Tagungsband

Scientific Railway Signalling Symposium 2022

Mehr Schiene – mehr Klimaschutz: Wie kann die Bahn das wachsende Verkehrsaufkommen nachhaltig meistern?

Herausgeber

Prof. Dr.-Ing. Andreas Oetting

18.05.2022

TECHNISCHE UNIVERSITÄT DARMSTADT

Institut für Bahnsysteme und Bahntechnik

Vorwort zur Begleitpublikation zum SRSS 2022

von **Prof. Dr.-Ing. Andreas Oetting**,
Leiter des Instituts für Bahnsysteme und Bahntechnik an der Technischen Universität Darmstadt

Liebe Mitglieder der Fachcommunity und Bahn-Interessierte,

aufgrund des Klimawandels wird eine massive Verkehrsverlagerung von der Straße auf die Schiene zwingend. Durch diesen Bedeutungszuwachs der Schiene muss die Eisenbahn bereits im Jahr 2030 ein Verkehrswachstum von 20 - 30 % bewältigen können. Bereits heute ist das Streckennetz jedoch vielerorts an der Belastungsgrenze. Im Rahmen des Scientific Railway Signalling Symposiums (SRSS) 2022 widmeten sich am 18. Mai daher ca. 90 Fachexpertinnen und Fachexperten aus Forschung und Praxis der Frage, wie die Bahn das wachsende Verkehrsaufkommen nachhaltig meistern kann. Nach dem erfolgreichen virtuellen SRSS 2021 konnte das fünfte SRSS 2022 wieder in Präsenz im Georg-Christoph-Lichtenberg-Haus in Darmstadt stattfinden.

Die Beiträge der Konferenz zeigten, dass eine der größten Herausforderungen die Entwicklung und das reibungslose Zusammenspiel der verschiedenen Technologien darstellt, die das zukünftige Eisenbahnsystem bilden werden. In den Keynotes berichtete zu Beginn Bernd Elsweiler von der DB Netz AG über eine Vielzahl von Projekten und Programmen, die zur Umsetzung des Zielbildes der Digitalen Schiene Deutschland beitragen sollen. Roman Treydel von der DB Netz AG erläuterte, wie Initiativen wie Shift2Rail und RCA in ERJU zu einem vereinheitlichten europäischen Bahnsystem führen sollen. Durch die Diskussion in Kleingruppen wurde bereits der Blick auf die übernächsten Innovationen geworfen.

Der Nachmittag widmete sich detaillierteren Themen. Neben wissenschaftlichen Vorträgen aus den Bereichen Zugvollständigkeitserkennung und digitaler automatisierter Infrastrukturplanung standen Themen aus der Praxis im Vordergrund. In dieser Publikation sollen ausgewählte Arbeiten zu den Praxis-Vortragsthemen veröffentlicht werden.

Sonja-Lara Bepperling von Nextrail berichtete von modernen Lösungsansätzen zur Strukturierung der Zulassungs- und Sicherheitsbewertungen, da der Sicherheitsnachweis für alle Innovationen im Bereich der Sicherungstechnik eine zentrale Rolle spielt. Neben funktionaler Sicherheit ist auch die Gewährleistung der Sicherheit gegen Angriffe (Security) ein zentrales Thema. Dabei ist ein schnelles Erkennen des Angriffs und der Angriffsart und darauffolgend ein zielgerichtetes Handeln essentiell. Damit die schnelle Bewertung von Angriffen gewährleistet werden kann, wurden von Markus Heinrich von der INCYDE GmbH Angriffsgraphen zur Unterstützung der Risikoanalyse sowie zur expliziten Zuordnung von Bedrohungen vorgestellt.

Um Kapazitätsvorteile im Bereich der LST zu erzielen, sind viele innovative Technologien auf eine präzise Ortung der Fahrzeuge angewiesen. Einige dieser Technologien basieren auf dem Prinzip von Fiber Optic Sensing (FOS), bei dem die akustischen Ereignisse entlang der Strecke mit Hilfe

der verlegten Glasfaserkabel in Echtzeit lokalisiert und durch Methoden der Mustererkennung klassifiziert werden. Roman Wilhelm von AP Sensing gab hierzu einen Einblick in neuartige Lösungsansätze zur zuverlässigen KI-basierten Zugortung in Echtzeit.

Neben der Entwicklung innovativer Technologien muss auch der Rollout dieser Technologien effizient und zeitnah umsetzbar sein. Hierfür ist ein effizienter Planungsprozess erforderlich. In diesem Zusammenhang stellte Volker Uminski von WSP die Vorteile der Verknüpfung des LST-Planungstools PlanPro mit der BIM-Planung der Infrastruktur vor.

Wir wünschen Ihnen viel Spaß beim Lesen der genannten Beiträge.

Univ. Prof. Dr.-Ing. Andreas Oetting

Zulassungs- und Sicherheitsbewertung der generischen Anwendung ETCS Level 2 Strecke - ein Erfahrungsbericht

Dr.-Ing. Sonja-Lara Bepperling[1], Dipl.-Ing. Viola Römer[2]

NEXTRAIL GmbH, DB Netz AG

1 Einleitung

Das ETCS-Rollout in der LST-Branche stellt alle daran mittelbar und unmittelbar Beteiligten vor große Herausforderungen. Insbesondere die Zulassungs- und Sicherheitsbewertungen stehen stark im Fokus. Viele Fragen müssen in diesem Zusammenhang beantwortet werden: *Welche Gesetzte/Normen müssen wir im Projekt einhalten? Welche Rollen gibt es und wer bekommt welche Dokumente zu welchem Zeitpunkt? Können wir Synergien nutzen?“ usw.*

2 Ziel

Im Folgenden wird ein möglicher Lösungsansatz zur Strukturierung der Zulassungs- und Sicherheitsbewertung für die streckenseitige LST aufgezeigt. Dabei schöpfen die Autorinnen aus Erfahrungen im Rahmen der mehrjährigen Begleitung der generischen Lastenheftentwicklung von ETCS Level 1 und 2 sowie deren (Teil-)Prüferklärungen.

Das vorliegende Paper konzentriert sich auf die Zulassungs- und Sicherheitsbewertungen der generischen Anwendung ETCS Level 2 Strecke, bei der zurzeit die Erstellung des Release 3.1 Lastenheftes für ETCS Level 2 Strecke begleitet wird. Die vorgestellten Beispiele beziehen sich in erster Linie auf das Safetymanagement, die Verifikation, die Validierung und die Gutachterbegleitung im Rahmen des vorgenannten Lastenheft Release.

3 Problem

Im Jahr 2005 bekam die Deutsche Bahn die Zulassung vom Eisenbahn Bundesamt (EBA) für die ETCS-Pilotstrecke Jüterbog-Leipzig. Seitdem wurde an einem Lastenheft für ETCS mit vollem Funktionsumfang gearbeitet, inklusive Risikoanalyse (RA) und betrieblicher Gefährdungsanalyse (bGA) in Zusammenspiel mit den damals geltenden europäischen Vorgaben der UNISIG.

Das generische Lastenheft für ETCS Level 2 Strecke (Baseline 2) wurde erstmalig für die Neubaustrecken VDE 8.1 und VDE 8.2 [7] geschrieben und begutachtet. Damals folgte der Zulassungsprozess der *Verwaltungsvorschrift Neue Typzulassung von Signal-, Telekommunikations- und Elektrotechnischen Anlagen* [10], die im Jahr 2013 zur Anwendung bei den Projekten VDE 8.1 / 8.2 erstellt und freigegeben wurde. Die im Jahr 2009 veröffentlichte *Verordnung (EG) Nr. 352/2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken* [1] war zu diesem

[1] Sonja-Lara Bepperling: sonja-lara.bepperling@nextrail.com

[2] Viola Römer: viola.roemer@deutschebahn.com

Zeitpunkt bereits gültig, wurde aber bei der Erstellung der VV NTZ [10] nicht genügend gewürdigt. Für die ETCS-Lastenhefte basierte daher die Sicherheitsbewertung bis zum Release 3.0 auf den Vorgaben der VV NTZ [10].

Ab 2019 wurde für die Lastenheftentwicklung im VV NTZ Prozess [10] dann ergänzend die CSM-RA Bewertung [1] auf Ebene der Change Requests (CRs) durchgeführt. Diese zusätzliche Bewertung aller CRs war sehr aufwendig. Die DB Netz AG hat daher für die Lastenheftentwicklung zum Release 3.1 eine neue Vorgehensweise gewählt, in welcher die Zulassungs- und Sicherheitsbewertungen noch stärker aufeinander abgestimmt und synchronisiert sind. In diesem Zusammenhang wurde auch die Umsetzung der Anforderungen aus der EN 50126 [3] (vor allem Verifikation und Validierung) neu organisiert. Somit konnten auch die Nachweise insbesondere für die neuen Gutachterrollen besser strukturiert werden, siehe dazu auch Abb. 4. Relevante Gutachterrollen in der Lastenheftentwicklung zum Release 3.1 sind der AsBo bzw. die UBS, der ISA[3], der PSV und der Systemgutachter. Im Projekt musste vor allem geklärt werden, wie eine Doppelbewertung durch die Gutachter verhindert werden kann.

Die Prozesstransformation von VV NTZ [10] zu EN 50126 [3] fasst die Abb. 1 grafisch zusammen. Wobei der Fokus des ETCS Level 2 Strecke-Projektes auf den Phasen 1 bis 4 liegt. Mit dem Begriff Phase ist im Rahmen dieses Paper die Lebenszyklusphase gemäß EN 50126 [3], nicht Phase gemäß Sektorleitlinie gemeint. Ein mögliches Zusammenspiel zwischen der Entwicklungsnorm EN 50126 [3] und der Zulassungsbewertung nach Sektorleitlinie [5] wird in Kapitel 7 als Ausblick adressiert.

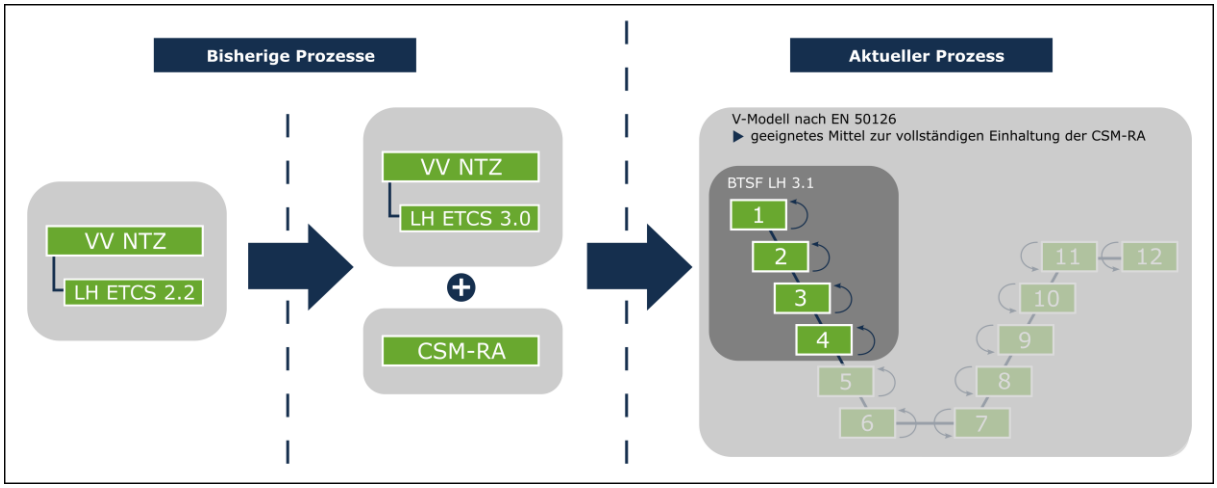

Abb. 1 Prozesstransformation von VV NTZ zu EN 50126
Quelle: Nextrail GmbH (eigene Darstellung)

4 Methode

Für die generische Lastenheftentwicklung ETCS Level 2 Strecke (für Release 3.1) plante die DB Netz AG zusammen mit der NEXTRAIL GmbH eine Prozesstransformation mit zwei großen Zielen:

1) Neue Einbindung der CSM-RA [1] Bewertung in den bestehenden VV NTZ Prozess.
2) Umstellung auf EN 50126 [3] Prozesse.

