M2C Expert Control
im Auftrag der SBB AG

M2C ExpertControl GmbH
Buchberger Str. 40
94560 Offenberg, Germany
T +49–9905-8161
F +49–9905-707763
info@m2cec.com
www.m2cec.com

Machbarkeitsstudie für eine genaue, sichere Lokalisierung (Auszug)

Einleitung

Eine Studie zur Machbarkeit einer genauen, sicheren Lokalisierung mittels mobiler Sensoren in der Eisenbahntechnik wurde von der SBB im Sommer 2017 im Rahmen des Programms smartrail 4.0 an M2C Expert Control beauftragt. Die wesentlichen Arbeiten fanden zwischen Sommer 2017 und Januar 2018 statt. Im Folgenden wird ein Auszug der Studie wiedergegeben. Er reflektiert mit wenigen Ausnahmen den Stand von Januar 2018. So beziehen sich zum Beispiel Referenzen zur Gesamtarchitektur von smartrail 4.0 in Kapitel 4 auf den damaligen Konzeptstand, der inzwischen angepasst wurde. In Kapitel 1 bis 5 hat die SBB ausgewählte Kürzungen vorgenommen und in Einzelfällen auch textliche Anpassungen vorgenommen, wo es die Kürzungen erforderten. In Kapitel 6 wurden neben Kürzungen auch einzelne Ergänzungen eingefügt, basierend auf den Erkenntnissen, die zwischen Februar und Oktober 2018 gewonnen wurden.

Inhaltsverzeichnis

1. Ziele der Machbarkeitsstudie

Lokalisierung ist im Bereich der Eisenbahntechnik eine zentrale Aufgabe und Schlüsselfunktion. Während gegenwärtig die Lokalisierung weitgehend infrastrukturseitig und damit nur punktuell gelöst wird, ist das Ziel der SBB Strategie Smart Rail 4.0, für einen nächsten Schritt in der Bahnautomatisierung, alles auf dem Gleis in Echtzeit „elektronisch“ sichtbar und steuerbar zu machen, jede Bewegung und Belegung zu beobachten und abzusichern sowie den „Faktor Mensch“ in den sicheren Prozessen zu reduzieren. Damit soll ein erheblicher Fortschritt an Qualität und Wirtschaftlichkeit in Schienenverkehr erzielt werden.

Die Ausgangslage und Zielsetzungen werden in diesem Kapitel weiter detailliert.

1.1 Definition der Lokalisierung

Die Aufgabe der Lokalisierung im Eisenbahnwesen - oder auch konventionell als Ortung bezeichnet - ist für die sichere Betriebsführung im Schienenverkehr von größter Bedeutung. Flankenschutz, Folgefahrschutz und Gegenfahrschutz werden durch die Kenntnis der Fahrzeugposition ermöglicht, Schutz vor Entgleisungen durch Überwachung der Geschwindigkeit [1]. Ortung wird nach [2] hier folgendermaßen definiert:

„Ortung ist die Bestimmung des Bewegungszustands eines bestimmten Verkehrsmittels (d.h. Position, Geschwindigkeit nach Betrag und Richtung bezogen auf einen Bezugspunkt des Verkehrsmittels) in einem Bezugssystem.“

Für die Erreichung der Ziele einer weiteren Bahnautomatisierung ist daher die Definition von Anforderungen an die Lokalisierungsaufgabe Voraussetzung. Diese wird in Form von Use Cases beschrieben. Aus diesen können einerseits die Anforderungen hinsichtlich des detektierten Lokalisierungszustandes eines Objekts im Bahnbereich, insbesondere bezüglich der Lokalisierungsgenauigkeit, und andererseits die Anforderungen hinsichtlich der Lokalisierungsfunktion, insbesondere bezüglich der Sicherheitsverantwortung und Verlässlichkeit hergeleitet werden.

Die Leistungen der dafür möglichen relevanten Sensoren wurden mit ihren charakteristischen Eigenschaften separat zusammengestellt. Dieses Gliederungsschema beruht auf einer Differenzierung der Lokalisierungseigenschaften in Umfang und Tiefe bis zu quantifizierbaren Werten und Einheiten. Ebenfalls werden die aus den Use Cases hergeleiteten Basisanforderungen nach einem ähnlichen Gliederungsschema im Kapitel 3 Use Case ausführlich hergeleitet, vertieft, verifiziert und weiter detailliert.

1.2 Ausgangslage (Ist-Zustand)

Derzeitige technische Lösungen zur Lokalisierung, insbesondere zur Ortung von Lokomotiven und Zugverbänden, nutzen Einrichtungen auf Fahrzeugen und im Gleis. Heute wird die Lokalisierung im Regelfall mit Gleisfreimeldung durch im Gleis montierte Achszähler, Gleisstromkreise oder Linienleiter realisiert. Diese Einrichtungen garantieren auch die gleisselektive Zugvollständigkeitsprüfung. Bei der Migration zu ETCS werden in größerem Umfang Balisen im Gleis verlegt. Durch die fahrzeugseitige Erfassung von im Gleis verlegten Einrichtungen wie Linienleitern oder Balisen wird auch punktuell die absolute Zugposition bestimmt, die durch fahrzeugseitige Odometrie wie Radimpulsgeber oder Radar zur kontinuierlichen Ermittlung der Zugposition im Gleis ergänzt wird.

Weiterhin kommen zur Lokalisierung und Information Lokalisierungstafeln hinzu, die auch die Lokalisierung für den Störungsfall oder bei Instandhaltungsarbeiten sicherstellen. Einrichtungen, z.B. zur Einrichtung von Baustellen und zur Warnung insbesondere der Rotten nutzen zur Lokalisierung spezielle optische oder akustische Signale.

Die Nachteile dieser Einrichtungen sind die hohen Kosten dieser Außenanlagen bei Errichtung und Instandhaltung, hohe Reserven in der Belegung, suboptimale Nutzung der Trassenkapazität und, da nicht alles im Gleisbereich lokalisierbar ist, auch Prozesslücken (Beispiel Rangieren, Bauen).

Auch muss im Zuge der Ausrüstung mit ETCS hinterfragt werden, ob sich der Aufwand für eine netzweite Installation mit ca. 10 Balisen je km und deren Instandhaltung lohnt. Abbildung 1.1 zeigt die Chance für eine Substitution der heutigen und zukünftigen Lokalisierung durch Balisen für die Zugsicherung.

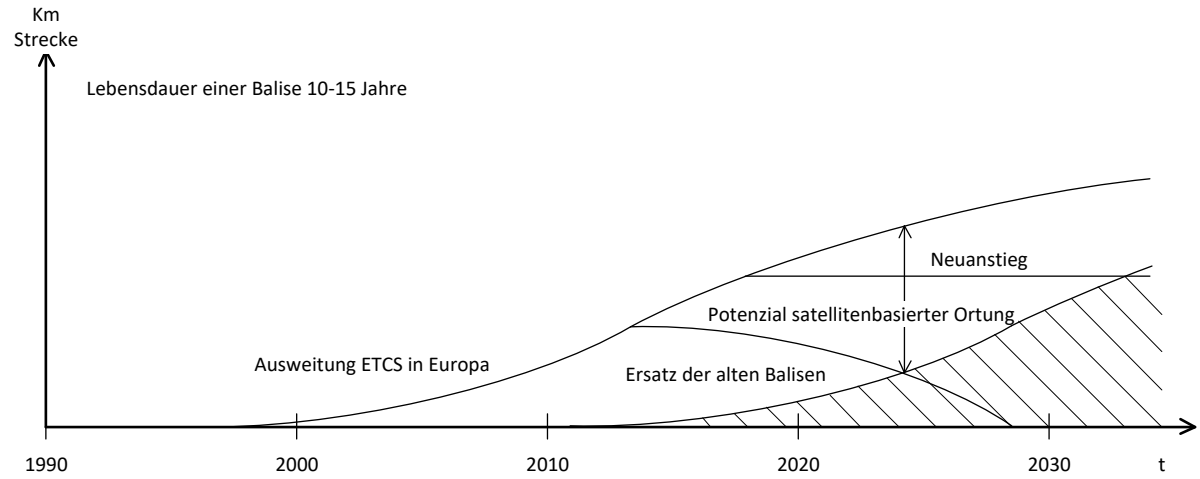


Abbildung 1.1: Potenzial für eine Substitution der heutigen und zukünftigen Lokalisierung durch Balisen für die Zugsicherung

Insgesamt wird festgestellt, dass sowohl in einem Schienenverkehrsnetz diverse technische Einrichtungen auf den (bewegten) Objekten und in der Infrastruktur zur Lokalisierung vorhanden sind. Nachteilig ist deren große technische Heterogenität und ihre mobile und stre-

ckenseitige Verteilung sowie kommunikationstechnische und organisatorische Einbindung in das Betriebssystem. Beide Eigenschaften binden erhebliche Investitionen und erfordern erhebliche Aufwendungen im Betrieb und Einschränkungen in ihrer Unterhaltung.

Speziell streckenseitige Einrichtungen müssen intensiv gewartet sowie instandgehalten werden und sind Witterung und Vandalismus ausgesetzt. Zudem bieten diese teilweise eine diskrete Ortung, was den derzeitigen Betriebsablauf des Fahrens im Blockabstand bedingt. Mit einer kontinuierlichen Ortung wäre das Fahren im absoluten Bremswegabstand durch das Einrichten des sogenannten „Moving Blocks“ und somit eine effizientere Abwicklung des Schienenverkehrs möglich. Zudem kann das interoperable Zugsicherungssystem ETCS mit der in dieser Machbarkeitsstudie untersuchten Lokalisierung mittels einer satellitenbasierten Ortung durch den Verzicht auf streckenseitige Einrichtungen mit einer kosteneffizienten Lösung unterstützt werden.

In dem Zusammenhang mit der Darstellung des Stands der technischen Sensorik wird auch eine erste Klassifizierung ihrer betrieblichen Nutzung getroffen und tabellarisch beschrieben. Diese wird im Kapitel 3 Use Cases wieder aufgegriffen und dort vertieft.

1.3 Zielsituation (Soll-Zustand)

In diesem Abschnitt werden zum einen kurz die Ziele

- der SBB als integrierte Betreiber des Eisenbahnsystems,
- die Ziele des Projektes „Genaue sichere Lokalisierung“,
- der Phase 0, d.h. der Machbarkeitsstudie

ausformuliert, gegliedert und ggf. priorisiert, zum anderen werden die Anforderungen an die Machbarkeit dargestellt.

1.3.1 Ziele der SBB als integrierte Betreiber des Eisenbahnsystems

Im Rahmen des Zukunftsprojektes SmartRail 4.0 der SBB mit einer revolutionären Neugestaltung der Eisenbahnleit- und Sicherungstechnik der SBB, wobei alle Kernprozesse der Bahnproduktion und Anlagenbereitstellung massiv automatisiert werden sollen, sind notwendige Voraussetzungen, Züge immer sicher in Echtzeit lokalisieren und immer steuern zu können und dafür über sichere mobile Endgeräte mit sicheren mobilen Lokalisierungssystemen zu verfügen, welche in den Aufgabengebieten ETCS L3, Flächenprozessen der Instandhaltung und Rangieren eingesetzt werden.

Für diesen nächsten Schritt in der Bahnautomatisierung wird damit eine genaue und sichere Lokalisierung essentiell sein, um alle Objekte auf dem Gleis in Echtzeit „elektronisch“ sichtbar und steuerbar zu machen, jede Bewegung und Belegung zu beobachten und abzusichern sowie den „Faktor Mensch“ in den sicheren Prozessen zu reduzieren. In einer Vielzahl von Anwendungen werden sich grosse Chancen zur Effizienz- und Sicherheitssteigerung eröffnen.

Aus einer kontinuierlichen genauen, sicheren Lokalisierung aller Objekte ergeben sich die folgenden Chancen:

- Jedes Objekt im Gleis ist zu jedem Zeitpunkt sichtbar und beeinflussbar.
- Eine neue, auf ETCS ausgerichtete Stellwerksgeneration kann die Risikobeziehung zwischen all diesen Objekten dynamisch bewerten und damit ihre Bewegungen sicher und trasseneffizient steuern.
- Das Traffic Management System wird ein vollständiges Bild zu allen Prozessen haben und deshalb viele Routinetätigkeiten automatisieren können (z.B. Gleise sperren, Warnbereiche für Baustellen einrichten).
- Dank starker Reduktion der Aussenanlagen wird ein sehr grosser Business Case entstehen: Weniger bis keine Zugortungs-/ Gleisfreimeldeeinrichtungen mehr, keine Rangiersignale, Balisen, Tafeln etc.

1.3.2 Ziele des Projektes „Genaue sichere Lokalisierung“

Ziele des Projektes „Genaue sichere Lokalisierung“ ist, die heutige infrastruktur- und odometriebasierte Lokalisierung zu einer kontinuierlichen, objektseitigen, autonomen und sicherheitsintegeren (z.T. SIL4) Lokalisierung weiter zu entwickeln. Eine „Genaue sichere Lokalisierungstechnik (GLAT, auch für „generic location-aware Toolbox“s) spielt als zentrale Funktion eine fundamentale Schüsselrolle. Die Verwirklichung dieser attraktiven Chance, die dem Schienenverkehr zahlreiche Vorteile verschafft (…), ermöglicht die Entwicklung einer Lokalisierungseinheit mit geeigneter Sensorik“ [3].

Folgende Teilziele werden dabei verfolgt [4]:

- Kosten
    - Deutlich geringere Menge an Sicherungsanlagen durch ETCS L2/L3 und durch neue Rangierlösungen
    - Automatisierungsschritte in Projektierung, Baustellensicherheit, Fahrdienstleitung, Fahrdienst
- Sicherheit
    - Lokalisierung und Steuerung jedes Objektes im Gleis - immer - auch in jeder Ausnahmesituation.
- Kapazität
    - Wirtschaftliche und schnelle Migration zur ETCS Führerstandsignalisierung.
    - Ausnutzung der Fähigkeiten von ETCS durch bessere Stellwerktechnik
    - Direkte adaptive Feinsteuerung und Moving Block.
- Funktion
    - Jedes Objekt im Gleis ermittelt seine Position autonom und übermittelt sie periodisch an ein zentrales System. Dadurch ist es zu jedem Zeitpunkt sichtbar und kann beeinflusst bzw. direkt gesteuert werden.

Könnte man sichere Endgeräte (Fahrzeugsysteme, Tablets und Tags) entwickeln, die ihre Position auf etwa 1m genau fail-safe an das neue Stellwerk mit geometrischer Sicherheitslogik melden können, dann würde folgendes möglich werden [5]:

- Günstige Implementierung von ETCS L3+ (Verlässlich bekannter Zugschluss) und damit Verzicht auf alle Gleisfreimeldeanlagen (36'000 existieren heute).
- Starke Reduktion der Infrastrukturausstattung (um bis zu 80%):
    - Mobile Führerstandsignalisierung für Rangieren und Manöver und damit Abbau von Zwergsignalen.
    - Vermeidung des Aufbaus von 60'000 ETCS Informations-Balisen durch gefunkte/gespeicherte ortsabhängige Informationen («virtuelle Balise»), die in der Lok vorliegen.
    - Vermeidung von 9'000 zusätzlichen Achszählerabschnitten für ETCS L2.
- Vermeidung von unzulässigen Signalüberfahrten. Eine präzise WarnApp2 oder mobile Führerstandsignalisierung für wirklich alle Betriebssituationen.
- Prozessvereinfachung im immer noch zu komplexen ETCS Bahnprozess: Vermeidung zusätzlicher Installationen, Topologiereserven und von Prozess-Erschwernissen (z.B. bzgl. der FASI- und SR Modi)
- Schutz des schnellen vor dem langsamen oder aufstartenden Verkehr. Nicht für jede langsame oder Manöverbewegung kann heute ein voller Flankenschutz erzeugt werden, z.B. bei neu aufgestarteten noch nicht an ETCS angemeldeten Fahrzeugen.
- «Tagging von Personen, Baustellen, Hindernissen und Wagen» (Vollüberwachung der Sicherheit):
    - Positionsmarker für diverse mobile Einheiten und Prozesse.
    - Die Sicherheit könnte z.B. auch für das Baustellenumfeld stark erhöht werden, wenn das „Entlaufen" von abgestellten Materialien an der Grenze dadurch erkannt wird, dass diese durch ein Lokalisierungsdevice markiert werden (Flankenschutz).
    - Werden Personen „getagged" (z.B. Streckeninspekteure, Ultraschallmessung oder Kleinunterhalt), so könnten sie beim Betreten des Gleises als Hindernis erkannt werden - und auch automatisch vor Zügen gewarnt werden.
- Sichere mobile Anwendungen für Mitarbeiter in verschiedenen Arbeitssituationen, bei denen sie ihren Standort sehr genau kennen müssen. „Navi-ähnliche" Funktionen und Service-Hilfen, die Schilderflut und Ortskenntnisse obsolet machen.
- Eine redundante Sicherheitsebene könnte quer über den gesamten Bahnprozess geschaffen werden, da trotz gestörter Anlagen (Zug, Infrastruktur) immer noch «alles mit Position und Geschwindigkeit sichtbar» ist. Notbedienungen oder Inbetriebnahmen hätten ein zusätzliches «Sicherheitsnetz».

1.3.3 Ziele der Phase 0 der Machbarkeitsstudie zur genauen sichere Lokalisierung

Ziel der SBB ist die Machbarkeit einer genauen, sicheren Lokalisierung sämtlicher Objekte im Gleis (Rollmaterial, Menschen, Hindernisse wie schweres Werkzeug etc.) in einem ersten Schritt („CENELEC Phase 0“) theoretisch und durch Simulationen zu untersuchen sowie durch exemplarische Messungen zu belegen.

Für die volle Entfaltung werden die in der Tabelle 1. aufgeführten Teilziele und entsprechende Anforderungen beachtet und erfüllt. Damit entsteht ein erster Aufschlag zu einer Anforderungsanalyse und -beschreibung. Diese dienen sowohl als Grundlage zur Prüfung der Machbarkeit und sind Grundlage für die Inhalte dieses „White Papers“ für eine neuartige und von der streckenseitigen Infrastruktur unabhängige, genaue und sichere Lokalisierung von Objekten.

1	Systemkonzept	Der Nutzen einer so vielseitig einsetzbaren Lokalisierungstechnik tritt nur ein, wenn sie als einfacher Baukasten in verschiedensten Anwendungssituationen und sicheren Endgeräten homogen nutzbar wird.
2		Funktional und technologisch modulare Realisierung, denn die Realisierung anwendungsspezifischer Lokalisierungstechnologien ist deutlich aufwendiger, da sie für jede Anwendung einzeln zugelassen werden müssen (auch bzgl. ihrer Interaktion).
3		Schaffung einer modularen, erweiterbaren Systemarchitektur, die die Anbindung diversitärer Sensoren erlaubt.
4		Mobil einsetzbar (als Tag oder in/mit einem Tablet, Stromverbrauch niedrig, sehr kleine Bauformen)
5		homogene Nutzbarkeit im Schienenverkehrssystem
6		Funktion eines Datenkonzentrators von verfügbaren Sensordaten und Bereitstellung einer Schnittstelle zur Kommunikation
7	System-merkmale	Fail-Safe: Gesicherte Ausfalloffenbarung, Ausfallwahrscheinlichkeit gefährlicher Fehler z.T. auf SIL 4 Niveau, je nach Gefährdungsgrad
8		Lokalisierung gleisgenau (<1m) zur eindeutigen Ortung in jedem Betriebszustand
9		Bereitstellung einer aktuellen Uhrzeit
10		Security Konzept (z. B. GNSS-Störer- und Täuscherdetektionseinheit)
11		Änderungssensibilität < 1 Sekunde zur Vermeidung von großen Reserveabständen mit der entwickelten Ortungsarchitektur soll auch die Lokalisierung von Menschen, Arbeitsprozesse oder nicht schienengebundene Fahrzeuge im Gleis ermöglicht werden, z.B. durch Konfiguration und Parametrierung
12		Maßnahmen zur Kontrolle der Zugintegrität
13	Schnittstellen	Beispielhaft für entsprechende Anwendungen mit den entsprechenden zu erprobenden Schnittstellen sind die verwendeten Lokalisierungs-Sensoren zusammen mit den zugehörigen Auswertealgorithmen zu qualifizieren
14		Harmonisierung und Aktualisierung der verwendeten Daten gewährleisten (auch Karten)

15	Technologie	GNSS-Empfänger mit offener Softwareschnittstelle zur Gewährleistung der Anpassbarkeit an den Schienenverkehr
		Komplementäre/ diversitäre Sensorik wie z. B. Inertialsensorik zur Unterstützung der satellitenbasierten Ortung
16	Sicherheit / Zulassung	Nachweis- und Zulassungsprozess generisch und typspezifisch zur Vermeidung von Einzelzulassungen, (Sicherheitsnachweisführung entsprechend dem Rechtsrahmen und den Richtlinien des Schienenverkehrs)
17		Zum Abschluss der technischen Betrachtung ist eine Simulation und Erprobung durch Messfahrten durchzuführen
18		Analyse der Gefährdungen bei der Nutzung
19		Analyse der technischen Risiken bei der Nutzung
20		Analyse der organisatorischen und betrieblichen Risiken bei der Einführung
21	Kosten	Abschätzung der Kosten der Lokalisierung

Tabelle 1.1: Teilziele und entsprechende Anforderungen zur Machbarkeit

2. Leer

3. Schwerpunktbereich „Use Cases“

Die Aufstellung von Basisanforderungen ausgehend von definierten Use Cases ist der zentrale Ansatz der Machbarkeitsstudie. Basisanforderungen umfassen vor allem Integritäts- und Genauigkeitsanforderungen für die Lokalisierung.

3.1 Definition von Use Cases

Allgemein werden unter einem **Use Case** gebündelt alle möglichen **Szenarien** verstanden, die eintreten können, um innerhalb eines Systems ein bestimmtes fachliches Ziel unabhängig von konkreten technischen Lösungen zu erreichen.

Die hier betrachteten Use Cases sind betriebliche Szenarien, die im Eisenbahnsystem lokaliserungsrelevant sind. Die Use Cases wurden von der SBB ermittelt und in einem eigenen Dokument zusammengestellt und erläutert (Zusammenzug siehe Tabelle 3.3). Sie umfassen repräsentative Situationen für bestehende und neue Aufgaben und Möglichkeiten im Eisenbahnsystem, welche sich aus neuen technischen Möglichkeiten einer genauen, sicheren und kontinuierlichen Lokalisierung von Objekten ergeben.

Die betreffenden Systeme sind damit im Einzelnen:

- das Eisenbahnleit- und Sicherungssystem ELSS (z.B. mit den Funktionsblöcken Fahrwegsicherung und -steuerung, Zugsicherung und -steuerung, Disposition einschließlich der technisch-menschlichen Realisierung), ergänzende Bestandteile sowie als Subsystem im ELSS auch das Lokalisierungssystem
- das Lokalisierungssystem (Ortungssystem), welches die Lokalisierung von (Lokalisierungs-)Objekten primär ermöglicht. Das Lokalisierungssystem stellt Ausgangsgrößen mit einer von der jeweiligen Aufgabe des ELSS abhängigen Genauigkeit und Integrität über definierte Schnittstellen zur Verfügung.
- das Umsystem, d.h. die Systemumgebung des Eisenbahnsystems im engeren Sinne, wie Menschen (z.B. Instandhalter/Rotten), Artefakte (z.B. Werkzeuge oder Maschinen), Schnittstellen der betrieblichen Systemumgebung (z.B. Depot, Laderampen, ...) und der natürlichen Systemumgebung (z.B. Lawinen, Erdrutsche).

3.2 Vorgehensweise zur Ermittlung der Basisanforderungen

Use Cases sind komplexe Beziehungsgefüge, in denen bahnbetriebliche Funktionen und Aufgaben mit den zu lokalisierenden Objekten (den Lokalisierungsobjekten) in Beziehung stehen:

- Diese Objekte müssen einerseits für die richtige, sichere und effiziente Erfüllung bahnbetrieblicher Funktionen genau und verlässlich lokalisiert werden. Diese Objekte werden als Lokalisierungsobjekte bezeichnet. Abbildung 3.2 zeigt diese Zusammenhänge im mittleren Teil.
- Diese Objekte müssen andererseits durch Sicherungsfunktionen des ELSS geschützt werden. Die zu schützenden Objekte werden als Gefährdungsobjekte bezeichnet. Abbildung 3.2 zeigt diese Zusammenhänge im oberen Teil.

Die Gefährdungsobjekte werden im Fall, dass die Lokalisierung nicht die Ansprüche insbesondere der Sicherheit erfüllt, infolge daraus resultierender betrieblicher Fehlentscheidungen gefährdet und ggf. geschädigt werden. Der zugehörigen Lokalisierungsfunktion kann somit ein akzeptables Risiko zugeordnet werden, indem der korrespondierenden Fehlfunktion ein Grenzrisiko im Sinne einer Tolerierbaren Gefährdungsrate THR zugewiesen wird. Es kann damit auch den Fall geben, dass ein Lokalisierungsobjekt ein Gefährdungsobjekt sein kann.

Aus dem betrieblichen Risiko kann nun einerseits der Lokalisierungsfunktion eines Lokalisierungsobjektes eine Anforderung von Verlässlichkeitseigenschaften und -merkmalen im Sinne von RAMSS zugeordnet werden, wie andererseits aus den betrieblichen Funktionen Anforderungen an die Lokalisierungszustände im Sinne von Genauigkeitsmerkmalen resultieren. In der Summe entstehen daraus die Anforderungen an die Genauigkeit des Lokalisierungszustandes und die Verlässlichkeit (Integrität und Zuverlässigkeit) der Lokalisierungsfunktion, die von dem Lokalisierungssystem insgesamt zu erfüllen sind. Abschließend muss noch nachgewiesen werden, ob die erreichten Eigenschaften der Verlässlichkeit und Genauigkeit auch tatsächlich die betrieblichen Belange erfüllen, oder ob ggf. weitere betriebliche Maßnahmen erforderlich sind. Ausgehend von einzelnen Use Cases werden die jeweiligen qualitativen und quantitativen Anforderungen an Sicherheit und Genauigkeit systematisch ermittelt.

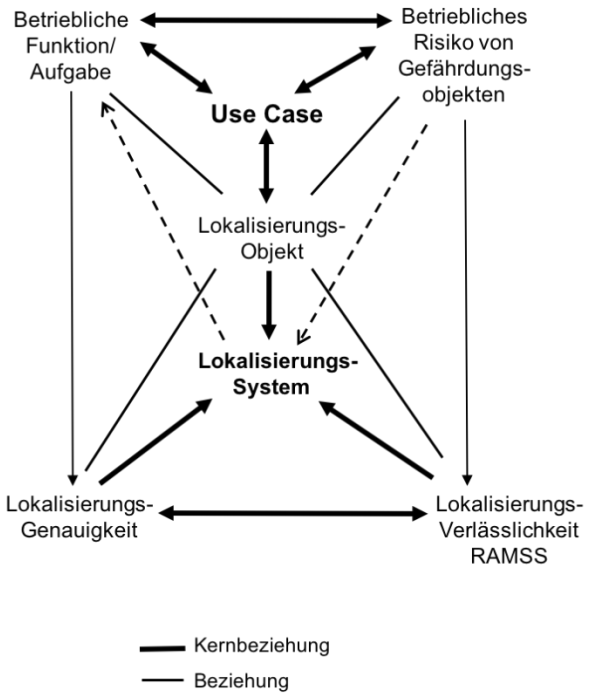


Abbildung 3.2: Zusammenhänge zwischen den Aspekten von Use Case und des Lokalisierungssystems

Für die Struktur der Anforderungen werden die allgemeinen Eigenschaften Sicherheit und Genauigkeit nach Maßgabe der Attributhierarchie (vgl. [6] und [7]) nach den Merkmalen und Größen sowie der für den Use Case erforderlichen Werte zusammengestellt und geclustert. Anhand dieser Klassifizierungsstruktur werden die mit den verschiedenen Sensoriken, Algorithmen und Systemstrukturen erzielbaren Werte später als Angebot den aus den UseCases resultierenden Anforderungen gegenübergestellt und hieraus ein Erfüllungsgrad abgeleitet. Eine anschließende Diskussion zielt auf eine möglichst universelle, aber in einzelnen Parameterwerten skalierbare Konfiguration des Lokalisierungssystems.

3.3 Analyse der Use Cases

Zur Ableitung der mit den Use Cases verbundenen Basisanforderungen wird eine systematische Analyse der Use Cases durchgeführt (Use Cases siehe Tabelle 3.3). Dazu gehören im Einzelnen:

- Auflistung der Use Cases und ihre Überprüfung auf Vollständigkeit durch einen Vergleich mit generischen Funktionsstrukturen von ELSS
- Überprüfung der Use Cases auf Risikorelevanz
- Identifikation und Definition der Bezüge zwischen Use Cases, betrieblichen Funktionen, Lokalisierungsobjekten und Gefährdungsobjekten durch Anwendung semi-formaler Beschreibungsmethoden wie UML-Klassendiagramme (siehe Abbildung 3.2)
  - Identifikation und Definition der Lokalisierungsobjekte
  - Identifikation und Definition von Lokalisierungsattribute
  - Identifikation und Definition von Gefährdungsobjekten

- Identifikation und Definition der Nutzung der Lokalisierungsinformation in bahnbetrieblichen Prozessen und korrespondierenden leittechnischen Aufgaben und Funktionen (Nutzungsfunktion)
- Identifikation und Definition der zu den leittechnischen Funktionen gehörenden Attribute (Gefährdungsraten, Sicherheitsintegritätsstufen)

In den einzelnen festgelegten Use Cases verweisen mehrere Szenarien auf wenige Lokalisierungsobjekte, z.B. Waggons, Lokomotiven, Personen und Güter. So resultiert hierdurch eine gewisse Bereinigung der Anzahl zu betrachtender Lokalisierungsobjekte.

Allerdings erfordern Nutzungen der einzelnen Use Cases unterschiedliche Ausprägungen an die einzelnen Lokalisierungsmerkmale (z.B. ist ein Zughalt im Bahnhof nicht so präzise notwendig wie vor einem Gefahrenpunkt, z.B. einer umlaufenden Weiche bzw. einem zugehörigen Grenzzeichen, ebenfalls sind in diesen Fällen unterschiedliche Sicherheitsintegritätsstufen erforderlich).

Für die Ermittlung der Basisanforderungen werden die einzelnen Eigenschaften

- des Lokalisierungsobjekts,
- der Nutzungsfunktion und
- der Lokalisierungsfunktion

im Einzelnen aufgeschlüsselt.

Für den zu erzielenden Nutzen durch eine neuartige Lokalisierung der Objekte des Schienenverkehrs müssen viele Einsatzbedingungen erfüllt werden, die in Form von sogenannten Use Cases spezifiziert sind (vgl. Tabelle 3.3). Die Use Cases beinhalten sicherheitsrelevante Funktionen wie die Warnung von Personen im Gleisbereich (Arbeitsstellenwarnung) bis hin zu nicht-sicherheitsrelevanten Funktionen wie die kapazitätssteigernde Funktion der Automatic Train Operation (ATO).

Die festgelegten Use Cases werden zuerst qualitativ analysiert. Die Strukturierung nach Lokalisierungsobjekten und Lokalisierungsinformationen, nach der Nutzung im Eisenbahnsystem und nach der zwischen ihnen vorhanden Bezügen ermöglicht eine Clusterung nach notwendigen Qualitätseigenschaften und daraus eine Klassifizierung zwecks synergetischer Bündelung von gleichartigen Anforderungen. In einem weiteren Schritt werden die erforderlichen Basisanforderungen qualitativ zusammengestellt und nach der unten beschriebenen Attributhierarchie strukturiert, nach Maßgabe der Use Cases quantifiziert und die Klassifizierung überprüft.

Die Anforderungen werden zunächst in einer Fallstudie für die folgenden Use Cases exemplarisch ermittelt:

- Personal im Gleis (z.B. Instandhalter zur Weichenschmierung, Gleisanlagenquerung, Arbeiten vor Ort, temporäre Unverfügbarkeit der Weiche, Gefährdungen des Mitarbeiters, Gefährdungen von Zügen, Wagen) [*Use Case Bezug 2.1.1 und 2.2.3*]

- Fahrzeugbewegung für Moving Block (Zugspitze, Zugende, schnelle und langsame Fahrt, Zugvollständigkeit) [*Use Case Bezug 1.1 bis 1.4*]
- Freifahren einer Weiche [*Use Case Bezug 1.1.2*]

3.3.1 Vollständigkeit der Use Cases

Die Aufgaben und Funktionen, in denen eine Lokalisierung von Objekten erfolgt, werden durch folgenden Ansatz ermittelt und charakterisiert. In Vorarbeiten wurde ein umfangreiches Modell der generischen Funktionsstruktur eines Eisenbahnleit- und -sicherungssystems (ELSS) erarbeitet (siehe Abbildung 3.3), welches im Einzelnen über 100 verschiedene Funktionsblöcke und die zugehörigen Informationsflüsse beschreibt. Damit wird eine Vollständigkeit der Use Cases ermöglicht. Das Funktionsmodell aus [8] wird für die Betrachtung in dieser Machbarkeitsstudie um weitere Nutzungsfunktionen außerhalb des ELSS für die festgelegten Use Cases im Eisenbahnverkehr ergänzt.

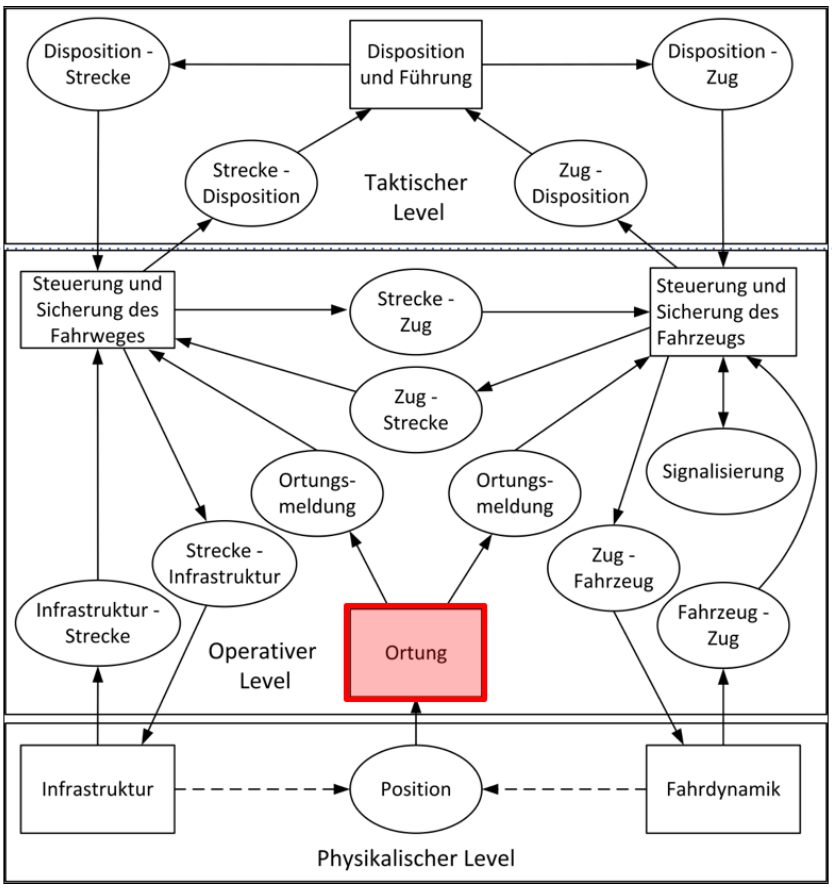


Abbildung 3.3: Modell der Generischen Funktionsstruktur eines Eisenbahnleit- und –sicherungssystems ELSS (Quelle [8])

Auf dieser generischen Modellierungsgrundlage wurde eine unabhängige und ggf. komplementäre Zusammenstellung von Einsatzfällen erstellt (Tabelle 3.2), mit denen die Use Cases der SBB überprüft, validiert und ggf. ergänzt werden, so dass die Vollständigkeit der Use Case als Grundlage für Lokalisierungsaufgaben gewährleistet ist.

Funktionskomplex	Einsatzfall		
Zugsteuerung und -sicherung	Fahr- und Bremssteuerung	Schnell-/Zwangsbrem-sung und -auflösung	
		Sanden	
	Ortung für Zugsteuerung und Zugsicherung, insbesondere Abstandshaltung	Für Stationshalt	Stärken und Schwächen von Zugverbänden
			Zugvollständigkeits-überwachung
		Für Halt an Gefahren-punkten (z.B. vor Bahnübergängen, vor Muren und Lawinen)	Gutverladung und Verladeanlagen und -geräte
		Für Depothalte	Für Rangierfahrten
			Für Rangierbahnhöfe
Fahrwegsteuerung und -sicherung	Fahrwegreservierung		
	Fahrstraßeneinstellung		
	Fahrstraßenauflösung		
	Zugvollständigkeitsüberwachung		
	für Rotten		
	Gleissperrungen		
	Weichenlagen		
Bahnübergangs-sicherung	Objekterkennung		
Disposition und Betriebs-mittelkoordination	Zuglaufverfolgung		
Einsatz- und Umlaufplanung	Zuglaufverfolgung		
	Personalverfolgung (TF)		
Intrusionsschutz	Objekterkennung (Bäume, Steine, Tiere, sonstige Stoffe und Materiale, z.B. Oberleitung, Masten,..)		
	Personalbeobachtung und -verfolgung		
Energieversorgung	Zuglaufverfolgung		
	Für Energieentgelte		
Instandhaltung von Roll-material, Infrastruktur und Energieanlagen	für Fahrweginspektionen		
	für Bau- und Instandhaltungsfahrzeuge		
	für Rotten		
Fahrgäste, Gepäck	Navigation für Fahrgäste in Bahnhöfen und in Zügen		
	Zur Platzreservierung und Fahrausweis-kontrolle		
	Für Gepäckverfolgung und -positionierung		
	Für Evakuierungen		
	Passagiere in Bahnhöfen		
	Behinderte Personen Navigation		
Sonderfälle, Einsatzfahrten	Polizeieinsatz		
	Katastropheneinsatz		
	Unfallrettung		
Güter	Güterverfolgung, Gutverladung und Verladeanlagen/geräte		
Betriebs- und Trassenplanung	Zuglaufverfolgung		
Abrechnung Dritte	Güterverfolgung, Gutverladung und Verladeanlagen/geräte		
	Für Dritte zur Auswertung (Big Data)		
	Fahrgastentgeltverrechnung		
Umweltbeobachtung	Zuglaufverfolgung für Lärmschutz		
Platzreservierung und -kontrolle			

Tabelle 3.2: Unabhängige und ggf. komplementäre Zusammenstellung nach Funktionskomplexen

Tabelle 3.3 enthält eine entsprechende Gegenüberstellung der Use Cases und der unabhängigen Zusammenstellung von Einsatzfällen. Das Ergebnis des Vergleichs zeigt, dass die Use Cases alle für die Lokalisierung relevanten Szenarien und die wichtigsten Informationen für die Erhebung und die Erarbeitung der Basisanforderungen weitgehend vollständig enthalten.

