwendungsfeld	Datenübertragung	IoT
Plattformunabhängigkeit	ja	ja
OSI-Modell		
OSI-Schicht	5	7
Untere OSI-Schicht vorgegeben		
Prozessschritte der Datenverarbeitung	B, C	B
Entwicklungsstadium		
im Einsatz	ja (seit 2008, seit 2015 öffentlich)	ja
in Entwicklung	wird weiter entwickelt	wird weiter entwickelt
Sensoranbindung		
Einsatzgebiete	Maschienendaten, Industrie, Auto-motiv	Machine-to-Machine
Plug and Play	ja	nein
Offene Schnittstellen	Client-Server Modell oder Pub-lisher-Subscriber-Modell	Publisher-Subscriber-Modell
Daten		
Erweiterbarkeit	ja skallierbar	ja
Security-Mechanismen	eigene Security-Implementation	ja sind möglich
Robustheit	Redundanz	ja, Quality of Service
Verfügbarkeit	Heartbeat Pufferung	
selbstbeschreibende Daten	semantische Beschreibung	n. a.
Datenprioriserung	nur mit integriertem TSN (Time Sensitive Networking-Technologie)	n. a.
Verschlüsselung	ja 128 oder 256 Bit signieren Au-thentifizierung mittels Zertifikats	ja, kann eingerichtet werden z. B. TLS

OPC UA

OPC Unified Architecture (OPC UA) ist ein plattformunabhängiger, serviceorientierter Datenaustausch-standard. Dies ermöglicht es, Daten von Maschinen (z. B. Regelgrößen, Messwerte, Parameter usw.) nicht nur zu übertragen, sondern auch semantisch für Maschinen zu beschreiben. [180][181]

OPC zählt zu den bedeutendsten Kommunikationsnormen für das IoT und die Industrie 4.0. OPC standardisiert den Zugang zu Maschinen, Geräten und anderen Systemen im industriellen Bereich und erlaubt einen gleichartigen und herstellerunabhängigen Datenaustausch. Der Unterschied zum Vorgänger besteht in der Plattformunabhängigkeit durch Abkehr von COM/DCOM und Verwendung von TCP/IP oder alternativ SOAP-Kommunikation. OPC UA bietet außerdem neben zahlreichen weiteren Verbesserungen auch die Möglichkeit, Daten semantisch zu beschreiben. [248][180][181]

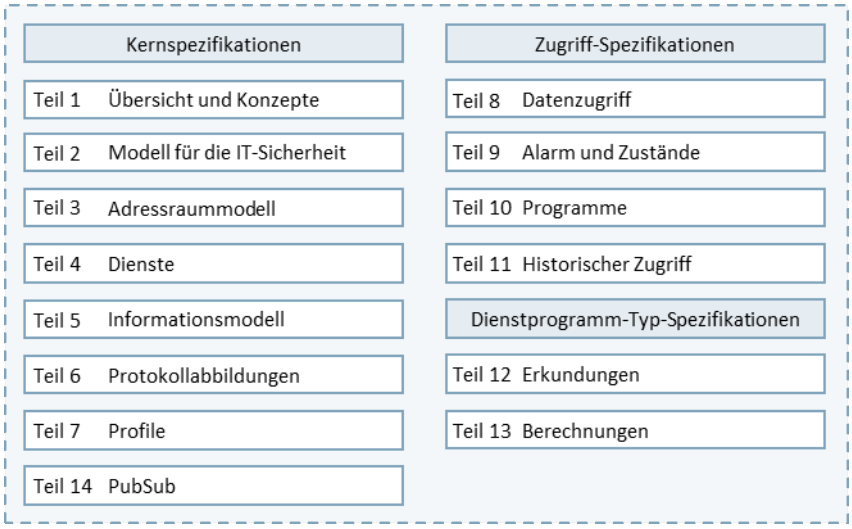


Abbildung 78: OPC UA Spezifikationen [Eigene Darstellung nach [239]]

Der OPC UA-Standard umfasst verschiedene Spezifikationen. Jede Spezifikation definiert eine Teilfunktion und legt fest, welche Server- und Clientschnittstellen für die Unterstützung dieser Funktion implementiert werden müssen. Nicht alle OPC-Server und Clients brauchen die Unterstützung aller Spezifikationen. Es werden häufig nur bestimmte Spezifikationen programmiert, abhängig vom Anwendungsbereich. Daher müssen bei der Verwendung eines OPC-Servers und auch eines Clients die Spezifikationen berücksichtigt werden, die vom Server und vom Client implementiert werden. [248]

Die Companion Specifications sind von Industrieunternehmen entwickelte Informationsmodelle, die auf dem Standardmodell des OPC UA basieren. Es werden Datenpunktstrukturen definiert, die für spezifische Anwendungen und Objekte in der Branche bestimmt sind. Dazu gehören Spritzgussmaschinen (Euromap 77), Werkzeugmaschinen/CNC (umati), Roboter, RFID und AutoID-Systeme (AutoID) sowie zahlreiche andere Modelle. [248]

OPC UA FX (OPC UA over TSN)

OPC UA über Time Sensitive Network (TSN) wurde für die Kommunikation in Echtzeit auf Feldebene zwischen Steuerungssystemen entwickelt. Es umreißt die Bedürfnisse von deterministischen Reaktionszeiten in Maschinennetzwerken. Bei OPC UA über TSN wird im Unterschied zum Client-Server-Betrieb von OPC UA das Publisher-Subscriber-Verfahren angewendet. OPC UA über TSN ist derzeit nicht relevant für die Verwendung von OPC UA in herkömmlichen Ethernet-basierten, Nicht-Echtzeit-Umgebungen. [248]

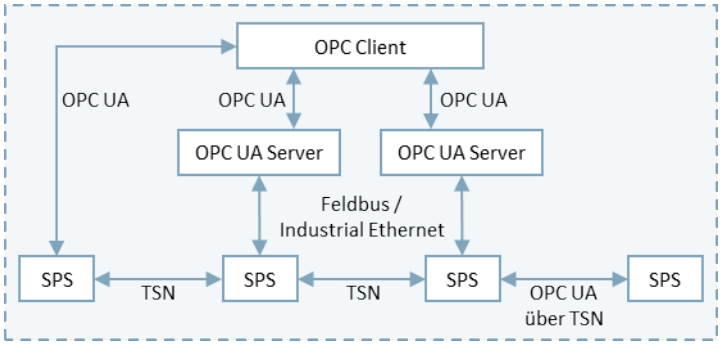


Abbildung 79: OPC UA over TSN [Eigene Darstellung nach [248]]

Perspektiven (OPC vs. OPC UA)

In [249] wird aufgeführt, dass der OPC-DA-Standard, obwohl er noch weit verbreitet ist, den aktuellen Automatisierungsanforderungen nicht mehr gerecht wird. Er nutzt veraltete Technologien, ist schwierig anzupassen und erfüllt nicht die aktuellen Sicherheitsstandards. Der aktuelle OPC UA-Standard ersetzte ihn mit der Möglichkeit, Daten zu verschlüsseln und einheitliche Sensordatenübertragungssysteme in die Cloud zu integrieren. Die Technologie zur Echtzeit-Datenübertragung wird durch die Kombination von OPC UA und TSN deutlich ausgebaut. Bestehende Systeme können nach und nach aktualisiert und mithilfe von Wrappern und Proxy-Modulen auf OPC UA angepasst werden. [249]

Anwendungsgebiete

OPC UA erfüllt die Konformitätsanforderungen für Industrie 4.0, darunter integrierte Sicherheit, Informationsmodellierung, automatische Geräteerkennung, Skalierbarkeit, Verwendung semantischer Daten und Protokollstandardisierung. [250]

MQTT und Sparkplug

Ein offenes Netzwerkprotokoll für die Machine-to-Machine-Kommunikation (M2M) ist MQTT (ursprünglich MQ Telemetry Transport). Es ermöglicht die Übertragung von Telemetriedaten in Form von Nachrichten zwischen Geräten und das vor allem auch bei Verzögerungen oder beschränkten Netzwerken. Sensoren und Aktoren, Mobiltelefone, eingebettete Systeme in Fahrzeugen oder Laptops sowie Standard-PC sind einige der entsprechenden Geräte. [244][245]

MQTT ist ein Kommunikationsprotokoll zwischen Client und Server. Nachdem die Verbindung hergestellt ist, schicken die Clients dem Server („Broker“) Nachrichten mit einem Thema, das die Nachricht hierarchisch ordnet. Außerdem brauchen die Themen nicht zuvor konfiguriert zu werden. Diese Themen können von den Clients abonniert werden, und der Server übermittelt den entsprechenden Abonnenten die erhaltenen Nachrichten. [244][246]

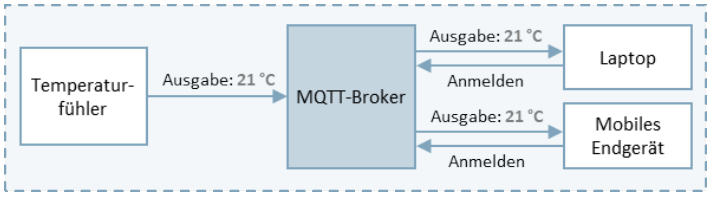


Abbildung 80: einfache Struktur einer MQTT-Architektur [Eigene Darstellung nach [244]]

Sparkplug ist eine Spezifikation der Industrie, die von der Eclipse Foundation entwickelt wurde und bestimmte Normen und Strukturen in die MQTT-Kommunikation einbezieht. Sparkplug nutzt MQTT als Grundlage und bietet Funktionen wie MQTT-Topic-Namespace, Datenmodell und -struktur, erweiterbare Prozessvariablen-Nutzlast sowie MQTT-Statusverwaltung. Diese sind für Anwendungsfälle im Bereich des IIoT und der Industrie 4.0 von großer Bedeutung. Die Sparkplug-Spezifikation dient der Erreichung der drei nachfolgend aufgeführten Ziele: Ein Topic-Namensraum wird definiert, die Datenstrukturen des Payloads werden spezifiziert und das Zustandsmanagement wird definiert. [182]

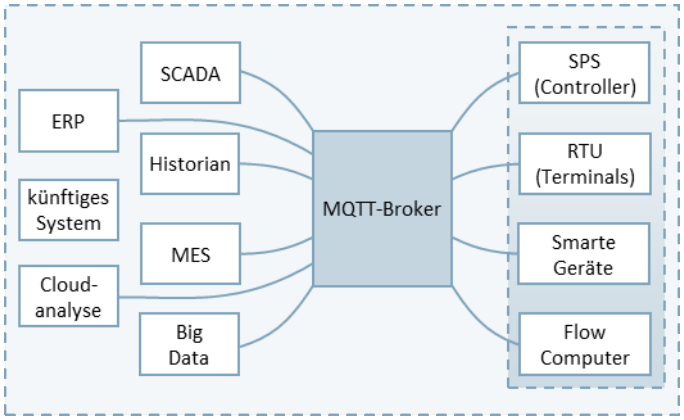


Abbildung 81: MQTT-Sparkplug-Architektur [Eigene Darstellung nach [245]]

Laut [245] bestehen folgende Anforderungen an Plug and Play im IIoT: “single source of truth”, “decoupled data”, “immediate discovery”, “inherited security” und “state awareness”.

Die Sparkplug-Infrastruktur wird OPC nicht ersetzen, sondern vielmehr ergänzen. In bestehenden Industriestandorten werden bspw. OPC UA-Polling-Engines eingesetzt, um Zugriff auf die Rohprozessvariablen zu erhalten. Allerdings ist Sparkplug in vielen Szenarien die bessere Wahl als OPC UA. Hier ein paar Punkte:

- Sparkplug bietet reine Device-to-OT Publish/Subscribe Message-orientierte Middleware-Architekturen (MOM).
- MQTT-Broker und Sparkplug sind einfach genug für die Telemetriekommunikation zwischen Sensoren und Geräten.
- Sparkplug ist einfach genug, um auf allen Arten von Edge-Geräten implementiert zu werden.

Besondere Vorteile

- Sehr weit verbreitet, da die Komplexität gering ist. [246]
- Die Menge der zu übertragenden Daten ist aufgrund der sehr schlanken Struktur des Protokolls relativ gering. [246]
- Es wurde speziell konzipiert, um die Übermittlung von Daten an Standorten mit begrenztem Infrastrukturnetz und energiesparenden Geräten mit geringem Leistungsumfang zu ermöglichen. [247]
- Die Publish/Subscribe-Architektur mit Verwendung des MQTT-Brokers. [247]
- Da jeder Client nur den Message Broker kennt, nicht aber die anderen Teilnehmer, so sind die Geräte und Anwendungen vollständig entkoppelt. Dies trägt insbesondere bei sicherheitsrelevanten Infrastrukturen, wesentlich zur Trennung zwischen IT und OT bei. [247]
- Protokollfunktionen von MQTT sind ein weiteres beliebtes Merkmal des Kommunikationsprotokolls in Bezug auf IoT-Anwendungsfälle. Typische Schwierigkeiten in begrenzter Infrastruktur, die die Bandbreite beeinträchtigt oder die Konnektivität instabil ist, werden durch diese Eigenschaften verbessert. [247]

Spezielle Nachteile

- Aufgrund fehlender Angabe des Inhalts der Nachricht müssen Sender und Empfänger zuerst eine Notation verhandeln. Dies erfordert technisches Know-how sowie einen gewissen Konfigurationsaufwand. [246]
- Die Funktionalität ist darauf beschränkt, Daten zu senden und zu empfangen. Es ist nicht möglich, gepufferte Daten nach Verbindungsausfall zu übertragen oder Webseiten zu routen. [246]

7.2.5 Spiegelung der Technologien am Leitbild

Die Vorgehensweise im Abschnitt 7.2.5 folgt der Abbildung 82. Die Vorgehensweise wurde aus dem Leitbild und den Anforderungen entwickelt und baut auf den vorangegangenen Arbeiten aus der Analyse auf. Die Abbildung zeigt damit das weitere Vorgehen mit der Analysetabelle auf. Hierbei werden die jeweiligen Vor- und Nachteile hinsichtlich des Leitbildes, sowie die Eigenschaften erarbeitet.

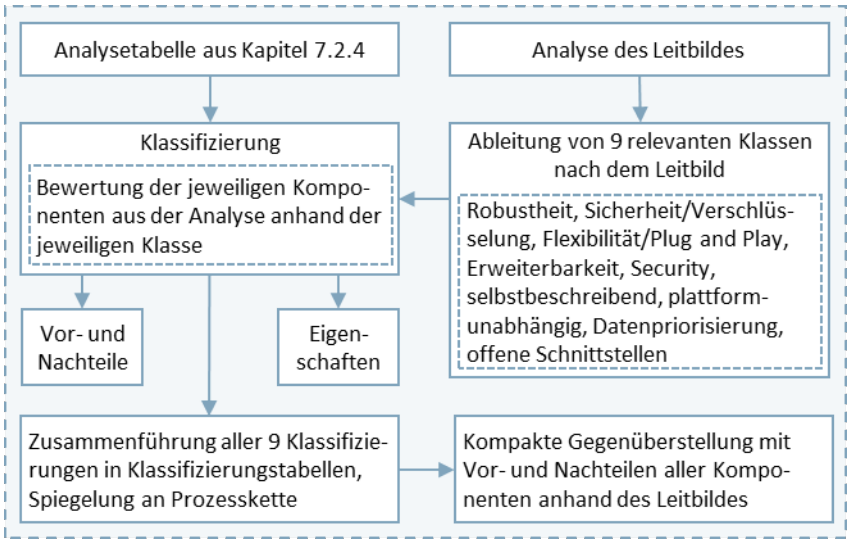


Abbildung 82: Vorgehensweise im Kapitel 7.2.5 Spiegelung der Technologien am Leitbild

Aus dem Leitbild wurden die neun relevantesten Eigenschaften ausgewählt. Die Sensorkomponenten wurden anschließend in Bezug auf ihre Eignung und ihren Funktionsumfang bewertet.

TABELLE 69: SPIEGELUNG AUSGEWÄHLTER KOMPONENTEN AM LEITBILD DES PROJEKTES

Komponente	Flexibili-tät Plug & Play	Erweiter-barkeit	Security	Selbst-be-schrei-bend	Platform-unabhäng-igkeit	Priorisie-rung	Offene Schnitt-stellen	Robust-heit	Sicherheit Verschlüs-selung
Personenverkehr									
TRDP	-		***	-	***	-	**	***	-
RMR	-	***			**		-		
Güterverkehr									
TIS/ITSS		***	-	-	**	-	***		-

Komponente	Flexibili-tät Plug & Play	Erweiter-barkeit	Security	Selbst-be-schrei-bend	Platform-unabhäng-igkeit	Priorisie-rung	Offene Schnitt-stellen	Robust-heit	Sicherheit Verschlüs-selung
Betriebstechnologie									
IO-Link	**	***	***	-	***	-	**	***	-
CIP			***	-	***	**	**	***	-
Lon(Works)	**	***	***	-	***	***	***	***	***
Informationstechnologie									
XML		***	-	***	***				-
JSON		***	-	***	***				-
SSN		***	-	***	***				-
USB	**	***	-	**	***	-	***	***	-
UDP			-	-	***	-		***	-
TCP/IP			-	-	***	-	***	***	-
UML		***	-	***	***				-
SysML		***	-		***				-
SensorML		***	-	***	***				-
Konvergenz von Betriebs- und Informationstechnologie									
OPC UA	***	***	***	***	***	**	**	***	***
MQTT (Sparkplug)	- (***)	***	***		***		**	***	***

Legende

*** Vorhanden

** Teilw. vorhanden

- Nicht vorhanden

Keine Angabe oder nicht relevant

Durch die Kombination der verschiedenen Technologien kann in vielen Anwendungen die gesamte Prozesskette der Datenverarbeitung abgedeckt werden. Verschiedene Kombinationsmöglichkeiten zeigen die Abbildung 56, Abbildung 64 und Abbildung 83 aus den vorangegangenen Kapiteln. Ausgangspunkt sind die Prozesskette der Datenverarbeitung (siehe Abbildung 53) und das OSI-Modell (siehe Abbildung 51) wie in den Vorarbeiten aufgezeigt.

7.2.6 Darstellung an ausgewählten Use Cases

7.2.6.1 Hintergrund und Zielstellung

Im Kapitel 4 Bestandsaufnahme Sensormarkt wurden zahlreiche Anwendungsfälle für Sensoren im Bahnbereich recherchiert (siehe Abschnitt 4.1.2). Gemeinsam mit Expertinnen und Experten wurde durch Interviews, Umfragen und Workshops eine Auswahl aus der Gesamtheit der Rechercheergebnisse

getroffen (siehe Abschnitt 4.2.2). Auf der Grundlage einer Anforderungsanalyse wurden die ausgewählten Use Cases detailliert beschrieben und erforderliche Sensorikkomponenten benannt (siehe Abschnitt 4.3.2).

Die ausgewählten Use Cases wurden in Tabelle 5 aufgelistet. Der nachfolgende Abschnitt 4.3.2 zeigt für jeden Use Case eine Abbildung mit möglichen Sensortypen und Installationsorten am Schienenfahrzeug auf. Die ausgewählten Use Cases beschreiben verschiedene Einsatzmöglichkeiten von Sensoren. Gemeinsam ist diesen Use Cases die Anwendung von Sensoren zur Durchführung einer Messaufgabe zur Bestimmung von Zuständen oder Eigenschaften der ebenfalls beschriebenen Messobjekte. Darüber hinaus wird ein Nutzen in der allgemeinen Bereitstellung und dem Austausch der Sensordaten gesehen.

In Kapitel 7 Bestandsaufnahme und Patentrecherche – Sensoriksysteme und Teilkomponenten wurden Technologien zur Gestaltung von Sensoriklösungen recherchiert. Abschnitt 7.1.3 beschreibt die entsprechenden Rechercheergebnisse. In den folgenden beiden Abschnitten werden diese in den Kontext der industriellen Automatisierung (Abschnitt 7.1.3) und des Bahnsystems (Abschnitt 7.1.4) gesetzt. In Abschnitt 7.2 wurde eine Auswahl an Technologien aus dieser Recherche getroffen, detailliert analysiert und am Leitbild gespiegelt.

Aus den bisherigen Ergebnissen wurde im aktuellen Abschnitt 7.2.6 eine universelle Sensoriklösung abgeleitet. Die Rechercheergebnisse aus der industriellen Automatisierung, dem IoT und der Bahnwelt zeigen, dass sich die Technologien auf einige wenige universelle Architekturen reduzieren lassen: Automatisierungspyramide, IoT und OT-IT-Konvergenz. Für die weitere Diskussion der Ergebnisse wurden zwei Use Cases aus Abschnitt 4.2.2 ausgewählt sowie ein Test Case aus den Shift2Rail-Projekten CONNECTA-2 und Safe4Rail-2.

7.2.6.2 Ableitung einer universellen Sensoriklösung

Abschnitt 7.1.2 enthält eine Darstellung der Rechercheergebnisse über Technologien zum Aufbau von Sensorikanwendungen. Ausgehend von den Sensoren wird wie in Abschnitt 7.1.2.2 dargestellt, ein Sensorsystem aufgebaut. Wie im Abschnitt 7.1.2.3 beschrieben sind auch heute noch viele Sensoren mit einer einfachen analogen oder digitalen Schnittstelle ausgestattet. Daher werden die Sensoren in einem ersten Schritt mit einer Auswerteelektronik (siehe Abschnitt 7.1.2.2) verbunden. Wurde ein smarter Sensor ausgewählt, ist die Auswertelektronik bereits integriert (siehe Abschnitt 7.1.2.5).

Ein solches Sensorsystem kann anschließend Messdaten aufnehmen, vorverarbeiten und an einer digitalen Schnittstelle bereitstellen. Dieser Vorgang wird als Prozess der Datenerfassung bezeichnet und ist in Abschnitt 7.1.2.7 in Abbildung 52 dargestellt. Nachdem das Sensorsystem die Daten erfasst hat, können sie ausgehend von dieser Schnittstelle übertragen, weiterverarbeitet, gespeichert oder angezeigt werden. Dieser Vorgang kann als Prozess der Datenverarbeitung beschrieben werden (siehe Abbildung 53). Nach Erfassung der Daten, hängt die Datenverarbeitung sehr stark vom Anwendungsfall ab. Es gibt jedoch etablierte Architekturen und wie die Recherche besonders in Abschnitt 7.1.3 zeigte, durch Digitalisierung, das IoT, Industrie 4.0 und andere smarte Anwendungen auch neue Systemarchitekturen. Diese berücksichtigen den Wunsch nach Vernetzung und einem umfassenderen Datenaustausch.

Der Aufbau einer klassischen Sensoranwendung könnte daher dem Beispiel der Automatisierungspyramide folgen (siehe Abschnitt 7.1.3.2). Dies ist eine in der industriellen Leittechnik etablierte und bewährte Struktur. Wie im Abschnitt beschrieben, sind die Möglichkeiten des Datenaustausches mit Systemen außerhalb des Leitsystems allerdings begrenzt und würden zudem nur über die höheren Ebenen der Pyramide realisiert. Dort sind die Daten bereits mehrfach verarbeitet. Zudem nimmt die Latenz der Datenübertragung ab. Nach dieser klassischen Struktur würde bspw. eine SPS die Funktion der Auswer-

teelektronik übernehmen und die Sensoren, wie in Abbildung 56 aufgezeigt, direkt mit dieser verbunden. Zur weiteren Datenübertragung in die höheren Ebenen würden Feldbusse oder Feldbusnetzwerke eingesetzt (siehe Tabelle 48).

Alternativ dazu kann der Fokus stärker auf Vernetzung und den Datenaustausch gelegt werden. Das Konzept des IoT (siehe Abschnitt 7.1.2.9) verfolgt eine umfassende Vernetzung aller physischen und virtuellen Dinge. Angewendet auf die industrielle Automatisierung geben die Bestrebungen von Industrie 4.0 (siehe Abschnitt 7.1.3.3) und dem industriellen IoT (siehe Abschnitt 7.1.3.4) einen strukturierten Ansatzpunkt. Dabei steht nicht nur die allumfassende Vernetzung, sondern auch die Zusammenführung von Betriebstechnologien und Informationstechnologie (siehe Abschnitt 7.2.4.5) im Fokus. Daraus lassen sich zwei weitere Systemarchitekturen ableiten. Die vollständige Vernetzung nach dem Konzept des IoT und der etwas stärker strukturierte Ansatz, welcher sich aus der Konvergenz von Betriebs- und Informationstechnologie ergibt. Eine entsprechende Systemarchitektur ist in Abbildung 64 aufgezeigt.

Das Kapitel 7.1 zeigt eine große Vielfalt an existierenden Technologien. Diese entsprechen dem aktuellen Stand der Technik. Entscheidend ist, dass sie sich auf nur wenige übergreifende universelle Systemarchitekturen reduzieren lassen. Die nachfolgende Use Case-Diskussion soll daher auf der Grundlage einer universellen Architektur nach dem Konzept der Konvergenz von Betriebs- und Informationstechnologie (siehe Abbildung 77 und Abbildung 64) durchgeführt werden. Die Use Cases zeigen Beispiele für eine universelle, eine aktuelle und eine zukünftige Umsetzung von Sensornetzen im Bahnverkehr.

7.2.6.3 Use Case “Fahrzeug überwacht Oberbau”

Die Basisinformationen des Use Cases „Fahrzeug überwacht Oberbau“ wurden in Tabelle 7 des Abschnittes 4.3.2 beschrieben. Mit Sensoren an den Schienenfahrzeugen sollen Daten über den Oberbauzustand gewonnen werden. Ziel ist die Verbesserung der Oberbauqualität und eine zustandsorientierte Instandhaltung der Infrastruktur. Mögliche Sensoren sind in Tabelle 8 benannt. Eingesetzt werden können Beschleunigungssensoren, IMUs, berührungslose Abstandssensoren und Linien-Laser-Scanner.

Im Abschnitt 7.2.6.2 wurde aus den Rechercheergebnissen des Abschnittes 7.1 und der Analyse in Abschnitt 7.2 eine universelle Sensoriklösung abgeleitet. Dieses Konzept verbindet Betriebs- und Informationstechnologien in einem flexiblen, vollständig vernetzten Sensorikkonzept mit Datenanbindung an ein Rechenzentrum oder eine Cloud. Eine mögliche Architektur basierend auf der universellen Sensoriklösung ist in Abbildung 83 dargestellt.

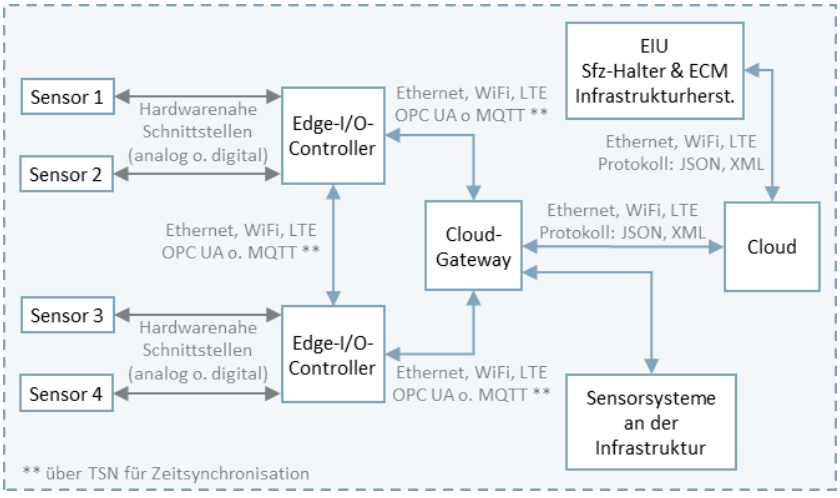


Abbildung 83: Darstellung anhand von Use Case „Fahrzeug überwacht Oberbau“ [Fraunhofer ENAS]

Die vorgeschlagenen Sensoren werden an geeigneten Positionen am Schienenfahrzeug montiert. Sie werden mit ihrer analogen oder digitalen, hardwarenahen Schnittstelle mit einem Edge-I/O-Controller verbunden. Zusammen mit diesem bilden sie das eigentliche Sensorsystem (siehe Abbildung 42). Der Edge-I/O-Controller ist dafür zum einen mit den entsprechenden Sensorschnittstellen (siehe Abschnitt 7.1.2.3) ausgestattet und zum anderen mit einer Netzwerkschnittstelle (siehe Abschnitt 7.1.2.6) für den Datenaustausch mit weiteren Edge-I/O-Controllern, anderen Netzwerkteilnehmenden oder einem Cloud-Gateway. Der Edge-I/O-Controller steuert die Datenerfassung von den Sensoren und synchronisiert diese, wenn notwendig. Konfigurierbare Sensoren können über ihn parametrisiert werden.

Die für den Use Case vorgeschlagenen Sensoren werden zur Vermessung des Oberbaus durch das Schienenfahrzeug während der Fahrt eingesetzt. Sie müssen daher kontinuierlich Daten mit hohen Abtastraten aufnehmen. Im Edge-I/O-Controller entstehen folglich größere Datenmengen. In vielen Fällen ist es nicht erforderlich diese Rohdaten lokal zu speichern oder in eine Cloud zu übertragen. Die Daten können daher direkt im Edge-I/O-Controller verarbeitet und interpretiert werden. Dies kann z. B. so aussehen, dass aus dem hochaufgelösten Signal eines dreiachsigen Beschleunigungssensors ein einzelner Kennwert über den Zustand des Oberbaus pro Abtastung berechnet wird. Dessen Übertragung ist im Vergleich zum Rohsignal sehr viel datensparsamer, schneller und kostengünstiger möglich.

Im industriellen Kontext können solche Edge-I/O-Controller meist mit vorhandenen Ethernet-Netzwerken verbunden werden und Daten in das firmeneigene Rechenzentrum oder zu einem externen Cloud-Anbieter übertragen. Am Schienenfahrzeug besteht nun die Frage, ob so ein Gerät an das fahrzeugeigene Bussystem oder Netzwerk angeschlossen werden kann. Dieser Frage wurde in Abschnitt 7.1.4 bei der Recherche zu sensorbasierten Technologien im Bahnsystem nachgegangen. Güterzüge sind bisher noch nicht mit einer Stromversorgung und Datenleitungen ausgestattet (siehe Abschnitt 7.1.4.3). Es finden jedoch intensive Entwicklungsarbeiten im Rahmen der DAK statt, sodass sich die Situation zukünftig ändern wird. Personenzüge sind weitestgehend mit Bussystemen ausgerüstet (siehe Abschnitt 7.1.4.2). Die bisherigen TCN auf Basis von WTB und MVB sind allerdings allein schon aufgrund ihrer begrenzten Bandbreite nur eingeschränkt für umfangreiche Sensoranwendungen geeignet. Die Situation verbessert sich mit der fortschreitenden Einführung von Ethernet-basierten TCN wie ETB und ECN. Wie Abschnitt 7.1.4.2 zeigt, sind auch drahtlose Netzwerke in Entwicklung.

In einem Ethernet-basierten leistungsfähigen Netzwerk würden die Daten zunächst an ein Cloud-Gateway übertragen und von dort an einen Cloudspeicher, ein Rechenzentrum oder eine Datendrehscheibe. Über diesen hätten dann auch alle Stakeholder Zugriff auf die Daten oder eine Teilmenge davon.

7.2.6.4 Use Case „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“

Die Basisinformationen des Use Cases „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“ wurde in Tabelle 11 des Abschnittes 4.3.2 beschrieben. Sensoren sollen Türen, u. a. Verriegelungen, überwachen, um die Abfahrbereitschaft des Zuges feststellen zu können. Darüber hinaus können manuelle Vorgänge eingespart und ungewöhnliche Ereignisse während der Zugfahrt erkannt werden. Weiterhin können Verschleißerscheinungen detektiert werden. Mögliche Sensoren sind in Tabelle 12 aufgeführt. Zu diesen zählen Sensoren zur optischen Objekterkennung, Radar, Abstands- und Kontaktsensoren, Druckwellenschalter, sowie Strom-, Körperschal- und Beschleunigungssensoren.

Prinzipiell könnte auch bei diesem Use Case die Architektur der universellen Sensorlösung eingesetzt werden. Sensoren sind mit einem Edge-I/O-Controller oder Steuergerät verbunden und erfassen Messwerte von Türen oder Verriegelungen. Die Situation ist allerdings anders als z. B. im Use Case „Fahrzeug überwacht Oberbau“. Zum einen besteht Sicherheitsrelevanz und zum anderen ist auf der Basis der Sensorsignale eine direkte Aktion erforderlich, wie z. B. das Verhindern der Türschließung oder der Abfahrt

des Zuges. Zum anderen besteht der Use Case je nach Ausprägung aus weiteren Subsystemen. Beispielhaft dafür können Türsteuersysteme für Personenzüge betrachtet werden (siehe Abschnitt 7.1.4.2). Diese sind nach einem dezentralen, zentralen oder Master-Slave-Konzept aufgebaut. Die Sensoren sind direkt mit dem Steuergerät verbunden, was vergleichbar mit einem Edge-I/O-Controller ist. Das Steuergerät nutzt die Sensorsignale zur Steuerung der Tür und um Statusmeldungen an das übergeordnete Zugsystem weiterzugeben. Ein direkter Zugriff auf die Sensorsignale ist dabei meist nicht vorgesehen. Die Abbildung 84 zeigt am Beispiel eines Bahnsteigtürsystems eine Systemarchitektur mit zentralem Kommunikationsserver.

Die Shatin to Central Line (SCL), die 560 dieser Türsysteme umfasst, wird in Hongkong betrieben. Die Linie wurde ohne Publikumsbetrieb gebaut. Die restlichen 720 Türsysteme wurden über Nacht in der Ma On Shan-Linie nachgerüstet, die seit 2004 betrieben wird. Der Betreiber MTR sorgt für 19 Stunden Zugverkehr pro Tag an 365 Tagen im Jahr. Trotz der geplanten Hochfrequenz von bis zu 130 Sekunden, wurde das Türsystem für eine Betriebsdauer von 35 Jahren konzipiert. [258]

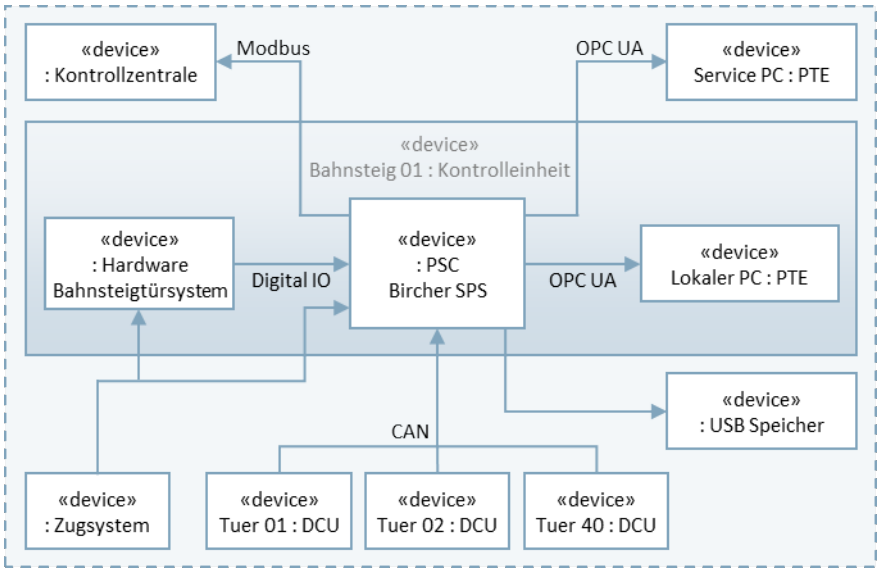


Abbildung 84: Türsteuerung [Eigene Darstellung nach [258]]

Der Hauptzweck des Kommunikationsservers (PSC) besteht darin, den gegenwärtigen Zustand des Türsystems zu erfassen und alle kritischen Zustände als Alarme an das stationäre Kontrollsystem zu melden. Gleichzeitig zeigt die lokale PC-Visualisierung den Zustand ausführlich an. Um eine Problemanalyse durchzuführen, werden die Daten und Alarme im remanenten Speicher sowie in Dateien festgehalten und gegebenenfalls über OPC UA, FTP oder USB zur Verfügung gestellt. Die Firmware kann mithilfe des zentralen Software Downloads geladen werden, um die Wartung der drei Steuersysteme pro Tür bequem und zügig durchzuführen. [258]

Sind die Sensoren Bestandteil eines Subsystems, wie z. B. einer Türsteuerung, liegt es beim Hersteller ob ein Zugriff auf die Sensordaten möglich ist. Wie Abbildung 84 zeigt besitzt der zentrale Kommunikationsserver zahlreiche Schnittstellen unter anderem auch das aus industriellen Anwendungen bekannte OPC UA. Dieser Kommunikationsstandard wird im folgenden Abschnitt an einem Test Case aus Shift2Rail näher betrachtet.

7.2.6.5 Test Case 2 „TSN Network & OPC UA” (Shift2Rail)

Im Abschnitt 7.2.5 erhielt der Kommunikationsstandard OPC UA bei der Spiegelung am Leitbild für Sensoriksysteme und Komponenten eine sehr gute Bewertung. Daher soll dieser ergänzet zu den beiden Sensorik Use Cases aufgeführt werden. In den Projekten CONNECTA-2 und Safe4Rail-2 wurden Untersuchungen zu OPC UA durchgeführt. Dabei wurden ausgewählte Komponenten eines Consists mit Ethernet verbunden und OPC UA zur Datenübertragung genutzt. Das Versuchsschema ist in der nachfolgenden Abbildung 85 dargestellt.

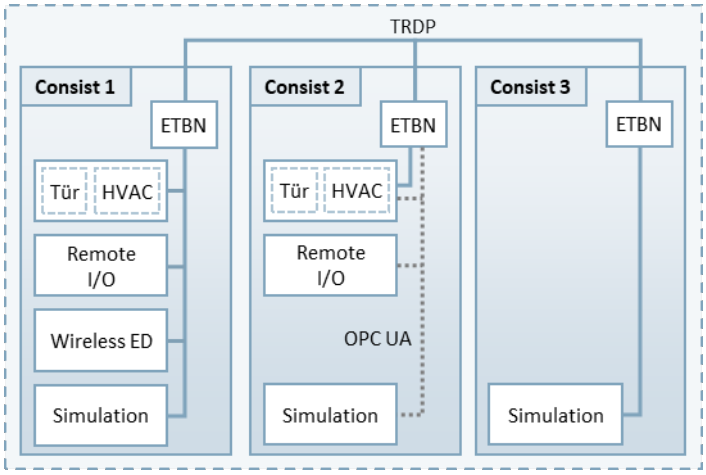


Abbildung 85: Shift2Rail Test Case 2 „TSN Network & OPC UA“ [Eigene Darstellung nach [259]]

Der Demonstrator bestand aus drei Consists, welche mit Ethernet ausgestattet waren. Die Datenverbindung wurde über ein IP/TSN basiertes TCN realisiert. Als Datenübertragungsprotokoll wurde Train Real Time Data Protocol (TRDP) eingesetzt. Im Consist 2 wurde ab dem ETBN OPC UA zur Datenübertragung verwendet. Genutzt wurde der Open Source OPC UA Stack open62541. Die Demonstration verlief erfolgreich und OPC UA wurde für eine weitere Erprobung im Bahnsystem als geeignet bewertet. Als Vorteile wurden unter anderem genannt: Herstellerunabhängigkeit, spezifiziert nach IEC 62541, spezifiziert sowie geprüft und zertifiziert bei der unabhängigen OPC Foundation. [259]

Weitere Informationen zu OPC UA sind im Abschnitt 7.2.4.5 und im Abschnitt 7.3.4.6 beschrieben.

7.2.7 Zusammenfassung des Abschnittes

Im Abschnitt 7.2.6 wurde ausgehend von den Rechercheergebnissen in Kapitel 7.1im Abschnitt 7.2.6.2die Vision eines zukünftigen, universellen Sensoriksystems für ausgewählte Use Cases im Bahnbereich ausgearbeitet. Davon ausgehend wurde ein universeller (siehe Abschnitt 7.2.6.3), ein aktueller (siehe Abschnitt 7.2.6.4) und ein zukünftiger (siehe Abschnitt 7.2.6.5) Use Case betrachtet.

7.3 Patentrecherche

7.3.1 Vorgehen und Methodik

Für die ausgewählten Technologien und Architekturen wurde eine Schutzrechtsanalyse durchgeführt. Zunächst wurden Normen und Standards recherchiert. Waren diese vorhanden, wurden die ausstellenden Organisationen wie z. B. Stiftungen oder Vereine ermittelt. Handelte es sich nicht um einen offenen

Standard, wurden die Lizenzrichtlinien und, soweit möglich, die Höhe der Lizenzgebühren ermittelt. Alle im Arbeitspaket 4 untersuchten Architekturen wurden im Wesentlichen bereits standardisiert, genormt oder befinden sich in einem dieser Prozesse. Überwiegend handelt es sich zudem um offene Standards oder Normen. Lizenzgebühren können jedoch für bestimmte Kombinationen von Technologien und Architekturen anfallen. Dies betrifft einige Feldbusse zur Sensoranbindung, Datenübertragungssysteme und Softwaretechnologien.

Abschließend wurde eine Patentrecherche über PatBase durchgeführt. Dabei wurde untersucht, ob einzelne Anwendungsfälle oder Ausführungsvarianten der ausgewählten Technologien und Architekturen mit Patenten belegt sind. Hierbei ist eine pauschale Beurteilung ohne eine genaue Spezifikation des angestrebten Produktes nicht möglich, da die vorhandenen Patente jeweils nur spezielle Ausführungsformen betreffen.

7.3.2 Standardessenzielle Patente

Um sicherzustellen, dass ein Standard die Technologie von höchster Qualität umfasst, muss diese in den Standard integriert werden. Allerdings kann der Standard nicht mehr ohne das Patent angewendet werden, wenn die Technologie ein Patent besitzt. Standardessentielle Patente (SEPs) werden dabei erwähnt. Der Umgang mit SEPs kann zu langwierigen rechtlichen Auseinandersetzungen führen und die Vorzüge der Standardisierung, wie etwa die Förderung von Innovationen, in Frage stellen. [260]

Mit dem CEN Workshop Agreement CWA 95000 „Core Principles and Approaches for Licensing of Standard Essential Patents“ haben mehr als 50 Organisationen aus verschiedenen Industriezweigen und allen Bereichen der Innovationskette einen Leitfaden zur Lizensierung standardessentieller Patente erstellt. Dies ebnete den Weg für die Verbreitung des IoT in Europa. [260]

FRAND-konforme Lizensierung von SEPs

Lizenzen für die relevanten standardisierten Technologien sind für Hersteller intelligenter Produkte erforderlich, die von Standardpatenten Gebrauch machen möchten. Nach geltendem Recht müssen Inhaber von standardessentiellen Patenten ihre Patente an potenzielle Nutzende des Standards unter fairen, angemessenen und nichtdiskriminierenden Bedingungen lizensieren (FRAND: Fair, Reasonable and Non-Discriminatory). [261]

7.3.3 Offener Standard

In der Genfer Erklärung 2008 (OpenForum Europe) unterstützten 17 Organisationen diese Definition, die auch vom Document Freedom Day und der FSFE verwendet wird: [262]

„Ein Offener Standard bezieht sich auf ein Format oder Protokoll, das

- einer vollständig öffentlichen Bewertung und Nutzung ohne Hemmnisse auf eine für alle Beteiligten gleichermaßen zugänglichen Weise unterliegt,
- ohne jegliche Komponenten oder Erweiterungen ist, die von Formaten oder Protokollen abhängen, die selbst nicht der Definition eines Offenen Standards entsprechen,
- frei ist von juristischen oder technischen Klauseln, die seine Verwendung von jeglicher Seite oder jeglichem Geschäftsmodell einschränken,
- unabhängig von einem einzelnen Anbieter geleitet und weiterentwickelt wird in einem Prozess, der einer gleichberechtigten Teilnahme von Wettbewerbern und Dritten offensteht,
- verfügbar ist in verschiedenen vollständigen Implementierungen von verschiedenen Anbietern oder als vollständige Implementierung gleichermaßen für alle Beteiligten.“ [262]

7.3.4 Recherche und Analyse der Patentsituation

7.3.4.1 Rechercheziele des Abschnittes

In der folgenden Tabelle 70 sind die Rechercheergebnisse der Schutzrechts- und Patentanalyse aufgelistet.

TABELLE 70: ERGEBNISSE DER SCHUTZRECHTSANALYSE

Begriff	IP	Standards	Kosten	Beschreibung
Personenverkehr				
TRDP	Open Source (Mozilla Lizenz MPL2)	IEC61375-2-3 (2015)		Netzwerkprotokoll
RMR				Zugkommunikationsnetz
Güterverkehr				
TIS/ITSS	nein	ITSS Standart Specification		Systemarchitektur
Betriebstechnologie				
IO-Link	IO-Link Lizenzmodell	IEC 61131-9	Lizenzgebühren	Kommunikationsstandard
CIP	Lizenzierung	ODVA	$ 2.000 bis $ 150.000	Kommunikationsprotokoll
Lon(Works)	Open Standard	ISO/IEC 14908		Feldbus
Informationstechnologie				
XML	Open Protocol	basiert auf SGML (ISO 8879)	keine	Auszeichnungssprache
JSON	Open Source	RFC 8259, ECMA-404	keine	Datenaustauschformat
SSN	nein	Open Geospatial Consortium Standard		Ontologie
USB	Lizenzierung	USB 1 bis 4	$ 3.500 bis $ 6.000, Mitgliedschaft: $ 5.000	Datenübertragungssystem
UDP	nein, lizenzfrei	RFC 768		Netzwerkprotokoll
TCP/IP	nein, lizenzfrei	RFC 9293 / RFC 8200		Netzwerkprotokoll
UML	RF-Limited	ISO/IEC 19505-1:2012, ISO/IEC 19505-2:2012		Modellierungssprache

Begriff	IP	Standards	Kosten	Beschreibung
SysML	Open Source	ISO/IEC 19514:2017		Modellierungssprache
SensorML	nein, lizenzfrei	OGC Standard		Auszeichnungssprache
Konvergenz von Betriebs- und Informationstechnologie				
OPC-UA	Open Source	IEC62541	Mitgliedschaft	Kommunikationsstand-ard
MQTT	Open Protocol	OASIS und ISO/IEC 20922:2016		Netzwerkprotokoll

Eine detaillierte Darstellung der Situation für die einzelnen Komponenten erfolgt in den folgenden Abschnitten.

7.3.4.2 Personenverkehr

TCN und NG-TCN

Der Austausch von Informationen im Zug hat sich inzwischen jedoch immer umfangreicher und komplexer entwickelt. Dies erfordert ständige Weiterentwicklungen des TCN. Um den wachsenden Leistungsanforderungen moderner Anwendungen und On-Board-Services wie Fahrzeugdiagnose, Sicherheitsfunktionen (Brake-by-Wire), Videoüberwachung oder WLAN-Internetzugriff gerecht zu werden, wurden die beiden in der IEC 61375-Reihe genannten seriellen Busse (Zugbus WTB und Fahrzeugbus MVB) durch Busse auf der Basis von Ethernet (ETB und ECN) ersetzt. [269]

Die Interoperabilität wird durch diese schnelleren TCN beeinträchtigt, da sie herkömmliches 100 Mbit/s-Ethernet mit verschiedenen, Kommunikationsprotokollen wie TRDP, CANopen, Customer Information Platform (CIP) (Alstom), Profinet (Siemens) oder IP Train Communications (IPTCom) (Bombardier) verbinden. Einige davon sind proprietär. Darüber hinaus verfügt das herkömmliche Ethernet über nicht genügend Mechanismen für Funktionen, die sicherheits- und zeitkritisch sind. [269]

Standardisierung und Lizensierung

Die einzelnen Standardisierungsschritte der IEC-61375-Reihe sind in Abbildung 74 aufgezeigt.

TRDP

Das Hauptziel von TCNOpen besteht darin, eine passende Umgebung, die Open Interest Group, zu schaffen, in der Partnerunternehmen gemeinsam neue Bauteile entwickeln können, die den TCN-Standard erfüllen. Ein bestimmtes Open-Source-Projekt wird für jeden einzelnen Bestandteil gestartet und durchläuft alle notwendigen Phasen: Spezifikation, Entwicklung, Test, Support. Derzeit wird ein erstes Projekt durchgeführt, das die Entwicklung des TRDP-Moduls betrifft. [263]

Ein Zwischenmodul zwischen den TCP- oder UDP-Protokollen und den Anwendungen, die das Netz verwenden, ist TRDP (Train Realtime Data Protocol). Hier wird seine Position innerhalb der generellen TCN-Architektur betont. Das Kommunikationsprofil gehört zum Zugkommunikationsnetz und erlaubt eine Interoperabilität zwischen einheitlichen Netzen (z. B. dem Ethernet-Konsistenznetz gemäß Teil 3 – 4) und dem Ethernet-Zug-Backbone gemäß Teil 2 – 5. [263]

Es ist möglich, eine zusätzliche Sicherheitsschicht (SDT) hinzuzufügen. Safe Data Transmission (SDT) ist ein End-to-End-Protokoll, das auf einem unzuverlässigen Kommunikationskanal verwendet wird. SDT entspricht der Norm IEC 62280 (EN 50159). Es ermöglicht, sicherheitsrelevante Daten zwischen einer oder mehreren sicheren Datensenken und einer sicheren Datenquelle zu übertragen. [263]

Die Grundlage für eine einheitliche Netzwerkkommunikation in Zügen ist das Train Realtime Data Protocol (TRDP), das in der Norm IEC 61375-2-3 Annex A spezifiziert ist, als Bestandteil des TCN. TRDP basiert auf IP und kann bspw. auf Ethernet aufbauen. Moderne Anwendungen und On-Board-Services wie Fahrzeugdiagnose, Sicherheitsfunktionen (wie Brake-by-Wire), Videoüberwachung oder WLAN-Internetzugang erfordern daher eine ausreichende Bandbreite des offenen Netzwerkprotokolls. [264]

In Zukunft wird das Train Realtime Data Protocol (TRDP), das auf IP basiert, die einheitliche Grundlage für die Kommunikation von Zügen miteinander sein. Eine dynamischere Zugtopologie und eine größere Vielfalt kompatibler Produkte und Anwendungen werden durch die universelle Vernetzbarkeit ermöglicht. Des Weiteren dient TRDP als Grundlage für künftige Zugnetzwerke, die auf TSN (Time Sensitive Network) basieren. [265]

Der Austausch von Prozessdaten (PD) und Message-Daten (MD) zwischen Geräten wie Türsteuerungen, Displays, Klimaanlagen und anderen ist möglich, da er auf UDP und optional auf TCP aufbaut. TRDP ist ein rahmenorientiertes Protokoll ohne Verbindungen und dient als Grundlage für die Kommunikation in kommenden Zügen. Das firmeneigene IPTCom-Protokoll von Bombardier Transportation gilt als Vorläufer, von dem TRDP zahlreiche Eigenschaften übernimmt. [265]

Die Arbeitsgruppe TC9/WG43 des IEC hat das Protokoll im Rahmen des TCN erstellt und in IEC 61375-2-3 standardisiert. An der Entwicklung und Standardisierung beteiligen sich bedeutende Produzenten und Lieferanten von rollendem Material für den Eisenbahnverkehr. [266]

Die TCNOpen, auch bekannt als „Train Communication Network Open Source Special Interest Group“, ist die Koordinatorin der Aktivitäten. TCNOpen, eine Open-Source-Initiative der Partner der Eisenbahnindustrie, zielt darauf ab, Schlüsselkomponenten für die bevorstehenden Kommunikationsstandards im Bahnbereich gemeinsam zu entwickeln. [266]

Eine „TRDP Light“-Referenzimplementierung in „C“ ist auf der SourceForge-Plattform unter der quelloffenen Mozilla-Lizenz MPL2 verfügbar. [266]

Standardisierung und Lizenzierung

Der Standardisierung ist in IEC 61375-2-3 (2015) beschrieben und unter die Lizenz „Open Source (Mozilla Lizenz MPL2)“ gestellt.

7.3.4.3 Güterverkehr

Das Ziel des TIS ist es, grundlegende Neuerungen für Eisenbahngüterwagen zu erkennen und zu unterstützen, die die folgenden Merkmale erfüllen oder unterstützen: leicht, laufstark, logistisch geeignet, Life-Cycle-Cost-orientiert. [270]

Standardisierung von Telematikdatenaustauschschnittstellen: [271]

- „Server-Server (Schnittstelle 1),
- Telematik Unit-Sensor (Schnittstelle 2),
- Telematik Unit/Sensor-Handheld (Schnittstelle 3) und
- InTrain Communikation (Schnittstelle 4)“. [271]

Standardisierung und Lizensierung

ITSS Standard Specification Interface 1 (Version 1.4) vom 23.01.2024.

7.3.4.4 Betriebstechnologie

IO-Link

IO-Link mit seinen Erweiterungen Safety und Wireless ist eine feldbus- und herstellerunabhängige Kommunikationslösung für Sensoren, Aktoren und Mechatronik, die in jedes bestehende Feldbus-, Informationstechnologie- oder Automations-System integriert werden kann. Derzeit existieren die folgenden IEC-Projekte:

- IEC 61131-9 Edition1 (basierend auf IO-Link Interface and System, V1.1.2)
- IEC 61131-9 Edition2 (basierend auf IO-Link Interface and System, V1.1.3)
- IEC 61139-2 (basierend auf IO-Link Safety - System Extensions)
- IEC 61139-3 (basierend auf IO-Link Wireless - System Extensions)

Die Internationale Elektrotechnische Kommission (IEC) ist ein Normungsgremium mit Sitz in Genf, Schweiz [284]. Sie setzt sich für internationale Standards ein, um Sicherheit, Effizienz, Zuverlässigkeit und Interoperabilität von elektrischen, elektronischen und Informationstechnologien zu gewährleisten.

Standardisierung und Lizensierung

Die Lizenzgebühren beziehen sich auf ein einzelnes Gerät, auf das durch die Geräte-ID verwiesen wird, oder auf einen Master, auf den durch die Bestellnummer verwiesen wird. Die folgenden Beträge sind festgesetzt:

- Für IO-Link Master 5.000 € pro drei Jahre
- Für IO-Link-Gerät 2.500 € pro drei Jahre

Die Gebühren für Erstlizenzen und Folgelizenzen sind identisch. In diesen Lizenzgebühren sind die beim IOLTC zu zahlenden Gebühren für die Testdienstleistungen und die Erstellung eines Testberichts nicht enthalten.

Es entstehen also keine zusätzlichen Kosten für externe Dienstleister. Auch fallen keinerlei Lizenzgebühren für die weltweite Vermarktung von Produkten mit der Wort- und Bildmarke IO-Link an. [285]

Es gibt aber auch die Möglichkeit, als Nicht-Mitglied IO-Link Produkte auf den Markt zu bringen. Dafür hat IO-Link ein neues Lizenzmodell entwickelt.