[3] Hinweis: Im Release 3.1 wird der ISA sowohl durch den AsBo als auch durch den PSV abgedeckt. Das Release 3.1 wurde nach VV NTZ gestartet und im Laufe des Projektes auf die Sektorleitlinie umgestellt. Daher entfällt die Rolle des Systemgutachters.

Es sollten mehr Synergien zwischen den Verfahren CSM-RA [1], VV NTZ [10] und EN 50126 [3] genutzt werden. Nach Einführung der *Sektorleitlinie für die Zulassungsbewertung von Signal-, Telekommunikations- und Elektrotechnischen Anlagen (Technische Vorschrift)* im September 2021 wurde im Projekt beschlossen, von der VV NTZ [10] auf die Sektorleitlinie [5] zu wechseln. Im Projekt kamen daher alle vier Verfahren zur Anwendung.

Hinweis: die TSI-Konformität, die von einem NoBo geprüft und in einem Bericht bestätigt wird, findet im Release 3.1 nachgelagert zu den Safetyprozessen der EN 50126 statt, siehe auch Abb. 4. Daher wird sie im Rahmen des vorliegenden Papers nicht adressiert.

5 Beispiele

Im vorliegenden Paper wird anhand von folgenden drei Beispielen die Prozesstransformation im ETCS Level 2 Strecke Projekt erklärt:

1. Umstellung der so genannten EuE-Papiere auf eine CSM-RA [1] Bewertung.
2. Beschreibung einer Objekt- und Phasenverifikation für die Phasen 1 bis 4 gemäß EN 50126 [3] und einer Gesamtvalidierung in Phase 4.
3. Beschreibung eines Qualitäts- und Konfigurationsmanagements (QM und KM) für das Projekt.

Die Beispiele sind nicht umfassend, sollen aber einen repräsentativen Einblick in die Prozesstransformation geben.

5.1 Umstellung der EuE-Papiere

Das erste große Anliegen des Projektes war es, die CSM-RA [1] Bewertung nicht mehr ergänzend zum VV NTZ [10] Prozess durchzuführen, sondern die CSM-RA [1] in den vorhandenen VV NTZ Prozess [10] aufzunehmen, um die Synergien beider Prozesse zu nutzen. Konkret hat sich das Projekt ETCS Level 2 Strecke dazu entschieden, die CSM-RA [1] Bewertung in den Prozess der sogenannten EuE-Papiere zu integrieren. Diese EuE-Erstellung ist Teil der Nachweisführung für VV NTZ [10] und war immer dann durchzuführen, wenn von den anerkannten Regeln der Technik (a.R.d.T.) abgewichen wird. Bei der LH-Erstellung von ETCS war dies häufig der Fall, da es bislang nur wenige a.R.d.T für ETCS Level 2 gibt, die sich auch in der Praxis bewährt haben.

Die resultierenden EuE-Papiere werden nach EN 50126 [3] der Phase 4 zugeordnet. Inhaltlich stellen sie eine Art generischen Sicherheitsnachweis dar, der zeigt, dass die Werte aus der Risikoanalyse (Phase 3) mit dem geplanten betrieblichen Konzept eingehalten werden oder der Nachweis der gleichen Sicherheit durch einen Vergleich zum Referenzsystem (LZB / PZB) erbracht wird.

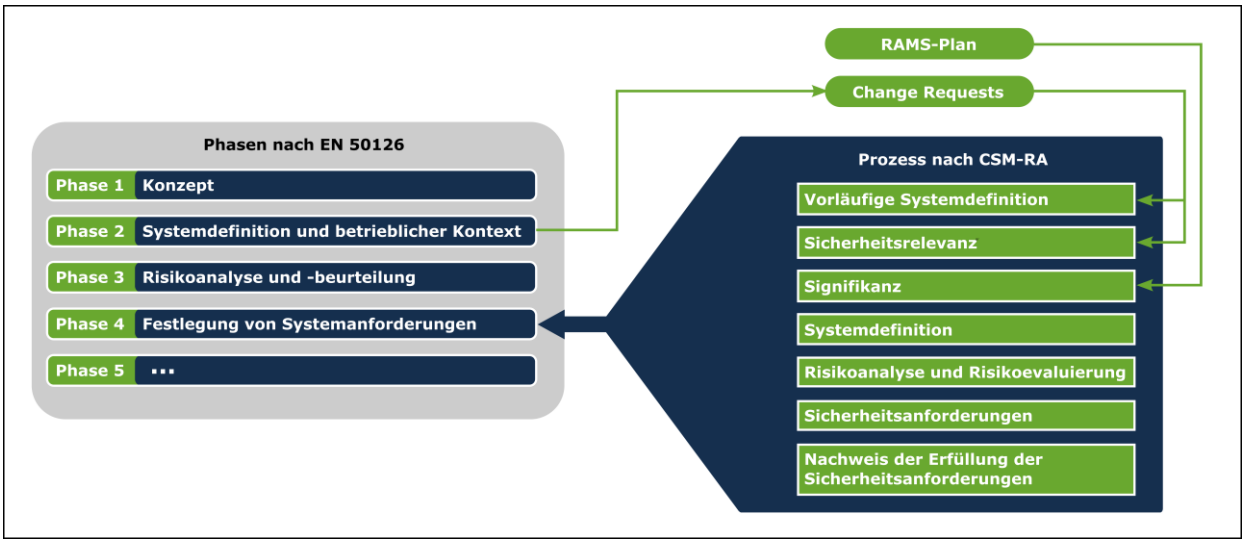

Abb. 2 CSM-RA Bewertung innerhalb der EuE- Papiere
Quelle: Nextrail GmbH und DB Netz AG (eigene Darstellung)

Abb. 2 zeigt schematisch, wie die Schritte der CSM-RA [1] auf die Phasen der EN 50126 [3] und den neuen EuE Prozess abgebildet wurden. Die Phase 2 „Systemdefinition und betrieblicher Kontext“ wurde neu gemäß EN 50126 [3] erstellt und beschreibt die generische Lastenheftentwicklung von ETCS Level 2 Strecke gesamthaft. Die Systemdefinition der CSM-RA [1] als Teil der EuE-Papiere in Phase 4 hingegen beschreibt die jeweilige Änderung, die im EuE-Papier auf Ebene der Lastenheftanforderungen betrachtet wird.

Im Projekt ETCS Level 2 Strecke werden 48 EuE-Papiere aufgrund von CRs fortgeschrieben. Die CRs beinhalten gemäß CSM-RA die vorläufige Systemdefinition der Änderung, da sie beschreiben, was am LH konkret geändert werden soll. Im Rahmen der CR-Erstellung wird auch eine vorläufige Aussage zur Sicherheitsrelevanz der beschriebenen Änderung getätigt. Diese wird dann in einer nachgelagerten CR-Auswirkungsanalyse durch den Safety Manager bestätigt oder nicht. Die CR-Auswirkungsanalyse analysiert, auf welche Gewerke (z.B. LH für die Stellwerke, Instandhaltung, andere ETCS Lastenhefte) der CR einen Einfluss haben könnte – insbesondere auch, ob die in Phase 3 angeordnete Risikoanalyse einschließlich ihrer Systemdefinition vom CR betroffen sein könnte.

Die Signifikanzbewertung erfolgt im Projekt ETCS Level 2 Strecke zentral im RAMS-Plan, der besagt, dass alle sicherheitsrelevanten Änderungen als signifikant eingestuft werden. Mit dieser zentralen Festlegung sollte der Umstellungsaufwand minimiert werden, da somit beispielsweise die Frage nach der additiven Wirkung von Änderungen innerhalb der EuE-Papiere mit den Wechselwirkungen zu anderen EuE-Papieren entfallen konnte. Die Systemdefinition der Änderung gemäß CSM-RA, die Risikobewertung der Änderung und die Ableitung der Sicherheitsanforderungen für die Änderung erfolgen im fortzuschreibenden EuE-Papier.

Ein Ziel der Umstellung war es, große Teile der Sicherheitsbewertung nach VV NTZ [10] der bestehenden EuE-Papiere zu übernehmen. Dazu zeigt Abb. 3 auf der linken Seite die alte EuE-Struktur (Überschriften für ein EuE-Beispieldokument) und auf der rechten Seite die neue EuE-Struktur. Rot markiert sind die Kapitel, die neu hinzukommen. Die Überschriften der Kapitel wurden an die CSM-RA [1] Begriffe angepasst – die Inhalte konnten aus den bestehenden Kapiteln übernommen werden, so

wurde beispielsweise aus dem Kapitel „Verhalten in Fehlersituationen und Verhalten bei Bedienfehlern“ das Kapitel „Gefährdungsermittlung und Einstufung“.

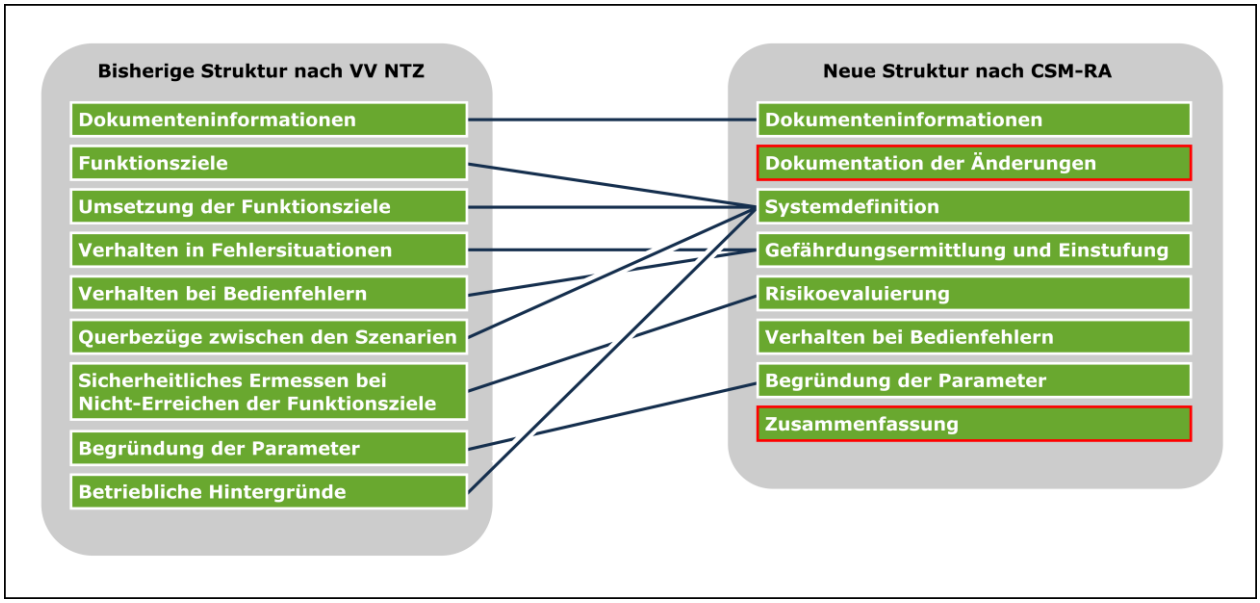

Abb. 3 Neue Struktur der EuE Dokumente
Quelle: ERC Rail für die DB Netz AG (eigene Darstellung)

Der Nachweis der Sicherheitsanforderungen (siehe Abb. 2) erfolgt nachgelagert in der bGA (bzw. in der neuen FMEA und im Gefährdungsprotokoll) als auch weiterhin im sicherheitlichen Ermessen bei EuE-Papieren, die nicht fortgeschrieben werden. Diese gelten prüferklärt weiter. Ein Ziel in den folgenden Releases ist es, alle EuE-Papiere auf die neue Struktur umzustellen, damit die geänderte CSM-RA Bewertung einheitlich dargestellt wird.