SBB Use Case		**M2C Use Case**
Nr.	**Bezeichnung**	**Bezeichnung**
1.1	Use Case „Schnelle und präzise Freimeldung Gleis, Weiche, Barriere“	Fahrwegsteuerung und -sicherung • Fahrwegreservierung • Fahrstraßeneinstellung • Fahrstraßenauflösung • Zugvollständigkeitsüberwachung • für Rotten • Gleissperrungen • Weichenlagen
1.1.1	Fast vollständige Reduktion der GFM, GFM nur noch in Netzzugangsbereichen zur Detektion nicht ausgerüsteter Fahrzeuge	
1.1.2	Schnelle Umstellung Weichen / Öffnung Barriere nach Zugüberfahrt (je nach heutiger Fahrstrassenlogik) mit weniger Komplexität / Systemaufwand möglich als mit heutigen GFM.	
1.1.3	Bessere, da dynamische Ausnutzung der Topologie mit Zügen (weniger Topologiereserven)	
1.1.4	Stärkere Mehrfachbelegung von heutigen Gleisen in der vollen Länge ohne Notwendigkeit von kurzen GFM-Abschnitten	
1.1.5	Vermeidung von Topologieanpassungen oder hohen Balisenmengen aufgrund der heute ungenauen oder nicht vertrauenswürdigen Lokalisierung der ETCS OBU	
1.2	Use Case „Präzise Zugendeposition (insbesondere Güterzüge)“	Zugsteuerung und -sicherung • Fahr und Bremssteuerung • Schnell-/Zwangsbremsung und -auflösung • Sanden • Ortung für Zugsteuerung und vor Bahnübergängen, vor Muren, Lawinen,...) • Gutverladung und Verladeanlagen/geräte • für Depothalt • für Rangierfahrten • für Rangierbahnhöfe
1.2.1	Zugintegrität, um ETCS L3 und moving block zu ermöglichen	Zugvollständigkeitsüberwachung
1.2.2	Automatische Zuglängenberechnung	
1.3	Use Case „Performante „elektronische Kopplung“ von Zügen, Optimierung Zugfolgezeit“	

SBB Use Case		M2C Use Case
Nr.	**Bezeichnung**	**Bezeichnung**
1.4	Use Case „Präzise Zugspitzenposition für ETCS-Prozess“	Sicherung, insbesondere Abstandshaltung • für Stationshalt • für Halt an Gefahrenpunkten
1.4.1	Effiziente, präzise und sichere Steuerung von Vereinen, Trennen, Wenden (VTW) und besetzten Einfahrte	Stärken und Schwächen
1.4.2	Sicheres Rangieren mit/ohne Shunting-Modus ohne Zwergsignale, trotzdem mit voller Absicherung gegen feindlichen Verkehr	
1.4.3	Für präzises Halten gemischter Kompositionen am Perron	
1.5	Use Case „Volle und genaue Orts- und Geschwindigkeitsüberwachung in jedem ETCS Modus (FS, SH, SR, OS, TR, ..) und auch wenn ETCS OBU offline ist“	Zugsteuerung und -sicherung • Fahr und Bremssteuerung • Schnell-/Zwangsbremsung und -auflösung
1.5.1	Schnelle Erkennung entlaufener Wagen (impliziert Tagging jedes abgestellten Wagens/Wagengruppe)	
1.5.2	Parallel anlaufendes Einfädeln/Ausfädeln in Bahnhöfen	
1.5.3	Genauer elektronisch gesicherter Flankenschutz (Daten für ES Logik) mit dynamischer Risikooptimierung	
1.5.4	Genauer elektronisch gesicherter Durchrutschweg (Daten für ES Logik) mit dynamischer Risikooptimierung	
1.5.5	Reduktion des Odometrie-Fehlers, der den Bremseinsatzpunkt beeinflusst, damit Verbesserung der Zugfolgezeit	
1.6	Use Case „Annäherungswarnung im Rangierfahrzeug“	
1.6.1	innerhalb Rangierbereich unabhängig vom ETCS-Modus oder Betriebszustand	
1.6.2	bei Gefährdung des schnellen Verkehrs außerhalb des Rangierbereiches	
1.7	Use Case „Real-Time Validierung des Beschleunigungs- und Bremsvermögens“ Dank Trägheitssensorik kann das Beschleunigungs- und Bremsverhalten real-time erfasst und überprüft werden. Der effektive Bremsweg wird in die ES Risikoberechnung aufgenommen und der Zug somit optimal gebremst. => Zugfolgezeiten optimierbar.	
2	Menschen, Arbeitsprozesse oder nicht schienengebundene Fahrzeuge im Gleis	Zugsteuerung und -sicherung • vor Muren, Lawinen,...) • Gutverladung und Verladeanlagen /geräte • für Depothalt • für Rangierfahrten • für Rangierbahnhöfe

SBB Use Case		M2C Use Case
Nr.	**Bezeichnung**	**Bezeichnung**
2.1	Use Case Präzise Warnung einzelner Menschen im Gleis (ggf. mit/ohne konfiguriertem Zug-Notstop oder Geschwindigkeitsreduzierung)“	
2.1.1	Warnung Inspektionsmitarbeiter. Z.B. Streckeninspekteure oder Mitarbeiter bei der manuellen Ultraschallmessung (heute zwangsweise oft zu zweit).	
2.1.2	Warnung Instandhalter, z.B. beim Kleinunterhalt. Sie müssen heute noch oft aus Sicherheitsgründen zu zweit gehen. Oder zB in den Gleisbereichen der Werkstätten	
2.1.3	Persönliches Tag für jeden Baustellenmitarbeiter (nicht nur Warnanlagen für Sicherheitswärter), das ihn auch vor lokalisierbaren Bewegungen in den Baustellen warnt.	
2.1.4	Warnung Personal in Manöverbereichen (z.B. beim Koppeln)	
2.1.5	Warnung Personal in Rangierzonen	
2.1.6	Sonderbegehungen mit großen Gruppen oder unerfahrenen Besucher	
2.1.7	Warngeräte für Aktivitäten neben dem Gleis, falls diese nahe am Lichtraumprofil erfolgen.	
2.2	Use Case Absicherung von Bereichen, z.B. von Baustellen und Arbeitsprozessen im Gleis“	Fahrwegsteuerung und -sicherung • Fahrwegreservierung • Fahrstraßeneinstellung • Fahrstraßenauflösung • Zugvollständigkeitsüberwachung • für Rotten • Gleissperrungen • Weichenlagen
2.2.1	Automatisierte mobile Baustellen-Warnanlagen (MWA aufstellen = Warnung steht automatisch, heutiger Fahrdienst-Prozess wird automatisiert), Einsparung Baustellensicherheitspersonal	
2.2.2	Automatisierung von Fahrdienst-Routinetätigkeiten	
2.2.3	Automatisches Sperren oder Freigeben ohne manuellen /fahrdienst-lichen Verwaltungsprozess, ausgelöst durch Tag im Gleis oder durch manuelle Anfrage via GLAT Endgerät	
2.2.4	Missverständnis-freie Ein-/Ausrichtung einer Gleissperre	
2.2.5	Schnelles Sperren einer Gefahrenzone vor Ort (z.B. bei erkannter Beschädigung, Autounfall, etc.)	

SBB Use Case		M2C Use Case
Nr.	**Bezeichnung**	**Bezeichnung**
2.2.6	Für Kurzbaustellen: Aufstellen zweier MWA vor Ort =Bereich zwischen ihnen ist automatisch gesperrt	
2.2.7	Autorisierung von Rangierbewegungen (gerichtet/ungerichtet, durchgehend/unterbrochen)	
2.2.8	Fehlerfreies und fernsteuerbares Tagging von Langsamfahrstellen bei Baustellen (virtuelle Langsamfahrstellen- Schilder) vor Ort, Verkürzung Ein-/ Ausrichtezeit. Tagging von leichten Lichtraumprofil-Einschränkungen	
3	Hindernisse im Gleis erkennen und absichern	Instandhaltung von Rollmaterial, Infrastruktur und Energieanlagen • für Fahrweginspektionen • für Bau- und Instandhaltungsfahrzeuge • für Rotten Intrusionsschutz • Objekterkennung (Bäume, Steine, Tiere, sonstige Stoffe / Materialien, z.B. Oberleitung, Masten,) • Personalbeobachtung und -verfolgung Güter • Güterverfolgung, Gutverladung und Verladeanlagen/geräte
3.1	Use Case „Tagging von Einzelobjekten (Voraussetzung für ATO)“	
3.1.1	Tagging abgestellte Eisenbahnfahr-zeuge	
3.1.2	Tagging Hangrutschabsicherung / gefährdete Hänge / instabile Bauten	Naturereignisse
3.1.3	Tagging Kranausleger	
3.1.4	Tagging schweres Werkzeug im Gleis	
3.1.5	Tagging Karren bei Überfahrt	
3.1.6	Tagging (mobile) Entgleisungsvorrichtungen	
3.1.7	Spontanes Tagging beschädigtes Gleis (Niedrighaltung). Tagging von nicht überwachten Toren, Schranken oder Barrieren am Gleis, die sicher geschlossen sein müssen (Fremdverkehr abhalten) oder von Objekten, die ins Lichtraumprofil ragen.	
4	Ortsabhängige Autorisierung	
4.1	Use Case „Bindung von ES- oder Fahrzeugfernbedienungen an einen Ort“	
4.2	Use Case „Automatisierte Freigabe von Gleisüberschreitungen (Tag warnt nicht-nur sondern zeigt auch eine Überschreitungserlaubnis ortsabhängig an).“	
5	Mobile Fernsteuerung der Infrastruktur (Weichen, Barrieren) oder der Fahrzeuge	

SBB Use Case		M2C Use Case
Nr.	**Bezeichnung**	**Bezeichnung**
5.1	Use Case „Notbedienungsterminal für ES“	
5.2	Use Case „Funkgleismelder-Funktionen“ (Anfrage von Fahrstrassen und Bestätigung derselben)	
5.3	Use Case „Manuelle Fernsteuerung einer Lok mit ETCS Ausrüstung (via TMS/ES/RBC/ETCS OBU, direkte V-Steuerung oder nur Zieleingaben zur Fernlenkung, auch für Driverless Train Operation wichtig)“	
6	Ortsinformationen, „Navi-Funktionen“, location based services	
6.1	Use Case „Elektronische Abbildung aller erforderlichen Ortskenntnisse auf dem sicheren Tablet (z.B. für internationale oder unerfahrene Lokführer)“	
6.2	Use Case „Ersatz der ETCS-Tafeln durch Anzeige auf einem GLAT Endgerät“	
6.3	Use Case „Automatic location based services, z.B. ortsabhängige Checkliste für die Manöver mit inter-nationalen Zügen oder automatisierte Anzeige von Versorgungsstellen“	
7	Vereinfachung und/oder Absicherung der heutigen ETCS Prozesse	
7.1	Use Case „Beispiel: Kontroverse zum ETCS SR-Modus lösen“	
7.2	Use Case „Keine ortsfesten Balisen“ Ein netzweites ETCS L2 der heutigen Form würde bei SBB ca. 60.000 ortsfeste Balisen erfordern. Und dabei wäre das Rangieren noch ohne Führerstand-signalisierung gelöst. Balisen führen zu Projektierungsaufwand. Rangier- und Manöverbetrieb mit Führerstand-signalisierung ist allein mit Balisen kaum zu lösen, bzw. die Balisen-mengen wären nochmals sehr gross.	
7.3	Use Case „Keine Tafeln“ Ein netzweites ETCS L2 der heutigen Form würde bei SBB ca. 65.000 ortsfeste Tafeln erfordern. Einzig um im Störungsfall noch zu wissen wo man sich befindet und wie weit man ungesichert verkehren kann.	
8	Kommerzielle und operative Nutzung	Disposition und Betriebsmittelkoordination • Zuglaufverfolgung Einsatz- und Umlaufplanung • Zuglaufverfolgung • Personalverfolgung (TF)

SBB Use Case		M2C Use Case
Nr.	**Bezeichnung**	**Bezeichnung**
		Betriebs- und Trassenplanung • Zuglaufverfolgung Güter • Güterverfolgung, Gutverladung und Verladeanlagen/geräte
8.1	Use Case „Tracking von Eisenbahnfahrzeugen, Containern, etc..“	
8.2	Use Case „Automatisierung der Verwaltung von rangierten Zügen“	
8.3	Use Case „Unterstützung Fieldforce-Management mit präzisen Situationsabbildern und genauer Lokalisierung aller Gefahren-Objekte (GOB) und Tags, sowie ggf. der einsetzbaren Ressourcen in der Nähe von Störungen“	
8.4	Use Case „Betriebsdatenerfassung für Arbeiten im Gleis inkl. Identifikation der Ausführenden“	Abrechnung Dritte • Güterverfolgung, Gutverladung und Verladeanlagen/geräte • Für Dritte zur Auswertung (Big Data) • Fahrgastentgeltverrechnung Bahnübergangssicherung • Objekterkennung Energieversorgung • Zuglaufverfolgung • Für Energieentgelte Umweltbeobachtung • Zuglaufverfolgung für Lärmschutz Platzreservierung und -kontrolle Sonderfälle, Einsatzfahrten • Polizeieinsatz • Katastropheneinsatz • Unfallrettung Fahrgäste, Gepäck • Navigation für Fahrgäste in Bahnhöfen und in Zügen • Zur Platzreservierung und Fahrausweiskontrolle • Für Gepäckverfolgung und -positionierung • Für Evakuierungen • Passagiere in Bahnhöfen • Behinderte Personen Navigation Gefahrgutverfolgung

Tabelle 3.3: Use Cases Vergleichstabelle zur Konsistenz- und Vollständigkeitsprüfung

Nicht in den Use Cases enthalten sind weitere Nutzungen insbesondere für die übergeordneten Leitfunktionen, die aber aus den verfügbaren Lokalisierungsinformation ermittelt werden können, und Lokalisierungsinformationen für die Passagierführung und Güterverfolgung sowie für den Bereich von Bahnübergängen.

Darüber hinaus sind im Dokument Szenarienhandbuch der SBB [9] typisierte Unfallereignisse im Betrieb Stand März 2017 mögliche Einsatzszenarien im Betrieb mit Angaben zu Schäden und Häufigkeiten zusammengefasst, die hinsichtlich der Relevanz zu den Use Cases bewertet wurden. Tabelle 3.3 enthält ebenfalls die relevanten Ereignisse aus dem Szenarienhandbuch.

3.3.2 Feststellung 1

Es wird festgestellt, dass die Use Cases alle für die Lokalisierung relevanten Szenarien und die wichtigsten Informationen für die Erhebung und die Erarbeitung der Basisanforderungen vollständig enthalten.

3.4 Identifikation der Lokalisierungsobjekte

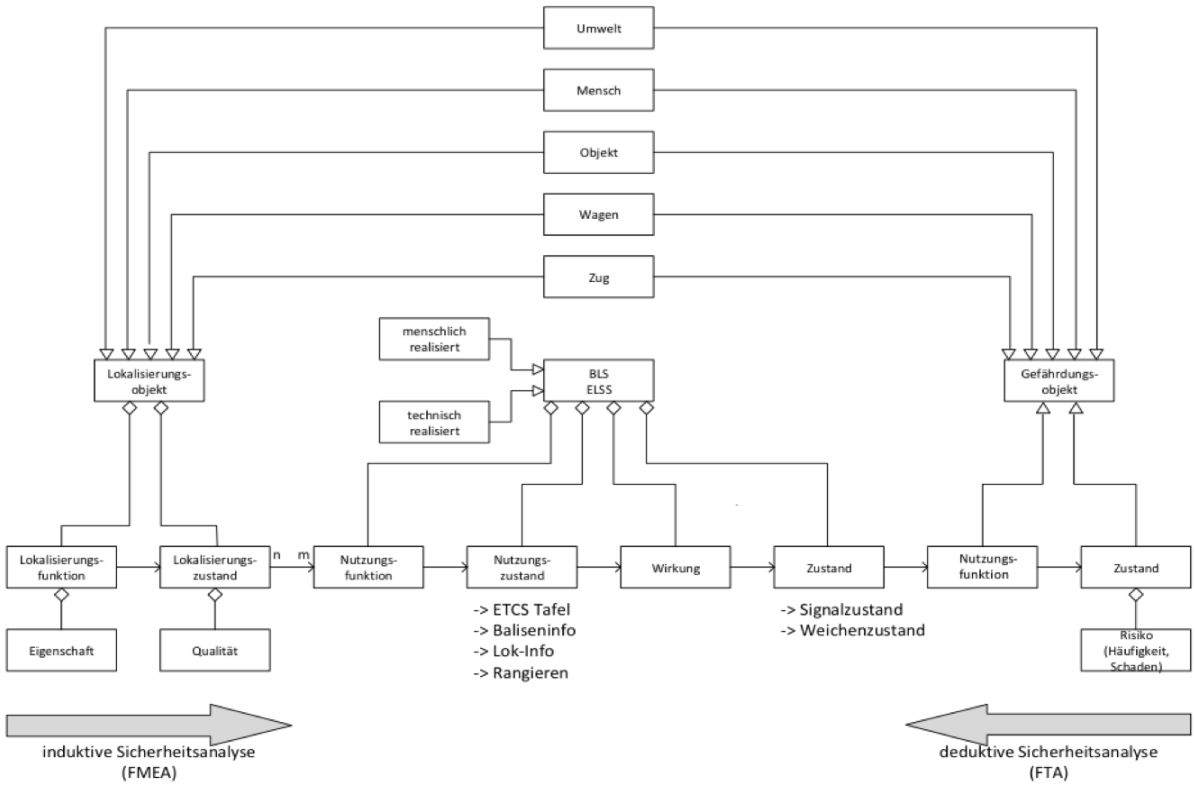


Abbildung 3.4: Kausalkette mit allen Entitäten als UML-Klassendiagramm

Die Use Cases beinhalten auf der einen Seite den Gegenstand der Lokalisierung (z.B. Zugende (UC 1.2), Zugspitze UC1.4, Baustelle UC2.2 usw.), d.h. das Lokalisierungsobjekt, und damit - in Anlehnung an eine „diensteorientierte Architektur SOA“ die - Lokalisierung als Basisfunktion und auf der anderen Seite die Anwendungsfunktion, welche die Lokalisierungsinformation nutzt (z.B. das Stellwerk UC1.5.3, die ETCS Fahrzeugausrüstung, UC1.4 oder eine Warnung für Gleisarbeiter und Rotten UC2. Zwischen dem Lokalisierungsobjekt und der Anwendungsfunktion befindet sich die Basisfunktion der Lokalisierung, welche aus der Position des Lokalisierungsobjekts die Information über den Lokalisierungszustand ermittelt, die ggf. mit Hilfe eines Übertragungssystems einer räumlich entfernten Anwendungsfunktion zur Verfügung gestellt wird (bspw. Gleisfreimeldung für ETCS Level 3) oder mit anderen Lokalisierungsergebnissen verglichen wird (bspw. Warnung eines Arbeiters im Gleis). Dieser Zusammenhang ist in Abbildung 3.4 in Form eines Klassendiagramms dargestellt.

Eine fehlerhafte Lokalisierungsinformation führt ggf. über diese Funktionsverkettung zu einer fehlerhaften Entscheidung, die sich objektschädigend auswirkt. Zum Beispiel kann eine

verfrühte Gleisfreimeldung zu einer Umstellung einer Weiche unter einem fahrenden Zug und damit zur Entgleisung führen.

Zur Beurteilung der erforderlichen und darüber hinaus komplementär der wirtschaftlich realisierbaren Ortungsgenauigkeit und der geforderten Sicherheit ist die Charakterisierung der Lokalisierungsobjekte selbst zwingend. Die Identifikation der Lokalisierungsobjekte und ihrer Attribute aus den Use Cases erfolgt nach den folgenden Kategorien:

Örtlichkeit:

- Im Gleisbereich
- Strecke
- Bahnhöfe
- Betrieblich
- Fahrgast-/Güterbezogen
- Am/neben Gleis
- Unmittelbar, entfernt

Objektart (bewegliche)

- Technische Artefakte
- Lebewesen: Menschen, Tiere, Pflanzen (Bäume,...)
- Naturobjekte (Steine, Felsen, Erde, Wasser, Schnee,..)
- Menschen (Personale, Fahrgäste, sonstige)

Eigenschaften der Objekte

- ID
- Bewegungsmuster (charakterisiert durch Referenztrajektorien und Abweichungsverteilungsfunktionen)
- Aufenthaltsbereich
- Bewegungsdynamik, Trajektorien, Aufenthaltsräume
- Häufigkeit des Vorkommens der lokalisierten Objekte
- Relevanz für das Bahnsystem (zur Risikobemessung)

Nr. 1)	Objekt und -art	Örtlichkeit 2)	Eigenschaften: Bewegungsmuster Objekt	Lokalisierung: Relevanz, Häufigkeit	Use Case	Unfallart und Datei
1.1	Fahrzeuge: Zug, Zugspitze, Zugende, Zuglänge Waggon schienengebundene Fahrzeuge, Karren bei Überfahrt, Container	Gleisbereich Weiche, Strecke Bahnhof Durchrutschweg Barriere (Bahnübergang)	spurgeführte Längsbewegung im Gleisbereich -250 - +250 km/h Positionen, Geschwindigkeiten, Beschleunigungen	sehr hoch dauernd	1.1 1.4 1.5 1.6 1.7 1.8 3.1.5 8.1 8.	ZZ2: Zusammenstoss Zug/Rangier ZZ1: Zusammenstoss zwei Züge, ZE1_2 Zugsentgleisungen ZZ3: Zusammenstoss Zug mit Hindernis/Strassenfahrzeug/externer Profilverletzung Baustelle; R3: Rangierunfall A1a-Rangier Bü: Bahnübergansunfall,
1.2ff	Fahrzeuge: Zug, Zugspitze, Zugende, Zuglänge Waggon schienengebundene Fahrzeuge,	Gleisbereich Weiche, Strecke Bahnhof Durchrutschweg Barriere (Bahnübergang)	spurgeführte Längsbewegung im Gleisbereich -250 - +250 km/h Positionen, Geschwindigkeiten, Beschleunigungen	sehr hoch dauernd	1.2 1.3 1.4 1.5 1.6 1.7 3.1.2 8.1 8.2	ZE1.d Zugentgleisungen ZE2.d Zugentgleisungen ZZ1.a Zwei Züge, wegen lückenhafter Technik, z.B. im Stellwerksbereich auch Signalfall ZZ1.b Zwei Züge, wegen menschlichen Fehlhandlungen, z.B. Stellwerksstörung, aber auch Auffahrunfall ZZ1.d Zwei Züge, wegen technischem Versagen der Infrastrukturanlagen ZZ2.a Zug/Rangier, wegen lückenhafter Technik, z.B. Stellwerk ZZ2.b Zug/Rangier, wegen menschlichen Fehlhandlungen, z.B. Rückfallebene, entlaufener Wagen,.. ZZ2.d Zug/Rangier, wegen technischem Versagen der Infrastrukturanlagen ZZ2.e Übrige Zusammenstöße ZZ3: Zusammenstoss Zug mit Hindernis/Strassenfahrzeug/externer Profilverletzung Baustelle; nicht

Nr. 1)	Objekt und -art	Örtlichkeit 2)	Eigenschaften: Bewegungsmuster Objekt	Lokalisierung: Relevanz, Häufigkeit	Use Case	Unfallart und Datei
						relevant, wird in Natur/Objekte separat behandelt R1: Entgleisung R2: Zusammenstoß Rangier mit Objekt R3: Zusammenstoß Rangier / Rangier einschließ abgestellten Schienenfahrzeugen Bü: Bahnübergangsunfall
2	Informationen: ETCS-Tafel, (vituelle) Balise	Gleisbereich	stationär	sehr hoch dauernd	6.2 1.6 1.7	Unbekannt
3	Infrastruktur-einrichtungen: Gleissperre, Prellbock?				2.2.4 3.1.6	ZE1.c Zugentgleisungen wegen technischem Versagen von Infrastrukturanlagen (bedingt, nur Schienenbrüche, Weichenbefahrung, Schienenfehler) ZE1.e Zugentgleisungen - übrige Entgleisungen ZE2.c Zugentgleisungen wegen technischem Versagen von Infrastrukturanlagen (bedingt, nur Schienenbrüche, Weichenbefahrung, Schienenfehler) ZE2 .e Zugentgleisungen - übrige Entgleisungen ZZ2.e Übrige Zusammenstöße ZZ3: Zusammenstoss Zug mit Hindernis/Strassenfahrzeug/externer Profilverletzung Baustelle; nicht relevant, wird in Natur/Objekte separat

Nr. 1)	Objekt und -art	Örtlichkeit 2)	Eigenschaften: Bewegungsmuster Objekt	Lokalisierung: Relevanz, Häufigkeit	Use Case	Unfallart und Datei
						behandelt R1: Entgleisung R2: Zusammenstoß Rangier mit Objekt
4	Menschen: Inspektionsmitarbeiter, Instandhalter, Personal in Manöverbereichen, Personal in Rangier-zonen, grosse Gruppen unerfahrene Besucher	Gleisbereich und Umgebungsbereich im Gleis	beliebige Bewegungen mit max 10 km/h	sehr hoch dauernd	2.1 8.4	A1 Arbeitsunfall im Gleisbereich mit bewegten Fahrzeugen bei a) Rangierarbeiten, b) Arbeiten im Gleisbereich, c) Überqueren der Gleise Unter die Kategorie PE können diese Use Cases nicht eingeordnet werden
5a	Geräte, Instandhaltungsartefakte Automatisierte mobile Baustellen-Warnanlagen Warngeräte für Aktivitäten neben dem Gleis, falls diese nahe am Lichtraumprofil erfolgen.	Strecke im Gleis Bereich im Gleis Umgebungsbereich im Gleis	stationär	(sehr) hoch (sehr) häufig	2.1 2.2 3.1.5 8.3	A1 ZE1.e ZE2.e ZZ2.a- e ZZ3 R2 R3 für 5a, b, c, d
5b	Kurzbaustellen	Strecke im Gleis Bereich im Gleis	stationär	sehr hoch häufig	3.1.7	in 5a subsummiert
5c	schweres Werkzeug im Gleis	Gleisbereich	stationär	mittel	3.1.4	in 5a subsummiert
5d	Kranausleger	Gleisbereich und Umgebungsbereich im Gleis	Bewegung mit max 20 km/h??	mittel gelegentlich	3.1.3	in 5a subsummiert
6	Naturobjekte: Hangrutschabsicherung, gefährdete Hänge, instabile Bauten	Umgebungsbereich im Gleis	stationär	mittel selten	2.1.3	ZE1.e ZE2.e ZZ3.a N.a -N.g: Naturereignisse

Nr. 1)	Objekt und -art	Örtlichkeit 2)	Eigenschaften: Bewegungsmuster Objekt	Lokalisierung: Relevanz, Häufigkeit	Use Case	Unfallart und Datei
7a	sonstige Objekte: Tore, Schranken oder Barrieren am Gleis Objekte, die ins Lichtraumprofil ragen	Umgebungsbereich im Gleis	stationär und bewegt (wenige m/s)	gering ???	3.1.7	keine äquivalente Kategorie im Szenarienhandbuch
7b	sonstige Objekte: Gefahren-Objekte (GOB) und Tags, sowie ggf. der einsetzbaren Ressourcen in der Nähe von Störungen“	Gleisbereich und Umgebungsbereich im Gleis-	stationär mobil XXkm/h	mittel häufig	1.1	GG: Tropfender Kesselwagen (toxisch, ätzend); kleine Freisetzung ZE1c ZE2c ZZ1d zu verifizieren

1) Nr. Gefahrenblatt

1) Örtlichkeit: Aufenthaltsbereich der Objekte (Punkt/Strecke/Bereich/Umgebung), Definition insbesondere der Grenzen

Tabelle 3.4: Identifikation der Lokalisierungsobjekte und ihrer Attribute aus den Use Cases

Das Ergebnis der Identifikation der Lokalisierungsobjekte und ihrer Attribute aus den Use Cases zeigt 1) *Nr. Gefahrenblatt*

1) Örtlichkeit: Aufenthaltsbereich der Objekte (Punkt/Strecke/Bereich/Umgebung), Definition insbesondere der Grenzen
Tabelle 3.4. Aufgrund ähnlicher betrieblicher Aufgaben, gleichartiger Bewegungsmuster, und ähnlicher Risikoklassen werden 7 verschiedene generische Lokalisierungsobjekte identifiziert. Die Häufigkeiten sind zwar in Abbildung 3.5 und Abbildung 3.6 zur Einstufung der Szenarien in Häufigkeits- und Ausmaßklassen enthalten, müssen jedoch anhand der Angaben im Szenarienhandbuch [9] noch näher analysiert werden, ob sie den Schadensursachen bzw. Gefährdungen entsprechen.

3.4.1 Feststellung 2

Aufgrund ähnlicher betrieblicher Aufgaben, gleichartiger Bewegungsmuster, und ähnlicher Risikoklassen werden folgende 7 verschiedene generische Lokalisierungsobjekte identifiziert.

1. Fahrzeuge
2. Informationen
3. Infrastruktureinrichtungen
4. Menschen
5. Geräte und Instandhaltungsartefakte
6. sonstige Objekte
7. Naturobjekte

3.5 Lokalisierungsattribute und Anforderungen

Unter Lokalisierungsattributen werden alle Eigenschaften, Merkmale, Werte und Einheiten sowie Zahlenwerte von Lokalisierungsgrößen verstanden, die insgesamt zur Charakterisierung von Lokalisierungsobjekten, von Lokalisierungsfunktionen und betrieblichen Nutzungen sowie insbesondere von Anforderungen an Lokalisierungssysteme dienen.

Zu den Lokalisierungsgrößen der Lokalisierungsobjekte gehören explizit:

- Identifikator des Lokalisierungsobjektes und dessen Parameter
- Position des Lokalisierungsobjektes mit spezifischem Bezugspunkt und Angabe der Bezugskoordinatenpunkte im Bezugskoordinatensystem und seiner Messqualität
- Weitere Informationen wie ggf. Bewegungsverhalten, Geschwindigkeit, Bewegungsrichtung,...

Da Genauigkeit, Integrität und Kontinuität für die definierten Use Cases des Eisenbahnsystems im Zusammenhang mit den Anforderungen für Eisenbahnsysteme nach CENELEC EN 5012x zu verstehen sind, werden diese Eigenschaften in ihrer Qualität für die Nutzung im Eisenbahnsystem nach Maßgabe der Use Cases qualifiziert. Um daraus Anforderungen seitens der Nutzung herzuleiten, werden die erforderlichen Eigenschaften wie

- Genauigkeit,
- Integrität,
- Kontinuität,
- Verlässlichkeit (RAMSS)
- usw.

mit ihren spezifischen Charakteristika u.a. unter Nutzung der allgemein anerkannten Regeln der Technik (AART) und jüngerer wissenschaftlicher Veröffentlichungen definiert und umfassend zusammengestellt. Insbesondere wird dabei eine Definition und Überführung der vorwiegend aus der Luft- und Raumfahrt herrührenden Eigenschaften und Größen in die Begriffswelt des Eisenbahnwesens nach dem in [10] und in der [11] für die Qualifizierung von

satellitenbasierten Ortungssystemen erarbeiteten Ansatz durchgeführt. Dies ist eine wesentliche Voraussetzung für eine Anforderungsbeschreibung und insbesondere Qualifizierung im Rahmen von SIL nach DIN EN 50126ff.. Hierbei handelt es sich vorwiegend um Attribute der Lokalisierungsfunktion, die von dem Lokalisierungssystem zu leisten sind.
Die Eigenschaften von Lokalisierungsobjekten, einer Lokalisierung(sfunktion) und der daraus resultierenden Lokalisierungsinformation von Objekten mit dem Ziel sicherer, verlässlicher und effizienter einschließlich wirtschaftlicher Eisenbahnsysteme im Zusammenhang mit den Anforderungen nach DIN EN 50126 ff. werden methodisch durch eine Abstraktionshierarchie verschiedener Eigenschaften und Merkmale charakterisiert (z.B. [12] oder ggf. nach Lastenheften der SBB, o.a. [9], [13], [10], [11], [6] usw.).

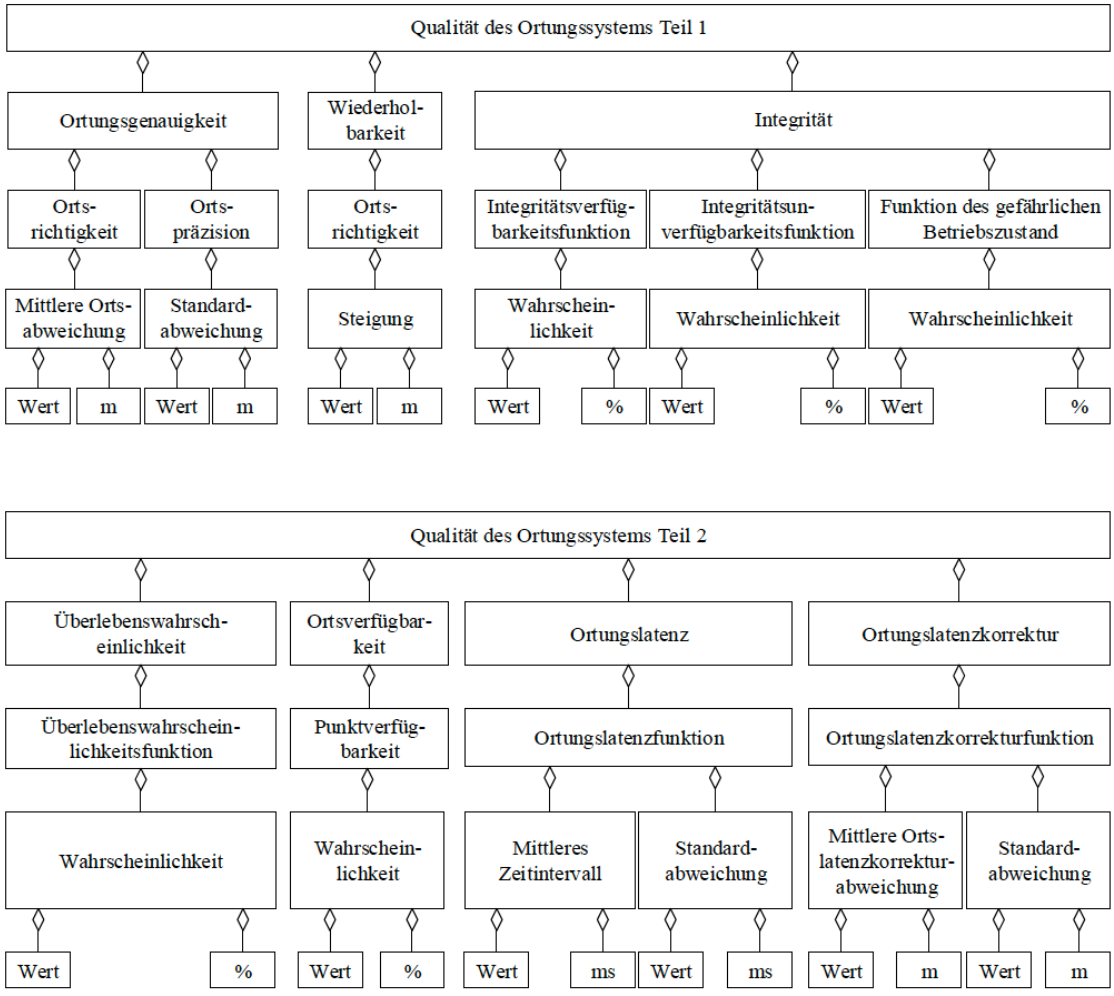


Abbildung 3.5: Attribute von Lokalisierungsobjekten,-funktionen und -nutzungen [11]

Speziell zur Charakterisierung der Genauigkeits- und Zuverlässigkeits- sowie Sicherheitsmerkmale (RAMSS) und ihrer notwendigen Quantifizierung und damit möglichen Qualifizierung wird das Schema der Abstraktionshierarchie genutzt. Mit Hilfe dieser Abstraktionshierarchie werden anfangs noch nicht näher definierte Begriffe nach einem hierarchischen Schema weiter ausdifferenziert, indem zuerst diese in Form von Eigenschaften noch sprachlich beschrieben werden und in einem nächsten Gliederungsschritt mit Hilfe einer weiteren

formalisierten Präzisierung durch vorwiegend physikalische Größen oder unterscheidbare Merkmale definiert. Diese werden im Einzelnen durch (mathematische) Funktionen und Größen mit Werten definiert und (später durch Variationen zur Optimierung) quantifiziert werden. Sie bilden auch die Grundlage für eine Verifikation im Zusammenhang mit der für die Zulassung benötigten Qualifikation zur Nachweisführung.

Methodisch werden dazu für die Eigenschaften einer Objektlokalisierung wie Genauigkeit, Integrität und Kontinuität u.a. die grundsätzlichen Merkmale und Größen für eine Lokalisierung nach einem kürzlich entwickelten Ansatz zusammengestellt und präzisiert, da diese Eigenschaften im Eisenbahnbereich im Kontext der Normenreihe DIN EN 50126 ff. zum Teil anders als im Avionikbereich interpretiert werden ([10], [11]). Abbildung 3.5 zeigt nach dem Strukturierungsschema der Attributhierarchie gegliederte Attribute von Lokalisierungsobjekten, -funktionen und -nutzungen.

Die Merkmale der Lokalisierungsgenauigkeit, nämlich Richtigkeit und Präzision selbst werden neuerdings mit Mahalonobis-Ellipsen besser als durch die üblichen Eukliddistanzen charakterisiert [14]. Diese haben den Vorteil, dass die Präzision in einem räumlichen Koordinatensystem definiert wird, welche die besonderen Eigenschaften von Bewegungen, z.B. in Fahrtrichtung und quer dazu, z.B. zur Gleisselektivität, besonders adressiert, wie der Vergleich in Abbildung 3.6 zeigt. Entscheidend für die Wahl einer Qualifikation von Lokalisierungssystemen im Eisenbahnbereich ist weiterhin die Referenzierung des Koordinatensystems. Anstatt der üblichen Nord-Süd-Ausrichtung ist eine objektbezogene, orts- und zeitbezogene Darstellung (Messbedingungen) mit Translations- und Vertikalkoordinaten sinnvoller (vgl. Abbildung 3.6). Insbesondere werden darin auch die Abhängigkeiten der Lokalisierungsgenauigkeit von Geschwindigkeit in Bewegungsrichtung und Winkelgeschwindigkeit der Objekte besonders deutlich.

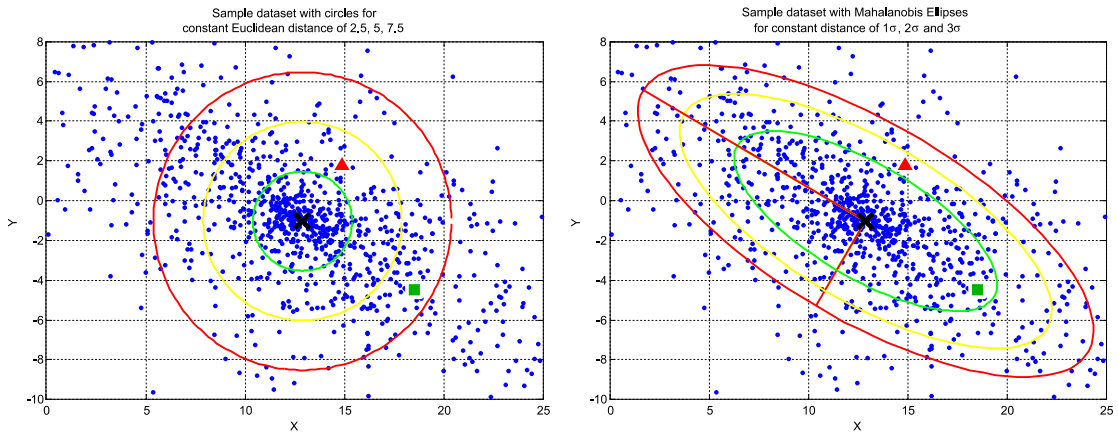


Abbildung 3.6: Beispiel-Dataset mit euklidischen Distanzkreisen (links) und konstanten Mahalanobis-Distanz-Ellipsen (rechts)

Die Ortsintegrität beschreibt den Grad des Vertrauens in die gelieferten Ortungsinformationen und die Fähigkeit des Systems, eine Warnung auszugeben, wenn es nicht mehr für die Ortsbestimmung genutzt werden sollte.

Die Überlebenswahrscheinlichkeit ist die Fähigkeit eines Systems, die spezifizierten Anforderungen ohne Unterbrechung einzuhalten, wenn die äußeren Hilfsmittel bereitgestellt sind.

Die Punktverfügbarkeit ist ein Maß für die Fähigkeit einer Betrachtungseinheit, zu einem gegebenen Zeitpunkt funktionstüchtig zu sein. Die Punktverfügbarkeit wird als relative Häufigkeit und damit als Wahrscheinlichkeit ausgedrückt, dass die Betrachtungseinheit zu einem bestimmten Zeitpunkt die geforderte Funktion unter den vorgegebenen Arbeitsbedingungenausführt. Die Punktverfügbarkeit wird genau für einen Zeitpunkt definiert, wohingegen die mittlere Verfügbarkeit für ein Zeitintervall spezifiziert ist. Die stationäre Verfügbarkeit bezieht sich auf den Betrachtungsraum der Unendlichkeit.

Wird ein Messergebnis als Grundlage einer Datenfusion genutzt, ist der Zeitpunkt der Bereitstellung der Ortsdaten an der Ausgabeschnittstelle bedeutend. Für diesen Fall ergibt sich eine kombinierte Messabweichung aus der Messabweichung im statischen Fall und der Messabweichung durch die zeitlich verzögerte Bereitstellung. Die Messabweichung durch die verzögerte Bereitstellung wird als Ortungslatenzkorrektur bezeichnet.

Zur Herleitung der qualitativen Basisanforderungen werden zuerst qualitative Begriffe formuliert und strukturiert, auf deren Grundlage dann für die einzelnen Lokalisierungsfunktionen von Lokalisierungsobjekten deren spezifische Werte ermittelt werden. Zu unterscheiden sind dabei die Messinformationen, d.h. die Attribute des Mess-Lokalisierungszustands des Lokalisierungsobjekts (Tabelle 3.5) und zum anderen die Attribute der Lokalisierungsfunktion (Tabelle 3.6).

Zur Vollständigkeit werden auch noch die Eigenschaften für die Anforderung des Lokalisierungssystems in der Tabelle 3.7 aufgeführt, die nicht in den ersten beiden Kategorien enthalten sind. Darin sind auch weitergehende Anforderungen zu technischen und betrieblichen Aspekten sowie zur Qualifizierung, Nachweisführung, und Zulassung sowie zu Rückwirkungen bei Implementierung und technische Migration, zu betrieblichen Auswirkungen/Änderungen als Voraussetzung bzw. Rückwirkung und ebenfalls zu rechtliche Auswirkungen/Änderungen als Voraussetzung bzw. Rückwirkung enthalten.