Eine Mitgliedschaft in der IO-Link-Community erfolgt durch eine Antragstellung beim IO-Link Support Center, das bei der PNO angesiedelt ist, und dem schriftlichen Anerkennen der Ergänzenden Regeln. Als IO-Link Mitglied genießen Sie insbesondere das Recht zur Mitarbeit in allen Arbeitskreisen, frühzeitigen Zugang zu allen Dokumenten und Nutzung der IO-Link Patente von Mitgliedsfirmen sowie kostenfreie Logonutzung. [286]

Referenzen: [287][288][289]

CIP

CIP ist ein medienunabhängiges Protokoll, das ein Producer-Consumer-Kommunikationsmodell verwendet und ein streng objektorientiertes Protokoll auf den oberen Schichten ist. Jedes CIP-Objekt verfügt über Attribute (Daten), Dienste (Befehle), Verbindungen und Verhaltensweisen (Beziehung zwischen Attributwerten und Diensten). CIP umfasst eine umfangreiche Objektbibliothek zur Unterstützung allgemeiner Netzwerkkommunikation, Netzwerkdienste wie Dateiübertragung und typische Automatisierungsfunktionen wie analoge und digitale Ein-/Ausgabegeräte, HMI, Bewegungssteuerung und Positionsrückmeldung.

Standardisierung und Lizensierung

Lizenzierung: $ 2.000 bis $ 150.000

TABELLE 71: GEBÜHREN UND ABGABEN FÜR MITGLIEDER

Charges	Regular	Associate	Principal
Initiation Fee	Waived at this time	Waived at this time	$ 75.000
First Year Annual Dues	$ 6.000	$ 2.000	$ 75.000
Total Amount Due	$ 6.000	$ 2.000	$ 150.000

ODVA [290][291]

Lon(Works)

Local Operatin Network (LonWorks)-Steuerungsnetzwerktechnologien werden seit einigen Jahren in den einzelstaatlichen Normen Europas (EN 14908), Amerikas (ANSI/CEA 709) und Chinas (GB/Z 20177) anerkannt. Die ISO/IEC-Normen wurden als natürliche Folge der Normenentwicklung in ihr Normenportfolio aufgenommen. Im Jahr 2007 reichte das US-amerikanische InterNational Committee for Information Technology Standards (INCITS) die Normenreihe EN 14908 dem Joint Technical Committee 1 (JTC 1) der ISO und IEC ein, um sie international zu standardisieren. [267]

Standardisierung und Lizensierung

ISO/IEC 14908; Open Standard

Es sind verschiedene Mitgliedschaften möglich: Sponsor, Partner, Associate und Individual. [268]

Je nach Anforderung ergeben sich unterschiedliche Mitgliedschaften. Dadurch entstehen laut [272] ebenfalls verschiedene Kosten und Restriktionen.

Hersteller von LonMark-zertifizierten Produkten sind bei den Partnermitgliedern präsent. Partner können sich an Arbeitsgruppen beteiligen und Produkte zur Überprüfung der LonMark-Konformität vorlegen. [268]

Unternehmen und Organisationen, die LonMark-zertifizierte Produkte nicht herstellen, sondern diese nutzen, integrieren, entwickeln oder vertreiben, werden als assoziierte Mitglieder bezeichnet. Diese Kategorie umfasst Distributoren, LonWorks Independent Developers (LIDs), Netzwerkintegratoren und

Systemintegratoren. Associate-Mitglieder haben die Möglichkeit, an Arbeitsgruppen teilzunehmen, stellen jedoch keine Produkte zur LonMark-Konformitätsprüfung vor. [268]

7.3.4.5 Informationstechnologie und IoT

XML

Extensible Markup Language (XML) ist ein einfaches, sehr flexibles Textformat, das von SGML (ISO 8879) abgeleitet ist. XML wurde ursprünglich entwickelt, um den Herausforderungen umfangreicher elektronischer Veröffentlichungen gerecht zu werden, spielt aber auch eine immer wichtigere Rolle beim Austausch einer Vielzahl von Daten im Web und anderswo.

Standardisierung und Lizensierung

Extensible Markup Language (XML) 1.1 (Second Edition) [2]; based on SGML (ISO 8879) [292][293]

JSON

JSON ist eine leichte, textbasierte, sprachunabhängige Syntax zum Definieren von Datenaustauschformaten. Es wurde von der Programmiersprache ECMAScript abgeleitet, ist jedoch unabhängig von der Programmiersprache. JSON definiert einen kleinen Satz Strukturierungsregeln für die portable Darstellung strukturierter Daten.

Standardisierung und Lizensierung

RFC 8259, ECMA-404; Die JSON-Lizenz [294] [295] [296] [275]

Semantic Sensor Network Ontology

Eine Gruppe, die unter der W3C-Patentrichtlinie tätig ist, hat Semantic Sensor Network Ontology (W3C Recommendation 19 October 2017) entwickelt. Anweisungen zur Offenlegung eines Patents sowie eine Liste aller Patentoffenlegungen, die im Zusammenhang mit den Leistungen der Gruppe gemacht werden, können unter [282] gefunden werden. Dabei muss eine Person, die ein Patent kennt, das sie für wesentlich hält, die in Abschnitt 6 der W3C-Patentrichtlinie vorgeschriebenen Informationen offenlegen. [282]

Standardisierung und Lizensierung

Die W3C-Patentpolitik legt fest, wie Patente im Rahmen der Webstandardsentwicklung behandelt werden. Mit dieser Richtlinie soll gewährleistet werden, dass die im Rahmen dieser Richtlinie erstellten Spezifikationen auf lizenzfreier (RF) Grundlage umgesetzt werden. [283]

USB

USB-Produkte müssen das Verbrauchererlebnis durch hohe Qualität und Benutzerfreundlichkeit weiter verbessern. Aus diesem Grund hat USB-Implementers-Forum, Inc. markenrechtlich geschützte Logos für die Verwendung mit qualifizierten Produkten eingeführt. Um das Recht zu erhalten, das zertifizierte USB-Logo in Verbindung mit einem Produkt anzuzeigen, muss das Produkt die USB-IF-Konformitätsprüfung für Produktqualität bestehen.

Für Nicht-USB-IF-Mitglieder fällt eine Logo-Verwaltungsgebühr in Höhe von 3.500 US-Dollar an, die zusammen mit der unterzeichneten Vereinbarung und einem Anbieter-ID-Formular einzureichen ist, wenn Ihr Unternehmen noch nicht über eine VID verfügt. Für USB-IF-Mitglieder entfällt die Gebühr.

Standardisierung und Lizensierung [306]

Lizenzierung USB 1 bis 4: $ 3.500 bis $ 6.000

Mitgliedschaft: $ 5.000

UDP

Dieses User Datagram Protocol (UDP) ist definiert, um einen Datagrammmodus der paketvermittelten Computerkommunikation in der Umgebung einer miteinander verbundenen Gruppe von Computernetzwerken verfügbar zu machen. Dieses Protokoll geht davon aus, dass das Internet Protocol (IP) [1] als zugrundeliegendes Protokoll verwendet wird.

Dieses Protokoll bietet Anwendungsprogrammen ein Verfahren zum Senden von Nachrichten an andere Programme mit einem Minimum an Protokollmechanismen. Das Protokoll ist transaktionsorientiert und Zustellung und Duplikatschutz sind nicht garantiert. Anwendungen, die eine geordnete zuverlässige Zustellung von Datenströmen erfordern, sollten das Transmission Control Protocol (TCP) [2] verwenden.

Standardisierung und Lizensierung

nein, lizenzfrei

RFC 768 [304]

TCP/IP

TCP ist ein wichtiges Transportschichtprotokoll im Internetprotokollstapel und hat sich im Laufe der jahrzehntelangen Nutzung und des Wachstums des Internets kontinuierlich weiterentwickelt. Im Laufe dieser Zeit wurden eine Reihe von Änderungen an TCP, wie es in Request for Comments (RFC) 793 spezifiziert wurde, vorgenommen, diese wurden jedoch nur bruchstückhaft dokumentiert. Dieses Dokument sammelt und führt diese Änderungen mit der Protokollspezifikation von RFC 793 zusammen. Dieses Dokument ersetzt RFC 793 sowie die RFCs 879, 2873, 6093, 6429, 6528 und 6691, mit denen Teile von RFC 793 aktualisiert wurden. Es aktualisiert die RFCs 1011 und 1122, und es sollte als Ersatz für die Teile dieser Dokumente betrachtet werden, die sich mit TCP-Anforderungen befassen. Außerdem wird RFC 5961 aktualisiert, indem eine kleine Klarstellung bei der Reset-Behandlung im SYN-RECEIVED-Status hinzugefügt wird. Die TCP-Header-Steuerbits von RFC 793 wurden ebenfalls auf Basis von RFC 3168 aktualisiert.

Standardisierung und Lizensierung

nein, lizenzfrei

RFC 9293 [302] / RFC 8200 [303]

UML

Die Object Management Group® Standards Development Organization (OMG® SDO) ist ein globales, offenes, gemeinnütziges Konsortium. Unsere Mitglieder arbeiten zusammen, um Technologiestandards zu entwickeln, die für eine Vielzahl vertikaler Branchen einen messbaren Mehrwert bieten.

Standardisierung und Lizensierung [297][298]

ISO/IEC 19505-1:2012 und ISO/IEC 19505-2:2012

IPR Mode: RF-Limited

SysML

SysML ist eine universelle Modellierungssprache für die Modellierung von Systemen, die einen modellbasierten Systems Engineering (MBSE)-Ansatz für die Entwicklung von Systemen ermöglichen soll. Es bietet die Möglichkeit, Modelle zu erstellen und zu visualisieren, die viele verschiedene Aspekte eines Systems darstellen. Dazu gehört die Darstellung der Anforderungen, der Struktur und des Verhaltens des Systems sowie die Spezifikation von Analysefällen und Verifizierungsfällen, die zur Analyse und Verifizierung des Systems verwendet werden. Die Sprache soll mehrere Methoden und Praktiken des Systems Engineering unterstützen. Die spezifischen Methoden und Praktiken können der Verwendung der Sprache zusätzliche Einschränkungen auferlegen.

Standardisierung und Lizensierung

ISO/IEC 19514:2017

IPR Mode: Non-Assert / Open Source

Referenzen: [299][300]

SensorML

SensorML ist ein Bestandteil der offenen OGC-Suite (Open Geospatial Consortium) und wird unter dem Namen Sensor Web Enablement (SWE) bezeichnet. Tsunami- und Murgangwarnsysteme, Wetter- und Meeresüberwachungssysteme, Systeme zur Überwachung, zum Zugriff und zur Verarbeitung von UAV- und Satellitenbildern/-videos, Innere Sicherheit sowie Verteidigung und Geheimdienst sind nur einige der vielen Anwendungen, die die SWE-Standards auf der ganzen Welt unterstützen. [279]

Standardisierung und Lizensierung

OGC Standard; Lizenzfrei

Referenzen: [280][281]

7.3.4.6 Konvergenz von Betriebs- und Informationstechnologie

OPC UA

OPC UA-Spezifikationen werden von der OPC-Stiftung entwickelt. Diese Gesellschaft wurde gemäß den Gesetzen des Bundesstaates Arizona in den Vereinigten Staaten ins Leben gerufen. [275]

Die OPC Foundation bietet eine Struktur für die Organisation internationaler Kooperationen. Dadurch ist es möglich, dass Anbieter, Nutzende und Konsortien zusammenarbeiten, um Datenübertragungsstandards für eine sichere und verlässliche Interoperabilität in der industriellen Automatisierung sowie für plattformübergreifende Datenübertragungen zu entwickeln. Die OPC Foundation arbeitet mit führenden Standardisierungsorganisationen zusammen, erstellt und pflegt Spezifikationen und stellt sicher, dass die OPC-Spezifikationen durch Zertifizierungstests eingehalten werden. [276]

Die Lizenzvereinbarung der OPC Foundation [277] legt die gesetzlichen Voraussetzungen fest, unter denen Spezifikationen, Software und Zertifizierungen genutzt werden können, die zur Entwicklung und Anwendung von OPC-basierten Produkten benötigt werden. [277]

Die Patensuche mit Patbase unter Verwendung des Suchterms (TAC=(OPC~ UA~)) AND (CC=EP) ergab 170 Ergebnisse.

Abbildung 86: Schlüsselwörter der 170 Ergebnis dargestellt von Patbase [Patbase-Software]

Standardisierung und Lizensierung

OPC UA wurde als Normenreihe IEC 62541 veröffentlicht.

Referenzen: [276][277][278]

MQTT

Die Patentsuche mit Patbase unter Verwendung des Suchterms (TAC=(MQTT~)) AND (CC=EP) ergab 151 Ergebnisse.

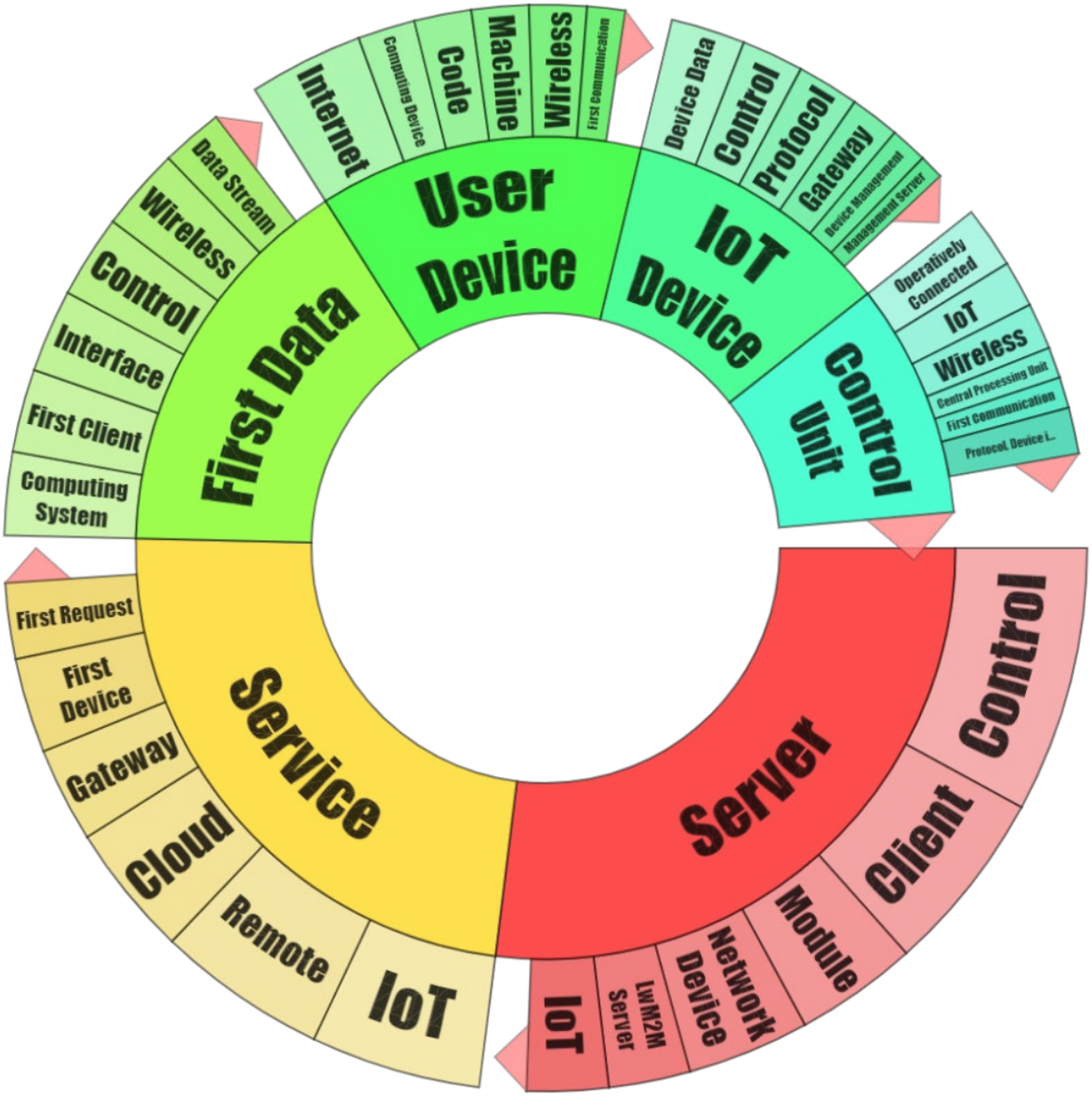


Abbildung 87: Schlüsselwörter der 151 Ergebnisse dargestellt von Patbase [Patbase-Software]

Standardisierung und Lizensierung

MQTT ist ein OASIS-Standard. Die Spezifikation wird vom OASIS MQTT Technical Committee verwaltet. [272]

Der „Non-Assertion Mode“ der OASIS-IPR-Richtlinie, der bei der Gründung des Technischen Komitees ausgewählte Modus, stellt diese Spezifikation zur Verfügung. Es gibt Informationsangebote zu Patentlizenzbedingungen und Informationen darüber, ob Patente offengelegt wurden, die für die Umsetzung dieser Spezifikation wesentlich sein könnten, auf der TC-Website. [273][274]

8 Bestandsaufnahme – Datensicherheit und Risikoanalyse, Cybersecurity

Innerhalb dieses Kapitels wird zunächst eine Recherche und Bestandsaufnahme zu relevanten Aspekten der Cybersecurity erstellt. Das Ziel dabei ist es zum einen vorhandene bahnspezifische Quellen zu identifizieren und zu analysieren und zum anderen Quellen aus verwandten Bereichen wie Industrie 4.0, IoT oder Mobilität mit Bezug zu Datensicherheit und Cybersecurity zu sammeln. Es erfolgte jeweils eine Durchsicht der Quellen und Aufbereitung der relevanten Inhalte. Diese Sammlung wird, während der Auseinandersetzung mit den Use Cases, weiter ergänzt.

Weiterhin wurde zur Vorbereitung der Arbeiten im zweiten Unterkapitel die Erarbeitung der Use Cases und der erste Workshop mit Stakeholdern begleitet. Eine wichtige Voraussetzung innerhalb der Arbeiten dieses Kapitels ist der fruchtbare Austausch innerhalb des Projektkonsortiums.

8.1 Recherche und Bestandsaufnahme

In diesem Unterkapitel soll zunächst systematisch eine Sammlung verschiedenster Publikationen zum Thema Cybersecurity zusammengestellt werden. Diese soll im weiteren Verlauf des Projekts die Grundlage der Bestandsaufnahme und der Risikoanalyse in Unterkapitel 8.2 bieten. Im weiteren Verlauf des Projekts wird die Recherche und Bestandsaufnahme auf Basis der Use Cases und Technologien, die in Kapitel 8.2 näher untersucht werden, ergänzt.

In einer ersten Bestandsaufnahme sollen bereits identifizierte Herausforderungen, Gefahren, Angriffsszenarien und Maßnahmen erfasst werden. Vergleichbare Risiken und Bewertungen sollen identifiziert werden. Dabei werden zum einen bahnspezifische Dokumente untersucht und zum anderen Dokumente aus verwandten Bereichen. Hierbei werden insbesondere die Bereiche IoT, Industrie 4.0 und Mobilität betrachtet und Dokumente zu Security von öffentlichen Einrichtungen, Branchenverbänden und anderen relevanten Akteuren untersucht.

Es sollen als wichtiger Kontext potenziell zukünftig eingesetzte Systemarchitekturen im Bahnumfeld identifiziert werden, um ein genaueres Verständnis für diese Systeme, auch im Hinblick auf Sensoren und ihre Schnittstellen, zu erhalten. Der Fokus liegt dabei auf Systemen am Zug und weniger auf Systemen zur Zug-Strecke-Kommunikation (Train-to-Ground) oder Systemen in Rechenzentren, um besonders bahnspezifische Aspekte zu fokussieren. Zusätzlich sollen die identifizierten Ansätze auf umgesetzte Sicherheitskonzepte und -strategien untersucht werden.

Zur Identifikation von relevanten Projekten und Dokumenten aus dem Bahnumfeld waren als Ausgangspunkt Hinweise von Expertinnen und Experten und der Austausch im Projekt wichtig. Hier sind besonders Dokumente aus Projekten zu nennen, in denen zukünftige Bahnarchitekturen sowohl im Personen-, als auch im Güterverkehr entwickelt werden und Dokumente aus Arbeitskreisen. Diese lassen sich in Systeme für den Personenverkehr und den Güterverkehr unterteilen. Betrachtet wurden die CONNECTA Projekte CONNECTA-1[5] [309][317], CONNECTA-2[6] [308][310][315][316] und CONNECTA-

[5]Weitere Informationen sind unter https://cordis.europa.eu/project/id/730539 zu finden.

[6]Weitere Informationen sind unter https://cordis.europa.eu/project/id/826098 zu finden.

3[7] [318] im Personenverkehr, die auf eine Modernisierung der TCMS Architekturen, sowie Forschung hinsichtlich neuer technologischer Konzepte und Standards abzielen. Im Güterverkehr wurden die ITSS (Industrieplattform für Telematik und Sensorik im Schienengüterverkehr) [311][312][313] des TIS[8] (Technischer Innovationskreis Schienengüterverkehr) und die Studie „Erstellung eines Konzeptes für die EU-weite Migration eines Digitalen Automatischen Kupplungssystems (DAK) für den Schienengüterverkehr – Fachbericht Identifikation von Standards bei der Strom-/Datenversorgung“, erstellt durch die OWITA GmbH [65], untersucht. Die Auswahl der betrachteten Projekte, Arbeitskreise und Quellen wurde ergänzend durch die im Projekt durchgeführten Interviews mit Expertinnen und Experten verifiziert. Im Rahmen der Recherche wurden insbesondere für die Arbeiten in Kapitel 7 und 8 Informationen über die jeweils spezifischen Sichten auf Quellen ausgetauscht.

Die Dokumente sollen auf verwendete Kommunikationstechnologien und -standards, Architekturkonzepte, Netzwerke und Topologien, Protokolle, Schnittstellen und Technologien untersucht werden. Außerdem sind geplante IT-Sicherheitsansätze bzw. Maßnahmen sowie Angriffsmodelle und identifizierte Angriffsziele von Interesse.

8.1.1 Recherche

Zunächst soll eine Bestandsaufnahme zu relevanten Aspekten der Cybersecurity erstellt werden. Zur allgemeinen, bahnübergreifenden Recherche zum Thema Cybersecurity wurden die Publikationen der Agentur der Europäischen Union für Cybersicherheit (ENISA), dem Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom) sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des BMDV herangezogen. Es wurde kein expliziter Untersuchungszeitraum festgelegt.

Ziel ist es, vorhandene bahnspezifische und Quellen aus verwandten Bereichen wie Industrie 4.0, IoT und Mobilität mit Bezug zu Datensicherheit und Cybersecurity zu identifizieren und zu sammeln, um von den Fortschritten in vergleichbaren Bereichen zu profitieren.

Auf der Website der ENISA wurden daher die Filter *by Topics IoT and Smart Infrastructures* und *by Topics Critical Infrastructures and Services* angewendet. Zudem sind alle Publikationen aufgenommen worden, die unter den Tags *Threat landscape*, *Internet of things*, *Smart Cars*, *Smart Cities*, *Rail*, *Railway*, *Industry 4.0* und *IoT* gelistet sind. Von Bitkom wurden alle Publikationen in deren Mediathek zum Thema *Datenschutz & Sicherheit* gesammelt. Zusätzlich wurden alle Publikation der Mitre Corporation, ein gemeinnütziges Forschungs- und Entwicklungszentrum in den Vereinigten Staaten, zu Cybersecurity und Computer Security aufgenommen. Des Weiteren wurden über die Datenbank Perinorm[9] alle DIN-Normen der Klassifikation ICS 35.030 (Informationstechnik, IT-Sicherheit) gesammelt.

Für eine konkretere Recherche wurden nach Hinweisen innerhalb des Konsortiums die Dateien der CONNECTA Projekte des Projekts *Shift2rail* sowie ITSS des Technischen Innovationskreis Schienengüterverkehr (TIS) ebenfalls in die Recherche integriert, um auch bahnspezifische Dokumente zu betrachten.

[7]Weitere Informationen sind unter https://cordis.europa.eu/project/id/101014811 zu finden.

[8]Weitere Informationen sind unter https://tis.ag zu finden.

[9]Weitere Informationen sind unter https://dbis.ur.de zu finden.

Zur weiteren Unterteilung der in die Sammlung aufgenommenen Dateien, werden alle Publikationen in einer Tabelle zusammengefasst und jeweils in eine von vier Kategorien einsortiert: *bahnspezifisch*, *vergleichbar*, *allgemein*, *anderes* (siehe Tabelle 72). Die vollständige Sammlung und Einteilung ist in Anlage B zu finden.

Tabelle 72: Beispielhafter Auszug aus der Tabelle zur Sammlung und Einteilung von Publikationen im Bereich Cybersecurity

Publikation	Einteilung
ENISA	
Lévy-Bencheton, C.; Darra, E. (2015): Cybersecurity and Resilience of Intelligent Public Transport – Good practices and recommendations, ENISA. Verfügbar unter: https://www.enisa.europa.eu/publications/good-practices-recommendations	Bahnspezifisch (Intelligent Public Transport)
Liveri, D.; Drougkas, A.; Zisi, A. (2021): Cloud Security for Healthcare Services. (2021) Verfügbar unter: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services	Andere
ENISA (2019): ENISA Good practices for security of smart cars, ENISA, DOI 10.2824/17802, Verfügbar unter: https://www.enisa.europa.eu/publications/smart-cars	Verwandt/Vergleichbar (Mobilität)
Bitkom	
Bitkom (2018): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Verfügbar unter: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf	Allgemein
MITRE	
Strom, B.; Battaglia, J.; Kemmerer, M.; Kupersanin, W.; Miller, D.; Wampler, C.; Whitley, S.; Wolf, R. (2017): Finding Cyber Threats with ATT&CK™-Based Analytics.	Allgemein
Folk, C.; Hurley, D.; Kaplow, W.; Payne, J. (2015) The security implications of the internet of things.	Verwandt/Vergleichbar (IoT)

Bahnspezifisch umfasst alle Dateien, die sich mit Schienenverkehr bzw. öffentlichem Personenverkehr oder Schienengüterverkehr befassen. *Vergleichbar* sind alle Dateien, die sich in Bereiche wie bspw. IoT, Industrie 4.0 oder Mobilität einordnen lassen. *Allgemein* sind generell für das Thema Security möglicherweise relevante Dateien, die sich nicht konkret auf Schienenverkehr oder vergleichbare Gebiete beziehen, wie bspw. verschiedene Methoden der Cybersecurity oder Threat Landscapes. Unter der vierten Kategorie *anderes/other* werden alle übrigen Dateien einsortiert, die für dieses Projekt nicht von Relevanz sind, wie z. B. Darstellungen zu Security-Maßnahmen mit dem Fokus auf klassische IT-Architekturen.

Zusätzlich zur Literatursammlung wurden Hinweise aus dem Konsortium zu bestehenden Projekten und Stakeholdern aufbereitet und auf Basis dessen nach weiteren verwandten Projekten zum Thema Cybersecurity im Schienenverkehr und der Mobilität allgemein gesucht. Als relevant identifizierte Projekte sind in Abbildung 88 und Abbildung 89 dargestellt. Dazu gehört der Arbeitskreis zum Projekt IT-Sicherheit des Center for Transportation & Logistics Neuer Adler e. V. (CNA) und Arbeitsgruppe Cybersecurity für sicherheitskritische Infrastrukturen (CYSIS) der Deutschen Bahn. Die Projekte des Shift2Rail der Europe‘s Rail bieten ebenfalls viele Anhaltspunkte. So sind auch die CONNECTA-Projekte, die im Weiteren beispielhaft näher betrachtet werden, ein Projekt des Shift2Rail. Projekte, die sich mit Cybersecurity im Bahnbereich befassen, konnten im Innovation Programme 2 identifiziert werden, wie Cybersecurity in the RAILway sector (CYRail=, X2Rail-3 and 4SECURail.

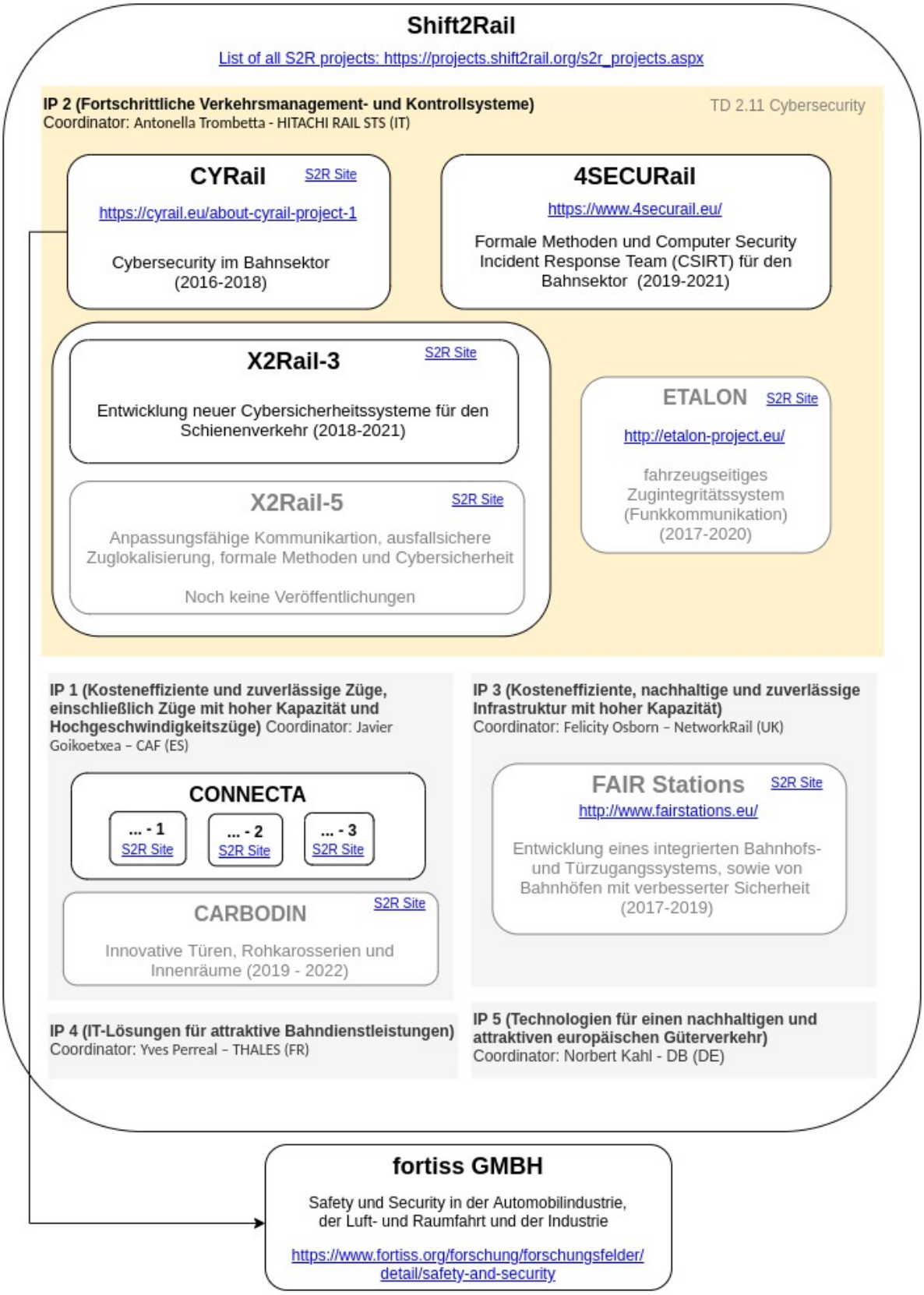


Abbildung 88: Relevante Projekte des Shift2Rail [Institut für Information Engineering, Ostfalia Hochschule]

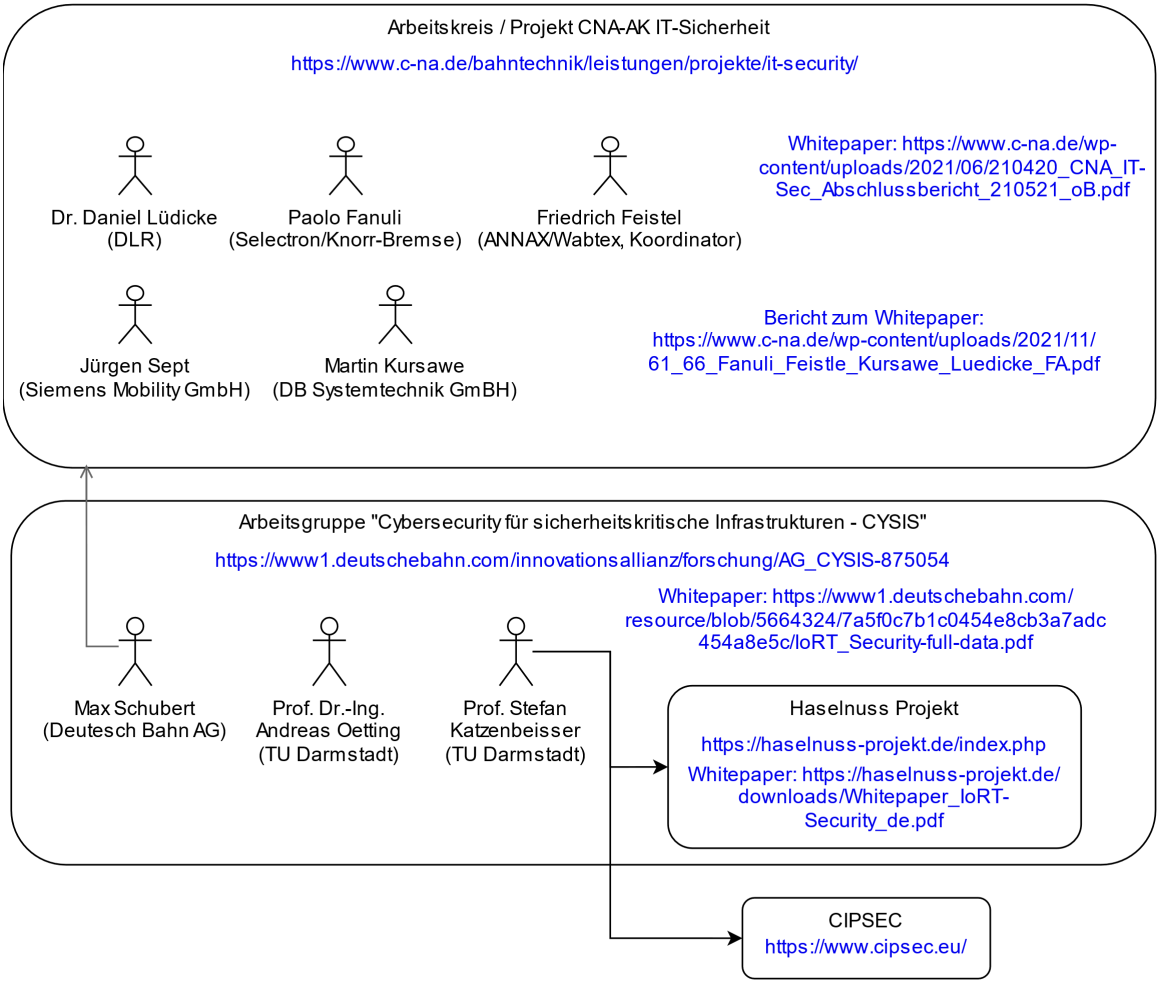


Abbildung 89: Relevante Arbeitsgruppen zu Security [Institut für Information Engineering, Ostfalia Hochschule]

8.1.2 Herausforderungen

Die ENISA hat im Schienenverkehr und im Bereich des intelligenten Nahverkehrs Herausforderungen identifiziert, die Cybersecurity in diesen Bereichen einschränken, erschweren oder verlangsamen. [320][321] Diese können zusammengefasst werden als:

1. Funktionale Sicherheit (Safety) sowie Effizienz, und Cybersecurity müssen in Einklang gebracht werden. Wobei die Wichtigkeit von Cybersecurity oftmals unterschätzt wird, sodass zu wenig Aufwände in Analysen und Gegenmaßnahmen investiert werden. Zudem ist das Bewusstsein für Sicherheitsrisiken zu gering.

2. Die Vorschriften und Regularien zu Cybersecurity sind komplex oder unzureichend. Es fehlt an der Integration von Richtlinien, einheitlichen Definitionen, unabhängigen Analyse- und Risikobewertungswerkzeugen, formalisierter Sicherheitspolitik und Standards.

3. Abhängigkeiten von Lieferketten und Lieferanten mit unterschiedlichen technischen Standards und Cybersicherheitskapazitäten führen zu weiteren Risiken. Zudem bleiben sie sehr lange im Einsatz durch die lange Lebensdauer.

Ähnliche Beobachtungen konnte die Studie „Security und geplanter Technologieeinsatz“ [322] mit Onlinebefragungen und darauf aufbauenden Interviews im Eisenbahnsektor feststellen. Hier wurden das mangelnde Bewusstsein für Cybersecurity sowohl des Managements als auch der Mitarbeitenden, die geringe Unterstützung von Behörden, die hohe Abhängigkeit von Lieferfirmen und herstellenden Unternehmen sowie das Abstellen von Support und Updates älterer Produkte als Schwächen im Eisenbahnsektor genannt.

8.1.3 Bedrohungen, Angriffsszenarien und Maßnahmen

Der Schienenverkehr ist, vergleichbar zu den meisten ähnlich gelagerten Systemen, potenziell gefährdet durch unbeabsichtigte Schäden (z. B. durch Bediener- und Benutzerfehler), Insider-Bedrohungen, bösartige Handlungen oder Missbrauch (wie Distributed Denial of Service (DDos)-Attacken, Manipulationen, Malware etc.), physische und groß angelegte Angriffe, Naturkatastrophen oder Umweltereignisse, Fehlfunktionen, Unterbrechungen oder Ausfälle [320][323]. Eine Übersicht über die Gefahren im Bahnverkehr, wie sie die ENISA [323] zusammengestellt hat, ist in Tabelle 73 zu sehen.

TABELLE 73: BEDROHUNGSTAXONOMIE (THREAT TAXONOMY) VON ENISA [323]

Böswillige Aktivitäten / Missbrauch
• Identitätsdiebstahl/Identitätsbetrug • Unerbetene E-Mail • Denial of Service • Schadhafter Code / schadhafte Software/Aktivitäten • Social Engineering • Erstellung und Verwendung von gefälschten Zertifikaten • Manipulation von Hardware und Software • Manipulation von Informationen • Betrug durch autorisiertes Personal • Unbefugte Nutzung oder Verwaltung von Geräten und Systemen • Network Intrusion • Unbefugte Installation von Software • Kompromittierung vertraulicher Informationen (Datenschutzverletzungen) • Brute Force • Missbrauch von Berechtigungen • Abfangen von Informationen • Netzwerkausspähung, Manipulation des Netzwerkverkehrs und Informationsbeschaffung • Man in the Middle/Sitzungsmanipulation
(vorsätzlicher) physischer Angriff
• Betrug durch Passagiere • Sabotage/Vandalismus • Diebstahl (Geräte, Speichermedien und Dokumente) • Durchsickern/Weitergabe von Informationen aus Dokumenten/Geräten • Unbefugter physischer Zugang / unbefugtes Betreten von Räumlichkeiten • Nötigung, Erpressung, Korruption • Terroristen-/Hacktivistenangriff/Kriegsschäden
Natur- und Umweltkatastrophen
• Natürliche Erdbeben, Überschwemmungen, Erdrutsche, Tsunamis, starke Regenfälle, starke Schneefälle, starke Winde, Sonneneruptionen, Blitzschlag, Verschmutzung, Staub, Korrosion, Wasser, Explosion, Schäden durch Tiere
Systemabstürze / Störungen und Fehlfunktionen
• Von Geräten oder Systemen

• Von Kommunikationsverbindungen • Von Dienstleistern (Lieferketten)
Ausfälle
• Verlust von Ressourcen • Stromausfall • Ausfall der Kühlung • Verlust von Öl und Gas • Ausfall von Personal (Streik, Pandemie, usw.) • Geringe Kompetenz des Personals • Internetausfall • Ausfall mobiler Kommunikation • Netzwerkausfall
Unbeabsichtigte Schäden/Verlust von Informationen oder IT-Assets
• Informationsverluste / Weitergabe von Informationen aufgrund von menschlichem Versagen • Fehlerhafte Verwendung oder Beschädigung von Geräten und Systemen • Verwendung von Informationen aus einer unzuverlässigen Quelle • Unzureichende Konzeption und Planung oder unsachgemäße Anpassung • Schäden, die durch einen Dritten (Lieferant oder Partner) verursacht werden • Schäden infolge von Penetrationstests • Verlust (der Integrität) sensibler Informationen • Zerstörung von Datensätzen

Im Schienenverkehr hat die ENISA zudem sieben Angriffsszenarien genauer spezifiziert [323]:

1. Kompromittierung von Signalen oder Steuerungssystemen, was zu einem Zugunfall führt.
2. Sabotage der Verkehrsüberwachungssysteme, die zu einer Unterbrechung des Zugverkehrs führt.
3. Ransomware-Angriff, der zu einer Unterbrechung des Betriebs führt.
4. Diebstahl von persönlichen Kundendaten aus dem Buchungsmanagementsystem.
5. Eine Datenpanne sensibler Daten aufgrund einer unsicheren, ungeschützten Datenbank.
6. Distributed Denial of Service (DDoS)-Angriff, der Reisende am Kauf von Fahrkarten hindert.
7. Katastrophenereignis, das die Einrichtung des Rechenzentrums zerstört und zu einer Unterbrechung der IT-Dienste führt.

Die Szenarien wurden auf ihren Ablauf, ihren Einfluss und die betroffenen Systeme untersucht. Zudem wurden zugehörige generelle und konkrete Sicherheitsmaßnahmen identifiziert und gelistet [323]. Weitere vergleichbare Szenarien aus dem Bereich der Mobilität, die genauer untersucht wurden, sind der großflächige Einsatz von schadhafter Firmware über die Backend-Server der Gerätehersteller, Sendung falscher Informationen zwischen Fahrzeugen durch ein anderes übernommenes Fahrzeug und die Täuschung von Sensoren durch Störungen [324].

Als Basis oder zur Unterstützung, um konkrete Cybersecurity Maßnahmen zu definieren, hat die ENISA generalisierte Maßnahmen erfasst und diese den Maßnahmen aus den Standards ISO/IEC 27002 und CLC/TS 50701 sowie des National Institute of Standards and Technology (NIST) Cybersecurity Frameworks zugeordnet. Dabei wurden die Maßnahmen vier Domainen zugeordnet: Governance (Steuerung), Protection (Absicherung), Defense (Abwehr) und Resilience (Resilienz), die in Tabelle 74 detailliert werden.

TABELLE 74: GENERALISIERTE MAßNAHMEN ZU CYBERSECURITY [323]

Governance	Absicherung	Abwehr	Resilienz
Risikoanalyse	Systemkonfiguration	Erkennung	Betriebskontinuitäts-management
Sicherheitspolitik	Systemabgrenzung	Protokollierung	Wiederherstellung im Katastrophenfall
Sicherheitsakkreditierung	Filterung des Datenverkehrs	Protokollanalyse	Organisation des Krisenmanagements
Sicherheit der menschlichen Ressource	Verwaltungsinformations-system	Kommunikation mit den zuständigen Behörden	
Abbildung des Ökosystems	Authentifizierung und Identifizierung		
Beziehungen des Ökosystems	Zugriffsrechte		
	Verfahren zu Wartung der IT-Security		
	Physische und umgebungsbezogene Sicherheit		

In Bezug auf intelligente Fahrzeuge wurden weitere Gefahren genannt, die sich auch auf den Schienenverkehr übertragen lassen können. Beispiele für ein Denial of Service sind die Beeinträchtigung oder Abschaltung der Schnittstelle zur drahtlosen Kommunikation zwischen straßenseitiger Infrastruktur und Onboard Units, die Überlastung des Systems oder der fahrzeuginternen Kommunikation sowie die Störung des Funkverkehrs. Schädliche Manipulationen könnten z. B. Veränderungen von Kartendaten, gefälschte Sicherheitsinformationen oder -nachrichten und die Injektion von Daten über den CAN Bus sein.

Innerhalb der untersuchten Dokumente der ENISA oder darin referenzierter Darstellungen aus Projekten wie CYRail wird als generelle Vorgehensweise ein Risikomanagement basierend auf ISO/IEC 31000 vorgeschlagen. Damit wird insgesamt festgestellt, dass Cybersecurity kein Zustand ist, den man erreichen kann, sondern ein Prozess, der den gesamten Lebenszyklus eines bahnspezifischen Service begleiten muss. Dabei werden Schutzziele, Bedrohungen, Angriffsszenarien und potenzielle Schäden untersucht und innerhalb des Risikomanagements auf etablierte Methoden wie bspw. Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE)[10], ein Threat Modelling Ansatz von Microsoft, und Maßnahmen verwiesen. Diese Methoden und deren Anwendbarkeit im Bahnsektor werden im Kontext der Anwendungsfälle im weiteren Projektablauf untersucht.

Nach dieser übergreifenden Analyse werden in den folgenden Abschnitten spezifische Ansätze aus dem Bahnsektor basierend auf Dokumenten aus dem Personenverkehr wie bspw. dem CONNECTA Projekt und dem Schienengüterverkehr insbesondere der DAK-Studien untersucht.

[10] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

8.1.4 Kommunikationstechnologien, Netzwerke und Topologien

Zu Beginn des Kapitels erfolgt eine Übersicht über die recherchierten Ergebnisse. Tabelle 75 zeigt die Kommunikationstechnologien im Schienenpersonenverkehr (SPV) und Tabelle 76 die entsprechenden im Schienengüterverkehr (SGV).

TABELLE 75: KOMMUNIKATIONSTECHNOLOGIEN IM SCHIENENPERSONENVERKEHR

Einordnung	Bezeichnung	Erläuterung
CONNECTA	NG-TCN/Drive by-Data	Übergreifende Bezeichnung für neue Netzwerkarchitektur, umfasst ECN, ETB, ETBN, WLTB, WLCN, MCG
	ECN	Ethernet-Ring innerhalb eines Consists
	ETB(-L/R)	Redundante Ethernetleitungen zwischen Consists
	ETBN	Router/Managed switch, Brücke zwischen ECN/ETB, sowie zwischen mehreren Consists
	WLTB	Wireless-Alternative zum ETBN, evtl. basierend auf LTE release 14 und 5G
	WLCN	Wireless-Alternative zum ECN, basierend auf WLAN
	MCG	Train-to-Ground-Kommunikation (Mobilfunk oder WLAN)
TCN (Train Communication Network)	TCN (IEC 61375)	Übergreifende Bezeichnung für alte/aktuelle Netzwerkarchitektur, u. a. basierend auf WTB, MVB, CANopen
	WTB	Bussystem zwischen Fahrzeugen
	MVB	Bussystem innerhalb eines Fahrzeugs/Consists
	CANopen	Kommunikationsstandard basierend auf CAN, innerhalb eines Consists

TABELLE 76: KOMMUNIKATIONSTECHNOLOGIEN IM SCHIENENGÜTERVERKEHR

Einordnung	Bezeichnung	Erläuterung
ITSS (Industrieplattform für Telematik und Sensorik im Schienengüterverkehr)	ITSS Schnittstelle 1	Internetbasierte Kommunikation zwischen Server des Telematikbetriebs und verarbeitenden Servern
	ITSS Schnittstelle 2	Kommunikation zwischen Sensoren und Telematikeinheit am Güterwagen (Kabel oder Funk)
	ITSS Schnittstelle 3	Kommunikation zwischen Handheld-Gerät und Telematikeinheit am Güterwagen
	ITSS Schnittstelle 4	Intrazug-Kommunikation zwischen Wagen und Triebfahrzeug

Einordnung	Bezeichnung	Erläuterung
DAK-Studie OWITA GmbH	Topologie-Alternative: Segmentierte Bussysteme	Evaluation: Topologie-Alternative, bei der kabelgebunden kommuniziert wird, die Nachrichten aber über separate Kommunikationsknoten weitergeleitet werden
	Topologie-Alternative: Segmentierte Bussysteme mit Technologiewechsel	Evaluation: Topologie-Alternative, bei der innerhalb eines Wagens ein kabelgebundenes Bussystem, an der Kuppelstelle aber ein Funksystem zum Einsatz kommt
	Topologie-Alternative: Durchgehende Leitung	Evaluation: Topologie-Alternative, bei der eine durchgehende Leitung über den gesamten Zug, ohne Trennung durch Kommunikationsknoten, eingesetzt wird
	Systemkonzept: Segmentiertes CAN/CAN-FD	Evaluation: Vorgeschlagenes Systemkonzept basierend auf dem CAN-FD Bussystem (segmentiertes Bussystem)
	Systemkonzept: Powerline PLUS	Evaluation: Vorgeschlagenes Systemkonzept basierend auf Powerline PLUS (Durchgehende Leitung)
	Systemkonzept: WLAN/Ethernet	Evaluation: Vorgeschlagenes Systemkonzept basierend auf WLAN und Ethernet (segmentiertes System mit Technologiewechsel)

Zum Personenverkehr werden hier zunächst die CONNECTA Projekte betrachtet. Im Rahmen des CONNECTA Projekts wird das NG-TCN (Next-Generation Train Communication Network), auch „Drive-by-Data“-Architektur, als Weiterentwicklung des TCN (IEC 61375) beschrieben [308]. Letzteres wird bereits heute in Zügen des Personenverkehrs eingesetzt. Im Folgenden werden grundlegende Aspekte zu Netzwerken, Technologien und Topologien aus diesen Systemarchitekturen zusammengefasst.

Das NG-TCN beinhaltet zwei grundlegende Netzwerke: Das ECN (Ethernet Consist Network), das innerhalb eines Consists (Verbund mehrerer Fahrzeuge) verwendet wird, sowie der ETB (Ethernet Train Backbone), der mehrere Consists verbindet und ein übergreifendes Netzwerk pro Zug darstellt.

Während das ECN auf eine Ringtopologie mit statischer Konfiguration (d. h. es erfolgt keine Änderung während des Betriebs) setzt, besteht das ETB aus zwei getrennten Ethernet-Leitungen (ETB-L/ETB-R), um Redundanz zu ermöglichen und erlaubt dynamische Änderungen innerhalb des Netzwerks durch das Hinzufügen oder Abtrennen von Consists.

Der ETBN (Ethernet train backbone node, router/managed switch) stellt die Verbindung zwischen Consists sowie eine Brücke zwischen ECN und ETB dar. Als Wireless-Alternative zum ETB wird der WLTB (Wireless Train Backbone) genannt, der bspw. auf LTE release 14 und 5G basieren könnte [309]. Ähnlich existiert auch eine Alternative zum ECN, das Wireless Consist Network (WLCN), basierend auf WLAN [310]. Das Mobile Communication Gateway (MCG) stellt eine weitere Schnittstelle dar, die ebenfalls auf Mobilfunk bzw. WLAN aufsetzt und die Train-to-Ground Kommunikation ermöglicht [308]. Bisherige Technologien im TCN setzten verstärkt auch auf Busse, wie WTB (Wire Train Bus) zur Intrazugkommunikation sowie MVB (Multifunction Vehicle Bus) und CANopen als Consist-Netzwerk.

Während im Bereich des Personenverkehrs bereits komplexe Netzwerke eingesetzt werden, setzte man im Güterverkehr lange auf Telematiklösungen einzelner Hersteller pro Wagen. Konventionelle Güterzüge sind meist nicht mit Möglichkeiten zur Datenkommunikation, oder überhaupt einer elektrischen Energieversorgung, ausgestattet [311]. Stattdessen setzen aktuelle Telematiklösungen auf Batterien sowie Kommunikation über Mobilfunk und sind meist an einen Güterwagen gebunden, da Güterzüge aus Güterwagen einer Vielzahl von Betreibern bestehen und häufig neu zusammengesetzt werden. Eine Interoperabilität und Zusammenwirken unterschiedlicher Telematikkomponenten eines Güterzugs ist für die Zukunft in Aussicht.

Die ITSS des TIS standardisiert vier Schnittstellen zur Unterstützung verschiedener Telematik-Anwendungsfälle. *Schnittstelle 1* umfasst die internetbasierte Kommunikation zwischen dem Server des Telematikbetriebs und verarbeitenden Servern bspw. für Enterprise-Resource-Planning (ERP), Logistik und Instandhaltung. *Schnittstelle 2* spezifiziert die Kommunikation zwischen Sensoren und der Telematikeinheit am Güterwagen, per Kabel oder Funk, wobei 2.4 GHz, basierend auf dem Standard IEEE 802.15.4, genannt wird. *Schnittstelle 3* beschreibt die Verbindung zwischen einem Handheld-Gerät und der Telematikeinheit am Güterwagen, bspw. zur Diagnose. Die Intrazug-Kommunikation zwischen Wagen und der Lok wird durch *Schnittstelle 4* beschrieben. Hierbei ist aktuell der CAN-Bus (als Alternativen werden Ethernet/Powerline/andere genannt) als Übertragungstechnologie vorgesehen. [311]

Für zeitkritische/sicherheitsrelevante Kommunikation wird eine direkte Übertragung per Funk oder kabelgebunden empfohlen. Anderenfalls kann auch ein Server als Zwischenstelle innerhalb der Kommunikation eingesetzt werden und der Abruf über Mobilfunk und ein Handheldgerät durch die Triebfahrzeugführung erfolgen. Während *Schnittstelle 1* bereits größtenteils spezifiziert ist [312], existiert für *Schnittstelle 2* bisher nur eine nicht-öffentliche „Lite"-Version[11], sowie eine öffentliche Spezifikation von Anwendungsprofilen für verschiedene Anwendungsfälle [313]. Für *Schnittstellen 3 und 4* wurden bisher keine spezifischeren Dokumente veröffentlicht[5]. In der DAK-Studie der OWITA GmbH wurden einige Kommunikationstechnologien hinsichtlich verschiedener Faktoren evaluiert [65]. Der Fokus lag dabei auf der Intrazugkommunikation. Unter den evaluierten Topologien fanden sich segmentierte Bussysteme, segmentierte Bussysteme mit Technologiewechsel sowie Systeme mit durchgehender Leitung. Im Vordergrund standen zuletzt vor allem segmentiertes CAN bzw. Controller Area Network Flexible Data Rate (CAN-FD) sowie Powerline PLUS, Single Pair Ethernet (IEEE 802.3cg) und 2.4 GHz WLAN (IEEE 802.11 b/g). Weiterhin werden fahrzeuginterne Busse genannt, wie z. B. der Interne Kommunikationsbus (Internal Communication Bus) des Triebfahrzeugs.

[11]Für weitere Informationen siehe https://tis.ag/downloads/ (abgerufen am 12.09.2022).

8.1.5 Protokolle und Schnittstellen

Zu Beginn des Kapitels erfolgt eine Übersicht über die recherchierten Ergebnisse. Tabelle 77 stellt die Protokolle und Schnittstellen im SPV und Tabelle 78 im SGV dar.