5.2 Einführung Phasenverifikation und Gesamtvalidierung

Seit der Neufassung der EN 50126 [3] aus dem Jahr 2017 wird nicht mehr nur in Phase 9 eine Systemvalidierung gefordert, sondern auch ein Validierungsbericht zu den Phasen 1 bis 4. Dies wurde in einem ersten Schritt im Vorgängerrelease (Release 3.0) zum Projekt ETCS Level 2 Strecke als Validierung der Fortschreibung des LH umgesetzt. Es bestand aber die Forderung nach einer Gesamtvalidierung für das Projekt ETCS Level 2 Strecke im Release 3.1. Im Zuge dieser Gesamtvalidierung wurde auch die Phasenverifikation neu eingeführt. Diese ergänzt die Fachprüfberichte, die einer objektbezogenen (Objekt = Dokument) Verifikation gleichgesetzt werden können. Insofern bestand die Einführung des neuen Prozesses aus folgenden Schritten:

1. Aufbereitung der bestehenden Fachprüfberichte und Erstellung von Verifikationstemplates (für die jeweiligen Objekte, z.B. CR, Auswirkungsanalyse oder EuE-Papier);
2. Einführung von Phasenverifikationsberichten, welche die objektbezogenen Verifikationsberichte auswerten und zusammenfassen;
3. Einführung eines Prozesses, in der die Validierung auf die Phasenverifikation aufsetzt.

Abb. 4 zeigt den schematischen Ablauf von der Erstellung eines Dokumentes, über die Verifikation dieses Dokumentes (Objektes), hin zur Phasenverifikation und Validierung. Dieses Gesamtpaket wird dann

dem Gutachter übergeben, wobei der Begriff Gutachter stellvertretend für mehrere Rollen verwendet wird. Diese Rollen sind der AsBo/UBS, der die signifikanten Änderungen nach CSM-RA [1] bewertet, der PSV, der die sicherheitsrelevanten nicht signifikanten Aspekte prüft und FGV, der nach Sektorleitlinie [5] arbeitet.

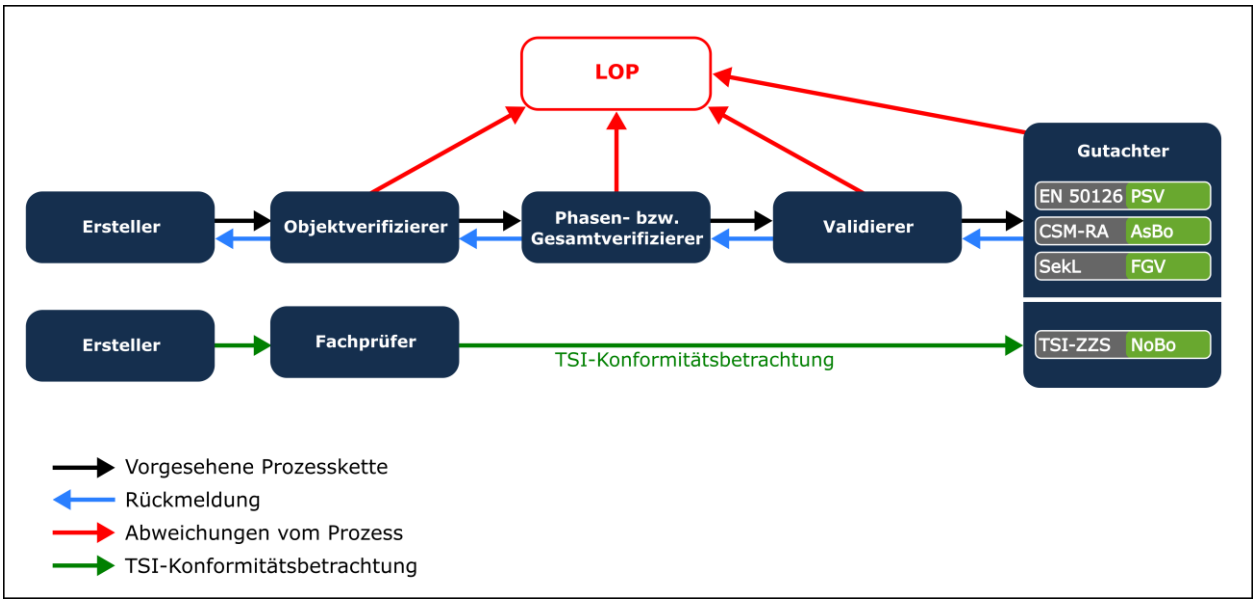

Abb. 4 Prozesstransformation im BTSF-Projekt
Quelle: NEXTRAIL GmbH (eigene Darstellung)

Mögliche Erkenntnisse innerhalb des Prozesses werden z.B. in Form von Listen offener Punkte (LOP) gesammelt und von der Projektleitung der DB Netz AG für das nächste Release bewertet.

5.3 Aktualisierung von QM und KM

Die DB Netz AG besitzt bislang keine ISO 9001 [4] Zertifizierung. Der AsBo muss daher nach Artikel 6 der CSM-RA [1] eine Bewertung der Verfahren für das Sicherheits- und Qualitätsmanagement durchführen. Um für das Sicherheits- und Qualitätsmanagement die Anforderungen der EN 50126 [3] vollumfänglich zu erfüllen, wurde sowohl das Qualitäts- als auch das Konfigurationsmanagement für das Projekt ETCS Level 2 Strecke angepasst und beschrieben. Dies soll auch für zukünftige Releases genutzt werden.

Der Qualitätsmanagementplan enthält z.B. Angaben (keine vollständige Auflistung)

- zu den Rollen im Projekt,
- zum Zeitplan,
- zur Kommunikation im Projekt,
- zur Projektsteuerung,
- zu Tools und Werkzeugen.

Es wird ein QM-Audit durchgeführt und die Einhaltung der Qualitätsziele in einem Qualitätsmanagementbericht festgehalten.

Der Konfigurationsmanagementplan enthält z.B. Angaben (keine vollständige Auflistung)

- zur projektspezifischen Dokumentation,
- zur Datensicherung,
- zum Versionsmanagement,

- zum Freigabeprozess von Dokumenten,
- zum Releasemanagement,
- zum Dokumentenmanagement.

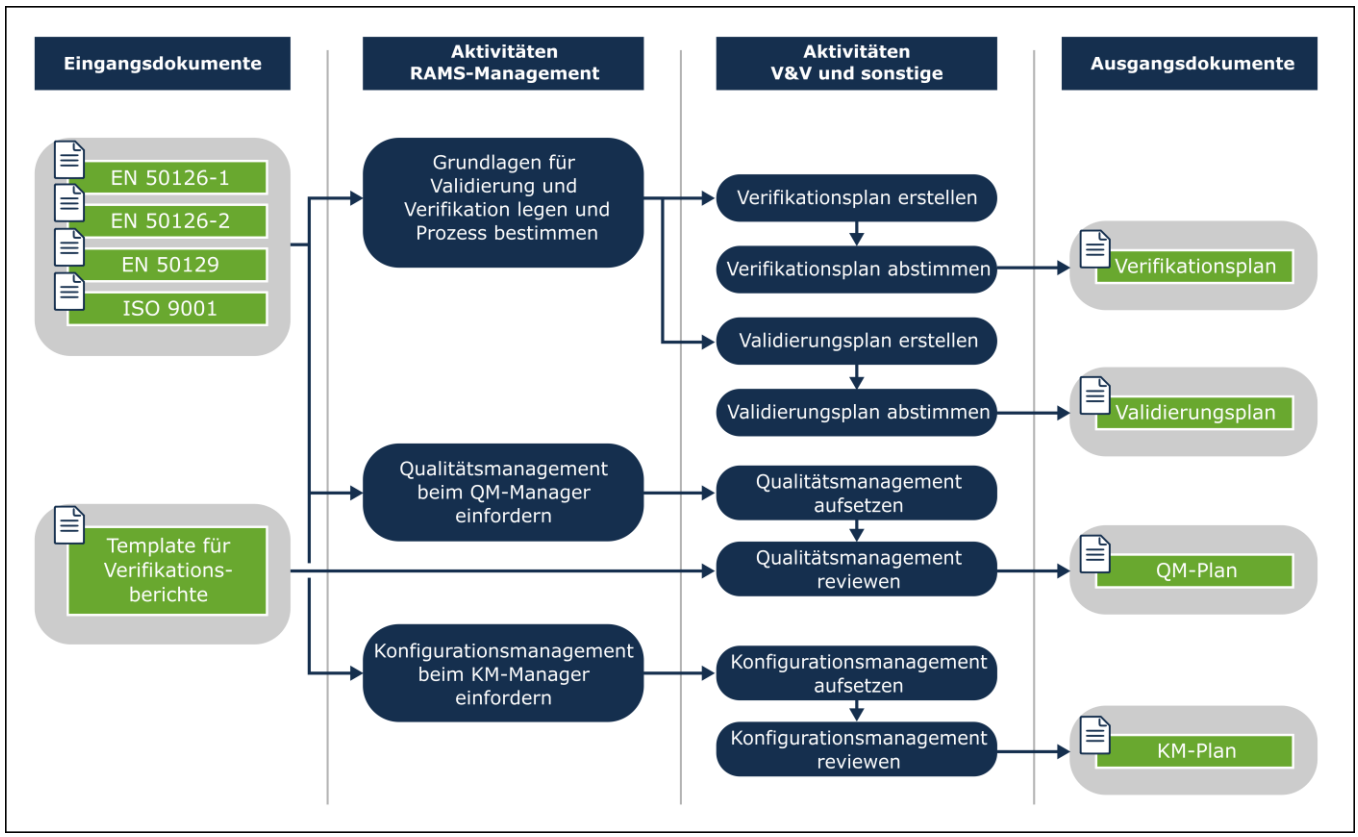

Abb. 5 Ablaufdiagramm der Dokumente pro Lebenszyklusphase (Beispiel)
Quelle: DB Netz AG (eigene Darstellung)

Neben den einheitlichen projektspezifischen Regelungen zum Dokumentenmanagement sei hier erwähnt, dass vor allem die grafischen Darstellungen der Dokumentenläufe einen Mehrwert für das Projekt erzielt haben. Dazu zeigt die Abb. 5 beispielhaft einen Auszug aus dem Ablaufdiagramm der Phase 2, in dem jeweils die Eingangsdokumente der Phase, die RAMS- und Verifikations- und Validierungsaktivitäten (V&V), als auch die Ausgangdokumente dargestellt werden. Dies wurde für alle Phasen im Projekt so dargestellt.

6 Ergebnisse

Die bisherigen Ergebnisse (das Release 3.1 ist noch in Bearbeitung) umfassen folgende Erkenntnisse:

- Die Prozesstransformation wurde unterschätzt, es braucht mehr Zeit für die generische Entwicklung.
- Eine große Herausforderung war nicht die Integration der CSM-RA [1], sondern die Umstellung auf die EN 50126 [3] Prozesse.

- Die Sektorleitlinie [5] brachte als Vorschrift für die Zulassungsbewertung keine Anwendungslösungen bezüglich Rollen und Verfahren (für den Entwicklungsprozess nach EN 50126 [3] insbesondere für die Phasen 1 bis 3).