Eigenschaft	**Merkmal**	**Größe**	**Einheit**
Lokalisierungsobjekt	Identifikator	spez. Nr.	
	Definition		
	Vorkommen, Lage		
	Abmessungen	Breite, Höhe, Tiefe	m
	Aufenthaltsbereich		
Ortsverfügbarkeit	Kontinuierlich		
	Diskret		
Relevanz			
Nutzungs-funktionen			
Lokalisierungs-koordinaten	Bezugskoordinatensystem	Topologisch Geografisch	

Eigenschaft	Merkmal	Größe	Einheit
		Odometrisch	
	Bezugskoordinaten-punkt		
Bewegungszustand	phys. Zustandsgrößen und Datenformate	Position 3D	
		Datenformate	
		Auflösung	
		Geschwindigkeit 3D	
		Datenformate	
		Auflösung	
		Beschleunigung 3D	
		Datenformate	
		Auflösung	

Tabelle 3.5: Messinformationen - Attribute von Lokalisierungsobjekten

Eigenschaft	Merkmal	Größe	Einheit
Genauigkeit der Position	3D-Verteilungsfunktion bzw. Histogramm Mahalonobis-Ellipse	Richtigkeit (3D) Achsen-Streuung 3D	m
		Präzision	m
Genauigkeit der Geschwindigkeit	3D-Verteilungsfunktion bzw. Histogramm Mahalonobis-Ellipse	Richtigkeit Achsen- –Streuung 3D	
		Präzision	
Kontinuität, Reliability (Überlebenswahrscheinlichkeit) für Position (3D)	Überlebenswahrscheinlichkeit-pdf	MTT(E)F (Mean time to (extended) Failure	m
Kontinuität für Geschwindigkeit	Überlebenswahrscheinlichkeit-pdf	MTT(E)F	m
Sicherheitsintegrität		SIL	
		Alarmgrenze	m
		Time to Alarm	s
		MTTHE (Mean time to hazar-dous event	h
Verfügbarkeit	Punktverfügbarkeit		
	Dauerverfügbarkeit		
Störresistenz	Spamming		
	Spoofing		
Dynamik	Abtastzeit-Verteilungsfunktion	Mittelwert Streuung	
	Synchronität	Zeitstempel	
	Latenz	Latenzdauer	s
Wiederholbarkeit			

Tabelle 3.6: Messinformationen - Attribute von Lokalisierungsfunktion

Eigenschaft	Merkmal	Größe	Einheit
Kosten		Investitionskosten	Euro
		Betriebskosten	Euro/Jahr
Abmessungen	3D	Länge	m
		Höhe	m
		Breite	m
Einbauorte	Sensoren		
	Kabel		
	Zentraleinheit		
	Lage		
Montage/ Anbringung			
Leistungsbedarf(e)	Zufuhr el. Energie		W
	Abfuhr thermischer Energie		W
Umweltanforderung	Emission Material RoHS (EU)		
Umgebungs-bedingungen	Schutzart		IP
	Emission EMV		Klasse
	Immission EMV		
	mechanisch Stoß Rütteln Schock usw.		
Brandschutz	Feuerwiderstandsklassen, Brandlast		
Schutz vor Manipu-lation	Widerstandsklasse		
Schnittstellen	informations-technisch		
Nachweisbarkeit nach DIN EN 50129 [15]	Erstellung der Sicherheits-nachweise (technische Si-cherheitsberichte)		
Qualifizierung/ Zertifizierung	Rahmen Normen Institution		
Bedienbarkeit	Kalibrierung		
	Konfigurierung		
	Parametrierung		
Instandhaltbarkeit	Instandhaltungskonzept	MTTR	
Auf-/Abrüstung	Dauern	s	
Begutachtung			
Rückwirkungen bei Implementierung			
technische Migrati-on			
betriebliche Migra-tion	ggf. ist eine Anpassung der Betriebsregeln erforderlich		

Eigenschaft	Merkmal	Größe	Einheit
normative Migration	ggf. ist eine Anpassung von Regelwerken erforderlich		
CSM RA			
behördliche Zulassung			
Interoperabilität	ETCS-Konformität		
	Schnittstellenkompatibität	technisch	
		Datenformat	
		funktional	

Tabelle 3.7: Technische, betriebliche und organisatorische Attribute von Lokalisierungssystemen

Diese Qualitätseigenschaften korrespondieren später mit den Angaben über die Leistungsfähigkeit der Sensortechnologien. Der Vorteil einer harmonisierten Beschreibung von Eigenschaften einzelner Lokalisierungstechnologien besteht dahin, die Vor- und Nachteile durch eine geeignete Sensordatenfusion und Systemkonstellation in eine Gesamtlösung (siehe Kapitel 6) sowie unter Berücksichtigung CENELEC-konformer Anforderungen und Qualifizierung in vergleichbarer und einheitlicher Weise zu nutzen.

Mit diesen neuen, aber bereits methodisch bewährten Ansätzen (vgl. [16]) werden die einzelnen Szenarien einerseits systematisch analysiert und strukturiert und andererseits daraus auch quantifizierbare Anforderungen hergeleitet.

3.5.1 Feststellung 3

Tabelle 3.5, Tabelle 3.2 und Tabelle 3.6 enthalten alle Merkmale für eine umfassende qualitative Beschreibung von Anforderungen bezüglich Lokalisierungszustand und Lokalisierungsfunktion die hinsichtlich der quantitativen Anforderungen und der Qualifizierung von Lokalisierungssystemen notwendig sind.

3.5.2 Feststellung 4

Tabelle 3.7 enthält alle Merkmale für eine umfassende qualitative Beschreibung von technologischen, betrieblichen und organisatorischen Anforderungen.

3.6 Genauigkeits- und Sicherheitsanforderungen

Vorgehensweisen zur Ermittlung von Genauigkeits- und Sicherheitsanforderungen

Zur Herleitung der Anforderungen aus den Use Cases gibt es mehrere Ansätze, die Abbildung 3.7 veranschaulicht.

Zum einen können aus den Use Cases oder aus unabhängigen Annahmen bestimmte Sicherheitsanforderungen mit verschiedenen Methoden hergleitet werden. Diese Sicherheitsanforderungen können nur mit definierten Genauigkeiten erzielt werden, woraus wiederum

bestimmte Betriebsleistungen resultieren. Diese Vorgehensweise wird im rechten Teil von Abbildung 3.7 dargestellt. Ein Beispiel ist die Herleitung von Anforderungen an die Lokalisierungsgenauigkeit aus der generischen Sicherheitsanforderungsstufe SIL 4

Zum anderen können in umgekehrter Weise aus den Use Cases bestimmte betriebliche Anforderungen an die Systemleistung oder die Betriebsverfahren hergeleitet werden, welche bestimmte Genauigkeiten der Lokalisierung verlangen, welche zu bestimmten Sicherheitsleistungen führen. Diese Vorgehensweise wird im linken Teil von Abbildung 3.7 dargestellt. Ein Beispiel für diese Vorgehensweise ist die Herleitung der Anforderungen für die Genauigkeit und anschließend der Sicherheitsintegrität auf der Basis von Use Cases

Allerdings können erst durch eine Iterative Synthese der Anforderungen Sicherheit, Genauigkeit und Systemleistung im Zusammenhang aufgestellt werden. Ihre Erfüllung im Lokalisierungssystem wird durch Konfigurierung und Parametrierung realisiert. In diesem Zusammenhang muss auch erwähnt werden, dass diese neuartige Lokalisierung ggf. auch neue Betriebsregeln und ggf. Änderung der Regelwerke erfordern könnte, was einen nicht unerheblichen zeitlichen und personellen Aufwand erfordert.

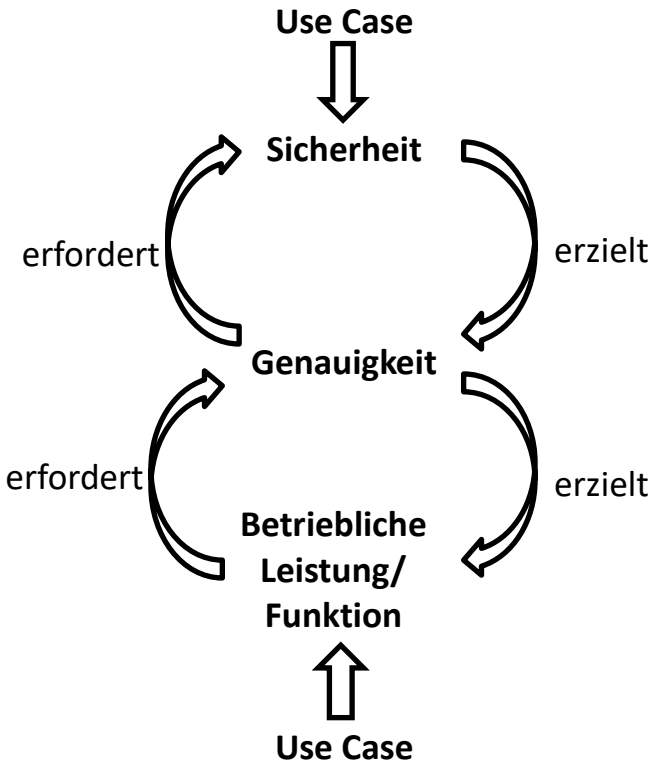


Abbildung 3.7: Vorgehensweisen zur Ermittlung von Genauigkeits- und Sicherheitsanforderungen

Anforderungen an Genauigkeit und Sicherheit stehen in einem kontraproduktiven Spannungsverhältnis. So ist leicht nachvollziehbar, dass eine niedrige Genauigkeit mit einem hohen Sicherheitsniveau realisiert werden kann und umgekehrt eine hohe Genauigkeit und hohe Sicherheitsanforderungen sehr anspruchsvolle Ziele sind. Die vordergründig triviale Aussage hat jedoch entscheidende Auswirkung auf die Merkmale einer Genauigkeitsanforderung. Die Genauigkeit wird in der Regel durch das Merkmal einer Werteverteilung ange-

geben. Für die Verwendung im Eisenbahnwesen ist daher die Art der Verteilung ausschlaggebend. Beispielsweise werden zum Zwecke der Sicherheitsgewährleistung bei einer Verteilung die äußeren Teile, die sog. Schwänze besonders betrachtet. Die außerhalb einer bestimmten Grenze liegenden Flächen der Verteilung dürfen nicht die zur zulässigen Ausfallrate zugehörige Wahrscheinlichkeit überschreiten.

Eine Lösung basiert auf dem Ansatz, dass die eine angenommene Dichtefunktion der Lokalisierungsmesswerte aus einer Häufigkeitsverteilung resultiert, wobei n Messwerte in einem Intervall der Dauer $T = \Delta \cdot n$ ermittelt wurden. Darin ist die Anzahl n_F die Zahl der fehlerhaften Messwerte, die irgendwann während der Messdauer T mit der Abtastperiode Δ anfallen und die mit der Gefährdungsrate korrespondieren sollen.

In einer Gleichung wird dieser Sachverhalt folgendermaßen beschrieben:

$$\lambda_H = \frac{n_F}{T} \tag{1}$$

Die Fehlerwahrscheinlichkeit bzw. relative Häufigkeit

$$P_F = \frac{n_F}{n} \tag{2}$$

kann durch eine einfache Erweiterung mit n in Formel (1) eingesetzt werden

$$\lambda_H = \frac{n_F}{T} = \frac{n_F \cdot n}{n \cdot T} = P_F \frac{n}{T} = P_F \frac{1}{\Delta} \tag{3}$$

Die weitere Herleitung basiert auf der zutreffenden Annahme, dass die relative Häufigkeits- bzw. Wahrscheinlichkeitsverteilung unabhängig von der Abtastrate ist (zentraler Grenzwertsatz) und eine Verteilung einer Stichprobe die gleiche Verteilungsfunktion hat. Somit gilt aber absolut, dass je kürzer abgetastet wird, desto mehr Fehler auftreten.

Mit (3) nach P_F aufgelöst erhält man für die gesuchte maximale Fehlerwahrscheinlichkeit

$$P_F = \lambda_H \Delta \tag{4}$$

Somit ist die Fehlerwahrscheinlichkeit nicht nur von der gegebenen Gefährdungsrate, sondern auch von der Abtastzeit proportional abhängig.

Mit Zahlenwerten wird dieser Ansatz konkretisiert. Für eine Abtastzeit von Δ = 1 sec und der angegebenen Gefährdungsrate λ_H = 10-9/h für SIL 4 erhält man

$$P_F = \lambda_H \Delta = \frac{10^{-9}}{\mathrm{h}} \cdot 1\mathrm{s} = \frac{10^{-9}}{3600\ \mathrm{s}} \cdot 1\mathrm{s} = 2{,}8 \cdot 10^{-12} \tag{5}$$

Die komplementäre Wahrscheinlichkeit $P_K$einer richtigen Messung liegt bei

$$P_K = 1 - P_F = 1 - 2{,}8 \cdot 10^{-12} = 0{,}999\,999\,999\,997\,2 \tag{6}$$

Bei der - rein hypothetischen - Annahme, dass die Messwerte normalverteilt sind, kann der Anteil außerhalb des zulässigen Intervalls als Vielfaches der Streuung berechnet werden.

Damit ist die k-fache Streuung (Präzision) ein Maß für die Fehlerwahrscheinlichkeit. Aus Tabellenwerken oder interaktiven Programmen (http://matheguru.com/stochastik/31-normalverteilung.html) erhält man für diesen Wahrscheinlichkeitswert etwa das 7-fache der Streuung. Der exakte Wert für die Wahrscheinlichkeit innerhalb des Intervalls ist 0,999 999 999 997440.

Bei einer Annahme, dass die Messungen eine Streuung von 2 m aufweisen, ist das zugehörige Intervall dann 14 m. Veränderungen ergeben sich einerseits durch Variationen des Abtastintervalls und andererseits durch den Wert der Streuung.

Umgekehrt wäre, wenn eine Gleisselektivität mit einem zulässigen Intervall von +/-1,5 m = 3 m gefordert wäre, eine Streuung von 1,5m/7 = 0,215m erforderlich. Hierbei wird von einer erfüllten Richtigkeit ausgegangen, d.h. Mittelwertfreiheit.

Dieser Ansatz wurde in den 1980er Jahren von einer Deufrako Arbeitsgruppe zur Wegmessung insbesondere hinsichtlich seiner Praktikabilität und seiner Schlüssigkeit diskutiert und durch einen anderen Ansatz ersetzt. Dieser Ansatz geht nicht mehr von der Voraussetzung aus, dass die Verteilungsfunktion parametrisch beschrieben wird. Es werden für das zulässige Messunsicherheitsintervall obere und untere Grenzen bestimmt. Hinsichtlich dieser Grenzen wird durch redundante Maßnahmen eine Detektion der Überschreitung definiert. Die Redundanz der Maßnahmen ergibt sich einerseits aus der Messqualität der redundanten Sensoren und andererseits aus der geforderten Sicherheitsintegritätsstufe. Damit kann ein Fail-safe Verhalten realisiert werden. Einzelheiten zu dieser Methodik sind in [17] beschrieben.

Der damals diskutierte Ansatz berücksichtigt insbesondere auch die Eigenschaften der neuen satellitenbasierten Lokalisierung. Denn hier kann sowohl keine Normalverteilung der gemessenen Positionswerte als auch der durch die Fusionsalgorithmen berechneten Werte zu Grunde gelegt werden. Es wird häufig vereinfachend angenommen, dass die Messabweichungen normalverteilt, unkorreliert und mittelwertfrei seien. Sowohl aus praktischen Erfahrungen als auch aus theoretischen Überlegungen folgt, dass diese drei Vereinfachungen unzulässig sind.

Als Resultat dieser Betrachtung wird für die Angabe der Genauigkeit für das Merkmal eine Anforderung in Form einer einhüllenden Gleichverteilung mit oberer und unterer Grenze bezüglich eines Mittelwertes empfohlen. Um die Qualität des Systems abhängig vom aktuellen Redundanzstatus zu beschreiben, kann als weiteres Merkmal ein Vertrauensintervall mit spezifischer statistischer Sicherheit verlangt werden. Die komplementäre Wahrscheinlichkeit, dass Werte außerhalb der Gleichverteilung liegen, entspricht damit einer Gefährdungswahrscheinlichkeit.

3.6.1 Feststellung 5

Für die Anforderung zur Genauigkeit wird als Merkmal eine einhüllende Gleichverteilung mit oberer und unterer Grenze bezüglich eines Mittelwertes empfohlen. Um die Qualität des Systems abhängig vom aktuellen Redundanzstatus zu beschreiben, kann als weiteres Merkmal ein Vertrauensintervall mit spezifischer statistischer Sicherheit verlangt werden.

3.7 Verfügbarkeit

Hinsichtlich der Verfügbarkeitsanforderungen muss noch der Einsatzfall spezifiziert werden. So kann zum Beispiel im Fall abgestellter Fahrzeuge keine unmittelbare Energieversorgung vorhanden sein. Mit der genormten Definition der Verfügbarkeit z.B. Nach IEV 191-02-05 ist die Verfügbarkeit die „Fähigkeit einer Einheit, zu einem gegebenen Zeitpunkt oder während eines gegebenen Zeitintervalls eine geforderte Funktion unter gegebenen Bedingungen erfüllen zu können, vorausgesetzt, dass die erforderlichen äußeren Hilfsmittel bereit gestellt sind“. Mit dieser Definition kann die Verfügbarkeit nur gewährleistet werden, wenn die Energieversorgung als äußeres Hilfsmittel vorhanden ist. Um diese Forderung auch zu erfüllen, muss die Lokalisierung auch die Energieversorgung ggf. einschließen. Damit müssen die Arbeits- bzw. Betriebsbedingungen im Einzelnen spezifiziert werde. So kann z.B. bei abgestellten Fahrzeugen eine dynamische Lokalisierung oder Initialisierung ereignisspezifisch verlangt werden. Ggf. ist eine permanente Speicherung der zugehörigen Lokalisierungsinformation zu fordern. Damit muss die Verfügbarkeitsangabe spezifisch erfolgen. Hierfür bieten sich die Definitionen der up time und down time nach IEC 191-42 an, die Abbildung 3.8 darstellt. In diesem Zusammenhang sind folgende Dauern zu fordern und zu quantifizieren:

- Up time (Klarzeitintervall)
- Operating time (Betriebszeit/ -dauer)
- Idle time (Leerlauf Dauer)
- Standby time (standby, Dauer des betriebsbereiten Zustands)
- Externally disabled time (extern bedingtes Nichtverfügbarkeitszeitintervall)

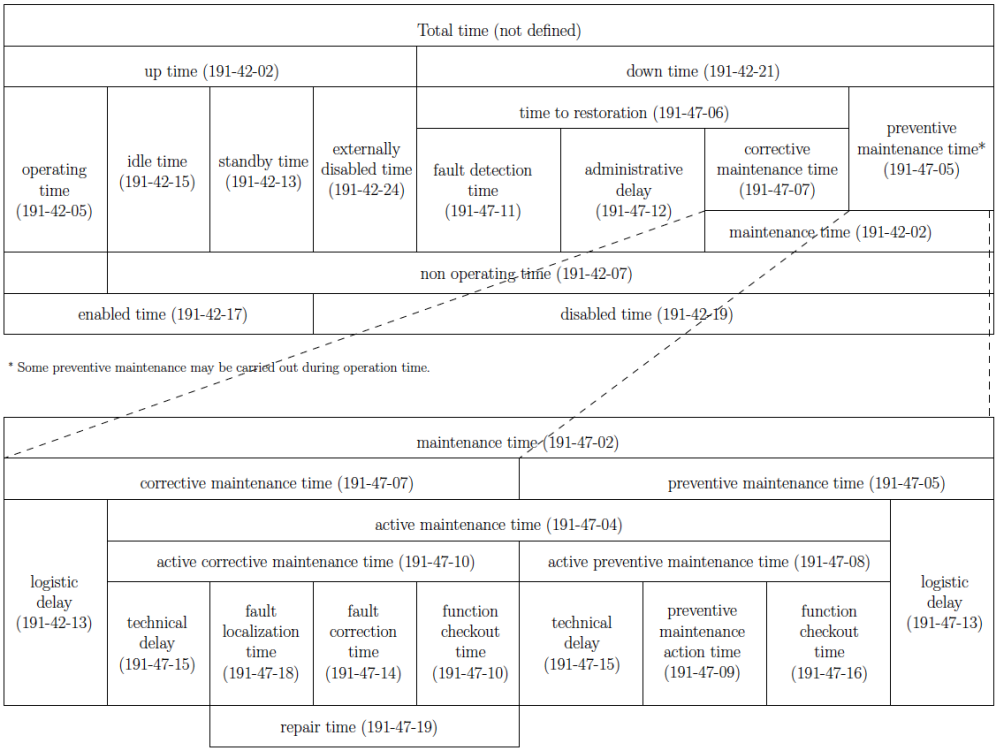


Abbildung 3.8: Definitionen der up time und down time nach IEC 191-42 (Habilitation Müller)

3.8 Basisanforderungen

Die Auflistung der Anforderungskategorien ist sehr umfassend, enthält aber dadurch eine weitgehende Vollständigkeit. Diese ist insbesondere für die einzelnen Sensorkomponenten von Lokalisierungssystemen hilfreich, um eine Vergleichbarkeit der relevanten Lokalisierungs-attribute ähnlicher Sensorsysteme zu ermöglichen. Weiterhin kann mit Hilfe dieser Kategorien eine normgerechte Qualifizierung erfolgen und darüber hinaus sind diese Eigenschaften für die Architektur hinsichtlich der Sensordatenfusion bedeutsam.

Für das Lokalisierungssystem in seiner Gesamtheit können einzelne Anforderungskategorien eine geringere Priorität bekommen. Durch eine Priorisierung werden daraus die unmittelbaren Basisanforderungen hinsichtlich des Lokalisierungszustands und der Lokalisierungsfunktion extrahiert, die in Tabelle 3.8 zusammengestellt sind. Die Tabelle ist in Anlehnung an eine FMECA (failure modes, effects, and criticality analysis) für das Gefährdungsobjekt aufgebaut und enthält auch die Bezüge zu den Lokalisierungsobjekten, zu der betrieblichen Funktion und zu den betrieblichen Risiken.

Herleitung von Anforderungen an die Lokalisierungsparameter bei einfachen betrieblichen Funktionen und Use Cases (Ein Blatt je Gefährdung)			
Anforderungsblatt Nr.			Version:
Bearbeiter			am:
Freigabe			am:
Geprüft			am
Nr.	System/	Systemmerkmal/-größe	

1	Eigenschaft		
1.1	Bezugs-Objekt (Lokalisierungs-objekt)	Name, ID	
1.2		Bezugspunkt	
3		Bewegungsmuster	
4	Bezugspunkt Systemarchitektur		
5	Use Case		
	Betriebliche Funktion/ Teilfunktion		
6	Gefährdung	Art	
7		Ursache insbes. wg. Ortung	
8	Exponat (Gefährdetes Objekt)	Typ	
9		Expositionshäufigkeit	
10		Stoch. Unabhängigkeit	
11	Sicherheit/Risiko	Unfallart	
12		Schwere	
13		relative Häufigkeit	
14		Sicherheitsintegritätsstufe	
15	Risiko Referenz	Referenzfunktion	
16		Referenzrisiko	
17	Genauigkeit	Position x longitudinal Restfehlerwahrscheinlichkeit	
18		Position y transversal Restfehlerwahrscheinlichkeit	
19		Position z-Richtung Restfehler-wahrscheinlichkeit	
20		Geschwindigkeit longitudinal Restfehlerwahrscheinlichkeit	
21		Geschwindigkeit transversal Restfehlerwahrscheinlichkeit	
23	Verfügbarkeit		
24		Überlebensfähigkeit, Ausfallrate	
25		Instandhaltungsfähigkeit Herstellungsrate	
26			
27	Latenz	Art, Typ	
28		Ursache	
29		Dauer	

Tabelle 3.8: Basisanforderungen des Lokalisierungszustands und der Lokalisierungsfunktion

3.8.1 Feststellung 6

Tabelle 3.8 enthält alle Merkmale und Größen, die für eine umfassende qualitative und quantitative Beschreibung von metrologischen Basisanforderungen des Lokalisierungszustands und von Verlässlichkeitsanforderungen der Lokalisierungsfunktion von allen relevanten Objekten der Use Cases notwendig sind.

3.9 Quantitative Anforderungen an die Messqualität einer Lokalisierung

Aus der Zuordnung von Lokalisierungsobjekten zu den definierten betrieblichen Anwendungsfunktionen resultieren entsprechende Anforderungen an die konkreten Werte der in den qualitativen Zusammenstellungen in Tabelle 3.5, Tabelle 3.6 und Tabelle 3.7 betreffenden Merkmalen und Größen. Z.B. wird für eine Gleisfreimeldung eine gewisse Genauigkeit durch quantitative Angabe der Verteilungsfunktionen der Messrichtigkeit und der Präzision in Gleisrichtung sowie in Querablage erforderlich sein. Hierfür kann z.B. die Anforderung der Balisenposition aus ETCS Subset-036 FFFIS herangezogen werden. Möglich sind auch Angaben über die Messunsicherheit oder über ein Vertrauensintervall und dessen Grenzen.

Quellen für die Ermittlung der Anforderung sind

- Analogie aus bestehenden Regelwerken oder Lastenheften (VDV 331 [18], 332 [19], ETCS TSI, Cenelec-Normen [15], UIC Merkblätter (Leaflets), LZB Lastenheft,..)
- aus Forschungsprojekten z.B. SatLoc, GaloROI, [16], [20]
- Betriebliche Leistungsfähigkeit (Zugfolge, Durchrutschweg)
- aus der Sicherheitsbetrachtung
- Aus Simulationen
- Aus Erfahrung
- Aus Expertenbefragungen

So resultieren aus der vorwiegend betrieblichen Nutzung mehr oder weniger Anforderungen, während die Lokalisierungsobjekte typische Eigenschaften hinsichtlich der Lokalisierung aufweisen, z.B. Bewegungsmuster und -areale. Beispielsweise erfordert der Use Case 1.4 „Präzise Zugspitzenposition für ETCS-Prozess“ spezielle Werte der Eigenschaften Genauigkeit, Integrität und Kontinuität für eine Bremskurvenberechnung und Überwachung nach ETCS Subset-26. Diese Anforderungen werden bezüglich des Lokalisierungsobjekts Zugspitze genau bestimmt.

Ein weiteres Beispiel ist die Gleisfreimeldung (GFM), welche sich auf den gesamten Zugverband als Lokalisierungsobjekt bezieht. Hier sind neben den Eigenschaften Genauigkeit, Integrität und Kontinuität auch die Latenzdauern von Bedeutung, um einerseits für die Funktion der verlässlichen und schnellen Gleisfreimeldung auch die betriebliche Leistung einzubeziehen. Und weiterhin wird auch hier die erforderliche Änderung bei Wegfall der infrastrukturseitigen GFM berücksichtigt.

Für die Fallstudie wurden die quantitativen Werte der einzelnen Größen ermittelt und in eigens ausgefüllten Tabellen nach dem Muster der Tabelle 3.8 eingetragen

Beispiele für Anforderungen aus der Literatur und anderen Quellen sind in Tabelle 3.9 und Tabelle 3.10 angegeben.

Properties	Characteristics	Value and Unit
Accuracy	95% confidence level	10 m
Reliability*	failure rate	$\lambda_{all} < 2 \times 10^{-4}/\ hour$
Availability*	percentage	99.98%
Safety Integrity	hazard rate	$\lambda_{DU} \leqslant 4.77 \times 10^{-6}/\ hour$
	alarm limit	20 m
	time to alarm	$\leqslant$ 1 sec
	safety margin	real-time calculated

** For reliability and availability analysis, HDOP > 6 should also be excluded.*

Characteristics	FRP* [133]	GPS SPS [22]	RTCA APV-I [134]	Railway** [135]
Horizontal Accuracy (95%)	1 - 20 m	$\leqslant$ 7.8 m	16 m	10 m
Vertical Accuracy (95%)			4 - 6 m	
Continuity Risk	TBD	2×10^{-4}/ h	8×10^{-6}/15 sec	2×10^{-4}/ h
Availability	> 95%	> 98%	99% - 99.99%	> 99.98%
Integrity Risk	TBD	1×10^{-5}/ h	2×10^{-7}/ 150 sec	TBD
Alarm Limit	2 - 20 m	34.48 m	40 m	20 m
Time to Alarm	5 sec	< 6 hour	6 sec	1 sec
Protection Limit	n.a.	n.a.	40 m	n.a.

TBD: To Be Defined, n.a.:not available

* Among the FRP applications, the navigation and route guidance is used here.

** The railway advisory uses the train control on medium density line as an example.

Tabelle 3.9: Angaben für Anforderungen für Lokalisierung für Züge auf mittel beanspruchten Strecken [10]

Tabelle 3.10: Angaben für Anforderungen für Lokalisierung für Züge aus mehreren Quellen **[10] [21] [22]**

3.9.1 Feststellung 7

Für die Anforderung zur Messqualität kann auf vergleichbare Angaben aus den ETCS Subsets für die Balisen und die Odometrie zurückgegriffen werden.

3.9.2 Feststellung 8

Für die Anforderungen an die Genauigkeit ist als Merkmal die Angabe in Form einer Gleichverteilung mit definierten Grenzen zweckmäßig. Häufigkeiten außerhalb der Grenzen werden durch die Sicherheitsanforderungsstufe definiert.

3.10 Qualitative Herleitung von Sicherheitsanforderungen

Eine quantitative Abschätzung der zulässigen Gefährdungsraten für eine Lokalisierungseinrichtung ist nicht einfach. Das liegt an mehreren Gründen

- Lokalisierung ist Bestandteil von Zugbeeinflussungssystemen, die Beiträge einzelner Subsysteme zum Gesamtrisiko werden nicht heruntergebrochen
- Qualitative Einschätzungen sind mit Unsicherheiten bzw. Wagheiten behaftet
- Risikoangaben existieren bezüglich der Ereignisse, werden jedoch kaum auf die individuellen Ursachen heruntergebrochen
- Vergleichbare Risiken sind nicht vorhanden bzw. dokumentiert
- Durch weitere neue auf neuer Lokalisierung beruhende Funktionen entstehen neue und unbekannte Risiken
- Modelle beinhalten Vereinfachungen, z.B. sind nicht alle Verteilungsfunktionen bzw. Häufigkeitsverteilungen durch existierende Verteilungen beschreibbar
- Angaben sind nominal und nicht metrisch skaliert
- Die Schadensrate ist nicht immer identisch mit der Gefährdungsrate
- Genauigkeit und Sicherheit stehen in enger Beziehung

Hier wird zuerst ein Vorgehen für eine erste Einschätzung des Referenzrisikos bzw. der zugehörigen Schadensrate gewählt, indem aus den existierenden Daten des Szenarienhandbuches und ggf. weiterer Quellen (Regelwerke, BAV-Projekt [23], Normen) zu den einzelnen Lokalisierungs- und darauf fußenden betrieblichen Funktionen die Lokalisierungsobjekte bzw. Gefährdungsobjekten und zuerst die Schadenshäufigkeit bestimmt wird und mit der Zahl der allgemein beteiligten Gefährdungsobjekte und der Expositionszeit in Beziehung gebracht wird und dazu noch eine untere oder obere Vertrauensgrenze mit der Chi-Quadrat-Verteilung bestimmt wird.

3.11 Gefährdungen und Gefährdungsobjekte

Ortung bzw. Lokalisierung ist eine zentrale Aufgabe im Eisenbahnwesen. Abbildung 3.3 veranschaulicht diese Aussage in einem Eisenbahnleit- und Sicherungssystem insbesondere für die Aufgaben der Sicherung und Steuerung sowie übergeordneter Funktion, wie es auch aus der Tabelle 3.3 hervorgeht.

Zur Beurteilung der erforderlichen Anforderungen an die Sicherheit der zugehörigen Lokalisierungsfunktionen geben die Gefährdungen bzw. Risiken Aufschluss. Erste Zuordnungen von Use Cases zu Risiken bzw. von Lokalisierungsobjekten zu Risiken sind in Tabelle 3.3 und 1) *Nr. Gefahrenblatt*

1) Örtlichkeit: Aufenthaltsbereich der Objekte (Punkt/Strecke/Bereich/Umgebung), Definition insbesondere der Grenzen
Tabelle 3.4 enthalten. Die noch offene Zuordnung von Use Cases zu Gefährdungsobjekten und den generischen betrieblichen Sicherungsfunktionen enthält die Tabelle 3.11.

Maßgebende Systemeigenschaft	Lange Bremswege durch geringe Haftreibung					Spurführung		
Aufgaben zur Gewährleistung der Sicherheit	Kollisionsvermeidung					Entgleisungsvermeidung		
Konfliktpartner bzw. –ort	Systemeigene Fahrzeuge			Systemfremde Verkehrsteilnehmer	Übrige Umwelt	Unstetige Stellen im Fahrweg	Stetige Stellen im Fahrweg	
Schutzfunktion	Flanken-Schutz	Folgefahrschutz	Gegenfahrschutz	Schutz an niveaugleichen Kreuzungen	Schutz vor externen Objekten	Sicherung beweglicher Fahrwegelemente	Geschwindigkeitsvorgabe	Geschwindigkeitsregelung und –überwachung
Primäre Folge bei Versagen der Schutzfunktion	Zusammenstoß			Zusammenprall	Aufprall	Entgleisung		
Use Case 1.1 „Schnelle und präzise Freimeldung Gleis, Weiche“	X	x	x	X				
Use Case 1.2 „Präzise Zugendeposition (insbesondere Güterzüge)“		x						
Use Case 1.3 „Performante „elektronische Kopplung“ von Zügen, Optimierung Zugfolgezeit“		x						
Use Case 1.4 „Präzise Zugspitzenposition für ETCS-Prozess“	X	x	x					
Use Case 1.5 „Volle und genaue Orts- und Geschwindigkeitsüberwachung in jedem ETCS Modus (FS, SH, SR, OS, TR, ..) und auch wenn ETCS OBU offline ist“	X (1.5.3)	x (1.5.4)	x					x (1.5.5)
Use Case 1.6 „Annäherungswarnung im Rangierfahrzeug“	X	x	x					
Use Case 1.7 „Real-Time Validierung des Bremsvermögens“								X
Use Case 2.1 „Präzise Warnung einzelner Menschen im Gleis“					x			
Use Case 2.2 „Absicherung von Bereichen, z.B. von Baustellen und Arbeitsprozessen im Gleis“					x			
Use Case 3.1 „Tagging von Einzelobjekten“					x			

Use Case 4.1 „Bindung von ES- oder Fahrzeugfernbedienungen an einen Ort“	(x)	(x)	(x)					
Use Case 4.2 „Automatisierte Freigabe von Gleisüberschreitungen‘				X				
Use Case 5.1 „Notbedienungsterminal für neues ETCS Stellwerk“	X	x	x	X	x	x	x	
Use Case 5.2 „Funkgleismelder-Funktionen“ (Anfrage von Fahrstrassen und Bestätigung derselben)	X	x	x	X	x	x	X	
Use Case 5.3 „Manuelle Fernsteuerung einer Lok mit ETCS Ausrüstung (via TMS/ES/RBC/ETCS OBU)“								
Use Case 6.1 „Elektronische Abbildung aller erforderlichen Ortskennt-nisse auf dem sicheren Tablet								
Use Case 6.2 „Ersatz der ETCS-Tafeln durch Anzeige auf einem GLAT Endgerät“	X	x	x					x
Use Case 7.1 „Beispiel: Kontroverse zum ETCS SR-Modus lösen“	X	x	x					x
Use Case 7.2 „Keine ortsfesten Balisen“	X	x	x					x
Keine Sicherheitsrelevanz								
Use Case 6.3 „Automatic location based services, z.B. ortsabhängige Checkliste für die Manöver mit internationalen Zügen oder automatisierte Anzeige von Versorgungsstellen“	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Use Case 8.1 „Tracking von Güterwagen, Containern, etc..“	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Use Case 8.2 „Automatisierung der Verwaltung von rangierten Güterzügen“	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Use Case 8.3 „Unterstützung Field-force-Management“	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.

Use Case 8.4 „Betriebsdatenerfassung für Arbeiten im Gleis“	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.

Tabelle 3.11: Zusammenhang zwischen Use Case und betrieblichen Sicherungsfunktionen, Funktion und Gefährdungsobjekt

Ziel ist nun, die Anforderung einer Sicherheitsqualität für eine Lokalisierungsfunktion eines Lokalisierungsobjektes zu definieren.

Die Schwierigkeit der Herleitung von Sicherheitsanforderungen für neuartige Lokalisierungsfunktionen und -systeme liegt jetzt in mehreren und neuen Aspekten der angestrebten Lokalisierung:

- Bislang ist die Ortung selbst nicht als eigenständige Komponente eines ELSS begrifflich erfasst worden. Im Gegenzug existieren nur wenige definierte Anforderungen an Lokalisierungseinrichtungen, z.B. für eine Balise im ETCS-Subset FFIS 36 [24] oder aus der Spezifikation der sog. Virtuellen Balise aus den Projekten, z.B. aus LOCOPROL [25] u.a.
- Eine Schwierigkeit besteht darin, dass zwar Sicherheitsanforderungen im Eisenbahnwesen existieren, diese sich jedoch auf umfassende Funktionskomplexe und weniger auf einzelne Komponenten beziehen, so dass die Sicherheitszuteilung, d.h. ein Rückschluss von den Sicherheitskennwerten auf Systemebene auf Komponenten einer unterlagerten Ebene schwierig ist.
- Die gleiche Schwierigkeit besteht, wenn nach dem GAMAB Ansatz vergleichbare Systeme mit bekanntem Risiko zu Grund gelegt werden sollen, da eine Rückführung von Risiken auf eine fehlerhafte Lokalisierung schwierig ist/ unzureichend analysiert bzw. dokumentiert ist.
- Die neue Lokalisierung von Lokalisierungsobjekten wird kontinuierlich durchgeführt, wenngleich die Lokalisierungsinformation nicht immer dauernd erforderlich ist, was von der betrieblichen Nutzung der Lokalisierungsfunktion abhängt.
- Es gibt neue Betriebsformen, wie Moving Block, wofür kaum vergleichbare Angaben vorliegen.
- Es gibt neue Aufgaben, wofür bisher keine Lokalisierung eingesetzt wurde, so dass keine nutzbaren Risikoangaben vorhanden sind.
- In ETCS ist keine Odometrie explizit spezifiziert
- Aus LZB sind Anforderungen an Teilwegrechner ermittelbar.

Zur Überwindung dieser Schwierigkeit bieten sich insbesondere im Kontext des europäischen normativen Rahmens folgende allgemeine Lösungsansätze

- Vergleichbare Fälle (GAMAB)
- Regelwerke (DIN 50126, CSM-Verordnung 402/2013 [26], VDV Schrift 332 [19])
- Explizite Risikoberechnung und Einordnung nach Akzeptanzkriterien.

Nach dem Prinzip GAMAB kann für eine vergleichbare Lokalisierungsaufgabe ein Risiko identifiziert werden, was als akzeptables Risiko gelten kann. Hierfür wird das Szenarienhandbuch der SBB und die Datenbank des BAV verwendet. Tabelle 3.8 zeigt eine Zuordnung von Ereignisklassen/Typen zu den jeweiligen Lokalisierungsfunktionen bzw. Lokalisierungsobjekten.