TABELLE 77: PROTOKOLLE UND SCHNITTSTELLEN IM SCHIENENPERSONENVERKEHR

Einordnung	Bezeichnung	Erläuterung
CONNECTA	IP, ICMP, UDP, TCP, SNMP	Standard-Protokolle im Internet, die auch im Ethernet-basierten NG-TCN eingesetzt werden
	MACsec (IEEE 802.1AE)	Standard zur Authentifizierung und Verschlüsselung auf der Sicherungsschicht, auch für das NG-TCN als Sicherheitsmaßnahme vorgeschlagen
	PNAC (IEEE 802.1X)	Standard zur port-basierten Netzwerkzugriffskontrolle
	TRDP	Protokoll zur Echtzeitkommunikation in Zügen, basierend auf UDP oder optional TCP
	SDTv4	Aktualisiertes Protokoll zur abgesicherten Kommunikation (Safety) bis SIL 4
	OPC UA	Umfassende Service-orientierte Architektur zum Datenaustausch inkl. semantischer Beschreibung; könnte innerhalb eines Consists zum Einsatz kommen
	Clock Synchronization (IEEE 802.1AS-rev & IEEE 1588v2)	Standard zur Synchronisation in Zeit-sensitiven Anwendungen
	Time-Sensitive Networking (IEEE 802.1Qbv)	Standard für Scheduling innerhalb von zeitkritischen Netzwerken
	Functional Distribution Framework (FDF) API	Schnittstellen des Functional Distribution Frameworks, einer Middleware auf der verschiedene zugbezogene Anwendungen aufbauen sollen
	Functional Open Coupling (FOC)	Schnittstellen zum Datenaustausch zwischen mehreren heterogenen Consists
	Application Profiles	Anwendungsprofile, die Eigenschaften und Schnittstellen verschiedener zugspezifischer Anwendungen in SysML beschreiben, bspw. HVAC oder das Türsystem
	Functional Telegrams	Nachrichten zum Austausch verschiedener Systeme beim FOC bzw. FDF

TABELLE 78: PROTOKOLLE UND SCHNITTSTELLEN IM SCHIENENGÜTERVERKEHR

Einordnung	Bezeichnung	Erläuterung
ITSS	ITSS Schnittstelle 1	Schnittstelle für Server-zu-Server-Datenaustausch über eine REST-Architektur unter Nutzung von HTTPS mit JSON-Schema; Verwendung sowohl ereignisbasierter Benachrichtigungen (Push), als auch Request/Response-Kommunikation
	ITSS Schnittstelle 2	Schnittstelle zwischen Sensoren und Telematikeinheit am Güterwagen, bei der ein eigenes binäres Protokoll genutzt wird. Verschiedene Anwendungsfälle sind durch vordefinierte Anwendungsprofile abgedeckt, bspw. „Valve State“ (Ventilzustand)
	TLS	Standard-Protokoll zur sicheren Kommunikation (Security), inkl. Schlüsselaustausch, Sicherstellung der Authentizität, Vertraulichkeit und Integrität; vorgeschlagen zur Nutzung innerhalb des Güterzugs, bei Verwendung von TCP/IP

Bei CONNECTA kommen auf den mittleren Schichten des OSI-Modells Standardprotokolle zum Einsatz, die auch im Internet Verwendung finden, wie IP, Internet Control Message Protocol (ICMP), UDP und TCP [308]. Auf der Vermittlungsschicht wurde zudem Internet Protocol Security (IPsec) zur Sicherung der Vertraulichkeit, Integrität und Authentizität genannt. Diese Empfehlung wurde jedoch wieder verworfen, da IPsec kein Multicast unterstützt [[308], S. 134]. Stattdessen wird Media Access Control Security (MACsec) (IEEE 802.1AE) auf der Sicherungsschicht in Verbindung mit Port Based Network Access Control (PNAC), IEEE 802.1X) empfohlen. Aufgrund der dabei entstehenden Kosten wird der Einsatz laut CONNECTA lediglich in Bereichen empfohlen, in denen es das Sicherheitslevel signifikant erhöht. Dabei werden als Beispiel Closed Circuit Television (CCTV)-Systeme (Videoüberwachungsanlagen) im Reisendenabteil genannt [[308], S. 126]. Es wird sich zeigen, inwiefern das Vorhandensein zahlreicher offener Implementierungen die Kosten ggf. gegenüber CAN-basierten Systemen oder proprietären Lösungen reduzieren können.

In den höheren Schichten des OSI-Modells kommen Protokolle wie Simple Network Management Protocol (SNMP), Train Real Time Data Protocol (TRDP) und Safe Data Transmission (SDTv4) zum Einsatz [[308], S. 46]. Letzteres kann z. B. auf dem TRDP aufbauen und ermöglicht eine abgesicherte Kommunikation bis SIL4 [[308], S. 142] (im aktuell standardisierten SDTv2, IEC 61375-2-3 lediglich bis SIL2).

In einem Demonstrator aus CONNECTA-2 wird auch der Einsatz von OPC UA innerhalb des Consists eines Herstellers erwähnt [315]. Weitere Technologien bei CONNECTA sind VLANs, Zeitsynchronisation (Clock Synchronization, IEEE 802.1AS-rev und IEEE 1588v2) sowie Time-Sensitive Networking (TSN, IEEE 802.1Qbv) [308]. Hierbei handelt es sich um Standards zur präzisen Uhrzeitsynchronisation im Sub-Mikrosekundenbereich in verteilten Systemen, sowie zur deterministischen Planung, Synchronisation, Hochverfügbarkeit und Latenzminimierung von Netzwerkverkehr.

Als Schnittstellen sind bei CONNECTA die API des Functional Distribution Framework (FDF) für Anwendungen [316], das Functional Open Coupling (FOC) [309] zwischen Consists und Anwendungsprofilen (Application Profiles) [317] zu nennen, wobei letztere mit SysML modelliert werden. Beim FDF kommen zudem Functional Telegrams zum Einsatz die auf dem JSON-Format basieren.

Im Güterverkehr kommen bei der ITSS REST-Architekturen per HTTP(S) mit JSON-Schema im Falle der *Schnittstelle 1* (Server-zu-Server) zum Einsatz [312]. Außerdem wird ein eigenes binäres Protokoll im Bereich der Anwendungsprofile zum Austausch von Sensordaten in *Schnittstelle 2* dargestellt [313]. *Schnittstelle 1* arbeitet dabei sowohl mit Ereignis-basierten Benachrichtigungen (Push), als auch Request/Response-Kommunikation. Für *Schnittstelle 2* werden sogenannte Application Profiles (Anwendungsprofile) [313] definiert, die verschiedene Anwendungsfälle, wie bspw. „Valve State“ (Ventilzustand) oder „Detected Shock“ (Erkannte Erschütterung) abbilden. Bisher sind *Schnittstelle 1 und 2* zumindest teilweise spezifiziert.

In der DAK-Studie wird abhängig von der verwendeten Technologie von Transport Layer Security (TLS) bei TCP/IP oder einem entsprechend adaptierten Protokoll, bspw. für CAN gesprochen [[65], S. 62]. Es werden zudem ein Service-Application-Layer sowie ein Service-Access-Point-Layer genannt, für die jedoch keine konkreten Protokolle vorgeschlagen werden. Beide Layer sind Bestandteile einer vorgeschlagenen Service-orientierten Architektur (SOA). Der Service-Application-Layer bildet die jeweilige Dienstefunktionalität ab. Der Service-Access-Point-Layer stellt die Schnittstellen für andere Komponenten zur Verfügung und agiert ggf. als Gateway für Anwendungen im Service-Application-Layer.

8.1.6 Architekturkonzepte

Zu Beginn des Kapitels erfolgt eine Übersicht über die recherchierten Ergebnisse. Tabelle 79 stellt die Architekturkonzepte im SPV und Tabelle 80 im SGV dar.

TABELLE 79: ARCHITEKTURKONZEPTE IM SCHIENENPERSONENVERKEHR

Einordnung	Bezeichnung	Erläuterung
CONNECTA	Functional Distribution Framework (FDF)	Middleware mit standardisierter API, ermöglicht untereinander isolierte (verschiedene Sicherheitslevel), portable Anwendungen, Kommunikation unabhängig von der jeweiligen Hardware. Vergleichbar mit AUTOSAR oder ARINC653
	Anwendungsprofile	Beschreibung der funktionalen und technischen Schnittstelle zwischen Subsystem und TCMS
	Functional Open Coupling (FOC)	Beschreibung von Schnittstellen eines Consists gegenüber dem restlichen Zug; ermöglicht Kopplung heterogener Consists
	Integrated Modul Platform (IMP)	(Embedded) Hardware-Plattform zur Ausführung der FDF-Middleware und Anwendungen der Subsysteme
	Simulation and Virtualization Framework (SVF)	Ermöglicht Teile eines Zugs zu simulieren und zu testen, um Verifizierungs- und Zertifizierungsprozess zu vereinfachen.

TABELLE 80: ARCHITEKTURKONZEPTE IM SCHIENENGÜTERVERKEHR

Einordnung	Bezeichnung	Erläuterung
ITSS	Anwendungsprofile	Standardisierte Beschreibung verschiedener Sensoren/Telemetrie-Daten
DAK-Studie OWITA GmbH	Service Oriented Architecture (SOA)	Architektur, bei der konkrete Implementierungen durch übergeordnete Dienste abstrahiert werden; fördert somit plattformunabhängigkeit und lose Kopplung (loose coupling)

Innerhalb der betrachteten Ansätze für Architekturen im Personenverkehr und Güterverkehr sind die folgenden grundlegenden Konzepte zu Systemarchitekturen vorgeschlagen worden, die hier zusammengefasst werden als Basis für die weiteren Überlegungen.

Im Rahmen der CONNECTA Projekte wurden einige Architekturkonzepte für den Bahnsektor zum Personenverkehr entwickelt und angepasst. Hierbei standen verschiedene Ziele im Vordergrund. Das Functional Distribution Framework (FDF) ist eine Middleware mit standardisierter API, mit der künftige Anwendungen portabel entwickelt, und isoliert voneinander in verschiedenen Sicherheitsleveln sowie unabhängig von der eingesetzten Hardware ausführbar sein und kommunizieren sollen. Es werden AUTomotive Open System Architecture (AUTOSAR) im Automobil-Sektor und ARINC653 im Luftfahrt-Sektor als vergleichbare Ansätze genannt.

Damit zusammenhängend wurden Anwendungsprofile definiert, die die funktionale und technische Schnittstelle zwischen einem Subsystem und dem restlichen TCMS bilden. Eine Erweiterung dieses Konzepts ist das Functional Open Coupling (FOC), das Schnittstellen eines Consists gegenüber dem restlichen Zug beschreibt und bspw. Kupplung von heterogenen Consists (z. B. unterschiedliche Hersteller) ermöglichen soll. Sowohl FOC als auch FDF werden mit SysML Modellen beschrieben.

Die Integrated Modular Platform (IMP) stellt eine flexible, sichere, fehlertolerante (embedded) Hardware-Plattform dar, auf der die FDF Middleware und die Anwendungen der Subsysteme ausgeführt werden. Die Standardisierung der Schnittstellen soll es in Zukunft ermöglichen Teile des Zugs zu simulieren und zu testen und somit den Verfizierungs- und (Re-)Zertifizierungsprozess zu vereinfachen. Hierfür dient das sogenannte Simulation and Virtualization Framework (SVF).

Im Güterverkehr wurden beim ITSS ebenfalls Anwendungsprofile (Application Profiles) in der *Schnittstelle 2* spezifiziert. In *Schnittstelle 1* wird auf eine Client-Server-Architektur mit REST und Push- sowie Pull-Kommunikation gesetzt.

In der DAK-Studie wird darüber hinaus eine Service Oriented Architecture (SOA) vorgeschlagen. Diese besteht aus dem Service Access Point Layer und Service Application Layer. Weiterhin wird eine logische Adressierung der Fahrzeuge vorgeschlagen, mit Neuvergabe der Adressen bei detektierter Änderung sowie statisch vorgegebene Service Access Point Identifier.

8.1.7 IT-Sicherheitsansätze und verwendete Maßnahmen

Zu Beginn des Kapitels erfolgt eine Übersicht über die IT-Sicherheitsansätze in Tabelle 81.

TABELLE 81: ÜBERSICHT ÜBER IT-SICHERHEITSANSÄTZE

Einordnung	Zusammenfassung
CONNECTA	Sicherheitsanalyse und Maßnahmen v. a. auf Ebene des NG-TCN, mit Fokus auf allgemeinere IT-Sicherheitsmaßnahmen, Einschränkung und Überwachung von Netzwerkzugriff, verstärkt auf unteren OSI-Ebenen (z. B. MACsec + PNAC)
ITSS	Bisher wenig Details zur IT-Sicherheit verfügbar; Fokus auf Nutzung von TLS und HTTP Basic Authentication bei Server-zu-Server-Kommunikation (Schnittstelle 1); Lediglich eine Berechtigungsart, die vollständigen Lese- und Schreibzugriff erlaubt; Logging von Logins und Zwischenspeicherung von Nachrichten
DAK-Studie OWITA GmbH	Sicherstellung der Zugintegrität mittels zyklischem Austausch einer abgesicherten und authentifizierbaren Nachricht zwischen letztem Wagen und Triebfahrzeug; TLS für Kommunikation bzw. Adaption für CAN

Die in den vorangehenden Abschnitten adressierten Architekturen im Bahnsektor nennen bereits eine Reihe von Konzepten und Maßnahmen zur IT-Sicherheit als Basis der Untersuchung der Use Cases in Kapitel 8.2.

Bezüglich IT-Sicherheit in CONNECTA waren vor allem das Deliverable „D4.2 – Intermediate Report on Cybersecurity measure for NG-TCMS“ [318] aus CONNECTA-3, sowie „D3.5 – Drive-by-Data Architecture Specification“ [308] aus CONNECTA-2 relevant. Im zuerst genannten Dokument wurden auch „Threats Landscape“ (Bedrohungslage), „Attacker Goals“ (Angreiferziele), und „Countermeasures“ (Gegenmaßnahmen) beschrieben, sowie eine Risikoanalyse durchgeführt. Das betrachtete System wurde in verschiedene Domänen aufgeteilt:

- TCMS (Train Control and Monitoring System, safety-related),
- OOS (Operator Oriented Services, non-safety),
- COS (Customer Oriented Services, non-safety).

Diese wurden weiter unterteilt in sogenannte „security zones“ (Sicherheitszonen). In CONNECTA-1 war zunächst vorgesehen, lediglich unidirektionalen Traffic zwischen COS, OOS und TCMS zu erlauben; dies wurde jedoch später aufgrund bidirektionaler Netzwerkprotokolle wie TCP wieder verworfen.

Zur Trennung der Zonen wurde nun ein hybrider Ansatz mittels VLANs, Router und Firewalls vorgeschlagen. Im Dokument wird auch von „security gateways“, „security barriers“, bzw. „secure application gateways“ gesprochen, um Protokolle und Inhalte über Deny-/Allow-Listen zu filtern [[318], S. 51]. Es wird vorgeschlagen diese in den ETBNs bzw. Wireless Train Backbone Nodes (WLTBN) einzusetzen.

Das Security Application Gateway soll dabei verhindern, dass schädlicher („malicious“) Traffic in das Consist-Netzwerk hinein oder heraus gelangt [[318], S. 17]. Es stellt sich die Frage, inwiefern dies generell überhaupt möglich ist bzw. ob dadurch nicht nur niedrigschwellige Angriffe abgewehrt werden können.

Generell werden eher allgemeine IT-Sicherheitsmaßnahmen vorgeschlagen, z. B. [[318], S. 52 – 54]

- *Überwachung*: Intrusion Detection System (IDS), Logins, Netzwerkzugriff
- *Filterung*: MAC-Adressen-Filter, Firewalls, Secure Gateways, Einschränkung der offenen Ports zum internen/externen Netzwerk
- *Security by obscurity*: versteckte oder geänderte Service Set Identifier (SSID), Reduzierung der Access Point/Router-Signalstärke, Geheimhaltung der externen IP-Adresse. Hierbei sollte allerdings angemerkt werden, dass diesem Ansatz alleingestellt heutzutage meist widersprochen

wird, so bspw. auch vom NIST: „System security should not depend on the secrecy 247 of the implementation or its components“ [307].
- *Geräte-Sicherheit*: Secure boot, Secure remote firmware update, TPM, Melden von fehlenden/gestohlenen Geräten, Zugriff auf gemeldeten Geräten verweigern
- *Sozial/Training***:** Schulung des Sicherheitsbewusstseins (Security awareness training)
- *Kryptographie*: Verschlüsselung (WPA3, MACsec, TLS, Datagram Transport Layer Security (DTLS)), Nutzung von Keyed-Hash Message Authentication Codes (HMAC) bei der Kommunikation mit Geräten, Virtual Private Networks (VPN), Verschlüsselung für Zugangsdaten und vertraulicher Datenaustausch
- *Authentifizierung*: sichere Passwörter & regelmäßiges Ändern (NIST 800-63 DB), Einmal-Passwörter, Multi-Faktor-Authentisierung
- *Verfügbarkeit*: Begrenzung der ausgehenden Datenrate, Denial of Service (DoS)/DDoS-Angriffs-Notfallplan (attack response plan), Erhöhung der Gesamtbandbreite oder Reservieren von ausreichend Bandbreite für kritischen Datenverkehr

In der Architekturspezifikation [308] werden u. a. folgende Maßnahmen bzw. grundlegende Methoden und Konzepte genannt:

- Firewalls [[308], S. 208]
- Erkennung von Sicherheitsereignissen (Security Event Detection) [[308], S. 211]
- Verschlüsselung [[308], S. 213] (MACsec)
- Netzwerkzugriffskontrolle [[308], S. 214]
  - MACsec
  - PNAC
- Traffic-Shaping gegen DoS [[308], S. 78, 126]

Die COS-Zone wird dabei explizit nicht weiter betrachtet („securing this zone would be expensive with a very uncertain return on investment“, dt.: Die Sicherung dieser Zone wäre mit hohen Kosten und einer ungewissen Rendite verbunden.) [[308], S. 55]. Außerdem sollen PNAC und MACsec aufgrund von Kosten nur in Bereichen eingesetzt werden, in denen das Sicherheitsniveau signifikant angehoben werden kann [[308], S. 126].

Zur Sicherheit auf der Transportschicht heißt es, dass das ein geschlossenes System angenommen wurde und Sicherheitsmechanismen für offene Systeme (z. B. Drahtlos (Wireless)) bisher nicht berücksichtigt wurden [[308], S. 135]. TLS wird als potenzielles Protokoll erwähnt, jedoch zumindest für „process data communication“ (Prozessdaten-Kommunikation) ausgeschlossen, da es auf TCP aufbaut [[308], S. 135].

Daher liegt der Fokus bisher vor allem auf der Sicherung des Zugangs/Zugriffs zum Netz durch die unteren Schichten und physisch abgesicherte Bereiche. In den Anforderungen an die Architektur (Architectural Requirements) [[319], S. 18] wird weiterhin erwähnt, dass Task T4.4 die Sicherheitsaspekte bzgl. des FDFs entwickeln soll. In diesem könnten also noch weitere Sicherheitsmechanismen auf Anwendungs- bzw. Middlewareebene vorgeschlagen werden. Hierzu lagen jedoch noch keine Dokumente vor.

Grundlegend lässt sich sagen, dass in den CONNECTA-Projekten eine durchaus komplexe Architektur vorgesehen ist, wobei noch offen ist, inwiefern diese vollständig umgesetzt werden wird. Weiterhin scheint es, als läge der Fokus überwiegend auf Safety, während Security bisher eher in einer groben Risikoanalyse, und auf Netzwerk-/Geräte-Zugangsebene berücksichtigt wurde.

Es stellt sich die Frage, inwiefern bspw. Angriffsszenarien mit manipulierten oder ausgetauschten Geräten, sowie Sicherheitslücken in der Software es ermöglichen könnten, Daten im System zu verfälschen oder zu verwerfen, wobei diese ggf. nicht weiter auf Sinnhaftigkeit überprüft würden, aber im Betrieb evtl. zu katastrophalen Ergebnissen führen könnten.

Es ist offen, inwiefern die Geräte sich untereinander vertrauen, oder ob zukünftig eher auf einen Zero-Trust-Ansatz gesetzt wird. Interessant wäre zudem, inwiefern sicherheitskritische Funktionen durch einen Angreifer ausgehebelt oder umgangen werden können, wenn davon ausgegangen wird, dass Geräte kompromittiert werden können und die Umsetzung dieser Funktionen lediglich auf manipulierbarer Software basiert.

Im Güterverkehr sind in den Veröffentlichungen der ITSS bisher wenig Details zur IT-Sicherheit verfügbar. Für *Schnittstelle 1* (Server-zu-Server) wird eine gesicherte Verbindung mittels TLS vorgeschrieben (Vertraulichkeit, Integrität). Zur Authentifizierung wird inzwischen die Hypertext Transfer Protocol (HTTP) Basic Authentication (RFC 7617) verwendet, während zuvor in einer älteren Version die Anmeldedaten als Uniform Resource Locator (URL)-Parameter übertragen wurden [[312], S. 11].

Es existiert lediglich eine Berechtigung, die vollständigen Lese- und Schreibzugriff erlaubt [[312], S. 92]. Bei fehlgeschlagenen Logins sollen die Systeme die Anfragen ohne spezifische Meldung verwerfen und ggf. eine Sicherheitswarnung auslösen. Nachrichten, die im Push-Verfahren übermittelt werden, werden bis zu 24 Stunden zwischengespeichert, falls der Server nicht erreichbar ist (Verfügbarkeit) [[312], S. 9].

In der DAK-Studie wird zur Sicherstellung der Zugintegrität ein zyklischer Austausch einer abgesicherten und authentifizierbaren Nachricht zwischen dem letzten Wagen und dem führenden Fahrzeug empfohlen [[65], S. 15]. Weiterhin wird TLS für die Kommunikation im Zug genannt sowie die Notwendigkeit eines vergleichbaren, eigenen Protokolls bzw. eine Adaption CAN/CAN-FD. Die hierfür notwendige Public-Key-Infrastruktur wurde jedoch im Dokument noch nicht näher ausgearbeitet [[65], S. 62].

8.2 Risikoanalyse Datensicherheit und Cybersecurity

Grundlage der folgenden Betrachtung zur Cybersecurity sind die vorangehend ermittelten Informationen zu Architekturen, Netzwerken, Protokollen und insgesamt digitalen Technologien im Bereich sensorbasierter Systeme im Kontext von Schienenfahrzeugen. Der Fokus liegt zunächst auf den Use Cases, die im Rahmen des Projektes ermittelt und in den Workshops aus Sicht der Stakeholder priorisiert wurden. Ausgehend von einer Analyse möglicher Architekturen eines Use Cases aus der Gruppe „Fahrzeug überwacht Fahrzeug“ wurde eine generalisierte Systemarchitektur abgeleitet und mittels der Methodik der Attack Trees Angriffsvektoren abgeleitet. Diese Angriffsvektoren wurden im nächsten Schritt ergänzt durch weitere wichtige Aspekte, die im Rahmen der Stakeholder Workshops aus den Bereichen KI, IoT, Software Updates und Cloudbasierte Software-Architekturen identifiziert wurden.

Anschließend werden diese Erkenntnisse im Rahmen des Risikomanagements mit dem Fokus auf Cybersecurity im Schienenverkehr eingeordnet. Das Risikomanagement bezieht sich dabei auf den gesamten Lebenszyklus der betrachteten Systeme. Außerdem wird dargestellt, dass ein Angriff aus einer ganzen Reihe aufeinanderfolgender Aktionen bestehen kann, die häufig jeweils von Spezialisten durchgeführt werden. Dazu werden zum einen exemplarisch Angriffsmodelle und deren Motivation auf Basis öffentlich zugänglicher Quellen herausgearbeitet und Angriffsvektoren mittels der Methodik der Kill Chains eingeordnet. Abschließend werden allgemeine Einschätzungen zu möglichen Risiken im Kontext der Use Cases gegeben, die im Rahmen des Risikomanagements in konkreten Kontexten eingesetzt werden können.

8.2.1 Untersuchung des Use Case „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“

Im Rahmen der IT-Sicherheitsanalyse wurde der Use Case „Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen“ ausgewählt, da hier vor allem im Schienenpersonenverkehr eine größere Anzahl an Komponenten beteiligt sind (und somit eine größere potenzielle Angriffsfläche besteht), und verschiedene Systemauslegungen zum Einsatz kommen. Außerdem sollte zunächst der Analyse-Fokus auf den Zug gesetzt werden, weniger auf die Infrastruktur. Die komplexeren Architekturen im Schienenpersonenverkehr lassen sich zudem abstrahieren und auf die aktuell noch deutlich weniger komplexen Architekturen im Schienengüterverkehr übertragen.

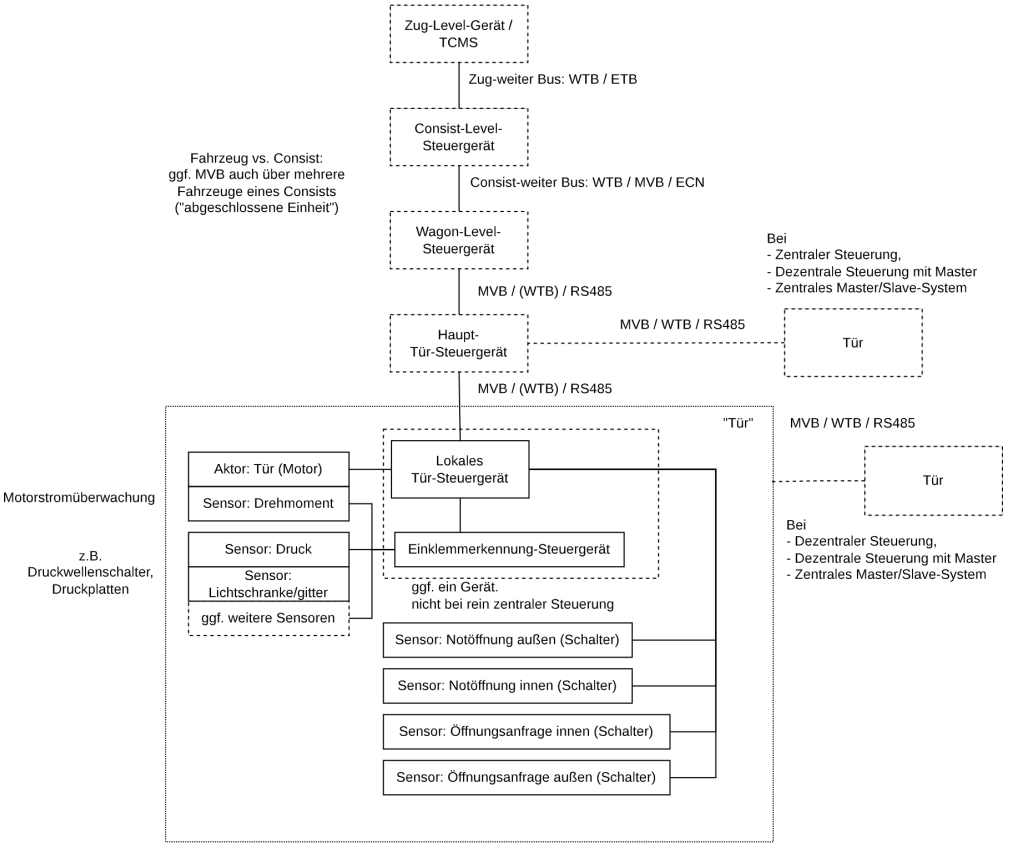


Abbildung 90: Generalisierte Systemarchitektur "Türsystem"

Als Quellen wurde u. a. die Vorarbeit der Bestandsaufnahme zu Sensoriksystemen herangezogen, wo bereits architekturelle Unterschiede bei der Ausprägung klassischer Türsysteme herausgearbeitet wurden. Außerdem wurden Produktbeschreibungen zu Türsteuerungen und Einklemmerkennungen einbezogen. CONNECTA bietet zudem in den Application Profiles mit dem Profil „Doors“ (Türen) eine Beschreibung verschiedener Use Cases, sowie zugehörige Ablaufdiagramme und Schnittstellendefinitionen, aus denen weitere Informationen für aktuelle und zukünftige Architekturen abgeleitet werden können. Aus diesen Informationen wurde im nächsten Schritt eine generalisierte komponentenorientierte Systemarchitektur des Sensorsystems Türsteuerung abgeleitet. Das Diagramm in Abbildung 90 teilt das System in Steuergeräte, Aktoren, Sensoren und Verbindungen auf. Blöcke sind Steuergeräte bzw. Aktoren oder Sensoren, die durch unterschiedliche Arten von Kommunikationskanälen miteinander verbunden sind. Gestrichelte Blöcke zeigen unterschiedliche Varianten an und sind somit nicht in jeder Ausprägung eines Türsystems vorhanden. Jede Komponente und jede Verbindung in diesem Diagramm kann

prinzipiell angegriffen werden, wobei Angriffe auf Steuergeräte von Angriffen auf die Kommunikationskanäle bzw. Angriffen auf Sensoren oder Aktoren unterschieden werden müssen, da hier meist ganz unterschiedliche Angriffsvektoren praktikabel sein können. Die betrachteten Türsysteme sind jeweils als integriert im Zug zu sehen, wobei verschiedene Varianten (siehe Bestandsaufnahme der Sensoriksysteme) möglich und auch im Einsatz sind. Daraus ergibt sich, dass die Komplexität und der Umfang an beteiligten Komponenten je nach Variante sehr unterschiedlich sein können. Der Block „Tür“ kennzeichnet genauer, welcher Teil des Systems als „lokale Tür“ angesehen wird. Alles darüber hinaus betrifft meist mehrere Türen bzw. die Kommunikation im Zugsystem. Betrachten wir zunächst die lokale Tür, so sind zwei grundlegende Ausprägungen möglich: Es kann jeweils pro Tür ein lokales Steuergerät vorhanden sein, oder alternativ bei der Variante „Zentrale Steuerung“ würden die Komponenten stattdessen direkt an einem Hauptsteuergerät für Türen angeschlossen sein. Im Falle von „Dezentraler Steuerung“, „Dezentraler Steuerung mit Master“ und „Zentrales Master/Slave-System“ kann eine lokale Türsteuerung zudem über ein Bussystem direkt mit einer anderen Tür(-steuerung) verbunden sein. Eine lokale Tür beinhaltet bereits häufig eine Vielzahl von Sensoren. Als Sensor wird in diesem Kontext auch ein einfacher Taster betrachtet (digitaler Eingang). In CONNECTA sind in diesem Zusammenhang mindestens vier „Schalter“ zu finden: Jeweils zwei für die Notöffnung bzw. eine normale Öffnungsanfrage innen und außen. Zur Vermeidung von Verletzungen wird eine Einklemmerkennung eingesetzt, die entweder als separates Gerät oder als Teil der Türsteuerung implementiert sein kann. Dabei kommen verschiedene Sensoren, wie z. B. Lichtgittersensoren, Druckwellenschalter bzw. Druckplatten zum Einsatz. Zur Türöffnung und -schließung ist mindestens ein Aktor (Motor) nötig. Häufig kommen mit diesem auch weitere Sensoren, beispielsweise zum Bestimmen des Drehmoments, hinzu, die auch zur Erkennung von Störungen eingesetzt werden können. Jeder Sensor bzw. Aktor ist jeweils über eine Verbindung mit dem übergeordneten Steuergerät verbunden. Dabei kann zwischen Verbindungen mit digitalen Protokollen und einfachen elektrischen Verbindungen unterschieden werden. Bspw. könnte ein resistiver Sensor direkt an einen analogen Eingang eines Steuergeräts angebunden werden, wobei die Bestimmung des Messwerts dann über den Widerstand bzw. Spannungsabfall erfolgt. Viele Sensoren sind allerdings schon mit einer Vorverarbeitung integriert und werden bspw. über Datenbusse (z. B. I^2C) angebunden. Bei solchen Sensoren könnte daher potenziell auch die Verarbeitung im Sensor selbst bereits angegriffen werden.

Die lokale Tür ist meist über ein Bussystem (z. B. MVB, WTB oder RS485) mit einem übergeordneten Steuergerät verbunden. Je nach Architektur existieren dabei unterschiedlich viele Zwischenebenen, an denen Daten aggregiert, verarbeitet und weitergeleitet werden können. Im Falle der „dezentralen Steuerung mit Master“ oder beim „zentralen Master/Slave-System“ existiert bspw. ein Haupt-Türsteuergerät. Darüber hinaus ist evtl. ein weiteres Steuergerät auf der Wagon-Ebene (eins pro Wagon) vorhanden, das weitere Aufgaben eines Wagons bündelt. Darüber kann ein Steuergerät auf Consist-Ebene vorhanden sein. Je nach Architektur sind Wagons oder Consists als abgeschlossene Einheiten zu betrachten. Jedoch sollte auch bei Consists beachtet werden, dass Datenkanäle zwischen den Wagons eines Consists vorhanden sein müssen, die wiederum angegriffen werden können. Consists kommunizeren eher über Datenbusse, wie WTB oder ETB, die entsprechend für längere Verbindungen und die Teilnahme vieler Geräte ausgelegt sind. Über der Consist-Ebene kann ein Zughauptrechner bzw. Hauptsteuergerät implementiert sein (TCMS), in dem alle Daten, die auf Zugebene benötigt werden, zusammengeführt werden, und teilweise auch im Triebfahrzeug angezeigt werden. Je nach verwendetem Bussystem und konkreter Architektur unterscheiden sich auch häufig die darauf gesprochenen Protokolle höherer OSI-Schichten, die ebenfalls jeweils spezielle Angriffsvektoren besitzen können.

Es lässt sich feststellen, dass es einige unterschiedliche Architekturausprägungen gibt, und sich somit die konkreten Angriffsvektoren auch nach der jeweiligen Implementierung unterscheiden. In diesem Zusammenhang ist es daher sinnvoller, einzelne Angriffselemente auf die abstrakten Komponenten und Kommunikationskanäle zu betrachten, als einen Angriff auf ein hypothetisches Gesamtsystem zu simulieren. Dabei müssen jeweils gewisse Annahmen getroffen werden, beispielsweise, dass eine angreifende Person die Möglichkeit hat, einen Kommunikationskanal zu manipulieren oder zu unterbrechen, eine

Schwachstelle eines Steuergeräts auszunutzen oder einen physikalischen Sensor zu stören. Ein reales und vollständiges Angriffsszenario kann nur realistisch untersucht werden, wenn das anzugreifende System bekannt bzw. verfügbar ist.

Eine weitere wichtige Erkenntnis aus der generalisierten Systemarchitektur ist, dass sich viele Eigenschaften weitgehend auch auf andere Use Cases übertragen lassen. Ob es sich bei dem untersuchten System um eine Tür oder eine andere Verriegelung handelt, spielt für die möglichen Angriffsarten auf Sensoren, Steuergeräte und Datenkanäle zunächst nur eine untergeordnete Rolle. Auch andere Messungen am Zug basieren letztendlich auf einer ähnlichen Grundarchitektur. Ebenso lässt sich das Modell auch auf Güterzüge übertragen, bei denen auch eine ähnliche hierarchische, wenn auch weniger komplexe Architektur von Steuergeräten geplant ist. Für eine konkrete Risikoanalyse eines bekannten Systems könnte dieses daher ähnlich in Sensoren, Aktoren, Steuergeräte und Verbindungen zerlegt werden, um anschließend relevante Angriffsvektoren zu identifizieren. Die Systemarchitektur lässt sich somit auch auf andere Sensor-Usecases auf dem Zug, wie die Überwachung der Bremse, übertragen. Weitergehend können konkrete Kommunikationsleitungen, Protokolle, Sensoren, Steuergeräte und die eingesetzte Software auf Risiken und Sicherheitslücken untersucht werden. Dennoch werden im Rahmen dieses Dokuments einige dieser Elemente, Angriffe und Mitigationsstrategien beispielhaft betrachtet, die im Rahmen der Stakeholder-Interviews und Recherchen als besonders relevant erachtet wurden.

8.2.2 Attack Trees und Angriffsvektoren

Um einen Überblick über mögliche Angriffsvektoren zu erhalten, wurde sich zunächst am Beispiel der „Attack Trees“ aus dem DZSF-Projekt „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte“ orientiert. Dabei wurde der Attack Tree in Abbildung 91 erarbeitet. Im Unterschied zum genannten Projekt, ist dieser Baum jedoch abstrakter gehalten, sodass konkrete Angriffsschritte entfallen. Dies ist u. a. in der Tatsache begründet, dass diese vor allem von der eingesetzten Architektur und weiteren Bedingungen abhängig wären. Z. B. wäre es bei einem Angriff auf die Verfügbarkeit eines Sensors relevant, wie das konkrete System bei einem Ausfall eines Sensors reagiert bzw. ob dieser überhaupt erkannt werden würde. Bei sicherheitskritischen Systemen ist hier die Annahme, dass das System in einem sicheren Zustand bleibt. Dabei wird jedoch hauptsächlich von nicht-manipulierten Systemen ausgegangen, was möglicherweise keine ausreichende Annahme im Sinne der IT-Sicherheit ist. Bei einem Angriff könnte also bspw. die Präsenz eines Sensors vorgetäuscht werden, obwohl dieser eigentlich ausgefallen ist bzw. keine korrekten Werte liefert. Im Fall von den üblicherweise vorhandenen mehrfachen Redundanzen (oder invertierten Signalen) wird auch die Verfügbarkeit im Sinne der IT-Sicherheit erhöht. Im Kontext aktiver, gezielter Angriffe, im Sinne der Betrachtung von Angriffsvektoren, stellen diese jedoch in der Regel, im Vergleich zum Umgehen ausgereifter IT-Sicherheitsmaßnahmen (z. B. Brechen einer modernen Verschlüsselung), kein größeres Hindernis dar. Dies rührt daher, dass der Angriff in einem solchen Fall nur an mehreren Stellen ausgeführt werden muss und sich somit der Aufwand erhöht, sich aber die grundlegende Schwierigkeit des Angriffs aus IT-Sicherheitssicht nicht nennenswert ändert.

Im Rahmen des Use Cases „Zustand von Türen und anderen Verriegelungen“ wurden als übergeordnete Angriffsfolgen die Kategorien „Verletzung der körperlichen Unversehrtheit“, „Finanzieller Schaden Betreiber“, „Reputationsschaden Betreiber“ sowie „Einschränkung einer kritischen Dienstleistung“ aus dem genannten Projekt für relevant erachtet. Darunter wurden jeweils Angriffsziele eingeordnet, aus denen die jeweiligen Folgen resultieren können:

- Verletzung der körperlichen Unversehrtheit:
    - Verhinderung der Türöffnung: Eine Person hat einen medizinischen Notfall, aber die Tür lässt sich nicht öffnen (evtl. auch Verhinderung der Notöffnung).
    - Tür als geschlossen ausgeben, obwohl offen: Passiert dies während der Fahrt könnten Personen bei höherer Geschwindigkeit aus dem Fahrzeug fallen, Hindernisse (z. B.

Pflanzen) in die Fahrzeugkabine gelangen, oder die Tür könnte abbrechen und einen Gegenzug treffen.
    - Türen schließen lassen, während Person in der Tür ist: Wurde die Einklemmerkennung manipuliert, kann die Tür evtl. eine Person einklemmen.
- Finanzieller Schaden Betreiber:
    - „Verhinderung der Weiterfahrt des Zuges im Bahnhof“ und „Verhinderung der Weiterfahrt des Zuges auf Strecke“: Dies kann zu einer Kettenreaktion führen, bei der auch andere Züge aufgrund eines blockierten Gleises nicht weiterfahren können. Dabei kann es bei Ausfall mehrerer Züge an zentralen Knotenpunkten ggf. sogar zu einem vollständigen lokalen Ausfall kommen. Durch die Verspätung bzw. den Ausfall aufkommende Kosten müssen ggf. erstattet werden.
-
- Reputationsschaden Betreiber:
    - Alle Angriffsziele: Bei allen Zwischenzielen sind die Konsequenzen meist deutlich für Mitfahrende sichtbar, was sich in der Regel negativ auf die Reputation des Betreibers auswirken dürfte.
- Einschränkung einer kritischen Dienstleistung:
    - Verhinderung der Weiterfahrt des Zugs im Bahnhof und Verhinderung der Weiterfahrt des Zugs auf der Strecke: In beiden Fällen ist die Dienstleistung des öffentlichen Personenverkehrs, die zur kritischen Infrastruktur zählt, eingeschränkt.

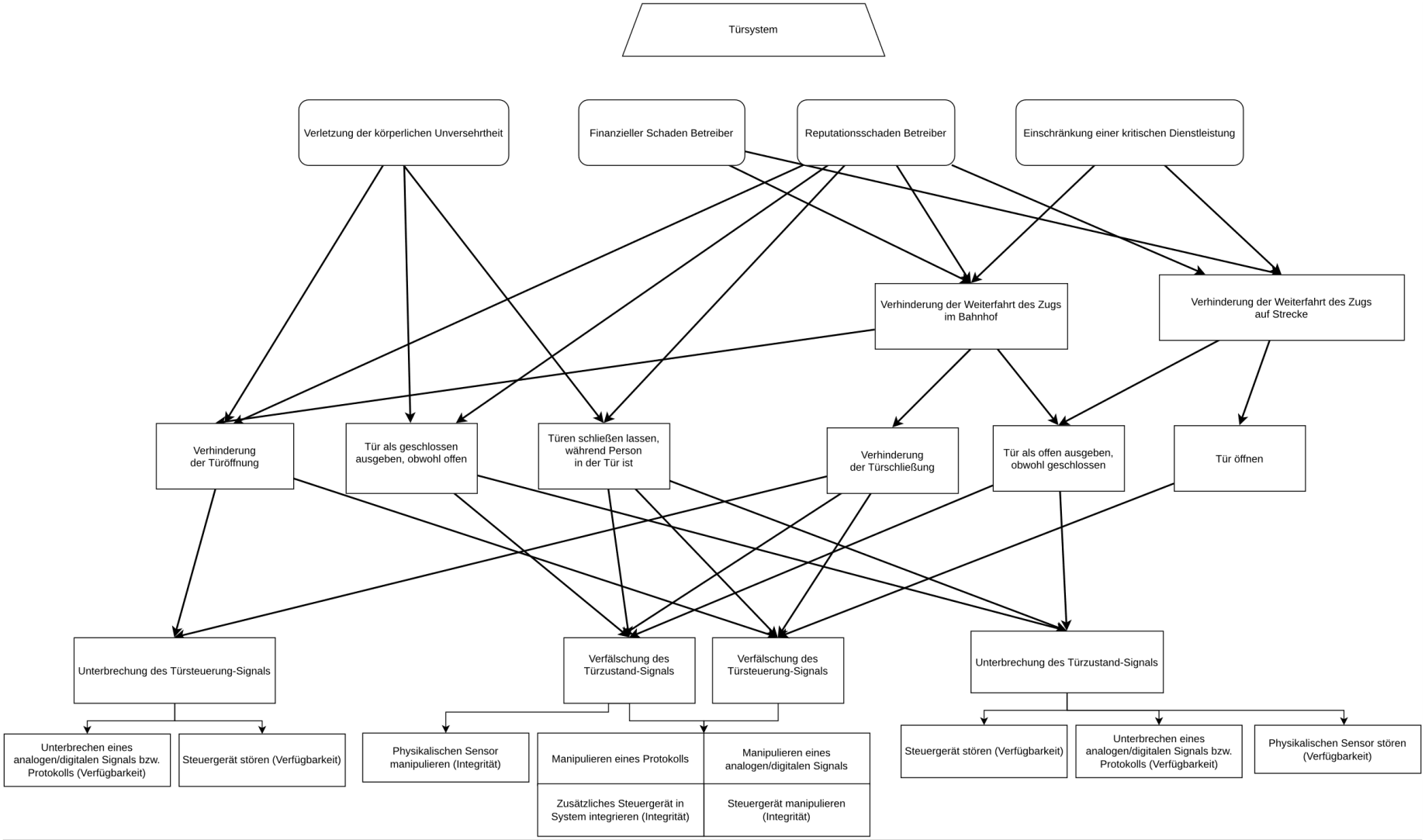


Abbildung 91: Attack Tree „Zustand von Türen u. a. Verriegelungen“

Unter den Zielen finden sich jeweils weitere Zwischenziele, mit denen die Ziele erreicht werden können. Sind einem Ziel oder einer Angriffsfolge mehrere Ziele untergeordnet, so sind diese, ähnlich wie im genannten Projekt, als implizite Disjunktion zu verstehen, d. h. es kann ausreichen, lediglich eines dieser Ziele zu erreichen, um die entsprechende Folge zu verursachen.

Auf der dritten Ebene finden sich mehrere (Zwischen-)ziele, die teilweise komplementär zueinanderstehen. Die Ziele sind dabei Schutzzielen der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) zugeordnet. So ergänzen sich folgende Ziele:

- „Verhinderung der Türöffnung“ und „Verhinderung der Türschließung“ (Angriff auf Verfügbarkeit)
- „Tür als geschlossen ausgeben, obwohl geöffnet“ und „Tür als offen ausgeben, obwohl geschlossen“ (Angriff auf Integrität: Zustand)
- „Türen schließen lassen, während Person in der Tür ist“ und „Tür öffnen“ (Angriff auf Integrität: Steuerung)

Auf der vierten Ebene werden Zwischenziele genannt, um diese Angriffe auf die Integrität bzw. Verfügbarkeit durchzuführen. Diese sind ebenfalls wieder komplementär – „Unterbrechung des Türsteuerung-“ bzw. „Türzustand-Signals“ (Verfügbarkeit) sowie „Verfälschung des Türsteuerung-“ bzw. „Türzustand-Signals“ (Integrität). In diesem Zusammenhang ist der Begriff des *Signals* sehr weit ausgelegt. Hierbei kann es sich um die analoge oder digitale „Ausgabe“ (z. B. Widerstand oder I²C-Datum) eines Sensors handeln, um die Ausgabe eines Steuerungsgeräts zur Ansteuerung eines Aktors, oder um eine Nachricht auf einem Kommunikationsbus bzw. innerhalb eines Netzwerkprotokolls.

Auf der untersten Ebene folgen abstrakte Angriffsvektoren. Bei diesen hat sich herausgestellt, dass sich diese innerhalb von Sensorsystemen wiederholen, weshalb sie gezielt abstrakt gehalten wurden und im Folgenden auch näher beleuchtet werden. Diese finden sich auch in Tabelle 82 wieder, wo außerdem Unterkategorien von Angriffen aufgeführt sind. Auch hier finden sich wieder die Schutzziele wieder, wobei die Vertraulichkeit – zumindest bei Sensorsystemen vor Ort (bzw. im Fahrzeug) – meist eine untergeordnete Rolle spielt.

TABELLE 82: ABSTRAKTE ANGRIFFSVEKTOREN IM SENSORSYSTEM BAHN

Nr.	Angriffsvektor	Verletztes Schutzziel
V.1	Unterbrechen eines analogen/digitalen Signals bzw. Protokolls	**Verfügbarkeit**
V.1.1	Unterbrechen eines Steuersignals	Verfügbarkeit
V.1.2	Unterbrechen eines Zustandssignals/Sensorinformation	Verfügbarkeit
V.1.3	Kabel durchtrennen	Verfügbarkeit
V.1.4	MitM Device einbauen, um Komm. Zu blockieren	Verfügbarkeit
V.2	Manipulieren eines Protokolls	**Integrität**
V.2.1	Manipulieren eines Steuerungssignals	Integrität
V.2.2	Manipulieren eines Zustandssignals/Sensorinformation	Integrität
V.2.3	MitM Device einbauen, um Komm. Zu manipulieren	Integrität
V.3	Manipulieren eines analogen/digitalen Signals	**Integrität**
V.3.1	Einbau eines MitM Device, um Signale zu manipulieren	Integrität
V.3.2	Elektromagnetische Störung	Integrität

Nr.	Angriffsvektor	Verletztes Schutzziel
V.4	Physikalischen Sensor manipulieren	**Integrität**
V.4.1	Austauschen des Sensors	Integrität
V.4.2	Sensoren außerhalb der Spezifikationen betreiben (z. B. Temperatur)	Integrität
V.4.3	Manipulation des zu messenden Werts (Saturation vs. Blocking vs. Spoofing)	Integrität
V.4.3.1	Verschmutzen (u. a. optische Sensoren)	Integrität
V.4.3.2	Abdunkeln/Blenden (optische Sensoren)	Integrität
V.4.3.3	Widerstand einbauen (resistive Sensoren)	Integrität
V.4.3.4	Kapazität ändern (kapazitive Sensoren)	Integrität
V.4.3.5	Vibration/Schwingung induzieren (z. B. Schall)	Integrität
V.4.3.6	Magnetfeld induzieren (z. B. Hall-Sensoren)	Integrität
V.4.3.7	Gefälschte/Verzögerte Messantwort (z. B. Radar, LIDAR, Ultraschall)	Integrität
V.5	Physikalischen Sensor stören	**Verfügbarkeit**
V.5.1	Sensoren außerhalb der Spezifikationen betreiben (z. B. Temperatur)	Verfügbarkeit
V.5.2	Sensor entfernen	Verfügbarkeit
V.5.3	Sensor zerstören	Verfügbarkeit
V.6	Steuergerät manipulieren	**Integrität**
V.6.1	(Remote-)Software-Update manipulieren	Integrität
V.6.2	Firmware überschreiben (physischer Zugriff oder Wartungsschnittstelle)	Integrität
V.6.3	Konfiguration ändern (physischer Zugriff oder Wartungsschnittstelle)	Integrität
V.6.4	Sicherheitslücke ausnutzen	Integrität
V.6.4.1	… für Code Execution	Integrität
V.6.4.2	… zur Veränderung von Daten (z. B. Einstellungen)	Integrität
V.6.5	Gerät austauschen	Integrität
V.7	Zusätzliches Steuergerät in System integrieren	Integrität
V.8	Steuergerät stören	**Verfügbarkeit**
V.8.1	Gerät physikalisch zerstören	Verfügbarkeit
V.8.2	Stromzufuhr unterbrechen	Verfügbarkeit
V.8.3	Steuergerät außerhalb der Spezifikationen betreiben (z. B. Temperatur)	Verfügbarkeit
V.8.4	Denial of Service Angriff über genutztes Protokoll	Verfügbarkeit
V.8.4.1	Zu viele Nachrichten	Verfügbarkeit
V.8.4.2	Zu viele Verbindungen	Verfügbarkeit
V.8.4.3	Verursachen von aufwändigen Berechnungen (Speicher-/Laufzeitkomplexität)	Verfügbarkeit
V.8.4.4	Manipulierte Nachricht um Programmabsturz zu verursachen	Verfügbarkeit
V.9	Algorithmus oder KI-Modell stören	**Integrität Verfügbarkeit**
V.9.1	Planning/Decision Making stören: DoS – Zug fährt langsam oder stoppt	Verfügbarkeit
V.9.2	Planning/Decision Making stören: Fehler – Kollision	Integrität
V.9.3	Adversarial Attack: Perception False Positive (Falsch erkannt)	Integrität
V.9.4	Adversarial Attack: Perception False Negative (Nicht erkannt)	Integrität
V.9.5	Einschleusen von Abweichungen in Multi-Sensor-Fusion	Integrität

Unterbrechen eines analogen/digitalen Signals bzw. Protokolls (Verfügbarkeit): Hierunter zusammengefasst sind verschiedene Möglichkeiten, eine Informationsübertragung zu stören. Hierbei kann es sich um einen analogen (z. B. Widerstand) oder digitalen (z. B. Schalter) Messwert handeln oder um ein komplexeres digitales Protokoll innerhalb eines Bussystems oder Netzwerks. Im einfachsten Fall werden beim Angriff Kabel durchtrennt, wodurch der korrekte Wert nicht mehr gemessen werden kann bzw. ein Gerät nicht mehr über den gestörten Kanal kommunizieren kann. Hierbei ist zu unterscheiden zwischen der Unterbrechung einer Zustandsinformation bzw. eines Sensordatums und eines Steuersignals (z. B. Signal zur Türöffnung). Neben der Unterbrechung eines Kabels kann auch gezielt elektrisch das Signal gestört werden oder Bits in einen Datenstrom eingeschleust werden, um etwa Prüfsummen ungültig zu machen und die Interpretation einer Nachricht zu verhindern. Ein komplexerer Angriff könnte zudem eine Hardware zwischen zwei Geräten (zwischen zwei Steuergeräten oder zwischen Steuergerät und Sensor/Aktor) hinzufügen, um gezielt nur bestimmte Informationen zu unterbinden (bspw. zu einem bestimmten Zeitpunkt). Dabei könnte eine angreifende Person etwa, ausgelöst durch ein Funksignal, eine Verbindung stören.

Manipulieren eines Protokolls (Integrität): Im Unterschied zum vorangegangenen Angriffsvektor wird beim Manipulieren eine Information gezielt manipuliert, statt lediglich die korrekte Übertragung zu verhindern. Da sich die Art der Manipulation je nach Übertragungsart stark unterscheidet, wurden solche Angriffe auf die Integrität in verschiedene Kategorien aufgeteilt. Das Manipulieren eines Protokolls ist dabei ein komplexerer Angriffsvektor, bei dem Schwachstellen eines Bus- oder Netzwerkprotokolls ausgenutzt werden, um Nachrichten zwischen Teilnehmenden zu verändern. Eine Absicherung mittels Prüfsummen, wie es z. B. zur Verhinderung zufälliger Datenkorrumpierung genügen würde, ist hier nicht ausreichend, da diese einfach beim Angriff berechnet werden können. Auch die Implementierung von Redundanz kann Angriffe solcher Art nicht verhindern, lediglich leicht erschweren. Ein solcher Angriff kann ebenfalls durch ein Man-in-the-Middle-Gerät (MitM) erfolgen oder durch einen Netzwerkteilnehmenden, der mittels Spoofing Nachrichten im Namen eines anderen Geräts senden kann.

Manipulieren eines analogen/digitalen Signals (Integrität): Hierbei handelt es sich um einen Angriff auf unterer Ebene, bei dem statt der Manipulation eines höheren Datenprotokolls ein analoger oder digitaler Messwert direkt manipuliert wird. Dabei muss in der Regel an der Verbindung des Sensors zum Steuergerät selbst manipuliert werden. Beispielsweise könnte ein Signal durch eine elektromagnetische Störung gezielt verzerrt werden oder ein Schalter durch eine entsprechende Schaltung umgekehrt werden. Auch hier könnte gegebenenfalls wiederum ein MitM-Gerät in die Schaltung integriert werden, das ein Signal verfälscht.

Physikalischen Sensor manipulieren (Integrität): Ein Manipulieren des Sensors selbst könnte durch das Austauschen des Sensors geschehen. Der Sensorersatz (z. B. eine Mikrocontroller-Schaltung) ist mit den Schnittstellen des originalen Sensors kompatibel, liefert aber andere Werte, ggf. nach Wunsch der angreifenden Person. Alternativ könnte ein Angriff auch dadurch erfolgen, dass der gewählte Sensor gezielt außerhalb seiner Spezifikationen (z. B. Temperatur- oder Spannungsversorgung) betrieben wird und somit falsche Werte zurückliefert. Je nach Sensorart kann auch eine direkte Manipulation des zu messenden Werts erfolgen: Verschmutzen/Abdunkeln/Blenden von optischen Sensoren, Einbauen zusätzlicher Widerstände bei resistiven Sensoren, Ändern der Kapazität bei kapazitiven Sensoren, Induktion von Vibrationen, Induktion eines Magnetfelds bei Hall-Sensoren sowie ein gezieltes Verzögern bzw. Senden von Messantworten bei aktiven Messungen, basierend auf Ultraschall, Lidar oder Radar.

Physikalischen Sensor stören (Verfügbarkeit): Alternativ kann ein Sensor (z. B. auch bei Vandalismus) mutwillig zerstört oder entfernt werden. Auch das Betreiben eines Sensors außerhalb seiner Spezifikationen könnte zum (temporären oder permanenten) Versagen des Sensors führen.