Da in Zukunft die Zulassungsbewertungen gemäß Sektorleitlinie [5] durchzuführen sind, wird im folgenden Ausblick darauf kurz eingegangen, wie die Synergien zwischen Sektorleitlinie [5], EN 50126 [3] und CSM-RA [1] für streckenseitige LST-Anlagen genutzt werden könnten.

7 Ausblick

Für den Entwicklungsprozess und die Zulassungsbewertung für streckenseitige ZZS-Systeme / Komponenten, die unter die Regelung der TSI ZZS [6] fallen, gelten insbesondere folgende normative Grundlagen:

Europa:

- TSI-ZZS [6]: EU 2016/919 mit EU 2019/776
- EN 50126-1 und -2 (2017) [3], EN 50128, EN 50129, EN 50159; diese Normen sind ein geeignetes Mittel zur vollständigen Einhaltung der
- CSM-RA [1]: EU 402/2013 mit EU 2015/1136. Es müssen die Rollen z.B. des AsBo berücksichtigt werden, auch bei Anwendung der oben genannten EN 50126-Normenreihen.

Deutschland:

- EIGV (2018) [2] inkl. Änderungen vom 17.06.2020: regelt die Bedingungen für die Erteilung einer Inbetriebnahme-Genehmigung; streckenseitige ZZS-Einrichtungen (Kapitel 4,5 und Anlagen 5,6)
- VV GIuV (2021) [8]: GIuV von sicherungstechnischen und elektrotechnischen Systemen und Komponenten
- Sektorleitlinie (2021) [5]: Zulassungsbewertung von STE-Anlagen (T ist noch nicht geregelt)
- VV IBG Infrastruktur (2020) [9]: Anwendung der EIGV für streckenseitige ZZS.

Im Zusammenspiel des Entwicklungsprozesses nach EN 50126 [3] mit der Zulassungsbewertung nach Sektorleitlinie sind zunächst Schnittstellen, mögliche Synergien, aber auch Verbesserungemöglichkeiten zu den Safetymanagement- und Zulassungsprozessen herauszuarbeiten.

Abb. 6 zeigt einen ersten Entwurf zu den Schnittstellen zwischen EN 50126 [3] und Sektorleitlinie [5] in den Phasen 1 bis 4.

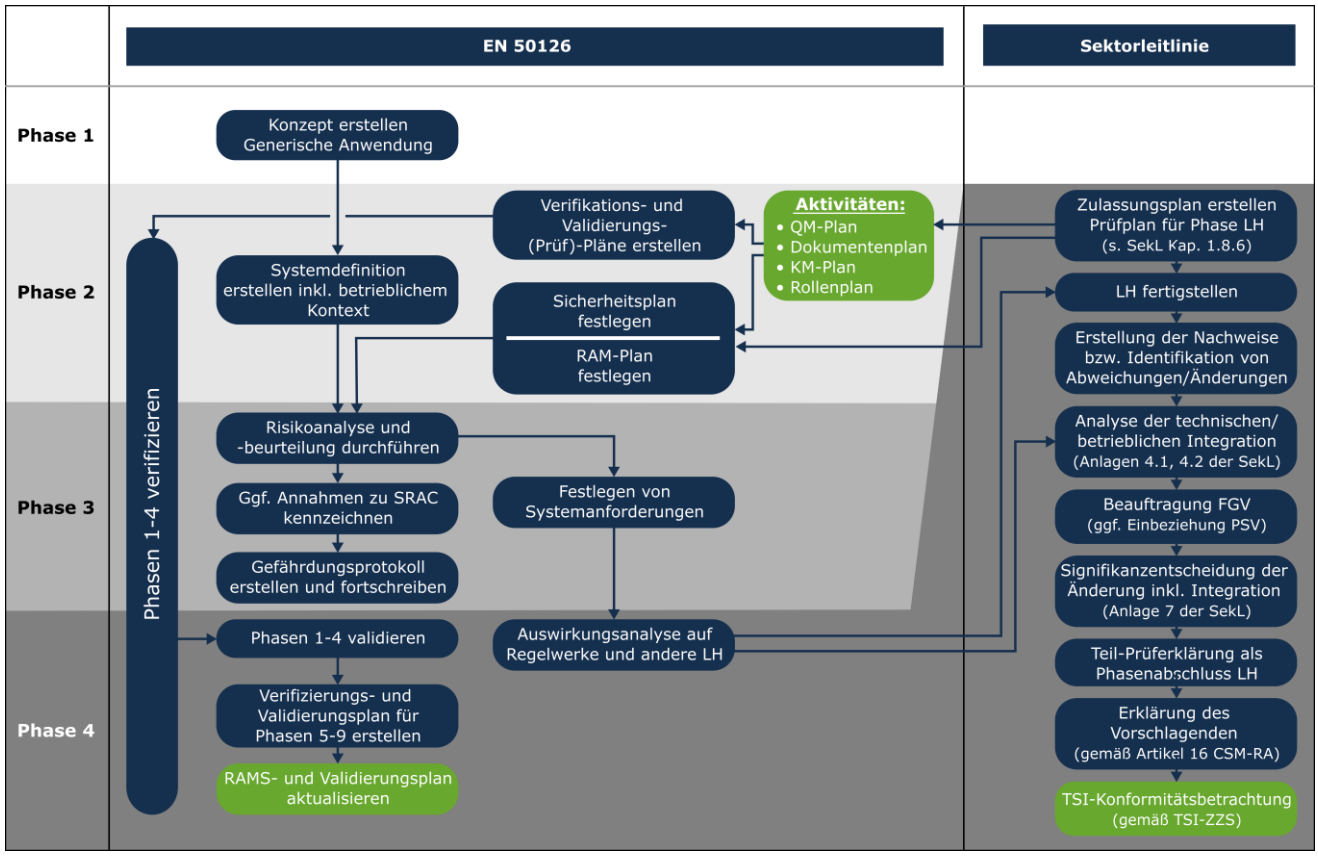

Abb. 6 Phase 1 bis 4 EN 50126 und Sektorleitlinie
Quelle: DB Netz AG (eigene Darstellung)

Die Darstellung inklusive einem sich entwickelnden FAQ soll allen ETCS-Projekten helfen, die verschiedenen Prozesse der Sicherheits- und Zulassungsbewertung zunächst für die LH-Entwicklung besser aufeinander abzustimmen, um dann mehr Handlungssicherheit im Rahmen von Ausrüstungsprojekten zu erlangen.

In einem nächsten Schritt müssen auch die anderen normativen Grundlagen einer entsprechenden Bewertung und Gegenüberstellung unterzogen werden.

8 Abkürzungen

Tab. 1 Abkürzungen

Abkürzung	Bedeutung
a.R.d.T	Anerkannte Regeln der Technik
AsBo	Assessment Body: Unabhängige Bewertungsstelle nach CSM-RA
bGA	betriebliche Gefährdungsanalyse
BTSF	Betrieblich technische Systemfunktion (generisches ETCS Lastenheft für Level 2)
CSM-RA	Common Safety Method on Risk Assessment: Gemeinsame Sicherheitsmethode zur Risikobewertung nach EG 402/2013
CR	Change Request: Änderungsanforderung
DB	Deutsche Bahn
EG	Europäische Gemeinschaft
EN	Europäische Norm
ETCS	European Train Control System: Europäisches Zugsicherungssystem
EuE	Erläutern und sicherheitliches Ermessen (nach VV NTZ)
FGV	Freigabeverantwortlicher nach Sektorleitlinie
ISA	Independent Safety Assessment: Unabhängiger Sicherheitsbewerter nach EN 50126
ISO	Internationale Organisation zu Normung
KM	Konfigurationsmanagement
LH	Lastenheft
LOP	List of Open Points: Liste offener Punkte
LST	Leit- und Sicherungstechnik
LZB	Linienzugbeeinflussung
NoBo	Notified Body: Benannte Stelle (in diesem Fall für TSI-ZZS)
NTZ	Neue Typzulassung
PSV	Prüfsachverständiger
PZB	Punktförmige Zugbeeinflussung
QM	Qualitätsmanagement
RA	Risikoanalyse
RAMS	Reliability, Availability, Maintainability, Safety: Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit
SekL	Sektorleitlinie für die Zulassungsbewertung von STE-Anlagen
STE	Signaltechnik, Telekommunikation und Elektrotechnische Anlagen
TSI	Technische Spezifikation für die Interoperabilität
UBS	Unabhängige Bewertungsstelle nach CSM-RA

VDE	Verkehrsprojekt Deutsche Einheit
VV	Verwaltungsvorschrift
V&V	Verifikation und Validierung
ZZS	Zugbeeinflussung, Zugsteuerung und Signalgebung

9 Literaturverzeichnis

[1] CSM-RA, DURCHFÜHRUNGSVERORDNUNG (EU) Nr. 402/2013 DER KOMMISSION vom 30. April 2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken und zur Aufhebung der Verordnung (EG) Nr. 352/2009; zusammen mit Durchführungsverordnung (EU) Nr. 2015/1136 der Kommission vom 13. Juli 2015 zur Änderung der Durchführungsverordnung (EU) Nr. 402/2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken; C/2016/1574 – Berichtigung der Durchführungsverordnung (EU) 2015/1136 der Kommission vom 13. Juli 2015 zur Änderung der Durchführungsverordnung (EU) Nr. 402/2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken (ABl. L 185 vom 14.7.2015); 13.07.2015.

[2] EIGV, Verordnung über die Erteilung von Inbetriebnahmegenehmigungen für das Eisenbahnsystem (Eisenbahn-Inbetriebnahmegenehmigungsverordnung - EIGV); Ausfertigungsdatum: 26.07.2018.

[3] EN 50126-1 und EN 50126-2: Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Generischer RAMS-Prozess; Deutsche Fassung EN 50126-1:2017, – Teil 2: Systembezogene Sicherheitsmethodik; Deutsche Fassung EN 50126-2:2017.

[4] ISO 9001, Norm DIN EN ISO 9001:2015-11 Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2015); Deutsche und Englische Fassung EN ISO 9001:2015

[5] Sektorleitlinie (SekL) für die Zulassungsbewertung von Signal-, telekommunikations- und elektrotechnischen Anlagen (und Anlagen zur Leitlinie) (Technische Vorschrift), gültig ab 01.09.2021; Version 1.0 vom 07.07.2021.

[6] TSI-ZZS, DURCHFÜHRUNGSVERORDNUNG (EU) 2019/776 DER KOMMISSION vom 16. Mai 2019 zur Änderung der Verordnungen (EU) Nr. 321/2013, (EU) Nr. 1299/2014, (EU) Nr. 1301/2014, (EU) Nr. 1302/2014, (EU) Nr. 1303/2014 und (EU) 2016/919 der Kommission sowie des Durchführungsbeschlusses 2011/665/EU der Kommission im Hinblick auf die Angleichung an die Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates und Umsetzung der in dem Delegierten Beschluss (EU) 2017/1474 der Kommission festgelegten spezifischen Ziele; 27.05.2019.

[7] VDE8, Verkehrsprojekt Deutsche Einheit Nr.8 (VDE8). Available at: https://www.vde8.de/ (Accessed: 28 February 2022).

[8] VV GIuV, Verwaltungsvorschrift für die Genehmigung zum Inverkehrbringen und Verwenden (GIuV) von sicherungstechnischen und elektrotechnischen Systemen und Komponenten VV GIuV; Ausgabe 1.0; gültig ab 01.09.2021.