Ereignisart	Code	Szenario	H_{kl}	A_{kl}
	ZZ2.d	**Zug/Rangier; wegen technischem Versagen von Infrastrukturanlagen inkl. Fahrbahn**	**V**	**D**
	ZZ2.e	**Zug/Rangier; übrige Zusammenstösse**	**IV**	**C**
	ZZ3.a	Zug mit Objekt auf oder neben dem Gleis (ohne Baustellen)	II	B
	ZZ3.b	Zug mit Strassenfahrzeug auf Gleis (ausserhalb BÜ)	**IV**	D
	ZZ3.c	Zug mit externer Profilverletzung an Baustelle	II	B
Rangierunfall (Unfall mit Rangierbewegungen)	R1	Entgleisung	II	B
	R2	Zusammenstoss Rangier mit Objekt	II	B
	R3	Zusammenstoss Rangier/Rangier	II	B
Bahnübergangsunfall	Bü1	Technisch nicht gesicherte Bahnübergänge	**IV**	D
	Bü2	Technisch gesicherte Bahnübergänge	III	D
Gefahrgutunfall	GG1	Grosse Freisetzung; toxische Gase mit Todesopfer (schwere Schädigung)	VI	F
	GG2	Tropfender Kesselwagen (toxisch, ätzend); kleine Freisetzung	VI	E
	GG3	Freisetzung; Explosion mit Todesopfer (schwere Schädigung)	VI	F
	GG4	Brand Gefahrgut; mit Sachschaden	V	E
	GG5	Brand Gefahrgut; mit Todesopfern (schwere Schädigung)	VI	F
	GG6	Freisetzung Flüssigkeiten (wassergefährdend)	VI	F
	GG7	Unfall mit Gefahrstoffen (stationär)	V	D
Brand	**BR.a**	Rollmaterial	I	B
	BR.b	Reisezug in Tunnel	VI	F
	BR.c	Güterzug in Tunnel	V	E
	BR.d	**Gebäude**	IV	D
Naturgefahren	**N.a**	**Erdbeben: Gebäude**	VI	F
	N.b	Erdbeben: Kunstbauten (Brücken, Tunnel, Anlagen)	VI	F
	N.c	Steinschlag/Felssturz/Lawinen: Gleisanlagen, Zug	II	C
	N.d	**Hochwasser/Überschwemmung: Gebäude**	IV	D
	N.e	Hochwasser/Überschwemmung: Gleisanlagen, Zug	II	C
	N.f	Rutschung: Gleise, Anlagen	II	C
	N.g	Starkwinde	II	B
Bauwerksversagen	BV1	Einsturz einer grossen Kunstbaute (Tragsicherheit)	VI	F
	BV2	Einsturz Gebäude (Tragsicherheit)	VI	F
	BV3	Versagen Stauanlage	VI	F
Nichtberufsunfälle	NBU1	Unfälle in Haus und Garten	I	B
	NBU2	Sportunfälle	I	B
	NBU3	Verkehrsunfälle	III	D
	NBU4	Übrige Nichtberufsunfälle	I	B

Abbildung 3.9: Einstufung der Szenarien in Schadenshäufigkeits- und -ausmaßklassen [9]

Ereignisart	Code	Szenario	H_{kl}	A_{kl}
Personenunfall (ohne Mitarbeiter)	PE1	Ein-/Aussteigen	IV	D
	PE2	Im fahrenden Zug	III	C
	PE3	Vorbeifahrt von Zügen	III	D
	PE4	Durch Verlust von Fahrzeugteilen/Ladung	IV	C
	PE5	Betreten der Gleise (ausserhalb BÜ)	III	C
	PE6	Stromschlag	IV	C
	PE7	Übrige Personenunfälle	I	B
Fahrleitungsunfall	FL1	Personen verletzt durch Fahrleitung	V	C
Panik	PA1	Grosse Personenansammlung	VI	E
	PA2	Zugstillstand in Tunnel (technischer Defekt)	VI	D
Arbeitsunfall	A1	Arbeitsunfälle im Gleisbereich mit bewegten Fahrzeugen	III	D
	A2	Stromschlag	IV	D
	A3	Stolpern / Stürzen und Überbelasten	I	B
	A4	Mechanische Einwirkung	I	B
	A5	Sturz aus Höhe	II	B
	A6	Übrige Arbeitsunfälle	I	**B**
Zugstillstand	ZS1	Personenunfall nach Zugstillstand ausserhalb Tunnel	V	D
Zugentgleisung	**ZE1.a**	**Reisezug; wegen technischem Versagen des Rollmaterials**	**IV**	**C**
	ZE1.b	**Reisezug; wegen menschlichen Fehlhandlungen**	**IV**	**C**
	ZE1.c	**Reisezug; wegen technischem Versagen von Infrastrukturanlagen inkl. Fahrbahn**	**IV**	**C**
	ZE1.d	**Reisezug; wegen lückenhafter Technik**	**IV**	**C**
	ZE1.e	**Reisezug; übrige Entgleisungen inkl. Naturgefahren**	**IV**	**C**
	ZE2.a	**Güterzug; wegen technischem Versagen des Rollmaterials**	**IV**	**C**
	ZE2.b	**Güterzug; wegen menschlichen Fehlhandlungen**	**IV**	**C**
	ZE2.c	**Güterzug; wegen technischem Versagen von Infrastrukturanlagen inkl. Fahrbahn**	**IV**	**C**
	ZE2.d	**Güterzug; wegen lückenhafter Technik**	**IV**	**C**
	ZE2.e	**Güterzug; übrige Entgleisungen inkl. Naturgefahren**	**IV**	**C**
Zusammenstoss	**ZZ1.a**	**Zwei Züge; wegen lückenhafter Technik**	**V**	**E**
	ZZ1.b	**Zwei Züge; wegen menschlichen Fehlhandlungen**	**IV**	**D**
	ZZ1.c	**Zwei Züge; wegen Profilverletzung eines Gegenzuges**	**II**	**B**
	ZZ1.d	**Zwei Züge; wegen technischem Versagen von Infrastrukturanlagen inkl. Fahrbahn**	**V**	**E**
	ZZ1.e	**Zwei Züge; übrige Zusammenstösse**	**IV**	**C**
	ZZ2.a	**Zug/Rangier; wegen lückenhafter Technik**	**V**	**D**
	ZZ2.b	**Zug/Rangier; wegen menschlichen Fehlhandlungen**	**IV**	**D**
	ZZ2.c	**Zug/Rangier; wegen Profilverletzung eines Gegenzuges**	**IV**	**B**

Abbildung 3.10: Einstufung der Szenarien in Häufigkeits- und Ausmassklassen (fett = Änderungen ggü. [9])

Qualitative Einteilung	Häufigkeit pro Jahr	Häufigkeits-klasse	Häufigkeits-Ausmass-Matrix					
häufig	über 100	I		PE7, A3, A4, **A6, BR.a**, NBU1, NBU2, NBU4				
	10 bis 100	II		A5, **ZZ3.a, ZZ3.c**, R1, R2, R3, **N.g**	**N.c, N.e, N.f**			
gelegentlich	1 bis 10	III		**ZZ1.c**	PE2, PE5	PE3, A1, BÜ2, NBU3		
	0.1 bis 1	IV		**ZZ2.c**	PE4, PE6, **ZE1.a bis ZE1.e, ZE2.a bis ZE2.e, ZZ1.e, ZZ2.e**	PE1, A2, **ZZ1.b, ZZ2.b, ZZ3.b, B01, BR.d, N.d**		
selten	0.01 bis 0.1	V			FL1	ZS1, **ZZ2.a, ZZ2.d**, GG7	**ZZ1.a, ZZ1.d**, GG4, **BR.c**	
	unter 0.01	VI				PA2	PA1, GG2	GG1, GG3, GG5, GG6, **BR.b, N.a, N.b**, BV1, BV2, BV3
Ausmassklasse			A	B	C	D	E	F
Finanzieller Schaden in CHF			unter 10'000	10'000 bis 100'000	100'000 bis 1 Mio.	1 Mio. bis 10 Mio.	10 Mio. bis 100 Mio.	über 100 Mio.
Personenschäden			eine leicht verletzte P.	mehrere leichtverletzte P., 1 mittelschwer verletzte P.	1 schwerverletzte P. oder 1 Todesopfer (RK 1)	mehrere schwerverletzte P. oder 1 Todesopfer (RK2)	Zahlreiche Schwerverletzte oder 1 bis 5 Todesopfer (RK3)	über 5 Todesopfer (RK3 oder 4)
Qualitative Einteilung			klein		mittel		gross	

Abbildung 3.11: Darstellung der Szenarien in der Häufigkeits-Ausmass-Matrix (fett = Änderungen ggü. [9])

Im Folgenden wird auf die Probleme beim Nachweis einer Gefährdungsrate eingegangen. Sollte die Gefährdungsrate entsprechend der MTTF experimentell ermittelt werden, so ergibt sich eine mittlere geschätzte Rate für gefährliche Ausfälle $\hat{\lambda}_H$ aus

$$\hat{\lambda}_H = \frac{N}{n_0 \; t_b} \tag{2.1}$$

Dabei ist N die Zahl der ermittelten gefährlichen Ausfälle und n_0 der mittlere Gerätebestand in einem Betrachtungszeitraum t_b. Der Betrachtungszeitraum ist so zu wählen, dass sich erfassungs-, wartungs- oder saisonbedingte Schwankungen der Fehlerhäufigkeit möglichst herausmitteln.

Interessant zur Ermittlung der Sicherheit ist aber nicht die mittlere „wahre“ Rate λ_H für gefährliche Ausfälle, sondern nur die obere Vertrauensbereichsgrenze $\lambda_{Ho,}$ da die untere Vertrauensgrenze keine Rolle spielt. Annahme ist, dass die Gefährdungsrate zeitlich konstant ist. Dann gilt mit Hilfe der Chi-Quadrat-Verteilung (χ^2) für die obere Grenze der Gefährdungsrate

$$\lambda_{Ho} = \frac{\chi^2_{2(N+1),1-\alpha}}{2N} \hat{\lambda}_H \tag{2.2}$$

Dabei ist $1-\alpha$ die Wahrscheinlichkeit, dass der wahre Wert von $\lambda_H \; kleiner \; ist \; als \; \lambda_{Ho}$ (Aussagewahrscheinlichkeit, d.h.

$$1-\alpha = P(0 \leq \hat{\lambda}_H \; \leq \lambda_{Ho}) \tag{2.3}$$

N und α sind die Freiheitsgrade der χ^2 Verteilung. Eine generell notwendiger Größenwert für n_0 und t_b kann nicht formuliert werden, da der Wert von λ_{Ho} auch von der Anzahl der tatsächlichen Ausfälle N abhängt.

Der Anlass für diese Betrachtung ist, dass es trotz eines hohen Bestandes an Komponenten bei einer hinreichend geringen Gefährdungsrate entsprechend SIL 4 eines unrealistisch großen Betrachtungszeitraumes bedarf, um zu einer korrespondierenden Anzahl gefährlicher Ausfälle zu gelangen.

Für die Anforderung zur Sicherheit wird als Merkmal die Sicherheitsintegrität definiert. Als Problem erweist sich die Angabe einer vergleichbaren Sicherheitsintegrität, da die Lokalisierung bisher nicht als singuläre Komponente spezifiziert wurde.

Als Ansatz kann auf vergleichbare Angaben für die Balisen und Odometrie aus den ETCS Subsets, z.B. Subset 088 [27], zurückgegriffen werden.

3.11.1 Feststellung 9

Für die Anforderung zur Sicherheit wird als Merkmal die Sicherheitsintegrität definiert (vgl. Kapitel 4 Sicherheit). Als Problem erweist sich die Angabe einer vergleichbaren Sicherheitsintegrität, da die Lokalisierung bisher nicht als singuläre Komponente spezifiziert wurde.

Als Ansatz kann auf vergleichbare Angaben aus den ETCS Subsets für die Balisen und Odometrie zurückgegriffen werden.

3.12 Quantitative Anforderungen an die Verfügbarkeit und Zuverlässigkeit von Lokalisierungssystemen

Die Anforderung an die Verfügbarkeit hängt von der betrieblichen Relevanz der Use Cases ab. Ausgangspunkt kann die betriebliche Unverfügbarkeit sein, die auf eine ausgefallene Lokalisierung zurückgeht. Für die Fallstudie wurden dafür folgender Ansatz und folgende Annahmen gewählt.

Ein erster Ansatz basierte auf der Annahme von 1500 auf dem SBB Netz fahrenden Zügen (die effektive Anzahl Züge ist ein Vielfaches davon), einer täglichen Betriebszeit von Tb = 20 h und der Annahme von MTTR = ½ h akzeptierter Ausfalldauer. Während der Ausfalldauer kann die ausgefallene Lokalisierung identifiziert und wieder in den funktionsfähigen Zustand durch Reparatur, Instandsetzung oder andere Maßnahmen versetzt werden.

Unter diesen Annahmen ergibt bei NZ = 150 Zügen pro Tag auf einer Relation (Netznutzungseffizienz bzw. Zugdichte laut SBB Statistik 160,9 Züge/Strecke/Tag) eine Verfügbarkeit allgemein

$$\mathrm{V} = \frac{\mathrm{Nz\ x\ Tb}}{\mathrm{Nz\ x\ Tb + MTTR}}$$

und für die o.a. Zahlenwerte

$$\mathrm{V} = \frac{150\mathrm{x}20\mathrm{h}}{150\ \mathrm{x}\ 20\ \mathrm{h} + 0{,}5\mathrm{h}} = 0{,}99983\ \text{bzw.}\ 1 - 0{,}000167.$$

Diese Annahmen korrespondieren gut mit den Angaben zur Pünktlichkeit laut SBB Statistik, Pünktlichkeit SBB 2016 88,8% und Anschlusspünktlichkeit 96,7%.

Bei Annahme einer gegebenen MTTR und der o.a. Verfügbarkeit V bzw. ihrem Komplement Unverfügbarkeit Q = 1-V ergibt sich mit der Definition der Verfügbarkeit

$$\mathrm{V} = \frac{\mathrm{MTBF}}{\mathrm{MTBF+MTTR}} = \frac{\mathrm{MTBF+MTTR-MTTR}}{\mathrm{MTBF+MTTR}} = 1 - \frac{\mathrm{MTTR}}{\mathrm{MTBF+MTTR}} \approx 1 - \frac{\mathrm{MTTR}}{\mathrm{MTBF}}$$

wenn $\mathrm{MTTR} \ll \mathrm{MTTF} \approx \mathrm{MTBF}$.

Aufgelöst nach MTBF ergibt sich

$$\mathrm{MTBF} \approx \frac{\mathrm{MTTR}}{1-\mathrm{V}} = \frac{\mathrm{MTTR}}{\mathrm{Q}}$$

Für höher beanspruchte Strecken (Beispiel Zürich Altstetten), wenn man nur den Ausfall eines von täglich 400 Zügen während 0.5 h tolerieren möchte, erhöht sich die Verfügbarkeit auf 0.9999375 bzw. 1 – 6,2510 -5 und die MTBF erhöht sich auf 8000 h. Diese Annahmen wurde für eine Reihe von Use Cases in Absprache mit der SBB zu Grunde gelegt.

3.13 Quantitative Herleitung von Anforderungen für die Fallstudie

Nach den in Abschnitt 3.10 beschriebenen Methoden werden in Kapitel 4 Sicherheit die konkrete Aufstellung von quantitativen Basisanforderungen für die Genauigkeit und Sicherheitsintegrität für die verschiedenen Lokalisierungsobjekte aus Tabelle 3.3 vorgenommen. In dem Kapitel 4 Sicherheit werden konkret für die verschiedenen Lokalisierungsobjekte die jeweiligen Ergebnisse der Risikoanalyse in Form der spezifischen und parametrierten Gefährdungsblätter und die Herleitung entsprechender Parameterwerte präsentiert. Die einzelnen Herleitungen wurden mit verschiedenen Ansätzen erarbeitet und z.T. ergänzend erläutert, so dass für jeden Fall auch eine Überprüfung geschieht und das methodische Spektrum der Ansätze z.T. komplementär verwendet wird.

Die jeweiligen Ergebnisse der verschiedenen Methodischen Ansätze sind in separaten Gefährdungsblättern enthalten.

3.13.1 Feststellung 10

Für die quantitative Erhebung der Basisanforderungen für Genauigkeit und Verlässlichkeit umfasst die Struktur der Gefährdungsblätter die relevanten Merkmale und Größen.

3.14 Zusammenfassung

Insgesamt werden nach dieser Vorgehensweise die einzelnen Use Cases mit ihren insgesamt ca. 60 Unterpunkten systematisch analysiert:

- Ein erstes Ergebnis ist dabei eine Strukturierung nach den Lokalisierungsobjekten mit ihren jeweiligen Bezugspunkten und charakteristischen Eigenschaften, die für die Lokalisierungsfunktion nutzbar sind.
- Ein zweites Ergebnis ist die Strukturierung der Nutzungen mit ihren jeweiligen Anforderungen und den funktionalen, prozessualen und betrieblichen Zusammenhängen (z.B. Zusammenhang zwischen Betrieblicher Leistung und Akquisitionszeit oder ggf. Ortungsunsicherheit und Durchrutschweg).

Weiterhin wird der Zusammenhang zwischen den Lokalisierungsobjekten und den Nutzungen mit ihren Eigenschaften tabellarisch dargestellt. Aus den daraus erkennbaren Bezügen resultiert eine erste qualitative Clusterung der Lokalisierungsfunktionen, welche den Lösungsraum einschränken.

In der Art einer tabellarischen Gegenüberstellung der geclusterten Use Case-Anwendungsfunktionen mit ihren jeweiligen Anforderungen zu den Bewegungseigenschaften der Lokalisierungsobjekte können die Basisabforderungen seitens Lokalisierungsfunktionen in Form der Attribute identifiziert und quantifiziert werden. Innerhalb der Cluster sollten dabei die Werte innerhalb einer Größenordnung bzw. Klassifizierungsebene (z.B. SIL-Stufe) liegen. Für die abschließende Basisanforderung an eine Lokalisierungsfunktion wird dabei

der anspruchsvollste Wert eines Clusters gefordert. Gleichzeitig wird aus dieser Gegenüberstellung auch der technologische Spielraum einer Lösung durch geeignete Komponenten und Architekturen hergeleitet und damit sichtbar.

Dieser Ansatz enthält implizit auch eine systematische Prüfung der Vollständigkeit, sowohl vom Bedarf der Funktionen zur Lokalisierung als auch vom „Angebot" einer Lokalisierung von Objekten.

Mit der methodischen Clusterung und nachfolgenden Klassifizierung von Lokalisierungsobjekten und Nutzungsfunktionen nach charakteristischen Merkmalswerten (z.B. gleiche SIL Anforderung) in wenigen Klassen wird eine gewisse Anzahl von gleichartigen Anforderungen für Lokalisierungsfunktionen aufgestellt, woraus wenige Lösungsansätze resultieren.

Durch diese Definition der Szenarien mittels der wechselseitigen Kausalkette zwischen Lokalisierungsobjekt, betrieblicher Nutzungsfunktion und Gefährdungsobjekt werden Anforderungen an die Lokalisierung hinsichtlich RAMSS und der damit verbundenen Genauigkeit an die Lokalisierung erarbeitet. Absehbar ist bereits, dass sich aus der gegenseitigen Wechselwirkung hinsichtlich der akzeptablen Genauigkeit und der notwendigen Sicherheit und der betrieblichen Leistung sowie dem wirtschaftlichen Aufwand ein skalierbares Optimierungspotenzial ergibt. Gleichzeitig erlaubt diese Strukturierung die Identifizierung von Risiken, was in Kapitel 4 Sicherheit von Belang ist.

Nach diesem Schema wird bereits eine sehr strukturierte Anforderungsbeschreibung erstellt, die dank ihrer Systematik später in ein strukturiertes Anforderungsdokument eines Requirement-Tools implementiert werden kann.

Die Nutzung operativer Synergien wird durch die Clusterung der Nutzungsfunktionen und ihre Befriedigung durch verschieden Merkmalsabstufungen der Anforderungen bzw. der daraus resultierenden Gesamtlösung berücksichtigt.

Ergebnis ist eine in Tabellenform zusammengefasste und geclusterte Aufstellung der in Größen und Werten mit Einheiten ausgedrückten Basisanforderungen für Lokalisierungsfunktionen der Nutzungsfunktionen.

3.15 Fazit

Infolge der neuartigen technologischen Realisierung von Lokalisierungslösungen mit dem Ziel einer kontinuierlichen sicheren Ortung seitens der relevanten Ortungsobjekte auf der Grundlage umfangreicher und verschiedenartiger Nutzungen in Form von Use Cases resultieren neue Anforderungen und Anforderungsqualitäten. Neben dem hier aufgezeigten methodischen Vorgehen zur Ermittlung der relevanten Basisanforderungen müssen auch die von dieser technologischen Änderung ausgehenden Änderungen der Systemarchitektur von ELSS und den betrieblichen Regeln bzw. Regularien mitberücksichtigt werden. In den Regelwerken besteht ein gewisses Primat der technologischen Spezifikation, die mittelbar von funktionalen Spezifikationen abgelöst werden. Damit geht die Änderung der Regelwerke und der

damit verbundenen Zulassung einher, die ebenfalls gebührende Aufmerksamkeit und ein entsprechendes finanzielles und zeitliches und kommunikatives Budget erfordert. In diesem Zusammenhang sei auch auf die Ermittlung sicherheitsrelevanter Bezugsgrößen und -werte verwiesen, da kaum eine Vergleichbarkeit existiert.

4. Schwerpunktbereich „Sicherheit“

Zusammenfassende Feststellungen

Mit der fortgeschrittenen Satellitentechnologie, z.B. mit Mehrfrequenzsignalen, Richtungsantennen, Referenzstationen, Empfängern und Detektions- oder Plausibilisierungsalgorithmen können Störungen zunehmend identifiziert und damit eliminiert werden. Damit erscheint die Verwendung einer im rechtlichen Rahmen des Völker- und EU-Rechts betriebenen Satellitentechnologie zur absoluten Lokalisierung von Objekten im Bahnbereich machbar.

Mit geeignet qualifizierten Sensorsystemen stehen geeignete unabhängige Komponenten zur Verfügung, welche in Kontext der Architektur und geeigneter Verarbeitungsalgorithmen einen signifikanten Beitrag zur Machbarkeit einer genauen und sicheren satellitenbasierten Lokalisierung von Objekten im Eisenbahnbereich ermöglichen.

Sicherheit kann durch Parallelredundanz stochastisch unabhängiger Teilsysteme mittels Koinzidenz ihrer Ergebnisse erzeugt werden. Die resultierende Gefährdungsrate ist dabei um Größenordnungen geringer als die Ausfallrate eines Teilsystems, wenn eine kurze Ausfalloffenbarungszeit gewährt wird.

Zu beachten ist allerdings, dass für die Verfügbarkeit einer satellitengestützten Lokalisierung weitere redundante Sensorkomponenten erforderlich sind, welche ein komplementäres Ausfallverhalten zeigen sollten. Zur Erhöhung der Sicherheit und der Verfügbarkeit ist eine höher redundante Struktur notwendig. Je nach Anwendungsbereich bzw. Lokalisierungsobjekt sind entsprechende Risiko- und Gefährdungsanalysen als Grundlage zur Fehlerdetektion durchzuführen.

Bei Kenntnis der individuellen Verlässlichkeitsmerkmale und ihrer Kennwerte der Ausfall- und Reparaturraten der Lokalisierungssensoren ist mit einer geeigneten redundanten Konfiguration und Überwachung mit entsprechender Ausfalloffenbarungszeit eine exakte Parametrisierung der Gefährdungsrate und der Verfügbarkeit des Gesamtsystems simulativ möglich und erforderlich.

Mit der fortgeschrittenen Entwicklung von Algorithmen zur Sensordatenfusion und Fehlerdetektion von Multisensorsystemen und ihren Anwendungen zur Lokalisierung von Fahrzeugen im Eisenbahnbereich liegen erprobte Grundlagen vor, die einen signifikanten Beitrag zur Machbarkeit einer genauen und sicheren Lokalisierung leisten.

Unter Beachtung der Normativen Voraussetzungen, insbesondere der Normenfamilie EN 5012X bei der Entwicklung von Lokalisierungssystemen mit Satellitenstützung und geeignet qualifizierten Sensorkomponenten einschließlich Gefährdungsanalyse, Implementierung auf sicheren Komponenten und normkonform entwickelter und getesteter Software sowie normkonformem Nachweis der Sicherheit können alle Voraussetzungen für die Machbarkeit erfüllt werden.

4.1 Übersicht und Bezüge zu den anderen Schwerpunkten

Ziel eines Lokalisierungssystems ist, für den sicheren und effizienten Betrieb im Eisenbahnverkehr eine verlässliche und genaue Information über die Position und Bewegung von relevanten Objekten zur Erfüllung verschiedener Use Cases zu generieren.

Der Ansatz und die Inhalte Im Schwerpunktbereich 4 Sicherheit werden im Folgenden zuerst überblicksartig skizziert und danach im Einzelnen vorgestellt.

Zuerst werden Begriffe der Sicherheit im Sinne von Safety und Security sowie die Begriffe des Lokalisierungssystems weitgehend normkonform definiert (Abschnitt 4.2).

Anschließend werden im Abschnitt 4.3 die im Kapitel 3 Use Cases angesprochenen Systemsichten berücksichtigt. Die Sicherheit von Lokalisierungssystemen in einem Eisenbahnsystem wird einerseits durch äußere Anforderungen bestimmt, um bei ihrer Nutzung keine unzulässigen Risiken hervorzurufen. Diese risikobezogene Betrachtung wird hier als exogene Sicherheit verstanden.

So wird konkret im Abschnitt 4.3 auf dem Use Case - Niveau betrachtet, welche Risiken einer fehlerhaften Ortung im Eisenbahnsystem von einer unrichtigen und unzuverlässigen Lokalisierung in den einzelnen Use Cases ausgehen. Entsprechend dem in Kapitel 3 Use Cases erläuterten Ansatz werden zu den von fehlerhafter Lokalisierung ausgehenden identifizierten Gefährdungen die notwendigen Anforderungen an die Eigenschaften und Merkmale einer Lokalisierung von definierten Lokalisierungsobjekten ermittelt. Diese werden methodisch in tabellenartiger Form qualitativ und quantitativ in sogenannten Gefährdungsblättern zusammengestellt. Zur Erfüllung dieser Anforderungen an Genauigkeit und Sicherheit muss das Lokalisierungssystem insbesondere die aus der Risikoanalyse herrührenden Anforderungen an die exogene Sicherheitsintegrität erfüllen.

Andererseits darf ein Lokalisierungssystem keine Gefährdungen verursachen, welche aus der Realisierung hervorgehen. Zur Lokalisierung stehen dafür die GNSS-Systeme und andere Sensortechnologien zur Verfügung, deren spezifische Eigenschaften, z.B. mit ihren Fehlerarten betrachtet werden müssen. Die auf GNSS u.a. Technologien aufbauende Lokalisierung adressiert im Sinne einer Fokussierung aufgrund technologischer Bedingungen und systemischen Abgrenzung im Kontext der Architektur und Migration in das ELSS auch das Thema Security. Entsprechend der sich durchgesetzten Erkenntnis, dass Safety auch auf Security aufbaut bzw. Security eine Voraussetzung für Safety ist, wird dieser Aspekt quasi modular bearbeitet.

Diese gefährdungsbezogene Betrachtung wird hier als endogene Sicherheit begriffen und im Abschnitt 0 Security und Safety - Gefährdungen der Lokalisierung und ihre Beherrschung behandelt. Dort werden diesbezüglich und im Sinne einer Gefährdungsanalyse des Lokalisierungssystems relevante Safety und Security Aspekte insbesondere bezüglich neuer Technologien für eine genaue und verlässliche Lokalisierung selbst angesprochen. In diesem Zusammenhang werden mögliche Strategien zur Minderung zusammengefasst.

Die sicherheitstechnische Gestaltung des Lokalisierungssystems zur Erfüllung der Use Case Anforderungen aus Abschnitt 4.3 unter Verwendung der Sensortechnologien und Berücksichtigung ihrer Fehlereigenschaften aus Abschnitt 0 wird in Abschnitt 4.5 behandelt. Darin wird gezeigt, wie die Anforderungen durch die Gestaltung einer spezifischen Funktionsarchitektur, Konfiguration, Parametrierung und Implementierung des Lokalisierungssystems mit seinen Sensoren und Verarbeitungseinheiten erfüllt werden (vgl. Abbildung 4.12). Diese Ansätze bilden die Grundlagen der sicherheitsgerichteten Entwicklung des Lokalisierungssystems, die abschließend im Abschnitt gezeigt wird.

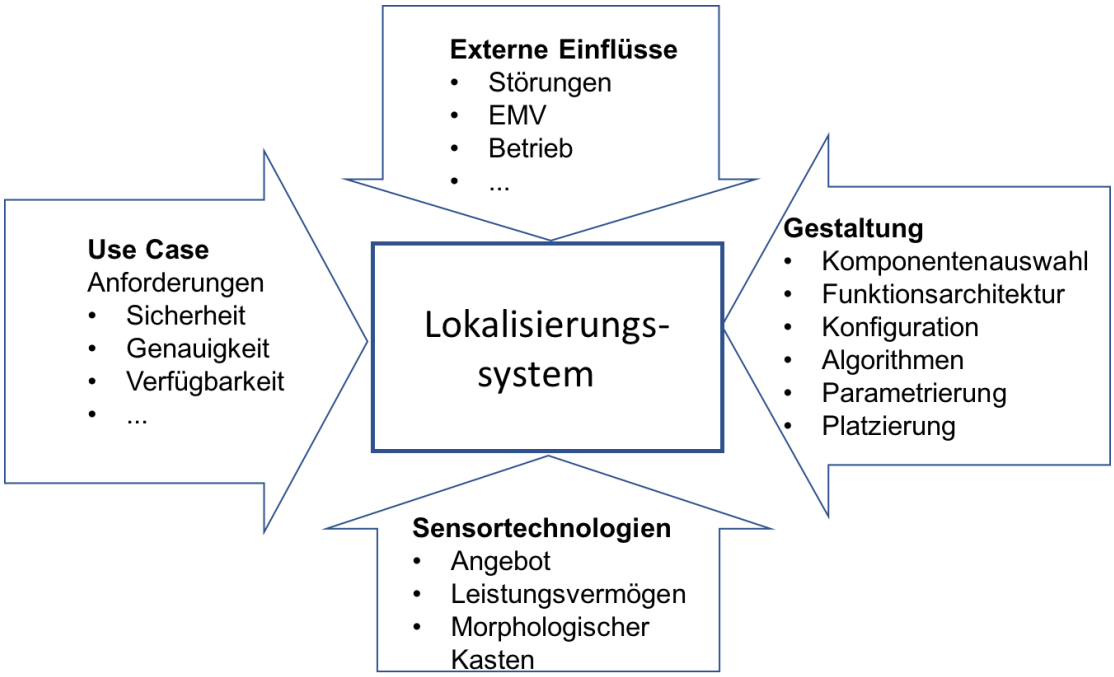


Abbildung 4.12: Anforderungen, Technologien und methodischer Gestaltungsansatz des Lokalisierungssystems

Die Erkenntnisse dieses Schwerpunktes fließen sowohl in den Schwerpunkt 5 Zulassung als auch insbesondere dann in den Schwerpunkt 6 Gesamtlösung ein (Abbildung 4.13)

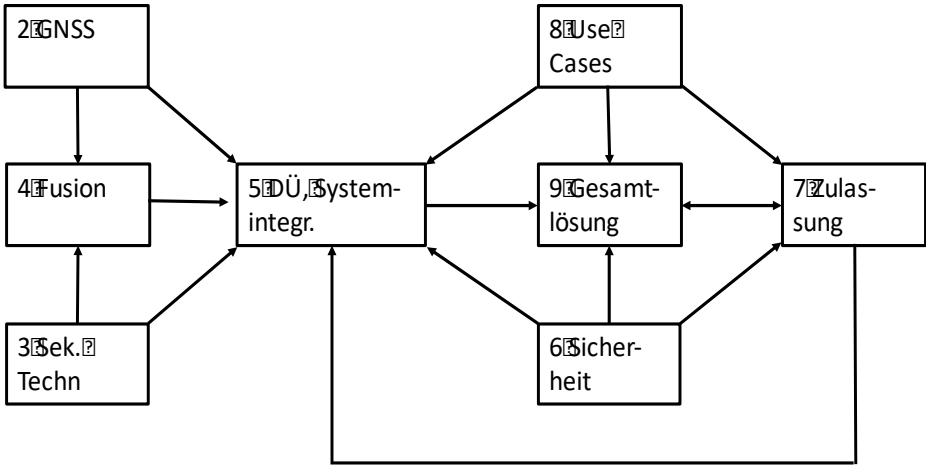


Abbildung 4.13: Zusammenhang zwischen den Schwerpunkten

4.2 Definition von Safety und Security und weiteren Begriffen

Zuerst werden die Begriffe Safety und Security normkonform rekapituliert und weitere Begriffe für das Verständnis definiert. Grundlage des Safety Begriffs ist die im Eisenbahnbereich übliche Definition nach DIN EN 5012X über den Risikobegriff als Kombination von Gefährdungs- bzw. Eintrittswahrscheinlichkeit und Unfallschwere, die dort in Anhängen mit entsprechenden Referenzen quantifiziert werden.

Sicherheit (nach EN 50128, 3.1.27): Freiheit von nicht-akzeptablen Risiken für Personenschäden. Unter den Risiken werden hier solche verstanden, welche sich auf Schäden der direkten oder indirekten Umgebung des Lokalisierungssystems beziehen.

Risiko (nach EN 50128, 3.1.26): Kombination der Häufigkeit des Auftretens von Unfällen oder Zwischenfällen, die zu einem Schaden führen (verursacht durch eine Gefährdung), und der Grad der Schwere dieses Schadens.

Gefährdung (in Anlehnung an EN 50126 3.17 dort Gefahr engl. Hazard): Eine physikalische Situation, die potenziell einen Schaden für den Menschen beinhaltet. Nach dem DIN Fachbericht 144 wird die Situation durch die Koinzidenz der Gefährdung und eines dieser exponierten Rechtsgutes beschrieben.

Security – als Sicherheit vor Bedrohung bezeichnet - wird auf die von außen möglichen intendierten und nichtintendierten Bedrohungen bezogen. Dies schließt auch informationstechnische und Kommunikationssysteme ein, was in DIN EN 50159 u.a. (z.B. DIN ISO IEC 27001 oder IEC 62443 bzw. DIN-Vornorm 0831-104) betrachtet wird. Im Fall satellitengestützter Lokalisierungssysteme muss dies auch bei der Ausstrahlung von Satellitensignalen gewürdigt werden.

Funktionseinheit (in Anlehnung an DIN EN ISO 10209, VDI 3682): Betrachtungseinheit, deren Abgrenzung nach Aufgabe oder Wirkung erfolgt und ihre physikalischen Ressourcen einschließt.

Komponente (in Anlehnung an EN 50128 3.1.4): ein Bestandteil eines Systems, die in Bezug auf Softwarearchitektur und -entwurf über klar definierte Schnittstellen verfügt, und ein bestimmtes Verhalten hat.

System: siehe Lokalisierungssystem

Fehler (nach EN 50128, 3.1.9): Mangel, Fehlentscheidung oder Ungenauigkeit, die zu einem Ausfall oder zu einer Abweichung von den beabsichtigten Leistungsmerkmalen oder zu unerwünschtem Verhalten einer Funktionseinheit führen kann.

Ausfall (IEV 191-01-12): (Unmittelbare) Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen

Sensor: hierunter wird ein physikalischer Sensor verstanden, welcher den aktuellen Wert einer Bewegungsgröße in eine weiter verarbeitbare meist elektrische oder informationstechnische Größe umsetzt.

Auswerteinheit: Eine nachfolgende Sensordatenauswertung ermittelt aus den Sensorsignalen, z.T. unter Zuhilfenahme von informationstechnischen Algorithmen einen evtl. korrigierten, kalibrierten oder von Fehlern bereinigten Größenwert und ggf. weitere Information über das Messergebnis.

Lokalisierungssystem: Das Lokalisierungssystem besteht insgesamt aus mehreren Komponenten. Mehrere Sensorsysteme werden zusammen mit einer weiteren Einheit oder mehreren zum Lokalisierungssystem zusammengefasst. Darin werden dann mehrere Größenwerte zusammen ausgewertet, um einen um Abweichungen bereinigten Größenwert des Lokalisierungszustandes zu ermitteln, um einzelne Sensorsysteme auf ihre Richtigkeit zu detektieren oder ggf. von der zusammenfassenden Werteermittlung ggf. temporär auszuschließen.

Messunsicherheit Das Internationale Wörterbuch der Metrologie (VIM) definiert Messunsicherheit als einen Kennwert, der den Bereich der Werte charakterisiert, die der Messgröße durch die durchgeführte Messung vernünftigerweise zugeschrieben werden können. Die nach einem einheitlichen Verfahren berechnete und in einer bestimmten Weise mitgeteilte Messunsicherheit drückt so die Stärke des Vertrauens aus, mit der angenommen werden darf, dass der Wert der gemessenen Größe unter den Bedingungen der Messung innerhalb eines bestimmten Werteintervalls liegt.

Messabweichung ist nach dem Internationalen Wörterbuch der Metrologie (VIM) definiert als eine Differenz „Messwert minus Referenzwert“. Ein **Referenzwert** ist a) ein Wert mit vernachlässigbarer Unsicherheit oder ein vereinbarter Wert, der in DIN 1319-1 und DIN 55350-13 als richtiger Wert bezeichnet wird, b) ein mit der Definition einer Messgröße übereinstimmender wahrer Wert.

4.3 Sicherheitsrisiken der Use Cases – Exogene Sicherheit

Die Anforderungen an die Qualität der Lokalisierung, insbesondere der Genauigkeit des Lokalisierungszustandes und der Sicherheit der Lokalisierungsfunktion sind auf der Grundlage von Use Cases ermittelt und in Kapitel 3 beschrieben.

Da die Sicherheit eines Eisenbahnsystems durch das komplexe Zusammenwirken von vielen menschlich und technisch ausgeführten Funktionen erreicht wird, ist die Beurteilung der Sicherheit von Einzelkomponenten nur im systemischen Zusammenhang, d. h. im gesamten Wirkungsgefüge zulässig.

Bei Neueinführung oder Änderung von Eisenbahnsystemen kann nach § 2 EBO von den anerkannten Regeln der Technik (ART) abgewichen werden (z. B. weil diese Regeln nicht die Neuerungen berücksichtigen), wenn mindestens die gleiche Sicherheit nachgewiesen wird, die bei Systemen erreicht wird, wo diese Regeln beachtet werden. Ähnliche Aussage finden sich im 2. Abschnitt: Sicherheit Art. 2 der Schweizer Eisenbahnverordnung.

Damit ist die Bestimmung eines Referenzwerts für die grundsätzliche Qualifizierung eines Eisenbahnsystems im Rahmen des geltenden Rechts notwendig. Dieser Wert sollte nach Möglichkeit auch quantitativ angegeben werden. Maßgeblich für die Sicherheitsbemessung im Eisenbahnverkehr ist die Bestimmung des Risikos in einem vergleichbaren Geltungsbereich bzw. Referenzbereich aus den Schadensstatistiken. Das Risiko selbst wird üblicherweise durch die mittlere Schadenschwere und -häufigkeit gekennzeichnet oder berechnet sich durch das akkumulierte Schadensausmaß.

Werte für die gleiche Sicherheit als quantitativer Referenzwert können aus dem Betrieb erhoben werden. Die Problematik, dass bei neuen Systemen noch keine Sicherheitsindikatoren aus dem Betrieb berücksichtigt werden können, wird dadurch gelöst, dass als Maß für die gleiche Sicherheit die im Sicherheitsnachweis nach einschlägigen Regeln und Verfahren im normativen Kontext nachgewiesenen Werte maßgeblich sind, bevor das System in Verkehr gebracht wird. Bei der Erörterung einer Referenz für die Sicherheitsbemessung spielt der Begriff „mindestens gleiche Sicherheit“ in Bezug auf die Sicherheitszuteilung von Komponenten und Funktionen eines Systems eine entscheidende Rolle. Dies ist insbesondere hinsichtlich der Nachweisführung und Prüfung wichtig, wenn bei der Änderung oder Neueinführung von Eisenbahnsystemen von den anerkannten Regeln der Technik abgewichen wird.

Im Kapitel 3 Use Cases wurden aus dem Kontext der Use Cases in Form von Risikobetrachtungen Anforderungen an die Lokalisierung von individuellen Lokalisierungsobjekten methodisch hergeleitet. Abbildung 4.14 zeigt die verwendete methodische Vorgehensweise zur Systemgefährdungsanalyse nach Slovák.

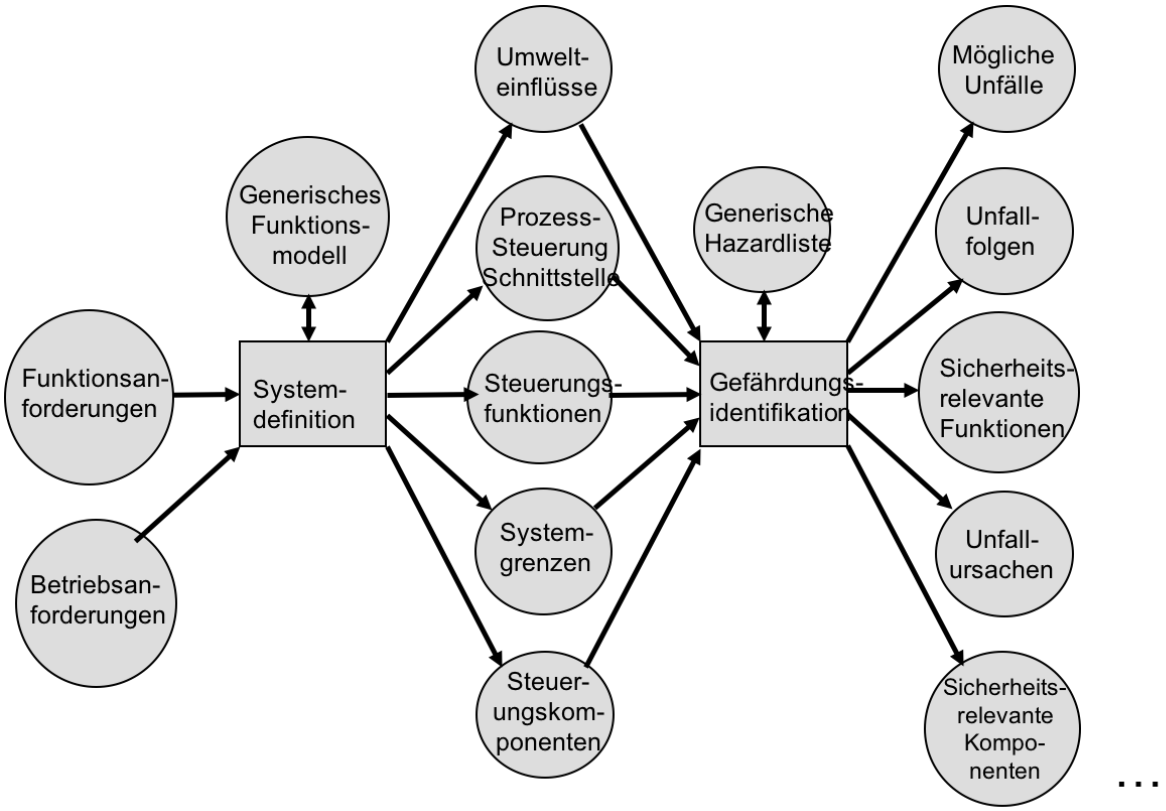


Abbildung 4.14: Methodische Vorgehensweise zur Systemgefährdungsanalyse (nach Slovák)

An dieser Stelle wird daher auf diese Ausführungen zu den Use Case und ihren Sicherheitsaspekten im Kapitel 3 verwiesen. Insbesondere wird dort im Abschnitt „Qualitative Herleitung von Sicherheitsanforderungen“ die Methodik ihrer Herleitung ausführlich und exemplarisch beschrieben. Eine isolierte Darstellung in diesem Kapitel würde den in Kapitel 3 beschriebenen notwendigen Gesamtzusammenhang nicht berücksichtigen.

Hier werden daher konkret für die verschiedenen Lokalisierungsobjekte die jeweiligen Ergebnisse der Risikoanalyse in Form der spezifischen und parametrierten Gefährdungsblätter und die Herleitung entsprechender Parameterwerte präsentiert. Tabelle 4.12 fasst die parametrierten Attribute der Lokalisierungsobjekte aus der Use Case Analyse übersichtlich zusammen.