Steuergerät manipulieren (Integrität): Unter dieser Kategorie finden sich eine ganze Reihe an möglichen Angriffen, die nicht direkt auf die Sensoren oder die Kommunikationskanäle zwischen Geräten abzielen,

sondern stattdessen die Verarbeitung auf einem Steuergerät angreifen. Da die Sensorinformationen hier interpretiert werden und evtl. weitere Aktionen ausgelöst werden, besteht hier viel Potential für eine Manipulation. Eine angreifende Person könnte ein Steuergerät durch ein eigenes austauschen. Falls dies nicht erkannt wird, könnte das Gerät im Normalfall die Arbeit des originalen Steuergeräts übernehmen, aber zu einem beliebigen Zeitpunkt ein anderes Verhalten anwenden. Für diesen Angriffsvektor ist aber nicht zwangsläufig ein Hardware-Austausch notwendig. Stattdessen könnte auch die Firmware des Steuergeräts oder dessen Konfiguration, bspw. über eine (gegebenenfalls auch entfernt kontaktierbare) Wartungsschnittstelle, verändert werden. Ein weiterer Angriffsvektor besteht in manipulierten Software-Updates, auf die in einem späteren Kapitel näher eingegangen wird (vgl. Kapitel 0). Außerdem könnte beim Angriff eine Sicherheitslücke im Gerät ausgenutzt werden, um Daten zu verändern oder eigenen Code auszuführen. Hierbei ist eine große Bandbreite an Sicherheitslücken möglich, die sich je nach eingesetzter Technologie unterscheiden.

Zusätzliches Steuergerät in System integrieren (Integrität): Wie bereits in anderen Angriffsvektoren erwähnt, können zusätzliche Geräte im Rahmen eines MitM-Angriffs eingesetzt werden. Ein zusätzlich eingefügtes Gerät kann aber auch unabhängig davon eigene Nachrichten in einem Bussystem oder Netzwerk versenden und somit die Integrität eines Systems kompromittieren.

Steuergerät stören (Verfügbarkeit): Neben der Möglichkeit der Störung eines Sensors oder einer Kommunikation können auch Steuergeräte gestört werden. Das Gerät kann physikalisch zerstört werden oder die Stromzufuhr kann unterbrochen werden. Das Betreiben des Geräts außerhalb der Spezifikationen kann ebenfalls zu einem Ausfall oder zu Berechnungsfehlern führen. Auf der anderen Seite können Denial of Service Angriffe auch softwareseitig erfolgen, häufig durch die Ausnutzung einer Schwachstelle in einem Protokoll oder einer Implementierung. Dabei können bspw. durch entsprechend konstruierte Nachrichten auf dem jeweiligen Gerät aufwändige Berechnungen ausgelöst werden, die andere Prozesse verlangsamen, die Verarbeitung anderer Nachrichten verzögern oder den Prozess aufgrund zu hoher Speicheranforderungen abstürzen lassen. Ein Absturz kann jedoch unter Umständen auch durch einen Programmierfehler in der Implementierung verursacht und durch eine entsprechend konstruierte Nachricht ausgelöst werden. Zudem kann eine übermäßige Anzahl an Nachrichten oder Verbindungen (z. B. bei TCP) zu einem (temporären) Ausfall eines Dienstes führen.

Algorithmus oder KI-Modell stören: Unter dieser Kategorie ordnen sich verschiedene komplexe Angriffsvektoren ein, die auf Fehler in Algorithmen oder KI-Modellen abzielen. Hierbei kann grundlegend unterschieden werden zwischen Angriffen auf das Decision Making bzw. die Planung und Angriffen auf die Perception. Ein Angriff auf die Verfügbarkeit der Planung und Entscheidungsfindung könnte einen (autonomen) Zug stark verlangsamen oder sogar stoppen, während ein Angriff auf die Integrität ebendieser zu einer Fehleinschätzung einer Situation und somit zu einer Kollision führen kann. Angriffe auf KI-Modelle zur Verarbeitung von Sensordaten werden meist unter dem Begriff der „Adversarial Attacks“ zusammengefasst. Dabei werden gezielt Schwachstellen bei der durch die Modelle durchgeführten Klassifikation ausgenutzt, um entweder falsche Erkennungen (False Positive; ein Objekt wird der falschen Klasse zugeordnet) oder Nichterkennungen (False Negative; ein Objekt wird nicht erkannt bzw. der Hintergrundklasse zugeordnet) zu provozieren. Ein weiterer Angriffsvektor findet sich bei Multi-Sensor-Fusion (MSF), bei der gezielt Abweichungen durch Manipulation einer oder mehrerer Sensorwerte eingeschleust werden, um das Resultat in eine bestimmte Richtung zu beeinflussen. Die zuvor genannten Angriffe auf die Klassifikation sind ebenfalls bei MSF-Systemen relevant.

Im Folgenden werden die Angriffsvektoren, die sich nicht direkt aus der generalisierten Systemarchitektur ableiten lassen, wie bspw. *Angriffe auf KI-Systeme,* ergänzend erläutert und Hinweise dazu ergänzt.

8.2.3 Angriffe auf KI-Systeme und komplexe Sensoren

Im Folgenden werden einige Angriffe auf Machine Learning Modelle, sowie kombinierte Sensoren näher betrachtet. Die Literaturrecherche hierzu hat im Bereich von Angriffen auf solche Systeme in autonomen Fahrzeugen v. a. Veröffentlichungen mit dem Schwerpunkt Automobile identifiziert.

Shen et al. führten eine Systematisierung des bestehenden Wissens zu sogenannter „Semantic AI Security“ im Bereich des autonomen Fahrens durch, wobei sowohl Angriffe als auch Verteidigungsmaßnahmen beschrieben wurden [325]. Die Angriffe umfassen sowohl Perzeption mittels Kamera, Lidar, Radar sowie Multi-Sensor-Fusions-Systeme (MSF) als auch Lokalisierung mittels verschiedener Maßnahmen und weitere Kategorien wie „End-to-end driving“. Insgesamt wurden weitaus mehr Paper zu Angriffen als zu Verteidigungsmaßnahmen identifiziert. Außerdem wurde als Trend ein exponentielles Wachstum bei der Anzahl der veröffentlichten Paper zwischen 2017 und 2021 festgestellt, ebenfalls mit deutlichem Unterschied in der Anzahl zwischen Angriffs- und Verteidigungsveröffentlichungen, wobei ein Fokus auf sogenannte „top-tier venues“ gelegt wurde. Die Veröffentlichungen wurden in verschiedenen Dimensionen, wie Angriffsziel (IT-Sicherheitsschutzziel), Angriffsvektor und Evaluationsebene klassifiziert. Neben der geringen Anzahl an Verteidigungsmaßnahmen wurden weitere Forschungslücken identifiziert: Mangelnde Evaluation auf System-Ebene, wenige erforschte Angriffe auf Cyber-Sicherheitsebene (z. B. kompromittierte Systeme durch Malware, Exploits, oder Machine Learning Backdoors) sowie auf nachgelagerte Schritte (z. B. Vorhersage und Planung), geringe Untersuchung von anderen Schutzzielen neben der Integrität sowie geringe Bereitschaft zur Beteiligung an Open Source Veröffentlichungen.

Zhao et al. beschreiben verschiedene „Adversarial Attacks“, die entweder auf das Verstecken eines Objekts („Hiding Attack“) oder das Fehlerkennen eines Objekts („Appearing Attack“) bei einer visuellen Perzeption (Kamera) mittels „Adversarial Examples (AE)“ abzielen [326]. Die Angriffe wurden dabei auch unter realistischen Bedingungen untersucht und auf diese optimiert. Im konkreten Beispiel wurden Stoppschilder durch Aufkleber ergänzt (Hiding) bzw. durch Attrappen ersetzt (Appearing). Aus menschlicher Sicht wären die Aufkleber für die Erkennung als Stoppschild irrelevant bzw. die Attrappen würden nicht als „normales“ Stoppschild verstanden werden. Durch die Einführung weiterer Nebenbedingungen in das Optimierungsverfahren können auch verschiedene Muster, Formen, Farben oder Text erzeugt werden („Style-customized AEs“), die weiterhin in der Lage sind, das Modell zu täuschen. Dadurch können Aufkleber bzw. Attrappen für Menschen bspw. als Vandalismus oder Werbung getarnt werden. Außerdem wurden die Erfolgsraten eines Angriffs unter verschiedenen Wetterbedingungen, Abständen und Winkeln getestet, wobei Hiding Attacks vor allem in höherer Distanz erfolgreich waren und Appearing Attacks vor allem in der Nähe (jedoch auch wetterabhängig). Es wurde zudem auch die Übertragbarkeit der Angriffe auf andere Modelle (Blackbox) untersucht, da der Optimierungsprozess auf Basis der Gewichte des jeweiligen Modells (White-box) durchgeführt wird. Dabei wurde bei einem bestimmten White-box Modell eine hohe Übertragbarkeit von über 90 % (bei fast allen Blackbox Modellen) festgestellt. Dies bedeutet, dass für die Durchführung eines erfolgreichen Angriffs nicht zwangsläufig der Zugriff auf die Gewichte des jeweiligen KI-Modells benötigt wird. Weiterhin werden verschiedene potenzielle Verteidigungsmechanismen vorgestellt, die jedoch bisher keine abschließende Lösung darstellen.

Es existieren jedoch auch Angriffe auf andere Sensoren. So untersuchten Cao et al. Adversarial Attacks auf Lidar-basierte Perzeption, wobei eine gefälschte Lidar-Antwort mittels einer Verzögerungskomponente und eines Lasers erzielt wurde [327]. Als simulierte Beispiele wurden eine Notbremsung durch ein plötzlich erscheinendes, nicht existentes Hindernis sowie die Verhinderung der Weiterfahrt an einer Ampel durch vorgetäuschte Hindernisse genannt. Während die genannten Angriffe einen White-Box-Zugang durch die angreifende Person voraussetzen, entwickelten Sun et al. einen Black-Box-Angriff, bei

dem nur wenige Punkte (≤ 200) verändert werden müssen [328]. Dabei wurde festgestellt, dass Punktwolken von verdeckten oder entfernten Objekten, wenn sie in Richtung des Scanners verschoben werden, weiterhin durch die verwendeten Modelle als solche erkannt werden. Außerdem werden von Sun et al. zwei Verteidigungsmaßnahmen, basierend auf Anomalie-Detektion, vorgeschlagen [328]. Shin et al. [329] zeigten, dass neben der Möglichkeit durch Spoofing Punkte näher am Sensor erscheinen zu lassen, ein weiterer Angriff in der Ausreizung der Sensor-Sättigung, d. h. in der Verstärkung des Laser-Signals, besteht, um die Verfügbarkeit des Sensors einzuschränken.

Auch Systeme, die auf Multi-Sensor-Fusion basieren, können angegriffen werden. Diese wird bspw. in der Lokalisierung eines Fahrzeugs eingesetzt. Shen et al. untersuchten Angriffe mittels GPS-Spoofing auf die MSF-Lokalisierung (Light detection and ranging (LiDAR), IMU und GPS) eines Fahrzeugs [330], um einen gezielten seitlichen Drift zu erzeugen, und das Fahrzeug somit aus der Spur zu bringen bzw. in den Gegenverkehr zu lenken. Während eine exakte Übertragung des Angriffs auf den Schienenverkehr unwahrscheinlich erscheint, könnte eine gezielte Abweichung der Lokalisierung auch hier Probleme verursachen, etwa einen fehlinterpretierten Gleiswechsel, oder eventuell auch die Verschiebung in Längsrichtung, wodurch evtl. andere Fahrzeuge vor bzw. hinter dem angegriffenen Fahrzeug in einem Moving Block Szenario zusätzliche Sicherheitsabstände einhalten müssen bzw. diese Abstände verletzt werden. Der untersuchte Angriff zeigt, dass es grundsätzlich auch möglich ist, gezielte Abweichungen in MSF-basierte Lokalisierungen einzuschleusen.

Ein anderer Angriff konnte ebenfalls eine Hinderniserkennung basierend auf einer Kombination aus Kamera-Bildverarbeitung und LiDAR durch Konstruktion gezielter „Adversarial 3D objects“ täuschen, um physisch existente Hindernisse vor der Erkennung zu verstecken [331]. Dadurch können Kollisionen des Hindernisses mit dem autonomen Fahrzeug hervorgerufen werden. Im konkreten Beispiel wurden 3D-gedruckte Objekte hergestellt, die durch ihre spezielle Form zur gleichen Zeit weder durch die Bildverarbeitungsmodelle noch durch die verwendete LiDAR-Verarbeitungspipeline erkannt werden konnten. Die Objekte können dabei für Menschen auf den ersten Blick unscheinbar wirken – im Beispiel wurde ein Verkehrsleitkegel mit rauer Oberfläche sowie ein Objekt ähnlich eines größeren Steins konstruiert. Das Erstellen passender Adversarial Objects basiert auch hier auf einem (gradientenbasierten) Optimierungsverfahren. Es wurden außerdem unterschiedliche Verteidigungsmechanismen untersucht. Für Modelle basierend auf Deep Neural Networks (DNNs) wurden verschiedene Ansätze basierend auf Transformation der Eingabedaten oder Augmentierung der Trainingsdaten untersucht, jedoch konnte das effektivste Verfahren (Median Smoothing der Eingabedaten) die Angriffserfolgsrate lediglich auf 66 % reduzieren, ohne die normale Erkennungsrate zu beeinträchtigen. Als weitere Möglichkeiten zur Verteidigung wird das Hinzufügen weiterer Sensorquellen, bspw. zusätzlicher Kameras mit veränderter Perspektive oder andere Sensorarten wie ein RADAR genannt, die jedoch den Angriff nur erschweren, aber nicht verhindern können und gleichzeitig die Kosten erhöhen.

Abschließend sind noch Angriffe auf die Planungs- bzw. Entscheidungsalgorithmen zu betrachten. Dabei sind grundlegend zwei verschiedene Angriffsklassen zu nennen: Verursachen von zu konservativer Fahrweise (Notbremsung oder Verweigerung der Weiterfahrt) oder von zu aggressiver Fahrweise (Kollision mit Hindernissen) [332]. Wan et al. untersuchten dabei speziell die zu konservative Fahrweise, die etwa durch gezielte Platzierung von Hindernissen oder Fahrzeugen verursacht werden kann [332]. Hier werden insbesondere Eigenschaften der Planungsalgorithmen angegriffen, die häufig noch durch expliziten Programmcode (statt gelerntem Verhalten) implementiert werden. Als Beispiel wird eine Schwachstelle genannt, bei der Hindernisse außerhalb der Fahrbahn stehen und es bei normaler Weiterfahrt zu keiner Kollision kommen sollte, dennoch führt diese spezielle Anordnung der Hindernisse zur Verhinderung der Weiterfahrt. Die Ursache in diesem Beispiel ist, dass der Algorithmus um die erkannten Hindernisse herum einen (konstanten) Sicherheitspuffer einplant, und bei dieser Anordnung die eingeplante Breite des Fahrzeugs den Bereich inkl. der Sicherheitspuffer beider Hindernisse überschreitet. Ein weiteres Problem im untersuchten Algorithmus war, dass sich die Längspositionen der beiden Hindernisse auch um bis zu fünf Meter versetzt befinden konnten, sodass für einen Menschen die Ursache

des Stopps nicht direkt erkennbar wäre. Wan et al. entwickelten zum Aufspüren solcher Schwachstellen einen Fuzzing-Ansatz basierend auf Evolutionären Algorithmen, der (mit Zugriff auf den Quelltext des Planers) in der Lage ist, eine Reihe solcher angreifbaren Konfigurationen automatisiert zu finden.

Eine Einschränkung einiger der genannten Angriffe ist meist, dass diese lediglich auf offenen Modellen bzw. Plattformen, wie bspw. der Apollo Autonomous Driving Platform von Baidu evaluiert wurden, da diese unter einer Open Source Lizenz verfügbar sind und somit von Sicherheitsforschenden untersucht werden können. Jedoch sollte daraus nicht geschlossen werden, dass proprietäre Systeme weniger angreifbar wären. Zum einen sollte die Sicherheit eines Systems nicht allein durch einen „Security by Obscurity“ Ansatz verteidigt werden. Zum anderen wurde in der Vergangenheit bereits mehrfach gezeigt, dass dennoch auch Sicherheitslücken in geschlossenen Systemen gefunden werden können, die entsprechende Motivation vorausgesetzt. Bereits im oben genannten Beispiel wurde bspw. die Übertragbarkeit von White-Box Angriffen mittels Adversarial Examples auf Black-Box-Modelle beschrieben.

8.2.4 Sicherheit von IoT-Protokollen

Da Sensornetzwerke auch als Teil des IoT gesehen werden können, sind auch die dort verwendeten Protokolle und Architekturen im Bahnbereich durchaus relevant. Interviews mit relevanten Stakeholdern zeigten, dass IoT-Protokolle wie MQTT und OPC UA bereits im Einsatz sind. Bezüglich OPC UA kann an dieser Stelle bereits auf die vom BSI durchgeführte Sicherheitsanalyse [333] verwiesen werden. Auch zu MQTT [334][335][336][337] und anderen Protokollen [338][339] wurden bereits umfangreiche Untersuchungen durchgeführt.

Da auch im Bahnbereich eine große Bandbreite von IoT-Protokollen eingesetzt wird, wird im Folgenden eine Übersichtsstudie genutzt, die Gemeinsamkeiten der Protokolle abstrahiert. Hierzu führten Tournier et al. eine Meta-Studie zu IoT-Protokollen unterschiedlicher OSI-Schichten, insbesondere mit Hinblick auf Sicherheitsschwachstellen, durch [340]. Dabei wurden die Architekturen in einem generischen IoT-Stack eingeordnet, sowie die Schwachstellen innerhalb einer IoT-Kill-Chain organisiert und von den zugrundeliegenden Protokollen abstrahiert. Die dadurch identifizierten generischen Angriffe lassen sich somit voraussichtlich auch auf zukünftige IoT-Architekturen anwenden, sofern diese dem abstrakten IoT-Stack folgen. Die Kill-Chain besteht dabei aus den drei Schritten „Beobachten und Manipulieren von Paketen“ – Paket-Fokus (aktive und passive kryptografische Angriffe), „Verändern der Topologie“ – Protokoll-Fokus (MitM-, Flooding-, Spoofing-, Sybil-, Wormhole-Angriff) und „Kompromittieren des Systems“ – System-Fokus (Sinkhole- und Selective-Forwarding-Angriff). Die verschiedenen von Tournier et al. beschriebenen Angriffe werden im Folgenden zusammengefasst [340]:

- *Passive (kryptografische) Angriffe* zeichnen sich dadurch aus, dass lediglich die Kommunikation aufgezeichnet wird, ohne aktiv daran teilzunehmen. Es handelt sich hierbei vor allem um Angriffe auf die Vertraulichkeit. Im einfachsten Fall ist die Kommunikation nicht verschlüsselt (*no cryptography*), sodass bei einem Angriff alle übertragenen Informationen abgegriffen werden können. Eine andere Ausprägung ist gegeben, wenn etwa schwache kryptografische Algorithmen oder geringe Schlüssellängen eingesetzt werden, für die mittlerweile Angriffe praktikabel sind (*ugly cryptography*). Alternativ kann auch die Implementierung der Algorithmen verwundbar sein (*bad cryptography*), bspw. durch Mängel bei der Schlüsselgenerierung (z. B. unsichere Zufallsgeneratoren, hardkodierte Schlüssel oder Initialisierungsvektoren), Schlüsselaustausch oder durch Seitenkanalangriffe. Auch bei Verwendung moderner Kryptografie und korrekter Implementierung, können weiterhin passive Angriffe möglich sein, etwa durch Ableitung von Informationen über Metadaten der Kommunikation (Größe, Zeitstempel etc.).
- *Aktive kryptografische Angriffe* erfordern ein aktives Eingreifen in die Kommunikation, bspw. durch Einschleusen zusätzlicher oder Manipulieren gesendeter Pakete.

    - *Same-nonce Angriff:* Bei Wiederverwendung einer Nonce (Number used once), ggf. ausgelöst durch einen vorherigen Fehlerzustand, kann die Sicherheit eines kryptografischen Protokolls untergraben werden, bspw. könnten Daten entschlüsselt werden.
    - *Replay Angriff:* Übermittelte Pakete können bei einem Angriff erneut gesendet werden, wodurch bspw. zuvor legitim durchgeführte Aktionen wiederholt werden können. Eine vorherige Entschlüsselung der Pakete ist für einen erfolgreichen Angriff nicht notwendig.
    - *Malleability Angriff:* Hierbei werden Same-nonce und Replay Angriff kombiniert – Über Nonce-reuse ist es möglich einen Keystream zu erhalten, mit dem sich neue Pakete verschlüsseln lassen. Bei einem Angriff können daher Pakete mit neuen (nicht zuvor gesendeten) Daten erstellt und verschlüsselt werden.
- *Man-in-the-Middle (MITM) Angriffe* fügen transparent ein neues Gerät in eine bestehende Kommunikation als Zwischenstelle ein. Ziel ist dabei, dass der Eingriff für die kommunizierenden Geräte nicht erkannt wird, sodass diese davon ausgehen direkt mit dem jeweiligen Ziel zu kommunizieren. Sämtliche Nachrichten von Gerät A zu Gerät B, als auch in die entgegengesetzte Richtung, werden zunächst vom angreifenden Gerät C empfangen, können dort verändert und weitergeleitet oder verworfen werden. Auch kryptografische Protokolle können dabei angegriffen werden, bspw. wenn die Geräte-Identitäten nicht korrekt geprüft werden. Das MITM-Gerät kann sich dann gegenüber Gerät B als Gerät A ausgeben und andersherum, die Kommunikation entschlüsseln und anschließend wieder für das nächste Gerät verschlüsseln. Auch bei korrekt geprüften Identitäten und Verschlüsselung, kann ein solches MITM-Gerät dennoch die Kommunikation stören (Verfügbarkeit), indem Nachrichten verworfen werden.
- *Flooding Angriff:* Eine hohe Anzahl von Anfragen werden an ein Gerät gesendet, um dessen Verfügbarkeit einzuschränken (Denial of Service). Eine Dienstunterbrechung kann auch zu weiteren (automatisierten) Maßnahmen führen, die weitere Angriffe ermöglichen.
- *Spoofing* Angriff: Das angreifende Gerät gibt vor ein anderes Gerät zu sein, und kann somit Aktionen im Namen dieses Geräts ausführen. Dies kann auch für Angriffe auf die Verfügbarkeit genutzt werden, z. B. in dem Geräte deregistriert werden oder angewiesen werden die Verbindung zu trennen.
- *Sybil Angriff:* Ein Gerät simuliert viele verschiedene Identitäten und hat dadurch einen größeren Einfluss auf das Netzwerk bzw. Routing.
- *Wormhole Angriff:* Dies ist ebenfalls ein Angriff auf das Routing, bei dem zwei Geräte eine vorgeblich sehr kurze/schnelle Route („Tunnel“) zwischen zwei Zonen zur Verfügung stellen, und dadurch für die Weiterleitung von Nachrichten bevorzugt werden.
- *Sinkhole Angriff:* Bei diesem Angriff wird ein Gerät für andere Geräte als Zentraler Knoten dargestellt (z. B. durch Manipulation von Routing-Nachrichten/einer Routing-Metrik), sodass sämtlicher Traffic durch das Angriffsgerät geleitet wird.
- *Selective-forwarding Angriff*: Ein kompromittiertes oder hinzugefügtes Gerät leitet nur bestimmte Pakete weiter. Der Angriff wird u. U. nicht erkannt, wenn bspw. Routing-Nachrichten weiterhin weitergeleitet werden.

Ebenfalls sollte beachtet werden, dass Geräte in Zukunft kompromittiert werden könnten, weshalb es auch nachträglich möglich sein sollte, diese gegebenenfalls als nicht vertrauenswürdig auszuschließen. Eine ähnliche Anforderung stellen End-of-Life Geräte dar, die ausgemustert werden. Hierbei sollte sichergestellt werden, dass auf den Geräten vorhandene Daten sicher gelöscht werden bzw. dass kryptografisches Material (Schlüssel, Kennwörter, Zertifikate) nutzlos wird, sodass diese Geräte nicht mehr im bestehenden Netzwerk kommunizieren können.

8.2.5 Sichere Software-Updates

Bei softwarebasierten Systemen ist es aufgrund der Weiterentwicklung des Gesamtsystems und insbesondere wegen neu identifizierter Sicherheitslücken im Hinblick auf Cybersecurity unabdingbar Software- bzw. Firmware-Updates durchzuführen. Komplexe Software ist nicht fehlerfrei und hat meist viele Abhängigkeiten unterschiedlichster Hersteller.

Für die Softwareentwicklung bedeutet dies, dass Abhängigkeiten verwaltet und überwacht werden müssen, sodass Schwachstellen rechtzeitig erkannt werden und Updates zeitnah an die produktiven Systeme ausgeliefert werden können. Hierfür sollte eine Software Bill Of Materials (SBOM) in den Softwareentwicklungsprozess integriert werden und regelmäßig und zeitnah auf veraltete Abhängigkeiten und Schwachstellen geprüft werden. Ein Beispiel hierfür ist der OWASP CycloneDX-Standard [341].

Weiterhin müssen die Geräte in der Lage sein, regelmäßig und zeitnah Updates zu erhalten. Dies erfordert die Möglichkeit Updates im Produktivsystem zu installieren, als auch diese über einen geeigneten Transportweg zu erhalten. Updates können neben aktualisierter Software auch geänderte Konfigurationen und andere Daten enthalten. Geräte, die nicht aktualisiert werden können, stellen auf Dauer ein Sicherheitsrisiko dar und könnten gegebenenfalls die Sicherheit des Systems als Ganzes untergraben. Erhält ein Gerät keine Updates mehr, so steigt das Risiko, dass nicht behobene Schwachstellen ausgenutzt werden, weshalb in einem solchen Fall ein Austausch des Geräts durch ein weiterhin aktualisierbares Gerät in Betracht gezogen werden sollte. Zur Sicherstellung der Robustheit müssen fehlgeschlagene Installationen in einen stabilen Zustand wiederhergestellt werden können. Ein Update darf jedoch auch nicht durch einen Angriff unbegrenzt lange verhindert werden können bzw. muss dieser durch entsprechende Systeme frühzeitig erkannt und gemeldet werden. Weiterhin ist die Skalierbarkeit zu beachten, damit alle Geräte die Aktualisierungen zeitnah erhalten, ohne die Update-Infrastruktur zu überlasten. Updates müssen zudem auf ihre Integrität geprüft werden und Manipulationen müssen erkannt, gemeldet und verhindert werden.

Für Software-Updates existieren bereits einige Standards und Verfahren, wie bspw. im OMA Lightweight M2M Protokoll [342] oder die Arbeiten der IETF Working Group SUIT (Software Updates for the Internet of Things) [343]. Einen resilienteren Standard bietet The Update Framework (TUF) [344]. Der Standard wurde bereits mehreren Security-Audits unterzogen und wird bereits von mehreren Unternehmen und Diensten eingesetzt bzw. Ideen aus TUF wurden und werden in die Update-Infrastruktur integriert. Auf der TUF-Website werden einige Beispiele genannt, u. a. Automotive Grade Linux [345], Airbiquity OTAmatic [346], Google Fuchsia [347] (Betriebssystem), HERE Technologies [348] sowie beginnende Umsetzungen bei Haskell, Python Package Index, PHP und OCaml. Auch in der Paketverwaltung APT von Debian-basierten Linux-Systemen flossen bereits einige Verbesserungen aus den Erfahrungen von TUF mit ein [349].

Eine zentrale Annahme von TUF ist, dass kryptografische Schlüssel die länger im Einsatz sind, irgendwann kompromittiert werden können. Im Falle eines klassischen Update-Systems, bei dem die Geräte die Software mithilfe eines zuvor bekannten öffentlichen Schlüssels prüfen, führt dies zu einem katastrophalen Versagen des Systems, da Angreifende mit einem kompromittierten Schlüssel eigene Updates signieren und installieren können und somit die Sicherheit des Systems vollständig untergraben ist. Bei TUF werden jedoch noch weitere Angriffe bzw. Schwachstellen berücksichtigt [350]:

- *Installation beliebiger Software:* Ein Angriff erlaubt es Download-Anfragen mit beliebigen Dateien zu beantworten, die vom Client nicht als illegitim erkannt werden und daher installiert werden.

- *Rollback attacks:* Durch einen Angriff wird ein Client auf alte Dateien (Software mit potenziellen Sicherheitslücken) verwiesen, obwohl der Client bereits neuere Dateien gesehen hat, aber ohne Möglichkeit dies zu prüfen installiert der Client diese Dateien dennoch.
- *Fast-forward attacks:* Bei einem Angriff wird die aktuelle Versionsnummer in den Update-Metadaten so weit erhöht, dass alle legitimen Updates als Rollbacks zu alten Versionen erscheinen. In manchen Szenarien kann die Versionsnummer eines Updates auch auf den maximal möglichen Wert gesetzt werden, wodurch Updates für immer verhindert werden.
- *Indefinite freeze attacks:* Bei diesem Angriff werden dem Client weiterhin Dateien präsentiert, die dieser bereits gesehen hat, obwohl neue Dateien existieren, wodurch der Client keine weiteren Updates mehr erhält.
- *Endless data attacks:* Eine Download-Anfrage wird mit einem endlosen Datenstrom beantwortet, wodurch die Verfügbarkeit des Clients gefährdet wird (gefüllter Arbeitsspeicher oder persistenter Speicher).
- *Extraneous dependencies attacks:* Bei diesem Angriff werden dem Client zusätzliche Abhängigkeiten zu einer Software angegeben. Die Software muss zwar aus einer vertraulichen Quelle stammen, kann aber dennoch Schwachstellen besitzen, die ausgenutzt werden können.
- *Mix-and-match attacks:* Bei diesem Angriff werden mehrere Stände des Update-Repositories kombiniert, um Dateien auszusenden, die in dieser Kombination nie zusammen ausgeliefert werden sollten. Dadurch können bspw. veraltete Abhängigkeiten installiert werden.
- *Wrong software installation:* Es werden andere vertrauenswürdige Dateien ausgesendet als jene, die vom Client angefragt wurden.
- *Malicious mirrors preventing updates:* Die angreifende Partei hat vollständige Kontrolle über einen Update-Mirror und kann verhindern, dass Clients Updates anderer (nicht-bösartiger) Mirror abrufen.
- *Vulnerability to key compromise:* Bei einem Angriff genügt es einen einzelnen kryptografischen Schlüssel (Single-Key-System) oder weniger als einen gegebenen Schwellwert an Schlüsseln zu kompromittieren, um Clients zu kompromittieren. Z. B. liegt eine solche Angriffsmöglichkeit vor, wenn die Sicherheit lediglich von einem einzelnen Online-Schlüssel (z. B. alleinige Absicherung durch TLS) oder einem einzelnen Offline-Schlüssel (z. B. bei den meisten auf Signaturschlüsseln basierenden Software-Updates) beruht.

Der TUF-Standard [351] ergreift Gegenmaßnahmen gegen sämtliche der gelisteten Angriffe, was bei korrekter Umsetzung im Gegensatz zu üblichen Software-Update-Systemen ein sehr hohes Sicherheitsniveau ermöglicht. Hierfür setzt TUF auf verschiedene Rollen (Root, Targets, Snapshot, Timestamp) mit jeweils unterschiedlichen Zuständigkeiten und Sicherheitsniveaus. Im Update-Repository werden zusätzlich Metadaten gehalten, die von der jeweils zuständigen Rolle kryptografisch signiert sind. Die Root-Rolle ist über ihre Metadaten-Datei für die Zuweisung der Schlüssel aller untergeordneten Rollen zuständig, weshalb die Root-Schlüssel nur offline und vergleichsweise selten genutzt werden sollten und in einem entsprechend hohen Sicherheitsniveau (z. B. in einem TPM) gehalten werden sollten. Da eine Kompromittierung der Root-Rolle die Kompromittierung des Gesamtsystems bedeutet, empfiehlt es sich ihr mehrere Keys in einem Thresholded-Signature-Verfahren zuzuordnen, sodass mehrere Parteien erforderlich sind. Im Falle einer anderen kompromittierten Teilmenge von Rollen kann die Root-Rolle die Integrität des Systems wiederherstellen, indem die Keys der kompromittierten Rollen ersetzt werden. Die Verteilung schädlicher Software-Updates ist nur durch die Kompromittierung aller drei untergeordneten Rollen (oder der Root-Rolle) möglich. In der durch die Targets-Rolle signierten Targets-Datei werden die konkreten Update-Dateien (z. B. Firmware-Images) mit ihren kryptografischen Hash-Werten und Dateigrößen gelistet. Bei Bedarf sind auch untergeordnete Targets-Rollen, sogenannte Delegated Targets, für bestimmte Pfade möglich. Die Snapshot-Metadatendatei (signiert durch Snapshot-Rolle) gibt die zum jeweiligen Zeitpunkt aktuellen Versionsnummern der anderen Metadaten-Dateien (außer der Timestamp-Datei) an, um sicherzustellen, dass ein Client nur einen konsistenten Zustand des Repositories akzeptiert. Die Timestamp-Datei (signiert durch Timestamp-Rolle) gibt die kryptografischen Hashwerte und Dateigröße der Snapshot-Datei an. Jede Metadaten-Datei hat ein Ablaufdatum

und muss somit vor Ablauf dieses Datums erneut signiert bzw. ersetzt werden. Die Timestamp-Datei hat jedoch die geringste Ablaufzeit und wird dementsprechend mit Online-Keys automatisiert regelmäßig neu signiert, um die Aktualität des Repositorys anzuzeigen und somit Freeze attacks entgegenzuwirken. Die Trennung auf verschiedene Rollen mit unterschiedlichen Sicherheitsniveaus erschwert es das Update-Repository zu kompromittieren. Eine Auswertung, welche Auswirkung die Kompromittierung einer (Kombination von) Rolle(n) hat, findet sich im TUF-Paper [352].

Für den Automobil-Sektor wurde außerdem Uptane [353][354], eine Variante von TUF, adaptiert, um den speziellen Anforderungen, insbesondere in Bezug auf eingebettete Steuergeräte, gerecht zu werden. Hierfür wird u. a. das Update-Repository in zwei Repositories aufgeteilt. Ein weiteres wichtiges Element ist die Möglichkeit für Steuergeräte die aktuelle Uhrzeit aus einer sicheren Quelle zu erhalten. In Update wird außerdem die Möglichkeit genannt, lediglich eine partielle Verifikation der Updates durchzuführen, bei der die Signatur der Metadaten, aber nicht die Hashwerte der Dateien überprüft werden. Diese partielle Verifikation ist jedoch nicht zu empfehlen und sollte vermieden werden, da ansonsten eventuell manipulierte Dateien installiert werden könnten.

Eine Weiterentwicklung von Uptane angepasst auf Züge wurde in [355] vorgestellt. Zusätzlich zu den Zielen aus Uptane werden außerdem die Aktualisierung unterschiedlicher Geräte, die Integration einer Testphase sowie der Zustimmung eines Kontrollgremiums (Control Board) im Rahmen der Safety-Regulatorien durchgeführt. Eine weitere Adaption bietet ASSURED [356], bei dem Uptane in Verbindung mit Geräte-Integritätsmechanismen wie Boot Integrität und Remote Attestation kombiniert werden.

Ein weiteres Problem neben der allgemeinen Verteilung von Software-Updates stellen Supply Chain Angriffe dar. Die ENISA definiert Supply Chain Angriffe wie folgt (übersetzt aus [357]): „Ein Supply Chain Angriff ist eine Kombination aus mindestens zwei Angriffen. Der erste Angriff zielt auf einen Zulieferer ab, der dann genutzt wird, um das eigentliche Ziel anzugreifen und Zugriff auf dessen Assets zu erhalten. Das Ziel kann die Endkundin oder der Endkunde sein oder ein anderer Zulieferer. Damit ein Angriff also als Supply Chain Angriff klassifiziert werden kann, müssen sowohl Zulieferer als auch Kundin oder Kunde Ziele sein.“ Zu diesem Thema sei auf eine aktuelle Studie der ENISA [358] verwiesen.

8.2.6 Sicherheit bei cloudbasierten Software-Architekturen

Heutige IT-Architekturen sind häufig cloudbasiert, weshalb Cloud-Sicherheit ein generelles Thema in der IT-Sicherheit darstellt. Daher verweisen wir an dieser Stelle auf aktuelle Studien zu Schwachstellen in Cloud-Architekturen [359][360].

Neben diesen Aspekten, die sich generell beim Einsatz von Cloud-Diensten ergeben und breit untersucht und dokumentiert sind, ist besonders die aktuell häufig cloudbasierte Software-Entwicklung ein weiterer wichtiger Aspekt, da im Bereich des Schienenverkehrs häufig spezifische Softwarelösungen eingesetzt werden. Hinsichtlich potenzieller Sicherheitslücken ist es wichtig Best Practices in der Software-Entwicklung, bei der Implementierung, bei der Konfiguration und im Betrieb umzusetzen und regelmäßig gegen den Stand der Technik zu prüfen.

In der Software-Entwicklung empfiehlt sich Continuous Integration, der umfangreiche Einsatz von Unit- und Integrationstests, statische („Linter“) und dynamische Codeanalyse (z. B. Fuzzing) und Code-Metriken (Komplexitätsmaße, Code Coverage) oder Überwachung anderer Aspekte wie „Technical Debt“ oder „Code-Smells“, sowie Code Reviews und die Umsetzung entsprechender Verbesserungen. Außerdem sollten Secure Coding Praktiken im Entwicklungsteam gelebt werden. Hierunter fällt bspw. der Grundsatz, dass Eingabedaten grundsätzlich nicht vertraut werden kann und sie deshalb validiert werden müssen oder dass Daten, von denen nicht bewiesen werden kann, dass sie aus einer sicheren Quelle stammen, als ebensolche Eingabedaten behandelt werden sollten. Generell sollte sich das Team kontinuierlich mit dem Stand der Technik vertraut machen und die Systeme in einem Security by Design

Prozess entwickeln, d. h. Sicherheit nicht als nachgelagerten Schritt bzw. Priorität betrachten, sondern Sicherheit von Anfang an als wichtige Qualität des Systems priorisieren. Ein weiteres Element stellt die Überwachung von Abhängigkeiten, insbesondere auf bekannte Schwachstellen (CVEs [361]), und die zeitnahe Aktualisierung bzw. Anwendung von Patches, dar.

Für Web-Anwendungen existieren bspw. mit den OWASP Top 10 [362] eine Übersicht der aktuell kritischsten Kategorien von Sicherheitslücken, die unterstützen können, eine entsprechende Awareness im Softwareentwicklungsteam zu schaffen. Die aktuelle Version von 2021 [362] enthält ebenfalls eine Auflistung der zu den jeweiligen Schwachstellen relevanten Common Weakness Enumerations (CWEs) [363] sowie Referenzen zu entsprechenden Best Practices. Weiterhin ist auch die OWASP Cheat Sheet Series [364] zu nennen, die für viele Themen eine umfangreiche Beschreibung aktueller Best Practices auf dem jeweiligen Gebiet bietet. Neben webspezifischen Sachverhalten werden auch angrenzende Aspekte, wie Docker, Kubernetes, Microservices sowie sichere Cloud-Architekturen oder Threat-Modelling-Ansätze beschrieben.

Neben der Implementierung ist auch die Konfiguration von Software bzw. Cloud-Lösungen potentiell für Sicherheitsprobleme anfällig. Ein klassisches Beispiel in der Vergangenheit sind unzureichend konfigurierte Cloud-Speicher-Systeme (z. B. Amazon S3), bei denen die Berechtigungen nicht ausreichend eingeschränkt wurden (CWE-306: Missing Authentication for Critical Function [365]). Continella et al. führten hierzu eine umfangreiche Analyse durch [366]. Ähnliche Probleme fanden sich u. a. auch bei NoSQL-Datenbanken [367] und anderen Server-Diensten [368]. Speziell hinsichtlich Kubernetes wurde auch kürzlich eine Studie von Rahman et al., mit dem Ziel Kubernetes Fehlkonfigurationen zu identifizieren, durchgeführt [369].

Das erfolgreiche Ausnutzen von Sicherheitslücken kann auch durch entsprechende Defense-in-Depth-Ansätze erschwert werden. Grundlegend können Web Application Firewalls (WAF), Intrusion Detection/Prevention Systeme (IDS/IPS) bzw. Security Information and Event Management (SIEM) Systeme zum Einsatz kommen, um Angriffe zu erkennen und ggf. zu unterbinden. Diese bieten allerdings keinen vollständigen Schutz und sollten nur als Ergänzung und nicht als Ersatz für die genannten Sicherheitsmaßnahmen betrachtet werden. Bspw. können neuartige Angriffe auch aus Sicht eines solchen Systems wie eine normale Interaktion mit dem Dienst erscheinen. Im Rahmen von Security by Design sollten auch Privilegien von Diensten auf das Minimum reduziert werden (Principle of Least Privilege), bzw. nach Zwecken separiert werden. Ein Einschränken (Sandboxing) von Prozessen bzw. Laufzeitumgebungen auf das notwendige Minimum mithilfe entsprechender Policies (z. B. unter Linux mittels seccomp, AppArmor, SELinux etc.) kann ebenfalls die Systemsicherheit stärken und Angriffe erschweren. Auch hier sind jedoch unter Umständen weiterhin Angriffe möglich, da die Prozesse weiterhin bestimmte Berechtigungen benötigen und somit Zugriff auf entsprechende Ressourcen (auch bei einem Angriff) besteht. Systeme sollten sich untereinander nicht ohne Prüfung vertrauen (Zero Trust), d. h. die Authentizität sollte geprüft werden und Angriffe auf die Integrität einer Kommunikation sollten erkannt werden. Ein weiteres Element ist das Sicherstellen der Vertraulichkeit der Übertragung, u. a. wenn schützenswerte Daten oder Geheimnisse wie Credentials anderenfalls im Klartext übertragen würden.

Wenn bereits, wie zuvor dargestellt wurde, ein umfassendes Security by Design Konzept etabliert ist, kann es sinnvoll sein, ergänzend die folgenden weiteren Elemente einzusetzen: Vor allem in Bezug auf kritische Infrastruktur, kann das regelmäßige Durchführen von Penetration Tests durch einen externen Dienstleister sinnvoll sein, um Schwachstellen frühzeitig aufzuspüren und das Vertrauen in die eigene Software-Qualität zu stärken. Bug Bounty Programme können ein weiterer Ansatz sein, um Anreize zu schaffen, gefundene Schwachstellen an den Hersteller zu übermitteln.

8.2.7 Maßnahmen

Während einige Maßnahmen bereits in Kapitel 8.2.6 beschrieben wurden, wird im Folgenden eine Übersicht über mögliche Maßnahmen zur Verbesserung der IT-Sicherheit von Sensorsystemen im Zug dargestellt. Eine tabellarische Übersicht der Maßnahmen ist in Tabelle 120 zu finden. Tabelle 121 ordnet den Angriffsvektoren entsprechende Maßnahmen zu. Diese lassen sich grob in die Bereiche „Physischer Schutz“ (M.1), „Geräte-Sicherheit (Software)“ (M.3), „Kommunikations-Integrität/Authentizität“ (M.2), „Gegenmaßnahmen Sicherheitslücken“ (M.4), „Gegenmaßnahmen Denial of Service“ (M.5), „Netzwerksicherheit“ (M.6), „Gegenmaßnahmen KI-Angriffe“ (M.7) und „Maßnahmen für komplexe Sensoren“ einordnen (M.8).

Ein besonders wichtiger Aspekt ist der Bereich „Physischer Schutz“ (M.1), v. a. in Hinblick auf die Infrastruktur im öffentlichen Raum. Sensorsysteme im Zug unterscheiden sich von Systemen wie etwa Server in Rechenzentren, die nicht mobil sind und physisch relativ gut geschützt werden können. Eine physische Nähe zum System ist zur Nutzung in der Regel nicht erforderlich, der zu schützende Bereich ist häufig lokal begrenzt und nicht mobil, und vielfältige Zugangsbeschränkungen und Kontrollen sind möglich. Insbesondere Sensoren benötigen jedoch aus Prinzip häufig einen direkten Kontakt zur überwachten Umgebung (z. B. im oder am Zug), sodass diese für Manipulationen und Störungen jeglicher Art anfälliger sind als es stationäre, überwachte und geschützte Systeme wären. Somit unterscheidet sich auch der Schwierigkeitsgrad des Zugriffs im Angriffsfall auf Sensoren im Vergleich zu bspw. Steuergeräten, die keinen direkten Kontakt zur Außenwelt erfordern. Eine Ausnahme bildet möglicherweise die physische Vernetzungsinfrastruktur (u. a. Glasfaser), die prinzipiell auch bei Rechenzentren eine ähnliche Verwundbarkeit aufweisen dürfte. Jedoch ist die heutige Internet-Infrastruktur hochgradig redundant aufgebaut, sodass selbst im Falle des Ausfalls eines Rechenzentrums ggf. ein anderes ortsfernes Rechenzentrum die Dienste z. T. übernehmen könnte und Pakete über alternative Routen geleitet werden könnten. Im Falle der Infrastruktur im Bahnsystem kann jedoch ein lokaler Ausfall der Infrastruktur bereits den Bahnverkehr weitgehend lahmlegen, da die betroffenen Züge auf eine lokale Verbindung angewiesen sind.

Zum physischen Schutz, insbesondere von Sensorsystemen, ist es daher zunächst vor allem wichtig den physischen Zugriff auf diese Systeme bestmöglich zu verhindern (M.1.1). Wie bereits erwähnt, ist dies im Falle von verarbeitenden Steuergeräten möglicherweise einfacher umzusetzen als im Falle von Sensoren. Die Steuergeräte selbst sollten sich an einem Ort befinden, der alarmgesichert ist und sich nicht ohne Spezialwerkzeug und eine zusätzliche Prüfung der Identität öffnen lässt. Dabei sollten auch Lock-Picking-Methoden und etwaige Manipulationen des Alarms in der Verteidigung berücksichtigt werden. Ein Zugriff sollte außerdem integritätsgesichert protokolliert werden. Bestenfalls kann der physische Zugriff auf das Gerät nur in speziell vorgesehenen Wartungsstationen erfolgen, in denen die Sicherheitsvorkehrungen entsprechend hoch sind. Falls der Alarm ausgelöst wurde, muss eine Prüfung der (System-)Integrität und ggf. Austausch der Komponenten erfolgen. Im Falle von Sensoren sollten diese ebenfalls bestmöglich vor Zugriffen geschützt werden. Des Weiteren könnte ein Schutz vor äußeren Störeinflüssen (M.1.2) erforderlich sein, bspw. vor elektromagnetischer Strahlung, oder vor physikalischen Einflüssen bezogen auf den jeweiligen Sensortyp. Hierbei sollten auch Störungen berücksichtigt werden, die evtl. nicht die physikalische Messgröße an sich beeinflussen, aber dennoch den Sensor stören bzw. manipulieren könnten. Zusätzlich könnte eine Manipulationserkennung (M.1.4) bzw. Störungserkennung (M.1.5) durch regelmäßige Selbsttests eingesetzt werden. Durch die Kombination verschiedener Messprinzipien (M.1.3) können Angriffe auf physikalischer Ebene erschwert werden. Zusätzliche Sensoren können ggf. auch zur Erkennung von Störeinflüssen verwendet werden. Weiterhin muss evtl. die Stromversorgung durch entsprechende physisch geschützte Backup-Lösungen (M.1.6) sichergestellt werden. Dies kann insbesondere zur Sicherstellung der Funktionalität der Alarmsicherung und zur kontinuierlichen Prüfung der Systemintegrität durch Selbsttests erforderlich sein.

Der Bereich „Kommunikations-Integrität/Authentizität“ (M.2) betrifft die Kommunikation zwischen Sensoren und Steuergeräten auf verschiedenen Ebenen. Einfache, bzw. nicht integrierte Sensoren verfügen möglicherweise nicht über die Möglichkeit die Integrität der Übertragung der Sensorinformation (über kryptografische Verfahren) zu gewährleisten. In der Regel existieren immer Stellen im Sensorsystem, an denen der Sensormesswert direkt in einer physikalischen Größe (z. B. elektrische Spannung) vorliegt. Diese Stellen müssen besonders geschützt werden (siehe „Physischer Schutz“ (M.1)), da eine Manipulation bei physischem Zugriff durchgeführt werden kann und anschließend ggf. schwer zu detektieren ist. Bei integrierten Sensoren folgt danach eine Digitalisierung der Messwerte und häufig eine Übertragung über einen Bus. Diese Übertragung kann möglicherweise bereits kryptografisch abgesichert werden. Anderenfalls gelten dieselben Bedingungen hinsichtlich des physischen Schutzes. Spätestens auf Netzwerkebene sollten kryptografische Maßnahmen zur Sicherung der Integrität und Authentizität und ggf. auch Verschlüsselung zum Schutz der Vertraulichkeit eingesetzt werden. Wie in CONNECTA vorgeschlagen, könnte bereits auf unterer Ebene der Zugang zum Netzwerk über PNAC (IEEE 802.1X-2010) und MACsec (IEEE 802.1AE) gesichert (M.2.1) werden. Dies erschwert es bei einem Angriff ein zusätzliches Gerät in das Netzwerk einzubinden. Dabei sollte auf jeden Fall auf eine aktuelle Spezifikation gesetzt werden, da ältere Standards eventuell angreifbar sind. Weiterhin sollten auch Verbindungen auf höheren OSI-Schichten separat, z. B. mittels TLS (M.2.2) und einer entsprechenden Public-Key-Infrastruktur, sowie beidseitiger Authentifizierung, abgesichert werden, um Angriffe weiter zu erschweren, auch wenn das angreifende Gerät bereits Teil des Netzwerks ist (Protokoll-Integrität und Geräte-Authentizität). Geräte sollten stets untereinander verifizieren, dass Nachrichten nur von authentischen und autorisierten Geräten an die jeweiligen Endpunkte gesendet werden. Auffälligkeiten, wie bspw. eine Nachricht des Heating, Ventilation and Air Conditioning (HVAC)-Systems, mit Sensorwerten, die die Tür betreffen, sollten protokolliert werden, einen Alarm auslösen und nicht weiterverarbeitet werden (M.2.3).

Ein weiteres wichtiges Element stellt die Geräte-Sicherheit (M.3) dar. Software-Updates sollten über sichere, moderne Verfahren durchgeführt werden, bspw. mittels TUF (M.3.1). Mindestens jedoch sollten die in TUF beschriebenen Risiken auch in Alternativen Update-Frameworks behandelt werden. Auch die Konfiguration der Systeme könnte mittels ähnlicher Update-Mechanismen installiert werden (M.3.2). Weiterhin sollten die Geräte lediglich korrekt signierte Firmware des Unternehmens installieren und sicherstellen, dass die Plattform-Integrität gegeben ist (Trusted Boot) (M.3.3). Kryptografisches Material sollte im Trusted Platform Module (TPM) des jeweiligen Geräts gespeichert werden und dieses nicht mehr verlassen (M.3.4). Ebenfalls müssen Prozesse zur sicheren Entsorgung ausgedienter Geräte (M.3.5) etabliert werden, die die sichere Löschung (inkl. TPM), sowie den Entzug von Privilegien der verwendeten Schlüssel bzw. Zertifikate (z. B. mittels Online Certificate Status Protocol (OCSP) bzw. Certificate Revocation Lists (CRLs)) einschließen.

Sicherheitslücken in Hardware und Software (M.4) sind ein weiteres Problem, das v. a. in vernetzten Systemen eine hohe Relevanz hat. Grundlegend sollte sämtliche im Einsatz befindliche Hardware und Software, inkl. aller Abhängigkeiten kontinuierlich auf veröffentlichte Sicherheitslücken (z. B. CVEs) überwacht werden und Schwachstellen sollten zeitnah durch sichere Updates (s. o.) behoben werden (M.4.1). Eine gute Basis sind außerdem Softwarequalitätsmaßnahmen (s. a. Kapitel 8.2.6) (M.4.4), sowie das Umsetzen von Secure Coding und anderen Best Practices (M.4.5) und die Entwicklung nach einem Security by Design Prozess und Anwendung entsprechender Prinzipien (M.4.6), wie bspw. Zero Trust (M.4.9) oder Least Privilege (M.4.8). So können bspw. Programme mit begrenzten Rechten, minimalen Schnittstellen mittels Sandboxing (M.4.8) vom Rest des Systems abgegrenzt werden (s. a. Kapitel 8.2.6). Weiterhin ist die Speichersicherheit von hoher Bedeutung. Hier empfiehlt sich vor allem der Einsatz einer speichersicheren Programmiersprache (z. B. Rust) (M.4.13). Weiterhin kann das Betriebssystem bzw. die Hardware durch Maßnahmen wie Address Space Layout Randomization (ASLR) oder Data Execution Prevention (DEP) / Non-Executable-Bit (NX) unterstützen (M.4.11). Ein weiteres Element ist der Compiler, der bspw. Stack Canaries oder Control Flow Integrity in das Programm integrieren (M.4.12) kann. Der Ein-

satz von Fuzzing (M.4.10), auch während der Entwicklung, kann u. U. auch frühzeitig Abstürze und Programmierfehler identifizieren. Es empfiehlt sich generell das Durchführen regelmäßiger, externer Penetrationstests (M.4.2). Außerdem könnten zumindest Konzepte auch extern validiert werden (M.4.3), z. B. durch größer angelegte Open Source Initiativen, oder Bug Bounty Programme. Als letzte Maßnahme sollte Logging (M.4.7), automatische Alarmierung, und nachträgliche Auditierung stattfinden, um Angriffe zu erkennen. Hierzu zählen auch WAFs, IDS/IPS und SIEM-Systeme.

Auch Denial of Service (DoS) Angriffe (M.5), also Angriffe auf die Verfügbarkeit, sollten bereits bei der Systementwicklung in Betracht gezogen werden. Hierbei sollte auch bedacht werden, dass das Erzwingen des Rückfalls in einen sicheren Zustand gemäß funktionaler Sicherheit, unter Umständen bereits einen erfolgreichen Angriff (Dienstverweigerung) darstellt. Hier können sich also die Ziele von funktionaler Sicherheit (Safety) und IT-Sicherheit unterscheiden, wenn die Verfügbarkeit weiterhin gewährleistet sein soll. Da der physische Schutz bereits besprochen wurde, steht hier die Verfügbarkeit von Geräten auf Software-Ebene im Vordergrund. Verwendete Protokolle sollten während der Entwicklung auf mögliche DoS-Angriffe geprüft werden (M.5.1), und diese sollten möglichst ausgeschlossen bzw. stark erschwert werden. Dies schließt eine Prüfung der Protokolle und verwendeter Parser auf Laufzeit- und Speicherkomplexität ein (M.5.3). Zudem könnte ein (gerätegebundener) Proof of Work (PoW) eingesetzt werden (M.5.2), um eine Überlastung zu verhindern, v. a. falls komplexere Berechnungen für die Bearbeitung der Anfrage notwendig sind, oder zu viele Anfragen erhalten werden.

Hinsichtlich der Netzwerksicherheit (M.6) wurden bereits einige Maßnahmen wie Überwachung mittels WAF (M.6.3) und IDS/IPS (M.6.2) bzw. SIEM (M.6.4), sowie Absicherung mittels PNAC und MACsec (M.2.1) und TLS (M.2.2) genannt. Außerdem sollten Firewalls (M.6.1) eingesetzt werden, sowie eine Erkennung und Blockierung von gespooften Paketen (M.6.5), sofern möglich.