[9] VV IBG Infra, Verwaltungsvorschrift zur Anwendung der Verordnung über die Erteilung von Inbetriebnahmegenehmigungen für das Eisenbahnsystem (Eisenbahn-Inbetriebnahmegenehmigungsverordnung – EIGV) in Bezug auf die Teilsysteme Infrastruktur, Energie, streckenseitige Zugsteuerung, Zugsicherung und Signalgebung sowie für die übrige Eisenbahninfrastruktur (VV IBG Infrastruktur); Ausgabe 1.1; gültig ab 01.07.2020.

[10] VV NTZ, Verwaltungsvorschrift für die Neue Typzulassung (NTZ) von Signal-, telekommunikations- und elektrotechnischen Anlagen VV NTZ ÜGR Stufe 2 (nicht mehr gültig seit 01.09.2021); Version 1.1 vom 01.07.2016.

Software-gestützte Bedrohungsanalyse durch Angriffsgraphen

Markus Heinrich[1], **Lukas Iffländer**[2]

[1] INCYDE GmbH

[2] Deutsches Zentrum für Schienenverkehrsforschung [beim Eisenbahn-Bundesamt]

1 Einleitung

Die IT- und OT-Sicherheit (=Security) erfordert eine ganzheitliche und regelmäßige Risikobewertung. Ein eigenständiges Produkt, das den Schutz vor Cyberangriffen sicherstellt, existiert genauso wenig wie eine einmalig zu integrierende Lösung. Stattdessen muss der Betrachtungsgegenstand (Asset) regelmäßig einer Risikoanalyse unterzogen werden, die die sich ständig verändernde Bedrohungslage berücksichtigt.

Die einschlägigen Methoden gehen im Kern auf die bekannte Gleichung Risiko = Eintrittswahrscheinlichkeit x Schadensausmaß zurück. Während man in der funktionalen Sicherheit (Safety) von Gefährdungen spricht, wird in der IT-/OT-Sicherheit das Risiko einer Bedrohung betrachtet. Insbesondere die Eintrittswahrscheinlichkeit einer Bedrohung kann dabei häufig nicht durch einen Dezimalbruch angegeben werden, sondern wird auf andere, semi-quantitative Art bewertet (bspw. niedrig, mittel, hoch). Der Eintritt eines IT/OT-Sicherheits-Ereignisses (ein Angriff) folgt keinem stochastischen Prozess, der sich durch eine Wahrscheinlichkeit beschreiben lässt. Die TS 50701 bspw. modelliert die Wahrscheinlichkeit (als Likelihood) über die Attribute Exposition und Verwundbarkeit des betrachteten Systems, die in Stufen von 1 bis 3 bewertet werden. Die DIN VDE V 0831-104 folgt dem Ansatz der IEC 62443 und fordert die Bewertung jeder Bedrohung durch das Wissen, die Ressourcen und die Motivation des Angreifers, was als indirekte semi-quantitative Modellierung der Eintrittswahrscheinlichkeit interpretiert werden kann.

Allen Risikoanalysemethoden ist gemein, dass sie eine Vielzahl von Bedrohungen auf das Asset berücksichtigen müssen, aus der eine umfangreiche Dokumentation resultiert, um die Einschätzung des Risikos aus jeder Bedrohung nachvollziehbar zu machen. Darüber hinaus kann ein hundertprozentiger Schutz vor Angriffen nicht existieren, weil sich die Bedrohungslage stetig ändert und Gegenmaßnahmen aus beschränkten finanziellen und personellen Ressourcen geschöpft werden müssen. Daher ist die Aufgabe der Risikoanalyse und ihrer Dokumentation zu bestimmen, welche Risiken zu mitigieren und welche Risiken zu akzeptieren sind. Damit liefert die Risikoanalyse eine priorisierte Liste von Maßnahmen zur Risikominderung. Gleichzeitig müssen bereits existierende Gegenmaßnahmen abgebildet werden, um eine valide Einschätzung des Risikos zu erhalten.

2 Angriffsgraphen

Zur Unterstützung der Risikoanalyse wird im Forschungsprojekt „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“ [1] die Methodik der Angriffsgraphen

[1] Korrespondierender Autor: markus.heinrich@incyde.com

entwickelt und mit Hilfe eines Software-Werkzeuges abgebildet, das die Analyse automatisiert. Durch das Tool werden der Arbeitsaufwand und die Fehleranfälligkeit des Prozesses reduziert sowie die Nachvollziehbarkeit und Aussagekraft erhöht. Eine Analyse bisher existierender Software-Werkzeuge hat gezeigt, dass es keine Software gibt, die die Anforderungen der Angriffsgraphen komplett abbildet. Es wurden sowohl Software aus der IT-Sicherheits-Forschung als auch kommerziell oder frei verfügbare Produkte betrachtet. Daher wurde entschieden, eine Software gemäß den Anforderungen zu entwickeln und quelloffen zur Verfügung zu stellen.

Die Angriffsgraphen basieren auf den Angriffsbäumen (Attack Trees). Attack Trees sind eine Methode, die in der Informationssicherheit verwendet wird, um Bedrohungen zu analysieren und Bedingungen darzustellen, die gelten müssen, um aus einer Bedrohung einen erfolgreichen Angriff durchzuführen. Es hat sich jedoch gezeigt, dass es von Vorteil ist, auf einige Eigenschaften von Bäumen aus der Graphentheorie zu verzichten. Zum einen erfordern Angriffsgraphen nicht, dass alle Knoten zusammenhängend sind, sodass voneinander unabhängige Angriffspfade auf ein Asset modelliert werden können. Zum anderen erlaubt der Verzicht auf die Anforderung, dass zwischen zwei Knoten nur genau ein Pfad existieren darf, die Wiederverwendung von Teilschritten eines Angriffes und ihrer Bewertung, die in unterschiedlicher Verkettung auch zu unterschiedlichen Konsequenzen führen können.

Ein Angriffsgraph analysiert genau einen Betrachtungsgegenstand (Asset) auf hinreichend spezifischem Abstraktionsniveau. Ein durch einen Angriffsgraphen analysierter Betrachtungsgegenstand könnte z.B. die intelligente Instandhaltung einer Weiche sein. Bei der intelligenten Instandhaltung (Predictive Maintenance) wird durch Überwachung der Betriebsparameter und maschinelles Lernen vorhergesagt wann mit einem Versagen zu rechnen ist, um rechtzeitig vorher eine Instandhaltung durchzuführen. Die exakte Definition des Assets ist nicht Teil der Angriffsgraphen-Methodik. Das Asset wird im Graphen durch ein Trapez dargestellt (siehe Abbildung 1).

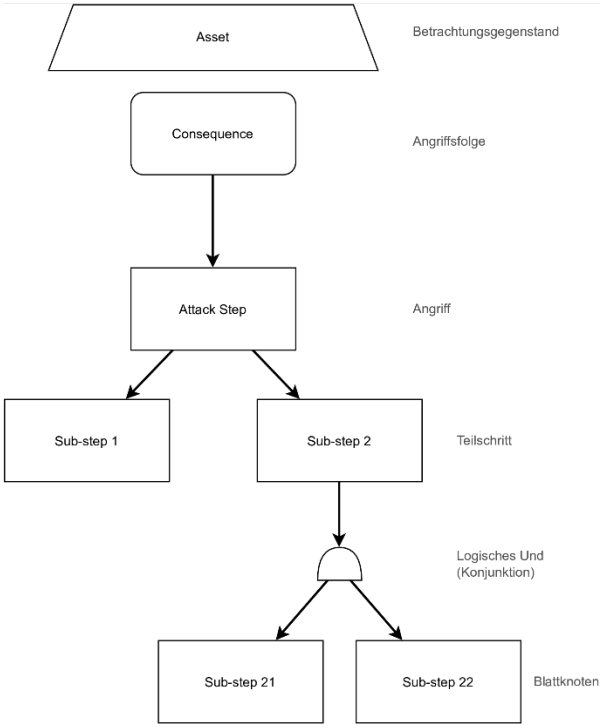

Abb. 1 Beispiel eines Angriffsgraphen für ein Asset

Durch Angriffe auf das Asset entstehen unterschiedliche Angriffsfolgen („Consequence“) oder Schadensereignisse, die im Graphen durch Rechtecke mit abgerundeten Ecken dargestellt werden. Zur Bestimmung der Folgen kommen durch Unternehmen vordefinierte Kataloge von schädlichen Ereignissen, wie z.B. Personenschaden, Reputationsschaden, finanzieller Schaden oder Einschränkung des operativen Geschäfts, in Frage. Genauso erlaubt die Methodik auch die Definition von Folgen durch die Analystin oder den Analysten, falls kein Katalog angewendet werden soll oder eine Erweiterung eines angewendeten Kataloges erfolgen soll.

3 Bedrohungskataloge und Threat Mining

Jede Angriffsfolge kann durch einen oder mehrere Angriffe ausgelöst werden („Attack Step“ in Abbildung 1). Diese Beziehung wird im Graphen durch eine gerichtete Kante von der Folge zum Angriffsschritt dargestellt. Durch diese Verknüpfung erhöhen die Angriffsgraphen die Nachvollziehbarkeit der Risikoanalyse, da sie die mögliche n:m-Beziehung zwischen Angriff und Schaden graphisch darstellen können.

Zur Identifikation der Angriffe können existierende Bedrohungskataloge (bspw. die Elementaren Gefährdungen des BSI [2]) und Methoden des Threat Modellings (bspw. STRIDE [3]) herangezogen werden. Das sog. Threat Modelling ist ein Prozess, um strukturiert IT-Sicherheit gezogene Schwachstellen auf ein System zu identifizieren und so seine Angriffsfläche zu bestimmen. Als Angriff ist hier die Realisierung oder Ausführung einer Bedrohung zu verstehen. Im Beispiel der intelligenten Instandhaltung ist ein Angriff die Manipulation der Vorhersage durch den Angreifer und daraus resultierendes Materialversagen ohne rechtzeitige Vorhersage. Die Folge des Angriffes könnte finanzieller Schaden durch Entgleisen eines Zuges wegen der defekten Weiche sein. Die Verwendung von Katalogen und Threat Mining stellt die hinreichende Vollständigkeit der Bedrohungsanalyse sicher. Angriffsgraphen unterstützen die Analyse durch die grafische Aufbereitung und die Zerlegung der Angriffe in Teilschritte (Sub-step 1 und Sub-step 2) zur Verfeinerung der Analyse und der folgenden

Risikobewertung. Teilschritte setzen sich immer durch logische Disjunktion („oder“) und Konjunktion („und“) zusammen, sodass Fallunterscheidungen in den Angriffsschritten modelliert werden können. Die Methodik erlaubt die Verschachtelung der logischen Verknüpfung und ist prinzipiell auf weitere logische Verknüpfungen erweiterbar.

Eine Aufteilung eines Schrittes in Teilschritte wird durch eine gerichtete Kante zwischen den Knoten dargestellt. Für die Darstellung der Disjunktion und Konjunktion werden entsprechende Knoten zwischen zwei Angriffsschritten erstellt (siehe Abbildung 1). Eine direkte Verbindung zwischen zwei Angriffsschritten stellt implizit eine Disjunktion dar. Die Zerlegung der Angriffsschritte wird iterativ fortgesetzt, bis Teilschritte vorliegen, die hinreichend präzise durch die Attribute zur Bewertung der Eintrittswahrscheinlichkeit (bspw. Ressourcen, Wissen, Motivation nach IEC 62443) beschrieben werden können.