GFB-Nr.	Use Case Nr	Lokalisierungssobjekt	SIL	Genauigkeit	MTTF	MTTR	Verfüg-barkeit	Latenz o. Periode	Version
1.1	1.1	**Gleisfreimeldung**	SIL3/ SIL4	x ≤66,4 m R y +/-1,5 m R	1 Jahr	0,5h	0,9999375	1s	1.6
1.2	1.2 – 1.7 8.1 – 8.2	**Zugposition Fahrzeuge**	SIL 3	10 m R	1 Jahr	0,5h	0,9999375	0,5 s 0.5 s	2.0
2	1.1.5 1.5 6.2 7.1 - 7.3	**Balisen/Tafeln (vituelle)Euro-Balise**	SIL 2 (an der Grenze zu SIL 3)	10 m R	1 Jahr	0,5h	0,9999375	0,5 – 1 s	2.1
3	2.2.4 3.1.6	**betriebliche Objekte Entgleisungsvorrichtung Prellbock**	≤ SIL 3	x 10m R y +/-1,5m R	1 Jahr	0,5h	0,9999375	max. 1 s	1.1
4a1	2.1 8.4	**Menschen im Gleis Doppelausrüstung (Zug siehe 1.2)**	SIL 0 (1-2)	x 2,5m G y 2,5m G y 3,5m G	15 Tage	9h	0,9975	max. 1s	2.2
4a2	2.1 8.4	**Menschen im Gleis ohne Warnanlagen (Zug siehe 1.2)**	SIL 2	x 2,5m G y 2,5m G y 3,5m G	15 Tage	9h	0,9975	max. 1s	1.0
4b	2.1 8.4	**Menschen im Gleis Zug-warnung (Zug siehe 1.2)**	SIL2	x 2,5m G y 2,5m G y 3,5m G	15 Tage	9h	0,9975	max. 1s	1.0
5/7	2.1 2.2 3.3.1 3.1.3 - 3.1.5	**Instandhaltungsartefakte /sonstige Objekte**	SIL 3	x 10m R y +/-1,5m R z 3,5m R	1 Jahr	0,5h	0,9999375	max. 1 s	1.3

GFB-Nr.	Use Case Nr	Lokalisierungssobjekt	SIL	Genauigkeit	MTTF	MTTR	Verfüg-barkeit	Latenz o. Periode	Version
	8.3								
6	3.1.2	**Naturobjekte**	SIL 2	x 10m R y 10m R z 10m R	1 Jahr	1 Tag (24h)	0,99726	max. 1 s	1.1

Tabelle 4.12: Zusammenfassung der parametrierten Attribute der Lokalisierungsobjekte aus der Use Case Analyse

Die einzelnen in der Tabelle 4.12 in der Spalte «GFB Nr.» genannten Gefährdungsblätter wurden separat erstellt und werden hier nicht wiedergegeben.

4.4 Security und Safety – Gefährungen der Lokalisierung und ihre Beherschung – Endogene Sicherheut

In diesem Abschnitt wird gezeigt, wie die Lokalisierungsinformation von Lokalisierungsobjekten im jeweiligen Lokalisierungssystem sicherungstechnisch prinzipiell erzeugt und garantiert wird, um die aus den Use Cases hergeleiteten Anforderungen an die spezifische Sicherheitsintegrität zu erfüllen. Es wird dargestellt, welchen inhärenten Ursachen und Einflüssen nicht intendierter und intendierter Natur, d.h. Bedrohungen begegnet wird (Resilienz), um die Information verlässlich zu erzeugen und im Fehlerfall auch anzugeben, dass sie nicht mehr vertrauenswürdig ist.

Diese Maßnahmen endogener Sicherheit bündeln sich zu einer konsistenten Strategie zur Minderung der Risiken zur Safety und Security. Eingeschlossen sind darin auch die Maßnahmen zur Fehlerbegrenzung bzw. Minderung von Auswirkungen (Mitigation).

Für die Zielsetzung, mit Hilfe von GNSS-gestützter Sensorik, entsprechend den Anforderungen der einzelnen Use Cases Objekte im Eisenbahnbereich genau, sicher und verlässlich zu lokalisieren, müssen

- das Lokalisierungssystem gemäß den **Sicherheitsnormen** im Eisenbahnwesen entwickelt, hinsichtlich der Sicherheitsanforderungen analysiert, implementiert und nachgewiesen werden. Neben der Betrachtung der Safety gemäß den CENELEC Normen EN 50126/8/9 schließt dies auch informationstechnische und Kommunikationssysteme ein, was in DIN EN 50159 u.a. (z.B. DIN ISO IEC 27001 oder IEC 62443 bzw. DIN-Vornorm 0831-104) betrachtet wird. Im Fall satellitengestützter Lokalisierungssysteme muss dies auch bei der Ausstrahlung von Satellitensignalen gewürdigt werden.
- die Prinzipien der **Resilienz** (vgl. [28]) beachtet werden. Im Einzelnen handelt es sich um die Defense in Depth Strategie und ihre Ausprägungen
    - Ende zu Ende Sicherung
    - Kapselung und Modularität
    - Schlankheit
    - Filterung bei Übergangspunkten
    - Dynamische Integritätsprüfung
    - Transparenz der Konfiguration und Parametrierung
    - Wiederherstellung korrekter Funktion
- eine entsprechende **Systemarchitektur** mit entsprechender Konfigurationen zur genauen Lokalisierung durch softwaretechnisch implementierte Algorithmen zur Sensordatenauswertung und -fusion sowie zur sicheren Fehlerdetektion entwickelt werden

- die **bewährten Konzepte** wie Movement Authority, Fail Safe und Ruhestrom, sowie Signalabhängigkeit als Sicherungsmaßnahmen einbezogen werden
- geeignete **verlässliche** Komponenten zur Sensorik und Verfahren zur verlässlichen Auswertung hinsichtlich Fehlerminimierung und -detektion ausgewählt werden
- geeignete **Algorithmen** zur hochgenauen Lokalisierung durch Sensordatenauswertung und -fusion sowie zur Fehlerdetektion ausgewählt und implementiert werden
- geeignete verlässliche Funktionskomponenten (Hardware und Software) zur Implementierung ausgewählt werden
- geeignete Sicherungstechniken bei der **Kommunikation** verwendet werden, z.B. kryptografische Verschlüsselungsverfahren mit entsprechenden Zertifikaten
- die **Natur der Lokalisierungsinformation** der einzelnen Sensorsysteme bezüglich metrologischer und sicherheitlicher Aspekte betrachtet werden.

Diese einzelnen Punkte werden in den folgenden Abschnitten detailliert dargestellt.

Hinsichtlich der Resilienz sei angemerkt, dass die grundsätzlichen Prinzipien in der Sicherheitstechnik des Eisenbahnbetriebes nicht neu sind und zum großen Teil, einschließlich der aktuellen Themen der IT-Security, bereits in den einschlägigen Regelwerken enthalten sind.

4.4.1 Natur der Lokalisierungsinformation bezüglich metrologischer und sicherheitlicher Aspekte

Messunsicherheiten und Messbedingungen

Die Bestimmung einer Position eines Objektes im Schienenverkehrsnetz führt zu einem realen Messwert in einem definierten Koordinatensystem. Dieser Messwert ist gemäß der Natur des Messsystems zur Lokalisierung, bestehend aus Sensorik und Messwertbestimmung, mit Unsicherheiten und Abweichungen behaftet, welche die Differenz des bestimmten Messwertes von einem idealen „wahren“ Messwert charakterisieren. Hinzu kommt, dass bei der Positionsbestimmung voraussichtlich Umwandlungen von einem Koordinatensystem in ein anderes Koordinatensystem erforderlich sind, was ggf. zu numerischen Fehlern führen kann.

Ziel einer Messeinrichtung ist, den realen Messwert richtig, genau, und korrekt zu bestimmen. Hierfür sind die jeweiligen Unsicherheiten des Messsystems qualitativ und quantitativ zu bestimmen. Im Einzelnen gehören dazu die Betrachtung des Messsystems hinsichtlich seines Messprinzips, seiner Messfehlerarten, seiner Messbedingungen und seiner messtechnischen und numerischen Unsicherheiten. Diese Informationen sind bei der Auswahl der einzelnen Teilmesssysteme zu bestimmen und anzugeben. Für die Angabe bzw. der Berechnung der Werte ist die metrologische Richtlinie der ISO, der Guide of Uncertainty Measurement GUM (JCGM 10X ISO/IEC Guide 98-3:2008 (JCGM/WG1/100) Uncertainty of measure-

ment -- Part 3: Guide to the expression of uncertainty in measurement (GUM:1995)) heranzuziehen, der in der Dissertation auf die Messung kontinuierlicher Zustandswerte ausgedehnt wurde (vgl. [29])

Kontinuierliche Lokalisierung

Unabhängige und verschiedenartige Sensorsysteme liefern Messwerte innerhalb gewisser Wertegrenzen. Durch Algorithmen der Sensordatenfusion kann eine ausreichende Genauigkeit erzielt werden. Die klassische Ausfalldetektion eines Vergleiches gleicher Werte einzelner Sensoren kann hier nicht mehr verwendet werden.

Wissensbasierte Methoden können sowohl zur Verbesserung der Genauigkeit als auch zur Fehlerdetektion verwendet werden. Dazu gehören z.B. die Stützung durch digitale Streckenkarten. Filteralgorithmen, Neuronale Netze, Analytische Redundanz, Fehlerkompensation, automatische Kalibrierung.

Daneben sind zur Genauigkeitserhöhung und Fehlerdetektion auch unabhängige redundante Berechnungsverfahren zur Lokalisierung zweckmäßig, z.B. durch Integrationsverfahren von Geschwindigkeit und Beschleunigung (z.B. Beobachter).

Störungen/Bedrohungen

Für den Einsatz der satellitenbasierten Ortung im Schienenverkehr muss gewährleistet werden, dass Signale in nutzbarer Qualität vorhanden sind. Satellitenbasierte Ortungssysteme sind systembedingt leicht unbeabsichtigt und noch leichter absichtlich zu stören. Die dafür verwendeten Geräte werden in Störer (engl. Jammer) und Täuscher (engl. Spoofer) unterschieden. Bei einem Störer handelt es sich um ein Gerät, dass elektromagnetische Wellen in einem Frequenzband abstrahlt, das für die Satellitennavigation genutzt wird. Unter einem Täuscher versteht man ein Gerät, das Signale aussendet, die den Navigationssignalen der GNSS Satelliten nachempfunden sind.

Störer können in drei Kategorien unterschieden werden:

- *Unabsichtliche Störer* können z.B. durch Schwingungen als Sinus-Störer auftreten. Diese können eine bestimmte Empfangsfrequenz eines UKW-Radios oder sich überlagernde Sendesignale im GNSS Spektrum sein.
- Zu *duldende Störer* sind militärische Anwendungen, welche die gleichen Frequenzbänder wie einige Frequenzbänder von GPS nutzt.
- *Absichtliche Störer* finden mittlerweile eine immer weitere Verbreitung und sind bereits ab deutlich unter 100 € über das Internet zu bekommen. Diese Störsender haben in der Regel das Ziel, die zivile GNSS Nutzung unmöglich zu machen, beispiels-

weise um ein Anti-Diebstahl-System eines Fahrzeugs auszuschalten oder Mautsysteme zu umgehen.

Unter einem **Täuscher** (engl. Spoofer) versteht man ein System, das Signale aussendet, die den Navigationssignalen der GNSS Satelliten nachempfunden sind. Täuschsignale stellen für Navigationsempfänger in sicherheitskritischen Anwendungen eine erhebliche Gefährdung dar. Durch künstlich generierte Navigationssignale (Spoofing) oder das Wiederabspielen von aufgezeichneten GNSS Signalen (Meaconing) können Navigationsempfänger unbemerkt von Dritten übernommen und dem Nutzer eine falsche Position vorgetäuscht werden.

Störer und Täuscher werden als problematisch bezüglich der Genauigkeit der Ortungsinformation und der sicheren Nutzbarkeit im Schienenverkehr betrachtet.

Durch fortgeschrittene Verfahren in den Satellitensignalempfängern können derartige Bedrohungen zumindest detektiert werden.

- Detektion von Störern: quasi-echtzeitfähige Algorithmen zur automatischen Detektion von Störern im Rohdatenstrom; Detektion und Klassifikation von typischen Störer-Signalen wie CW, Pulse, Chirps; Vergleich von verschiedenen Ansätzen hinsichtlich PD (probability of detection), PFA (probability of false alarm), spektraler Auflösung und Rechenaufwand; Störer-Detektion mit Hilfe von Compressed Sensing.
- Detektion von Täuschern: Algorithmen und Technologien zur sicheren Detektion und Unterdrückung von Täuschersignalen. Hierbei vorrangig drei Arten von Verfahren zur Detektion von Täuschersignalen. Weiterhin Eigenschaften und zeitliche Veränderung der Korrelationsfunktion, Monitoring der Trägerphase sowie Verfahren auf Positionsebene, um fehlerhafte oder getäuschte Signale festzustellen.

Z.T. sind diese Maßnahmen bereits in den einzelnen Sensorsystemen selbst implementiert. Insbesondere bei den Empfängern von Satellitensignalen zur Ortung sind ausgefeilte Algorithmen zur Erhöhung der Genauigkeit und Fehlererkennung sowie Maskierung implementiert. Diese Algorithmen werden als Receiver Autonomous Integrity Monitoring (RAIM) bezeichnet.

Weiterhin werden durch einen heterogenen Multisensoransatz derartige Störungen und Täuschungen erkannt und maskiert.

Die Störungen der Satellitensignale sind bezüglich des Aufenthaltsbereiches der Lokalisierungsobjekte zu unterscheiden. Handelt es sich um lokale Störungen, werden diese bei bewegten Objekten nur innerhalb des Störgebietes wirksam. Bei stationären Objekten muss eine längerfristige Beeinträchtigung ausgeschlossen werden, was durch geeignete Referenzierung möglich ist. Problematisch sind großflächige Signalstörungen. Hier ist die geografische Verfügbarkeit, auch unter politischen und rechtlichen Rahmenbedingungen ein wichti-

ges Kriterium. Insbesondere bieten hier unter ziviler Kontrolle betriebene Satellitennavigationssysteme wie Galileo gewisse Vorteile (vgl. [30]).

In diesem Zusammenhang wird auf die EU GNSS Regulation 1285/2013 vom 11. Dezember 2013 verwiesen, wo in Artikel 2 Absatz 4 das Ziel, die Nutzbarkeit der Signale für die folgenden Funktionen zu gewährleisten, im Einzelnen aufgeführt ist:

a. Ein mittels Signalen des frei zugänglichen Dienstes von Galileo und/oder in Zusammenarbeit mit anderen Satellitennavigationssystemen erbrachter und mit den internationalen Normen in Einklang stehender Beitrag zu Integritätsüberwachungsdiensten, die für die Nutzer sicherheitskritischer Anwendungen ("Safety-of-Life"-Anwendungen) bestimmt sind
b. Erbringung eines "kommerziellen Dienstes", der die Entwicklung von Anwendungen für professionelle oder kommerzielle Zwecke aufgrund besserer Leistungen und Daten mit höherem Mehrwert als im "offenen Dienst" ermöglicht
c. Erbringung eines öffentlich regulierten Dienstes, der ausschließlich staatlich autorisierten Benutzern für sensible Anwendungen, die eine hochgradige Dienstkontinuität verlangen, vorbehalten ist und für die Mitgliedstaaten, den Rat, die Kommission, den EAD und gegebenenfalls die ordnungsgemäß ermächtigten Agenturen der Union kostenlos ist; der "öffentlich regulierte Dienst" verwendet robuste, verschlüsselte Signale. Ob von den anderen PRS-Teilnehmern gemäß Artikel 2 des Beschlusses Nr. 1104/2011/EU Gebühren erhoben werden, wird von Fall zu Fall entschieden, und in den gemäß Artikel 3 Absatz 5 dieses Beschlusses geschlossenen Abkommen sind entsprechende Bestimmungen aufzunehmen

In der aktuellen Stakeholder Consultation GSA/ S C/ 30 / 17 on Galileo Commercial Service High Accuracy Provision Ref: 235530 Issue: 1 Rev 1 vom 17 November 2017 wird in der Einleitung formuliert: Galileo should “offer a commercial service (CS) for the development of applications for professional or commercial use by means of improved performance and data with greater added value than those obtained through the open service".

The Galileo Commercial Service (CS) is designed to deliver two services:

- A High Accuracy (HA) service offering centimetre - level accuracy worldwide through Precise Point Positioning (PPP) techniques. The target of this service is the professional market such as mapping, construction, agriculture or offshore.
- A Signal Authentication service to protect Galileo signals from hacking or spoofing attacks, mainly for critical applications as tracking of dangerous or valuable goods, or synchronisation of power grids or data networks. “

Damit liegen sehr gute Voraussetzungen vor, verlässliche Signale von Galileo zur genauen und sicheren Lokalisierung nutzen zu können.

Feststellung

Mit der fortgeschrittenen Satellitentechnologie, z.B. mit Mehrfrequenzsignalen, Richtungsantennen, Referenzstationen, Empfängern und Detektions- oder Plausibilisierungsalgorithmen können Störungen zunehmend identifiziert und damit eliminiert werden. Damit erscheint die Verwendung einer im rechtlichen Rahmen des Völker- und EU-Rechts betriebenen Satellitentechnologie zur absoluten Lokalisierung von Objekten im Bahnbereich machbar.

4.4.2 Auswahl geeigneter Komponenten zur Sensorik und Auswertung hinsichtlich Fehlerminimierung und –detektion

Unabhängigkeit der Sensorsysteme

Für ein hochgenaues, sicheres und verlässliches Lokalisierungssystem ist eine entsprechende Konfiguration von einzelnen Sensorsystemen Voraussetzung. Die Konfiguration des Lokalisierungssystems mit verschiedenartigen, unabhängigen Sensorsystemen ist erforderlich, da die inhärenten Fehlerarten einzelner Sensorsysteme mittels der Fehlerdetektion nur erkannt werden, wenn diese nicht gleichzeitig auftreten, was durch das Prinzip Verschiedenartigkeit (Dissimilarität, Diversität) axiomatisch und a priori ausgeschlossen wird. Gleichzeitig ermöglicht auch die Unabhängigkeit der Sensorsysteme die Detektion äußerer Störungen, da sich diese nicht systematisch auf mehrere Sensorsysteme gleichzeitig auswirken können.

Fehlerarten

Prinzipiell sind als Fehlerarten zu unterscheiden systematische und zufällige Fehler, zu ersteren können bei Sensoren z.B. Driftfehler und bei letzteren Sprung- und Impulsfehler gezählt werden. Fehlerarten systematischer Natur treten primär bei Algorithmen und Software auf, sind jedoch auch bei Hardware zu verzeichnen.

Eine andere Art der Fehlerklassifikation geht von der Fehlerursache aus. Hier sind aus dem Lokalisierungssystem selbst herrührende Fehler zu betrachten. Demgegenüber stehen Fehler, welche ihre Ursache außerhalb des Lokalisierungssystems haben. Neben Fehlern infolge Montage, Energieversorgung, äußerer Einwirkungen durch natürliche oder infrastrukturelle Umgebungseinflüsse und Instandhaltungsmaßnahmen sind insbesondere absichtliche oder unabsichtliche Störungen in Form von Bedrohungen, insbesondere elektromagnetischen Störungen im Umfeld des Bahnsystems, zu betrachten.

Fehleranalyse

Zur systematischen Analyse der Fehler bei den einzelnen Komponenten des Lokalisierungssystems ist eine FMEA zweckmäßig, aus der dann methodisch einzelne Maßnahmen zur Fehleridentifizierung, -vermeidung bzw. -minimierung auf den Ebenen der Sensoren bzw. der Sensordatenauswertung bzw. auf der Systemebene hergeleitet werden. Mit dem methodischen Ansatz der Generischen Gefährdungsliste nach Drewes/May werden für die in Frage kommenden Sensoren entsprechende Gefährdungen analysiert. Die betrachteten Fehlerarten sind in der Tabelle 4.13 zusammengestellt.

Systeme/Merkmale	**Potentielle Fehler**	**Potentielle Folgen des Fehlers**
Sensor - physikalisch	Mechanisch Elektrisch Thermisch/Klimatisch Elektromagnetisch Chemisch/Stofflich/Material	
Sensor – messtechnisch, funktional	Messtechnisch (w.B. Drift) Synchronisierung, Kalibrierung Datenfehler (code) Aktualität (zu früh, zu spät) Datenfehler (zu groß, zu klein) Algorithmenfehler	
Sensor - systematisch	Verbindungsfehler (z.B. Verdrahtung) Versorgungsfehler Montagefehler, Einbaufehler Vandalismus Instandhaltungsfehler Beschriftungsfehler	

Tabelle 4.13: Zusammenstellung potenzieller Fehlerarten von Sensoren nach dem Ansatz der generischen Gefährdungsliste

Digitale Karte

Als wesentliches Element zur Steigerung der Genauigkeit der Lokalisierung und Detektion möglicher Fehler ist die Integration eines digitalen Abbildes der aktuellen geografischen Eigenschaften des Streckennetzes, die sog. digitale Streckenkarte erforderlich. Mit dieser ist eine weitgehende Stützung der Satellitenlokalisierung durch etablierte Verfahren des Map Matching bzw. Mapping und Verfahren der Plausibilisierung zugunsten höherer Genauigkeit bzw. eindeutiger Fehlerdetektion möglich. Für die Sicherheit des Lokalisierungssystems wer-

den damit hohe Anforderungen an die aktuelle Richtigkeit der in den Karten verwalteten Informationen gestellt.

Feststellung

Mit geeignet qualifizierten Sensorsystemen und aktuellen Karteninformationen stehen geeignete unabhängige Komponenten zur Verfügung, welche in Kontext der Architektur und geeigneter Verarbeitungsalgorithmen einen signifikanten Beitrag zur Machbarkeit einer genauen und sicheren satellitenbasierten Lokalisierung von Objekten im Eisenbahnbereich ermöglichen.

4.5 Methodische Konzeption der sicheren Systemarchitektur

Die Systemarchitektur des genauen und sicheren Lokalisierungssystems wird in mehreren aufeinanderfolgenden Schritten konzipiert (vgl. [31]), die in diesem Abschnitt beschrieben werden:

1. Funktionsarchitektur (logisch-kausale Anordnung der Funktionsträger zur Erfüllung der Funktion, Auswahl des Überwachungskonzeptes
2. Redundanzkonzeptes der Sicherheits- und Verfügbarkeitsarchitektur
3. Parametrisierung der Gefährdungsrate
4. Platzierung der Komponenten (Systemintegration und Zuteilung der Sicherheitsanforderungen, räumliche Lokalisierung der Funktionsträger an/in den Einrichtungen des Systems, Zuteilung der Sicherheitsanforderungen
5. Kommunikationsarchitektur (Kommunikationsverbindungen zwischen den Funktionskomponenten)

4.5.1 Funktionale Systemarchitektur zur Lokalisierung durch Sensordatenauswertung und -fusion sowie zur Fehlerdetektion

Der Anspruch nach Sicherheit geht weit über den der Zuverlässigkeit hinaus. Für die Sicherheit müssen insbesondere die unzulässigen Systemzustände sorgfältig analysiert werden. Hier wird zwischen erkannten Fehlzuständen, aufgrund derer das System in einen gefahrlosen Zustand gesteuert wird und unerkannten Fehlzuständen, bei denen das Risiko einer Gefährdung bleibt, unterschieden.

Bei der Ermittlung der richtigen Position kann die Lokalisierung mit Hilfe absoluter Lokalisierung und relativer Lokalisierung erfolgen. Bei temporärer Unverfügbarkeit der absoluten Ortbestimmung kann durch Stützung mit der relativen Ortsmessung die absolute Position innerhalb zulässiger Fehlergrenzen ermittelt werden.

Da jedes Messsystem grundsätzlich fehlerbehaftet und damit a priori keine Integrität gewährleistet ist, müssen durch eine geeignete Architektur 1. einerseits die Fehler insbesondere hinsichtlich der Genauigkeit minimiert werden und 2. andererseits müssen Fehler insbesondere detektiert werden, um deren Einfluss auf das Messergebnis hinsichtlich der Vertrauenswürdigkeit sicherer Ergebnisse auszuschließen und ggf. darüberhinaus 3. fehlerbehaftete Quellen identifiziert und von der Ergebnisermittlung ausgeschlossen werden und 4. nach Wiedererlangung der Funktionsfähigkeit - durch Beseitigung der Ursachen - wieder in die Funktionsstruktur eingeschleust werden.

Das Grundprinzip einer Architektur zur Lokalisierung von Objekten im Schienenverkehr basiert auf verschiedenen Prämissen:

- Verschiedenartigkeit ist das Prinzip zur Vermeidung systematischer Fehler. Damit müssen die einzelnen Sensorsysteme verschieden und unabhängig sein.
- Nur ein einziger (zufälliger) Fehler tritt zum selben Zeitpunkt auf. Diese axiomatische Begründung setzt die Unabhängigkeit gleichwohl homogener wie heterogener Sensorsysteme voraus. Damit wird ein Mehrfachausfall zu einem Zeitpunkt ausgeschlossen. Zur Erkennung eines Ausfalls eines Sensorsystems und dessen Anzeige zur Gewährung eines Fail Safe Verhaltens ist daher ein weiteres Sensorsystem erforderlich.
- Zur Erkennung eines fehlerhaften Sensorsystems dient das Prinzip des Vergleichs oder der Mehrheitsentscheidung. Zu dieser Erkennung muss die Verarbeitung sicher durchgeführt werden. Diese Entscheidung einer Ausfallerkennung – entweder der Sensoren oder der Verarbeitung - muss abgeschlossen sein, bevor ein zweiter Ausfall stattfindet und somit eine falsche Majoritätsentscheidung zur Fehlerdetektion gefällt wird. Damit ist eine Fehleroffenbarungsdauer so zu wählen, dass innerhalb dieses Zeitraums mit der verlangten tolerierbaren Gefährdungsrate kein zweiter Ausfall auftritt, so dass die Übereinstimmung zweier falscher Werte ausgeschlossen wird.
- Zur Erhöhung der Verfügbarkeit sind auch nach Erkennung eines Ausfalls weitere richtig funktionierende Sensorsysteme erforderlich. Das fehlerhafte Sensorsystem muss für die Fehlerdauer von der Lokalisierungsermittlung ausgeschlossen sein (Maskierung). Eine Prüfung der Wiedererlangung seiner richtigeren Funktion eröffnet die Wiedereingliederung in das Lokalisierungssystem zur Erhöhung der Verfügbarkeit.

4.5.2 Funktionale Architekturvarianten

Um zu verhindern, dass der Messprozess einen sicherheitskritischen, d.h. unzulässigen Zustand einnimmt, entweder infolge eines Defekts im Sensorsystem oder eines Defekts im Auswertungssystem, sind zwei verschiedene funktionale Sicherungskonzepte anwendbar (vgl. [32]).

Präventivsicherung. Hier ist der Messprozess selbst sicher, d.h. alle Funktionen der Messung müssen sicherungstechnischen Prinzipien gehorchen. Abbildung 4.15 veranschaulicht dieses Konzept.

In einem ersten Funktionsblock wird aus den verschiedenen Informationen der einzelnen Sensorkomponenten einschließlich einer digitalen Karte durch die Algorithmen der Sensordatenfusion der Ortszustand ermittelt. Ergänzend werden die verfügbaren Informationen zur Residuenbildung benutzt, d.h. die einzelnen Informationen werden hinsichtlich bestehender Unterschiede und Abweichungen analysiert. Auf Grund dieser Informationen wird dann geprüft, ob ihre Abweichungen noch akzeptabel sind und daraufhin entschieden, ob die Integrität der Lokalisierung noch besteht oder nicht. Diese Information kann nachfolgend verwendet werden, um die Nutzungsfunktion durch Maßnahmen der Sicherung in einen sicheren Zustand (fail safe) zu überführen.

Diese integrierte sichere Messung erfordert infolge der hohen Anforderungen an die Sicherheitsintegrität einen hohen Aufwand für die Entwicklung, Implementierung und Nachweisführung aller Funktionsblöcke.

Kausalsicherung. Durch eine von der eigentlichen Lokalisierungslösung unabhängige und getrennte sichere Überwachung wird der Messprozess beobachtet, wie Abbildung 4.16 zeigt. Würde dadurch ein unzulässiger Messzustand erkannt, so wird eine entsprechende Integritätsmeldung ausgegeben. Diese klare Trennung zwischen Messprozess und Überwachung erlaubt einfache und überschaubare informationelle wie technische Lösungen der Sicherungsfunktionen.

Die Strukturen der Präventiv- und Kausalsicherung können noch weiter dekomponiert werden, indem sie auch für einzelne Ortungsgrößen oder Ortungsvektorkomponenten verwendet werden.

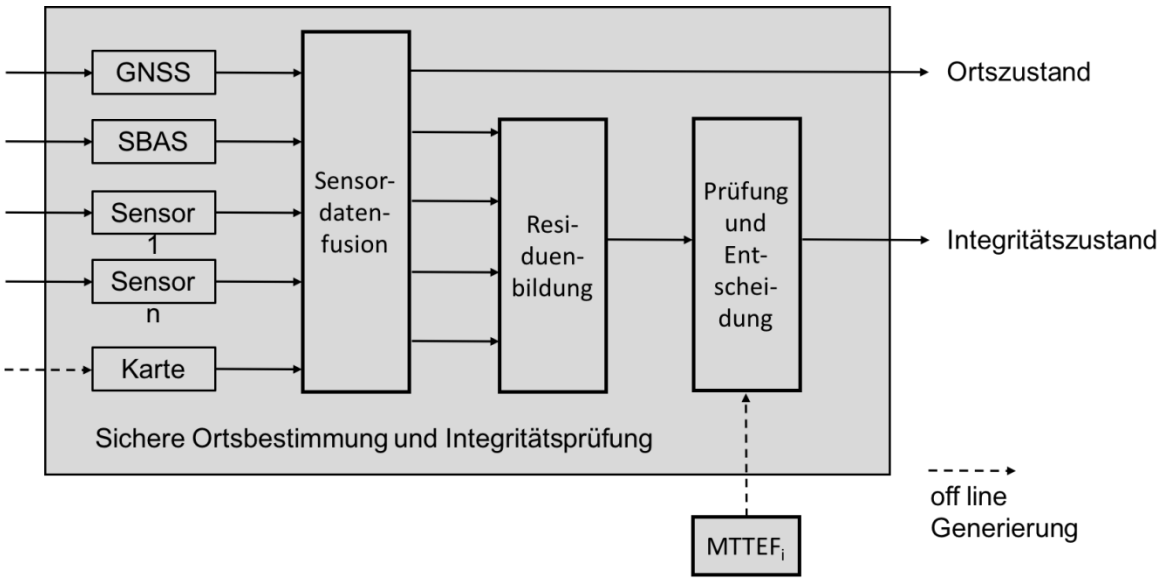


Abbildung 4.15: Funktionale Architektur des Lokalisierungssystems mit sicherer Ortbestimmung und Integritätsprüfung

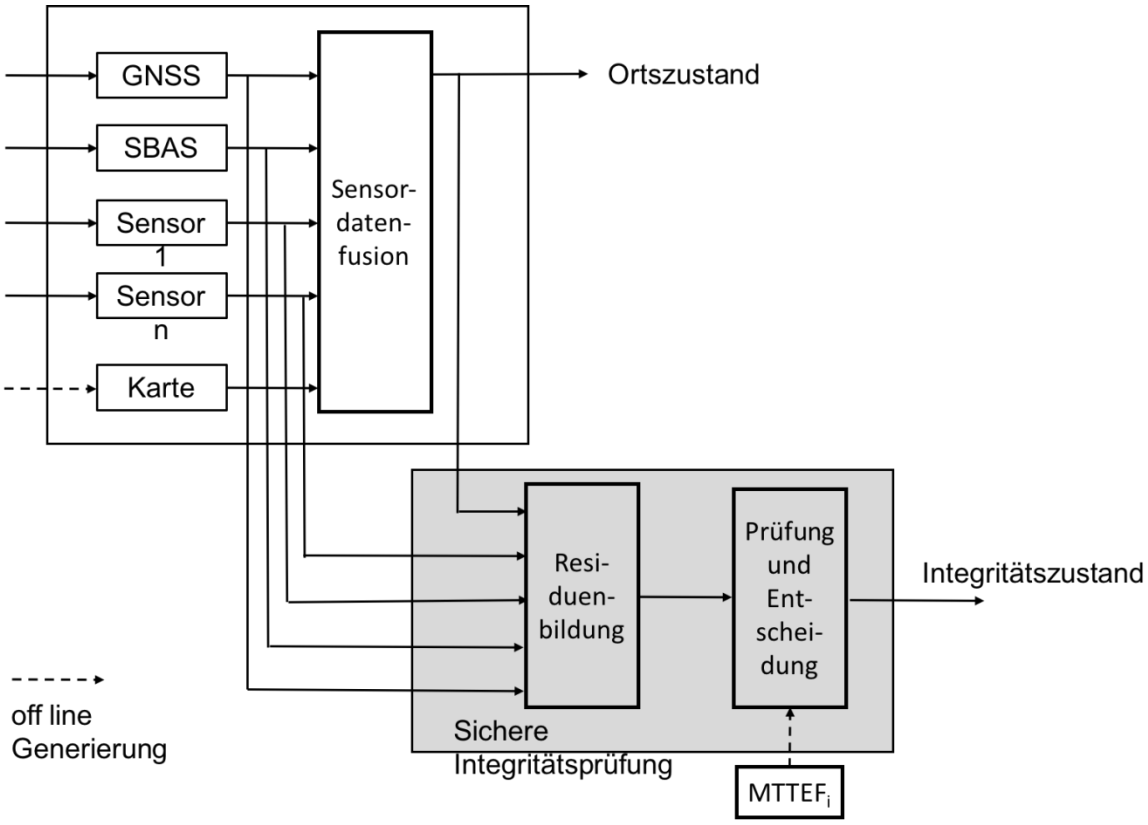


Abbildung 4.16: Funktionale Architektur des Lokalisierungssystems mit sicherer Integritätsprüfung

Aufgrund der zu erwartenden komplexen Algorithmen für die genaue und sichere Lokalisierung ist eine Trennung der Funktionsblöcke nach folgender Aufgabenteilung zweckmäßig:

- Berechnung der genauen Lokalisierungslösung mit einem hochzuverlässigen Multisensorsystem, Ausgabe des Lokalisierungszustandes und ggf. Angabe eines Vertrauensintervalls. Diese Aufgabe kann bestenfalls ohne Sicherheitsverantwortung realisiert werden.
- Überwachung der richtigen Lokalisierung mit einem hochverfügbaren sicheren Überwachungssystem unter Verwendung qualifizierter Sensorsysteme, Ausgabe des Integritätszustandes - entweder binär oder mit Vertrauensintervall**.**

Feststellung: Im ersten Ansatz resultiert aus dieser Betrachtung, die Lokalisierung durch ein redundantes diversitäres Multisensorsystem mit qualifizierter Sensorsystemen und hochverfügbaren Verarbeitungseinheiten zu verwirklichen. Die Berechnung der genauen Lokalisierungslösung ist mit einem hochzuverlässigen Multisensorsystem und die Integrität der richtigen Lokalisierung ist mit einem hochverfügbaren und sicheren Überwachungssystem unter Verwendung qualifizierter Sensorkomponenten machbar. Eine detaillierte Anforderungsbestimmung der Sicherheitsintegrität der einzelnen Sensorkomponenten des Überwachungssystems und der Sensorsysteme muss dazu gesondert durchgeführt werden.

4.5.3 Konzeption der Redundanzstruktur

Die Sicherheit wird durch das Prinzip des Vergleichs mit einfacher oder Majoritätsredundanz erreicht. Zur Erfüllung der Sicherheit werden in der Regel parallel redundante Teilsysteme verwendet. Eine einfache Anordnung ist die 2v2 Struktur.

Dabei wird allgemein vorausgesetzt,

- dass alle Teilsysteme stochastisch unabhängig sind
- dass jedes Teilsystem für sich nach einem Ausfall wieder in den funktionsfähigen Zustand nach Änderung der Messbedingungen kommt oder durch Reparatur wieder in den funktionsfähigen Zustand gelangt
- dass eine unabhängige Vergleichsfunktion oder mehrere die Abweichung innerhalb einer definierten Fehleroffenbarungszeit erkennen

Diese Erkennung wird durch eine eigenständige Vergleichsfunktion erzeugt, die ebenfalls ein- oder zweikanalig realisiert werden kann. Die Vergleichskomponente wird im Folgenden als fehlerfrei angenommen, um die prinzipielle Vorgehensweise darzustellen. Nur wenn beide Teilsysteme das gleiche Ergebnis liefern, wird es als richtig erkannt. Unterschiedliche Ergebnisse werden als fehlerhaft erkannt. Die fehlerhafte Komponente kann mit dieser 2v2 Anordnung nicht identifiziert werden. Dazu ist eine Majoritätsredundanz mit einer m v n Struktur und m größer n/2 und kleiner n notwendig, z.B. 2v3.

Sicherheit wird immer dann gewährt, wenn mindestens eine oder mehrere Komponenten intakt sind, d.h. wenn eine mvn-Struktur mit $n \geq m > n/2$, d.h. Parallelredundanz für die Funktion der Ausfallerkennung vorausgesetzt wird. Innerhalb der Fehleroffenbarungszeit τ kann durch die Vergleichsfunktion entschieden werden, ob die Ergebnisse übereinstimmen oder nicht. Die Fehleroffenbarungszeit τ bestimmt sich aus der Antwortzeit der Überwachungsfunktion mit ihrer Prüfung und Entscheidung. Diese kann nach einer Berechnungsvorschrift (10-23) nach [32] ermittelt werden, die jüngst in der Dissertation von Diekhake bestätigt wurde (vgl. [33]).

Komplementär tritt eine Gefährdung auf, wenn $m > n/2$, d.h. mehrere oder alle Komponenten ausgefallen sind und im schlechtesten Fall keine Abweichung festgestellt wird, z.B. beide bei einer 2v2 Struktur. Dies trifft auch für den Fall systematischer Fehler zu. Es wird dann vereinfachend und schlechterdings angenommen, dass die Gefährdung und der Schaden sofort eintritt und keine Reparatur aus der Gefährdung herausführt.

4.5.4 Parametrisierung der Gefährdungsraten

Bei der Messung kontinuierlich veränderlicher Positionen treten prinzipiell Messunsicherheiten und -abweichungen auf (vgl. 4.4.2). Infolge der Natur kontinuierlicher Zustandswerte und Unsicherheiten bei deren messtechnischer Erfassung weisen einzelne Sensorsysteme unterschiedliche Streuungen der Messwerte sowie verschiedene Mittelwerte auf, welche durch die Merkmale Präzision und Richtigkeit beschrieben werden und in der Eigenschaft Genauigkeit zusammengefasst werden. Aufgrund des oben begründeten Ansatzes zur Fehlerdetektion sind einerseits mehrere unabhängige Sensorsysteme zur Lokalisierung erforderlich. Für den Vergleich der Messwerte wird ein sicherheitsrelevantes Vertrauensintervall SRIC angesetzt, in dem sich verschiedene Messwerte befinden dürfen, ohne dass eine fehlerhafte Abweichung detektiert wird.

Im Folgenden werden methodische Aspekte zur Erzeugung sicherer Lokalisierungswerte und zur Detektion fehlerhafter Werte beschrieben. Der hierfür vorgeschlagene Ansatz beruht auf der Überlegung, dass eine statistische Betrachtung von Verteilungen der Messwerte sowohl für die Genauigkeit als insbesondere für die Sicherheit hoher SIL-Stufen nicht zielführend ist, wie bei der Betrachtung zu den Use Cases 1.1.5/6 und dortigen Feststellung 5 argumentiert wird. An dessen Stelle wird für die sicherheitsrelevante Fehlerdetektion ein Ansatz verwendet, der - wie in den Anforderungen auf Grundlage der Use Cases genutzt - eine Rechteckverteilung als Begrenzung zulässiger Lokalisierungswerte fordert. Die Grenzen dieser Rechteckverteilung werden als sicherheitsrelevantes Vertrauensintervall (Safety Related Interval of Confidence SRIC) bezeichnet. Solange das Sensorsystem Werte innerhalb dieser Grenzen liefert, wird es als zuverlässig funktionsfähig angesehen und diesem Zeitraum eine Time To (Extended) Failure (MTTEF) im Sinne der Theorie der Zuverlässigkeit zugeschrieben.

Mit diesem Ansatz wird der Übergang von der Modellwelt der kontinuierlichen Verteilungsfunktionen der Genauigkeit in die Modellwelt stochastischer Prozesse der Zuverlässigkeit ermöglicht. Damit wird die problematische Zuordnung der Sicherheitsintegrität zu Verteilungsfunktionen umgangen. Diese wird jedoch z.B. für die Parametrierung der Filter für die Sensordatenfunktion genutzt, welche nicht mehr sicherheitsrelevant ist, wobei das Prinzip der Kausalsicherung verwendet wird. Diese Bearbeitung kann zur Verbesserung der Genauigkeit beitragen, wenn die Methoden der Sensordatenfusion und andere, z.B. Fehlerkompensation oder automatische Kalibrierung genutzt werden.

4.5.5 Leer

4.5.6 Leer

4.5.7 Systemintegration und Zuteilung der Sicherheitsanforderungen

Die Integration der Lokalisierung in das Gesamtsystem zeigt die Abbildung 4.17 für das gesamte System. Die in den GLAT-Endgeräten der Lokalisierungsobjekte generierte Information wird dabei über ein nachrichtentechnisches Transfersystem an die GLAT-Zentrale kommuniziert.