Werden Methoden des maschinellen Lernens, wie bspw. Deep Neural Networks (DNNs) bzw. Convolutional Neural Networks (CNNs), bspw. zur Bildverarbeitung, eingesetzt, müssen hierfür gezielte Maßnahmen in Betracht gezogen werden. Dabei sollte aktuell beachtet werden, dass das Feld, v. a. im Bereich sogenannter Adversarial Attacks, weiterhin Gegenstand der Forschung ist und somit neue Angriffe entdeckt, sowie alte Angriffsmethoden stabilisiert werden. Gleichzeitig werden aber auch neue Verteidigungsmöglichkeiten (wenn auch weniger) entworfen. Es existieren damit zurzeit wahrscheinlich keine Modelle, die gegen sämtliche Angriffe robust sind. Wie in einer Veröffentlichung von Shen et al. [325] beschrieben, existieren grundlegend zwei verschiedene Abwehrstrategien: Konsistenzprüfung (Consistency Checking) (M.7.1), d. h. Prüfung der Erkennungen mittels zusätzlicher Informationen auf Konsistenz, sowie Stärkung der Robustheit gegenüber Adversarial Examples (M.7.2). Hinsichtlich der Konsistenzprüfung kann bspw. eine Gegenprüfung mittels anderer Sensoren (an anderen Orten oder mit anderen Messverfahren) (M.7.1.1), bzw. eine Sensor-Fusion (M.7.1.2) eingesetzt werden, ggf. sogar gezielt um Adversarial Examples aufgrund ihrer Gegebenheiten auszuschließen (z. B. falscher Kontext). Eine weitere Möglichkeit ist die Prüfung physikalisch invarianter Eigenschaften (M.7.1.3), wie etwa das Vorhandensein bestimmter Reflexionen bei Lichtquellen. Die Verbesserung der Robustheit gegenüber Angriffen kann u. a. über Adversarial Training (M.7.2.1) (Training des Modells mit spezifischen Angriffen als negative Beispiele), oder Vorhersage und/oder Entfernen (bspw. Median-Filter) von entsprechenden Manipulationen (M.7.2.2) erfolgen. Diese Methoden sind jedoch jeweils nur für bestimmte Angriffe hilfreich und können bei einem gezielten Angriff durch adaptive Verfahren leicht umgangen werden.

Im Bereich der komplexen Sensoren gibt es je nach Sensortyp spezifische Gegenmaßnahmen. Eine wiederholt genannte Maßnahme ist jedoch auch hier die Nutzung verschiedener Sensoren zur Konsistenzprüfung, bzw. Sensor-Fusion (M.8.3.2.1). Bei gezielten Angriffen auf Sensor-Fusionssysteme empfehlen Shen et al. [330] Gegenmaßnahmen gegen das Spoofen einzelner Sensoren (M.8.1.2) (bspw. GPS), die Verbesserung der Konfidenz des Filters und damit Genauigkeit der Sensoren (M.8.1.1), sowie die Nutzung weiterer Datenquellen (M.8.1.3) zur Positionsbestimmung. Für GPS kann die Signalstärke überwacht werden (M.8.2.1), mehrere Antennen zur Erkennung der Signalrichtung verwendet werden

(M.8.2.2), oder auf lange Sicht eine kryptografische Authentifizierung eingesetzt werden (M.8.2.3), die jedoch weiterhin anfällig für Replay-Angriffe ist [330]. Für LiDAR-Systeme schlagen Sun et al. [328] zwei neue Verfahren vor, zum einen CARLO (Occlusion-Aware Hierarchy Anomaly Detection) (M.8.3.1.3), das als nachgelagerter Validierungsschritt eingesetzt wird, und zum anderen SVF (Sequential View Fusion) (M.8.3.1.4), das im Gegensatz dazu eine Anpassung des Erkennungsmodells und der Modell-Architektur erfordert. Cao et al. [327] unterscheiden für LiDAR-Sensoren zwischen Maßnahmen auf der System-Ebene (M.8.3.1), Maßnahmen auf der Sensor-Ebene (M.8.3.2), sowie Maßnahmen auf Machine Learning Modell-Ebene (s. M.7). Auf der System-Ebene wird das Herausfiltern von Reflexionen in der Vorverarbeitung (M.8.3.1.1), sowie das Reduzieren von Informationsverlust in der Verarbeitung (M.8.3.1.2) vorgeschlagen. Auf Sensor-Ebene wird zwischen Erkennung, Mitigation und Randomisierung unterschieden. Zur Erkennung wird ebenfalls eine Sensor-Fusion bzw. Nutzung alternativer/zusätzlicher Sensoren (M.8.3.2.1) genannt. Zur Mitigation wird empfohlen den Empfangswinkel zu reduzieren (M.8.3.2.3), sowie unerwünschte Lichtspektren herauszufiltern (M.8.3.2.4). Unter Randomisierung wird das zufällige Gruppieren von Laser-Impulsen (M.8.3.2.6) bzw. Zufälliges Ausschalten des Laser-Transmitters (M.8.3.2.8) verstanden, um unerwartete Eingangssignale zu erkennen. Auf Machine Learning Ebene wird ebenfalls auf Adversarial Training (M.7.2.1) bzw. Detektions- und Verteidigungsmaßnahmen aus anderen Veröffentlichungen verwiesen. Ebenfalls im LiDAR-Bereich empfehlen Shin et al. [329] die Nutzung mehrerer LiDARs mit überlappenden Bereichen, bzw. Sensor-Fusion (M.8.3.2.1). Außerdem wird vorgeschlagen, eine Sättigung des Sensors zu erkennen (M.8.3.2.2), Gegenmaßnahmen bzgl. Effekte aufgrund von gebogenem Glas anzuwenden (M.8.3.2.5), sowie ebenfalls den Empfangswinkel einzuschränken (M.8.3.2.3) bzw. eine Randomisierung des Pings durch zufällige Richtungen (M.8.3.2.7) oder zufällige Wellenformen (M.8.3.2.6) durchzuführen.

8.2.8 Angreifermodelle im Schienenverkehr

Die Ziele von Cybersicherheit sind Vertraulichkeit, Integrität, Sicherheit, Verlässlichkeit und Verfügbarkeit. Wenn diese nicht erreicht werden, kann dies zum Verlust des Vertrauens der Öffentlichkeit, zu Reputationsschäden, zu Ungenauigkeiten oder dem Verlust von Daten, zu fehlerhaften Entscheidung oder den Verlust von Zuverlässigkeit, Sicherheit und Kontinuität führen. Ebenso sind rechtliche Folgen bei Nichterreichen der Sicherheitsziele erwartbar. [371]

Um sich gegen Angriffe schützen zu können, muss nicht nur bekannt sein, auf welche Weise ein Angriff stattfinden könnte und was für Auswirkungen dieser hat, sondern auch gegen wen der Schutz erfolgen muss. Aus diesem Grund ist es hilfreich, die Angreifenden hinter Vorfällen von Cyberangriffen im Schienenverkehr zu untersuchen.

Angreifende können unterschiedlich kategorisiert werden. Han und Dongre [372] haben eine mögliche Kategorisierung vorgestellt. Zunächst kann es sich bei einer oder einem Angreifenden um Insider, wie unzufriedene, finanziell motiviert oder unabsichtlich schädlich handelnde Mitarbeitende oder um Outsider handeln. Outsider wiederum können unterteilt werden in Amateure, Hackerinnen und Hacker (wie Black Hats und White Hats) und organisierte Angreifende. Angreiferorganisationen können Terroristen, Hacktivisten, staatlich organisiert oder kriminelle Vereinigungen sein. Hacktivisten sind hierbei Gruppen, deren Ziel politische Statements sind und deren Absicht weniger in Schäden, sondern vielmehr darin besteht, auf bestimmte Themen aufmerksam zu machen.

Um Angreifende einzuordnen, sind auch deren Beweggründe und Motive von Relevanz. Traer and Benar [373] haben eine Übersicht über verschiedene Motive hinter Cyberangriffen erstellt. Hierbei haben sie die Motive finanzieller Gewinn, Vergeltung, Ablenkung, Cyber-Kriegsführung, Protest, Spaß sowie bezahlte und unbeabsichtigte Angriffe unterschieden. Angriffe aus Spaß wiederum haben sie unterteilt in Wettbewerbe und egoistisch motiviert Angriffe, die auch als intellektuelle Herausforderung angesehen werden können. Ebenso haben sie das Motiv des finanziellen Gewinns nochmals durch das Motiv der

Erpressung erweitert. Womit auch der Angreifertyp des finanziell motivierten Insiders abgegrenzt werden kann.

Es wurden 19 dokumentierte Sicherheitsvorfälle im Bereich des Schienenverkehrs weltweit exemplarisch untersucht (siehe Tabelle 83). Eine umfassendere Darstellung findet sich in [314]. Zehn Vorfälle waren Ransomware Angriffe, durchgeführt von Cyberkriminellen, die auf finanziellen Gewinn aus sind, indem sie das Geld erpressen. Drei Vorfälle sind durch staatlich oder vermutet staatlich organisierte Hacker durchgeführt wurden. Diese dienten der Aufdeckung von Schwachstellen und im Falle der Störung des Schienensystems in Belarus, der Aufhaltung militärischer Bewegungen. Es ist darauf hinzuweisen, dass Ursachen von Handlungen und Verhaltensweisen vor allem im Angreiferbereich nicht immer klar sind und daher hier mit der stärksten Vermutung gearbeitet wird. Nach Han und Dongre [372] kann man die drei bis möglicherweise vier Vorfälle dem Motiv der Cyber-Kriegsführung unterordnen. Die Ermittlung zur Sabotage des GSM-R Netzes in Deutschland ist zum Zeitpunkt dieser Studie noch nicht abgeschlossen [374].

Tabelle 83: Cybersicherheitsvorfälle im Schienenverkehr

Jahr	Vorfall	Angreifer
2008	Ein Teenager hat in Polen eine Fernbedienung gebaut, mit der er die Weichen nach Belieben verstellen konnte. Der Vorfall führte zu Verletzungen. [375][376]	Individuum (Amateur) zum Spaß
2012	Hacker haben in den USA Bahnsignale gestört, wodurch Verspätungen aufkamen. [375][377]	Hacker, wobei dies angeblich ein zufälliges Ziel zu sein schien
2016	Ukrainische Bahngesellschaft mit Malware (BlackEnergy und KillDisk) infiziert. [375][378]	(womöglich staatliche) Hacker, um nach Schwachstellen zu suchen und die Infrastruktur zu schädigen
2016	Eindringen in das System einer britischen Bahngesellschaft über 12 Monate. [375][379]	Staatlich unterstützte Angreifende, um Schwachstellen aufzudecken.
2016	Ransomware Angriff auf die Verfügbarkeit des Ticketsystems in San Francisco. [375]	Cyberkriminelle für Profit
2017	Ransomware Angriff auf Daten der Deutschen Bahn sowie russische und chinesische Bahngesellschaften. [375][380]	Cyberkriminelle für Profit
2017	DDoS Angriff auf ein schwedisches System zur Überwachung des Schienenverkehrs. [375][381]	Streich durch Individuen oder Untersuchung der Schutzmaßnahmen
2018	DDoS Angriff auf die dänischen Ticket-, Mail- und Telefonsysteme der Bahn. [375][382]	Unbekannte Angreifende, um das System zu blockieren

Jahr	Vorfall	Angreifer
2019	Verkauf von Zugriffsdaten eines chinesischen Schienenkontrollsystems im Dark Web. [375]	Cyberkriminelle für Profit
2020	Ransomware Angriff auf die Server der Verkehrsgesellschaft von Montreal. [375]	Cyberkriminelle für Profit
2020	Ransomware Angriff auf amerikanischen Güterverkehr. [375]	Cyberkriminelle für Profit
2020	Ransomware Angriff auf das Bezahlsystem und GPS-Funktionen eines kanadischen Verkehrsunternehmens. [375]	Cyberkriminelle für Profit
2021	Hacker haben iranische Hinweistafeln manipuliert und die Telefonnummer des Staatsoberhaupts als Kontakt für weitere Informationen angegeben. [375][383][384]	Politisch motivierter Angriff durch Hacktivisten zum Protest oder als Vergeltung
2021	Ransomware Angriff auf ein kanadisches Ticket- und Kommunikationssystem. [375]	Cyberkriminelle für Profit
2021	Ransomware Angriff auf britisches Schienensystem. [385]	Cyberkriminelle für Profit, zufälliges ‚Spray and Pray'-Ziel
2022	Störung des Schienensystems in Belarus. [386]	Hacker, um militärische Bewegungen zu stören
2022	Ransomware Angriff in Dänemark auf ein drittes Unternehmen, das Lösungen für die Verwaltung von Unternehmensanlagen für die Eisenbahngesellschaft bereitstellte und damit Stillstand aller Züge aufgrund des Ausfalls aller Server dieses dritten Unternehmens. [387]	Cyberkriminelle für Profit
2022	Ransomware Angriff auf den italienischen Bahnbetrieb mit Störung des Fahrkartenverkaufs, der Fahrgastinformationsbildschirme und der vom Bahnpersonal verwendeten Tablets. [388]	Cyberkriminelle für Profit
2022	Durchtrennung von zwei Glasfaser-Kabeln in Berlin und Herne führte zum Ausfall dem GSM-R Netzes. Die Deutsche Bahn musste den Zugverkehr in Norddeutschland für mehrere Stunden einstellen. [374]	Möglicherweise staatlich gesteuerte Sabotage (Ermittlungen noch nicht abgeschlossen)

Der älteste betrachtete Vorfall galt lediglich der intellektuellen Herausforderung eines einzelnen Teenagers und auch der DDoS Angriff in Schweden 2017 könnte laut dem beteiligten Geschäftsführer ein Streich durch Individuen gewesen sein [381]. Zudem gab es einen Einzelfall, der auf Protest durch Hacktivisten zurückzuführen ist. Bei diesem politisch motivierten Angriff sei es anzunehmen, dass nicht die Transportinfrastruktur das primäre Ziel darstellte, sondern die Blamage des neuen Präsidenten im Vordergrund stand [384]. Es sei aber auch nicht auszuschließen, dass es sich ebenso um einen Vergeltungsangriff handeln könnte [384].

Es wird ersichtlich, dass bis auf Einzelfälle die meisten Vorfälle organisiert sind, um Schwachstellen aufzudecken oder andere staatlich motivierte Ziele zu erfüllen oder um finanziellen Gewinn zu erwirtschaften. Es ist zudem anzumerken, dass die Ransomware Angriffe, welche die häufigsten Cybersicherheitsvorfälle darstellen, auch dann durchgeführt wurden, wenn die Chancen unwahrscheinlich bis unmöglich waren, dass das Lösegeld bezahlt wurde. Für den Angriff auf das britische Schienensystem war dies z. B. der Fall gewesen [385]. Ransomware Angriffe sind demnach auch dann nicht unwahrscheinlich, wenn die Organisation kein attraktives Ziel für eine solchen Angriff darstellt.

Die meisten Angreifenden scheinen im Schienenverkehr somit Outsider und vermehrt organisiert zu sein. Bei den Sicherheitsvorfällen sind die möglichen physischen und psychischen Schäden an Personen nicht das Ziel und womöglich auch nicht beabsichtigt, wie es bei terroristischen Angriffen der Fall wäre. Am häufigsten stehen finanzielle Motive im Vordergrund, wobei erfahrene Angreifende die Ziele der Vertraulichkeit, der Integrität, der Verlässlichkeit und der Verfügbarkeit gezielt unterbinden, um deren Erfüllung als Druckmittel nutzen zu können (siehe Tabelle 84).

Tabelle 84: Einordnung der Vorfälle in die Motive nach Traer und Bednar [373]

Motiv	Anzahl
Finanzieller Gewinn	10
Cyber-Kriegsführung	4
Protest und Hacker-Gruppen	2
Vergeltung	1
Spaß oder intellektuelle Herausforderung	2

8.2.9 Cybersecurity als Prozess eingebettet in das Risikomanagement

Im vorangehenden Abschnitt wurden konkrete Beispiele für Cybersecurity Angriffe, typische Angreifermodelle und deren Motivation vorgestellt. Insbesondere wurde dabei herausgestellt, dass den meisten Angriffen ein mehrphasiges, häufig auch arbeitsteiliges Handeln zugrunde liegt. In den meisten der dargestellten Fälle handelte es sich um professionelle Angreifende – Cyberkriminelle oder vermutlich staatliche Akteure, die damit in der Lage sind, komplexe Angriffe auch über einen längeren Zeitraum durchzuführen und dabei Dienstleistungen und Tools von Dritten einzusetzen. Um besonders im Rahmen des Risikomanagements die zugrundeliegenden komplexen und längerfristigen Prozesse berück-

sichtigen zu können, ist es wichtig, Methodiken einzusetzen, die die Modellierung von solchen komplexen Bedrohungen ermöglichen. Ergänzend sind Methoden wie Attack Trees nützlich, um innerhalb einzelner Teilsysteme Angriffsvektoren zu identifizieren, wie in Kapitel 8.2.2 dargestellt.

Basis der folgenden Betrachtung ist das Risikomanagement gemäß ISO/IEC 31000. Im Kern handelt es sich dabei um einen fortlaufenden Prozess, bei dem in einem definierten Kontext die folgenden Schritte zyklisch wiederholt werden:

- Risiko-Identifikation
- Risiko-Analyse
- Risiko-Bewertung
- Risikobehandlung

Diese Schritte werden begleitet durch das *Überwachen und Überprüfen* der Risiken und der Effektivität der umgesetzten Maßnahmen zur Behandlung der Risiken. Daneben sind *Kommunikation und Konsultation* sowie das *Aufzeichnen und Berichten* begleitende Schritte. Bei den Maßnahmen zu Risikobehandlung sind die folgenden Strategien möglich:

- Risikovermeidung: beispielsweise durch Umstrukturierung des Prozesses
- Risikoreduktion: durch Maßnahmen zur Erhöhung der IT-Sicherheit können die Wahrscheinlichkeit oder die Auswirkungen des Auftretens eines Risikos reduziert werden
- Risikotransfer: durch Versicherungen oder die Auslagerung der betreffenden Dienste an Dritte mit geeigneter vertraglicher Absicherung
- Risikoakzeptanz

Wenn gegebenenfalls durch die Anwendung geeigneter Maßnahmen das *Restrisiko* auf ein Maß reduziert werden kann, sodass es im Einklang mit den Kriterien der *Risikoakzeptanz* der Organisation ist, kann das Risiko akzeptiert werden.

Im Bereich der Cybersecurity werden im Rahmen des Risikomanagements zur Modellierung komplexer mehrphasiger Angriffe die Methoden Cyber Kill Chain [389] und das MITRE ATT&CK framework [390] eingesetzt. Die beiden Methodiken werden im Folgenden kurz vorgestellt. Das Modell der Cyber Kill Chains wurde von Lockhead Martin 2011 im Kontext militärischer Anwendungen entwickelt [389][391]. Das Ziel dieser Methodik ist es, die aufeinanderfolgenden Schritte eines komplexen Angriffs zu visualisieren, um dann gezielt die Kette an einzelnen Stellen durch Gegenmaßnahmen zu unterbrechen und damit den Angriff im Sinne des Risikomanagements zu verhindern oder mindestens das Risiko zu reduzieren. Als Phasen komplexer Angriffe werden dabei die folgenden Phasen berücksichtigt (nach [389][391]):

1. *Reconnaissance*: Die/den Angreifende wählt das Angriffsziel aus, untersucht dieses und versucht Schwachstellen im Netzwerk des Angriffsziels zu identifizieren.
2. *Weaponization*: Die/den Angreifende generiert oder beschafft eine für die identifizierten Schwachstellen spezifische Schadsoftware, über die ein Remote Zugriff ermöglicht werden kann, wie einen Virus, Trojaner oder ähnliches.
3. *Delivery*: Die/den Angreifende überträgt die Schadsoftware ins Zielnetzwerk (z. B. über eine Webseite, einen USB Stick oder einen Email Anhang)
4. *Exploitation*: Die Schadsoftware kann im Zielnetzwerk durch das Ausnutzen einer Schwachstelle einen ersten Zugang zum Zielnetzwerk ermöglichen.
5. *Installation*: Die Schadsoftware realisiert einen Zugang zum Zielnetzwerk (Backdoor) für die Angreiferin oder den Angreifer.
6. *Command and Control*: Die Schadsoftware ermöglicht der Angreiferin oder dem Angreifer dauerhaften Zugriff zu den für den Angriff nötigen Komponenten des Zielnetzwerks.

7. *Actions on Objective*: Angreifer führt Aktionen aus, um die eigentlichen Ziele des Angriffs zu erfüllen, wie beispielsweise das Manipulieren von Systemen, das Auslesen von Daten, die Verschlüsselung oder generell Zerstörung von Daten.

Von einzelnen Autoren werden auch Kill Chains für spezifische Technologien vorgeschlagen, wie bspw. die IoT Kill Chain [340], die in Kapitel 8.2.4 vorgestellt wurde. Vorteil der Cyber Kill Chain ist, dass das Modell relativ leicht verständlich ist und damit gut in Workshops zur Analyse eingesetzt werden kann. Auf der anderen Seite sind Angriffe besonders im Kontext Cloudbasierter Architekturen zunehmend komplexer geworden. Das wird durch das MITRE ATT&CK Framework [390][391] adressiert, das auf Basis eines Phasenmodells mit ergänzenden sogenannten Tactics aufbaut und ein Modell zur Analyse von Bedrohungen darstellt. Zu diesem Modell werden auch umfassende Zusatzinformationen dargestellt [392]. Das eigentliche Phasenmodell ist stark angelehnt an das Modell der Cyber Kill Chain:

1. Recon
2. Weaponize
3. Deliver
4. Exploit
5. Control
6. Execute
7. Maintain

Dabei werden die letzten drei Phasen *Control, Execute, Maintain* ergänzend durch zehn Gruppen von Tactics detailliert, die besonders in diesen Phasen, in denen im Anschluss an die initiale Etablierung eines initialen Zugangs zum Zielnetzwerk in der Phase *Exploit*, die Aktivitäten im Zielnetzwerk umgesetzt werden. Die folgenden Gruppen werden dabei betrachtet [390][391]:

- Persistence
- Privilege Execution
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Wichtig ist, dass im Rahmen der Tactics bereits wichtige Gruppen von Angriffsmethoden abgebildet werden, wie bspw. *Privilege Execution, Credential Access* und *Lateral Movement*. Diese Methoden werden durch konkrete Techniken detailliert, zu denen dann weitergehende technische Informationen innerhalb des Modells verfügbar sind.

Insbesondere innerhalb der ENISA Threat Landscape [392], einer einmal jährlich erscheinenden Studie der ENISA zur aktuellen Bedrohungslage im Bereich Cybersecurity, werden inzwischen neben Hinweisen zu ISO/IEC 27001:2013 und dem NIST Cybersecurity Framework auch im Anhang detaillierte Hinweise auf Basis des MITRE ATT&CK Frameworks zu den wichtigsten Bedrohungen herausgearbeitet. Bspw. werden die in Kapitel 8.2.8 genannten Angriffe *Ransomware* und *DDoS Angriffe* dort genannt und beispielhaft Aktivitäten angegeben. Einzelne solcher Aktivitäten und die Informationsquellen dazu wurden auch bereits im Kapitel 8.2.6 zum Thema cloudbasierter Software-Architekturen genannt. Diese Informationen können zum einen im Bereich der vorbeugenden Maßnahmen eingesetzt werden, um bereits während der Konzeption und Entwicklung durch einen Security by Design Ansatz potentielle Angriffspunkte zu vermeiden. Daneben gibt es auch Hinweise, wie mögliche Angriffe im Rahmen des Monitorings identifiziert werden können.

Da der Schienenverkehr im KRITIS-Bereich Transport und Verkehr bei Überschreiten von differenziert nach Anlagenkategorien definierten Schwellenwerten[12] als Kritische Infrastruktur gewertet wird, ist das BSI-Gesetz anwendbar. Dort werden zum einen Betreiber Kritischer Infrastrukturen verpflichtet, gemäß § 8a Abs. 1 BSI-Gesetz „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind." Gemäß § 8a Abs. 1a BSI-Gesetz umfasst das auch geeignete Systeme der Angriffserkennung. Weiterhin müssen Betreiber Kritischer Infrastrukturen nach § 8b Abs. 4 BSI-Gesetz „Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen" geführt haben oder führen können, dem BSI als zentrale Meldestelle melden.

Die hier geforderten angemessenen technischen und organisatorischen Vorkehrungen im Kontext der Schutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit entsprechen den Aspekten, die auch von allen oben dargestellten Modellen, insbesondere dem MITRE ATT&CK Framework, adressiert werden. Nach den dort dargestellten Phasen und Methoden komplexer Angriffe ist ebenfalls eine Strategie zur Angriffserkennung unabdingbar, da zwar eine Reduktion von Risiken möglich ist, aufgrund einer sich ständig ändernden Bedrohungslage aber eine vollständige Reduktion generell nicht möglich ist. Hilfreich ist deshalb auch die Meldepflicht, weil so die Chance besteht durch die transparente Dokumentation von Vorfällen eine gemeinsame Wissensbasis zu Angriffen zu erstellen, um generalisierte Frameworks, wie das MITRE ATT&CK Framework, durch spezifische Informationen zu Störungen in kritischen Infrastrukturen durch eine Wissensbasis zu ergänzen, die anschließend im Rahmen der Cyber Threat Intelligence genutzt werden kann.

Neben den technischen und organisatorischen Maßnahmen zur Risikobehandlung im Bereich Cybersecurity ist ein sehr wichtiger Bereich das generelle Überwachen und Überprüfen von Risiken im Sinne des Risikomanagements. Durch den Bereich Aufzeichnen und Berichten im Risikomanagement sollte ein automatisches Logging und Reporting etabliert werden. Auf dieser Basis können technische Systeme der Angriffserkennung, wie Security Incident and Event Management (SIEM) Systeme, die basierend auf individuell zu definierenden Metriken und der Aggregation von Logs eine Alarmierung ermöglichen, etabliert werden. Wenn möglich sollte auch eine automatisierte Reaktion erfolgen. Durch ein Security Operations Center (SOC) können Alarme dann ergänzend zu automatischen Reaktionen eingeordnet und adressiert werden. Wichtig ist dabei insbesondere eine zeitnahe Meldung an das BSI als Meldestelle nach dem BSI-Gesetz. Im Falle eines Vorfalls sind dann die entsprechenden Organisationen des BSI einzubeziehen. Ergänzend kann der Einsatz von Penetration Tests sinnvoll sein.

Die hier dargestellten organisatorischen und technischen Maßnahmen sollten eingebettet in ein Information Security Management System (ISMS) gemäß ISO/IEC 27001 etabliert werden. Dabei sollten insbesondere Mindestanforderungen an die Cybersecurity etabliert werden. Hier sind insbesondere Standards und Best Practices hilfreich. Ergänzend können im Rahmen des Risikomanagements ausgehend von dem konkreten Kontext und dem betrachteten Systemverbund individuell Risiken untersucht werden. Deshalb ist eine pauschale Aussage zu den Risiken ohne einen konkret betrachteten technischen Systemzusammenhang inklusive der damit verbundenen Prozesse und Informationen über den Kontext des Einsatzes nur sehr rudimentär möglich. Zu vielen einzelnen Komponenten, wie bspw. OPC UA gibt es gesonderte Sicherheitsanalysen [333], die im Rahmen einer Risikoanalyse unterstützend eingesetzt werden können. Dabei sollten jeweils die Motivation der Angreifenden und häufige Angriffe berücksichtigt werden. Insbesondere ist dabei wichtig zu berücksichtigen, dass es neben gezielten Angriffen auf einzelne Systeme oder Dienste auch breite, ungezielte Angriffsmuster gibt, wie teilweise der Einsatz von

[12] Für weitere Informationen siehe https://www.bsi.bund.de/dok/sektor-transport-und-verkehr

Ransomware und Supply Chain Attacks, die durch manipulierte Updates von Software eine große Menge an Angriffszielen adressieren. Deshalb ist es wichtig, dass generell solide Mindestanforderungen etabliert werden und insbesondere Ansätze, wie Zero Trust (siehe Kapitel 8.2.6), die helfen Angriffsvektoren im Sinne der Risikovermeidung zu reduzieren, weiterverfolgt werden.

9 Zusammenfassung und Ausblick

Dieser Bericht präsentiert die Ergebnisse des Forschungsprojektes „Sensorbasierte Technologien im Bahnsystem: Markt- und Technologieanalyse“.

Im Kapitel 4 Bestandsaufnahme Sensormarkt wurden unter Berücksichtigung zahlreicher Literaturquellen und Expertinnen- und Experteninterviews insgesamt 43 Anwendungsfälle von Sensorik am Fahrzeug und in der Infrastruktur herausgearbeitet. Ein im Anschluss stattfindender Workshop diente dazu, diese Fälle hinsichtlich ihrer Relevanz zu bewerten und eine Entscheidungsgrundlage für eine im Rahmen dieses Projektes handhabbare Menge an relevanten Use Cases zu ermitteln. Es wurden folgende sieben Anwendungsfälle für eine weitere Betrachtung herausgearbeitet, die eine möglichst große Bandbreite umfassen:

- Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)
- Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen
- Infrastruktur überwacht Fahrzeug – nicht sicherheitsrelevant
- Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant
- Fahrzeug überwacht Oberbau
- Weichenferndiagnose
- (Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)

In Kapitel 4.3 wurden Anforderungskriterien vorgestellt, die an Sensoren für einen Einsatz im Bahnsystem gestellt werden. Diese können den Kategorien Betriebsbedingungen, Umwelt, Schnittstellen (Allgemein, Elektro, Daten, Kommunikation), Montage, Störung anderer Systeme/EMV, Betriebssicherheit & Zuverlässigkeit, Verfügbarkeit, Instandhaltung, Safety und Security zugeordnet werden. Auch der Zulassungsprozess wurde in den Blick genommen, wobei dieser je nach Komplexität und Aufgabe der Sensorlösung einfacher oder schwerer umsetzbar ist.

Das Kapitel 5 beinhaltet eine Stakeholderanalyse. Es wurden die verschiedenen Stakeholder ermittelt, die mit ihren Entscheidungen und ihrem Einfluss mitbestimmen, welche Sensoranwendungen in welcher Art und Weise und mit welchen Komponenten im Bahnsystem umgesetzt werden. Dazu wurden insgesamt 34 Stakeholder-Hauptgruppen ermittelt, die sich in die folgenden Kategorien einordnen lassen:

- Sensorik und IT
- Hersteller von Schienenfahrzeugen
- Instandhalter von Schienenfahrzeugen
- Bahnbetreiber
- Hersteller von Schieneninfrastruktur
- Instandhalter und Betreiber von Schieneninfrastruktur

Bei allen untersuchten Sensoranwendungen liegen recht komplexe Wertschöpfungsverflechtungen und damit gegenseitige Abhängigkeiten, Einflüsse und Einflussmöglichkeiten vor. Dies gilt bereits, wenn der Sensoreinsatz innerhalb einer der Anwendungsdomänen – Fahrzeug bzw. Infrastruktur – stattfindet und verstärkt sich noch, wenn zwischen beiden Domänen ein Austausch erfolgt. Das bedeutet auch, dass sich entsprechende Anwendungen nur durchsetzen werden, wenn sie aus Perspektive der verschiedenen beteiligten Marktteilnehmer wirtschaftlich und aus Sicht aller Stakeholder (auch der rahmensetzenden) hinsichtlich der Chancen und Risiken Erfolg versprechend und vertretbar sind. Aus den analysierten Stakeholderbeziehungen konnten 24 Innovationsbarrieren abgeleitet werden, die als Hürden für eine stärkere Verbreitung sinnvoller Use Cases wirken. Sie lassen sich den Kategorien Technologie, Recht, Standardisierung, Geschäftsmodelle und Markt einteilen.

Diese Erkenntnisse dienen im Anschluss auch als Basis für das Kapitel 6 Handlungsableitungen und Marktausblick. In diesem konnten 36 Maßnahmenvorschläge in zehn Handlungsfeldern der Kategorien Technik und Recht, Markt, Daten- und Informationsmanagement sowie Innovationsförderung ausgearbeitet werden. Ein weiterer wichtiger Faktor für die Einführung von Sensorlösungen ist das Geschäftsmodell. Hier sind insbesondere das Veränderungspotential und der Neuheitscharakter entscheidend. Ebenso gilt es die Marktattraktivität und die Marktreife zu betrachten.

Das Kapitel 7 handelt von der Bestandsaufnahme und Patentrecherche zu Sensoriksystemen und Teilkomponenten. Dazu wurde zunächst eine Recherchetabelle entwickelt, in der Informationen zu den folgenden 13 Kategorien eingetragen wurden: Systemarchitekturen, Zugbeeinflussungssysteme, Türsteuerungen, Funksysteme, Netzwerkprotokolle, Feldbusse, Kommunikationsstandards, Auszeichnungssprachen, Modellierungssprachen, Datenformate, Semantik, Ontologien und Hardwarekomponenten. Anhand des Leitbildes wurden 10 Technologien und Architekturen für die weitere Analyse und Klassifizierung ausgewählt: TCN, NG-TCN, TIS/ITSS, MQTT, OPC UA, SensorML, Semantic Sensor Network (SSN) Ontology, Automatisierungspyramide, IoT-Architektur und OT/IT-Architektur. Für diese wurden die Prozessschritte der Datenverarbeitung, die Eigenschaften sowie die Vor- und Nachteile benannt und daraus die Veränderungen und Auswirkungen durch die Digitalisierung und das IoT diskutiert. Des Weiteren wurde eine Schutzrechtanalyse durchgeführt. Eine Recherche unter Normen und Standards ergab, dass alle untersuchten Architekturen im Wesentlichen bereits standardisiert oder genormt sind und sich in einem dieser Prozesse befinden. Eine Patentrecherche über PatBase kann allerdings nur sinnvoll durchgeführt werden, wenn die spezielle Ausführungsform bekannt ist.

Das Kapitel 8 beschäftigte sich mit einer Recherche und Bestandsaufnahme zu relevanten Aspekten der Cybersecurity. Es konnten bahnspezifische Quellen identifiziert und analysiert sowie Quellen aus verwandten Bereichen wie Industrie 4.0, IoT oder Mobilität mit Bezug zu Datensicherheit und Cybersecurity gesammelt werden. Dadurch wurden Herausforderungen für die Cybersecurity, Bedrohungen, Angriffsszenarien und Maßnahmen sowie Kommunikationstechnologien herausgearbeitet. Ebenso konnten verwendete Protokolle und Schnittstellen, Architekturkonzepte und IT-Sicherheitsansätze bestimmt werden. Wichtig ist hierbei, dass es sich bei Cybersecurity um einen Prozess handelt, der während des gesamten Lebenszyklus fortgeführt und bei Bedarf angepasst werden muss. Abschließend wurden allgemeine Einschätzungen zu möglichen Risiken im Kontext der Anwendungsfälle gegeben.

10 Abbildungsverzeichnis

11 Tabellenverzeichnis

12 Quellenverzeichnis

[1] **Eisenbahn-Bundesamt** (2022): Themen – Fahrzeugzulassung [Online], [Zugriff am: 05.10.2022]. Verfügbar unter: https://www.eba.bund.de/DE/Themen/Fahrzeugzulassung/fahrzeugzulassung_node.html;jsessionid=3D1C75EA5ED48E9256375612A1F45351.live11314

[2] **Eisenbahn-Bundesamt** (2022): Themen – Infrastruktur – Zulassung [Online], [Zugriff am: 10.10.2022]. Verfügbar unter: https://www.eba.bund.de/DE/Themen/Infrastruktur/Zulassung/zulassung_node.html

[3] **HBM Sensor Inside Redaktion** (o. A.): Messtechnik auf der Schiene [Online], in: HBM Sensor, [Zugriff am: 25.03.2022]. Verfügbar unter: https://www.hbm.com/de/2393/messtechnik-auf-der-schiene/

[4] **Erhard**, F.; Gabler, H.; Hempe, T.; Wolter, K. (2014): Fahrzeugseitige Überwachung der Infrastruktur im Regelbetrieb, in: Eisenbahntechnische Rundschau (ETR), Jg. 63, Nr. 07 – 08, S. 32 – 26

[5] **Hunn**, S.; Nerlich, I.; Schlatter, C.; Dr. Wolter, K. U.; Züger, S. (2020): Onboard Monitoring in der Schweiz, ein Gemeinschaftswerk dreier Bahnen [Online], in: ZEVrail, Jg. 144, Nr. 04, [Zugriff am: 24.05.2022]. Verfügbar unter: https://www.zevrail.de/artikel/onboard-monitoring-der-schweiz-ein-gemeinschaftswerk-dreier-bahnen

[6] **DB Systemtechnik GmbH** (o. A.): CIM – Continuous Infrastructure Monitoring [Online], [Zugriff am: 08.02.2023]. Verfügbar unter: https://www.db-systemtechnik.de/dbst-de/Produktgruppen/Continuous-Infrastructure-Monitoring-CIM--6225016?

[7] **Brandl**, D.; Neuhold, J.; Oberbauer, H.; Orta, J.; Schönhuber, B. (2022): Smarte Schieneninstandhaltung in der Metro Barcelona, in: Der Eisenbahningenieur (EI), Jg. 73, Nr. 03, S. 22 – 26

[8] **Bundesministerium für Digitales und Verkehr (BMDV)** (2021): Onboard-Daten für die Erkennung von Gleisfehlstellen – OnboardEU [Online], [Zugriff am: 08.02.2023]. Verfügbar unter: https://bmdv.bund.de/SharedDocs/DE/Artikel/DG/mfund-projekte/onboardeu.html

[9] **Asmussen, B. (UIC)** (2013): Description of the vibration generation mechanism of turnouts and the development of cost effective mitigation measures (WP 3.3), [Zugriff am: 08.02.2023]. Verfügbar unter: http://www.rivas-project.eu/fileadmin/documents/RIVAS_UIC_WP3-3_D3_6_V01.pdf

[10] **Automotive & Rail Innovation Center (ARIC)** (2021): Rangierassistent als Vorstufe zum autonomen Betrieb, in: Der Eisenbahningenieur (EI), Jg. 70, Nr. 04, S. 62

[11] **Amberg Group** (2022): Amberg: Neues Messsystem für Gleisgeometrieprüfungen, in: Der Eisenbahningenieur (EI), Jg. 73, Nr. 05, S. 12

[12] **Prof Dr. Freudenstein**, S.; Kotter, F.; Lillin, N.; Prof. Dr. Martin, U.; Mitlmeier, F.; Prof. Dr. Moormann, C. (2022): Frühzeitige Detektion von punktuellen Instabilitäten an Bahnkörpern in konventioneller Schotterbauweise [Online], in: ZEVrail, Jg. 146, Nr. 03, [Zugriff am: 11.04.2022]. Verfügbar unter: https://www.zevrail.de/artikel/fruehzeitige-detektion-von-punktuellen-instabilitaeten-bahnkoerpern-konventioneller

[13] **Lang**, H. P. (2021): Digital- und Technikstrategie der DB, in: Eisenbahntechnische Rundschau (ETR) Jg. 70 Jubiläumsausgabe, Nr. 10, S. 56 – 62

[14] **ZEVrail Nachrichtenredaktion** (2021): ZF und DB Systemtechnik vereinbaren Zusammenarbeit [Online], in: ZEVrail, 15.09.2021, [Zugriff am: 20.04.2022]. Verfügbar unter: https://www.zevrail.de/news/zf-und-db-systemtechnik-vereinbaren-zusammenarbeit

[15] **SYN_Sensoren Inside Redaktion** (o. A.): Sensoren für Bahn- und Schienenverkehr [Online], in: SYN_Sensoren, [Zugriff am: 24.03.2022]. Verfügbar unter: https://www.hbm.com/de/2393/messtechnik-auf-der-schiene/

[16] **Antony**, B.; Dr. Fellinger, M.; Dr. Hansmann, F.; Prof. Dr. Marsching, S.; Dr. Neuhold, J. (2021): Einzelfehler der Gleislage und ihre Behebung – ein internationaler Benchmark [Online], in: ZEVrail, Jg. 145, Nr. 10, [Zugriff am: 20.04.2022]. Verfügbar unter: https://www.zevrail.de/artikel/einzelfehler-der-gleislage-und-ihre-behebung-ein-internationaler-benchmark

[17] **Kraft**, C.; Master of Arts Europ. Studies (2020): Testanlagen für die Digitalisierung im Bahnsektor, Teil 2 [Online], in: ZEVrail, Jg. 144, Nr. 01/02, [Zugriff am: 31.05.2022]. Verfügbar unter: https://www.zevrail.de/artikel/testanlagen-fuer-die-digitalisierung-im-bahnsektor-teil-2

[18] **Casper**, M.; Grippenkoven, J.; Hungar, H.; Meirich, C.; Roth, M. (2020): Teleoperierte Triebfahrzeugführung als Rückfallebene der Hochautomation, in: Signal+Draht, Jg. 112, Nr. 06, S. 6 – 13

[19] **Dr. Robl**, C.; Sagmeister, C.; Dr. Schild, R.; Prof. Dr. Schnieder, E.; Stättner, M. (2019): Sichere, hochgenaue und verfügbare Lokalisierung für gleisgebundene Objekte [Online], in: ZEVrail, Jg. 143, Sonderheft Graz, [Zugriff am: 22.06.2022]. Verfügbar unter: https://www.zevrail.de/artikel/sichere-hochgenaue-und-verfuegbare-lokalisierung-fuer-gleisgebundene-objekte

[20] **Falgenhauer**, R.; Franzen, J.; Geischberger, J.; Grunwald, A.; Hanisch, R. (2021): RangierTerminal4.0: Automatisiertes Rangiegen im JadeWeserPort, in: Der Eisenbahningenieur (EI), Jg. 72, Nr. 12, S. 43 – 46

[21] **ZEVrail Nachrichtenredaktion** (2020): Zuverlässig ins Ziel [Online], in: ZEVrail, 16.09.2020, [Zugriff am: 20.05.2022]. Verfügbar unter: https://www.zevrail.de/news/zuverlassig-ins-ziel

[22] **PJM; SBB Cargo** (2021): Bahntechnische Gesamtlösungen für den weltweiten Schienenverkehr von PJM, in: Eisenbahntechnische Rundschau (ETR), Jg. 70 Jubiläumsausgabe, Nr. 10

[23] **Bremer**, B.; Franke, U.; Hübner, L.; Jonas-Kops, J. (2021): SensoDIMARiS: Das Ohr an der Maschine für zustandsbasierte und vorausschauende Instandhaltung, in: Eisenbahntechnische Rundschau (ETR), Jg. 70, Nr. 09, S. 58 – 63

[24] **Glöckner**, S.**;** Pakull, T. (2021): Digitalisierung von 16,7 Hz-Bestandsunterwerken, in: Elektrische Bahnen (eb), Jg. 119, Nr. 06, S. 250 – 266

[25] **DB Systemtechnik** (o. A.): Detektionsanlage für unrunde Räder (DafuR) [Online], [Zugriff am: 15.03.2022]. Verfügbar unter: https://www.db-systemtechnik.de/resource/blob/1664918/7f09f08949f64178c97f5c742bbde8e4/27_p_D_detektionsanlage_dafur-data.pdf

[26] **RailWatch/Metrans** (2021): Zustandserfassung von Güterzügen, in: Der Eisenbahningenieur (EI), Jg. 72, Nr. 07, S. 54

[27] **Dr. Achs**, G.; Hauser, T.; Maicz, D.; Töll, H. (2021): Immissionsschutz auf Basis eines jahrelangen Monitorings mittels Oberbau-Messanlagen [Online], in: ZEVrail, Jg. 145, Nr. 11/12, [Zugriff am: 11.03.2022]. Verfügbar unter: https://www.zevrail.de/artikel/immissionsschutz-auf-basis-eines-jahrelangen-monitorings-mittels-oberbau-messanlagen

[28] **Dr. Achs**, G.; Hauser, T.; Maicz, D.; Töll, H. (2020): Oberbau-Messanlagen als Instrument für Gleis- und Fahrzeuginstandhaltung, in: Eisenbahntechnische Rundschau (ETR), Jg. 69, Nr. 7+8, S. 52 – 56

[29] **Dr. Mittermayr**, P.; Schmid, R.; Zottl, W. (2019): Messung von Radprofilen und Fahrstabilität bei bis zu 250 km/h [Online], in: ZEVrail, Jg. 143, Sonderheft Graz, [Zugriff am: 22.06.2022]. Verfügbar unter: https://www.zevrail.de/artikel/messung-von-radprofilen-und-fahrstabilitaet-bei-bis-zu-250-kmh

[30] **Wassenberg**, M. (2021): Dynamische Gewichtsmessung im Güterverkehr, in: Eisenbahntechnische Rundschau (ETR), Jg. 70, Nr. 06, S. 58 – 59

[31] **Paulovic**, P. (2021): Anwendungsbereiche von Fiber Optic Sensing im digitalen Bahnsystem, in: Eisenbahntechnische Rundschau (ETR), Jg. 70, Nr. 04, S. 17 – 19

[32] **Grundnig, G.**; Pucher, C. (2014): Anwendungsmöglichkeiten von Raddetektionssystemen mit induktiven Radsensoren, in: Signal+Draht, Jg. 106, Nr. 06, S. 24 – 28

[33] **Dr. Attinger**, R.; Dr. Beckenbauer, T. (2020): Bahnlärmmonitoring in der Schweiz-Erkennung lauter Güterwagen, in: Eisenbahntechnische Rundschau (ETR), Jg. 69, Nr. 11, S. 20 – 25

[34] **Saewe**, J.; Dr. Stollenwerk, J.; Dr. Vedder, C.; Vervoort, S. (2021): Intelligente Sensorik für die Bahn - Sicherheit und Service durch LPBF und KI [Online], in: Fraunhofer ILT, [Zugriff am: 24.03.2022]. Verfügbar unter: https://www.ilt.fraunhofer.de/de/presse/pressemitteilungen/2021/10-29-intelligente-sensorik-im-forschungsprojekt-sensetrain.html

[35] **Hempe**, T.; Obrenovic, M.; Schmid, G.; Thiele, T. (2021): Digitale Instandhaltung - Das Projekt "E-Check" bei der DB Fernverkehr AG, in: Der Eisenbahningenieur (EI), Jg. 72, Nr. 11, S. 62 – 64

[36] **Steger**, M. (2022): Roboterbasierte Instandhaltung von Fahrzeug und Fahrweg, in: Der Eisenbahningenieur (EI), Jg. 73, Nr. 03, S. 14 – 16

[37] **Dr. Quintus**, E. (2021): Rädermanagement – Wie eine optimierte Instandhaltungsplanung die Fahrzeugverfügbarkeit erhöht und zu einem verbesserten Räderzustand führt [Online], in: ZEVrail, Jg. 145, Sonderheft Graz, [Zugriff am: 04.05.2022]. Verfügbar unter: https://www.zevrail.de/artikel/raedermanagement-wie-eine-optimierte-instandhaltungsplanung-die-fahrzeugverfuegbarkeit

[38] **DB Inside Redaktion** (2021): Digitale Weichendiagnose mit DIANA [Online], in: DB Inside, [Zugriff am: 15.03.2022]. Verfügbar unter: https://inside.bahn.de/digitale-weichendiagnose-diana/

[39] **Ilge**, F. (2020): Überwachung von Weichensteuerungen und Fernsteuerung von Weichenheizungen Straßenbahnen, in: Signal+Draht, Jg. 112, Nr. 03, S. 23 – 28

[40] **Bernerstätter**, R.; Steindl, M.; Vidovic, I. (2021): Die Weiche: smarte(ste) Komponente der Eisenbahninfrastruktur, in: Der Eisenbahningenieur (EI), Jg. 72, Nr. 10, S. 25 – 29

[41] **Grundnig, G.**; Pucher, C. (2014): Anwendungsmöglichkeiten von Raddetektionssystemen mit induktiven Radsensoren, in: Signal+Draht, Jg. 106, Nr. 06, S. 24 – 28

[42] **Iris-GmbH** (2020): IRMA Matrix, [Zugriff am: 10.01.2023]. Verfügbar unter: https://www.iris-sensing.com/fileadmin/user_upload/support/IRMA_MATRIX/DE/Produktinformationen/2109_IRMA_MATRIX_DE.pdf

[43] **Verdict Media Limited** - Railway Technology – Smart Light Grids (o. A.): Smart Light Grids [Online], [Zugriff am: 11.01.2023]. Verfügbar unter: https://www.railway-technology.com/products/smart-light-grids/

[44] **DOT Telematik und Systemtechnik GmbH** (o. A.): X-Rayl Solar Pointer S3 mit Türsensor [Online], [Zugriff am: 11.01.2023]. Verfügbar unter: https://www.dot-telematik.com/loesungen/telematik-hardware/x-rayl-solar-pointer-mit-tuersensor/

[45] **Janicki, J., Reinhard, H.** (2008): Schienenfahrzeugtechnik, 2. Überarbeitete und erweiterte Auflage, Mainz: Bahn Fachverlag Heidelberg

[46] **Hüning, F.** (2016): Sensoren und Sensorschnittstelle, 1. Auflage, Oldenburg: De Gruyter Studium

[47] **Kuther, Thomas** (2019): Sensoren für die Elektromobilität [Online], [Zugriff am: 18.11.2022]. Verfügbar unter: https://www.next-mobility.de/sensoren-fuer-die-elektromobilitaet-a-893353/

[48] **HBM** (o. A.): Methoden zur Drehmomentmessung [Online], [Zugriff am: 08.05.2022]. Verfügbar unter: https://www.hbm.com/de/3706/tips-und-tricks-methoden-zur-drehmomentmessung/

[49] **Meyer, Manfred** (1985): Elektrische Antriebstechnik Band 1, Berlin, Heidelberg: Springer Verlag GmbH

[50] **RailWatch GmbH** (o. A.): Die Produkte – Vorausschauende Instandhaltung für alle [Online], [Zugriff am: 09.02.2023]. Verfügbar unter: https://www.rail-watch.com/de/produkte

[51] **iMAR Navigation GmbH im Auftrag des Deutschen Zentrums für Schienenverkehrsforschung beim Eisenbahn-Bundesamt (DZSF)** (2022): Mindestausrüstung von Güterwagen – Effektives und wirtschaftliches Condition Monitoring für zustandsorientierte Instandhaltung, Bericht 26 (2022), Dresden: DZSF

[52] **GRT Global Rail Academy and Media GmbH – TrackPedia** (o. A.): Digitale Weichendiagnose [Online], [Zugriff am: 15.12.2022]. Verfügbar unter: https://www.trackopedia.com/lexikon/infrastruktur/weiche/digitale-weichendiagnose

[53] **Obermayr, G.** (o. A.): Weichendiagnose [Online], [Zugriff am: 15.12.2022]. Verfügbar unter: https://www.eisenbahn.gerhard-obermayr.com/produzenten/vae/die-weichendiagnose/

[54] **BDS Solutions GmbH** (o. A.): BoltValid [Online], [Zugriff am: 15.12.2022]. Verfügbar unter: https://bds-solutions.de/BoltValid.html

[55] **Technischer Innovationskreis Schienengüterverkehr (TIS)** (o. A.): ITSS – Industrieplattform für Telematik und Sensorik im Schienengüterverkehr [Online], [Zugriff am: 15.01.2023]. Verfügbar unter: https://tis.ag/downloads/

[56] **Schubert**, S. (2007): Wettbewerbsvorteile durch Vereinheitlichung am Beispiel der europäischen Schienenfahrzeugindustrie, Dissertation, Martin-Luther-Universität Halle-Wittenberg

[57] **Neumann**, L.; Krippendorf, W. (2016): Branchenanalyse Bahnindustrie: Industrielle und betriebliche Herausforderungen und Entwicklungskorridore, Study der Hans-Böckler-Stiftung, No. 331, ISBN 978-3-86593-239-6, Hans-Böckler-Stiftung, Düsseldorf

[58] **Gille**, J.; de Swart, L.; Giannelos, I.; Delory, E., Castro, A. (2014): Marine sensors; the market, the trends and the value chain [Online], Conference: Sensor Systems for a Changing Ocean (SSCO), 2014 IEEE, [Zugriff am: 17.12.2022]. Verfügbar unter DOI: http://dx.doi.org/10.1109/SSCO.2014.7000369

[59] **Llobet**, E. (2019): Advanced Nanomaterials for Inexpensive Gas Microsensors. Synthesis, Integration and Applications, ISBN 9780128148280, Amsterdam: Elsevier

[60] **Rehme**, M.; Oehme, S.; Götze, U.; Claus, S. (2020): Smart Rail – Bewertung von Innovationsideen und Management von Innovationsbarrieren am Beispiel integrierter Mobilitätsketten für ländliche Räume, in: Proff, H. (Hrsg.): Neue Dimensionen der Mobilität. Technische und betriebswirtschaftliche Aspekte, Wiesbaden: Springer, S. 107 – 125

[61] **Singh**, P.; Elmi, Z.; Meriga, V. K.; Pasha, J.; Dulebenets, M. A. (2022): Internet of Things for sustainable railway transportation: Past, present, and future, in: Cleaner Logistics and Supply Chain, Vol. 4, 100065, doi: https://doi.org/10.1016/j.clscn.2022.100065

[62] **Krips**, D. (2017): Stakeholdermanagement – Kurzanleitung, Heft 5, 2. Auflage, Berlin, Heidelberg: Springer

[63] **Gesmann-Nuissl**, D, (2022): Sachbericht zum Verwendungsnachweis des WIR!-Projekts KI-bezogene Test- und Zulassungsmethoden (SRCC-KI), FKZ 03WIR1205, TU Chemnitz

[64] **Abdelkafi**, N.; Makhotin, S.; Posselt, T. (2013): (Business Model) Innovations for Electric Mobility – What can be learned from existing Business Model Patterns?, in: International Journal of Innovation Management, Vol. 17, No. 1, 1340003, S. 12

[65] **Witte**, S.; Gerke, S.; Hess, R.; Röckermann, K. (2020): Fachbericht ‚Identifikation von Standards bei der Strom-/Datenversorgung' – Erstellung eines Konzeptes für die EU weite Migration eines Digitalen Automatischen Kupplungssystems (DAK) für den Schienengüterverkehr, Ort: OWITA GmbH, Lemgo. Verfügbar unter: https://www.bmvi.de/SharedDocs/DE/Anlage/E/fachbericht-dak-studie-strom-daten.pdf?__blob=publicationFile

[66] **DIN** (1995): DIN 1319-1 Blatt 1 Grundlagen der Messtechnik

[67] **Pepperl+Fuchs** (2012): Intelligente Sensoren rationell via IO-Link anbinden. Sensorschnittstelle zur Übertragung sämtlicher Kommunikationsdaten Hg. v. TIMGlobal Media. [Online], [Zugriff am: 23.01.2024]. Verfügbar unter: https://www.ien-dach.de/artikel/intelligente-sensoren-rationell-via-io-link-anbinden/

[68] **Dabacan, M.** (2020): Pulsmodulationstechnik verstehen und anwenden [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.elektronikpraxis.de/pulsmodulationstechnik-verstehen-und-anwenden-a-2107022bd1d3b1c54617d91556bad8e7/

[69] **Viehmann, O.** (2022): Geberschnittstellen für hochdynamische Positionieranwendungen [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.konstruktionspraxis.vogel.de/geberschnittstellen-fuer-hochdynamische-positionieranwendungen-a-fb64bae44d90c27b01faad21d37f5500/

[70] **EIA/TIA-232-F:1997-10**, Interface Between Data Terminal Equipment and Data Circuit- Terminating Equipment Employing Serial Binary Data Interchange

[71] **EIA/TIA-422-B:1994-05**, Electrical Characteristics of Balanced Voltage Digital Interface Circuits

[72] **EIA/TIA-485-A:1998-03**, Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems

[73] **Pepperl+Fuchs** (2011): Sensorschnittstellen Busfähige Sensoren [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: http://files.pepperl-fuchs.com/catalog/files/assets/downloads/page0013.pdf

[74] **White, T.** (2022): Grundlagen der SENT-Schnittstelle für Sensordaten [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.all-electronics.de/elektronik-fertigung/grundlagen-der-sent-schnittstelle-fuer-sensordaten-61-211.html

[75] **Wörner, N.** (2018): Mit PSI-Kräften vernetzen [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.elektroniknet.de/messen-testen/sensorik/mit-psi-kraeften-vernetzen.158603.html

[76] **NXP** (2021): I²C-bus specification and user manual [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.nxp.com/docs/en/user-guide/UM10204.pdf

[77] **Dhaker**, P. (o. A.): Introduction to SPI Interface [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.analog.com/en/resources/analog-dialogue/articles/introduction-to-spi-interface.html

[78] **AS-International Association e.V.** (o. A.): Economical and easy [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.as-interface.net/en/technology

[79] **CAN in Automation e.v.** (o. A.): CAN: From physical layer to application layer and beyond [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.can-cia.org/can-knowledge

[80] **CAN in Automation e.v.** (o. A.): CANopen – The standardized embedded net-work [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.can-cia.org/can-knowledge/canopen

[81] **WAGO GmBH & Co. KG** (o. A.): Einfach automatisieren mit LonWorks [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.wago.com/de/lonworks

[82] **FieldComm Group** (o. A.): HART – DIGITAL TRANSFORMATION FOR ANALOG INSTRUMENTS [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.fieldcommgroup.org/technologies/hart

[83] **CC-Link Partner Association** (o. A.): CC-Link V1.10/V2 Specifications [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.cc-link.org/en/cclink/spec.html?spec_4

[84] **ODVA** (o.A.): ControlNet ODVA [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.odva.org/technology-standards/other-technologies/controlnet/

[85] **ODVA** (o.A.): DeviceNet ODVA [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.odva.org/technology-standards/key-technologies/devicenet/

[86] **OMS** (2011): Open Metering System Specification [Online], [Zugriff am: 26.10.2023]. Verfügbar unter: https://oms-group.org/fileadmin/files/download4all/specification/Vol2/4.1.2/OMS-Spec_Glossary_v101.pdf

[87] **Modbus.org** (2006): MODBUS over Serial Line Specification and Implemen-tation Guide V1.02 [Online], [Zugriff am: 26.10.2023]. Verfügbar unter: https://modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

[88] **Farnell** (2024): Farnell Deutschland – Anbieter von elektronischen Bauteilen [Online], [Zugriff am: 31.o1.2024]. Verfügbar unter: https://de.farnell.com/

[89] **Digi-Key Corporation** (2024): DigiKey Deutschland – Distributor elektronischer Komponenten [Online], [Zugriff am:31.01.2024]. Verfügbar unter: unter https://www.digikey.de/

[90] **Pepperl+Fuchs** (2024): Pepperl+Fuchs Deutschland. Industrielle Sensoren + Explosionsschutz [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.pepperl-fuchs.com/germany/de/index.htm

[91] **Lenord**, Bauer & Co. (2024): Startseite: Lenord+Bauer [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.lenord.de/

[92] **SICK** (2024): SICK. Sensor Intelligence [Online], [Zugriff am: 31.01.2024]. Verfügbar unter https://www.sick.com/de/de/

[93] **Hüning**, Felix (2016): Sensoren und Sensorschnittstellen. Berlin, Boston: De Gruyter Oldenbourg (De Gruyter Studium). Verfügbar unter: http://www.degruyter.com/view/product/458022.