4 Risikobewertung

Die Blattknoten der Angriffsgraphen werden in der Analyse durch einen zuvor gewählten Vektor von Attributen bewertet, um die Eintrittswahrscheinlichkeit zu modellieren. Die Attribute können grundsätzlich frei gewählt werden, um sie der gängigen Praxis der betrachteten Domäne, existierenden Standards und der Risikoaffinität der analysierenden Organisation anpassen zu können. Die DIN VDE V 0831-104 verwendet die aus der IEC 62443 bekannten Attribute „Ressourcen“ sowie „Wissen“ und ersetzt die Motivation durch drei bahnspezifische Risikofaktoren, von denen wir den „Ort“ als Beispiel aufnehmen. So ergibt sich der Attributvektor (Ressourcen, Wissen, Ort), der im Beispiel verwendet wird. Die Attribute werden im Software-Werkzeug über einen Dialog für den Angriffsgraphen festgelegt oder aus einer Vorlage übernommen. Die Einschätzung der Belegung der Attribute erfolgt typischerweise in Workshops mit Expertinnen und Experten und wird in den Angriffsgraphen in die Blattknoten eingetragen und mit Hilfe von Icons visualisiert (siehe Abbildung 2 und Legende in Abbildung 3).

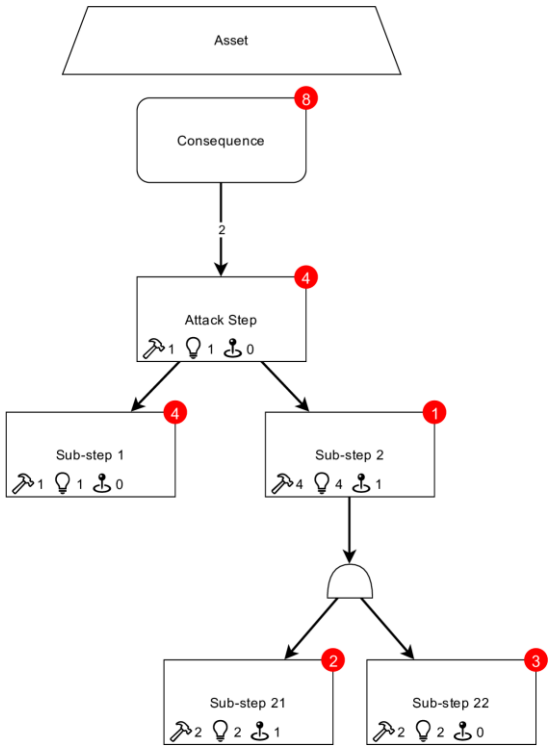

Abb. 2 Angriffsgraph mit erfolgter Bewertung und Aggregation

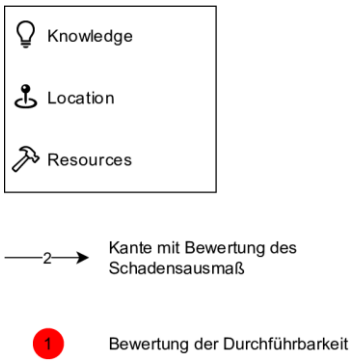

Abb. 3 Legende zum Angriffsgraph

Der Mehrwert der Angriffsgraphen entsteht durch die atomaren Blattknoten, für die sich die Einschätzung der Attribute leichter vornehmen lässt als für komplexere, zusammengesetzte Angriffe. Daraus folgt allerdings die Notwendigkeit, die Bewertung der Blattknoten entlang des Pfades zur Angriffsfolge zu aggregieren, um die Teilschritte wieder zu einer Gesamtbewertung zusammenzusetzen. Das Software-Werkzeug für die Angriffsgraphen unterstützt die Analystin durch vorbereitete und automatisierte Verknüpfung der Teilschritte gemäß der in der Zerlegung definierten logischen Verknüpfungen. Der vorgeschlagenen Disjunktion liegt die Annahme zugrunde, dass sich der Angreifer von mehreren möglichen Teilschritten zur Umsetzung eines Angriffsschrittes für den am leichtesten durchführbaren entscheidet. Eine mathematische Ordnungsrelation über die Attributvektoren erlaubt den Vergleich der Durchführbarkeit der Teilschritte und die Bestimmung der höchsten Durchführbarkeit. In Abbildung 2 ist zu erkennen, dass die Bewertung von „Sub-step 1“ in „Attack Step“ übernommen wird, da er die höhere Durchführbarkeit im Vergleich zu „Sub-step 2“ aufweist.

Aus der Konjunktion mehrerer Teilschritte folgt die erschwerte (geringere) Durchführbarkeit des zusammengesetzten Schrittes. Die für einen erfolgreichen Angriff benötigten Ressourcen sowie das

benötigte Wissen steigen (ähnlich der arithmetischen Addition), wie in Abbildung 2 zu sehen ist. Zur Illustration werden hier über den zwischengeschalteten Und-Knoten die Attribute der Kindknoten „Sub-step 21“ und „Sub-step 22“ addiert.

Das Software-Werkzeug unterscheidet zwischen Aggregationsfunktionen und Funktionen zur Berechnung eines abgeleiteten Attributes. Aggregationsfunktionen dienen zur logischen Verknüpfung der Attributvektoren der Kindknoten zu einem Attributvektor des betrachteten Knotens. Ein abgeleitetes Attribut, wie die Durchführbarkeit, ist ein aus dem lokalen Attributvektor abgeleiteter Skalar (roter Kreis oben rechts im Knoten). Eine mitgelieferte Vorlage für die Angriffsgraphen beinhaltet bereits Vorschläge für die Umsetzung sowohl der Aggregationsfunktionen als auch der abgeleiteten Attribute. Sie sind in der Programmiersprache JavaScript implementiert und können durch die Benutzerin über einen Dialog betrachtet und modifiziert werden. Zur Abbildung eigener Risikoanalysemethoden erlaubt das Werkzeug die Definition eigener Funktionen über die vorgegebenen hinaus. Nach der Hinterlegung global pro Angriffsgraph lassen sich neu definierte Funktionen sowie bestehende für jeden Knoten individuell auswählen. Über eine Namenskonvention werden Knoten zur Dis- und Konjunktion automatisch mit den Funktionen „OR“ bzw. „AND“ belegt.

Über die Funktionen werden die Attributvektoren automatisch bis zum Angriffsschritt („Attack Step“ in Abbildung 2) vor den Knoten mit den Angriffsfolgen aggregiert (gegen die Richtung der Kanten). Beim Übergang von Angriffsschritt auf Angriffsfolge wird das Ausmaß eines Angriffes oder dessen Einfluss auf eine bestimmte Folge durch Expertinnen und Experten bewertet. Die Bewertung wird als Skalar, als Kantengewicht der Kante zwischen den beiden Knoten dargestellt, sodass die n:m-Beziehung zwischen Angriff und Schaden mit unterschiedlicher Stärke bewertet werden kann. Eine Aggregationsfunktion im Angriffsfolgeknoten nimmt pro Kindsknoten den Attributvektor sowie das Kantengewicht entgegen, verknüpft diese zum Betrag des Risikos und kann somit den Angriff mit dem höchsten Risiko für das im Knoten beschriebene Schadensereignis bestimmen. In Abbildung 2 wird dies beispielhaft mit nur einem Angriffsschritt dargestellt: Risiko = Durchführbarkeit * Schadensausmaß = 4 x 2 = 8.

Die in den Abbildungen gezeigten Werte dienen der Illustration und spiegeln keine konkrete Risikobewertung wider. Die genaue Definition und Feinjustierung der Aggregationsmethodik wird im weiteren Verlauf des Forschungsprojektes vorgenommen.

5 Gegenmaßnahmen

Die Risikoanalyse und Bewertung der Bedrohungen werden zunächst ohne Berücksichtigung der Gegenmaßnahmen durchgeführt. Grundsätzlich sollen im iterativen Prozess der Risikoanalyse jedoch bereits etablierte Gegenmaßnahmen berücksichtigt, bewertet und dargestellt werden. Die Angriffsgraphen und das Software-Werkzeug erleichtern daher auch die Erfassung der Wirkung von Gegenmaßnahmen auf Angriffsschritte. Auch hier ist eine n:m-Beziehung zwischen Angriff und Maßnahme anzunehmen, da typischerweise je nach Fallkonstellation eine einzelne Maßnahme gegen mehrere Angriffe schützen kann und umgekehrt mehrere Maßnahmen zum Schutz vor einem Angriff zur Auswahl stehen können oder erst die Kombination mehrerer Maßnahmen einen wirksamen Schutz darstellt.

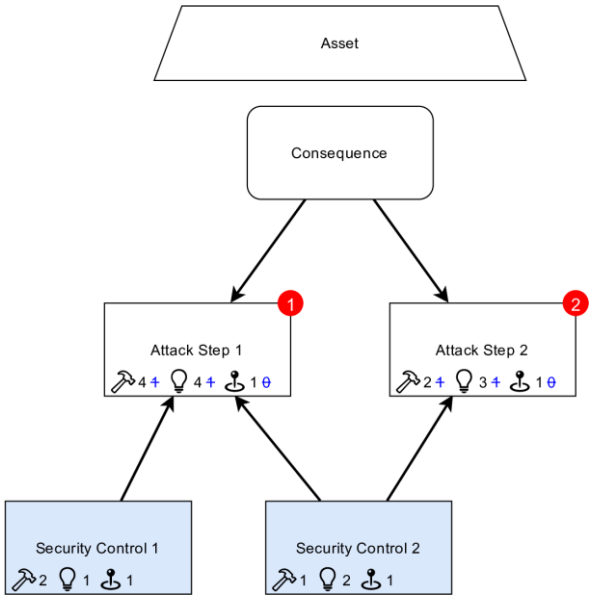

Abb. 4 Angriffsgraph stellt die Wirkung der Gegenmaßnahmen dar.

Das Beispiel in Abbildung 4 zeigt die Wirkung von zwei Gegenmaßnahmen auf zwei Angriffsschritte. Auch die Gegenmaßnahmen werden mit demselben Attributvektor bewertet und nehmen so Einfluss auf den Angriff. Die ursprüngliche Bewertung des Angriffsschrittes wird mit blauer Schriftfarbe und durchgestrichen im Knoten weiterhin dargestellt, während die schwarz gedruckten Werte auch den Einfluss der Gegenmaßnahmen enthalten und so das durch die Maßnahme reduzierte Risiko widerspiegeln. Auf „Attack Step 1“ wirken beide Gegenmaßnahmen mit im Beispiel addiertem Effekt. Auf „Attack Step 2“ hingegen wirkt nur „Security Control 2“, sodass hier bei gleicher Ausgangsbewertung, wie „Attack Step 1“ eine geringere Reduktion der Durchführbarkeit erfolgt.

6 Fazit und Ausblick

Mit dem Software-Werkzeug für Angriffsgraphen lassen sich verschiedene Risikoanalysemethoden abbilden, automatisieren und auf die Bedürfnisse und die Risikoaffinität der analysierenden Organisation abstimmen. Die Angriffsgraphen ermöglichen die explizite Zuordnung von Bedrohungen zu daraus folgenden Schäden inklusive einer Bewertung der Schadenshöhe. Durch die Verfeinerung der Bedrohungen in Angriffsschritte werden die semi-quantitative Bewertung der Eintrittswahrscheinlichkeit sowie der risikomindernde Einfluss von Gegenmaßnahmen mit denselben Attributen, wie ein Angriffsschritt, transparent und nachvollziehbar. Durch diesen Schritt wird ein harmonisiertes Risikomanagement im Unternehmen möglich. Die Semi-Quantifizierung unterstützt IT-Sicherheitsverantwortliche dabei, Maßnahmen für Fachpersonale und Management gleichermaßen nachvollziehbar in ihrer Wirkung darzustellen. Dies erhöht Verständnis, Awareness und Sicherheit in der Qualität der Einschätzung.