Insgesamt ergeben sich dabei mehrere Kontaktstellen zu den Funktionseinheiten

- Kommunikations-/Transfersystem mit Kontaktstellen seitens der Lokalisierungsendgeräte und seitens der Lokalisierungszentrale
- GLAT-Zentrale
- Zugseitige Leit- und Sicherungstechnik (ETCS OBU)
- Warnung von Personen im Gleisbereich
- GLAT Tag

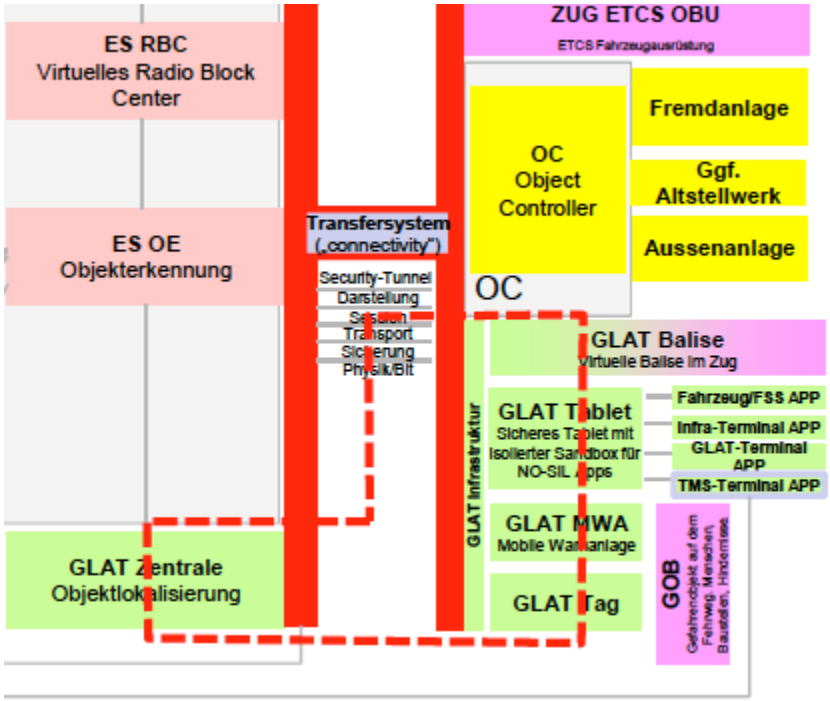


Abbildung 4.17: Integration der Lokalisierung in das Gesamtsystem

Im Rahmen eines übergeordneten, aber modularen Sicherheitskonzepts wird zuerst eine Betrachtung der Kapselung der sicheren Lokalisierung der Endgeräte vorgenommen. Durch diesen modularen Ansatz gekapselter sicherer (Teil-)Systeme ist eine Migration und später auch eine rückwirkungsfreie Adaption des Systems möglich.

Das GLAT-Endgerät ist die technische Einrichtung, welche selbständig und autonom, z.T. unter verfügbarerer elektrischer Energieversorgung von außen, die Position eine Objektes im Eisenbahnbereich für eine spezifische Anwendung (Use Case) hinreichend genau und sicher durch Angabe von Positions- und Bewegungsinformationen digitaler Form bezüglich eines definierten topologischen oder geographischen Bezugskoordinatensystems zeitgerecht ermittelt und an definierten Schnittstellen sicher zur Verfügung stellt.

Die GLAT-Zentrale empfängt über das Transfersystem die Lokalisierungsinformationen der GLAT-Endgeräte. Zwecks weiterer Erhöhung der Sicherheitsintegrität und Genauigkeit können hier weitere Be- und Verarbeitungen der Lokalisierungsinformationen durchgeführt werden. So ist z.B. die Vorhaltung einer – vom Stellwerk aktualisierten - digitalen Streckenkarte des gesamten Netzes hier zweckmäßig, um nicht die Konsistenz zu gefährden und Verteilung sowie die Datenhaltung auf den Endgeräten zu belasten.

Aus diesen Überlegungen resultiert unter Berücksichtigung des GLAT Konzepts mit dezentralen Sensorkomponenten in den Lokalisierungsobjekten und einem zentralen GLAT Server (auch als GLAT-Zentrale bezeichnet) ein verteiltes Architekturkonzept, welches den Aufwand zur Sicherheitsgewährung klein hält:

1. Trennung der Lokalisierungsfunktion (LL) von der Sicherheitsprüfung (Ü). Ergebnis dieser getrennten Funktionen sind a) eine genaue Ortungsinformation (OI) und b) eine signaltechnisch sichere Integritätsinformation (Integrität).
2. Verteilte Platzierung der Funktionen.
   2.1 Mit den im Lokalisierungsobjekt verfügbaren Sensorsignalen werden hier im GLAT Endgerät die genaue Ortungsinformation berechnet und in einer separaten Überwachung auf Integrität geprüft.
   2.2 Ortungs- und Integritätsinformation werden vom GLAT Endgerät zum GLAT Server übertragen.
   2.3 Dem GLAT Server werden der aktuelle Streckenatlas (Karte) und/einschließlich aktuelle Informationen über die Weichenlagen geliefert (dies verringert den Aufwand eine konsistente Datenhaltung aktueller Karten bei den Lokalisierungsobjekten).
   2.4 Der GLAT Server berechnet die aktuellen genauen Ortungsangaben der Lokalisierungsobjekte und prüft diese in einer separaten Überwachung auf Integrität. Diese Informationen werden anderen Funktionseinheiten, z.B. Stellwerk kommuniziert.
   2.5 Ggf. wird die Integritätsmeldung dem GLAT Endgerät beim Lokalisierungsobjekt kommuniziert (direkt oder über eine MA).

Abbildung 4.18 zeigt einen Ansatz zur Funktions-, Sicherheits- und Kommunikationsarchitektur für eine Fahrzeuglokalisierung nach dieser Konzeption.

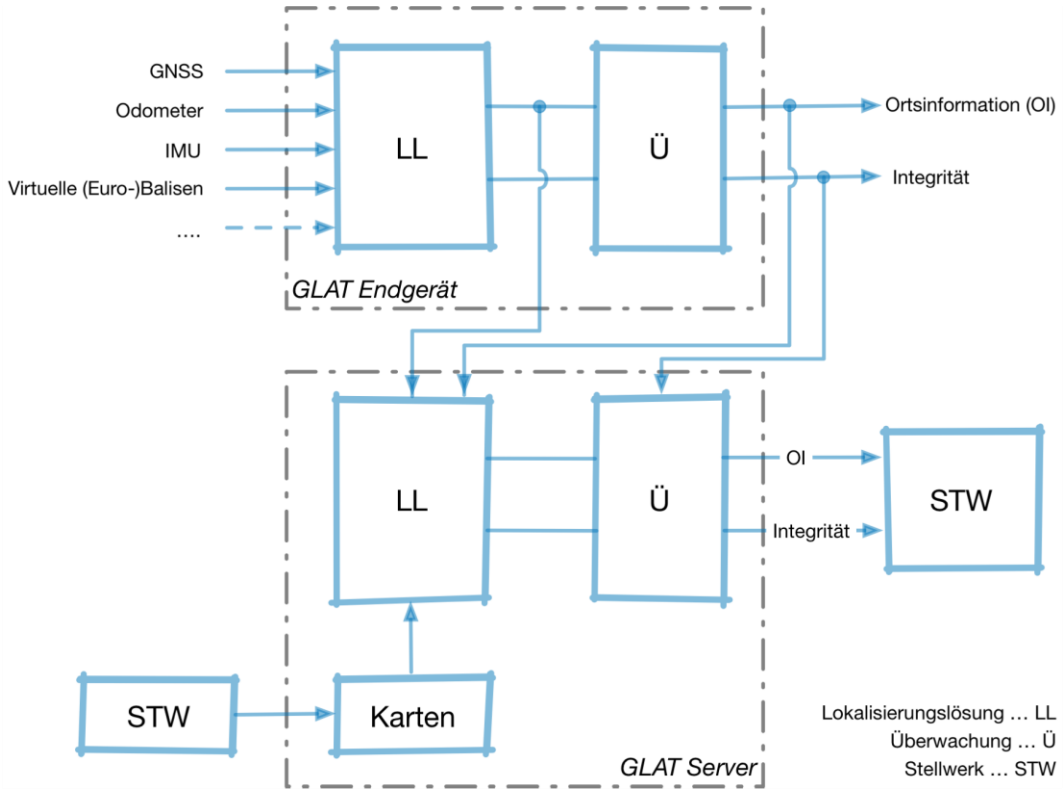


Abbildung 4.18: Modulare Funktions- und Sicherheitsarchitektur für eine Fahrzeuglokalisierung

Hier ist einerseits die sichere Kommunikation eine Voraussetzung, andererseits die richtige Ortsangabe. Unter der Voraussetzung, dass die Kommunikation sicher ist einschließlich der Detektion falscher Kommunikation, werden die Auswirkungen einerseits der Latenz richtiger Positionsangaben und andererseits die Auswirkung bzw. Detektion falscher Positionsangaben hinsichtlich einer Gefährdung und Risikos analysiert.

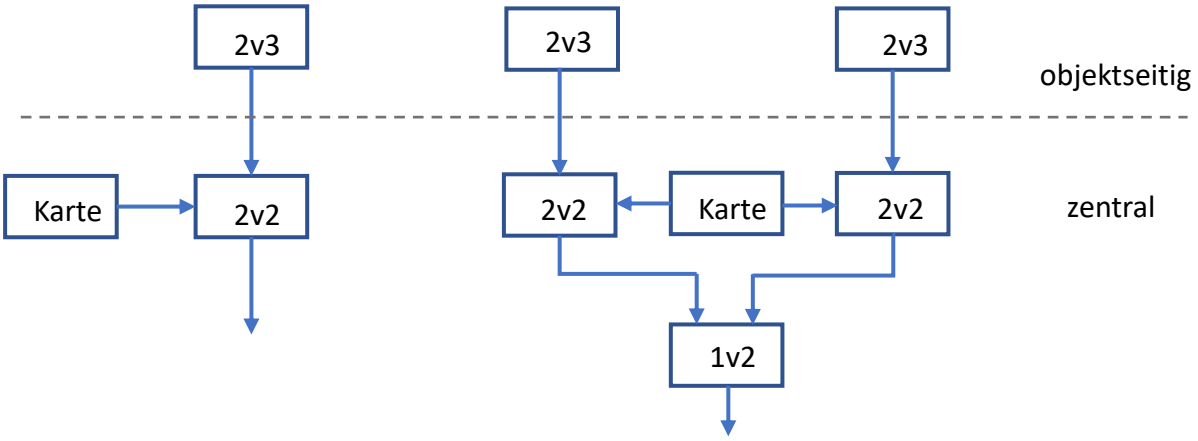


Abbildung 4.19: Prinzipielle Konfigurationen zur sicheren Lokalisierung, links eine einfache Struktur und rechts eine aufwendigere zur Erhöhung der Verfügbarkeit

Abbildung 4.19 zeigt zwei Beispiel für prinzipielle Konfigurationen zur sicheren Lokalisierung.

4.5.8 Feststellung

Sicherheit kann durch Parallelredundanz stochastisch unabhängiger Teilsysteme mittels Koinzidenz ihrer Ergebnisse erzeugt werden. Die resultierende Gefährdungsrate ist dabei um Größenordnungen geringer als die Ausfallrate eines Teilsystems, wenn eine kurze Ausfalloffenbarungszeit gewährt wird.

Zu beachten ist allerdings, dass für die Verfügbarkeit einer satellitengestützten Lokalisierung weitere redundante Sensorkomponenten erforderlich sind, welche ein komplementäres Ausfallverhalten zeigen sollten. Zur Erhöhung der Sicherheit und der Verfügbarkeit ist eine höher redundante Struktur notwendig. Je nach Anwendungsbereich bzw. Lokalisierungsobjekt sind entsprechende Risiko- und Gefährdungsanalysen als Grundlage zur Fehlerdetektion durchzuführen.

Bei Kenntnis der individuellen Verlässlichkeitsmerkmale und ihrer Kennwerte der Ausfall- und Reparaturraten der Lokalisierungssensoren ist mit einer geeigneten redundanten Konfiguration und Überwachung mit entsprechender Ausfalloffenbarungszeit eine exakte Parametrisierung der Gefährdungsrate und der Verfügbarkeit des Gesamtsystems simulativ möglich und erforderlich.

Mit der fortgeschrittenen Entwicklung von Algorithmen zur Sensordatenfusion und Fehlerdetektion von Multisensorsystemen und ihren Anwendungen zur Lokalisierung liegen erprobte Grundlagen vor, die einen signifikanten Beitrag zur Machbarkeit einer genauen und sicheren Lokalisierung von Fahrzeugen und andern Objekten im Eisenbahnbereich leisten.

Damit stehen die notwendigen Grundlagen für die Machbarkeit einer genauen, sicheren und verfügbaren satellitenbasierten Lokalisierung zur Verfügung.

5. Schwerpunktbereich „Zulassungsfähigkeit“

Zusammenfassung

In dieser Machbarkeitsstudie konzentriert sich die Betrachtung der Zulassungsfähigkeit auf die technische Machbarkeit entsprechend dem technischem Sicherheitsbericht der EN 50129. In Zusammenhang mit einem übergeordneten Risikomanagement werden Fragen der Zulassung, wie Konformität mit den Regularien der europäischen Interoperabilität und der Rechtssicherheit von Satellitensystemen, nicht behandelt und sollten separat untersucht werden.

Die Betrachtung der Zulassungsfähigkeit basiert auf folgenden Voraussetzungen

- Normativer Rahmen
- Use Cases und Zulassung
- Entwicklung einschließlich Nachweisführung
- Zulassung von Satellitengestützten Lokalisierungssystemen für Eisenbahnen

Normativer Rahmen

Für die Zulassung eines Satellitengestützten Lokalisierungssystems im Eisenbahnbereich existiert in Europa ein umfassender Rechtsrahmen, in den sich auch die Schweiz eingliedert. Der Rechtsrahmen umfasst Eisenbahngesetze, Verordnungen und insbesondere Normen für die Entwicklungs- und Begutachtungsprozesse von Eisenbahnanlagen und -einrichtungen. Satellitensysteme sind ebenfalls in entsprechende Rechtssysteme eingebunden. Allerdings liegen für die Integration der reinen Satellitenortung in die Eisenbahntechnik keine Regelwerke vor.

Use Cases und Zulassung

Dank der Clusterung der Use Case hinsichtlich ihrer Lokalisierungsfunktion, Sicherheitsanforderungsstufen und Platzierung auf Lokalisierungsobjekten kann die Zulassung modular hinsichtlich generischer und anwendungsspezifischer Nachweisführungen durchgeführt werden.

Obwohl der Aufwand für die Nachweisführung aufgrund fundamental anderer Technologien nicht unerheblich sein wird, ist doch die damit gewonnene Abdeckung für sehr viele Use Cases von wirtschaftlichem Vorteil.

Es empfiehlt sich, die Nachweisführung in lokale und zentrale Anteile zu trennen, zugelassene Produkte und vorhandene Nachweise einzelner Komponenten zu nutzen und die spezifischen Nachweise sukzessiv durchzuführen, um vom fortschreitenden Erkenntnisgewinn bei

Nachweisführung, Begutachtung und Zulassung zu profitieren. In jedem Fall ist eine entwicklungsbegleitende Begutachtung effizient und machbar, wenn geeignet qualifiziertes Personal verfügbar ist.

Entwicklung einschließlich Nachweisführung

Für den Zulassungsprozess mit seinen Aufgaben und Rollen ist die Vorlage eines positiv begutachteten Sicherheitsnachweises mit dem normgerechten erstellten technischen Sicherheitsbericht und Anerkennung eines Qualitäts- und Sicherheitsmanagementsystems notwendig. Durch die Struktur des Sicherheitsnachweises und -berichtes sowie das damit verbundenen Vorgehen wird nachgewiesen, dass Gefährdungen mit Hilfe eines geeigneten Prozesses identifiziert wurden und praktikable Maßnahmen zur Schadensminderung und zum Umgang mit Risiken, die von den identifizierten Gefährdungen ausgehen, eingeführt wurden. Methodisch ist Machbarkeit des Sicherheitsnachweises sichergestellt, allerdings sind die durch die Satellitenstützung entstehenden neuen Risiken aufzuzeigen und ihre organisatorische und technische Beherrschung spezifisch darzulegen.

Zulassung von Satellitengestützten Lokalisierungssystemen für Eisenbahnen

Die offene Frage der Integration einer außerhalb des Eisenbahnwesens existierenden Infrastruktur der Satellitensysteme mit ihren Raum- und Bodensegmenten kann durch Cross Acceptance und einen speziellen methodischen Ansatz für das Nutzersegment (Empfänger und Antenne) gelöst werden. Der Ansatz fußt auf einer sicheren Überwachung der Integrität einer verfügbaren satellitengestützen Lokalisierung. Seine Voraussetzungen sind

1. Garantierte Signalversorgung durch das Raum- und Bodensegment des Satellitenortungssystems und
2. qualifizierte Sensoren und Ermittlung von Merkmalsgrößen wie Dauer zwischen Ausfällen (MTTEF), Genauigkeiten u.a.

Insbesondere müssen dazu die GNSS-Empfänger nach metrologischen Verfahren qualifiziert werden, um ihre spezifischen Merkmalsgrößen zu ermitteln. Erfüllbare Voraussetzungen dafür sind normkonforme Beschreibungen der Messbedingungen, der Prüfprozeduren und Referenzen und der Prozeduren für die Auswertung der Tests und Darstellung der Ergebnisse sowie eine Zertifizierung, die von existierenden akkreditierten Institutionen erbracht werden können. Weiterhin gehört hierzu die konventionelle Qualifizierung von weiteren Sensoren oder die Nutzung bereits im Eisenbahnwesen verwendeter. Hinzu kommt die Verfügbarkeit einer qualifizierten aktuellen referenzierten digitalen Karte des Streckennetzes. Die Erstellung einer sicheren Detektion zur fehlerhaften Lokalisierung mit normkonform entwickelten

und implementierte Algorithmen auf der Grundlage der qualifizierten Parameterwerte erfolgt nach bewährten Vorgehensweisen.

Die Entwicklung des sicheren Lokalisierungssystems insgesamt kann somit normgerecht nach den einschlägigen Vorschriften der Entwicklung sicherheitskritischer Systeme des Eisenbahnsektors durchgeführt werden.

Eine Zulassung eines sicheren satellitengestützten Lokalisierungssystems im Eisenbahnbereich erscheint unter Beachtung der genannten Voraussetzungen machbar.

5.1 Leer

5.2 Leer

5.3 Normativer Rahmen

Dieses Thema wurde im Rahmen der Machbarkeitsanalyse ebenfalls behandelt. Die Zusammenfassung des Themas (Feststellung) ist untenstehend aufgeführt. Die detaillierten Erörterungen zu

- Europäischer Rechtsrahmen zur Verlässlichkeit bei Eisenbahnen
- Nationaler Schweizer u.a. Rechtsrahmen zur Verlässlichkeit bei Eisenbahnen
- Europäische Normen zur Verlässlichkeit bei Eisenbahnen (CENELEC)
- Internationaler Rechtsrahmen zur Konformitätsbewertung
- Rechtsrahmen zur Satellitenortung
- Institutionen, Rollen, Zuständigkeiten Verantwortungen im Eisenbahnwesen

werden hier nicht wiedergegeben.

Feststellung
Für die Zulassung eines Satellitengestützten Lokalisierungssystems im Eisenbahnbereich existiert in Europa ein umfassender Rechtsrahmen, in den sich auch die Schweiz eingliedert. Der Rechtsrahmen umfasst Eisenbahngesetze, Verordnungen und insbesondere Normen für die Entwicklungs- und Begutachtungsprozesse von Eisenbahnanlagen und -einrichtungen sowie Stellen, die in diesen Prozessen verantwortlich sind. Satellitensysteme sind ebenfalls in entsprechende Rechtssysteme eingebunden. Allerdings liegen für die Integration der reinen Satellitenortung in die Eisenbahntechnik keine Regelwerke vor.

5.4 Use Cases und Zulassungsprozess

Im Abschnitt 5.4 werden die im Schwerpunkt „Use Cases“ herausgearbeiteten Klassen von Lokalisierungen von Lokalisierungsobjekten, die durch gemeinsame Aufgaben, Funktionen und Prozesse sowie Anforderungen der genauen und sicheren Lokalisierung gekennzeichnet sind, unter Berücksichtigung einer prinzipiellen Zulassungsfähigkeit für ein zu entwickelndes Lokalisierungssystem bis zur Sicherheitsintegritätsstufe SIL 4 im Kontext des ELSS diskutiert.

Zuerst werden im Abschnitt 5.4.1 der Normativer Rahmen und zuständigen Institutionen für die Zulassung der einzelnen Lokalisierungsfunktionen vorgestellt.

Als Voraussetzung für die Nachweisführung werden dann im Abschnitt 5.4.2 generische und spezifische Aspekte der Zulassung und Nachweisführung zuerst allgemein betrachtet, um nach Zuordnung der Use Cases zu den Funktionen und dazu geforderten Integritätsstufen in Abschnitt 5.4.3 sowie den Grundkonzepten der sicherheitsbezogenen Architektur aus dem Schwerpunktkapitel 4 die einzelnen Komponenten in generischen und spezifischen Teilen eines modularen Zulassungskonzeptes zu entwickeln.

Auf dieser Grundlage werden dann spezifische Aspekte der Zulassungsfähigkeit behandelt.

5.4.1 Use Case bezogene Zulassungsaspekte

Die im Schwerpunkt „Use Cases“ herausgearbeiteten Klassen von Lokalisierungsfunktionen und -objekten, die durch gemeinsame Aufgaben, Funktionen und Prozesse sowie Anforderungen der genauen und sicheren Lokalisierung gekennzeichnet sind, werden unter Berücksichtigung einer prinzipiellen Zulassungsfähigkeit für ein zu entwickelndes Lokalisierungssystem bis zur Sicherheitsintegritätsstufe SIL 4 im Kontext des normativen Rahmens, Zuordnung der Regelwerke und Stellen der Begutachtung sowie der Zulassung betrachtet.

Auf dieser Grundlage können dann spezifische Aspekte der Zulassungsfähigkeit behandelt werden. Denn aufgrund der unterschiedlichen Rahmenbedingungen müssen die jeweiligen Use Cases der zutreffenden Normativen Grundlage, der betreffenden Institution zur Begutachtung und der verantwortlichen Institution zur Inbetriebnahmegenehmigung zugeordnet werden. Tabelle 5.14 zeigt die Zuordnung der Use Cases mit den Lokalisierungsobjekten zu den Regelwerken, den zuständigen Stellen für die Begutachtung und den verantwortlichen Institutionen zur Zulassung für die einzelnen Lokalisierungsfunktionen.

Lokalisierungs-Gegenstand/ -funktion	Use Case	Normative Grundlage	Stelle zur Begutachtung	Institution zur Inbetriebnahmegenehmigung
Fahrzeuge u.a. zur Zugbeeinflussung	1.1.5, 1.4, 1.5	EU-Regelwerke NNTV NTV	NoBo DeBo DeBo	ERA BAV
Informationen: ETCS-Tafel, (virtuelle) Balise	1.1.5, 1.5 6.2 7.1, 7.2, 7.3	EU Regelwerke	NoBo DeBo AsBo	ERA BAV
Fahrzeuge u.a. zur Gleisfreimeldung	1.1, 1.2, 1.3, 1.6,	NNTV NTV	DeBo AsBo	BAV
Menschen im Gleis	2	NTV	AsBo	BAV Aufsichtsämter
Infrastrukturobjekte zur Baustellensicherung	3	NTV	AsBo	BAV Aufsichtsämter
Naturobjekte	3.1.7	NTV	AsBo	BAV Aufsichtsämter
sonstige Objekte	1.1	NTV	AsBo	BAV Aufsichtsämter

Tabelle 5.14 Normativer Rahmen und Institutionen für die Zulassung der einzelnen Lokalisierungsfunktionen

5.4.2 Generische und spezifische Aspekte der Zulassung und Nachweisführung

Für die Zulassung eines im Eisenbahnsystem sicherheitsverantwortlichen Systems durch eine zuständige Institution, z.B. das BAV oder EBA, muss dabei im Einzelnen unterschieden werden nach

- einer generischen Typzulassung für ein neues Lokalisierungssystem, sich beziehend auf die Lokalisierungslösung ohne konkreten Anwendungsfall und
- einer anwendungsspezifischen Zulassung. Dies ist Voraussetzung für die Anwendung des Lokalisierungssystems, z.B. in konkreten Einsatzfällen eines Eisenbahnsystems, die z.B. nach Lokalisierungsfunktionen und Objekten der Use Cases beschrieben werden (vgl. auch Kapitel 3).

In ähnlicher Methodik wie bei der generischen Typzulassung wird auch für eine spezielle Anwendung bei der für die Zulassung der Anwendung des Lokalisierungssystems, z.B. in kon-

kreten Einsatzfällen eines Eisenbahnsystems vorgegangen. In dessen umfassenderen Sicherheitsnachweis wird für die vorzulegende Gefährdungs- und Risikoanalyse die Nutzung der Lokalisierung im gesamten System betrachtet, indem die Auswirkung von Gefährdungen der Lokalisierungslösung im systemischen Zusammenhang des ELSS betrachtet wird, wobei wiederum auf die Use Case Cluster bzw. fallspezifisch auf eine FMEA zurückgegriffen wird. Als hilfreich wird sich hier die Clusterung der Nutzungsfunktionen (vgl. Tabelle 5.14 und Tabelle 5.15) erweisen, um den Aufwand nicht für 60 Use Cases explizit durchzuführen.

Als weitere Voraussetzung für die Erstellung des Sicherheitsberichtes und der Risikoanalyse im Sicherheitsnachweis wird auch die Europäische Verordnung CSM RA 2015/1136 in der Nachfolge der Verordnung 402/2013 angesehen. Hier sind speziell im Annex 3 drei Verfahren zur Risikoabschätzung angegeben. Ein konkreter Vorschlag hierzu ist der Ansatz zur Risikoanalyse nach den Gefährdungsblättern und deren Erläuterungen im Systemzusammenhang mit den geclusterten Use Cases der Lokalisierungsfunktionen bzw.-objekte aus dem Kapitel 4 Sicherheit (vgl. dort Tabelle 4.12).

5.4.3 Modulares Zulassungskonzept

Gemäß der Unterscheidung in eine generische Typzulassung und eine anwendungsspezifische Zulassung kann für die Entwicklung und Nachweisführung nach CENELEC die Zulassung und Nachweisführung modularisiert werden. Auf der einen Seite ergeben sich anwendungsspezifische Aspekte, welche die Lokalisierungsfunktionen und – objekte charakterisieren. Tabelle 5.15 zeigt eine Zusammenstellung der Sicherheitsintegritätsstufen der Lokalisierungsfunktionen und -objekte aus der Use Case Analyse aus dem Schwerpunktkapitel 4 Sicherheit

GFB-Nr.	Use Case Nr.	Lokalisierungssobjekt	SIL
1.1	1.1	Gleisfreimeldung	SIL3/SIL4
1.2	1.2 – 1.7 8.1 – 8.2	Zugposition Fahrzeuge	SIL 3
2	1.1.5, 1.5 6.2 7.1 - 7.3	Balisen/Tafeln (virtuelle)Euro-Balise	SIL 2 (an der Grenze zu SIL 3)
3	2.2.4 3.1.6	betriebliche Objekte Entgleisungsvorrichtung Prellbock	$\leq$ SIL 3
4a1	2.1 8.4	Menschen im Gleis Doppelausrüstung (Zug siehe 1.1)	SIL 0

GFB-Nr.	Use Case Nr.	Lokalisierungssobjekt	SIL
4a2	2.1 8.4	Menschen im Gleis ohne Warnanlagen (Zug siehe 1.1)	SIL 2
4b	2.1 8.4	Menschen im Gleis Zugwarnung (Zug siehe 1.1)	SIL 2
5/7	2.1, 2.2 3.1.3 -3.1.5 8.3	Instandhaltungsartefakte /sonstige Objekte	SIL 3
6	3.1.2	Naturobjekte	SIL 2

Tabelle 5.15: Zusammenfassung der parametrierten Attribute der Lokalisierungsobjekte aus der Use Case Analyse

Aus dieser Zuordnung ist ersichtlich, dass folgende Gruppen mit ähnlicher Aufgabe und gleicher Sicherheitsintegrität anwendungsspezifisch geclustert werden können:

- Position von Zügen und Fahrzeugen, Gleisfreimeldung, Balisen/Tafeln (GFB 1.1, 1.2, 2)
- Menschen im Gleis (GFB 4)
- Instandhaltungsobjekte und betriebliche Objekte (GFB 3, 4 alle, 5,7)
- Naturobjekte (GFB 6)

Eine zweite Clusterung geht von der Architektur der Lokalisierungssysteme und ihrer Funktion aus. Aus den im Schwerpunktkapitel 4 Sicherheit Abschnitt 4.5 Systemarchitektur und -integration ausgewiesenen Funktionseinheiten

- Kommunikations-/Transfersystem mit Kontaktstellen seitens der Lokalisierungsendgeräte und seitens der Lokalisierungszentrale
- GLAT-Zentrale
- Zugseitige Leit- und Sicherungstechnik (ETCS OBU)
- Warnung von Personen im Gleisbereich
- GLAT Tag

ergibt sich eine weitere anwendungsspezifische Modularisierung hinsichtlich der technischen Einrichtungen, die Tabelle 5.16 zeigt.

Lokalisierungssobjekt/-funktion	Lokalisierungs-endgerät	Lokalisierungs-zentrale und Karte	Kommuni-kation
Position von Zügen und Fahrzeugen, Gleisfreimeldung, Balisen/Tafeln (GFB 1.1, 1.2, 2)	Fahrzeugseitige Lokalisierung	+	+
Menschen im Gleis (GFB 4)	GLAT Tag	+	+

Lokalisierungssobjekt/-funktion	Lokalisierungs-endgerät	Lokalisierungs-zentrale und Karte	Kommuni-kation
Instandhaltungsobjekte und betriebliche Objekte (GFB 3, 4 alle, 5,7)	GLAT Tag	+	+
Naturobjekte (GFB 6)	GLAT Tag	+	+

Tabelle 5.16: Anwendungsspezifische Modularisierung hinsichtlich der technischen Einrichtungen

Eine weitere Aufteilung für die Zulassung ergibt sich aus der funktionalen Architektur nach den Funktionskomponenten und ihrer Sicherheitsverantwortung, die Tabelle 5.17 darstellt.

Funktionskomponente	Platzierung	Nachweisart	generisch/spezifisch
GNSS-Raum/Bodensegment	global	Zertifizierung, Cross Acceptance	generisch
GNSS-Empfänger, Antenne (Nutzersegment)	lokal	Qualifizierung, Cross Acceptance	generisch/spezifisch
Sensorik	lokal	Nachweis, Cross Acceptance	generisch/spezifisch
Überwachung (SW, HW)	lokal	Nachweis	generisch
Schnittstellen/Integration	lokal	Nachweis	spezifisch
Kommunikation	global	Nachweis, Cross Acceptance	generisch
Überwachung (SW, HW)	zentral	Nachweis	generisch/spezifisch
Karte	zentral	Nachweis	generisch
Schnittstellen/	zentral	Nachweis	spezifisch
Systemintegration	global	Nachweis	spezifisch

Tabelle 5.17: Arten der Nachweisführung für die einzelnen Funktionskomponenten

Während die verschiedenen GNSS-Raum- und Bodensegmente eine mehr oder weniger ausgeprägte Rechtsgrundlage aufweisen, sind Regelwerke für die Anwendung von Satellitenempfängern sehr branchenspezifisch und im Eisenbahnwesen für sicherheitsverantwortliche Anwendungen noch nicht thematisiert geschweige konsolidiert. Diese Problematik wird durch einen alternativen Ansatz überwunden, der in Abschnitt 5.6 dargestellt wird.

In einigen Fällen kann es möglich sein, auf vorhandene Nachweisführungen oder bereits zugelassene Produkte zurückzugreifen. Ihre Integration in das Lokalisierungssystem muss dann in einem Integrationsgutachten geprüft und anwendungsspezifisch zugelassen werden.

5.4.4 Feststellung:

Dank der Clusterung der Use Case hinsichtlich ihrer Lokalisierungsfunktion, Sicherheitsanforderungsstufen und Platzierung auf Lokalisierungsobjekten kann die Zulassung modular hinsichtlich generischer und anwendungsspezifischer Nachweisführungen durchgeführt werden.

Obwohl der Aufwand für die Nachweisführung aufgrund fundamental anderer Technologien nicht unerheblich sein wird, ist doch die damit gewonnene Abdeckung für sehr viele Use Cases von wirtschaftlichem Vorteil.

Es empfiehlt sich, die Nachweisführung in lokale und zentrale Anteile zu trennen, zugelassene Produkte und vorhandene Nachweise einzelner Komponenten zu nutzen und die spezifischen Nachweise sukzessiv durchzuführen, um vom fortschreitenden Erkenntnisgewinn bei Nachweisführung, Begutachtung und Zulassung zu profitieren. In jedem Fall ist eine entwicklungsbegleitende Begutachtung effizient, wenn geeignet qualifiziertes Personal verfügbar ist.

Aus gutachterlicher Einschätzung erscheint unter den genannten Voraussetzungen die Zulassung eines satellitengestützten Lokalisierungssystems im Schienenverkehr machbar.

5.5 Entwicklung und Nachweisführung nach CENELEC

Dieses Thema wurde im Rahmen der Machbarkeitsanalyse aus Phase 0 ebenfalls behandelt. Die Zusammenfassung des Themas (Feststellung) ist untenstehend aufgeführt. Die detaillierten Erörterungen zu

- Zulassungsprozess – Aufgaben und Rollen
- Phasenmodell im Überblick
- Risikoanalyse und Sicherheitsziele für Systemkomponenten
- Gefährdungsanalyse
- Nachweisführung und Nachweisdokumentation (nach [34])

werden hier nicht wiedergegeben.

Feststellung
Für den Zulassungsprozess mit seinen Aufgaben und Rollen ist die Vorlage eines positiv begutachteten Sicherheitsnachweises mit dem normgerechten erstellten technischen Sicherheitsbericht und Anerkennung eines Qualitäts- und Sicherheitsmanagementsystems notwendig. Durch die Struktur des Sicherheitsnachweises und -berichtes sowie das damit verbundenen Vorgehen wird nachgewiesen, dass Gefährdungen mit Hilfe geeigneter Prozesse identifiziert wurden und praktikable Maßnahmen zur Schadensminderung und zum Umgang mit Risiken, die von den identifizierten Gefährdungen ausgehen, eingeführt wurden. Methodisch ist Machbarkeit des Sicherheitsnachweises sichergestellt, allerdings sind die durch die

Satellitenstützung entstehenden neuen Risiken aufzuzeigen und ihre organisatorische und technische Beherrschung spezifisch darzulegen.

5.6 Zulassung von Satellitengestützten Lokalisierungssystemen für Eisenbahnen

Für die Entwicklung, Begutachtung und Zulassung von Lokalisierungssystemen, welche zur absoluten Ortung GNSS nutzen, existiert insbesondere für die Lokalisierung mittels Satellitenempfängern allgemein kein etablierter Rahmen nach anerkannten Regeln der Technik. Daher ist hier ein neuer Lösungsansatz notwendig. Dieser Ansatz wird im Abschnitt 5.6.1 vorgestellt. Der Ansatz beruht auf folgenden Voraussetzungen.

- Erste Voraussetzung ist, das Satellitensystem in seinen Leistungsmerkmalen als zugelassen zu akzeptieren. Im Sinne der Cross-Acceptance kann dies für die auf Völker- o. ä. Rechtsgrundlage errichteten, zugelassenen und betriebenen Raum und Kontrollsegmente eines GNSS gelten. Diese Voraussetzung wird in Abschnitt 5.6.2 erläutert.
- Zweite Voraussetzung ist, das spezifische Lokalisierungssystem nach dem normativen Rahmen des Eisenbahnwesens zu entwickeln, zuzulassen und zu betreiben. Dazu gehört insbesondere auch das Nutzersegment, d.h. die Empfänger des GNSS. Diese Voraussetzung wird in Abschnitt 5.6.3 behandelt.

Bei der Entwicklung, eines satellitengestützten Lokalisierungssystems einschließlich der Nachweisführung, insbesondere der Lokalisierungsendgeräte, als Voraussetzung der Begutachtung und Zulassung muss allerdings akzeptiert werden, dass es aus wirtschaftlichen Gründen kaum machbar ist, eine CENELEC-konforme Entwicklung der Satellitenempfänger durchzuführen.

Satellitenempfänger werden hier als COTS-Komponenten in das Eisenbahnsystem integriert. Hierfür kann eine Zertifizierung aus dem Luft- und Raumfahrtbereich im Sinne der Cross-Acceptance genutzt werden, die auf Gültigkeit im Eisenbahnbereich geprüft werden muss, was wegen der andersartigen Einsatzbedingungen kritisch ist.

Daher wird hier ein bereits bei anderen Systemen des Eisenbahnverkehrs die z.T. auf COTS-Systemen fußen, z.B. der LZB, sicheren Rechnersystemen oder der sicheren Kommunikation, bereits verwendetes, etabliertes und akzeptiertes Vorgehen vorgeschlagen. Dieses alternative Vorgehen wird als Verfahrenssicherheit bezeichnet, welches sich von der technologisch-physikalischen Sicherheit durch geeignete Verfahren, d.h. die Kombination von Methoden und physischen Ressourcen abgrenzt. Hierfür ist eine Qualifikation der Empfängerleistungsdaten erforderlich, die im Abschnitt 5.6.3 vorgestellt wird.

5.6.1 Mehr-Ebenen Ansatz für die Nachweisführung, Qualifizierung und Zulassung

Voraussetzung für eine satellitengestützte Lokalisierung ist natürlich die Infrastruktur des Satellitensystems mit seinem Raumsegment und Kontrollsegment am Boden. Hier wird von einer rechtssicheren Gewährung dieser Segmente ausgegangen (vgl. 5.6.2). Nur wenn die Satellitenempfänger verlässlich mit Signalen versorgt werden, kann überhaupt die Satellitenstützung der Lokalisierung längerfristig gewährleistet werden. Wenn diese Voraussetzung zutrifft und die Empfänger gewissen Qualitätsansprüchen genügen, kann mit Hilfe einer entsprechend konfigurierten und parametrierten Überwachungseinrichtung eine fehlerhafte satellitengestütze Lokalisierung detektiert werden, was komplementär Sicherheit gewährt.

Die Sicherheit eines Systems wird prinzipiell durch Prüfung der Übereinstimmung gleicher Informationen unterschiedlicher Herkunft in Echtzeit gewährleistet, wie im Schwerpunktkapitel «Sicherheit» ausführlich beschrieben ist. Daher muss die Funktionseinheit zur Prüfung auf Übereinstimmung normkonform entwickelt werden. Dazu gehören geeignete und richtig parametrierte Prüfalgorithmen, in welchen die Eingangssignale be- und verarbeitet werden, um eine Entscheidung über ihre Integrität zu erhalten.

Die Algorithmen zur Auswertung der Satelliten- und Sensorsignale zur Prüfung auf Übereinstimmung benötigen zur Berechnung bestimmte Parameterwerte, welche die Natur der Signale beschreiben. Dies sind z.B. statistische Maße, z.B. von Verteilungsfunktionen der Messabweichung. Wenn die z.T. stochastisch variierenden Messabweichungen bestimmte Grenzen überschreiten, können die Dauern der Überschreitung als Ausfalldauern interpretiert werden (MTTEF). Diese Werte werden benötigt, um die Algorithmen der Fehlerdetektion zu parametrieren. Insofern müssen die erforderlichen Parameterwerte verlässlich sein. Daher sind diese Werte nach einschlägigen Verfahren zu ermitteln, was hier als Qualifizierung bezeichnet wird. Die Qualifizierungen der Sensorsysteme sollten als Grundlagen der Nachweisführung des Herstellers und Anerkennung durch Begutachtungs- und Zulassungsstelle von akkreditierten Institutionen ermittelt werden.

Mit diesen Voraussetzungen einer sicheren Überwachung der Integrität einer verfügbaren satellitengestützen Lokalisierung mit den vier Ebenen

1. Garantierte Signalversorgung durch das Raum- und Bodensegment des Satellitenortungssystems (Abschnitt 5.6.2)
2. qualifizierte Sensoren und Ermittlung von Merkmalsgrößen wie MTTEF, Genauigkeiten u.a. (Abschnitt 5.6.3)
3. qualifizierte aktuelle referenzierte digitale Karte des Streckennetzes (Abschnitt 5.6.4)
4. sichere Detektion, normkonform entwickelte und implementierte Algorithmen auf der Grundlage der qualifizierten Parameterwerte (Abschnitt 5.6.5)

kann eine prinzipielle Zulassungsfähigkeit für eine zu entwickelndes SIL 4 CENELEC konforme Lokalisierung ermöglicht werden.

Methodisch bettet sich dieser Ansatz in die Allgemeine Struktur des Sicherheitsnachweises und seines Technischen Sicherheitsberichtes ein, der um die üblichen Teile nach EN 50129 ergänzt wird.