[94] **PROFIBUS Nutzerorganisation** (o. D.): IO-Link im Durchblick [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://io-link.com/de/Technologie/Was_ist_IO-Link.php?thisID=63

[95] **McGrath**, Michael J. (2013): Sensor Technologies. Healthcare, Wellness, and Environmental Applications. Erscheinungsort nicht ermittelbar: Springer Nature [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://library.oapen.org/bitstream/id/1bf313b6-d2d3-4846-8110-0644d12c532b/1001841.pdf

[96] **Schütze**, Andreas; Helwig, Nikolai; Schneider, Tizian (2018): Sensors 4.0 – smart sensors and measurement technology enable Industry 4.0. In: J. Sens. Sens. Syst. 7 (1), S. 359 – 371. DOI: 10.5194/jsss-7-359-2018.

[97] **European Technology Platform on Smart Systems Integration** (o. A.): SSI Smart Systems Integration. EPoSS [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.smart-systems-integration.org/ssi-smart-systems-integration

[98] **McGrath**, Michael J. (2013): Sensor Technologies. Healthcare, Wellness, and Environmental Applications. Erscheinungsort nicht ermittelbar: Springer Nature [Online], [Zugriff am: 31.01.2024].

Verfügbar unter: https://library.oapen.org/bitstream/id/1bf313b6-d2d3-4846-8110-0644d12c532b/1001841.pdf, S. 84 ff.

[99] **KUNBUS** (o. D.): Feldbus Grundlagen [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.kunbus.com/de/feldbus-grundlagen

[100] **BACnet** (o.A.): Building Automation and Control Network [Online], [Zugriff am: 26.02.2024]. Verfügbar unter: https://bacnet.org/

[101] **CC-Link Partner Association** (o. A.): CC-Link IE Field Network [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.cc-link.org/en/cclink/cclinkie/cclinkie_f.html

[102] **CC-Link Partner Association** (o. A.): Wireless Network [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.cc-link.org/en/cclink/wireless/index.html#guideline

[103] **EtherCAT Technology Group** (o. A.): EtherCat der Ethernet-Feldbus [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.ethercat.org/de.htm

[104] **ODVA** (o.A.): EtherNet/IP ODVA [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.odva.org/technology-standards/key-technologies/ethernet-ip/

[105] **Wiesemann & Theis GmbH** (o. A.): Modbus-TCP Standardprotokoll für Auto-matisierungstechnik [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.wut.de/e-57www-04-apde-000.php

[106] **B&R Industrial Automation GmbH** (o. A.): Ethernet Powerlink [Online], [Zugriff am: 22.01.2024]. Verfügbar unter: https://www.br-automation.com/en/technologies/powerlink/

[107] **PROFIBUS Nutzerorganisation e.V.** (PNO) (o. A.): PROFIBUS Nutzerorganisation e.V. (PNO) [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.profibus.com/technologies/profinet/technology

[108] **SERCOS the automation bus** (o. A.): Die Sercos Technologie: Bewährt, einfach, schnell, offen [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.sercos.de/technologie/was-ist-sercos/

[109] **Brun, R., Rausch, R.** (2001): WorldFIP [Vortrag, Online], [Zugriff am: 24.11.2022]. Verfügbar unter: https://qps.web.cern.ch/download/pdf/FIP_protocole_JCOP_short4.pdf

[110] **DB InfraGO** (o. A.): GSM-R [Online], [Zugriff am: 24.11.2022]. Verfügbar unter: https://www.dbinfrago.com/web/schienennetz/gsm-r

[111] **Telekom** (o. A.): LTE: Wie es funktioniert. Was es kann. Wo es verfügbar ist. [Online], [Zugriff am: 24.11.2022]. Verfügbar unter: https://www.telekom.com/de/konzern/details/die-neun-wichtigsten-fakten-zu-lte-604990

[112] **BSI** (o. A.): Was versteht man unter 5G? [Online], [Zugriff am: 24.11.2022]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/5G/5g-was-versteht-man-darunter.html

[113] **Deutsche Bahn AG** (o. A.): FRMCS/5G-Datenkommunikation [Online], [Zugriff am: 24.11.2022]. Verfügbar unter: https://www.digitale-schiene-deutschland.de/FRMCS-5G-Datenkommunikation

[114] **Bluetooth SIG** (o. A.): Bluetooth® Drahtlose Technologie [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.bluetooth.com/de/learn-about-bluetooth/tech-overview/

[115] **LineMetrics GmbH** (2020): Endlich verständlich: LoRa (und LoRaWAN) einfach erklärt! [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.linemetrics.com/de/lora-und-lorawan-einfach-erklaert/

[116] **Connectivity Standards Alliance** (o. A.): zigbee The FULL-Stack Solution for All Smart Devices [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://csa-iot.org/all-solutions/zigbee/

[117] **Z-Wave Alliance** (o. A.): How Z-Wave Works [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://z-wavealliance.org/learn-about-z-wave/

[118] **BMWK** (o.A.) 6LoWPAN [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Redaktion/DE/Standardartikel/Themen-und-Technologiekatalog/6lowpan.html

[119] **BSI** (o. A.): Radio Frequency Identification (RFID) [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/RFID/rfid_node.html

[120] **Deutsche Telekom IoT GmbH** (o. A.): NarrowBand IoT / LTE-M [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://iot.telekom.com/de/netze-tarife/narrowband-iot-lte-m

[121] **Infineon Technologies AG** (o. A.): Wissenswertes zu Near Field Communication (NFC) [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.infineon.com/cms/de/discoveries/near-field-communication/

[122] **Recommendation ITU-T X.200** (1994): Information technology – Open Systems Interconnection – Basic Reference Model [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://handle.itu.int/11.1002/1000/2820

[123] **Cerf**, Vinton G.; Cain, Edward (1983): The DoD internet architecture model. In: Computer Networks (1976), 7 (5), S. 307-318. DOI: 10.1016/0376-5075(83)90042-9.

[124] **Obermaier, D.** (2017): So funktioniert MQTT [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.elektroniknet.de/kommunikation/so-funktioniert-mqtt.148672.html

[125] **imc Test & Measurement GmbH** (2023): imc Feldbus-Anbindungen [Technisches Datenblatt, Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.imc-tm.de/fileadmin/Public/Downloads/Datasheets/imc_optional_accessories/imc_Accessories_DE_TDs/TD_Feldbus-Anbindungen.pdf

[126] **Peeriot** (2023): Peeriot. Peer-to-peer meets IoT [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.peeriot.io/

[127] **ComputerWeekly.de**, TechTarget (2016): HDLC (High-Level Data Link Control) [Online], [Zugriff am: 23.11.2023]. Verfügbar unter: https://www.computerweekly.com/de/definition/HDLC-High-Level-Data-Link-Control

[128] **Deinhard, F.** (2024): Was ist Advanced Message Queuing Protocol (AMQP)? [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.it-schulungen.com/wir-ueber-uns/wissensblog/was-ist-advanced-message-queuing-protocol-amqp.html

[129] **Luber, S**; Litzel N. (2021): Was ist das Constrained Application Protocol (CoAP)? [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.bigdata-insider.de/was-ist-das-constrained-application-protocol-coap-a-1039737/

[130] **DDS Foundation** (o. A.): What is DDS? [Online], [Zugriff am: 24.11.2023]. Verfügbar unter: https://www.dds-foundation.org/what-is-dds-3/

[131] **Van Eijk, P**; Eckstein, M. (2019): LoRaWAN im Detail: So arbeitet die IoT-Funktechnik [Online], [Zugriff am: 27.11.2023]. Verfügbar unter: https://www.elektronikpraxis.de/lorawan-im-detail-so-arbeitet-die-iot-funktechnik-a-836031/

[132] **Girdvainis, D**; Rathfelder C (2019): Dynamic LwM2M Data Model Mapping to OPC UA [Paper, Online], [Zugriff am: 27.11.2023]. Verfügbar unter: https://stag.hahn-schickard.de/assets/resources/publications/LwM2M%20Mapping%20paper.pdf

[133] **PubNUB** (o. A.): What is XMPP? [Online], [Zugriff am: 27.11.2023]. Verfügbar unter: https://www.pubnub.com/guides/xmpp/

[134] **Di Paolo Emilio**, Maurizio (2013): Data Acquisition Systems: From Fundamentals to Applied Design. Niederlande: Springer New York. DOI: 10.1007/978-1-4614-4214-1

[135] **Terra**, John (2024): What Is Data Processing? Definition, Examples, Trends [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://pg-p.ctme.caltech.edu/blog/data-science/what-is-data-processing-examples-trends

[136] **Britannica**, The Editors of Encyclopaedia (2024): markup language. Encyclopedia Britannica [Online], [Zugriff am: 23.02.2024]. Verfügbar unter: https://www.britannica.com/technology/markup-language

[137] **Fleischmann**, Albert (2018): Ganzheitliche Diitalisierung Von Prozessen. Perspektivenwechsel - Design Thinking – Wertegeleitete Interaktion. Unter Mitarbeit von Stefan Oppl, Werner Schmidt und Christian Stary. Wiesbaden: Springer Fachmedien Wiesbaden GmbH [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6422823

[138] **Engels**, Gregor (2019): Modellierungssprache. Unter Mitarbeit von Norbert Gronau, Jörg Becker, Natalia Kliewer und Jan Marco Leimeister. Hg. v. Sven Overhage. GITO. Berlin (Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon) [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://wi-lex.de/index.php/lexikon/technologische-und-methodische-grundlagen/sprache/modellierungssprache/

[139] **Becker, Klaus-Peter** (2014): Exkurs – Datenformate [Online], [Zugriff am: 25.01.2024]. Verfügbar unter: https://web.archive.org/web/20151121055617/http://inf-schu-le.de/information/informationsdarstellungxml/xmlsprachen/exkurs_datenformat

[140] **OPC Router** (o. A.): Was ist JSON? Praxisnahes Basiswissen. inray Industriesoftware GmbH [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.opc-router.de/was-ist-json/

[141] **Recommendation ITU-T Y.2060** (2012): Y series: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities. Next Generation Networks – Frameworks and functional architecture models [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://handle.itu.int/11.1002/1000/11559

[142] **Grosch**, Dorian (2021): Das Öfit-Trendsonar Internet der Dinge. 1. Auflage. Berlin: Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS (Forschung für den digitalen Staat).

[143] **Plattform Industrie 4.0** (o. A.): Was ist Industrie 4.0? Bundesministerium für Wirtschaft und Klimaschutz, Referat Soziale Medien/Online-Kommunikation [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html

[144] **Schulz**, Christopher (o. A.): Das Datenmodell – die Strukturen eines Anwendungsbereiches eindeutig erfassen. Palladio Consulting [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.palladio-consulting.de/datenmodell/

[145] **Ernst, Susanne** (o. A.): Was ist ein Austauschformat? [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://nexoma.de/austauschformat/

[146] **Rhayem**, Ahlem; Mhiri, Mohamed Ben Ahmed; Gargouri, Faiez (2020): Semantic web technologies for the internet of things: Systematic literature review. In: Internet of Things, 11, 100206. DOI: 10.1016/j.iot.2020.100206

[147] **Projekt** (2018): Semantics for PerfoRmant and scalable INteroperability of multimodal Transport – SPRINT [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://cordis.europa.eu/project/id/826172

[148] **W3C** (2013): W3C SEMANTIC WEB ACTIVITY [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/2001/sw/

[149] **W3C** (2014): RDF Schema 1.1 [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/TR/rdf-schema/

[150] **W3C** (2001): DAML+OIL [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/TR/daml+oil-reference/

[151] **Kifer, M.** (2005): Rules and Ontologies in F-Logic, in Reasoning Web, S. 22 – 34, ISBN 0302-9743, Heidelberg: Springer Verlag Berlin

[152] **W3C** (2012): Web Ontology Language (OWL) [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/OWL/

[153] **W3C** (2005): Web Service Modeling Language (WSML) [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/submissions/WSML/

[154] **W3C** (2004): Overview of SGML Resources [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/MarkUp/SGML/

[155] **W3C** (2024): HTML Living Standard [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://html.spec.whatwg.org/multipage/

[156] **Adobe** (o. A.): Evolution of the PostScript Language [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.adobe.com/de/products/postscript.html

[157] **Adobe** (o. A.): Rich Text Format: Was genau ist eine RTF-Datei? [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.adobe.com/de/acrobat/resources/document-files/text-files/rtf-file.html

[158] **The LATEX Project** (o. A.): LaTeX – A document preparation system [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.latex-project.org/

[159] **W3C** (2008): Extensible Markup Language (XML) [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/TR/REC-xml/

[160] **YAML Language Development Team** (2021): YAML Ain't Markup Language (YAML™) version 1.2 [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://yaml.org/spec/1.2.2/

[161] **W3C** (2011): Scalable Vector Graphics (SVG) 1.1 (Second Edition)) [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.w3.org/TR/SVG11/

[162] **Studyflix GmbH** (o. A.): Programmablaufpläne [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://studyflix.de/informatik/programmablaufplane-828

[163] **Drust, D.**; Hertkorn, S.; Eischer, C.; Schweisser, N.; (2020): Petri-Netze einfach erklärt – Definition und Erklärung! [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://der-prozess-manager.de/aktuell/wissensdatenbank/petri-netz

[164] **DATACOM Buchverlag GmbH** (2013): specification and description language (SDL) [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.itwissen.info/specification-and-description-language-SDL.html

[165] **BSON** (o. D.): BSON (Binary JSON) Serialization [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://bsonspec.org/

[166] **Google LLC** (2024): Protocol Buffers Version 3 Language Specification [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://protobuf.dev/reference/protobuf/proto3-spec/

[167] **Kleinemeier**, Michael (2014): Von der Automatisierungspyramide zu Unternehmenssteuerungsnetzwerken. In: Thomas Bauernhansl, Michael ten Hompel und Birgit Vogel-Heuser (Hg.): Industrie 4.0 in Produktion, Automatisierung und Logistik. Wiesbaden: Springer Fachmedien Wiesbaden, S. 571 – 579.

[168] **Meudt**, Tobias; Pohl, Malte; Metternich, Joachim (2017): Die Automatisierungspyramide - Ein Literaturüberblick. Technische Universität Darmstadt. Darmstadt [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://tuprints.ulb.tu-darmstadt.de/id/eprint/6298

[169] **Heinrich**, Berthold; Linke, Petra; Glöckler, Michael (2020): Grundlagen Automatisierung. Erfassen – Steuern – Regeln. 3., überarbeitete und erweiterte Auflage. Wiesbaden: Springer Vieweg (Springer eBooks Computer Science and Engineering).

[170] **Bettenhausen**, Kurt D.; Kowalewski, Stefan (2013): Cyber-Physical Systems. Chancen und Nutzen aus Sicht der Automation. Verein Deutscher Ingenieure e.V., VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA). Düsseldorf (Thesen und Handlungsfelder) [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.vdi.de/ueber-uns/presse/publikationen/details/cyber-physical-systems-chancen-und-nutzen-aus-sicht-der-automation

[171] **Kagermann**, Henning; Wahlster, Wolfgang; Helbig, Johannes (2013): Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Deutschlands Zukunft als Produktionsstandort sichern. Abschlussbericht des Arbeitskreises Industrie 4.0. Promotorengruppe Kommunikation der Forschungsunion Wirtschaft – Wissenschaft. Frankfurt/Main [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.bmbf.de/bmbf/shareddocs/downloads/files/umsetzungsempfehlungen_industrie4_0.html

[172] **IEC PAS 63088:2017-03**, Smart manufacturing – Reference architecture model industry 4.0 (RAMI4.0)

[173] **Plattform Industrie 4.0** (2019): Leitbild 2030 für Industrie 4.0 – Digitale Ökosysteme global gestalten. Positionspapier. Bundesministerium für Wirtschaft und Energie (BMWI), Öffentlichkeitsarbeit. Berlin [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/Leitbild-2030-f%C3%BCr-Industrie-4.0.html

[174] **Plattform Industrie 4.0** (2018): RAMI 4.0 Ein Orientierungsrahmen für die Digitalisierung. Berlin [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/rami40-eine-einfuehrung.html

[175] **Lin**, Shi-Wan; et al. (2017): Architecture Alignment and Interoperability. An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper (IIC:WHT:IN3:V1.0:PB:20171205) [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/whitepaper-iic-pi40.html

[176] **Plattform Industrie 4.0** (2018): Referenzarchitekturmodell 4.0. Plattform Industrie 4.0 und ZVEI [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Redaktion/DE/Infografiken/referenzarchitekturmodell-4-0.html

[177] **Plattform Industrie 4.0** (2018): RAMI 4.0 - Ein Orientierungsrahmen für die Digitalisierung. Berlin [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/rami40-eine-einfuehrung.pdf?__blob=publicationFile&v=1

[178] **Plattform Industrie 4.0** (2019): Die Verwaltungsschale im Detail. von der Idee zum implementierbaren Konzept. Berlin [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/verwaltungsschale-im-detail-pr%C3%A4sentation.pdf?__blob=publicationFile&v=1

[179] **Boyes**, Hugh; Hallaq, Bil; Cunningham, Joe; Watson, Tim (2018): The industrial internet of things (IIoT): An analysis framework. In: Computers in Industry 101, S. 1 – 12. DOI: 10.1016/j.compind.2018.04.015.

[180] **OPC Foundation** (o. A.): What is OPC? [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://opcfoundation.org/about/what-is-opc/

[181] **OPC Foundation** (o. D.): Unified Architecture. [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://opcfoundation.org/about/opc-technologies/opc-ua/

[182] **Eclipse Foundation** (o. D.): The Sparkplug Specification [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://sparkplug.eclipse.org/specification/

[183] **Fraunhofer IIS** (o. D.): mioty – Drahtlose LPWAN Technologie. Fraunhofer IIS [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://mioty.de

[184] **mioty alliance e. V.** (2024): mioty alliance[Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://mioty-alliance.com/

[185] **Pepperl+Fuchs** (2024): IO-Link: Die intelligente Kommunikationstechnologie [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.pepperl-fuchs.com/germany/de/io-link.htm

[186] **Wulf**, Steffen (2022): Ist die Automatisierungspyramide aus der Zeit gefallen? Kommentar. Vogel Communications Group [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.industry-of-things.de/automatisierungspyramide-a-caaf07b9ae98b3d5d0e65b5dc79deffb/

[187] **Schade, Christian** (o. A.): Train Communication Network [Online], [Zugriff am: 25.01.2024]. Verfügbar unter: https://www.hardware-aktuell.com/lexikon/Train_Communication_Network

[188] **Bettenhausen**, Kurt D.; Kowalewski, Stefan (2013): Cyber-Physical Systems. Chancen und Nutzen aus Sicht der Automation. Verein Deutscher Ingenieure e.V., VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA). Düsseldorf (Thesen und Handlungsfelder) [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.vdi.de/ueber-uns/presse/publikationen/details/cyber-physical-systems-chancen-und-nutzen-aus-sicht-der-automation

[189] **Kunbus GmbH** (2022): Das Train Communication Network [Online], [Zugriff am: 16.08.2022]. Verfügbar unter: https://www.kunbus.de/train-communication-network

[190] **Kirrmann**, H. (1999): Train Communication Network IEC 61375 – 4 Wire Train Bus [Online], [Zugriff am 16.08.2022]. Verfügbar unter: https://web.archive.org/web/20110616204215/http://lamspeople.epfl.ch/kirrmann/Pubs/TCN/IEC61375-4-WTB.ppt

[191] **Speedgoat GmbH** (o. A.): MVB/WTB [Online], [Zugriff am 16.08.2022]. Ver-fügbar unter: https://www.speedgoat.com/products-services/i-o-connectivity/protocols/mvb-wtb

[192] **Hardware Aktuell** (o. A.): Feldbus Train Communication Network [Online], [Zu-griff am: 16.08.2022]. Verfügbar unter: https://www.hardware-aktuell.com/lexikon/Train_Communication_Network

[193] **UIC** (2009): Anlage A – Liste der zu übertragenden Informationen – Spezifikation (Version 002.03, gültig ab 01.03.2009) [Online], [Zugriff am: 28.10.2022]. Verfügbar unter: https://uic.org/IMG/pdf/d556aa_06032009.pdf

[194] **Goikoetxea**, J. (2020): The Connected Trams Demonstrator – Showcase of the next generation of the Train Control Monitoring System [Online], [Zugriff am: 20.07.2022]. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=eb76b8b7-617a-4300-a700-91c498152894

[195] **Lütze Transportation GmbH** (o.A.): Skalierbare Netzwerk-Intelligenz [Online], [Zugriff am 16.08.2022]. Verfügbar unter: https://www.luetze-transportation.com/de-de/produkte/leittechnik/netzwerktechnik/skalierbare-netzwerk-intelligenz

[196] **Mariano**, C. (2017): CONTRIBUTING TO SHIFT2RAIL'S NEXT GENERATIONOF HIGH CAPABLE AND SAFE TCMS AND BRAKES. [Online], [Zugriff am: 19.07.2022]. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=3dc35427-3ebc-4a75-8f83-11916991fdbe

[197] **Goikoetxea,** J. (2018): Shift2Rail CONNECTA: The Next Generation of the Train Control and Monitoring System. In: Proc. of 7th Transport Research Arena, April 16-19, 2018, Vienna, Austria

[198] **Bahnsignalisierung.eu** (2015): Was ist ein Zugsteuerungs- und Überwachungssystem (TCMS)? [Online], [Zugriff am: 17.08.2022]. Verfügbar unter: https://www.railwaysignalling.eu/train-control-and-monitoring-systems-tcms

[199] **Minde**, F. (2007): Grundlagen der Eisenbahnbremstechnik, S. 9 ff. [Online], [Zugriff am: 28.10.2022]. Verfügbar unter: https://docplayer.org/68681334-Grundlagen-der-eisenbahn-bremstechnik.html

[200] **GEZ Rail Solutions GmbH** (2022): Dezentrale Steuerung [Online], [Zugriff am: 05.10.2022]. Verfügbar unter: https://www.gez-rs.com/wp-content/uploads/Dezentrale-Steuerung_DE.pdf

[201] **GEZ Rail Solutions GmbH** (2022): Dezentrale Steuerung [Online], [Zugriff am: 05.10.2022]. Verfügbar unter: https://www.gez-rs.com/wp-content/uploads/Zentrale-Steuerung_DE.pdf

[202] **GEZ Rail Solutions GmbH** (2022): Dezentrale Steuerung [Online], [Zugriff am: 05.10.2022]. Verfügbar unter: https://www.gez-rs.com/wp-content/uploads/Dezentral-mit-Master_DE.pdf

[203] **GEZ Rail Solutions GmbH** (2022): Dezentrale Steuerung [Online], [Zugriff am: 05.10.2022]. Verfügbar unter: https://www.gez-rs.com/wp-content/uploads/Zentrales-Master_Slave_DE.pdf

[204] **Siemens** (2022): SIDOOR – Automatische Türsteuerungssysteme für Bahnanwendungen [Online], [Zugriff am: 06.10.2022]. Verfügbar unter: https://new.siemens.com/de/de/produkte/automatisierung/produkte-fuer-spezifische-anforderungen/sidoor-automatic-door-controls/sidoor-for-railway-applications.html

[205] **Siemens** (2022): SIDOOR - Automatische Türsteuerungssysteme [Online], [Zugriff am: 06.10.2022]. Verfügbar unter: https://new.siemens.com/de/de/produkte/automatisierung/produkte-fuer-spezifische-anforderungen/sidoor-automatic-door-controls.html

[206] **BBC Bircher** (2022): Kommunikationsserver für U-Bahn Türsysteme [Online], [Zugriff am: 06.10.2022]. Verfügbar unter: https://automation.bircher.com/fileadmin/user_upload/bbcgroup.biz/downloads/pcontrol/used/Automation_Report_Gilgen.pdf

[207] **Griessbach GmbH** (2016): Wir verbinden Mensch & Maschine, Innentürsteuerung. [Online], [Zugriff am: 06.10.2022]. Verfügbar unter: https://www.griessbach-luckenwalde.de/wp-content/uploads/2016/11/Datenblatt-T%C3%BCrsteuerungssysteme-08_2016_komplette-Brosch%C3%BCre_14_final.pdf

[208] **UIC** (2002): UIC Code 560 - Doors, footboards, windows, steps, handles and handrails of coaches and luggage vans, 12th edition, Punkt 2.1.1

[209] **UIC** (2002): UIC Code 560 - Doors, footboards, windows, steps, handles and handrails of coaches and luggage vans, 12th edition, Punkt 3.1.1 und 3.1.2

[210] **Die Ingenieurwerkstatt GmbH** (2009): Risikoanalyse zur Einstiegssituation bei Schienenfahrzeugen in Abhängigkeit des Abfertigungsverfahrens [Online], [Zugriff am: 14.09.2022]. Verfügbar unter: https://www.eba.bund.de/SharedDocs/Downloads/DE/Fahrzeuge/Fahrzeugtechnik/Funktionale_Sicherheit/Anwendungsbeispiel/31_SIRF_Risikoanalyse.pdf?__blob=publicationFile&v=3

[211] **Bundesarbeitsgemeinschaft der Aufgabenträger des SPNV e.V** (2016): Empfehlungen für Anforderungen an Fahrzeuge im Vergabeverfahren für Mitglieder der BAG-SPNV [Online]. [Zugriff am: 27.20.2022], Verfügbar unter: https://www.schienennahverkehr.de/wp-content/uploads/2021/07/2016-02-23-Fahrzeuganforderungen_final_gesamt.pdf

[212] **UIC** (2002): UIC Code 560 – Doors, footboards, windows, steps, handles and handrails of coaches and luggage vans, 12th edition, Punkt 1.2.3.2.1 und Punkt 1.1.6 im Allgemeinen

[213] **DIN** (2017): DIN EN 12453 - Nutzungssicherheit kraftbetätigter Tore – Anforderungen und Prüfverfahren sowie DIN (2013, ergänzt 2015): DIN EN 16005 – Kraftbetätigte Türen – Nutzungssicherheit – Anforderungen und Prüfverfahren

[214] **DB Netz AG** (2014): European Train Control System (ETCS) bei der DB Netz AG [Online], [Zugriff am: 14.09.2022]. Verfügbar unter: https://www.anbindung-fbq.de/files/downloads/Infobroschueren/Anhang_Themendienst_ETCS-data.pdf

[215] **DB Netz AG** (2022): Sicherheit und ETCS, [Zugriff am: 14.09.2022]. Verfügbar unter: https://www.anbindung-fbq.de/de/planung-genehmigung/sicherheit-und-etcs.html

[216] **Steingröver**, A. (2018), Automatisiertes Fahren: Was können wir bei der Vollbahn von CBTS lernen? In: Siemens Ingenuity for Life.

[217] **railsystem.net** (2022): Communications-Based Train Control (CBTC) [Online], [Zugriff am: 15.09.2022]. Verfügbar unter: https://railsystem.net/communications-based-train-control-cbtc/

[218] **Eisenbahn-Bundesamt** (2022): Thema: Bahnbetrieb ERTMS [Online], [Zugriff am: 14.09.2022]. Verfügbar unter: https://www.eba.bund.de/DE/Themen/ERTMS/ertms_node.html

[219] **Jabri**, S. (2010): European railway traffic management system validation using UML/Petri nets modelling strategy [Online], [Zugriff am: 20.07.2022]. Verfügbar unter: https://etrr.springeropen.com/articles/10.1007/s12544-010-0030-5

[220] **Malfait**, W. (2022): TSI CCS ETCS – Modifications and its resulting impact [Online], [Zugriff am: 28.09.2022]. Verfügbar unter: https://www.era.europa.eu/sites/default/files/events-news/docs/ertms2022_workshop6_supportingslides.pdf

[221] **Jabri, Sana**; El Koursi, El Miloudi; Bourdeaud'huy, Thomas; Lemaire, Etienne (2010): European railway traffic management system validation using UML/Petri nets modelling strategy [Paper], [Zugriff am: 14.09.2023]. Verfügbar unter: https://etrr.springeropen.com/articles/10.1007/s12544-010-0030-5

[222] Beginn Quellenabschnitt 2 [Q50] Q50 **Ludicke**, Daniel; Lehner, Andreas (2019): Train Communication Networks and Prospects. In: IEEE Commun. Mag. 57 (9), S. 39 – 43. DOI: 10.1109/MCOM.001.1800957

[223] **Buczynski**, Josef (2017): Industrieplattform Telematik und Sensorik im Schienengüterverkehr. ITSS practice group [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://docplayer.org/45492433-Itss-practice-group-industrieplattform-telematik-und-sensorik-im-schienengueterverkehr.html

[224] **DAC4EU** (2022): Pilot project for the demonstration, testing and approval of the digital automatic coupler for rail freight traffic. Interim Report: Completion of Phase I. Frankfurt/Main (File reference: E12 5185.4/9) [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://bmdv.bund.de/SharedDocs/EN/Documents/E/dac-demonstrator-interim-report-completion-of-phase-1.pdf?__blob=publicationFile

[225] **Deutsche Bahn AG** (2022): FAKTENBLATT SCHIENENGÜTERVERKEHR Digitale Automatische Kupplung (DAK) [Online], [Zugriff am: 28.09.2022]. Verfügbar unter: https://www.deutschebahn.com/resource/blob/7175570/165473294776a2cb088df858b52d3fd1/220119_DAK_Faktenblatt-data.pdf

[226] **DB Engineering & Consulting GmbH** (2020): DIANA. Zustandsüberwachung und Diagnose. DB Engineering & Consulting GmbH. Berlin [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://infraview.net/de/unsere-loesungen/

[227] **KONUX** (2024): Wir transformieren den Schienenverkehr für eine nachhaltige Zukunft[Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.konux.com/de/

[228] **Siemens Mobility** (2024): Railigent X [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.mobility.siemens.com/global/de/portfolio/digitale-loesungen-software/digitale-services/railigent-x.html

[229] **DB Netz AG** (2018): European Train Control System (ETCS) [Broschüre, Online], [Zugriff am 16.08.2023]. Verfügbar unter: https://fahrweg.dbnetze.com/resource/blob/9728786/461729e9fed0107df85271ba1bbddf8b/etcsbroschuere_2018-data.pdf

[230] **U.S. DEPARTMENT OF TRANSPORTATION** (2023): Positive Train Control (PTC) [Online], [Zugriff am 16.11.2023]. Verfügbar unter: https://railroads.dot.gov/research-development/program-areas/train-control/ptc/positive-train-control-ptc

[231] **Hiura, Noboru** (2013): Overview of the ATACS Radio Train Control System [Special edition paper], [Zugriff am 16.11.2023]. Verfügbar unter: https://www.jreast.co.jp/e/development/tech/pdf_25/Tec-25-15-18eng.pdf

[232] **Technische Spezifikation** für die Interoperabilität (TSI) zum Teilsystem „Zug-steuerung, Zugsicherung und Signalgebung“ des konventionellen transeuro-päischen Bahnsystems (2006): Anhang, [Anhang], [Zugriff am 16.11.2023]. Verfügbar unter http://ec.europa.eu/transport/rail/interoperability/doc/ccs-tsi-de-annex.pdf

[233] **Научно-исследовательский** и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте (o. A.): Комплексное локомотивное устройство безопасности КЛУБ-У [Online], [Zugriff am 29.01.2024]. Verfügbar unter: https://niias.ru/products-and-services/products/bortovye-kompleksy/kompleksnoe-lokomotivnoe-ustroystvo-bezopasnosti-unifitsirovannoe/

[234] **Allianz pro Schiene** (o. A.): ETCS (European Train Control System) [Online], [Zugriff am: 16.08.2022]. Verfügbar unter: https://www.allianz-pro-schiene.de/glossar/etcs-european-train-control-system/

[235] **Ruge, Michael** (2014): Die Elektrolokomotiven der Baureihe 181 der DB, Seite 33-36 [Online], [Zugriff am: 26.01.2023]. Verfügbar unter: https://web.archive.org/web/20151229172500/http://www.181er.de/br181_entwicklung.pdf

[236] **Weißer, Dirk**; Franke, Torsten; Bandelin, Holger; Radermacher, Berthold; Wehrmann, Andreas; Meier-Lu, Walter (2014): Internetprotokoll basiertes integriertes Bordinformationssystem IBIS-IP [Online], [Zugriff am: 26.01.2023]. Verfügbar unter: https://www.vdv.de/vdv-301-1-ibis-ip-teil-1-systemarchitektur.pdfx

[237] **Paraskevopoulos, D.** (2022): 5 things to know about IoT protocols [Online], [Zugriff am 16.11.2023]. Verfügbar unter: https://iot-analytics.com/iot-protocols/

[238] Beginn AP 4.2 [Q59] Q59 **TCNOpen Initiative** (o. A.): TCN Open [Online], [Zugriff am: 31.01.2024]. Verfügbar unter https://www.tcnopen.eu/Page.aspx?CAT=STANDARD&IdPage=2996a297-6558-499d-852f-782cd675dd07

[239] **KUNBUS** (o. D.): Das Train Communication Network [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.kunbus.com/de/train-communication-network

[240] **Schmitz**, Barbara; Seger, Thomas (2009): Informations-und Steuerungstechnik auf Schienenfahrzeugen. In: Der Eisenbahningenieur 60 (2), S. 42 – 44.

[241] **CONNECTA** (2017): Contributing to Shift2Rail's next generation of high capable and safe TCMS and brakes: D3.2 – Drive-by-Data Technology Evaluation Report. CTA-T3.2-D-BTD-003-07

[242] **Jakovljevic**, Mirko; Geven, Arjan; Simanic-John, Natasa; Saatci, Derya Mete (2018): Next-Gen-TrainControl/Management (TCMS) Architectures:“Drive-By-Data”SystemIntegrationApproach. In: ERTS2018.

[243] **VPI European Rail Service** (o. A.): Industrieplattform Telematik und Sensorik im Schienengüterverkehr (ITSS) [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://vpiham-burg.de/vers/die-vers/itss

[244] **OPC Router** (o. A.): Was ist MQTT? Protokoll für das Internet der Dinge (IoT). inray Industriesoftware GmbH [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.opc-router.de/was-ist-mqtt/

[245] **Eclipse Sparkplug Working Group** (o. A.): MQTT + Sparkplug = 'Plug & Play' IIoT. The Eclipse Foundation [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://sparkplug.eclipse.org/

[246] **AnyViz** (o. A.): Das MQTT Protokoll zur Kommunikation in die Cloud. Mirasoft GmbH & Co. KG. [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.anyviz.de/blog/das-mqtt-protokoll-zur-kommunikation-in-die-cloud/

[247] **Welotec** (o. A.): Was ist MQTT? [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.welotec.com/de/was-ist-mqtt/

[248] **OPC Router** (o. A.): Was ist OPC UA? Die wichtigsten Begriffe im Überblick [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.opc-router.de/was-ist-opc-ua/

[249] **IPC2U GmbH** (o. A.): Die Standards OPC DA und OPC UA ganz einfach erklärt [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://ipc2u.de/artikel/wissenswertes/die-standards-opc-da-und-opc-ua-ganz-einfach-erkl-rt/,

[250] **Paessler AG** (o. A.): Monitoring Ihrer industriellen Umgebung mit OPC UA [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: unter https://www.paessler.com/de/opc-ua-monitoring

[251] **52north** (o. A.): SensorML [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://52north.github.io/sensor-web-tutorial/03_sensorml.html

[252] **Open Geospatial Consortium** (o. A.): Sensor Model Language (SensorML [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.ogc.org/standard/sensorml/

[253] **OGC** (o. A.): Semantic Sensor Network Ontology [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.w3.org/TR/vocab-ssn/

[254] **IPH gGmbH** (o. A.): Automatisierungspyramide: Aufbau und Bedeutung [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.iph-hannover.de/de/dienstleistungen/automatisierungstechnik/automatisierungspyramide/

[255] **TechTarget** (o. A.): Top advantages and disadvantages of IoT in business [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.techtarget.com/iotagenda/tip/Top-advantages-and-disadvantages-of-IoT-in-business

[256] **OnLogic** (o. A.): IT vs. OT: Wie sich Informationstechnologie und operative Technologie unterscheiden [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.onlogic.com/company/io-hub/de/it-vs-ot-wie-sich-informationstechnologie-und-operative-technologie-unterscheiden/

[257] **Yokogawa Europe** (o. A.): IT/OT Convergence: Bringing Two Worlds Together [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.yokogawa.com/eu/library/resources/white-papers/itot-convergence-bringing-two-worlds-together/

[258] **BBC Bircher Automation** (o. A.): Kommunikationsserver für U-Bahn Türsysteme [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://automation.bircher.com/de/automation-swiss-made-wir-entwickeln-massgefertigte-loesungen-fuer-sie/kommunikationsserver-2/

[259] **Shift2Rail** (o. A.): Presentations of CONNECTA-2's & Safe4Rail-2's Final event [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=a1ea7b2f-5a06-44dc-b06e-354f9d15d532

[260] **DIN** (o. D.): Leitfaden für standardessentielle Patente [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.din.de/de/din-und-seine-partner/presse/mitteilungen/leitfaden-fuer-standardessentielle-patente-334174

[261] **Rößler**, Matthias (2020): Standardessentielle Patente (SEP) [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.karo-ip.de/de/blog/sep/, zuletzt aktualisiert am 20.11.2020.

[262] **Free Software Foundation Europe** (o. A.): Offene Standards [Online], [Zugriff am: 26.01.2023]. Verfügbar unter: https://fsfe.org/freesoftware/standards/standards.de.html

[263] **TCNOpen** (o. A.): TCNOpen [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.tcnopen.eu/Page.aspx?CAT=STANDARD&IdPage=242e8d0b-8cb8-4ded-87ad-801b95d29470

[264] **NewTec GmbH** (o. A.): And the Winner is: FDF und TRDP – [Studie zu Netzwerkprotokollen in Bahnfahrzeugen], [Zugriff am: 27.01.2023]. Verfügbar unter: https://www.newtec.de/fileadmin/media/presse_news/NewTecStudieTRDP_Auszug_safeNTsecure.pdf

[265] **NewTec GmbH** (o. A.): TRDP – Entwicklung, Services & Tools [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.newtec.de/loesungen/railway/

[266] **NEIF GmbH** (o. A.): Train Real Time Data Protocol. NEIF GmbH [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://dewiki.de/Lexikon/Train_Real_Time_Data_Protocol

[267] **LonMark** (2021): Standards [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.lonmark.org/technology/lon-technology/standards/

[268] **LonMark** (2021): Membership [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.lonmark.org/membership/

[269] **NewTec GmbH** (2022): And the Winner is: TRDP! [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.newtec.de/blog/and-the-winner-is-trdp/, zuletzt aktualisiert am 03.01.2022.

[270] **TIS** (2019): TIS – Vom Innovativen Güterwagen zum Intelligenten Güterzug [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://tis.ag/

[271] **TIS** (2019): Innovativer Güterwagen [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://tis.ag/2-innovativer-gueterwagen/

[272] **MQTT** (2022): MQTT Specifications [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://mqtt.org/mqtt-specification/

[273] **OASIS** (2019): MQTT Version 5.0. [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html, zuletzt aktualisiert am 07.03.2019

[274] **OASIS** (2020): OASIS Message Queuing Telemetry Transport (MQTT) TC [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://www.oasis-open.org/committees/mqtt/ipr.php

[275] **OPC Foundation** (2013): Bylaws of OPC Foundation [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://opcfoundation.org/wp-content/uploads/pdfs/opc-foundation-bylaws.pdf, zuletzt aktualisiert am 08.08.2013.

[276] **OPC Foundation** (o. A.): Mission Statement [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://opcfoundation.org/about/opc-foundation/mission-statement/

[277] **OPC Foundation** (o. A.): OPC Foundation License Agreement [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://opcfoundation.org/license-agreement/

[278] **OPC Foundation** (2020): INTELLECTUAL PROPERTY RIGHTS POLICY [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://opcfoundation.org/wp-content/uploads/2020/05/OPCF-IPR-Policy-Ver-2.2-25MAY2020.pdf

[279] **Botts Innovative Research Inc** (2013): Standards [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: http://www.sensorml.com/standards.html

[280] **Botts Innovative Research Inc** (2013): Welcome [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: http://www.sensorml.com/

[281] **Open Geospatial Consortium** (2021): Project Licenses Welcome [Online], [Zugriff am: 31.01.2024]. Verfügbar unter: https://cite.opengeospatial.org/teamengine/about/sensorml20/2.0/site/license.html

[282] **W3C** (2017): Semantic Sensor Network Ontology [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.w3.org/TR/vocab-ssn/

[283] **W3C** (2020): W3C Patent Policy [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.w3.org/Consortium/Patent-Policy-20200915/

[284] **International Electrotechnical Commission** (o. A.): Webseite [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: www.iec.ch

[285] **PROFIBUS Nutzerorganisation e.V.** (2017): IO-Link setzt auf Qualität Policy [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://io-link.com/de/Global/newsmeldung.php?showId=459

[286] **PROFIBUS Nutzerorganisation e.V.** (o. A.): Community Regeln [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://io-link.com/de/WirUeberUns/Konsortialregeln.php

[287] **PROFIBUS Nutzerorganisation e.V.** (o. A.): Standardisierung [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://io-link.com/de/Technologie/standardisierung.php?thisID=61

[288] **PROFIBUS Nutzerorganisation e.V.** (2022): IO-Link License Model [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://io-link.com/share/Downloads/Quality/IOL-License-model_10302_V120_Mar22.pdf

[289] **PROFIBUS Nutzerorganisation e.V.** (o. A.): IO-Link [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.profibus.com/technology/io-link

[290] **ODVA** (o. A.): Common Industrial Protocol (CIP™) [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.odva.org/technology-standards/key-technologies/common-industrial-protocol-cip/

[291] **ODVA** (o. A.): Document Library [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.odva.org/technology-standards/document-library/

[292] **W3C** (2016): Extensible Markup Language (XML) [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.w3.org/XML/

[293] **W3C** (2006): Extensible Markup Language (XML) 1.1 (Second Edition) [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.w3.org/TR/2006/REC-xml11-20060816/

[294] **JSON.org** (2002): The JSON License [Online], [Zugriff am: 26.01.2024]. Verfügbar unter: https://www.json.org/license.html]

[295] **JSON.org** (o. A.): Introducing JSON [Online], [Zugriff am: 24.01.2024]. Verfügbar unter: https://www.json.org/json-de.html

[296] **Ecma International** (2017): ECMA-404 The JSON data interchange syntax 2nd edition [Online], [Zugriff am: 27.01.2024]. Verfügbar unter: https://www.ecma-international.org/publications-and-standards/standards/ecma-404/

[297] **Object Management Group®, Inc** (o. A.): Webseite [Online], [Zugriff am: 27.01.2024]. Verfügbar unter: https://www.uml.org/

[298] **Object Management Group®**, OMG® (2017): ABOUT THE UNIFIED MODEL-ING LANGUAGE SPECIFICATION VERSION 2.5.1 [Online], [Zugriff am: 27.01.2024]. Verfügbar unter: https://www.omg.org/spec/UML/

[299] **Object Management Group®**, OMG® (o. A.): Webseite [Online], [Zugriff am: 27.01.2024]. Verfügbar unter: https://www.omgsysml.org/

[300] **Object Management Group®**, OMG® (2024): ABOUT THE OMG SYSTEM MODELING LANGUAGE SPECIFICATION VERSION 2.0 BETA 2 [Online], [Zugriff am: 27.04.2024]. Verfügbar unter: https://www.omg.org/spec/SysML

[301] **USB Implementers Forum, Inc.** (2024): Universal Serial Bus 3.2 Link Layer Test Specification [Online], [Zugriff am: 13.03.2024]. Verfügbar unter: https://www.usb.org/sites/default/files/USB%203%202%20Link%20Layer%20Test%20Specification%202024%2003%2003.pdf

[302] **Eddy, Wesley** (2022): Transmission Control Protocol (TCP) [Online], [Zugriff am: 02.02.2024]. Verfügbar unter: https://datatracker.ietf.org/doc/html/rfc9293

[303] **Deering, Stephen**; Hinden, Robert (2017): Internet Protocol, Version 6 (IPv6) Specification [Online], [Zugriff am: 02.02.2024]. Verfügbar unter: https://datatracker.ietf.org/doc/html/rfc8200

[304] **Postel, J.** (1980): User Datagramm Protocol [Online], [Zugriff am: 02.02.2024]. Verfügbar unter: https://datatracker.ietf.org/doc/html/rfc768

[305] **König, Reiner**; Hecht, Markus; Eberlein, Christina (2012): Weissbuch Innovater Eisenbahngüterwagen 2030, ISBN 978-3-00-039376-1, Dresden: addprint AG

[306] **ITSS practice group** (2021): ITSS Standard Specification, [Online], [Zugriff am: 22.11.2023]. Verfügbar unter: https://tis.ag/download/itss-standard-specification-interface-1-v1-3-2021-11-neu/

[307] **Scarfone**, K. A.; Jansen, W.; Tracy, M. (2008): Guide to general server security, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-123, 2008. doi: 10.6028/NIST.SP.800-123.

[308] **Elorza**, N.; u. a. (2018): D3.5 – Drive-by-Data Architecture Specification, Ort: CAF, SIEMENS, BTG, ASTS, SNCF-M. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=700c29b5-0574-4130-9060-f6f25c94d11e

[309] **Mayeux**, V. (2018): Drive-by-Data & Integrated Modular Platform – Joint Final Conference CONNECTA & Safe4RAIL, Ort: Paris. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=e82cf2e2-7b00-4c12-8592-66d5419d8bc5

[310] **Lopez**, I.; Arriola, A. (2021): Introduction to the Next Generation Train Control and Monitoring System (NG-TCMS) – Final Conference Shift2Rail TD1.2. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=a1ea7b2f-5a06-44dc-b06e-354f9d15d532

[311] **Hagenlocher**, S. (2019): Weißbuch Intelligenter Güterzug. Verfügbar unter: https://tis.ag/download/tis_weissbuch_intelligenter_gueterzug/?wpdmdl=652

[312] **ITSS practice group** (2021): ITSS Standard Specification: ITSS Interface IF1 (Telematics Application – Customer System), Version 1.2 final. Verfügbar unter: https://tis.ag/download/itss-standard-specification-interface-1-v1-3-2021-11-neu/?wpdmdl=1258

[313] **ITSS practice group** (2021): ITSS Interface 2 Specification - Profiles, V1.1 rev01

[314] **Iffländer**, L.; Buder, T.; Buchetmann, B. (2023): Cyberangriffe auf das Bahnsystem – Was bisher geschah. Rückblick auf bisher entdeckte und dokumentierte Cyberangriffe gegen Teilkomponenten des Bahnsystems, in: Der Eisbenbahningenieur (08/2023), S. 17 – 21

[315] **Abuteir**, M.; Waschulzik, T. (2021): Introduction of Test Case 2 ‚TSN Network & OPC UA' – Final Conference Shift2Rail TD1.2. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=a1ea7b2f-5a06-44dc-b06e-354f9d15d532

[316] **Waschulzik**, T.; u. a. (2019): D1.2 – Definition of new FDF requirements and new Application Profiles, Revision 9. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=03f0f7d8-8155-4fe3-a34f-0b4869451ffa

[317] **Waschulzik**, T.; u. a. (2018): D4.3 – Application profile definition guideline and example, Revision 05. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=25b5a153-d36c-4555-8b7a-86d24444a3a0

[318] **Gutierrez**, D.; Biermann, F.; Hans, G.; Youssef, M.; Sept, J.; Lapporte, P. (2021): D4.2 – Intermediate Report on Cybersecurity measure for NG- TCMS (under review), Revision 08. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=24507801-4184-4e04-9a3e-91d687b8bcbb

[319] **Vivegnis**, P.; u. a. (2017): D4.1 – Requirement specification for each sub task, Revision 9. Verfügbar unter: https://projects.shift2rail.org/download.aspx?id=f83f6c3f-6cdf-421c-b341-0e23f07c4a80

[320] **Lévy-Bencheton**, C.; Darra, E. (2015): Cybersecurity and Resilience of Intelligent Public Transport – Good practices and recommendations, ENISA

[321] **Liveri**, D.; Theocharidou, M.; Naydenov, R. (2020): Railway Cybersecurity – Security measures in the Railway Transport Sector, ENISA

[322] Nord, M.; Möller, D.; Krause, P.; Lenski, N.; Czerkewski, P. im Auftrag des Deutschen Zentrums für Schienenverkehrsforschung beim Eisenbahn-Bundesamt (2023): Studie „Security und geplanter Technologieeinsatz". Untersuchung und Bewertung des ÖPNV- und Eisenbahnsektors anhand von Reifegrad- und SWOT-Analysen

[323] **Theocharidou**, M.; Stanic Z.; u.a. (2021): Railway Cybersecurity – Good practices in cyber risk management, ENISA

[324] **ENISA** (2019): ENISA Good practices for security of smart cars, ENISA, DOI 10.2824/17802

[325] **Shen**, J., et al. (2022): SoK: On the Semantic AI Security in Autonomous Driving, arXiv, 10. März 2022. Zugegriffen: 29. März 2023. [Online]. Verfügbar unter: http://arxiv.org/abs/2203.05314

[326] **Zhao**, Y.; Zhu, H.; Liang, R.; Shen, Q.; Zhang, S.; Chen, K. (2019): Seeing isn't Believing: Towards More Robust Adversarial Attack Against Real World Object Detectors, in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, in CCS '19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, S. 1989 – 2004. doi: 10.1145/3319535.3354259.

[327] **Cao**, Y., et al. (2019): Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving, in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, in CCS '19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, S. 2267 – 2281. doi: 10.1145/3319535.3339815.

[328] **Sun**, J.; Cao, Y.; Chen, Q. A.; Mao, Z. M. (2023): Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures, gehalten auf der 29th USENIX Security Symposium (USENIX Security 20), 2020, S. 877 – 894 [Online], [Zugriff am: 19.06.2023]. Verfügbar unter: https://www.usenix.org/conference/usenixsecurity20/presentation/sun

[329] **Shin**, H.; Kim, D.; Kwon, Y.; Kim, Y. (2017): Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications, in Cryptographic Hardware and Embedded Systems – CHES 2017, W. Fischer und N. Homma, Hrsg, in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017, S. 445 – 467. doi: 10.1007/978-3-319-66787-4_22.

[330] **Shen**, J.; Won, J. Y.; Chen, Z.; Chen, Q. A. (2020): Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing, in 29th USENIX security symposium (USENIX security 20), USENIX Association, Aug. 2020, S. 931 – 948 [Online]. Verfügbar unter: https://www.usenix.org/conference/usenixsecurity20/presentation/shen

[331] **Cao**, Y., et al. (2021): Invisible for both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks, in 2021 IEEE Symposium on Security and Privacy (SP), Mai 2021, S. 176 – 194. doi: 10.1109/SP40001.2021.00076.

[332] **Wan**, Z., et al. (2022): Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks, in Proceedings 2022 Network and Distributed System Security Symposium, San Diego, CA, USA: Internet Society, 2022. doi: 10.14722/ndss.2022.24177.