Das Werkzeug stellt eine JavaScript-Schnittstelle zur automatisierten Aggregation der Attribute im Angriffsgraphen bereit. Die Definition der Funktionen wird im weiteren Verlauf des Projektes „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“ vorgenommen und verfeinert. Das Werkzeug wird in diesem Forschungsprojekt dazu verwendet, eine Risikoanalyse der prognostizierten Anwendungsfälle vorzunehmen und Abuse-Cases für sie zu entwickeln und zu bewerten. Das Software-Werkzeug wurde als Plugin für die frei verfügbare Diagramm-Software

Draw.io [4] entwickelt und steht quelloffen unter der MIT Lizenz auf GitHub zum Herunterladen zur Verfügung [5].

7 Forschungsförderung

Die vorgestellte Lösung entstand im Rahmen des vom Deutschen Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt beauftragten und finanzierten Projekts „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“.

8 Literatur

[1] www.dzsf.bund.de/SharedDocs/Standardartikel/DZSF/Projekte/Projekt_49_Securitybedarf.html

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html

[3] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

[4] https://www.diagrams.net/

[5] https://github.com/incyde-gmbh/drawio-plugin-attackgraphs

Faseroptische Sensorik zur sicheren Zugortung: Fortschritte und Herausforderungen

Roman Wilhelm, Huynh Van Luong, Bernd Drapp[1]

[1] *AP Sensing GmbH, Herrenbergerstraße 130, 71034 Böblingen*

1 Einleitung

Der ,,Green Deal“ – eine klimaneutrale Europäische Union bis 2050 – ist ein Markenzeichen der EU-Kommission. In Europa sollen die Unternehmen und die Menschen verstärkt die Bahn als nachhaltiges Verkehrsmittel nutzen. Ein höherer Anteil von Fahrzeugen auf der Schiene bedeutet eine höhere Verkehrsdichte. Die soll unter anderem durch die Digitalisierung der Leit- und Steuerungstechnik und den „moving block“ - das Fahren im variablen Raumabstand - erreicht werden. Das European Train Control System (ETCS) unterstützt den ,,moving block“ auf ETCS Level 3, benötigt dafür aber regelmäßige Informationen bezüglich der Zugintegrität und der sicheren Zuglänge, um Folgeabschnitte freigeben zu können (ETCS-Spezifikation, S.41).

Fiberoptische Sensorik (FOS) ist ein Messprinzip, bei dem eine handelsübliche Glasfaser – wie sie an den meisten deutschen Bahnstrecken bereits zur internen Kommunikation verlegt ist – in eine Kette von akustischen Sensoren verwandelt wird. Dabei wird ein Laserimpuls in die Glasfaser gesendet und die sogenannte Rayleigh-Rückstreuung des Lichts an kleinen Inhomogenitäten der Faser gemessen. Wirken akustische Schwingungen auf die Faser ein – zum Beispiel durch vorbeifahrende Züge verursacht - verändert sich die gemessene Rückstreuung. Dadurch lassen sich akustische Ereignisse entlang der Faser in Echtzeit lokalisieren und durch Methoden der Mustererkennung dann ihrem Ursprung nach klassifizieren.

Entgegen anderen infrastrukturseitigen Lokalisierungsmethoden (wie zum Beispiel Balisen) zeichnet FOS die räumliche (Quasi-)Kontinuität aus: Die Messpunkte sind je nach Konfiguration alle 2,5 bis 10 Meter entlang der Strecke. Im Gegensatz zu den fahrzeugseitigen Lokalisierungsmethoden (zum Beispiel GPS oder Kamera) ist FOS unabhängig von externen Faktoren wie Satellitenverbindung oder Lichtverhältnissen.

Vergangene Untersuchungen bezüglich FOS im Bahnbetrieb haben bereits die prinzipielle Tauglichkeit der Technologie demonstriert. Eine der ersten Arbeiten stammt dabei von Timofeev et al. (2015), in der basierend auf der Energie des FOS-Signals eine Genauigkeit der Positionsangabe von 15 Metern erreicht wurde. Peng et al. (2016) haben einen Algorithmus vorgestellt, der auf verschiedenen akustischen Frequenzbändern des FOS-Signals operiert, allerdings war dieser mit einer Latenz von 5 Sekunden nicht echtzeit-tauglich. Später wurde dies in Wiesmeyr et al. (2020) anhand einer ,,Support Vector Machine“ verbessert und mit einer Latenz von einer Sekunde eine Genauigkeit im Rahmen der vorhandenen ,,ground-truth“ von 40 Metern erreicht. Die Untersuchung Robl et al. (2020) hat basierend auf einem fix gewählten Frequenzbereich eine Genauigkeit im Bereich von unter 10 Meter (Robl et al., S.111f) ergeben.

[1] Korrespondierender Autor: roman.wilhelm@apsensing.com

Allen bisherigen Ansätzen gemeinsam ist, dass Signale von benachbarten Orten an der Faser unabhängig voneinander klassifiziert werden. Damit werden allerdings nützliche Korrelationen ignoriert, da bei einem vorbeifahrenden Zug mehrere benachbarte Orte den Zug gleichzeitig messen und mit dieser zusätzlichen Information eine robustere Klassifikation möglich ist. Aus dieser Überlegung heraus basiert unser Ansatz auf zeitlich-räumlichen Eingabedaten, aus denen ein neuronales Netz dann Muster über einen größeren räumlichen und zeitlichen Kontext erlernen kann.

Im Folgenden fassen wir Fortschritte und Erkenntnisse aus dem Forschungsprojekt ,,Fossil 4.0"[2] an einer 35 Kilometer langen Strecke im Raum Berlin über einen Zeitraum von mehr als einem Jahr zusammen und stellen exemplarisch drei Herausforderungen für FOS und unsere Lösung dazu vor:

1. Da der akustische Sensor alle akustischen Ereignisse entlang der Faser misst, ist eine zentrale Herausforderung bei der robusten Ortung von Zügen die Unterscheidung zwischen Zugsignal und Störsignal. Wir zeigen, dass sich die verschiedenen Signale anhand ihrer räumlichen und spektralen Eigenschaften auch in Echtzeit (Latenz: 0,5 Sekunden) unterscheiden lassen.
2. Wie bereits frühere Untersuchungen gezeigt haben, ist die Detektion der Züge bei sehr niedriger Geschwindigkeit aufgrund der veränderten Signalcharakteristik herausfordernd (Robl et al. 2020, S. 8). Mit modernen Methoden der Mustererkennung (,,Deep Learning") und einem hinreichend großen Trainingsdatensatz konnten wir die kritische Geschwindigkeit, ab der Züge nicht mehr sicher erkannt werden, auf bis zu 5 km/h senken.
3. Aus Sicht der sicheren Zug-Ortung stellt sich der Kreuzungspunkt mehrerer Züge als besondere Situation für FOS dar, da hier eine Signalüberlagerung der involvierten Züge stattfindet. Durch eine spezielle Logik konnten wir die kritische Zeit, in der die kreuzenden Züge nicht sicher geortet werden können, je nach Szenario um bis zu 100% reduzieren.

2 Methodik

Im Folgenden soll die FOS-Technologie und der entwickelte Algorithmus zur Zugortung kurz vorgestellt werden.

2.1 FOS-Daten und Signalvorverarbeitung

Im Rahmen der Untersuchung wurde ein faseroptisches Messgerät der Firma AP Sensing an einer 35 Kilometer langen Strecke im Großraum Berlin installiert. Bei einem räumlichen Messintervall von 2,5 Metern korrespondieren damit 14000 virtuelle ,,Mikrofone" (im Folgenden Channel genannt) zu der gesamten Strecke.

Durch das Senden von Lichtimpulsen in die Faser und das Messen der Rayleigh-Rückstreuung können selbst kleinste physikalische Einwirkungen auf die Faser gemessen werden und dann über eine Laufzeitmessung dem entsprechenden Channel zugewiesen werden. In dieser Weise liefert der akustische Sensor 2000 Mal pro Sekunde ein Datenarray mit 14000 Einträgen. Die resultierenden

[2] ,,Faseroptische Sensorik für sicherheitsrelevante Bahnanwendungen", mehr Informationen dazu unter https://www.bmvi.de/SharedDocs/DE/Artikel/DG/mfund-projekte/fossil-4_0.html

Daten über einen Zeitraum von 100 Sekunden und eine Strecke von zwei Kilometern sind in Abb. 1 (links) visualisiert.

Um eine maschinelle Datenverarbeitung in Echtzeit zu ermöglichen, werden diese hochdimensionalen Daten dann mit einer Fourier-Transformation in den Frequenzraum überführt und die Energie des Signals in verschiedenen Frequenzbändern bestimmt. Das Resultat ist für jeden Channel der zeitliche Verlauf der akustischen Energie in einem bestimmten Frequenzbereich; also pro Frequenzband eine Matrix, in der die Spalten den Channeln entsprechen und die Zeilen den Zeitschritten (vgl. Abb. 1, rechts).

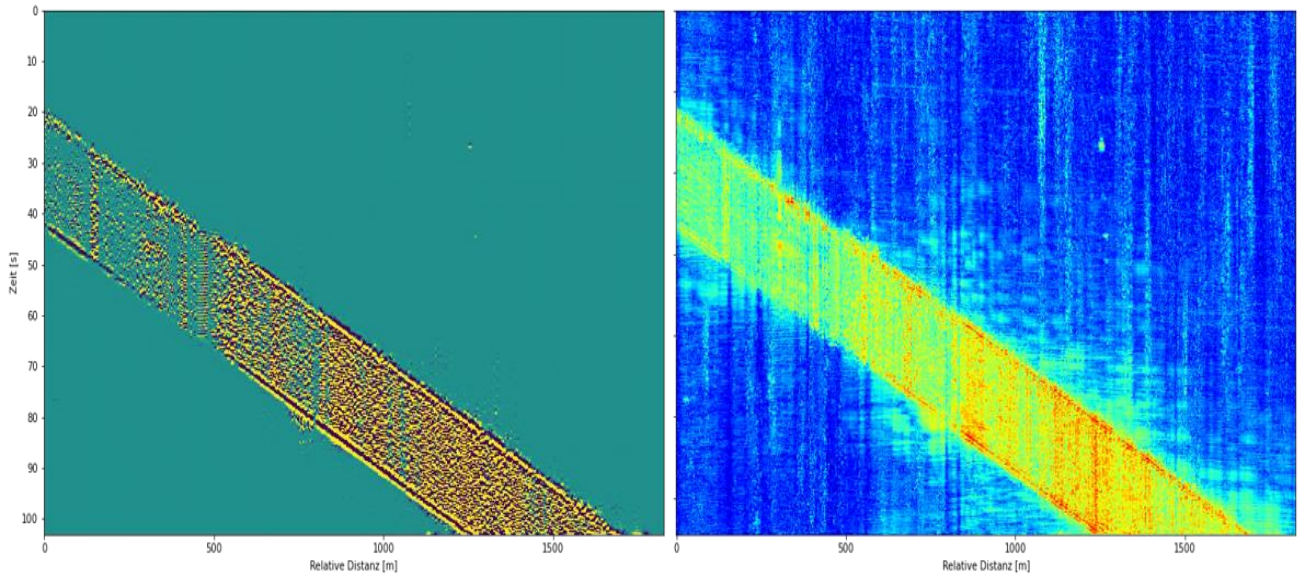

Abb. 1 Phase der Rayleigh-Rückstreuung (links) und transformiertes Signal im Frequenzband 20 Hz – 50 Hz (rechts).

2.2 Zug-Erkennung und -Verfolgung

Betrachtet man mehrere solcher Frequenzbänder gleichzeitig, so ergibt sich eine dreidimensionale Struktur mit den Dimensionen Zeit, Raum und Frequenzbereich. Diese 3D-Struktur ist analog zu einem RGB-Bild mit den Dimensionen Höhe, Breite und Farbkanal, kann also dementsprechend als Eingabe für Algorithmen der maschinellen Bildverarbeitung (zum Beispiel Deep Learning) genutzt werden.