Die komplementäre Gefährdungsanalyse im Sicherheitsnachweis kann anhand der durch die bei der Qualifizierung erhoben Sensormerkmalsdaten insbesondere zur Genauigkeit und RAMS mittels modellbasierter Analyse z.B. durch Fehlerbäume oder durch eine in dem vor kurzem dazu erschienen ERA Leitfaden zu der europäischen Verordnung 2015/1136 CSM–RA-DT angegebene Vorgehensweise unter Nutzung der IEC 62551 erfolgen.

Im Folgenden werden die Voraussetzungen zum Nachweis einer sicheren Überwachung der Integrität einer verfügbaren satellitengestützen Lokalisierung im Einzelnen erläutert.

5.6.2 Rechtsrahmen des Satellitensystems - Zertifizierung und Haftung

Da die Gewährleistung eines sicheren GNSS-Betriebes prinzipiell von allen Verkehrsmoden für sicherheitsverantwortliche Aufgaben gefordert wird, war es notwendig, einen geeigneten Rechtsrahmen zu konzipieren und zu legitimieren.

Eine rechtsverbindliche Garantie des Betriebs und seiner Leistungserbringung wurde auf einer der ersten Konferenzen zu dieser Thematik, der CERGAL (Certification of GALILEO), die sogenannte „Braunschweig CERGAL Resolution for Certification of Satellite Based Positioning Systems, its Services and Components for Safety Relevant and Liable Applications“ [35] gefordert und verabschiedet.

In organisatorischer Hinsicht wurde im europäischen Rechtsrahmen die GSA (GALILEO Supervisory Agency) etabliert [36], welche u. a. aufgrund dieser Resolution 2007 einen Auftrag ausschrieb. Darin wurde für den Rechtsrahmen der Errichtung und des Betriebs ein Zertifizierungsprogramm gefordert, welches die Belange aller Verkehrsmoden abdecken sollte. Unter Führung von GAUSS (GALILEO Zentrum für sicherheitskritische Anwendungen, Zertifizierungen und Dienstleistungen Braunschweig) wurde dazu von einem internationalen Konsortium ein Konzept erarbeitet, das einem allgemeinen, modenunabhängigen aber umfassenden Kern der Zertifizierung enthält, auf dem dann modenspezifisch aufgesetzt werden könnte. Damit war einerseits eine effiziente und ökonomische, andererseits aber auch eine integrative Vorgehensweise konzipiert [37].

Das im April 2008 von der GSA akzeptierte Zertifizierungskonzept beinhaltet die Vorgehensweise zur Zertifizierung, die zu berücksichtigenden Anforderungen aus den jeweiligen normativen Rahmen der einzelnen Verkehrsmoden sowie auch einen institutionellen Rahmen,

welcher ebenfalls deren verschiedene Sicherheitskulturen berücksichtigt und dem demokratischen Grundverständnis der Gewaltenteilung in Europa entspricht.

Ähnlich wie ein von einem außerhalb des Bahnsystems im engen Sinne stehender Funknetzbetreiber oder Energieversorger wird auch das GNSS als externer Erbringer sicherheitsverantwortlicher Leistungen in das Eisenbahnsystem integriert werden. Wird durch die oben beschriebene Zertifizierung der Ortungsdienste eine gewisse Qualität zugesichert, muss darüber hinaus jedoch auch für die Nichteinhaltung eine Gewährleistung im Sinne einer Haftung rechtsverbindlich abgesichert werden [38]: Erst durch die Übernahme der Betreiberverantwortung durch die EU wurde die entscheidende Voraussetzung erfüllt, eine Verwendung von GNSS für sicherheitsrelevante Aufgaben im Eisenbahnverkehr ernsthaft zu erwägen.

Hier sei der Vollständigkeit halber erwähnt, dass die Schweiz im Rahmen eines bilateralen Abkommens volles Mitglied im Galileo und EGNOS-Programm ist und Zugang zu allen Signalen und Strukturen innerhalb der ESA/GSA hat: „The agreement governs Switzerland's participation in the EU's Galileo and EGNOS programmes“. „The cooperation Agreement authorises Switzerland to take part in the European satellite navigation programmes Galileo and EGNOS”.

https://www.eda.admin.ch/dea/en/home/bilaterale-abkommen/ueberblick/bilaterale-abkommen-nach-2004/satellitennavigation.html

Um alle Einsatzmöglichkeiten ohne erhebliche technische und organisatorische Schwierigkeiten, die den betrieblichen Einsatz begleiten können, erschließen zu können, sind einige wichtige vorbereitende Maßnahmen nötig. Von höchster Priorität sind diesbezüglich:

- Zertifizierung der GALILEO-Signale für sicherheitsrelevante Anwendungen. In diesem Zertifizierungsprozess ist es zweckmäßig, dass die Bahnen, die Luft- sowie die Seefahrt und andere Nutzergruppierungen mit ESA und GSA zusammenarbeiten, um die Zertifizierungsdokumente gemäß den für jedes einzelne System relevanten Normen zu schaffen.
- Bereitstellung der notwendigen qualifizierten oder zertifizierten Infrastruktur zur Referenzierung der Satellitensignale im Empfänger
- Schaffung der in den Rechtshaftungsnormen enthaltenen Grundbeziehungen zwischen dem GALILEO-Betreiber und den Eisenbahnbetreibern, wobei ein gesamter Rechtsrahmen zwischen GALILEO und einem Vertreter der in Eisenbahnbetrieb und Organisation involvierten Parteien gebildet wird. Ein Ziel ist dabei eine langfristige Bestandsgarantie des GALILEO GNSS zu garantieren.

Feststellung: GALILEO ist das einzige GNSS, welches unter ziviler Kontrolle im europäischen Rechtsrahmen betrieben wird. Aufgrund dieser Tatsache kann es als machbare Grundlage einer satellitengestützten Lokalisierung im Schienenverkehr dienen.

5.6.3 Qualifizierung von GNSS-Empfängern - Ermittlung von Merkmalsgrößen wie MTTEF, Genauigkeiten u.a.

Eine Satellitensysteme nutzende Lokalisierung im Eisenbahnbereich ist neu und muss für den betrieblichen Einsatz entsprechend qualifiziert werden. Der Prozess und die Ergebnisse der Qualifizierung des Systems sind Bestandteil des Technischen Sicherheitsbericht, welcher wesentlicher Teil des vorzulegenden Sicherheitsnachweises für die Zulassung ist.

Die Nachweisführung benötigt die Angabe definierter Merkmale, Größen und Werte. Hierfür ist die Überführung der garantierten spezifizierten Leistungsmerkmale des jeweiligen GNSS, z.B. GALILEO, die ausschließlich aus der normativen Begriffswelt der Luft- und Raumfahrt stammen und nicht ohne weiteres auf die Begriffe der Eisenbahnen übertragen werden können, z. B. durch Angabe des SIL, notwendig. Hier kann die begriffliche und parametrische Konvertierung aus der Dissertation von Lu im Sinne einer zu akzeptierenden Cross Acceptance von Qualifizierungsvorschriften bzw. Ergebnissen anderer Branchen mit ähnlichem Sicherheitsniveau, wie der Luftfahrt Bezug genutzt werden. Abbildung 5.20 zeigt eine Gegenüberstellung der GALILEO Spezifikation in einer Darstellung der Eisenbahntechnischen Begriffswelt. Dadurch werden auch die bei der GALILEO-Entwicklung zugrunde gelegten Merkmale und Größen der Luft- und Raumfahrttechnik soweit überführt, so dass die Größen, welche die Verlässlichkeits(RAMS)-Eigenschaften beschreiben, im Bereich der Eisenbahn, problemlos anwendbar sind (sog. Cross-Acceptance).

Qualifizierungsvorschriften: Bei GNSS ist die Zertifizierung auf die verschiedenen Segmente bezogen. Während das Raum- und Bodensegment von den Systembetreibern qualifiziert wird, ist für die Empfängersysteme die Qualifizierung bzw. Zertifizierung im Bereich des Herstellers oder Anwenders erforderlich.

Problematisch ist, dass zur Qualifizierung einer satellitenbasierten Lösung im Eisenbahnbereich keine einschlägigen Qualifizierungsvorschriften existieren. So wurde z.B. zwar im EU/GSA-Projekt GALCERT ein Prozess für die Qualifikation des Galileo GNNS erarbeitet, welcher nach seiner Umsetzung zur Qualifizierung des Raum- und Bodensegmentes führte, jedoch nicht das Satellitenempfängersegment umfasste.

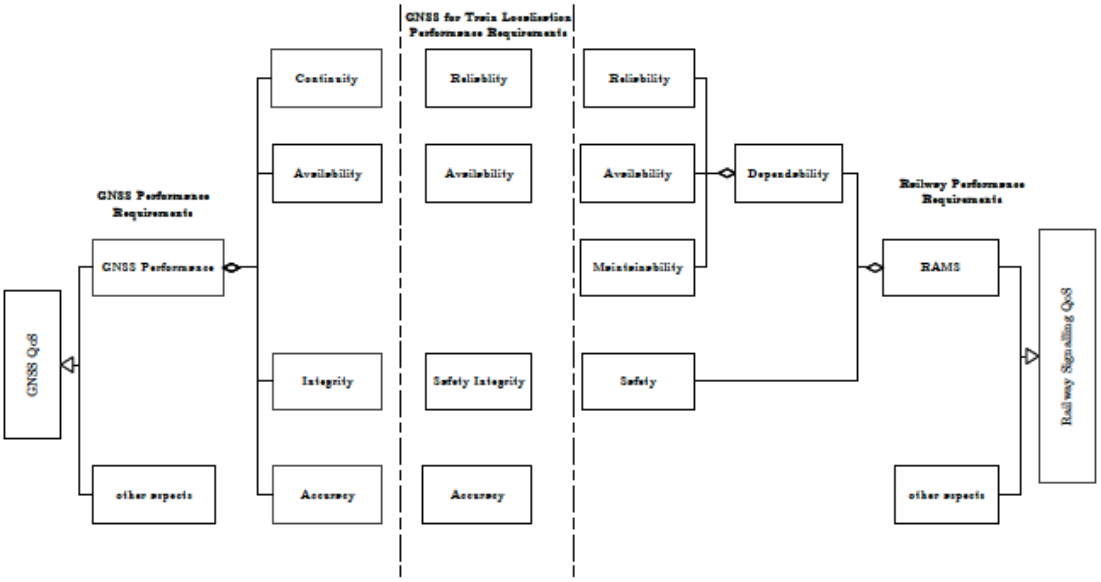


Abbildung 5.20: Gegenüberstellung der GNSS Spezifikation in einer Darstellung der Eisenbahntechnischen Begriffswelt (nach Lu).

Außerhalb des generischen Rahmens zur Zertifizierung des GALILEO Raum- und Kontrollsegmentes sind nun weitere Vorgehensweisen auszuarbeiten, um die geforderten Nachweise des Nutzersegmentes, d.h. der Empfänger und Antennen, hinsichtlich der eisenbahnspezifischen Eigenschaften, insbesondere im Bereich RAMS unter Beachtung der einschlägigen CENELEC-Standards, für die GNSS-Sensorik als Ortungskomponente zu erbringen. Hierzu gehört die Entwicklung eines normkonformen Prüfverfahrens, mit dessen Ergebnissen signaltechnisch sichere Lokalisierungssysteme, die GNSS-Informationen verwenden, konfiguriert und parametriert werden können.

Für GNSS Empfängersysteme sind bislang kaum spezifische Qualifizierungsnormen, insbesondere für den Bodenverkehr und vor allem Eisenbahnbetrieb vorhanden. In der Dissertation von Spiegel wurden die vorhandenen Normen EN 61108-3:2010, EN 16803-1 (Draft), ETSI TR 101593(Entwurf), ION STD 101, ISO 17123-8, JRC 51300 und RTCA DO 229 für die Qualifizierung von satellitenbasierten Ortungssystemen zusammengestellt und analysiert. Es zeigte sich, dass

- „keine eindeutige Terminologie verwendet wird. In der Norm EN 16803-1 werden beispielsweise die Termini „Ground Truth“ und „Referencetrajectory“ synonym benutzt, obwohl diese in EN 16803-1 eine divergierende Bedeutung haben [vgl. DIN EN 16803-1].
- die Qualitätsmerkmale, anhand derer die satellitenbasierten Ortungssysteme bewertet werden, nicht eindeutig definiert sind. Es werden verschiedene Qualitätsmerkmale beziffert, die für die Verifikation genutzt werden sollen. Es fehlen jedoch eindeuti-

ge Rechenvorschriften, um diese zu berechnen. Insbesondere im Bereich der Ausreißerelimination sind differente Interpretationen möglich.
- die Messbedingungen in den Normen nur unzureichend berücksichtigt werden. Lediglich in der EN 16803-1 werden die Messbedingungen mittels eines GNSS-Referenzempfängers dokumentiert. Dabei werden das stochastische Verhalten und der Einfluss der Technologie und Filterung des GNSS-Referenzempfängers vollkommen vernachlässigt. Dies führt dazu, dass es quasi unmöglich ist, die Messergebnisse für kurze Prüffahrten zu vergleichen [vgl. DIN EN 16803-1].
- das stochastische Verhalten der Prüfgegenstände nicht berücksichtigt wird. Dies führt insbesondere bei kurzen Prüffahrten zu viel Interpretationsspielraum."

Speziell für die Nutzung unter bestimmten Mess- und Einsatzbedingungen sind geeignete Angaben zur Genauigkeit und Verlässlichkeit einschließlich der Sicherheit erforderlich. Die Problematik beginnt schon mit einer einheitlichen Terminologie der metrologischen und RAMS Eigenschaften. Für eine Qualifizierung von GNSS Empfängern wurden dafür normkonforme Vorschläge einer eindeutigen Definition von Qualitätsmerkmalen für die Qualifizierung von GNSS-Empfängern erarbeitet, wie sie z.B. in den Dissertationen von Yurdakul, Wegener, Lu oder Spiegel beschrieben sind.

Die resultierende praktische Aufgabenstellung im Kontext der Zertifizierung und Nachweisführung ist die messtechnische Qualifizierung des GNSS und insbesondere ihrer Empfänger im fahrzeugseitigen Ortungssystem unter eisenbahnbetrieblichen Bedingungen und Beachtung einschlägiger Normen, z. B. des „Guide to the Expression of Uncertainty in Measurement" für die Bestimmung von Genauigkeitseigenschaften [39]. Es muss beachtet werden, dass in einer Eisenbahnumgebung der Empfang und die Bewertung der GALILEO-Signale von denen im offenen Raum verschieden sind. Hierfür sind Normalen und anerkannte Referenzmaßstäbe erforderlich, welche für dynamische Messungen erarbeitet werden [40], [41].

In den EU Projekten Qualisar und StandOrt sind Vorgehensweisen zur Qualifizierung [7] und darauf aufbauenden Nachweisführung einer auf Satellitensignalen und bordeigenen Sensorik beruhenden Fahrzeuglokalisierung entstanden [34] z.T. in Kooperation mit staatlichen Behörden (Physikalisch-Technische Bundesanstalt) sowie einem akkreditierten Labor (NavCert) erarbeitet. Dieses Verfahren basiert auf

- der Erstellung einer unabhängigen Referenz für Lokalisierungen im Landverkehr (Referenzprojekte Qualisar und Standort sowie [7])
- der Vorgabe von Prozeduren und Durchführung von Lokalisierungen auf bewegten Objekten, der Definition entsprechender Qualifizierungsgrößen
- Prozeduren für die Auswertung der Tests und Darstellung der Ergebnisse.

Messbedingungen

Für die Spezifizierung von Anforderungen an ein Ortungssystem und ihre Qualifizierung ist es notwendig, die relevanten Messbedingungen zu definieren und zu kategorisieren. Bis heute ist dies für den Bodenverkehr nicht möglich, da die Anforderungen in der Norm ISO/IEC 17025 hinsichtlich der präzisen und eindeutigen Definition der Qualitätsmerkmale, der Dokumentation der Messbedingungen während der Qualifizierung und der Eindeutigkeit von Messergebnissen bedingt durch das stochastische Verhalten von GNSS-Empfängern nicht erfüllt werden.

Denn Messbedingungen sind bei der Durchführung einer Zertifizierung von satellitenbasierten Ortungssystemen zu berücksichtigen, wozu es unabhängiger Prüflabore bedarf, welche nach DIN EN ISO/IEC 17025 akkreditiert sind. Ein Prüflabor nutzt für die Zertifizierung ein unabhängiges Messsystem, das als Referenz herangezogen werden kann und die Anforderungen aus Industrie und Normung wie z. B. DIN V ENV 13005 erfüllt.

Prüfprozedur und Referenz

Voraussetzung ist die Definition einer praktikablen, standardisierbaren Prüfprozedur sowie einer hierfür notwendigen, normkonformen Referenz für satellitenbasierte Ortungssysteme im Verkehr. Hierzu wurden in [7] Anforderungen an einen vom Prüflabor zu verwendenden Referenzmessaufbau für die satellitenbasierte Ortung im Verkehr entwickelt und geeignete Systeme erprobt. Weiter wurden repräsentative, einheitliche, realistische und vor allem praktikable Prüfprozeduren erarbeitet, die alle relevanten Einflüsse auf die Messqualität von satellitenbasierte Ortungssystemen für Anwendungen im Verkehr berücksichtigt. Erst durch die systematische Definition und Ausführung von Prüfszenarien wird die Vergleichbarkeit von Prüfergebnissen ermöglicht. Abbildung 5.21 zeigt die Bestandteile einer generischen Prüfprozedur zur Qualifizierung von Satellitenempfängern

Institutionen zur Qualifizierung und Zertifizierung

Für eine Zertifizierung stehen bereits wenige unabhängige und akkreditierte Prüflabore zur Verfügung. Ein Beispiel ist die NavCert GmbH, die als akkreditiertes Prüflabor unabhängige Bewertungen von GNSS basierten Produkten und Lösungen durchführt. Diese Zertifizierungstellen können sich für die Qualifizierung von Prüflaboren bedienen. Für die Qualifizierung von Satellitenempfängern für eine Lokalisierung stehen z.B. bei der deutschen Technisch-Physikalische Bundesanstalt oder beim Projektpartner IVA geeignete stationäre und mobile Einrichtungen zur Simulation und Durchführung der Tests mit Referenzen zu Lokalisierung zur Verfügung.

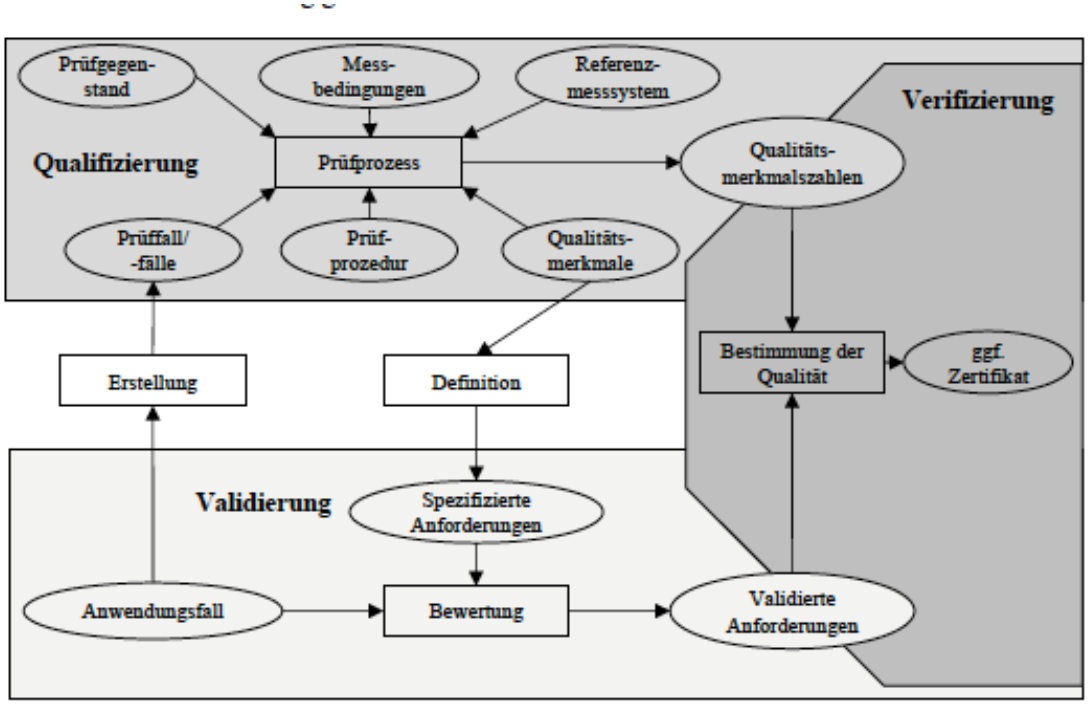


Abbildung 5.21: Bestandteile einer generischen Prüfprozedur zur Qualifizierung von Satellitenempfängern (Diss. Spiegel)

Prozeduren für die Auswertung der Tests und Darstellung der Ergebnisse

Da die den Stichproben der Messungen für die Zertifizierung zugrundeliegende Verteilungen begrenzt durch zeitliche und örtliche Effekte nicht repräsentativ sind, wird sowohl eine parametrische Beschreibung als auch die nicht parametrische Beschreibung vorgeschlagen. Um das stochastische Verhalten von GNSS-Empfängern zu quantifizieren, wird in der Dissertation Spiegel ein neues Qualitätsmaß eingeführt, welches keine durch Parameter beschreibbare Stichprobenverteilung benötigt.

Damit die Messbedingungen dokumentiert werden können und um zu verstehen, unter welchen Bedingungen die Messungen durchgeführt wurden, wird in Dissertation Spiegel ein neues Maß – der bestmögliche Ort – eingeführt, welcher die Messbedingungen in einer Größe verdichtet. Die Messbedingungen werden dabei durch Referenzmessungen bestimmt. Diese streuen und folglich wird der bestmögliche Ort um eine Messunsicherheit nach dem Verfahren des GUM erweitert. Um den bestmöglichen Ort zu bestimmen wurde das Programm – CONCAL – entwickelt und verifiziert.

In dieser Arbeit wird eine beispielhafte normenkonforme Qualifizierung eines GNSS-Empfängers durchgeführt. Die Ergebnisse von Prüffahrten zeigen, dass die Angaben von Hersteller von Satellitenempfängern bezüglich der Ortsgenauigkeit für die Prüffahrt nicht einge-

halten werden konnten. Werden jedoch die systematischen Abweichungen durch die Messbedingungen berücksichtigt, lässt sich zeigen, dass die Genauigkeitsangaben eingehalten werden.

Qualifizierung von weiteren Sensoren

Für Analyse der Gefährdungen neuer Sensorsysteme und ihrer Abhilfe sind die Vorgehensweisen nach EN 50126 bzw. EN 50128 zu beachten. Zweckmäßig bei der Auswahl sind bereits geeignete und im Eisenbahnbereich zugelassenen Sensoren oder Sensorsysteme. Fahrzeugseitig können dabei insbesondere bereits vorhandene odometrische Einrichtungen, z.B. Radimpulsgeber oder Radarsysteme genutzt werden, wenn sichergestellt und nachgewiesen ist, dass sich durch die neue Lokalisierung keine Rückwirkungen auf bestehende Systeme ergeben oder keine systematischen Fehler auftreten. Wenn dies nicht der Fall ist, müssen entweder anderweitig erbrachte Qualifizierungen oder Zertifizierungen auf ihre Anerkennung im Eisenbahnwesen im Sinne der Cross Acceptance geprüft werden oder es müssen entsprechende normkonforme Qualifizierungen erbracht werden.

5.6.4 Qualifizierung der digitalen Karte

Eine wichtige Voraussetzung für die Zulassungsfähigkeit ist die Existenz einer genauen und aktuellen digitalen Karte.
Bereits früher wurde vom IVA ein organisatorischer Ansatz zur Erstellung und insbesondere Aktualisierung gesicherter Kartendaten in Zusammenarbeit mit der Deutschen Bahn im Projekt SafeMap erarbeitet. Aus diesem Projekt können die folgenden, wesentlichen Anforderungen und grundlegenden Konzepte für die Zulassungsfähigkeit eines Streckenatlas übernommen werden:
Gegenwärtig wird die Zuordnung von Zügen zur Strecke unmittelbar mit Hilfe von Gleisfreimeldeanlagen dort selbst hergestellt, oder mittelbar mit streckenseitig angeordneten, physikalischen Komponenten wie Balisen fahrzeugseitig ermittelt. Bei Verzicht auf diese streckenseitig angeordneten Komponenten muss das Fahrzeug den Bezug zur Strecke selbst herstellen. Eine Referenz ist also immer notwendig, um die Informationen der fahrzeug- oder objektseitigen Sensoren auf die Strecke zu beziehen. Bei einer fahrzeugautarken Or-tung kann diese Referenz in Form eines digitalen Streckenatlas auf dem Fahrzeug mitgeführt werden. Eine im zentralen Teil des Lokalisierungssystems verwaltete digitale Karte begüns-tigt die Konsistenz und Aktualisierung der Datenhaltung, welche bei einer dezentralen Verortung nur mit größerem Aufwand und ggf. nicht immer gewährleistet werden kann.
In der Karte sind die aktuellen Eigenschaften der Strecke, z.B. geometrische Eigenschaften der Strecke, Eigenschaften des Oberbaus oder Merkmale der Umgebung abgelegt. Mit Hilfe dieser gespeicherten Referenz im Streckenatlas wird der Bezug der objektseitig aufgenommenen Sensorinformationen auf die Bahnstrecke und ihre Umgebung korreliert.

Da dieser Streckenatlas den sicherheitsrelevanten, bisher physikalisch hergestellten Bezug zur Strecke informationstechnisch ablöst, müssen die im Streckenatlas enthaltenen Informationen ebenfalls als sicherheitsrelevant eingestuft werden.
Für eine sicherheitsrelevante digitale Kartierung ist die Konzeption eines Qualitäts- und Sicherungsmanagements von sicheren Daten erforderlich. Dazu muss zunächst analysiert werden, welche Informationen in einem Streckenatlas enthalten sein müssen, sowie deren geforderte Qualität hinsichtlich Genauigkeit (Messunsicherheit) und Sicherheit (Sicherheitslevel) bestimmt werden. Weiterhin muss analysiert und geklärt werden, wie die für Liegenschaftsverwaltungen konzipierten und vorgehaltenen Datenbestände aufbereitet und strukturiert werden müssen, die bei der SBB und anderen Bahnbetreibern bereits existieren, um für Zwecke der Ortung und Sicherung in geeigneter Form vorliegen.
Ferner muss geklärt werden, wie die Qualität bestehender Daten so quantifiziert werden kann, dass sie ganz oder teilweise für Zwecke der Ortung und Sicherung weiterverwendet werden können.
Abschließend ist ein Verfahren für die zukünftige Aufnahme sicherheitsrelevanter Daten zu definieren, das von vornherein einen für den spurgebundenen Verkehr gültigen Sicherheitsnachweis besteht.
Die Entwicklung, Implementierung und Betrieb und Wartung eines derartigen digitalen Streckenatlasses müssen zwecks Nachweisführung, Begutachtung und Zulassung nach Maßgabe der einschlägigen CENELEC Normen, insbesondere für Software EN 50128 geschehen.

5.6.5 Gesamtqualifizierung - Qualifizierung nach CENELEC bis zur Sicherheitsanforderungsstufe SIL 4 für ein Lokalisierungssystem

Die Entwicklung des sicheren Lokalisierungssystems insgesamt kann normgerecht nach den einschlägigen Vorschriften der Entwicklung sicherheitskritischer Systeme des Eisenbahnsektors durchgeführt werden.

Insbesondere sind für die Systementwicklung die Vorgaben nach DIN EN 50126 und speziell für die Softwareentwicklung nach EN 50128 zu berücksichtigen. In den zugehörigen Tabellen sind die für die jeweilige Sicherheitsanforderungsstufe notwendigen und stark empfohlenen Methoden, z.B. modellbasiert, Simulation u.a. Verfikations- und Validierungsmethoden empfohlen. Insbesondere ist hier eine sicherheitsgerichtete Erprobung im Bahnumfeld erforderlich.

5.6.6 Feststellung

Die offene Frage der Integration einer außerhalb des Eisenbahnwesens existierenden Infrastruktur der Satellitensysteme mit ihren Raum- und Bodensegmenten kann durch Cross Acceptance und einen speziellen methodischen Ansatz für das Nutzersegment (Empfänger und Antenne) gelöst werden. Der Ansatz fußt auf einer sicheren Überwachung der Integrität einer verfügbaren satellitengestützen Lokalisierung. Seine Voraussetzungen sind

1. Garantierte Signalversorgung durch das Raum- und Bodensegment des Satellitenortungssystems und
2. qualifizierte Sensoren und Ermittlung von Merkmalsgrößen wie MTTEF, Genauigkeiten u.a.

Insbesondere müssen dazu die GNSS-Empfänger nach metrologischen Verfahren qualifiziert werden, um ihre Merkmalsgrößen wie MTTEF, Genauigkeiten u.a zu ermitteln. Erfüllbare Voraussetzungen dafür sind normkonforme Beschreibungen der Messbedingungen, der Prüfprozeduren und Referenzen und Prozeduren für die Auswertung der Tests und Darstellung der Ergebnisse sowie einer Zertifizierung, die von existierenden akkreditierten Institutionen erbracht werden können. Weiterhin gehört hierzu die konventionelle Qualifizierung von weiteren Sensoren oder die Nutzung bereits im Eisenbahnwesen verwendeter. Hinzu kommt die Verfügbarkeit einer qualifizierten aktuellen referenzierten digitalen Karte des Streckennetzes. Die Erstellung einer sicheren Detektion zur fehlerhaften Lokalisierung mit normkonform entwickelten und implementierten Algorithmen auf der Grundlage der qualifizierten Parameterwerte erfolgt nach bewährten Vorgehensweisen.

Die Entwicklung des sicheren Lokalisierungssystems insgesamt kann somit normgerecht nach den einschlägigen Vorschriften der Entwicklung sicherheitskritischer Systeme des Eisenbahnsektors durchgeführt werden.

Eine Zulassung eines sicheren satellitengestützten Lokalisierungssystems im Eisenbahnbereich erscheint unter Beachtung der genannten Voraussetzungen machbar.

Abbildung 5.22: Vorgeschlagene Struktur der Entwicklung und Dokumentation für den Sicherheitsnachweis einer satellitenbasierten Lokalisierung nach (Manz)

5.7 Zusammenfassende Feststellung

Durch die Zusammenführung dieser Ansätze wird dargelegt, dass die prinzipielle technische Zulassungsfähigkeit sowohl nach der CENELEC Norm EN 50129 als auch nach der CSM_RA möglich ist, wenn die entsprechenden Vorgaben der Entwicklung berücksichtigt werden und eine entsprechende Dokumentation und Erprobung nach Maßgabe der Qualifizierung erfolgt, welche eine positive Begutachtung ermöglicht.

Aus gutachterlicher Einschätzung erscheint die Zulassung eines satellitengestützten Lokalisierungssystems im Schienenverkehr machbar.

Im Detail muss in einer späteren Phase, z.B. bei der Entwicklung, geprüft werden, ob die Genauigkeitsanforderungen mit den Sicherheitsanforderungsstufen mit dem erforderlichen Aufwand im Sinne des ALARP Kriteriums in Einklang zu bringen sind.

Im Rahmen des übergeordneten Risikomanagements einer satellitenbasierten Lokalisierung müssen die Fragen einer TSI-Konformität und Systemgarantie für GNSS hinsichtlich einer längerfristigen Verfügbarkeit des Raum- und Bodensegmentes geklärt werden.

6. Gesamtlösung

6.1 Gleisgebundene Lokalisierungsobjekte

Gleisgebundene Lokalisierungsobjekte führen grundsätzlich eine Bewegung entlang der Gleises aus. Daraus ergibt sich ein einschränkender Determinismus in Gleisrichtung. Dadurch ist eine diversitäre Lokalisierung unter Miteinbeziehung der Gleisstrukturen und den damit verbundenen Einschränkungen möglich.

6.1.1 Lokalisierung Triebfahrzeug

Mittels den aktuell laufenden Proofs of Concept werden die in der Machbarkeitsstudie erarbeiteten Lösungsvarianten vertieft, überprüft und ggf. weiterentwickelt. Zudem erfährt die Gesamtarchitektur von SmartRail 4.0 noch diverse Anpassungen. Entsprechend sind die hier aufgeführten Varianten (mögliche Lösungen) unter Vorbehalt neuer Erkenntnisse zu verstehen.

Für das Triebfahrzeug werden drei Lösungsvarianten abgeleitet. Im Folgenden werden die für die drei Varianten verwendeten Sensoren bzw. funktionalen Einheiten beschrieben.

Die **GLAT OnBoard** am Triebfahrzeug - ausgebildet als **Lokalisierungseinheit (LL) mit Überwachungsfunktion (Ü)** - besteht aus den Sensoren:

GNSS im Navigationsmodus RTK bzw. PPP: Es werden die Systeme GALILEO (europäisch, zivile Führung) und GPS (amerikanisch, militärische Führung) genutzt. Eine getrennte und kombinierte Verwendung von GPS und GALILEO erlaubt wechselseitige Überprüfung und in Kombination mit “Receiver Autonomous Integrity Monitoring (RAIM)” sowie dem SBAS System EGNOS höchst mögliche Genauigkeit und Integrität der Lokalisierung.

GNSS (i.e. GPS + GALILEO + EGNOS) liefert einen dreidimensionalen Orts-, Richtungs- und Geschwindigkeitsvektor sowie die **Referenzzeit (UTC) für das gesamte GLAT**.

Die interne Taktrate von GNSS sollte mindestens 10 Hz betragen.

Die Einspeisung der Korrekturdaten von Basisstationen ermöglicht den Navigationsmodus “Real-Time-Kinematic (RTK)”. Dieser Navigationsmodus liefert auf Basis den präzisesten Orts-, Richtungs- und Geschwindigkeitsvektor. Allerdings erfordert dies zwecks kontinuierlicher Übertragung der Korrekturdaten von Basisstationen eine permanente Kommunikation der GLAT OnBoard über Mobilfunk. Das erforderliche Datenvolumen wird ca. 1 MByte pro GLAT OnBoard und Tag betragen (oder ca. 97 bit/s). Der Navigationsmodus PPP wird in Bezug auf die Genauigkeit der Lokalisierung voraussichtlich (hier werden in den weiteren GLAT Phasen Messungen notwendig) den Anforderungen gerecht. Orts-, Richtungs- und Ge-

schwindigkeitsvektor sind weniger genau als im Modus RTK. Dafür wird im Modus PPP eine deutlich geringere Menge an Korrekturdaten von Basisstationen, die nicht notwendiger Weise über Mobilfunk, sondern auch über SBAS übertragen werden kann, benötigt. Das erforderliche Datenvolumen im Modus PPP beträgt ca. 100 KByte pro GLAT OnBoard und Tag, wobei diese Daten im “broadcast” übertragen werden.

Trägheitsnavigationssystem (IMU) auf Basis **“Faser Optische Gyroskope (FOG)”** mit Beschleunigungssensoren auf siliziumbasierten Mikro-Elektro-Mechanischen Sensoren und Systemen (MEMS): Die IMU in “strap-down” Ausführung, idealer Weise am oder in der Nähe des Drehgestells montiert, liefert einen dreidimensionalen Richtungs- und Geschwindigkeitsvektor. Die interne Taktrate der IMU sollte mindestens 100 Hz betragen.

Odometrie: Diese ist als direkter Abgriff des Radumdrehungsimpulses (mit Drehrichtungsbestimmung) ausgebildet. Der Abgriff erfolgt parallel zum ETCS und ist entweder durch hochohmige oder einspulige Trennung rückwirkungsfrei bezüglich ETCS. Der Radumdrehungsimpuls wird von analog auf digital gewandelt und entsprechend verarbeitet. Das System liefert einen in Gleisrichtung eindimensionalen Geschwindigkeitsvektor. Dieser wird vom Schlupf der Räder in der Genauigkeit beeinträchtigt. Der Schlupf entsteht durch die angetriebenen Räder während Phasen starker Beschleunigungen des Triebfahrzeugs i.e. beim Anfahren und Bremsen. Im Rahmen der Sensorfusion im GLAT OnBoard soll bei guter Verfügbarkeit von GNSS und über die IMU die vom Radimpuls abgeleitete Geschwindigkeit und damit verbundenen systematischen Fehler (Rad/Schiene) “mit kalibriert” und in Phasen von Beschleunigungen des Triebfahrzeugen (Bremsen, Anfahren) möglichst ausgeglichen werden.

Doppler Radar: Das System liefert einen in Gleisrichtung eindimensionalen, schlupffreien Geschwindigkeitsvektor, ist jedoch - wie der Radimpulsgeber - bei niedrigen Geschwindigkeiten und Stillstand sowie Eis und (nassem) Schnee störungsbehaftet.

Physische und Virtuelle (Euro-)Balisen: Die Funktionalität der physischen (Euro-)Balisen ermöglicht einen “Reset” der Lokalisierung, da Ort der Balise und Zeitpunkt des Überfahrens exakt ermittelt werden können. Die physischen (Euro-)Balisen sind gleisselektiv gesetzt und erlauben eine deterministische, exakte Lokalisierung des Objektes. In der Sensorfusion der Lokalisierungseinheit wird durch physische (Euro-)Balisen der Filter der Lokalisierungslösung zurückgesetzt und etwaige Fehler durch GNSS oder bei nicht Vorhandensein von GNSS der “freischwingenden” IMU z.B. in einem Tunnel ausgeglichen.

Virtuelle (Euro -)Balisen ausgeprägt als einzelne oder kombinierte “Geo-Objekte” substituieren soweit betrieblich möglich physischen (Euro -)Balisen in Bezug auf deren Funktionalität im Rahmen von ETCS >= L2.

Die Schnittstelle zur physischen (Euro-)Balisen bzw. die Übertragung der Ereignisdaten (Ort bzw. ID und Zeit) erfolgt entweder

- über eine Schnittstelle zwischen der GLAT OnBoard und der ETCS Einheit am Triebwagen; oder
- über eine Übertragung der Ereignisdaten (Ort bzw. ID und Zeit) vom Stellwerk über den GLAT Server an die GLAT OnBoard. Die damit verbundenen Übertragungslatenzen werden bei der Verarbeitung der Daten in der GLAT OnBoard Sensorfusion berücksichtigt.

On Board Lokalisierungseinheit (LL) mit Überwachungsfunktion (Ü): Die genannten Sensoren werden in der GLAT OnBoard fusioniert, wobei eine "eng gekoppelte" Fusion d.h. eine Vereinigung aller Sensoren in einem gemeinsamen Filter (i.d.R. eine erweiterter Kalman-Filter) präferiert wird. Das Ergebnis der "Sensorfusion" ist ein kohärenter, dreidimensionaler Orts-, Richtungs- und Geschwindigkeitsvektor auf Basis der Referenzzeit (UTC). Durch die Kopplung führt ein temporärer Ausfall eines Sensors z.B. GNSS durch Abschattung in einem Tunnel oder Vegetation zu einer graduellen Verschlechterung des dreidimensionalen Orts-, Richtungs- und Geschwindigkeitsvektors im Rahmen der für den Use Case bzw. das Lokalisierungsobjekt geforderten Genauigkeitsgrenzen. Die Lokalisierungsfunktion bleibt während der Störung aufrecht.

Die Taktrate der Ausgabe des dreidimensionalen Orts-, Richtungs- und Geschwindigkeitsvektor und Referenzzeit (UTC) erfolgt mit mindestens 10Hz.

Die Überwachung der funktionalen Integrität der Lokalisierungseinheit und der generierten Lokalisierung erfolgt relativ im Ausschlussverfahren. Es werden die Sensoren einzeln und in Kombination wechselseitig überwacht und deren Parameter auf Plausibilität überprüft. Bei GNSS erfolgt das im Rahmen von "Receiver Autonomous Integrity Monitoring (RAIM)". Bei RAIM werden die geglätteten Pseudorange Messungen der einzelnen Satelliten gegeneinander auf Konsistenz verglichen[1]. Zusätzlich werden die Lösungen von GPS und GALILEO einzeln auf Konsistenz überprüft. Ein Vergleich der Beschleunigungen und Richtungsänderungen der IMU gekoppelt mit der Odometrie (Geschwindigkeit) mit den auf Basis von GNSS ermittelten Werten zeigt Bereiche, in denen die GNSS Signale offensichtlich Störungen unterlegen sind. Weicht der auf Basis von GNSS berechnete Richtungs- und Geschwindigkeitsvektor bzw. die Änderung dessen deutlich von dem über die IMU und Odometrie ermittelten Vektor ab, kann mit großer Zuverlässigkeit von einem schlechten bzw. nicht zuverlässigen GNSS

[1] siehe: http://www.navipedia.net/index.php/RAIM

Ortsvektor ausgegangen werden. Die Gleisgebundenheit und die damit verbundene Eindimensionalität sind für die Überwachungsfunktion von großem Vorteil.

Die tatsächliche Genauigkeit einer integritätsbewehrten Lokalisierungslösung kann durch die Gleisgebundenheit, bei vorab gegebener Gleisselektivität durch einen absoluten Bezug quer – y-Achse – und hoch – z-Achse – zum bekannten Gleis in Bezug zur deterministischen, genauen Gleiskarte berechnet werden. Die Genauigkeit der integritätsbewehrten Lokalisierungslösung längs zum Gleis wird durch eine Differentiallokalisierung mittels zwei Antennen am Triebfahrzeug geschätzt. Die Möglichkeiten und Grenzen der Integritätsbewehrung längs zum Gleis bedürfen in Folgephasen noch einer Vertiefung.