[333] **O. A.** (2022): Sicherheitsanalyse Open Platform Communications Unified Architecture (OPC UA), Bundesamt für Sicherheit in der Informationstechnik [Online], [Zugriff am: 29.06.2023]. Verfügbar unter: https://www.bsi.bund.de/dok/7819284

[334] **Firdous**, S. N.; Baig, Z.; Valli, C.; Ibrahim, A. (2017): Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol, in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), S. 748 – 755. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115

[335] **Atilgan**, E.; Ozcelik, I.; Yolacan, E. N. (2021): MQTT Security at a Glance, in 2021 International Conference on Information Security and Cryptology (ISCTURKEY), S. 138 – 142. doi: 10.1109/ISCTURKEY53027.2021.9654337

[336] **Hintaw**, A. J.; Manickam, S.; Aboalmaaly, M. F.; Karuppayah, S. (2021): MQTT Vulnerabilities, Attack Vectors and Solutions in the Internet of Things (IoT), IETE J. Res., S. 1 – 30, doi: 10.1080/03772063.2021.1912651

[337] **Sadio**, O.; Ngom, I.; Lishou, C. (2019): Lightweight Security Scheme for MQTT/MQTT-SN Protocol, in: 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), S. 119 – 123. doi: 10.1109/IOTSMS48152.2019.8939177

[338] **Meneghello**, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. (2019): IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices, IEEE Internet Things J., Bd. 6, Nr. 5, S. 8182 – 8201, doi: 10.1109/JIOT.2019.2935189

[339] **Neshenko**, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. (2019): Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations, IEEE Commun. Surv. Tutor., Bd. 21, Nr. 3, S. 2702 – 2733, 2019, doi: 10.1109/COMST.2019.2910750

[340] **Tournier**, J.; Lesueur, F.; Le Mouël, F.; Guyon, L; Ben-Hassine, H. (2020): A survey of IoT protocols and their security issues through the lens of a generic IoT stack, Internet Things, Bd. 16, S. 100264, doi: 10.1016/j.iot.2020.100264

[341] **OWASP** (o. A.): OWASP CycloneDX [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://owasp.org/www-project-cyclonedx/

[342] **Prado**, J. (o. A.): Lightweight M2M (LWM2M), OMA SpecWorks [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/

[343] **IETF Datatracker** (o. A.): Software Updates for Internet of Things (suit) [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://datatracker.ietf.org/wg/suit/about/

[344] **O. A.** (2022): The Update Framework (TUF) [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://theupdateframework.io/

[345] **O. A.** (o. A.): Automotive Grade Linux [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://docs.automotivelinux.org/en/needlefish/2_Architecture_Guides/2_Security_Blueprint/8_Update_OTA/

[346] **Airbiquity** (2017): Airbiquity Unveils New OTAmatic™ Release Further Strengthening Over-The-Air (OTA) Software And Data Management Offering For Automotive [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.airbiquity.com/news/press-releases/airbiquity-unveils-new-otamatictm-release-further-strengthening-over-air-ota-software-and-data-management-offering-automotive

[347] **Fuchsia** (2021): Software Update System [Online], 30.12.2021, [Zugriff am: 12.07.2023]. Verfügbar unter: https://fuchsia.dev/fuchsia-src/concepts/packages/software_update_system

[348] **HERE** (2019): HERE Technologies joins the Uptane Alliance [Online], 28.05.2019, [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.here.com/about/press-releases/en/2019-28-05

[349] **Debian-Wiki** (2018): SecureApt – TufDerivedImprovements [Online], 10.05.2018, [Zugriff am: 12.07.2023]. Verfügbar unter: https://wiki.debian.org/SecureApt/TufDerivedImprovements

[350] **The Update Frameworks authors** (2022): TUF – Security, The Update Framework [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://theupdateframework.io/security/

[351] **Cappos**, J.; Kuppusamy, T. K.; Lock, J.; Moore, M.; Pühringer, L. (2023): The Update Framework Specification, The Update Framework [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://theupdateframework.github.io/specification/latest/

[352] **Samuel**, J.; Mathewson, N.; Cappos, J.; Dingledine, R. (2010): Survivable key compromise in software update systems, in Proceedings of the 17th ACM conference on Computer and communications security, Chicago Illinois USA: ACM, Okt. 2010, S. 61 – 72. doi: 10.1145/1866307.1866315.

[353] **Karthik**, T.; et al (2016): Uptane: Securing Software Updates for Automobiles

[354] **Kuppusamy**, T. K.; DeLong, L. A.; Cappos, J. (2018): Uptane: Security and Customizability of Software Updates for Vehicles, IEEE Veh. Technol. Mag., Bd. 13, Nr. 1, S. 66 – 73, März 2018, doi: 10.1109/MVT.2017.2778751.

[355] **Galibus**, T. (2020): Securing Software Updates for Trains, in Critical Information Infrastructures Security, S. Nadjm-Tehrani, Hrsg. in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, S. 137 – 148. doi: 10.1007/978-3-030-37670-3_11.

[356] **Asokan**, N.; Nyman, T.; Rattanavipanon, N.; Sadeghi, A.-R.; Tsudik, G. (2018): ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., Bd. 37, Nr. 11, S. 2290 – 2300, doi: 10.1109/TCAD.2018.2858422.

[357] **European Union Agency for Cybersecurity** (2021): ENISA threat landscape for supply chain attacks. LU: Publications Office, [Online], [Zugriff am: 21.06.2023]. Verfügbar unter: https://data.europa.eu/doi/10.2824/168593

[358] **Papaphilippou**, M.; Konstantinos, M; Theocharidou, M. (2023): Good practices for supply chain cybersecurity, European Union Agency for Cybersecurity (ENISA) [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

[359] **O. A.** (o. A.): 2023 Cloud Security Report | Check Point Software [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://pages.checkpoint.com/2023-cloud-security-report.html

[360] **O. A.** (2021): Studie Cloud Security 2021, IDG Business Media GmbH, 2021

[361] **CVE** (2023): CVE [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://cve.mitre.org/

[362] **OWASP Top 10 team** (2021): OWASP Top 10:2021 [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://owasp.org/Top10/

[363] **O. A.** (o. A.): CWE – Common Weakness Enumeration [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://cwe.mitre.org/index.html

[364] **CheatSheets Series Team** (2021): OWASP Cheat Sheet Series [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://cheatsheetseries.owasp.org/

[365] **CWE** (2023): CWE-306: Missing Authentication for Critical Function [Online], 29.06.2023, [Zugriff am: 12.07.2023]. Verfügbar unter: https://cwe.mitre.org/data/definitions/306.html

[366] **Continella**, A.; Polino, M.; Pogliani, M.; Zanero, S. (2018): There's a Hole in that Bucket!: A Large-scale Analysis of Misconfigured S3 Buckets, in Proceedings of the 34th Annual Computer Security Applications Conference, San Juan PR USA: ACM, S. 702 – 711. doi: 10.1145/3274694.3274736.

[367] **Bundesamt für Sicherheit in der Informationstechnik** (o. A.): CERT-Bund-Reports [Online] [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.bsi.bund.de/dok/8730208

[368] **Bundesamt für Sicherheit in der Informationstechnik** (o. A.): Reports zu offenen Server-Diensten [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.bsi.bund.de/dok/8381738

[369] **Rahman**, A.; Shamim, S. I.; Bose, D. B.; Pandita, R. (2023): „Security Misconfigurations in Open Source Kubernetes Manifests: An Empirical Study", ACM Trans. Softw. Eng. Methodol., Bd. 32, Nr. 4, S. 1 – 36, doi: 10.1145/3579639

[370] **Wolf**, M.; Scheibel, M. (2012): A systematic approach to a qualified security risk analysis for vehicular IT systems. Gesellschaft für Informatik e.V. [Online], [Zugriff am: 15.09.2023]. Verfügbar unter: https://dl.gi.de/handle/20.500.12116/17557

[371] **Kour**, R. (2020): Cybersecurity in railway: a framework for improvement of digital asset security. Doktorarbeit. Luleå University of Technology

[372] **Han**, C.; Dongre, R. (2014): Q&A. What Motivates Cyber-Attackers?. Technology Innovation Management Review, 4(10): S. 40 – 42. http://doi.org/10.22215/timreview/838

[373] **Traer**, S.; Bednar, P (2021): Motives Behind DDoS Attacks. In: Metallo, C., Ferrara, M., Lazazzara, A., Za, S. (eds) Digital Transformation and Human Behavior. Lecture Notes in Information Systems and Organisation, vol 37. Springer, Cham. https://doi.org/10.1007/978-3-030-47539-0_10

[374] **Sawall**, A. (2022): Anschlag auf Bahn-Kabel erfolgte mit Insiderwissen [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.golem.de/news/glasfaser-anschlag-auf-bahn-kabel-erfolgte-mit-insiderwissen-2210-168833.html

[375] **Soderi**, S.; Masti, D.; Lun, Y. Z. (2023): Railway Cyber-Security in the Era of Interconnected Systems: A Survey, in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 7, S. 6764 – 6779, July 2023, doi: 10.1109/TITS.2023.3254442

[376] **The Register** (2008): Polish teen derails tram after hacking train network [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.theregister.com/2008/01/11/tram_hack

[377] **Zetter**, K. (2012): Hackers Breached Railway Network, Disrupted Service [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.wired.com/2012/01/railyway-hack/

[378] **Kovacs**, E: (2016): BlackEnergy, KillDisk Infect Ukrainian Mining, Railway Systems [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.securityweek.com/blackenergy-killdisk-infect-ukrainian-mining-railway-systems/

[379] **Cheshire**, T. (2016): Four Cyber Attacks On UK Railways In A Year [Online], 12.07.2016, [Zugriff am: 12.07.2023]. Verfügbar unter: https://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558

[380] **O. A.** (2017): International cyber attacks put ransoms on German rail stations screens [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.thelocal.de/20170513/international-cyber-attacks-put-ransoms-on-german-train-departure-boards

[381] **O. A.** (2017): Swedish transport agencies targeted in cyber attack [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.thelocal.se/20171012/swedish-transport-agencies-targeted-in-cyber-attack

[382] **McCreanor**, N. (2018): Danish rail network DSB hit by cyber attack [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.itgovernance.eu/blog/en/danish-rail-network-dsb-hit-by-cyber-attack

[383] **Reese**, C. (2021): Hackers breach Iran rail network, disrupt service [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.reuters.com/world/middle-east/hackers-breach-iran-rail-network-disrupt-service-2021-07-09/

[384] **Townsend**, K. (2021): Detail Emerge on Iranian Railroad Cyberattack [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.securityweek.com/details-emerge-iranian-railroad-cyberattack/

[385] **Townsend**, K. (2021): Ransomware Attack on UK Rail System – Spray und Pray or Targeted [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.securityweek.com/ransomware-attack-uk-rail-system-spray-and-pray-or-targeted/

[386] **O. A.** (2022): Belarus hackers attack train systems to disrupt Russion troops [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.railway-technology.com/news/belarus-hackers-attack-train-systems/

[387] **Kovacs**, E. (2022): Cyberattack Causes Trains to Stop in Denmark [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.securityweek.com/cyberattack-causes-trains-stop-denmark/

[388] **Briginshaw**, D. (2022): Italian railway IT system suffers major cyber-attack [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://www.railjournal.com/infrastructure/italian-railway-it-system-suffers-major-cyber-attack/

[389] **Khan**, M.S.; Siddiqui, S.; Ferens, K. (2018): A Cognitive and Concurrent Cyber Kill Chain Model. In: Daimi, K. (eds) Computer and Network Security Essentials. Springer, Cham. https://doi.org/10.1007/978-3-319-58424-9_34

[390] **Strom**, B. E.; Battaglia, J. A.; Kemmerer, M. S.; Kupersanin, W.; Miller, D. P.; Wampler, C.; Wolf, R. D.; et al. (2017): Finding cyber threats with ATT&CK-based analytics. The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202. Verfügbar unter: https://www.mitre.org/sites/default/files/2021-11/16-3713-finding-cyber-threats-with-attack-based-analytics.pdf

[391] **Straub**, J. (2020): Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks, 2020 IEEE International Conference on Smart Cloud (SmartCloud), Washington, DC, USA, 2020, S. 148 – 153, https://doi.org/10.1109/SmartCloud49737.2020.00035

[392] **The MITRE Corporation** (2023): ATT&CK Matrix for Enterprise [Online], [Zugriff am: 12.07.2023]. Verfügbar unter: https://attack.mitre.org/

[393] **Svetozarov Naydenov**, R.; Malatras, A.; Lella, I.; Theocharidou, M.; Ciobanu, C.; Tsekmezoglou, E. (2022): ENISA threat landscape 2022: July 2021 to July 2022, European Union Agency for Cybersecurity, Verfügbar unter: https://data.europa.eu/doi/10.2824/764318

[394] **HBM Sensor Inside Redaktion** (o.A.): Messtechnik auf der Schiene [Online], in: HBM Sensor, [Zugriff am: 25.03.2022]. Verfügbar unter: https://www.hbm.com/de/2393/messtechnik-auf-der-schiene/

13 Anhänge

13.1 Anwendungssteckbriefe priorisierter Use Cases im Workshop 1

In diesem Kapitel werden in Abbildung 92 bis Abbildung 97 die im Workshop 1 ausgefüllten Anwendungssteckbriefe priorisierter Use Cases dargestellt, auf die in Kapitel 4.2 eingegangen wurde.

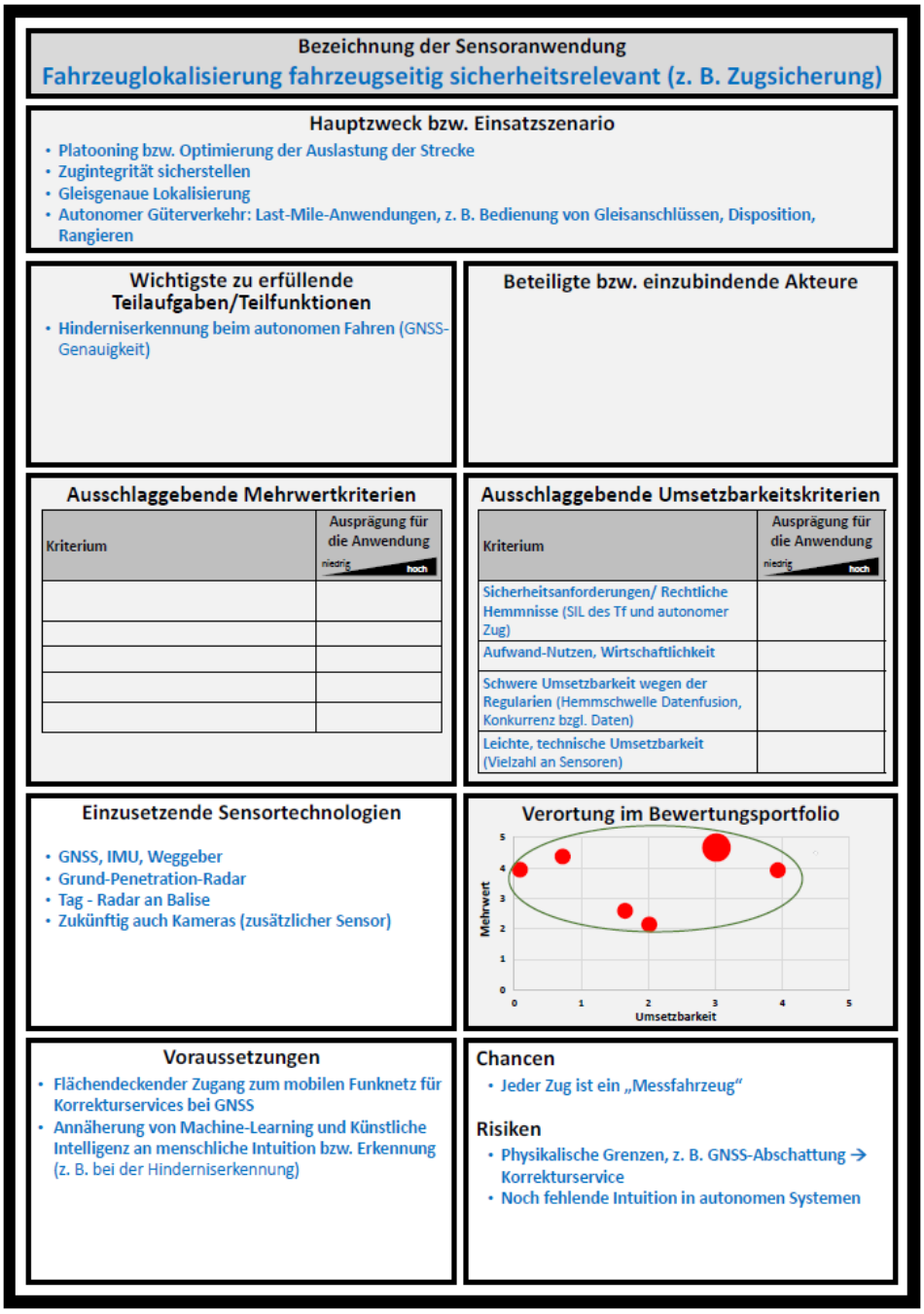


Abbildung 92: Anwendungssteckbrief zum Use Case Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant (z. B. Zugsicherung)

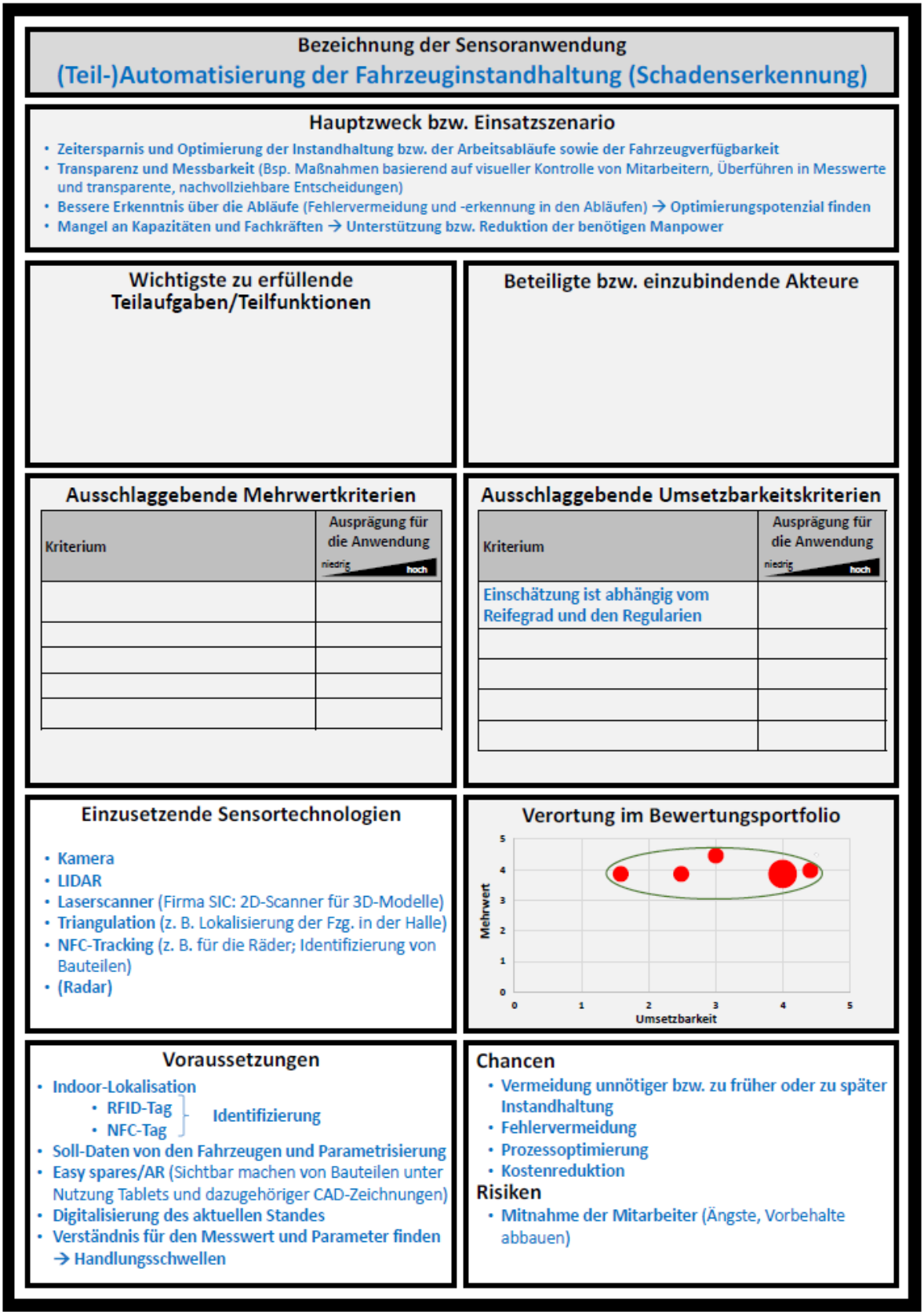


Abbildung 93: Anwendungssteckbrief zum Use Case *(Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)*

Bezeichnung der Sensoranwendung

Umfeldüberwachung bzw. Objekterkennung fahrzeugseitig

Hauptzweck bzw. Einsatzszenario

- Erkennen von Veränderungen beim Grünschnitt und bei an Fahrweg angrenzenden Objekten
- Identifikation von Objekten bei Aufprall
- **Einsatz im Rangierverkehr** (derzeit müssen beide Zugspitzen besetzt sein, Mitarbeiter bei Personalmangel so effizient wie möglich einsetzen)
- Fahrwegkontrolle bei Automatic Train Operation

Wichtigste zu erfüllende Teilaufgaben/Teilfunktionen

- Vegetationskontrolle
- Zustandsfeststellung der Strecke nach Ereignissen (Befahrbarkeit nach Stürmen o. ä.)
- **Überprüfung des Fahrweges** (sehen wo ich hinfahre)

Beteiligte bzw. einzubindende Akteure

- Technisches System selbst und dessen Bereitsteller
- Eisenbahnverkehrsunternehmen
- Eisenbahninfrastrukturunternehmen

Ausschlaggebende Mehrwertkriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Senkung von Betriebskosten	2,6
Verbesserung der Sicherheit	3,6
Erhöhung der Systemzuverlässigkeit	3,8
Prozessoptimierung	3,6
Synergien m. anderen Technologien	2,6

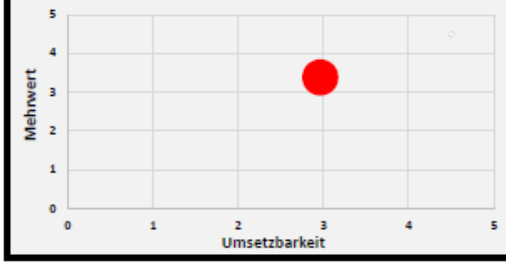
Ausschlaggebende Umsetzbarkeitskriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Kosten-Nutzen-Verhältnis	2,6
Technologischer Reifegrad	2,0
Marktseitige Durchsetzbarkeit	2,8
Akzeptansaussichten	3,4
Beherrschbarkeit der Komplexität	1,2
Finanzierung	2,6

Einzusetzende Sensortechnologien

- Kamera
- Lidar
- Radar

Verortung im Bewertungsportfolio



Voraussetzungen

- Rechtlicher Rahmen
- Digitale dynamische Karten
- Auswertbarkeit (Ort an der Strecke) muss gegeben sein

Chancen

- Kostenreduktionen
- Vorbereitung Automatic Train Operation

Risiken

- Zuverlässigkeit bei ungünstigen Witterungsbedingungen
- Sicherstellung der Echtzeitauswertung der Informationen immer möglich? (via maschinelles Lernen)

Abbildung 94: Anwendungssteckbrief zum Use Case *Umfeldüberwachung bzw. Objekterkennung fahrzeugseitig*

Bezeichnung der Sensoranwendung

Überwachung Bremse

Hauptzweck bzw. Einsatzszenario

- **Vereinfachung/Automatisierung der Bremsprobe vor jeder Zugfahrt** (heutige, sehr zeitintensive Wagenmeister-aufgabe, Druck die Mitarbeiter aufgrund von Personalmangel so effizient wie möglich einzusetzen)
- **Insb. im Güterverkehr (ständige Zugneubildung) viel manuelle Arbeit ersetzbar** (Hebel umlegen; Wiegeventile)
- **Zustandsfeststellung für jede einzelne Bremse im Betrieb**
- **Zustandsorientierte Instandhaltung mit Condition Monitoring**

Wichtigste zu erfüllende Teilaufgaben/Teilfunktionen

- **Zustandsfeststellung**
  (Bremse ist angelegt & wirksam oder gelöst)
- **Informationsübertragung inkl. Human-Machine-Interfaces**
- **Stromversorgung**
  (Batterietausch in Intervallen, ggf. Energy Harvesting)

Beteiligte bzw. einzubindende Akteure

- Stakeholder der Digitalen Automatischen Kupplung (DAK) als übergeordnetes Thema
- Fahrzeug-/Wageneigentümer bzw. -halter
- Eisenbahnverkehrsunternehmen
- Triebfahrzeugführer

Ausschlaggebende Mehrwertkriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Produktivitätssteigerung	4,5
Senkung von Instandhaltungskosten	3,2
Senkung von Betriebskosten	3,8
Erhöhung der Systemzuverlässigkeit	1,6
Verbesserung der Sicherheit	1,0

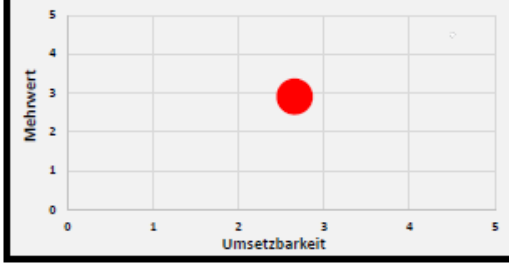
Ausschlaggebende Umsetzbarkeitskriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Technologischer Reifegrad	1,2
Marktseitige Durchsetzbarkeit	2,4
Beherrschbarkeit der Komplexität	2,0
Höhe der Investitionsbedarfe	3,8
Organisatorische Umsetzbarkeit	3,8

Einzusetzende Sensortechnologien

- Drucksensoren
- Kraftsensoren
- Temperatursensoren

Verortung im Bewertungsportfolio



Voraussetzungen

- Europäische Lösung finden
- „Dürfen" von Seiten der Aufsichtsbehörden
- Neuentwicklungen sind erforderlich (u. a. keine bereits vorhandenen Schnittstellen)
  → modernere Güterwagen
- Stromversorgung für die Sensoren muss sichergestellt werden (bisher alles pneumatisch)

Chancen

- Erhebliche Produktivitätssteigerungen
- Längere Nutzung mechanischer Bauteile als bei rein zeitorientierter Instandhaltung möglich
- Nutzung der Kommunikationsmodule für weitere Anwendungen

Risiken

- Eventuell unzureichende Zuverlässigkeit?

Abbildung 95: Anwendungssteckbrief zum Use Case *Überwachung Bremse*

Bezeichnung der Sensoranwendung

Fahrzeug überwacht Oberbau

Hauptzweck bzw. Einsatzszenario

- **Zustandsdatensammlung Gleise, Schwellen, Weichen durch Regelverkehrsfahrzeuge** („Masse statt Klasse")
- **Kürzere Zeitintervalle im Vergleich zu Fahrten mit Prüfzügen** (kritische Fälle und Trends frühzeitig erkennen)
- **Predictive Maintenance Infrastruktur** (in Verbindung mit solcher am Fahrzeug, z. B. Flachstellen am Radsatz)
- **Aktuelle Datensätze** (Prüfzug ggf. aller 3 Monate) → **Generierung von Live-Daten**
- **Besseres Verständnis des Witterungseinflusses auf den Schienenzustand** (Antriebs- und Schlupfoptimierung)

Wichtigste zu erfüllende Teilaufgaben/Teilfunktionen

- Prioritätensetzung, z. B. Schienenbruchdetektion, Schlupferkennung
- Präzise räumliche Verortung durch die Sensorik
- Integration und Auswertung der Datensammlung im Backend → Nutzen durch Datenmanagement und Autonomie des Systems
- Datenübertragung und -ablage (Cloud)

Beteiligte bzw. einzubindende Akteure

- Fahrzeughersteller und -instandhalter
- Infrastrukturbetreiber
- Akteure mit Datenverarbeitungskompetenz
- Zulassungsbehörden
- Gutachter

Ausschlaggebende Mehrwertkriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Aktualität der Daten	5,0
Frühere und zielgerichtetere Daten in der Instandhaltung und für den Einsatz von Messzügen	5,0

Ausschlaggebende Umsetzbarkeitskriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Autonomie	5,0
Wartungsfreiheit	4,0
Rückwirkungsfreiheit in Bezug auf Fahrzeug und Infrastruktur	5,0
Verwertbare Datenqualität	3,0
Standardisierung der Daten und Datenverarbeitungsschnittstellen	4,0

Einzusetzende Sensortechnologien

Verortung im Bewertungsportfolio

Voraussetzungen

- Nutzen/Anreiz für das Eisenbahnverkehrsunternehmen, diese Dienstleistung für Infrastrukturbetreiber anzubieten, muss existieren
- Beim Ersatz der Messzüge als Fernziel muss der Nachweis der mindestens gleichen Genauigkeit wie die bisher üblichen Messzüge erbracht werden

Chancen

Risiken

- Auf Fahrten mit Prüffahrzeugen kann nicht gänzlich verzichtet werden, da diese technisch bedingt genauere Daten liefern

Abbildung 96: Anwendungssteckbrief zum Use Case *Fahrzeug überwacht Oberbau*

Bezeichnung der Sensoranwendung

Umfeldüberwachung bzw. Objekterkennung infrastrukturseitig

Hauptzweck bzw. Einsatzszenario

- Freiraumüberwachung an Bahnübergängen als „einfaches" Anwendungsfeld, insbesondere:
  → als Lösung für technisch nicht gesicherte Übergänge (= nur Andreaskreuz vorhanden)
  → Beschleunigung von Folgeprozessen nach einem stattgefundenen Ereignis (z. B. eingeschlossenes Auto)
- In kritischen Bereichen mit vielen Menschen und viel Personenbewegung
- Sonderfall Bahnsteigüberwachung (besonders herausfordernd hinsichtlich Fehlalarme)

Wichtigste zu erfüllende Teilaufgaben/Teilfunktionen

- Freiraumerkennung/Gleisfreimeldung (z. B. Identifikation stehenbleibender Autos, weil Straßenverkehr nicht abfließen kann)
- Sensorintegration
- (technische Sicherung mit Lichtanlage)
- Informationsübertragung an den Triebfahrzeugführer inkl. Human-Machine-Interface

Beteiligte bzw. einzubindende Akteure

- Signaltechnikhersteller
- Infrastrukturbetreiber
- Gutachter
- Datenschützer (Bsp. Kamera)
- Zulassungsbehörde
- Vulnerable Road User (Fußgänger, Radfahrer) mit ihren mobilen Endgeräten

Ausschlaggebende Mehrwertkriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Sensorintegration in Signallaufprozess	5,0
Zuverlässigkeit	5,0
Gesellschaftliche Akzeptanz	3,0
Smarte Sensorik für komplexere Szenarien (Bsp. Fuchs oder Zeitung)	4,0
Problemerkennung/Klassifizierungsfähigkeit (Grenzwerte definieren)	5,0

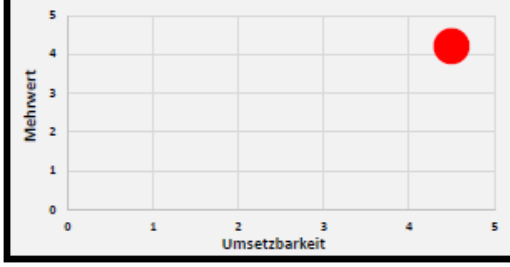
Ausschlaggebende Umsetzbarkeitskriterien

Kriterium	Ausprägung für die Anwendung (niedrig – hoch)
Zuverlässigkeit der Systeme	5,0
Schnittstelle zur Betriebszentrale	4,0
Unterscheidung realer Alarm/Fehlalarm (Haftungsklärung)	5,0
Wirtschaftlichkeit	4,0

Einzusetzende Sensortechnologien

- Kamera
- Lidar
- Radar

Verortung im Bewertungsportfolio



Voraussetzungen

- Sensorsystem darf keine Störungen im Bahnsystem verursachen
- Datenschutzthematik muss geklärt werden
- hohe Zuverlässigkeit der Sensorik
- System muss Hindernisse am Bahnübergang differenzieren können
- Quantifizierung der Opfer und/oder Schadensfälle an Bahnübergängen (für die Ermittlung der allowable costs)

Chancen

- Erhöhung der Sicherheit an Bahnübergängen, der Verfügbarkeit von Strecken, der Robustheit des Gesamtsystems (weniger Kollisionen, Störungen)
- Infrastrukturseitige Unterstützung von Automatic Train Operation

Risiken

- Fehlfunktionen; unklare Haftungsfragen
- Keine hinreichende Wirtschaftlichkeit bzw. keine Bereitschaft zur Kostentragung

Abbildung 97: Anwendungssteckbrief zum Use Case *Umfeldüberwachung bzw. Objekterkennung infrastrukturseitig*

13.2 Anforderungskriterien

Dieses Kapitel enthält die Anforderungskriterien an Sensoren. Im ersten Unterkapitel erfolgt eine Erläuterung bevor im zweiten Unterkapitel die Kriterien auf die Use Cases angewendet werden.

13.2.1 Erläuterung

An dieser Stelle werden in Tabelle 85 bis Tabelle 97 die Anforderungskriterien der zugehörigen Anforderungsgruppen entsprechend Kapitel 4.3.3 ausgeführt.

Betriebsbedingungen

TABELLE 85: ANFORDERUNGSKRITERIEN DER GRUPPE „BETRIEBSBEDINGUNGEN“

Nr.	Schlagwort	Anforderungskriterium
B1	Beschleunigung	Robustheit ggn. Beschleunigung bzw. Verzögerung
B2	Erschütterung	Robustheit ggn. Rütteln, Schütteln, Erschütterungen
B3	Schwingungen	Robustheit ggn. ertragbaren Schwingungen
B4	Stoß	Robustheit ggn. Stoß und Ruck
B5	Vibration	Robustheit ggn. Vibrationen
B6	Druck	Resistenz ggn. Druckimpulsen und Staudruck durch Zugbegegnungen bei hoher Geschwindigkeit und Tunnelfahrten
B7a	Temperatur	Gewährleistung der Arbeitsfähigkeit im Betriebstemperaturbereich gemäß DIN EN 50155 und einer + 15°C höheren Einschalttemperatur
B7b	Temperatur	Ertragen von schnellen Temperaturänderungen, z. B. während Tunneldurchfahrten
B8a	Materialien	Ertragen von Staub
B8b	Materialien	Ertragen von Schotterflug
B9	Schadstoffe	Robustheit gegenüber Störeinflüssen wie Schadstoffe und Einwirkungen abrasiver Medien (z. B. aufgewirbelter Sand)
B10a	Masse	Geringer Einfluss auf die Masse des Fahrzeugs
B10b	Masse	Einhalten der Radsatzlast
B11	Lichtraumprofil	Einhalten des Lichtraumprofils
B12	Sichtfeld	Freihaltung der Sichtfelder der Scheiben
B13	Fahrkomfort	Keine Platzeinschränkungen und Lärmbelästigung für Fahrgäste und Zugpersonal
B14	Daten	Bestimmung der notwendigen Aktualität der Sensordaten
B15	Einsatzzeit	Gewährleistung der Arbeitsfähigkeit während der notwendigen Einsatzzeit
B16a	Fehlhandlungen	Menschliche Fehlhandlungen dürfen nicht zu Funktionsausfällen führen
B16b	Fehlhandlungen	Diagnoseeinrichtungen, die den Betriebsablauf überwachen und ausführen können, benötigen eine Verriegelung, um den Betrieb nicht zu unterbrechen.

Umwelt

TABELLE 86: ANFORDERUNGSKRITERIEN DER GRUPPE „UMWELT“

Nr.	Schlagwort	Anforderungskriterium
U1	IP-Klasse	Bestimmung der IP-Klasse
U2a	Konstruktive Auslegung	Auslegung unter Beachtung der Schutzmaßnahmen vor Rost und Korrosion
U2b	Konstruktive Auslegung	Auslegung, sodass Wasseransammlungen und damit verbundener Schimmel sowie Ablagerung von Materialien, wie Sand, Pollen, Blätter, Schwefelrege, Fasern, schädliche Insekten vermieden wird
U3	Höhenlage	Beständigkeit gegenüber unterschiedlichen Umgebungsdrücken durch Höhenlage
U4a	Luftfeuchtigkeit	Beständigkeit ggn. hoher Luftfeuchtigkeit gemäß Werten aus DIN EN 50125-1
U4b	Luftfeuchtigkeit	Keine Funktionsausfälle durch Schwitzwasser/Kondensation
U5	Temperatur	Einhaltung des Arbeitsbereiches der Temperaturklasse gemäß DIN EN 50125-1 sowie eventueller zu bestimmender höherer Temperaturen nahe dem Gleiskörper oder über dem Dach
U6	Sonne	Ertragen von Sonneneinstrahlungen bis zu 1120 W/m²
U7	UV	Ertragen von UV-Strahlung
U8	Ozon	Bei Einsatz von Gummi- oder Kunststoffmaterialien: Beständigkeit ggn. Ozonstrahlung
U9a	Niederschlag	Keine Funktionseinschränkungen durch Niederschlag in Form Regen, Schnee, und Hagel
U9b	Niederschlag	Vermeidung von Eisbildung, herabfallendes Eis und Eislasten
U10	Materialien	Robustheit gegenüber größeren Elementen, wie Vögel, Kohle, Steinschlag
U11a	Schadstoffe	Vermeidung umweltbelastenden Abriebs
U12b	Schadstoffe	Resistenz ggn. Schadstoffen, wie z. B. Ölen, Schmierstoffen, Lösungsmitteln, ätzenden Lösungen sowie atmosphärischen, chemischen und biologisch aktiven Stoffen sowie Salznebel
U13	Wind	Beständigkeit gegenüber (Seiten-)Wind
U14	Nebel	Funktionsfähigkeit im Nebel
U15	Helligkeit	Funktionsfähigkeit bei Dunkelheit und Blendung bzw. Tag und Nacht
U16	Blitz	Ertragen der Auswirkungen von Blitzschlägen

Schnittstellen

a. Allgemein

TABELLE 87: ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN – ALLGEMEIN“

Nr.	Schlagwort	Anforderungskriterium
S-A1	Kompaktheit	Geringe Anzahl an Schnittstellen: mechanisch, elektrisch, datentechnisch, kommunikationstechnisch
S-A2	Schnittstellen	Vollständige Schnittstellendokumentation
S-A3	Standard	Herstellerübergreifende Standardschnittstellen

b. Elektro

TABELLE 88: ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN – ELEKTRO"

Nr.	Schlagwort	Anforderungskriterium
S-E1	Stromversorgung	Einhaltung der Anforderungen zur Stromversorgung gemäß DIN EN 50155, z. B. zu Themen wie Spannungs- und Stromversorgung, Schutzeinrichtungen
S-E2	Sicherheit	Einsatz und Zugänglichkeit von Überstrom- und Überspannungsschutz-einrichtungen
S-E3	Isolation	Geringe Potenzialdifferenzen und Einhaltung der Isolationskoordination nach DIN EN 50124-1
S-E4	Erdung	Gewährleistung einer Erdung
S-E5	Entwicklung	Einhaltung des Vorgehens nach DIN EN 50129 für sicherheitsrelevante elektronische Systeme

c. Daten

TABELLE 89: ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN – DATEN"

Nr.	Schlagwort	Anforderungskriterium
S-D1	Daten	Sicherstellung einer Priorisierung bei der Übertragung von Daten
S-D2	Gefährdungsrate	Verzögerungsfreie Signalübertragung
S-D3a	Datenverarbeitung	Definition der Datenverarbeitung
S-D3b	Datenverarbeitung	Definition des Datenabrufs
S-D4	Entwicklung	Softwareentwicklung nach DIN EN 50657

d. Kommunikation

TABELLE 90: ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN – KOMMUNIKATION"

Nr.	Schlagwort	Anforderungskriterium
S-K1	Internet	Verfügbarkeit von Wifi und Ethernet
S-K2	Kompatibilität	Kompatibilität mit Signalen anderer Sensoren
S-K3	Mobilfunk	Bestimmung eines Mobilfunkstandards
S-K4	Protokoll	Bestimmung eines Protokollstandards

Montage

TABELLE 91: ANFORDERUNGSKRITERIEN DER GRUPPE „MONTAGE“

Nr.	Schlagwort	Anforderungskriterium
M1	Bauraum	Einhaltung des vorgegebenen Bauraumes
M2	Position	Geeigneter Einbauort für Sensortyp
M3	Befestigungsart	Einhaltung der Norm für gewählte Befestigungsart, z. B.: Kleben DIN 6701 und DIN EN 17460 Schweißen DIN EN 15085 Festigkeitsnachweis für Schrauben
M4	Haltbarkeit	Auslegung der Elastizität und Dauerfestigkeit der Befestigung entsprechend Einsatzbedingungen

Nr.	Schlagwort	Anforderungskriterium
M5	Verkabelung	Montage der Verkabelung nach DIN EN 50343
M6	Energiefluss	Gefahrloser Energie- und Wärmefluss
M7	Rückwirkungsfreiheit	Rückwirkungsfreiheit bei nachträglicher Montage
M8	Einbauanweisung	Definition der spezifischen Einbauanweisungen zu thermischen Anforderungen, Handhabung, Kabellänge und Montage ohne Beschädigung benachbarter Bauteile

Störung anderer Systeme/EMV

TABELLE 92: ANFORDERUNGSKRITERIEN DER GRUPPE „STÖRUNG ANDERER SYSTEME/EMV“

Nr.	Schlagwort	Anforderungskriterium
EMV1	EMV-Prüfung	Durchführung einer EMV-Prüfung zur Einhaltung aller allgemeinen EMV-Anforderungen sowie bahnspezifischen Anforderungen gemäß DIN EN 50121 Teil 1 – 5.
EMV2	Funk	Funkschutz von/vor anderen Funkkommunikationen durch Bestimmung des Frequenzspektrums, insbesondere in direkter Nähe des Fahrzeugs und im benachbarten Gleisbereich (ETCS-Datenfunk, Zugfunk, Rangierfunk, Funkfernsteuerung Rangierlokomotiven, Elektronische Fahrplandaten)
EMV3	Induktion	Schutz vor Induktion durch Fahrdraht, Indusi, Wirbelstrombremse, Magnetschienenbremse
EMV4	Zugsicherung	Schutz vor Einwirkungen von Zugbeeinflussungssystemen und Zugortungsanlagen im Gleis und auf dem Fahrzeug
EMV5	Hochspannung	Schutz von/vor Hochspannungsfreileitungen
EMV6	Magnete	Resistenz von/vor Streufeldern von Fahrmotoren, Umrichtern, Drosseln, Kabeln
EMV7	Metalle	Keine Beeinflussung durch Metallteile im Einwirkbereich der Gleisschaltmittel
EMV8	Radar	Schutz vor sonstigen Radareinrichtungen
EMV9	Sensoren	Schutz von/vor anderen Sensoren

Betriebssicherheit & Zuverlässigkeit

TABELLE 93: ANFORDERUNGSKRITERIEN DER GRUPPE „BETRIEBSSICHERHEIT & ZUVERLÄSSIGKEIT“

Nr.	Schlagwort	Anforderungskriterium
BZ1	Ausfallsicherheit	Geringe Ausfallrate
BZ2	Defektsignalisierung	Erkennung und Signalisierung eines Defekts
BZ3	Ergebnissicherheit	Vermeidung falsch positiver und falsch negativer Sensorergebnisse
BZ4	Zuverlässigkeit	Erstellung eines Nachweises der Zuverlässigkeit
BZ5	Brauchbarkeitsdauer	Gewährleistung der Funktionsfähigkeit gemäß der Brauchbarkeitsdauerklasse nach DIN EN 50155
BZ6a	Konstruktive Auslegung	Dauerfeste Auslegung der Befestigung unter Berücksichtigung der FEM-Festigkeitswerte der Werkstoffe
BZ6b	Konstruktive Auslegung	Gewährleistung von thermischen Integrationseinschränkungen
BZ7	Redundanz	Sicherstellung einer Redundanz in Abhängigkeit des SIL-Levels

Verfügbarkeit

TABELLE 94: ANFORDERUNGSKRITERIEN DER GRUPPE „VERFÜGBARKEIT“

Nr.	Schlagwort	Anforderungskriterium
V1	Marktverfügbarkeit	Einfache Beschaffung durch Marktverfügbarkeit
V2	Lieferzeit	kurze Lieferzeit
V3	Kosten	geringe Anschaffungs- und Instandhaltungskosten
V4	Betriebszeit	Bestimmung der mittleren Betriebszeit, MUT (Mean up time)
V5	Abtastrate	Geeignete Abtastrate
V6	Stromversorgung	Gewährleistung der Strom-/Spannungsversorgung
V7	Toleranzen	Geeignete Systemtoleranzen
V8	Selbstprüfung	Funktion der Selbstdiagnose
V9	Überwachung	Überwachungsfunktion zur Gewährleistung eines Wiederanlaufs
V10	Ausfallanzeige	Aufzeichnung oder Anzeigen von Ausfallereignissen
V11	Instandhaltungszeit	Geringe Instandhaltungszeit

Instandhaltung

TABELLE 95: ANFORDERUNGSKRITERIEN DER GRUPPE „INSTANDHALTUNG“

Nr.	Schlagwort	Anforderungskriterium
I1	Identifizierbarkeit	Möglichkeit der Identifizierung der Komponente
I2	Reparaturzeit	Möglichst geringe mittlere Zeit zur Wiederherstellung (MTTR)
I3	Vorbeugende Instandhaltung	Idealerweise Gewährleistung von Wartungsfreiheit. Wenn dies nicht möglich ist, Abstimmung der Instandhaltungs- und Kalibrierzeitpunkte der Sensorlösung auf die des Fahrzeugs.
I4	Dokumentation	Übergabe des Datenblattes, der Bedienungsanleitung und des Instandhaltungshandbuches an den Anwender
I5	Reinigbarkeit	Gewährleistung der Reinigbarkeit
I6	Reparierbarkeit	Zugang für die Diagnose und die Reparatur soll ohne Beschädigung oder unangemessene Beeinträchtigung der Bauelemente oder der Verdrahtung erfolgen.
I7	Werkstatt	Ermöglichen von Standardwerkstattanforderungen
I8	Werkzeug	Einsatz von Standardwerkzeugen
I9	Ersatzteile	kurze und einfache Lieferbarkeit von Ersatzteilen
I10	Zeitbedarf	Schnelle (De)montage
I11	Betriebsstofffreiheit	Ermöglichen von Betriebsstofffreiheit
I12	Lebensdauer	Gewährleistung der Verfügbarkeit von Ersatzteilen trotz Obsoleszenz

Security

TABELLE 96: ANFORDERUNGSKRITERIEN DER GRUPPE „SECURITY“

Nr.	Schlagwort	Anforderungskriterium
SE1	SIL	Bestimmung des Software-SIL-Levels
SE2	Sicherheit	Ausreichende Sicherheit des Netzwerks
SE3	Angreifbarkeit	Schutz des Sensors und des Kontrollsystems vor Softwareangriffen
SE4	Vandalismus	Vermeidung von beabsichtigter und fahrlässiger Beschädigung
SE5	Updatebarkeit	Updatebarkeit von Software
SE6	Austauschbarkeit	Austauschbarkeit der Recheneinheit, der Software und des Schlüssels
SE7	Schnittstellen	Auswahl zwischen offener oder geschlossener Schnittstelle vor dem Hintergrund der Sicherheit
SE8	Integration	Erfüllung der Anforderungen für die Software-Hardware-Integration
SE9	Rückfallebene	Vorsehen einer Rückfallebene bei Installation einer neuen Softwareversion
SE10	Verschlüsselung	Einhaltung von Verschlüsselungsstandards

Safety

TABELLE 97: ANFORDERUNGSKRITERIEN DER GRUPPE „SAFETY“

Nr.	Schlagwort	Anforderungskriterium
SA1	funktionale Sicherheit	Nachweis funktionaler Sicherheit
SA2	SIL	Bestimmung des SIL-Levels (Safety Integrity Level)
SA3	Risikoakzeptanz	Einhaltung der Risikoakzeptanzkriterien gemäß CSM
SA4a	Gefährdungen	Geringe Gefährdungsrate
SA4b	Gefährdungen	Erstellung eines Gefahrenlogbuches
SA5	Fail-Safe	Gewährleistung eines sicheren Zustandes im Fehlerfall inkl. ausreichender Kühlung und keiner Beeinflussung der Notstromverfügbarkeit
SA6	Ausfallerkennung	Einhaltung von Strategien zur Ausfallerkennung
SA7	Fehleranalyse	Durchführung einer FMEA/FMECA-Analyse vor Inbetriebnahme und einer FRACAS-Analyse nach Inbetriebnahme
SA8	Fehlerrate	Erstellung eines Reliability Block Diagramms
SA9	Autorisierung	Gewährleistung eines räumlichen Zuganges nur mit Autorisierung
SA10	Schutz von Personen	Schutz von Personen gegen: - elektrische Gefahren - Auswirkungen überhöhter Temperaturen - Betriebsmittel, Konstruktion und Verwendung von Materialien
SA11	Betreiber	Einhalten der Anforderungen der Anwender, EIUs, EVUs sowie Infrastruktur- bzw. Fahrzeughalter
SA12a	Brandschutz	Einhalten der Brandschutzanforderungen für Kabel nach DIN EN 50306, DIN EN 50264 und DIN EN 50382
SA12b	Brandschutz	Einhalten der Anforderungen der Brandschutzklassen für spezifische Komponenten
SA12c	Brandschutz	Ausreichende Feuerwiderstandsklasse
SA13	Explosionsschutz	Schutz in ATEX Bereichen

13.2.2 Anwendung der Kriterien auf die Use Cases

Für eine bessere Übersicht erhalten die Use Cases hier die Nummern aus der Gesamt Use Case Liste. Demnach gelten die folgenden Nummerierungen:

- 3b – Fahrzeug überwacht Fahrzeug: Antriebszustand (Elektro)
- 3f – Fahrzeug überwacht Fahrzeug: Zustand von Türen u. a. Verriegelungen
- 5 – Infrastruktur überwacht Fahrzeug - nicht sicherheitsrelevant
- 6 – Fahrzeuglokalisierung fahrzeugseitig sicherheitsrelevant
- 24 – Fahrzeug überwacht Oberbau
- 31 – Weichenferndiagnose
- 34 – (Teil-)Automatisierung der Fahrzeuginstandhaltung (Schadenserkennung)

Sofern genaue Werte angegeben werden können, ist dies bei den einzelnen Kriterien der Fall. Wenn es sich um allgemeinere Anforderungen handelt, wird eine Bewertung vorgenommen, ob das jeweilige Kriterium zutreffend ist oder nicht. „Zutreffend“ meint in diesem Fall, dass das Kriterium für den jeweiligen Use Case wichtig ist und beachtet werden sollte, es jedoch keine genaueren Anforderungen in Standards und Richtlinien dazu gibt bzw. diese jetzt noch nicht näher definiert werden können.

Betriebsbedingungen

TABELLE 98: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „BETRIEBSBEDINGUNGEN“

<table>
<tr><th>Nr.</th><th>3b</th><th>3f</th><th>6</th><th>24</th><th>5</th><th>31</th><th>34</th></tr>
<tr><td rowspan="2">B1</td><td colspan="4">Nach DIN EN 12663: Am Wagenkasten gilt:
y: ±1g, z: (1±c)*g, bei Güterwagen in x: ±5 g, bei Lokomotiven in x: ±3 g, bei Personenfahrzeugen in x: ±2/3/5 g je nach Kategorie</td><td colspan="3" rowspan="2">Auslegung nach EN 60721-3-3/3-4 oder Tabelle 6 in DIN EN 50125-3 (Ableitung aus ERRI A 118 RP 4) für Schiene, Schwelle, Gleisbett und Schaltkasten am Betonpfahl außerhalb der Gleise (1 – 3 m Abstand)</td></tr>
<tr><td>Nach DIN EN 13749: Beschleunigungen für Anbauteile am DG-Rahmen: Außergewöhnlich: vertikal ±20 g, quer ±10 g, längs ±3 g oder ±5 g Dauernd: vertikal ±6 g, quer ±5g , längs ±2,5 g</td><td>-</td><td colspan="2">Nach DIN EN 13749: Beschleunigungen für Anbauteile am DG-Rahmen: Außergewöhnlich: vertikal ±20 g, quer ±10 g, längs ±3 g oder ±5 g Dauernd: vertikal ±6 g, quer ±5 g, längs ±2,5 g Beschleunigungen für Anbauteile am Radsatzlager: Außergewöhnlich: vertikal ±70 g, quer ±10 g, längs ±10 g Dauernd: vertikal ±25 g, quer ±5 g, längs ±5 g</td></tr>
<tr><td>B2</td><td colspan="4">Es können die gleichen Werte wie bei Beschleunigungen herangezogen werden.</td><td colspan="3">Auslegung nach EN 60721-3-3/3-4 oder Tabelle 6 in DIN EN 50125-3 (Ableitung aus ERRI A 118 RP 4) für Schiene, Schwelle, Gleisbett und Schaltkasten am Betonpfahl außerhalb der Gleise (1 – 3 m Abstand)</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>3b</th><th>3f</th><th>6</th><th>24</th><th>5</th><th>31</th><th>34</th></tr>
<tr><td rowspan="2">B3</td><td colspan="4">Nach Tabelle 1 in DIN EN 61373 Kapitel 8 für verschiedene Kategorien. Frequenzbereich Tabelle 2 in Kap. 9.</td><td colspan="3" rowspan="2">Auslegung nach EN 60721-3-3/3-4 oder Tabelle 5 in DIN EN 50125-3 für Schiene, Schwelle, Gleisbett und außerhalb der Gleise (1 – 3 m Abstand); ab einem Abstand von 3 m ist die vom Gleis ausgehende Belastung vernachlässigbar</td></tr>
<tr><td>Kat. 1 für Fahrzeugkasten</td><td>Kat. 1 für Fahrzeugkasten</td><td>Kat. 1 für Fahrzeugkasten, Kat. 2 für Drehgestell, Kat. 3 für Radsatz</td><td>Kat. 2 für Drehgestell, Kat. 3 für Radsatz</td></tr>
<tr><td rowspan="2">B4</td><td colspan="4">Nach Tabelle 3 in DIN EN 61373 Kapitel 10 für verschiedene Kategorien.</td><td colspan="3" rowspan="2">Auslegung nach EN 60721-3-3/3-4 oder Tabelle 6 in DIN EN 50125-3 (Ableitung aus ERRI A 118 RP 4) für Schiene, Schwelle, Gleisbett und Schaltkasten am Betonpfahl außerhalb der Gleise (1 – 3 m Abstand)</td></tr>
<tr><td>Kat. 1 für Fahrzeugkasten</td><td>Kat. 1 für Fahrzeugkasten</td><td>Kat. 1 für Fahrzeugkasten, Kat. 2 für Drehgestell, Kat. 3 für Radsatz</td><td>Kat. 2 für Drehgestell, Kat. 3 für Radsatz</td></tr>
<tr><td>B5</td><td colspan="4">Es können die gleichen Werte wie bei Beschleunigungen herangezogen werden.</td><td colspan="3">Auslegung nach EN 60721-3-3/3-4 oder Tabelle 5 in DIN EN 50125-3 für Schiene, Schwelle, Gleisbett und außerhalb der Gleise (1 – 3 m Abstand); ab einem Abstand von 3 m ist die vom Gleis ausgehende Belastung vernachlässigbar</td></tr>
<tr><td>B6</td><td>Nicht zutreffend, da im Innenbereich</td><td colspan="3">wenn im Außenbereich nach DIN EN 50125-1: Druckstöße müssen ertragen werden. K.A. über Größe, gemäß DIN EN 50125-3 bis zu +/- 5 kPa mit einer Änderungsgeschwindigkeit bis zu 1 kPa/s</td><td>Nur zutreffend, wenn Anlagen im Tunnel verbaut werden. Ist aber übertragbar, damit hohe Vorbeifahrgeschwindigkeiten ausgehalten werden: Nach Kap. 4.2.2 DIN EN 50125-3</td><td colspan="2">nicht zutreffend, da Durchfahrtsgeschwindigkeit an Werkstatteinfahrt gering sein wird</td></tr>
<tr><td>B7 a</td><td colspan="4">Standardmäßig: -25 bis +70 °C</td><td colspan="3">Temperaturbereich nach DIN EN 50125-3 übertragbar</td></tr>
<tr><td>B7 b</td><td>Nicht zutreffend, da im Innenbereich</td><td colspan="3">Kap. 4.3.4 in DIN EN 50155</td><td colspan="3">0,5 °C/min über Bereich von 20 °C nach DIN EN 50125-3 übertragbar</td></tr>
<tr><td>B8 a</td><td>Nicht zutreffend, da im Innenbereich</td><td colspan="3">Zutreffend</td><td colspan="3">Zutreffend</td></tr>
<tr><td>B8 b</td><td>Nicht zutreffend, da im Innenbereich</td><td colspan="3">Zutreffend, wenn im Außenbereich</td><td colspan="3">Zutreffend</td></tr>
<tr><td>B9</td><td>Nicht zutreffend, da im Innenbereich</td><td colspan="3">Zutreffend, wenn im Außenbereich</td><td colspan="3">Zutreffend</td></tr>
</table>

Nr.	3b	3f	6	24	5	31	34
B10a	möglichst gering, kann nicht genauer spezifiziert werden				Nicht zutreffend		
B10b	Zutreffend				Nicht zutreffend		
B11	Nicht zutreffend, da im Innenbereich	Zutreffend			Zutreffend		
B12	Nicht zutreffend, da nicht im Führerstand	nicht zutreffend, Montage außerhalb des Sichtfeldes angedacht			Nicht zutreffend		
B13	Zutreffend	Zutreffend im SPV	Platzeinschränkungen nicht zutreffend, Lärmbelästigung kann bei den hier außen angebrachten Sensoren (insbesondere am Dach) & im HGV-Bereich relevant sein	Platzeinschränkungen nicht zutreffend, Lärmbelästigung kann bei den hier außen angebrachten Sensoren evtl. im HGV-Bereich relevant sein	Nicht zutreffend		
B14	1x vor Abfahrt des Zuges und wenn sich Sensorsignal ändert		für ETCS-Prüfung 3s (inkl. Übertragung), für Zugintegrität 1s, Abfrage mit 10 Hz [aktuell bei DAK so angedacht]	bei Messwerten, die einen Grenzwert überschreiten sofort, ansonsten wenn Übertragungskapazität verfügbar ist oder bei Abstellung des Fahrzeugs	1x bei Durchfahrt des Zuges	1x bei Umstellen einer Weiche und in regelmäßigen Abständen, z. B. bestimmter Vorlauf vor Zugdurchfahrt	1x bei Durchfahrt des Zuges
B15	Vor Abfahrt, nach Ankunft und auch während des Fahrbetriebs		durchgehend, außer bei Abstellung des Zuges (erkennbar daran, dass System aus-/eingeschaltet wird)		(De-)Aktivierung über Radsensoren	(De-)Aktivierung über Radsensoren und Zeitstempel	(De-)Aktivierung über Radsensoren
B16a	Zutreffend		Zutreffend, wenn Mensch die Daten auswertet oder bei der		Zutreffend		

Nr.	3b	3f	6	24	5	31	34
			Instandhaltung sowie bei Eingriff im Fehlerfall.				
B1 6b	Zutreffend	Zutreffend	Nicht zutreffend, System ist dafür ausgelegt Handlungen zu erzielen	Nicht zutreffend, gibt keine Möglichkeit dafür	Nicht zutreffend, gibt keine Möglichkeit dafür	Zutreffend	Nicht zutreffend, gibt keine Möglichkeit dafür

Umwelt

TABELLE 99: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „UMWELT“

Nr.	3b	3f	6	24	5	31	34
U1	Bestimmen nach genauer Spezifikation des Einbauortes						
U2a	Zutreffend						
U2b	Nicht zutreffend, da im Innenbereich	Zutreffend					
U3	Auslegung nach Kap. 4.2 DIN EN 50125-1				Nicht zutreffend, einheitlicher Druck		
U4a	Auslegung nach Kap. 4.4 DIN EN 50125-1				Auslegung nach Tabelle 3 DIN EN 50125-3 übertragbar		
U4b	Zutreffend						
U5	Auslegung nach Kap. 4.3 DIN EN 50125-1				Temperaturbereich nach DIN EN 50125-3 übertragbar		
U6	Nicht zutreffend, da im Innenbereich	Zutreffend bei Montage im Außenbereich und wenn Sonnenlicht dorthin kommt			Zutreffend		
U7	Zutreffend						
U8	Zutreffend, wenn vorhanden						
U9a	Nicht zutreffend, da im Innenbereich	Zutreffend im Außenbereich			Zutreffend		
U9b	Nicht zutreffend, da im Innenbereich	Zutreffend im Außenbereich			Zutreffend		
U10	Nicht zutreffend, da im Innenbereich	Zutreffend im Außenbereich			Zutreffend		
U11a	Nicht zutreffend, da im Innenbereich	Zutreffend im Außenbereich			Nicht zutreffend		
U12b	Zutreffend						
U13	Nicht zutreffend, da im Innenbereich	Zutreffend im Außenbereich			Zutreffend		

Nr.	3b	3f	6	24	5	31	34
U14	Nicht zutreffend, da im Innenbereich	Zutreffend bei Einsatz von Kameras	Nicht mehr als 1 – 2 m, bei Bilderkennung ggf. mehrere Meter	Nicht mehr als 1 – 2 m	Ca. 2 bis max. 3 – 5 m	Mehrere Meter, je nach Weichenart bis zu 10 m	Ca. 2 bis max. 3 – 5 m
U15	Nicht zutreffend, da im Innenbereich	Zutreffend bei Einsatz von Kameras	Zutreffend bei Bilderkennung	Zutreffend, Sensoren sollten von sich aus aber unabhängig davon sein	Zutreffend		
U16	Nicht zutreffend, da es das gesamte Fahrzeug/ den gesamten Wagenkasten treffen wird	Zutreffend					

Schnittstellen

a. Allgemein

TABELLE 100: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN – ALLGEMEIN“

Nr.	3b	3f	6	24	5	31	34
S-A1	So gering wie möglich						
S-A2	Zutreffend						
S-A3	Zutreffend						

b. Elektro

TABELLE 101: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN – ELEKTRO"

Nr.	3b	3f	6	24	5	31	34
S-E1	Zutreffend				Nicht zutreffend, da für Fzg.		
S-E2	Zutreffend						
S-E3a	Zutreffend						
S-E3b	Zutreffend						
S-E4	Zutreffend						

c. Daten

TABELLE 102: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN – DATEN"

Nr.	3b	3f	6	24	5	31	34
S-D1	Zutreffend: da nicht sicherheitsrelevant sollte Fokus auf Grenzwertüberschreitungen liegen, darunter ist Reihenfolge nicht wichtig	zutreffend, Einklemmschutz muss höher sein als Schließzustand	Alle Daten sind wichtig, da sicherheitsrelevanter Fall	alle Daten sind wichtig, da sicherheitsrelevant. Reihenfolge der eingebauten Sensoren muss bestimmt werden.	nicht notwendig, weil gebündelt nur 1x pro Zug	Zutreffend, zunächst solche mit Grenzwertüberschreitungen, anschließend nach Relevanzbewertung der Sensoren	nicht notwendig, weil gebündelt nur 1x pro Zug
S-D2		Zutreffend, so gering wie möglich		Zutreffend, so gering wie möglich, wenn ein Grenzwert überschritten wurde	Nicht notwendig, andernfalls nur Zeitverzögerung	Zutreffend, so gering wie möglich	Nicht notwendig, andernfalls nur Zeitverzögerung
S-D3a	Zutreffend						
S-D3b	Zutreffend						
S-D4	Zutreffend				Nicht zutreffend, da für Fzg.		

d. Kommunikation

TABELLE 103: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „SCHNITTSTELLEN - KOMMUNIKATION"

Nr.	3b	3f	6	24	5	31	34
S-K1	zutreffend, sowohl auf dem Fahrzeug als auch in den Gebieten, wo das Fahrzeug fährt	zutreffend, wenn Übertragung an Tf nicht per Kabel durch Zug erfolgt	zutreffend, sowohl auf dem Fahrzeug als auch in den Gebieten, wo das Fahrzeug fährt		Zutreffend		
S-K2	Zutreffend						
S-K3a	Bestmöglich, d.h. 5G	Bestmöglich, d.h. 5G, wenn Übertragung an	Bestmöglich, d.h. 5G				

Nr.	3b	3f	6	24	5	31	34
		Tf nicht per Kabel durch Zug erfolgt					
S-K3b	Best geeignetster						

Montage

TABELLE 104: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „MONTAGE“

Nr.	3b	3f	6	24	5	31	34
M1	möglichst gering, kann nicht genauer spezifiziert werden				Größe ist nicht von großer Bedeutung, nur das Lichtraumprofil darf nicht verletzt werden		
M2	Zutreffend						
M3	Best mögliche, kann nicht genauer spezifiziert werden						
M4	Zutreffend						
M5	Zutreffend				Nicht zutreffend, da für Fzg. gültig		
M6	Muss erbracht werden						
M7	Zutreffend						
M8	Zutreffend				Nicht zutreffend, da Neukonstruktion		

Störung anderer Systeme/EMV

TABELLE 105: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „STÖRUNG ANDERER SYSTEME/EMV“

Nr.	3b	3f	6	24	5	31	34
EMV1	Zutreffend						
EMV2	Zutreffend						
EMV3	Zutreffend						
EMV4	Zutreffend						
EMV5	Zutreffend						
EMV6	Zutreffend						
EMV7	Zutreffend						
EMV8	Zutreffend						
EMV9	Zutreffend						

Betriebssicherheit & Zuverlässigkeit

TABELLE 106: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „BETRIEBSSICHERHEIT & ZUVERLÄSSIGKEIT“

Nr.	3b	3f	6	24	5	31	34
BZ1	Möglichst gering bei gegebener	Möglichst gering, da	Sehr gering, da sicherheitsrelevant		Möglichst gering, da	Möglichst gering, da	Möglichst gering, da

	Wirtschaftlichkeit, da ansonsten keine Diagnose möglich ist	ansonsten manuelle Handlungen notwendig sind		ansonsten manuelle Handlungen notwendig sind	ansonsten keine Diagnose möglich ist	ansonsten manuelle Handlungen notwendig sind
BZ2	Zutreffend					
BZ3	Zutreffend					
BZ4	Zutreffend					
BZ5	Zutreffend		Standardmäßig: 20 Jahre	Nicht zutreffend, da Infrastruktur Use Cases		
BZ6a	Zutreffend, jedoch nur für nicht standardmäßig eingebaute Sensoren notwendig	Zutreffend				nicht zutreffend, Lockerung fällt durch Nähe zur Werkstatt schnell auf und kann einfach erneuert werden
BZ6b	Zutreffend			Nicht zutreffend, keine Beeinflussung des Fahrzeugs durch Montage		
BZ7	Zutreffend			Nicht zutreffend		

Verfügbarkeit

TABELLE 107: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „VERFÜGBARKEIT“

Nr.	3b	3f	6	24	5	31	34
V1	Zutreffend						
V2	Bei Neubau nicht relevant, bei Ersatzteilen gewünscht						
V3	So günstig wie möglich bei möglichst hoher Qualität						
V4	So lange wie möglich, während des Betriebs bestimmen						
V5	Individuelle Wahl als Mittelweg zwischen stetiger Datenaufnahme für Diagnose und seltener Abtastrate wegen fehlender Sicherheitsrelevanz	10 Hz (in DAK aktuell so vorgesehen wegen ETCS-Prüfung) im Stillstand bei Öffnungs-/ Schließvorgang, sonst geringer (1x pro Minute?)	10 Hz (in DAK aktuell so vorgesehen wegen ETCS-Prüfung)	in Abhängigkeit der Geschwindigkeit und Messgröße einstellen, alle 16-25 cm [394]	1x pro Durchfahrt des Zuges	Individuelle Wahl als Mittelweg zwischen stetiger Datenaufnahme und nicht zu vielen Sensordaten	1x pro Durchfahrt des Zuges
V6	Zutreffend						
V7	In Abhängigkeit des spezifischen Sensors zu wählen						
V8	Zutreffend						

Nr.	3b	3f	6	24	5	31	34
V9	Zutreffend						
V10	Zutreffend						
V11	So kurz wie möglich bei moderaten Kosten, da nicht sicherheitsrelevant	So kurz wie möglich, da Fahrzeug ohne Instandhaltung nicht fahren darf aufgrund der Sicherheitsrelevanz bzw. manuelle Tätigkeiten wieder notwendig wären	So kurz wie möglich, da Fahrzeug ohne Instandhaltung nicht fahren darf aufgrund der Sicherheitsrelevanz	So kurz wie möglich, grundsätzlich aber nicht von allzu großer Bedeutung, da sich dann nur eine Fahrt verzögert und trotzdem ein höheres Messintervall als bisher erzeugt werden kann	so kurz wie möglich bei moderaten Kosten, da nicht sicherheitsrelevant. Wenn Fahren der Fahrzeuge beeinflusst wird, unabhängig der Kosten	So kurz wie möglich	so kurz wie möglich bei moderaten Kosten, da nicht sicherheitsrelevant. Wenn Fahren der Fahrzeuge beeinflusst wird, unabhängig der Kosten

Instandhaltung

TABELLE 108: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „INSTANDHALTUNG“

Nr.	3b	3f	6	24	5	31	34
I1	Zutreffend						
I2	So kurz wie möglich bei gegebener Wirtschaftlichkeit, da nicht sicherheitsrelevant.	So kurz wie möglich, da Fahrzeug ohne Instandhaltung nicht fahren darf aufgrund der Sicherheitsrelevanz bzw. manuelle Tätigkeiten wieder notwendig wären	So kurz wie möglich, da Fahrzeug ohne Instandhaltung nicht fahren darf aufgrund der Sicherheitsrelevanz	So kurz wie möglich, grundsätzlich aber nicht von allzu großer Bedeutung, da sich dann nur eine Fahrt verzögert und trotzdem ein höheres Messintervall als bisher erzeugt werden kann	So kurz wie möglich bei gegebener Wirtschaftlichkeit, da nicht sicherheitsrelevant. Wenn Fahren der Fahrzeuge beeinflusst wird, unabhängig der Kosten	So kurz wie möglich, da es sicherheitsrelevante Auswirkungen haben kann	So kurz wie möglich bei gegebener Wirtschaftlichkeit, da nicht sicherheitsrelevant. Wenn Fahren der Fahrzeuge beeinflusst wird, unabhängig der Kosten

Nr.	3b	3f	6	24	5	31	34
I3	Zutreffend				Nicht zutreffend		
I4	Zutreffend						
I5	Zutreffend						
I6	Zutreffend						
I7	Zutreffend				Nicht zutreffend, da ein spezifisches Team für Messstation zuständig ist		
I8	Zutreffend						
I9	So schnell wie möglich bei gegebener Wirtschaftlichkeit, um Prozesse nicht zu verlangsamen	Möglichst schnell, um Prozesse nicht zu verlangsamen durch manuelle Ersatztätigkeiten	So schnell wie möglich, da Fahrzeug ohne die Ersatzteile nicht fahren darf aufgrund der Sicherheitsrelevanz	So schnell wie möglich, da Einsatz sicherheitsrelevant werden kann, wenn Messfahrten dadurch ersetzt werden	Möglichst schnell, um Prozesse nicht zu verlangsamen durch manuelle Ersatztätigkeiten		
I10	So schnell wie möglich						
I11	Zutreffend						
I12	Zutreffend						

Security

TABELLE 109: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „SECURITY“

Nr.	3b	3f	6	24	5	31	34
SE1	Mittleres Level, da nicht sicherheitsrelevant	Hohes Level, wenn sicherheitsrelevant	Hohes Level, da sicherheitsrelevant	Hohes Level, wenn Messfahrten dadurch ersetzt werden	Mittleres Level, da nicht sicherheitsrelevant	Hohes Level, da sicherheitsrelevant	Mittleres Level, da nicht sicherheitsrelevant
SE2	Zutreffend						
SE3	Zutreffend						
SE4	Zutreffend						
SE5	Zutreffend						
SE6	Zutreffend						
SE7	Zutreffend						
SE8	Zutreffend						
SE9	Zutreffend						
SE10	Best geeignetster						

Safety

TABELLE 110: ANWENDUNG DER ANFORDERUNGSKRITERIEN DER GRUPPE „SAFETY“

Nr.	3b	3f	6	24	5	31	34
SA1	Zutreffend						
SA2	Muss bestimmt werden, abhängig von eingebauten Sensoren	Muss bestimmt werden, keine genauere Angabe möglich	Hohes Level	Hohes Level, wenn Messfahrten dadurch ersetzt werden	Muss bestimmt werden, keine genauere Angabe möglich		
SA3	Zutreffend						
SA4a	Zutreffend, so gering wie möglich						
SA4b	Zutreffend						
SA5	Zutreffend						
SA6	Zutreffend						
SA7	Zutreffend						
SA8	Zutreffend						
SA9	Zutreffend						
SA10	Zutreffend						
SA11	Zutreffend						
SA12a	Zutreffend				Nicht zutreffend, da für Fzg. Use Cases		
SA12b	Zutreffend						
SA12c	Zutreffend, je nach Einsatzgebiet des Fahrzeugs				Zutreffend		
SA13	Nicht zutreffend, elektrisch angetriebene Fahrzeuge werden nicht in ATEX-Bereiche fahren	Zutreffend, wenn Fahrzeug für ATEX-Bereiche ausgelegt ist			Zutreffend, falls in ATEX-Bereichen aufgestellt, sollte aber vermieden werden		

13.3 Glossar der Stakeholdergruppen

Anbieter von Datenanalysen und Künstlicher Intelligenz

Die Anbieter von Datenanalysen und Künstlicher Intelligenz generieren unter Anwendung statistischer Methoden und Verfahren des maschinellen Lernens wertvolle Informationen aus umfangreichen, schnelllebigen, verschiedenartigen bzw. komplexen (und ggf. fusionierten) Sensor(system)daten für spezifische Anwendungen in Unternehmen und Institutionen, welche es erlauben komplexe Entscheidungen zu automatisieren. Ihre Leistungen werden von unterschiedlichsten Anwendern von Sensorsystemen aber auch von deren Herstellern in Anspruch genommen.

Aufgabenträger/Verkehrsverbünde

Aufgabenträger sind für die Organisation und Finanzierung des öffentlichen Schienenpersonennahverkehrs (SPNV) gemäß Allgemeinem Eisenbahngesetz (AEG) und des öffentlichen Straßenpersonennahverkehrs (ÖSPV) gemäß Personenbeförderungsgesetz (PBefG) zuständig. Je nach Bundesland und differenziert nach SPNV und ÖSPV sind diese Funktionen unterschiedlichen Behörden und Organisationen auf Landes- oder kommunaler Ebene übertragen. In den meisten Fällen werden Verkehrsverbünde – als rechtlicher und organisatorischer Zusammenschluss von Gebietskörperschaften und/oder Verkehrsunternehmen – mit der Aufgabe einer abgestimmten Durchführung des Öffentlichen Personennahverkehrs (ÖPNV) betraut. Bestellerorganisationen der Aufgabenträger oder Verkehrsverbünde sind für die Ausschreibung oder Direktvergabe von Verkehrsleistungen an EVU und andere Verkehrsunternehmen zuständig und tragen so (neben erhobenen Fahrentgelten von den Fahrgästen) erheblich zur Finanzierung des ÖPNV bei.

Behörden

Relevante Behörden sind sämtliche für den Sensoreinsatz im Bahnwesen relevante öffentliche Stellen in diversen Themenbereichen wie Zulassung, Aufsicht, Unfalluntersuchung, Marktregulierung, Datenschutz und öffentliche Förderung von Innovationen.

Betreiber von Bahnstationen

Betreiber von Bahnstationen sind EIU bzw. Geschäftsfeldsparten von diesen, welche Verkehrsstationen (Personenbahnhöfe, Haltepunkte oder Güterbahnhöfe) entlang des Schienennetzes betreiben und instandhalten.

Betreiber von Güterverkehrs-Hubs

Güterverkehrs-Hubs sind Güterverkehrsstationen, die einen möglichst nahtlosen Umschlag von Ladeeinheiten (Container, Wechselbrücken oder Lkw-Sattelauflieger) oder kompletten Glieder- bzw. Sattelzügen zwischen der Straße (für kürzere Distanzen) sowie der Schiene und Wasserwegen (für längere Distanzen) im Kombinierten Verkehr (KV) ermöglichen. Die Betreiber sorgen für den reibungslosen Verladevorgang an KV-Terminals, welche sich in Güterverkehrszentren, See- oder Binnenhäfen befinden und sind auch für den Bau und die Instandhaltung der Verladeeinrichtungen zuständig.

Betreiber von Mobilitäts-Hubs

Mobilitäts-Hubs – auch bekannt unter den Begriffen Mobilitätsstationen oder Mobilitätspunkte – sind Personenverkehrsstationen, die eine möglichst nahtlose Verknüpfung von unterschiedlichen Verkehrsmitteln sowie ergänzenden Mobilitätsdienstleistungen und auf diese Weise multi- bzw. intermodale Verkehrsangebote (vor allem als nachhaltige Alternative zum privaten Pkw) ermöglichen. Sie können sich hinsichtlich Größe, Ausstattung und primärer Funktionserfüllung stark unterscheiden. Betreiber von Mobilitäts-Hubs sind dafür verantwortlich, die Infrastrukturen, technischen Anlagen und Schnittstellen in einem nutzbaren Zustand zu erhalten und können sich hierfür aus verschiedenen Finanzierungsquellen (öffentlich, Kofinanzierung durch Mobilitätsdienstleister) bedienen. Neben Hubs als physischen Zugangspunkten sind für die Nutzung multi- bzw. intermodaler Angebote auch digitale Zugänge und damit Kooperationen zu entsprechenden Anbietern erforderlich.

Einsatzorganisationen

Einsatzorganisationen nehmen mit den von ihnen vorgehaltenen Kräften und Mitteln im Rahmen der Vollziehung öffentlicher Aufgaben die Gefahrenabwehr und Schadensbekämpfung wahr (z. B. Polizei, Feuerwehr, Rettungsdienst, Katastrophenschutz). Sie können bei ihrem Einsatz gewollt oder ungewollt in Sensoren, Sensorsysteme oder in mit solchen generierten Daten einwirken.

Eisenbahninfrastrukturunternehmen (EIU)

Eisenbahninfrastrukturunternehmen sind bundeseigene oder nichtbundeseigene Unternehmen, die eine Eisenbahninfrastruktur (Schienenwege und Betriebsanlagen der Eisenbahnen einschließlich der Bahnstromfernleitungen, Unterwerke und Schaltwarten) betreiben, was auch den Bau und die Instandhaltung der Infrastrukturen umfasst. Unter dem Oberbegriff soll auch der Betrieb der Leit- und Sicherungstechnik sowie von Energieversorgungsanlagen nicht-elektrischer Bahnen (z. B. Dieseltankstellen) gezählt werden. Als gesonderte Stakeholdergruppe werden aufgrund der anderen Use Cases und (End-) Anwender sensorbasierter Lösungen im Rahmen dieser Studie die Betreiber von Bahnstationen betrachtet.

Eisenbahnverkehrsunternehmen (EVU)

Eisenbahnverkehrsunternehmen sind in öffentlichem, privatem oder gemischtwirtschaftlichem Eigentum stehende Unternehmen, die Personen- und/oder Güterverkehrsleistungen auf den Schienenwegen von Eisenbahninfrastrukturunternehmen erbringen. Sie müssen dafür bestimmte Zulassungskriterien (Zuverlässigkeit, Fachkunde, finanzielle Leistungsfähigkeit, Haftpflichtversicherung) erfüllen. Häufig sind sie zugleich die Halter der eingesetzten Schienenfahrzeuge.

Entity in Charge of Maintenance (ECM)

Die Entity in Charge of Maintenance (die für die Instandhaltung zuständige Stelle) bezeichnet die Rolle des Verantwortlichen gegenüber der pflichtgemäßen Instandhaltung von Eisenbahnfahrzeugen. Sie muss hierfür zertifiziert werden, wobei verschiedene Teilrollen (ECM 1 bis ECM 4: Managementfunktion, Instandhaltungsentwicklung, Fuhrparkmanagement, Instandhaltungsfunktion) unterschieden werden. ECM sind häufig EVU oder Fahrzeughalter bzw. -eigentümer, die diese Rolle selbst ausüben, aber auch freie Werkstätten, welche Instandhaltungsleistungen am Markt anbieten.

Fahrgäste

Fahrgäste sind alle Kundinnen und Kunden, die Personenverkehrsleistungen von EVU und weiteren Mobilitätsdienstleistern in Anspruch nehmen und dabei ggf. auch Mobilitäts-Hubs nutzen. Fahrgäste können hinsichtlich ihrer Mobilitätsbedarfe, -anforderungen und -einstellungen sehr heterogene Gruppen umfassen.

Forschungseinrichtungen

Forschungseinrichtungen generieren mit ihrer Grundlagen-, translationalen und angewandten Forschung im Bereich der Sensorik eine wichtige Basis für die Entwicklung und Verbesserung von Sensorkomponenten, Sensorsoftware, Sensoren und Sensorsystemen sowie darüber hinaus für deren Einsatz und Einbettung innerhalb des Gesamtsystems Bahn. Hierzu zählen öffentliche Einrichtungen wie Institute oder Fakultäten an Hochschulen, Einrichtungen der Fraunhofer-Gesellschaft, der Helmholtz-Gemeinschaft Deutscher Forschungszentren, der Leibniz-Gemeinschaft, die Institute der Max-Planck-Gesellschaft, die Ressortforschungseinrichtungen des Bundes (wie das DZSF), Institute in Trägerschaft der Länder und Gemeinden sowie von privaten Stiftungen, Vereinen und Unternehmen getragene Einrichtungen.

Gesellschaftliche Stakeholder

Gesellschaftliche Stakeholder sind indirekt auf die Gesetzgebung aber auch auf die Marktnachfrage Einfluss nehmende Interessengruppen und Nichtregierungsorganisationen wie Umweltverbände, Industrieverbände, Gewerkschaften und Verbraucherschutzorganisationen.

Gesetzgeber/Ministerien

Gesetzgeber und Ministerien sind die politischen Entscheidungsträger, welche über entsprechende Rechtsvorschriften sowie ihr Wirken über Behörden den Rahmen für den zulässigen Einsatz von Sensorik im Bahnwesen setzen.

Hersteller von Fertigungsanlagen

Hersteller von Fertigungsanlagen versorgen auf sämtlichen Ebenen die Hersteller von Sensoren, Schienenfahrzeugen, Schieneninfrastruktur, Bahnstationen und Hubs mit der jeweils benötigten Produktionstechnik (Energietechnik, Fertigungstechnik, Verfahrenstechnik).

IKT-Dienstleister

Dienstleister im Bereich der Informations- und Kommunikationstechnologien sind unabdingbar für die praktische Nutzung generierter Sensordaten für verschiedene Anwendungen und nehmen daher eine zentrale Schlüsselposition zwischen den Herstellern und Anwendern sensorbasierter Lösungen im Wertschöpfungsnetz ein. Das Leistungsspektrum von IKT-Dienstleistern ist grundsätzlich sehr breit. Am relevantesten für den Sensoreinsatz im Bahnwesen werden die folgenden vier Untergruppen angesehen: (1) die Anbieter bzw. Betreiber von IT-Infrastruktur wie z. B. Server- und Desktop-Systeme mit Rechen- und Speicherleistungen, Netzwerke, Cloud- und Edge-Dienste, (2) die Anbieter bzw. Betreiber von Kommunikationsinfrastruktur wie z. B. Glasfasernetze, öffentliche oder exklusive Mobilfunknetze, (3) die Bereitsteller von Betriebs- und Anwendungssoftware für diverse sensordatenbasierte Anwendungen sowie (4) Datendrehscheiben für das effiziente und automatisierte Teilen von Sensordaten oder daraus abgeleiteten veredelten Informationen (sowohl für den Passagier- als auch für den Güterverkehr) an diverse direkte und indirekte Anwender.

Infrastrukturhersteller

Infrastrukturhersteller sind Systemintegratoren komplexer Eisenbahninfrastrukturen (Schienenwege, Bahnstationen, Bahnenergieversorgung, Leit- und Sicherungstechnik). Sie erbringen ihre Leistungen für Eisenbahninfrastrukturunternehmen.

Infrastrukturinstandhaltungsdienstleister

Infrastrukturinstandhaltungsdienstleister sind Anbieter von Leistungen spezifischer Instandhaltungsarbeiten, denen sich die EIU (inkl. der Betreiber von Bahnstationen) zur Erfüllung ihrer Aufgabe bedienen können. Beispiele hierfür sind Spezialisten für Gebäudereinigung, die Wartung bahnbetrieblicher Kommunikationstechnik sowie für diverse Mess- und Prüfverfahren mit entsprechender Technik.

Komponentenhersteller Sensorik

Als Komponentenhersteller für Sensorik werden die Anbieter von elektrischen, elektromechanischen, mechanischen, optoelektronischen/-mechanischen oder elektrochemischen Bauelementen bzw. Baugruppen für Sensoren oder Sensorsysteme verstanden. Beispiele hierfür sind Rezeptoren, Transistoren, Leiterplatten, Mikrochips (SoC, ASIC etc.), Stecker, Schalter, Gehäuse, Akkumulatoren und sensorspezifische Bauteile (z. B. zur optischen Strahlenablenkung). Anbieter in diesem Sinne können eine unterschiedliche Wertschöpfungstiefe aufweisen. Sie können sich auf die Entwicklung oder die Fertigung und den Vertrieb der jeweiligen Komponenten konzentrieren oder diese Leistungen vertikal integriert erbringen. Neben den Herstellern existieren auch Distributoren, die sich auf den reinen Vertrieb konzentrieren.

Logistikkunden

Logistikkunden sind alle Kunden, die Güterverkehrsleistungen von EVU und weiteren Logistikdienstleistern in Anspruch nehmen und dabei ggf. auch Güterverkehrs-Hubs nutzen.

Modul-/Systemhersteller Infrastruktur

Modul-/Systemhersteller für Infrastruktur sind Integratoren wichtiger Subsysteme von Schieneninfrastruktur. Beispiele hierfür sind Eisenbahnunterbau und -oberbau, Signaltechnik, Stellwerke, Zugsicherung, und Betriebsleitzentralen. Sie erbringen ihre Leistungen entlang der Wertschöpfungskette für nachgelagerte Akteure der Infrastrukturherstellung und -instandhaltung.

Modul-/Systemhersteller Schienenfahrzeuge

Modul-/Systemhersteller für Schienenfahrzeuge sind Integratoren wichtiger Subsysteme von Schienenfahrzeugen. Beispiele hierfür sind Bahnmotoren und -generatoren, Leistungselektronikmodule, Bremssysteme und Klimaanlagen.

Prüfer/Zertifizierer

Prüfer/Zertifizierer sind unparteiische Dritte, die durch ihre Prüfmaßnahmen aufzeigen und bestätigen, dass (mit einem angemessenen Vertrauen) die Konformität eines Produktes, eines Systems, eines Prozesses oder einer Institution mit in einer bestimmten Norm definierten und einzuhaltenden Anforderungen besteht. Hierzu gehören entsprechende Zertifizierungsstellen bzw. ihre Auditoren. Dies betrifft die Produktzertifizierung von Sensorik, Schienenfahrzeugen und Schieneninfrastruktur auf Komponenten-, Modul- und Systemebene aber auch die Zertifizierung der Rollen als ECM oder anerkannter Bahnlieferant.

Rohstoff-/Materiallieferanten

Rohstoff-/Materiallieferanten versorgen auf sämtlichen Ebenen der Herstellung von Sensoren, Schienenfahrzeugen, Schieneninfrastruktur, Bahnstationen und Hubs sowie bei allen zugehörigen Instandhaltungsprozessen die jeweils zuständigen Stakeholder mit den benötigten Grund- und Werkstoffen. Dies sind hauptsächlich die jeweiligen Teile-/Komponentenhersteller.

Schienenfahrzeug-Hersteller

Schienenfahrzeughersteller sind Systemintegratoren vollständiger Schienenfahrzeuge. Durch starke Konzentrationsprozesse wird der weltweite Neufahrzeugmarkt von wenigen Herstellern dominiert (z. B. in Europa: Alstom, Siemens und Stadler).

Schienenfahrzeug-Halter

Schienenfahrzeughalter sind Eigentümer oder sonst Verfügungsberechtigte von Eisenbahnfahrzeugen, welche – in der Regel wirtschaftlichen Absichten dienend – zu Beförderungszwecken eingesetzt werden. Sie tragen die Instandhaltungsverantwortung und die ggf. bestehende Versicherungspflicht. Sie müssen jedem ihrer Fahrzeuge eine für die Instandhaltung zuständige Stelle (ECM) zuweisen (sich selbst oder Dritte) und werden im Fahrzeugeinstellungsregister eingetragen. Eine Vermietung beseitigt die Haltereigenschaft nicht.

Schienenfahrzeug-Instandhaltungsdienstleister

Instandhaltungsdienstleister für Schienenfahrzeuge sind Anbieter von Leistungen spezifischer Instandhaltungsarbeiten, denen sich die ECM zur Erfüllung ihrer Aufgabe als für die Instandhaltung zuständige Stelle bedienen können. Beispiele hierfür sind Spezialisten für Graffitientfernung, Industrielackierungen, Folierung, Bodensanierung, Scheibenversiegelung und Polsterreinigung.

Sensorhersteller

Unter Sensorherstellern sollen die Anbieter von einzelnen, auf einem (oder wenigen) spezifischen Wirkprinzip(ien) beruhenden und damit eine bestimmte Eigenschaft oder die stoffliche Beschaffenheit der Umgebung qualitativ oder quantitativ erfassenden Messgrößenaufnehmern verstanden werden. Beispiele hierfür sind spezielle Druck-, Kamera-, Lidar-, Radar-, Ultraschall- oder Infrarotsensoren. Anbieter in diesem Sinne können eine unterschiedliche Wertschöpfungstiefe aufweisen. Sie können sich auf die Entwicklung oder die Fertigung und den Vertrieb der jeweiligen Sensortypen konzentrieren oder diese Leistungen vertikal integriert erbringen. Neben den Herstellern existieren auch Distributoren, die sich auf den reinen Vertrieb konzentrieren.

Sensorsystemhersteller

Unter Sensorsystemherstellern sollen die Anbieter komplexer Sensorprodukte für einen übergeordneten Anwendungsfall (Use Case; z. B. Automatic Train Operation oder Digitale Automatische Kupplung) verstanden werden, bei welchen eine Vielzahl von Sensoren (und meist verschiedene Sensortypen), Kommunikationsmodule sowie Auswerteelektronik und -software in einem hierarchisch strukturierten technischen Gesamtsystem zusammenwirken. Die Tätigkeit von Sensorsystemherstellern umfasst typischerweise die Systemintegration, inklusive der Sensorcharakterisierung, -validierung und -adaption, aber auch vor- und nachgelagerte Funktionen wie den Systementwurf sowie Wartung und Support.

Softwarehersteller Sensor und Sensorsystem

Als Softwarehersteller für Sensorik werden alle Entwickler der in Sensoren und Sensorsystemen zum Einsatz kommenden Programme verstanden. Das reicht von Firmware und Embedded Software für bestimmte Hardwarekomponenten und Sensoren über Betriebssysteme bis hin zu Programmen für die Sensordatenfusion, für Safety und Cybersecurity in komplexen Sensorsystemen. Neben den Herstellern existieren auch Softwaredistributoren, die sich auf den reinen Vertrieb konzentrieren.

Sonstige

Unter die Gruppe der Sonstigen sollen im Rahmen dieser Studie alle weiteren, gewollt oder ungewollt in Kontakt mit Sensoren und Sensorsystemen oder mit Sensordaten kommenden Akteurinnnen und Akteure verstanden werden. Dabei kann es sich beispielsweise um unbeteiligte Dritte handeln, deren Spuren von der Sensorik miterfasst werden oder um absichtlich störend oder manipulierend Eingreifende.

Teile-/Komponentenhersteller Infrastruktur

Teile-/Komponentenhersteller für Infrastruktur sind Fertiger bzw. Zulieferer sämtlicher Bauteile und Baugruppen, die in Schieneninfrastrukturen verbaut werden. Beispiele hierfür sind Weichen, Schienen, Schwellen, Befestigungsmittel, Fahrleitungsmaste, Gleisschaltmittel und Stellwerksmonitore. Sie erbringen ihre Leistungen entlang der Wertschöpfungskette für nachgelagerte Akteure der Infrastrukturherstellung und -instandhaltung.

Teile-/Komponentenhersteller Schienenfahrzeuge

Teile-/Komponentenhersteller für Schienenfahrzeuge sind Fertiger bzw. Zulieferer sämtlicher Bauteile und Baugruppen, die in Schienenfahrzeugen verbaut werden. Je größer Teile-/Komponentenhersteller sind, umso geringer sind meist ihre bahntechnikspezifischen Umsatzanteile und damit ihre Abhängigkeiten von der Schienenfahrzeugindustrie.

Weitere Logistikdienstleister

Bei weiteren Logistikdienstleistern handelt es sich um die Erbringer von Gütertransport- und Güterumschlagsleistungen sowie fertigungsnahen Dienstleistungen (Lagerung, Kommissionierung, Assemblierung, Fakturierung), die nicht durch das EVU erfolgen, sondern im Kombinierten Verkehr auftreten. Beispiele sind Speditionen, Reedereien, Anbieter von Kurier-, Express- und Paketdiensten sowie Systemintegratoren und Optimierer komplexer Logistikketten mit Waren- und Informationsströmen.

Weitere Mobilitätsdienstleister

Bei weiteren Mobilitätsdienstleistern handelt es sich um die Erbringer von direkten und unterstützenden bzw. ergänzenden Mobilitätsleistungen für den Personenverkehr, die nicht durch das EVU erfolgen, sondern im multi- bzw. intermodalen Verkehr auftreten. Hierzu zählen die Erbringer von Personenbeförderungsleistungen (wie Verkehrsbetriebe, Taxi- und Ridepooling-Unternehmen), die Bereitsteller von Fahrzeugen (wie Bike-, E-Scooter- und Carsharer), Anbieter ergänzender Leistungen (wie Pannenhilfe, die Be-

reitstellung von WLAN-Hotspots, Paketautomaten oder von Möglichkeiten zum Parken und Stromtanken), aber auch Vermittler bzw. Integratoren, welche dafür sorgen, dass nahtlose Serviceketten vom Informieren, Planen und Buchen bis hin zum Bezahlen und Begleiten während einer Reise möglich werden.

13.4 Risikoanalyse IT-Security

TABELLE 111: WAHRSCHEINLICHKEITSNIVEAUS DER ANGRIFFSVEKTOREN

Nr.	Zeit	Expertise	Wissen	Zugriff	Ausstattung	*AP Summe*	*Wahrscheinlichkeits-niveau*	*Wahrscheinlichkeits-leitwort*
V.1							4	Wahrscheinlich
V.1.1	3	6	3	4	4	20	2	Unwahrscheinlich
V.1.2	3	6	3	4	4	20	2	Unwahrscheinlich
V.1.3	1	3	3	4	0	11	4	Wahrscheinlich
V.1.4	3	6	3	4	7	23	2	Unwahrscheinlich
V.2							1	Unvorstellbar
V.2.1	3	6	7	4	7	27	1	Unvorstellbar
V.2.2	3	6	7	4	7	27	1	Unvorstellbar
V.2.3	7	6	7	4	7	31	1	Unvorstellbar
V.3							4	Wahrscheinlich
V.3.1	3	6	3	4	4	20	2	Unwahrscheinlich
V.3.2	1	3	3	1	4	12	4	Wahrscheinlich
V.4							4	Wahrscheinlich
V.4.1	7	8	7	4	7	33	1	Unvorstellbar
V.4.2	3	3	3	1	4	14	3	Möglich
V.4.3							4	Wahrscheinlich
V.4.3.1	1	3	3	4	0	11	4	Wahrscheinlich
V.4.3.2	1	3	3	4	0	11	4	Wahrscheinlich
V.4.3.3	1	3	3	4	4	15	3	Möglich
V.4.3.4	1	3	3	4	4	15	3	Möglich
V.4.3.5	1	3	3	1	4	12	4	Wahrscheinlich
V.4.3.6	1	3	3	1	4	12	4	Wahrscheinlich
V.4.3.7	7	8	7	1	9	32	1	Unvorstellbar
V.5							5	Sehr wahrscheinlich
V.5.1	0	0	3	1	4	8	5	Sehr wahrscheinlich
V.5.2	1	3	3	4	4	15	3	Möglich
V.5.3	0	0	3	1	0	4	5	Sehr wahrscheinlich
V.6							2	Unwahrscheinlich
V.6.1	7	6	11	0	0	24	2	Unwahrscheinlich
V.6.2	7	6	7	4	7	31	1	Unvorstellbar
V.6.3	3	6	3	4	7	23	2	Unwahrscheinlich
V.6.4							2	Unwahrscheinlich
V.6.4.1	7	6	7	1	4	25	1	Unvorstellbar
V.6.4.2	3	6	7	1	4	21	2	Unwahrscheinlich
V.6.5	7	8	7	4	7	33	1	Unvorstellbar
V.7	3	6	3	4	4	20	2	Unwahrscheinlich
V.8							4	Wahrscheinlich
V.8.1	1	0	7	4	0	12	4	Wahrscheinlich
V.8.2	1	3	3	4	0	11	4	Wahrscheinlich
V.8.3	3	3	3	4	4	17	3	Möglich

Nr.	Zeit	Expertise	Wissen	Zugriff	Ausstattung	*AP Summe*	*Wahrscheinlichkeits-niveau*	*Wahrscheinlichkeits-leitwort*
V.8.4							4	Wahrscheinlich
V.8.4.1	1	6	3	0	0	10	4	Wahrscheinlich
V.8.4.2	1	6	3	0	0	10	4	Wahrscheinlich
V.8.4.3	7	6	7	0	0	20	2	Unwahrscheinlich
V.8.4.4	7	6	7	0	0	20	2	Unwahrscheinlich
V.9							2	Unwahrscheinlich
V.9.1	7	6	7	1	0	21	2	Unwahrscheinlich
V.9.2	7	6	7	1	7	28	1	Unvorstellbar
V.9.3	7	6	3	1	7	24	2	Unwahrscheinlich
V.9.4	7	6	3	1	7	24	2	Unwahrscheinlich
V.9.5	7	8	7	4	9	35	1	Unvorstellbar

TABELLE 112: ANGRIFFSPOTENTIALE (AP) UND WAHRSCHEINLICHKEITSNIVEAUS (NACH [318])

AP Wertebereich	AP Niveau (Aufwand)	Wahrscheinlichkeitsniveau
0 – 9	Sehr gering	Sehr wahrscheinlich
10 – 13	Gering	Wahrscheinlich
14 – 19	Moderat	Möglich
20 – 24	Hoch	Unwahrscheinlich
>24	Sehr hoch	Unvorstellbar

TABELLE 113: BEWERTUNGSSCHEMA ANGRIFFSPOTENTIALE (NACH [318])

AP Faktor	Umfang	Beschreibung	Wert
Benötigte Zeit	Stunden	Benötigte Zeit für Vorbereitung und Durchführung des Angriffs	0
	Tage		1
	Wochen		3
	Monate		7
Expertise	Laie	Ist im Vergleich zu Expertinnen und Experten eine unwissende Person Person; ohne besondere Fachkenntnisse	0
	Kompetent	Ist eine kompetente Person, die sich mit dem Sicherheitsverhalten des Produkts/Systemtyps auskennt	3
	Expertin oder Experte	Ist eine Person, die sich mit zugrundeliegenden Algorithmen, Protokollen, Hardware, Strukturen, Sicherheitsverhalten, Prinzipien und Konzepten der eingesetzten Sicherheit, Techniken und Werkzeugen zur Erstellung neuer Angriffe, Kryptografie, Klassischen Angriffen des Produkttyps, Angriffsmethoden usw. hinsichtlich des jeweiligen Produkts/Systemtyps auskennt	6
	Mehrere Expertinnen oder Experten	Mehrere Expertinnen oder Experten aus unterschiedlichen Fachbereichen sind notwendig	8
Wissen über das Ziel	Öffentlich	Informationen bezüglich des Ziels sind öffentlich verfügbar (ohne Verschwiegenheitserklärungen).	0

AP Faktor	Umfang	Beschreibung	Wert
	Eingeschränkt	Informationen werden zwischen verschiedenen Organisationen geteilt (unter Verschwiegenheitserklärung)	3
	Sensitiv	Informationen werden nur innerhalb einer Organisation geteilt (unter Verschwiegenheitserklärung)	7
	Kritisch	Informationen sind nur für einige wenige Personen innerhalb einer Organisation verfügbar; der Zugriff wird stark kontrolliert (z. B. Geheimer Signaturschlüssel)	11
Zugriff	Nicht notwendig/unbegrenzt	Kein physischer Zugriff notwendig, z. B. Remote oder drahtlos, kein Risiko / sehr geringes Risiko dass Angriffsversuch erkannt wird	0
	Einfach	Physischer Zugriff notwendig (innen oder außen), keine spezialisierten Werkzeuge notwendig (handelsübliche Werkzeuge, wie Schraubendreher sind noch abgedeckt)	1
	Moderat	Physischer Zugriff weiterhin notwendig, mehrere Demontageschritte notwendig oder spezialisiertes Werkzeug, Zeitaufwand i. d. R. höher	4
	Schwierig	Umgehung von Manipulationsschutz etc. (z. B. alarmgesichert) oder Umgehung von komplexeren Sicherheitsmaßnahmen	10
Ausstattung	Standard	Alltagswerkzeuge, die im üblichen Handel beschafft werden können	0
	Spezialisiert	Spezialisierte Werkzeuge, im Fachhandel zu erwerben	4
	Maßgeschneidert	Für den Angriff speziell konzipierte Werkzeuge, oder nur von Bahn-spezialisierten Herstellern zu erwerben, oder sehr teuer (> 50.000€)	7
	Mehrere Maßgeschneiderte	Mehrere maßgeschneiderte Werkzeuge müssen kombiniert werden, um mehrere Schritte des Angriffs durchzuführen	9

TABELLE 114: BEWERTUNGSSCHEMA SCHADENSAUSMAß (NACH [318])

Schadensbereich	Konsequenzen	Wert
Safety	Lebensbedrohliche Verletzungen (Überleben ungewiss), tötliche Verletzungen und/oder extremer Schaden an der Umgebung	10000
	Schwere und lebensbedrohliche Verletzungen (Überleben wahscheinlich) und/oder großer Schaden an der Umgebung	1000
	Leichte und moderate Verletzungen und/oder geringer Schaden an der Umgebung	100
	Keine Verletzungen	0
Finanziell	Existenzgefährdender finanzieller Schaden und/oder das Ereignis führt zu Personen, die	1000

	die Firma verklagen; Schwerer Schaden am öffentlichen Ansehen	
	Substantieller finanzieller Schaden, der noch nicht Existenz gefährdend ist; Gravierender Schaden am öffentlichen Ansehen	100
	Unerwünschter finanzieller Schaden und/oder Schaden am öffentlichen Ansehen	10
	Kein oder tolerierbarer finanzieller Schaden	0
Operativ	Zug unbenutzbar, d. h. eine oder mehrere grundlegende Funktionen sind betroffen.	100
	Wartung ist erforderlich, d. h. eine wichtige Funktion ist betroffen. Das Fahrzeug kann nur mit massiven Einschränkungen eingesetzt werden	10
	Komfort ist betroffen. Das Fahrzeug kann mit einigen Einschränkungen eingesetzt werden.	1
	Keine relevanten Effekte, d. h. es ist höchstens eine unwichtige Funktion betroffen und das Fahrzeug kann ohne Einschränkungen genutzt werden.	0

TABELLE 115: ÜBERGEORDNETE ANGRIFFSZIELE (TÜR)

Nr.	Angriffsziel
Z.1	Verhinderung der Türöffnung
Z.2	Tür als geschlossen ausgeben, obwohl offen
Z.3	Türen schließen lassen, während Person in der Tür ist
Z.4	Verhinderung der Weiterfahrt des Zugs im Bahnhof
Z.5	Verhinderung der Weiterfahrt des Zugs auf der Strecke

TABELLE 116: EINTRITTSWAHRSCHEINLICHKEITEN DER ANGRIFFZIELE (TÜR)

Nr. (Z)	Wahrscheinlichkeitsniveau
Z.1	4
Z.2	5
Z.3	5
Z.4	5
Z.5	5

TABELLE 117: SCHADENSAUSMAß DER ANGRIFFSZIELE (TÜR)

Nr. (Z)	Safety	Finanziell	Operativ	*Schadenswert*	*Schadensniveau*	*Schadensausmaß Leitwort*
Z.1	100	10	10	120	3	Kritisch
Z.2	10000	100	100	10200	4	Katastrophal
Z.3	100	10	10	120	3	Kritisch
Z.4	0	100	10	110	3	Kritisch
Z.5	1000	100	10	1110	4	Katastrophal

TABELLE 118: RISIKO DER ANGRIFFSZIELE (TÜR)

Nr. (Z)	*Wahrscheinlichkeit*	*Schadenausmaß*	*Risiko*
Z.1	4	3	Hoch
Z.2	5	4	Extrem
Z.3	5	3	Extrem
Z.4	5	3	Extrem
Z.5	5	4	Extrem

TABELLE 119: RISIKOMATRIX (NACH [318])

Schadensausmaß → Wahrscheinlichkeit ↓	1	2	3	4
1	Niedrig	Niedrig	Niedrig	Moderat
2	Niedrig	Moderat	Moderat	Hoch
3	Niedrig	Moderat	Hoch	Hoch
4	Moderat	Hoch	Hoch	Extrem
5	Moderat	Hoch	Extrem	Extrem

TABELLE 120: MAßNAHMEN IT-SICHERHEIT

Num-mer	Gegenmaßnahme
M.1	Physischer Schutz
M.1.1	Physischen Zugriff verhindern
M.1.2	Schutz vor äußeren Störeinflüssen
M.1.3	Einsatz mehrerer Messprinzipien
M.1.4	Manipulationserkennung durch Selbsttests
M.1.5	Störungserkennung durch Selbsttests
M.1.6	Backup-Stromversorgung
M.2	Kommunikations-Integrität/-Authentizität
M.2.1	Sicherung des Netzwerkzugriffs und Teilnehmer-Authentizität PNAC (IEEE 802.1X-2010)+MACsec (IEEE 802.1AE)
M.2.2	Sicherung der Protokoll-Integrität und Teilnehmer-Authentizität mittels TLS
M.2.3	Protokollierung, Verwerfen und Alarmierung von Auffälligkeiten in Protokoll-Nachrichten (z. B. falscher Absender)
M.3	Geräte-Sicherheit (Software)
M.3.1	Sicheres Software Update (TUF)
M.3.2	Konfiguration über sichere Updates (TUF)
M.3.3	Geräte-Sicherheit: Signierte Firmware & Integritätschecks (Trusted Boot)
M.3.4	Geräte-Sicherheit: Kryptografisches Material in TPM
M.3.5	Geräte-Sicherheit: Sichere Entsorgung/Löschung/Priviliegien-Entzug
M.4	Gegenmaßnahmen Sicherheitslücken
M.4.1	Überwachung von CVEs in Software und Abhängigkeiten & Zeitnahe Aktualisierung
M.4.2	Regelmäßige Penetrationstests
M.4.3	Konzepte validieren lassen (Open Source, Bug Bounty Programme)
M.4.4	Softwarequalitätsmaßnahmen
M.4.5	Secure Coding & Best Practices
M.4.6	Security by Design Prozess & Prinzipien
M.4.7	Logging & Überwachung
M.4.8	Sandboxing & Least Privilege
M.4.9	Zero Trust
M.4.10	Fuzzing von Programmen um Abstürze/Programmierfehler zu identifizieren
M.4.11	Speichersicherheit durch System (ASLR, DEP/NX)
M.4.12	Speichersicherheit durch Compiler (Stack Canary, Control Flow Integrity)
M.4.13	Speichersicherheit durch Programmiersprache (z. B. Rust)
M.5	Gegenmaßnahmen DoS
M.5.1	Prüfung von Protokollen auf DoS
M.5.2	Anfordern von (gerätegebundenem) Proof of Work (PoW) um Überlastung zu verhindern
M.5.3	Prüfen der Protokolle/Parser auf Komplexität, ggf. Überlastung einschränken durch PoW o.ä.
M.6	Maßnahmen Netzwerksicherheit
M.6.1	Firewalls
M.6.2	IDS/IPS
M.6.3	WAF
M.6.4	SIEM
M.6.5	Erkennung und Verhinderung von Spoofing
M.7	Gegenmaßnahmen KI-Angriffe
M.7.1	Konsistenzprüfung
M.7.1.1	Gegenprüfung mittels anderer Sensoren (andere Orte bzw. andere Sensor-Typen)

Num-mer	Gegenmaßnahme
M.7.1.2	Sensor Fusion
M.7.1.3	Prüfung physikalisch invarianter Eigenschaften
M.7.2	Verbesserung der Robustheit gegenüber Angriffen
M.7.2.1	Adversarial Training
M.7.2.2	Vorhersage und/oder Entfernen von Manipulationen (z. B. Median Filter)
M.8	Gegenmaßnahmen Komplexe Sensoren
M.8.1	Gegenmaßnahmen Sensor-Fusion-Angriffe
M.8.1.1	Verbesserung der Filter-Konfidenz bzw. Sensor-Genauigkeit
M.8.1.2	Gegenmaßnahmen gegen Spoofing einzelner Sensoren
M.8.1.3	Nutzung weiterer Datenquellen
M.8.2	Gegenmaßnahmen GPS Spoofing
M.8.2.1	Überwachung der Signalstärke
M.8.2.2	Erkennung der Signalrichtung mittels mehrerer Antennen
M.8.2.3	Kryptografische Authentifizierung der GPS-Daten
M.8.3	Gegenmaßnahmen LiDAR Spoofing
M.8.3.1	Maßnahmen auf System-Ebene
M.8.3.1.1	Herausfiltern von Reflexionen in der Vorverarbeitung
M.8.3.1.2	Reduzieren von Informationsverlust in der Verarbeitung
M.8.3.1.3	CARLO (Occlusion-Aware Hierarchy Anomaly Detection) (nachgelagerte Validierung)
M.8.3.1.4	Sequential View Fusion (SVF) (Anpassung des Modells erfoderlich)
M.8.3.2	Maßnahmen auf Sensor-Ebene
M.8.3.2.1	Erkennung – Sensor-Fusion oder Nutzung alternativer/zusätzlicher Sensoren
M.8.3.2.2	Erkennung – Sättigung des Sensors erkennen
M.8.3.2.3	Mitigation – Empfangswinkel reduzieren
M.8.3.2.4	Mitigation – Unerwünschte Lichtspektren herausfiltern
M.8.3.2.5	Mitigation – Gegenmaßnahmen bzgl. Effekte aufgrund von gebogenem Glas
M.8.3.2.6	Randomisierung – Zufälliges Gruppieren von Laser-Impulsen/ Zufällige Wellenformen
M.8.3.2.7	Randomisierung – Ping in zufällige Richtungen
M.8.3.2.8	Randomisierung – Zufälliges Ausschalten des Transmitters zur Erkennung unerwarteter Eingangssignale

TABELLE 121: ZUORDNUNG ANGRIFFSVEKTOREN ZU GEGENMAßNAHMEN

Angriffsvektorgruppe	Gegenmaßnahmen
V.1	M.1.1; M.1.2; M.1.3; M.1.5; M.1.6
V.2	M.2.1; M.2.2; M.2.3; M.3
V.3	M.1.1; M.1.2; M.1.4
V.4	M.1.1; M1.2; M.1.3; M.1.4; M.8
V.5	M.1.1; M.1.2; M.1.3; M.1.5; M.8.3.2.2
V.6	M.3; M.4
V.7	M.1.1; M.2; M.3.4; M.3.5
V.8	M.1.1; M.1.6; M.1.5; M.4; M.5; M.6
V.9	M.7; M.8.1