GLAT Server Lokalisierungseinheit (LL) mit Überwachungsfunktion (Ü): Die Lokalisierungsfunktion der GLAT OnBoard dient neben der grundlegenden Funktionalität einer Lokalisierung der orts- und zeitabhängigen Detektion von Ereignissen und damit verbundenen operativen Konsequenzen (z.B. Passieren einer physischen oder virtuellen (Euro-)Balise und eine Freigabe zur Befahrung eines bestimmten Streckenabschnittes). Die Lokalisierung erfolgt als dreidimensionaler Orts-, Richtungs- und Geschwindigkeitsvektor sowie der Referenzzeit (UTC). Der Bezug zum Gleis (Gleiskarte) dient der Überwachung der Genauigkeit.

Aufbauend auf den übermittelten Daten der GLAT OnBoard führt der GLAT Server den dreidimensionalen Orts-, Richtungs- und Geschwindigkeitsvektor zur Referenzzeit (UTC) durch Map-Matching (Gleiskarte) in einen eindimensionalen Orts-, Richtungs- und Geschwindigkeitsvektor zur Referenzzeit (UTC) über und transformiert die geometrische Lokalisierung im System GLAT in eine für das Stellwerk geeignete relative, topologische Lokalisierung. Über die Gleiskarte und die Weichenlage, übertragen vom Stellwerk, wird die Gleisselektivität, quer und hoch zum Gleis garantiert. Längs zum Gleis (x-Achse Lokalisierungsobjekt) erfolgt die Lokalisierung anhand der Projektion des dreidimensionalen Ortsvektors auf das Gleis.

Vom GLAT OnBoard werden die folgenden für den GLAT Server relevanten Daten in einer 1Hz Taktrate über Mobilfunk übertragen:

Dreidimensionaler Orts-, Richtungs- und Geschwindigkeitsvektor mit Referenzzeit (UTC): Dieser beinhaltet die geometrische Position im Bezugssystem (WGS84 für GNSS und LV95 nach der Sensorfusion), sowie die Geschwindigkeit, Richtung und Zeit. Die Zeitauflösung beträgt hundertstel Sekunden (durchgängig im gesamten smartrail 4.0 System).

Basisdaten zur GNSS Lösung und Status Sensorfusion: Zum Zeitpunkt der Lösung empfangene und genutzte GNSS Satelliten mit ID, Azimut und Elevation sowie “Signal Rausch Verhältnis (SNR)” sowie die Statusdaten der Sensorfusion (i.e. Kalman-Filter Varianz und Kovarianzmatrix).

Die folgende Abbildung zeigt die GLAT Architektur als funktionales Blockdiagramm mit Verbindungen und Datenflüssen.

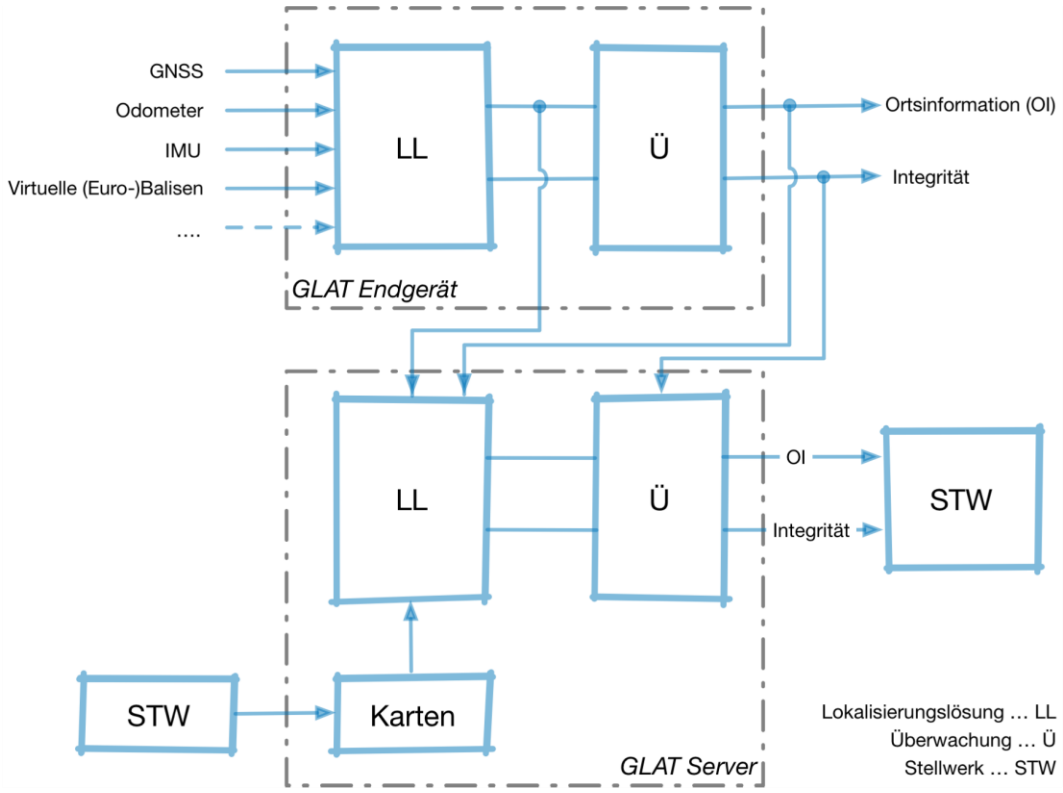
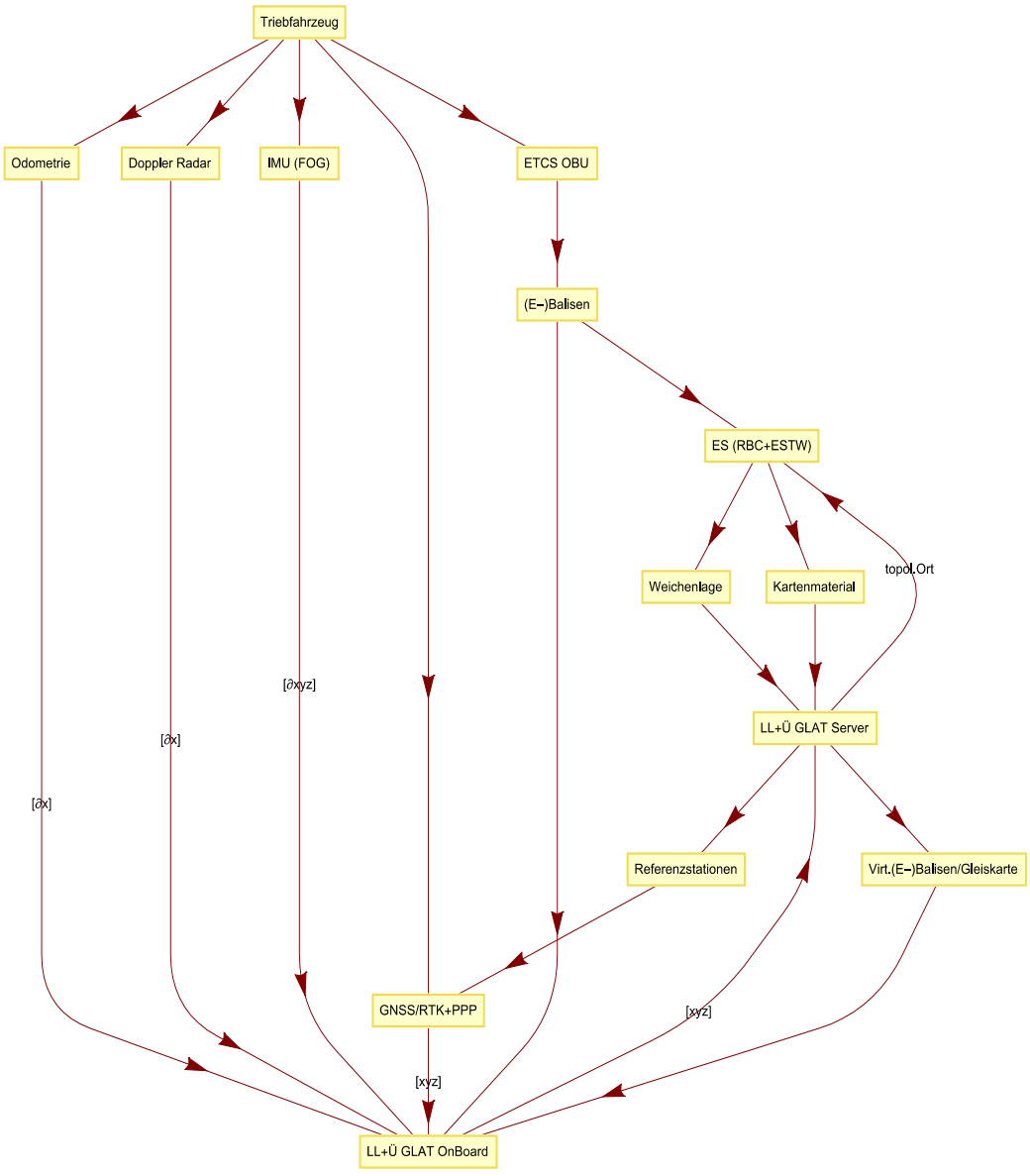


Abbildung 6.23: GLAT Architektur

Die Lösung 1 für ein Triebfahrzeug ist im Folgenden als Graph dargestellt.

Triebfahrzeug Lösung 1 →



Die **Triebfahrzeug Lösung 2** unterscheidet sich von der Lösung 1 durch Wegfallen der Odometrie und Doppler Radar und stattdessen Hinzufügen des Wirbelstromsensors zur exakten, schlupffreien Geschwindigkeitsmessung.

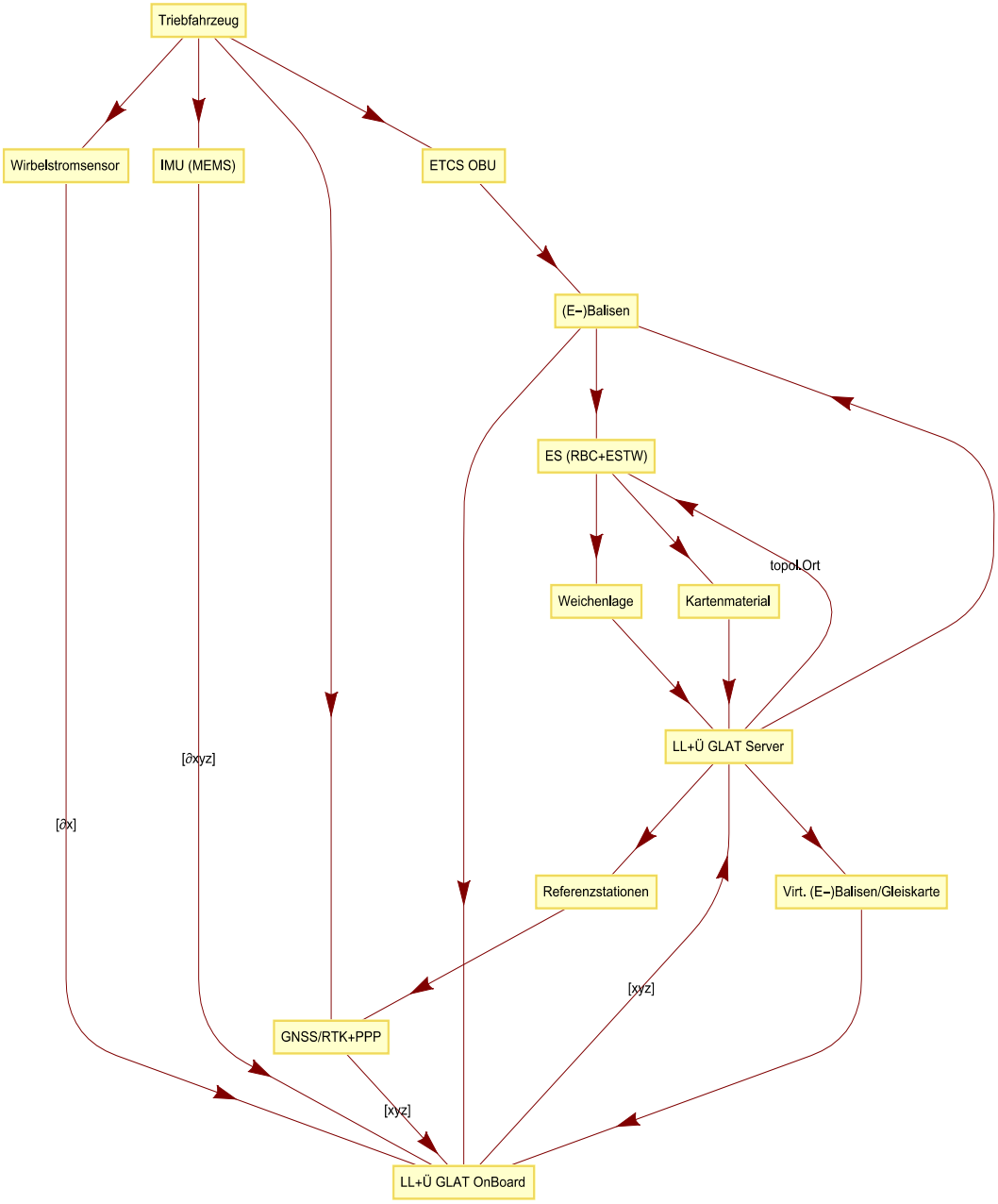
Der **Wirbelstromsensor** hat gegenüber anderen Technologien zur Geschwindigkeitsmessung schienengebundener Objekte den Vorteil einer exakten, schlupffreien Messung der Geschwindigkeit und Fahrtrichtung in Längsrichtung zum Gleis (x-Achse). Auch Weichen und die Weichenlagen werden erkannt. Zusätzlich erweisen sich Prototypen vergleichsweise zum

Doppler Radar als robuster gegenüber Umwelteinflüssen. Ein weiterer Vorteil ist das Wegfallen des Radumdrehungsimpulses (mit Drehrichtungsbestimmung) und damit verbundener rückwirkungsfreier Trennung von GLAT zum ETCS. Nachteilig sind die fehlende Erfahrung im laufenden Betrieb, da sich die Entwicklung des Sensors im Prototypenstadium befindet und der Umstand, dass es aktuell keine Pläne seitens Hersteller in Richtung Produktentwicklung gibt.

Trägheitsnavigationssystem (IMU) rein auf siliziumbasierten **Mikro-Elektro-Mechanischen Sensoren und Systemen (MEMS):** Die IMU in “strap-down” Ausführung, idealer Weise am oder in der Nähe des Drehgestells montiert, liefert einen dreidimensionalen Richtungs- und Geschwindigkeitsvektor. Die interne Taktrate der IMU sollte mindestens 100 Hz betragen. Gegenüber der IMU Ausführung FOG ist die IMU in Ausführung MEMS unter Umständen etwas weniger stabil d.h. der Fehler nimmt mit der Zeit schneller zu. Während eine auf FOG basierte IMU von Werk aus kalibriert wird und nach dem Einschalten sofort exakte Werte liefert, muss sich eine MEMS IMU nach einem Start auf Basis der GNSS Daten zunächst kalibrieren.

Im Rahmen der weiteren GLAT Phasen werden die betrieblichen Unterschiede zwischen FOG und MEMS basierten IMUs über hinreichende Messungen evaluiert.

Triebfahrzeug Lösung 2 →



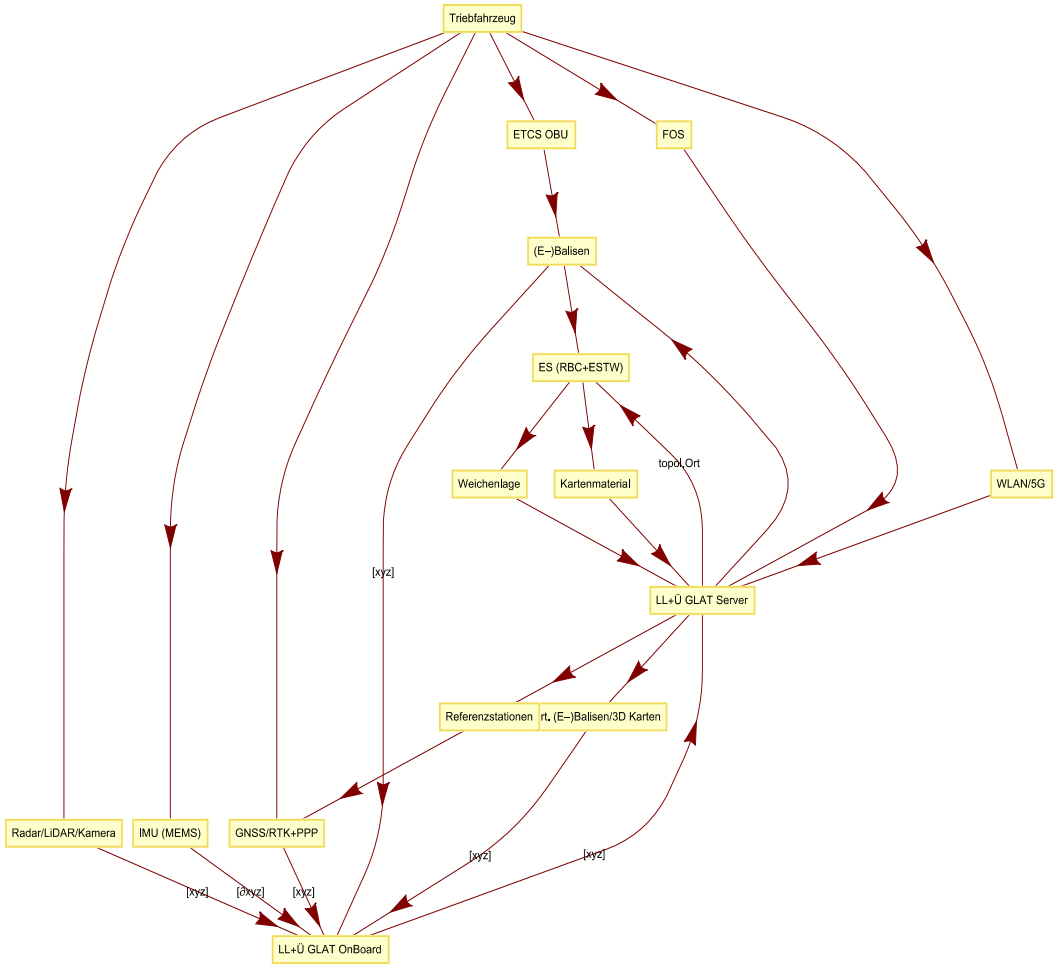
Die **Triebfahrzeug Lösung 3** unterscheidet sich von der Lösung 1 und 2 durch Wegfallen von Odometrie, Doppler Radar sowie Wirbelstromsensor. Stattdessen wird eine schlupffreie Geschwindigkeits- und Ortsbestimmung über eine Kombination aus Radar, LiDAR, optischer Kamera realisiert.

Die **Kombination Radar, LiDAR, optischer Kamera** wird im Bereich des autonomen Fahrens von Straßen gebundenen Objekten (Autos, Busse, etc.) entwickelt und befindet sich aktuell

in einem fortgeschrittenen Prototypenstadium mit teils verfügbaren Ausprägungen im Rahmen von Fahrerassistenzsystemen. Der Vorteil einer Kombination Radar, LiDAR, optischer Kamera besteht, neben der schlupffreien Geschwindigkeitsmessung und Unabhängigkeit von der Odometrie, in einer zusätzlichen, absoluten Ortsbestimmung, was die Sicherheit und Integrität der Lokalisierung im Rahmen von GLAT erhöht und gleichzeitig die Notwendigkeit und Anzahl von physischen (Euro-)Balisen verringert. Nachteilig sind aktuell fehlende Erfahrungen im Bahnbetrieb, potentielle Probleme durch Witterungseinflüsse und die Notwendigkeit von 3D Kartenmaterial am GLAT Endgerät.

Zusätzlich lässt sich mittels **WLAN/5G** eine weitere Plausibilisierung der Lokalisierung, wenngleich auch mit geringerer Genauigkeit, bewerkstelligen. Im Rahmen der Lösung wird diese Technologie der Vollständigkeit halber erwähnt. Die erreichbare Genauigkeit und Zuverlässigkeit einer Lokalisierung lässt sich aktuell nicht abschätzen.

Der Einsatz **von "Fiber Optic Sensing (FOS)"** wurde im Rahmen von ersten Tests in Bezug auf erreichbare Genauigkeiten einer Lokalisierung getestet. Erste Messresultate weisen darauf hin, dass FOS aktuell nicht die notwendige Genauigkeit oder Gleisselektivität ermöglicht, um zur Plausibilisierung im GLAT Server eingesetzt zu werden. Auch gestaltet sich das Fehlen einer eindeutigen Adressierbarkeit von Lokalisierungsobjekten im System FOS als problematisch. In wie weit neue FOS Auswerteeinheiten einen nutzbringenden Beitrag zur Lokalisierung liefern können, muss in Folgephasen vertieft werden.



6.1.2 Lokalisierung Fahrzeug und Nebenfahrzeug

Mittels den aktuell laufenden Proofs of Concept werden die in der Machbarkeitsstudie erarbeiteten Lösungsvarianten vertieft überprüft und ggf. weiterentwickelt. Entsprechend sind die hier aufgeführten Varianten (mögliche Lösungen) unter Vorbehalt neuer Erkenntnisse zu verstehen.

Eine der wesentlichsten Einschränkungen in der Sensorik für Fahrzeuge ist das Fehlen einer durchgängigen d.h. für alle Fahrzeuge verfügbare Geschwindigkeitsmessung mittels Odometrie, Wirbelstromsensor oder ähnlichem. Auch ist die Nutzung von (Euro-)Balisen für alle Fahrzeuge nicht möglich, aber zumindest bei bestimmten Nebenfahrzeugen (Baumaschinen) potentiell machbar. Die Konsequenz daraus ist, dass die Basisausführung einer Lokalisierungslösung - das **„GLAT Tag”** - primär auf GNSS im SPS Modus mit einfacher GNSS Antenne und einer einfachen MEMS basierten IMU beruht. Abgesichert wird die Lokalisierungsfunkti-

on im GLAT Server durch Miteinbeziehen von infrastrukturbasierten Sensoren wie RFID und WLAN/5G sowie bekannter Weichenlage vom Stellwerk. Die Stromversorgung der Basisausführung GLAT Tag erfolgt mit einem Akku. Somit ist die Basisausführung GLAT Tag auf Stromverbrauchsminimierung ausgelegt.

Durch die Vielfalt an Fahrzeugen reichend vom einfachen Güterwagen bis zum hochgeschwindigkeitstauglichen Personenwagen soll das GLAT Tag modular erweiterbar sein. In letzterem Fall kann ein GLAT Tag, mit einem RTK/PPP tauglichen GNSS Modul, einer MEMS IMU und einer Geschwindigkeitsmessung durch Abgriff des Radumdrehungsimpulses (mit Drehrichtungsbestimmung) an der Fahrzeugachse Genauigkeiten und eine Verfügbarkeit annähernd eines GLAT OnBoard erreichen.

Die Nutzung von RFID mit fahrzeugseitig verbauten, passiven RFID Tags und RFID Leseeinheiten entlang des Gleises wird von Seiten SBB für operative Aufgaben abseits von GLAT getestet. Ein großräumiger Einsatz als vergleichsweise günstige Lokalisierung, mit voraussichtlich geringerer Zuverlässigkeit als (Euro-)Balisen, ist machbar.

Zusätzlich lässt sich mittels WLAN/5G eine weitere Plausibilisierung der Lokalisierung, wenngleich auch mit geringerer Genauigkeit, bewerkstelligen. Im Rahmen der Lösung wird diese Technologie der Vollständigkeit halber erwähnt. Die erreichbare Genauigkeit und Zuverlässigkeit einer Lokalisierung lässt sich aktuell nicht abschätzen.

Die **Lösung 1 für Fahrzeuge und Nebenfahrzeuge** beruht auf einer kombinierten GNSS und IMU fusionierten Lokalisierungsfunktion im GLAT Tag in der ein dreidimensionaler Orts-, Richtungs- und Geschwindigkeitsvektor auf Basis der Referenzzeit (UTC, Auflösung 1/100 Sekunde) gebildet wird. Die Überwachung der funktionalen Integrität der Lokalisierungseinheit und der generierten Lokalisierung beschränkt sich auf RAIM, einer Konsistenzprüfung auf Basis Lösungen von GPS und GALILEO, sowie den Vergleich der Beschleunigungen und Richtungsänderungen der IMU mit Werten auf Basis GNSS.

SPS+EGNOS ist ausreichend, um eine Lokalisierung längs zum Gleis innerhalb der geforderten Genauigkeitsgrenzen (Annahme zurzeit 10m rechteckverteilt) zu ermöglichen. Die Gleisselektivität d.h. die erforderliche Genauigkeit quer zum Gleis, i.e. 1,5 m rechteckverteilt wird über den logischen Zugschluss und über Infrastruktur (z.B. RFID) und Logik (Weichenlage im GLAT Server) erreicht.

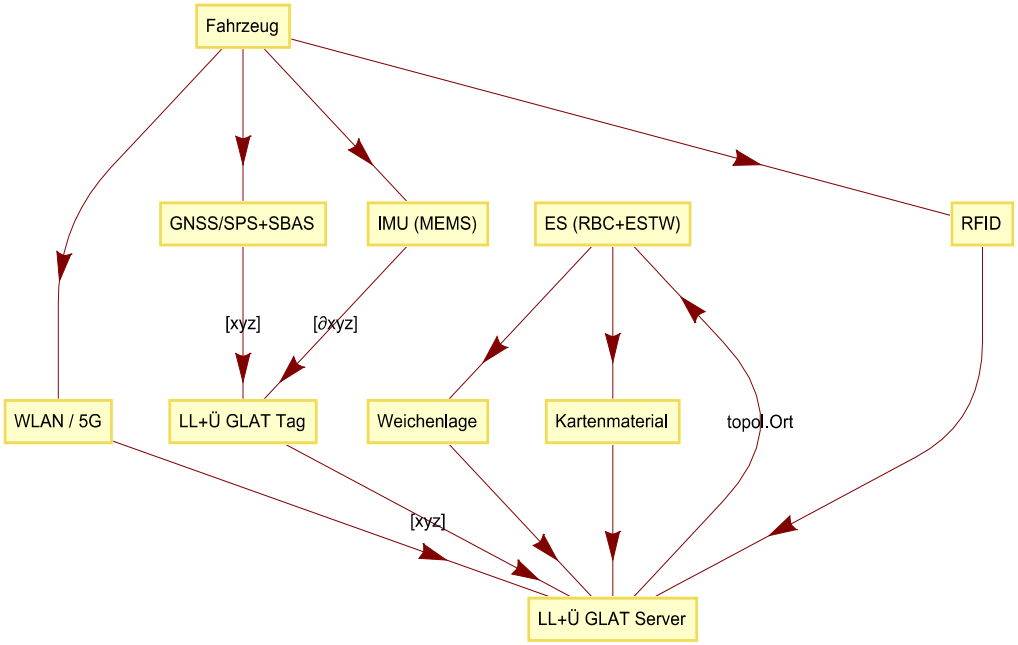
Aufgrund der Einschränkungen der GLAT Tags (neben der Sensorik auch die Stromversorgung) erfolgt die eigentliche Lokalisierung und Überprüfung der Integrität (Überwachung) von Fahrzeugen am GLAT Server. Dort wird anhand der vom GLAT Tag übermittelten Daten (Ortsvektor und Zeit sowie GNSS Daten wie beim Triebfahrzeug sowie die Statusdaten der Sensorfusion, d.h. Kalman-Filter Varianz und Kovarianzmatrix; Übertragung in einer 1Hz Taktrate mittels Mobilfunk) anhand der Gleiskarte ein “Map Matching” in einen eindimensi-

onalen Orts-, Richtungs- und Geschwindigkeitsvektor zur Referenzzeit (UTC) durchgeführt und die geometrische Lokalisierung im System GLAT in eine für das Stellwerk geeignete relative, topologische Lokalisierung transformiert. Über die Gleiskarte und die Weichenlage, übertragen vom Stellwerk, wird die Gleisselektivität, quer und hoch zum Gleis garantiert. Längs zum Gleis (x- Achse Lokalisierungsobjekt) erfolgt die Lokalisierung anhand der Projektion des dreidimensionalen Ortsvektors auf das Gleis.

Die Kombination aus Lokalisierung anhand einer kombinierten GNSS und IMU Lösung und mit einem kontinuierlichen “Reset” ergibt in Abhängigkeit der Dichte der RFID Leser entlang des Gleisnetzes eine relativ hoch verfügbare und sichere Lokalisierung von Fahrzeugen. Die Möglichkeiten und Grenzen der Integritätsbewehrung längs zum Gleis bedürfen in Folgephasen noch einer Vertiefung.

Die Lösung 1 wird als kompaktes autonomes Gerät realisiert, dass sich im Bedarfsfall einfach an zu lokalisierende Objekte wie z.B. dem letzten Wagen eines Güterzuges anbringen und auch wieder entfernen lässt.

Fahrzeug Lösung 1 →



Eine mögliche **Lösung 2 für Fahrzeuge und Nebenfahrzeuge** setzt auf der Lösung 1 auf, integriert das GLAT Tag aber in die Fahrzeugachse. Dies würde dann wie bei GLAT Onboard einen Odometrie-Abgriff ermöglichen und somit einige der oben formulierten Einschränkungen

relativieren, was wiederum die Anforderungen bzgl. streckenseitiger Infrastruktur wie RFID Leser reduzieren kann. Ein Einbau an der Fahrzeugachse erlaubt auch die Nutzung der Bewegungsenergie zur Stromerzeugung, so dass das Thema Stromversorgung gelöst werden kann. Während langer Standzeiten müsste allerdings ein geeigneter Schlafmodus mit nur sporadischer Positionsübermittlung eingenommen werden, um den Strombedarf zu reduzieren. Ob sich diese Lösung aufgrund der potenziell grossen Anzahl von Fahrzeugen, die fest ausgerüstet werden müssten (z.B. jeder Güterwagen, der am Schluss oder im Falle einer geschobenen Fahrt am Anfang eines Zuges eingereiht werden kann), wirtschaftlich darstellen lässt, ist in Folgephasen zu prüfen. Ebenfalls ist im Rahmen von einem geplanten Proof of Concept die technische Leistungsfähigkeit der Lösung (z.B. die Frage der Empfangsbedingungen an der Radachse) zu prüfen.

6.1.3 Resultate aus Messungen etc.

Beispielhafte Resultate von Messfahrten und Nachbearbeitung der Messresultate finden sich auf smartrail40.ch, unter „Publikationen – Lokalisierung, Connectivity, Security“.

6.2 Leer

6.3 Anfangsbedingungen GLAT Lokalisierung

Um sicherzustellen, dass im Rahmen von GLAT mit der Inbetriebnahme eines Lokalisierungsobjektes unmittelbar eine genaue und zuverlässige Lokalisierung im Stellwerk zur Verfügung steht, wird die folgende “Arbeitshypothese” aufgestellt. Diese wird im Rahmen der weiteren Phasen zur Realisierung von GLAT überprüft.

Das GLAT OnBoard und auch das GLAT Tag sind permanent und jederzeit in der Lage, im gesamten Netz die aktuelle Position zu bestimmen. Das erfordert neben der Kombination der Sensorik eine permanente Versorgung zumindest mittels Batterie und soweit möglich eine Zwischenspeicherung von Parametern (z.B. MEMS IMU Kalibrierung) in einem Flash-Speicher. Inwieweit die komplette Sensorik (z.B. Strombedarf für den Radsensor) mit Strom versorgbar ist, gilt es in den weiteren Projektphasen zu verifizieren.

Das GLAT OnBoard (direkt) und das GLAT Tag (im GLAT Server) können relativ zum Gleis und über zwei Antennen die Genauigkeit längs, quer und hoch zum Gleis und die damit verbundene Integrität ermitteln:

- ist die Lokalisierung innerhalb der Grenzen (abhängig vom Use Case) möglich, operiert das Lokalisierungsobjekt nominal im GLAT System;
- ist die Lokalisierung außerhalb der Grenzen, operiert das Lokalisierungsobjekt bis zu einem „Position Reset” mit Einschränkungen;

- ist die Lokalisierung nicht möglich, wird eine Weiterfahrt im System GLAT nicht möglich. Der Bereich um das Lokalisierungsobjekt wird gesperrt.

Ein „Position Reset“ muss räumlich und zeitlich so erfolgen, dass die GLAT Lokalisierung im Normalfall sicher innerhalb der Grenzen bleibt. Ein „Position Reset“ erfolgt entweder über GNSS, wenn wieder verfügbar (offene Strecke), oder über Infrastruktur i.e. (Euro-)Balisen, RFID.

Bei der Umsetzung eines „Position Reset” über (Euro-)Balisen bzw. RFID gibt es grundsätzlich und wie in den Diagrammen oben dargestellt zwei Möglichkeiten:

- Schnittstelle zur ETCS OBU bzw. ETCS BTM (Balise Transmission Modul) im Fahrzeug. Die Balisen „Position & Time“ wird übertragen. Das ist technisch machbar aber potentiell in der Umsetzung komplex und evtl. mit Fehlern behaftet.
- Die Balisen (RFID) „Position & Time“ kommt über das Stellwerk und den GLAT Server die GLAT On-Board (Festnetz und Funk) bzw. wird beim GLAT Tag im GLAT Server berücksichtigt. Diese Variante ist potentiell die einfachere Variante aber in der Umsetzung ebenfalls komplex. Zusätzlich könnte ein “Position Reset” bei der Variante auch über weitere Technologien, z.B. Videoüberwachung an einer Abstellanlage ausgelöst werden.

Beide Varianten eines “Position Resets” werden im Rahmen der weiteren GLAT Phasen geprüft.

7. Verzeichnisse

7.1 Literaturverzeichnis

[1] U. Maschek, Sicherung des Schienenverkehrs - Grundlagen und Planung der Leit- und Sicherungstechnik, Springer, 2015.

[2] E. Schnieder, „Qualität dynamischer Satellitenortung im Eisenbahnverkehr," in *tm - Technisches Messen (4),* April 2012, pp. 210-219.

[3] S. Schmidt, „SBB-Folienauszug NextGen und GLAT," 24.11.2015.

[4] M. Zehnder, „Das Potenzial der genauen, sicheren Lokalisierung," in *16. Internationaler SIGNAL+ DRAHT Kongress,* Fulda, 2016.

[5] S. Schmidt, „SBB, Entwurf Grobkonzept zur Anwendung GLAT v0.3," 21.01.2016.

[6] VDI-Richtlinie 4001 Blatt 3 (Entwurf): Formalisierte Begriffsbildung der Zuverlässigkeit, Düsseldorf: Verein Deutscher Ingenieure, 2014.

[7] M. Wegener, Über die metrologische Qualität der Fahrzeugortung, Dissertation, Technische Universität Braunschweig, 2013.

[8] M. Meyer zu Hörste, Methodische Analyse und generische Modellierung von Eisenbahnleit- und Sicherungssystemen, Dissertation, Technische Universität Braunschweig: VDI-Verlag, 2004.

[9] SBB AG, Szenarienhandbuch, 2016.

[10] D. Lu, GNSS for Train Localisation Performance Evaluation and Verification, Dissertation, Technische Universität Braunschweig, 2014.

[11] D. Spiegel, Qualifizierung sicherheitsrelevanter satellitenbasierter Ortungssysteme, Dissertation in Vorbereitung TU Braunschweig, 2017.

[12] 1474.1-2004 - IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements, 2004.

[13] E. Schnieder, „Qualität dynamischer Satellitenortung im Eisenbahnverkehr," tm - Technisches Messen. (4), 2012, pp. 210-219.

[14] F. Grasso Toro, Entwicklung intelligenter GNSS-basierten Landfahrzeug Lokalisierungssysteme, Dissertation, Technische Universität Braunschweig, 2015.

[15] DIN EN 50129:2003-12; Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik, 2003.

[16] F. Reinbold, M. Wegener und E. Schnieder, QualiSaR - Development of a Qualification Procedure for the Usage of Galileo Satellite Receivers for Safety Relevant Applications, Gdansk, Polen: European Navigation Conference 2012, 2012.

[17] S. Kiriczi, Signaltechnisch sichere Fehlergrenzen für die Erfassung der Bewegungszustände von Bahnen, Düsseldorf: Dissertation, VDI Verlag, 1996.

[18] VDV-Schrift 331: Sicherheitsintegritätsanforderungen für für Signal- und Zugsicherungsanlagen gemäß BOStrab, Köln: Verband Deutscher Verkehrsunternehmen, 2008.

[19] VDV-Schrift 332: Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei

Nichtbundeseigenen Eisenbahnen (NE), Köln: Verband Deutscher Verkehrsunternehmen, 2008.

[20] M. Grimm et.al., „Anforderungen an eine sicherheitsrelevante Ortung im Schienenverkehr," [Online]. Available: http://elib.dlr.de/20857/1/Poster_2_Grimm.pdf.

[21] United States Department of Defense, United States Department of Homeland Security, and Department of Transportation, 2010 Federal Radionavigation Plan, DOT-VNTSC-RITA-08-02/DoD-4650.05, 2010.

[22] G. Barbu, J.-M. Wiss, P. Frosig, M. Schröder, K. Walter, A. Filip, A. Sage und S. Forsyth, Requirements of Rail Applications, GNSS Rail User Forum, 2000.

[23] G. von Buxhoeveden, E. Schnieder und R. Slovák, Comparison and ranking of Swiss railway incident data from 2000 - 2009, COMPRAIL 2012 - 13th International Conference on Design and Operation in Railway Engineering, 2012.

[24] ETCS-Subset FFIS 36.

[25] M. Rousau und D. Cadet, „The Locoprol Project - Low Cost Satellite Train Location System for Train Protection on low Sendity Railway Lines," 2006. [Online]. Available: http://uic.org/cdrom/2006/wcrr2006/pdf/799.pdf.

[26] CSM-Verordnung 402/2013.

[27] Subset 088.

[28] CYSIS, [Online]. Available: https://www.cysec.tu-darmstadt.de/fileadmin/user_upload/Group_CYSEC/Documents/CYSIS-Whithpaper.pdf.

[29] M. Wegener, F. Grasso Toro und E. Schnieder, „Enhancement of the GUM method to dynamical systems: A straightforward approach.," in *ADM 2014 - 8th Workshop on Analysis of Dynamic Measurements*, Turin, Italien, May 2014.

[30] E. Schnieder, „Nutzung von Satelitensystemen für die Eisenbahnen im rechtlichen Rahmen," *ZEVrail*, Nr. 9, pp. 351 - 357, September 2009.

[31] E. Schnieder, Methoden der Automatisierung, Vieweg, 1999.

[32] E. Schnieder, Prozessinformatik. Automatisrung mit Rechensystemen, Vieweg, 2. Auflage 1993.

[33] P. Diekhake, „Systematische Modellierung und Analyse verteilter Automatisierungssysteme.," Dissertation, Technische Universität Braunschweig, Mai 2016.

[34] H. Manz, „Methode zur Sicherheitsnachweisführung einer bordautonomen satellitenbasierten Ortungseinheit für den Schienenverkehr.," Dissertation, technische Universtiät Braunschweig, Braunschweig, 2016.

[35] E. Schnieder, „Braunschweig CERGAL Resolution for Certification of Satellite Based Positioning Systems, its Services and Components for Safety Relevant and Liable Applications," Seybold, j: Summary of the CERGAL 2005. In: Deutsche Gesellschaft für Ortung und Navigation e.V.: Proceedings of the International Symposium on Certification of Galileo System & Services - CERGAL, Braunschweig, 2005.

[36] L. Smith, „Legal Framework for Satellite Supported Applications - GALILEO," Zahradnik, j.: Schnieder, E. (Hrsg.) EURNEX - ŽEL 2008: Proceedings of the Workshop ŽEL GNSS 2008 - GNSS-Based Train Position Detection Device, Starý Smokovec/Slovakia, 2008.

[37] C. Butzmühlen und H. Evers, „GALCERT-Project: Support for the Certification of the

GALILEO Signal-in-Space,“ Proceedings of the International Symposium on Certification of GNSS Systems & Services - CERGAL, Braunschweig, 2008.

[38] O. Heinrich, „Haftungsrisiken und Haftungsmanagement für Unternehmen im Sat-Nav-Bereich,“ Tagungsband der POSITIONs, Braunschweig, 2007.

[39] DIN Deutsches Institut für Normung e.V., „Guide to the Expression of Uncertainty in Measurement,“ Deutsche Übersetzung, Beuth Verlag GmbH, ISBN 3-410-13405-0, 1995.

[40] E. Schnieder, J. Marais, F. Hänsel, J. Poliak und U. Becker, „Methods and Tools for the Certification of GALILEO for Railway Applications,“ Proceedings of the 8th World Congress on Railway Research - WCRR, Seoul/Korea, 2008.

[41] J. Zahradnik und E. Schnieder, „Proceedings of the Workshop ŽEL GNSS 2008 - GNSS-Based Train Position Detection Device,“ EURNEX-ŽEL, Starý Smokovec/Slovakia, 2008.

[42] M. Wegener, M. Hübner und E. Schnieder, „Anforderungen an ein Referenzmesssystem zur Untersuchung der GPS-Messqualität,“ tm – Technisches Messen. (7/8), 2011, pp. 354-363.

[43] DIN EN ISO/IEC 17025:2017-02: Allgemeine Anforderung an die Kompetenz von Prüf- und Kalibrierlaboratorien, 2017.

[44] J. May, „Sicherheitsuntersuchung für einen innovativen Schienenverkehr am Beispiel fahrzeugautarker Ortung,“ Dissertation, technische Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, Braunschweig, 2010.

7.2 Abbildungsverzeichnis

7.3 Tabellenverzeichnis