Für die Zugerkennung in Echtzeit wurde ein spezielles ,,Convolutional Neural Network“ (CNN), welches in der Bildverarbeitung neue Maßstäbe gesetzt hat (He et al. 2016, S. 775f), angepasst und das modifizierte Modell dann auf einem manuell annotierten Datensatz trainiert. Das finale Modell ist in der Lage, für jeden Zeitschritt und jeden Channel auszugeben, ob ein Zug vorbeifährt oder nicht (vgl. Abb. 2). Zusätzlich können über dieses Ausgabeformat auch implizit Anfang und Ende aller Züge pro Zeitschritt ausgelesen werden.

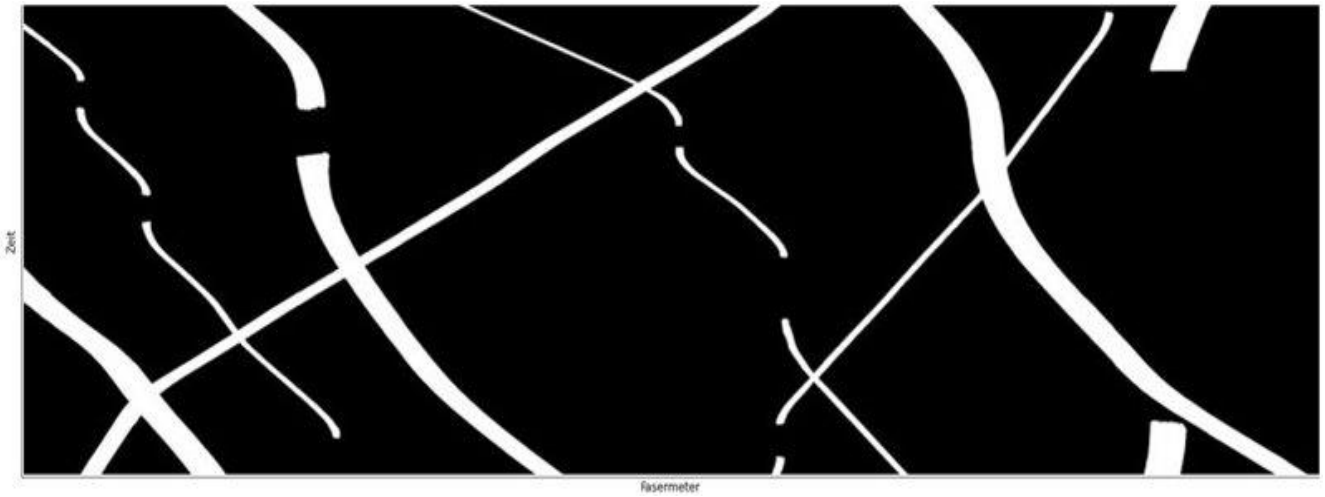

Abb. 2 Kumulierte Ausgabe des neuronalen Netzes über einen Zeitraum von 10 Minuten. Die weißen Regionen kennzeichnen die erkannten Zugsignale.

Um den erkannten Zügen eine Identität zuordnen zu können und damit Aussagen über den Zeitverlauf treffen zu können („Hat der Zug noch die gleiche Länge?") werden die in jedem Zeitschritt erkannten Züge über eine Assoziationslogik verknüpft und der zeitliche Verlauf eines jeden Zuges mit einem Kalman-Filter geglättet.

Die Ausgabe ist eine eindeutige Zugidentität und für jeden Zeitschritt die Zugparameter Ort, Geschwindigkeit, Länge und Integrität (vgl. Abb. 3)

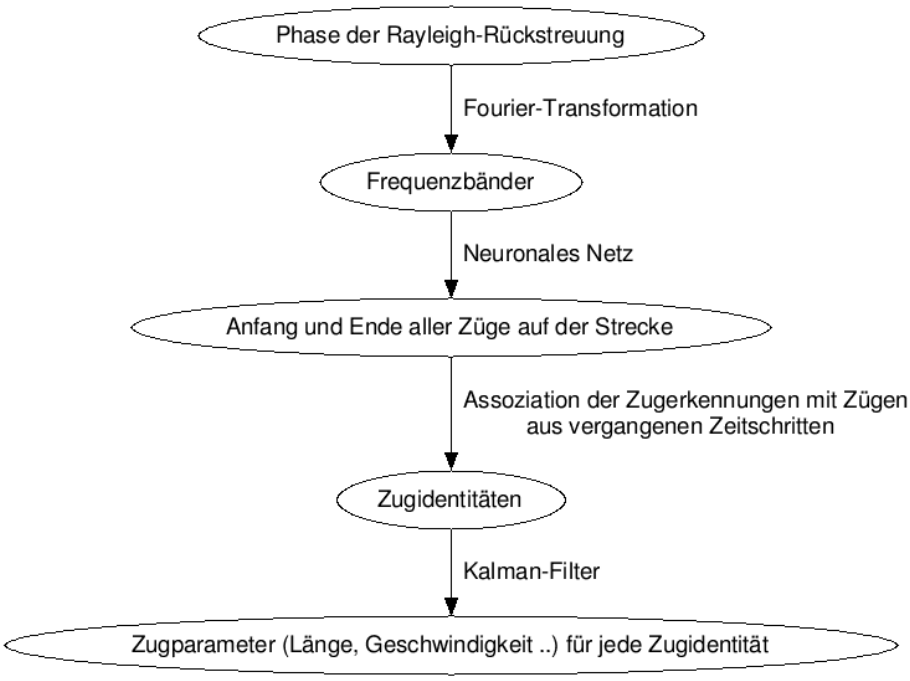

Abb. 3 Flussdiagramm des Algorithmus für einen Zeitschritt.

3 Ergebnisse

Im Folgenden werden drei Szenarien vorgestellt die sich in unseren Untersuchungen als herausfordernd für die FOS-Technologie erwiesen haben und entsprechende Lösungswege aufgezeigt.

3.1 Signalklassifizierung

Da der FOS-Sensor alle akustischen Ereignisse entlang der Strecke aufnimmt, ist es für die robuste Ermittlung der Zuglänge besonders wichtig das Zugsignal von Störgeräuschen - wie zum Beispiel durch Industrieanlagen und Verkehr verursacht - zu unterscheiden.

Vergangene Untersuchungen (Robl et al. 2020, S. 77ff) haben bereits gezeigt, dass dies im Frequenzraum gut möglich ist, da gängige Störgeräusche aus der Gleisumgebung oft auf einen bestimmten Frequenzbereich beschränkt sind, während das Zugsignal im Allgemeinen in allen Frequenzbändern eine erhöhte Intensität aufweist.

Dies ist beispielhaft in der Abb. 4a dargestellt, die ein komplexes Szenario in Bahnhofsnähe zeigt. Das stationäre Störgeräusch bei ca. 600 Metern ist eine Autobahn, die unter dem Gleis kreuzt. Das Muster im Bereich zwischen 1200 Meter und 2200 Meter stammt von mehreren Lastkraftwagen, die in diesem Streckenabschnitt in wenigen Metern Entfernung zum Gleis verkehren. Im Frequenzband von 20 Hz bis 50 Hz sind die verschiedenen Signale nur schwer zu unterscheiden und es kommt folglich zu Fehlklassifikationen.

In der Abb. 4b ist die gleiche Situation im Frequenzband von 100 Hz bis 1000 Hz dargestellt. Man erkennt, dass das stationäre Störgeräusch der Autobahn vollkommen verschwunden ist und das Signal der Lastkraftwagen deutlich abgeschwächt ist. Die Information aus beiden Frequenzbändern zusammen erlaubt also eine robustere Klassifikation der Signale und verdeutlicht die Wichtigkeit von multispektralen Eingabedaten für die Mustererkennung. Die resultierende Klassifikation des neuronalen Netzes ist in der Abb. 4c zu sehen.

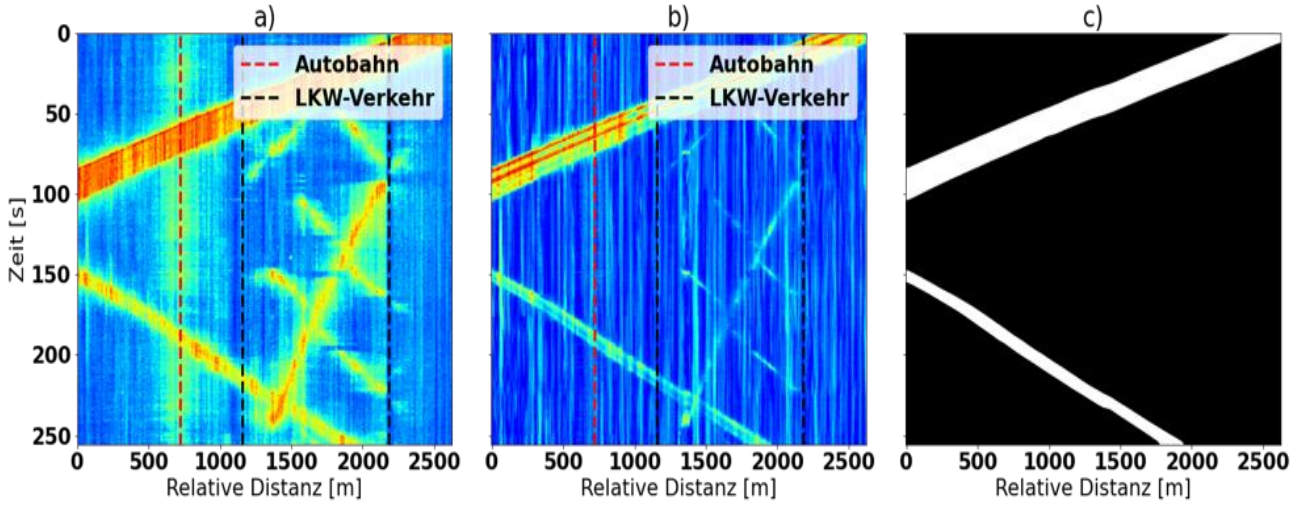

Abb. 4 Gleisabschnitt mit hohem Rauschen. (a) Im Frequenzband 20 Hz - 50 Hz. (b) Im Frequenzband 100 Hz - 1000 Hz. (c) Klassifizierung des neuronalen Netzes.

3.2 Niedrige Geschwindigkeit

Vergangene Studien zu FOS im Bahnbetrieb hatten Schwierigkeiten bei der sicheren Detektion von Zügen mit niedriger Geschwindigkeit festgestellt (Robl et al. 2020, S. 8). Dies folgt aus der dann schwächeren akustischen Energie des Zuges und der damit einhergehend schwächeren Einwirkungen auf die Sensorfaser.

Die Analyse zeigt, dass diese Signalabschwächung nicht in allen Frequenzbereichen gleich ausgeprägt ist. Wie in Abb. 5 zu sehen ist, unterscheiden sich die verschiedenen Frequenzbänder bei niedrigen Geschwindigkeiten in ihrer Signalstabilität. Um auch bei niedrigen Geschwindigkeiten eine robuste Detektion zu erreichen, werden die Informationen aus dem gesamten Frequenzspektrum kombiniert. Bei einer einfachen Addition über alle Frequenzbereiche würden allerdings auch die Rauschanteile aus allen Frequenzbereichen akkumuliert (vgl. Abschnitt 3.1).

Eine Lösung besteht darin, die verwendeten Frequenzbereiche durch das trainierte neuronale Netz adaptiv wählen zu lassen, um so bestimmte Frequenzbänder hervorzuheben oder abschwächen. Ein ähnliches Verfahren wurde bereits zur natürlichen Sprachverarbeitung erfolgreich eingesetzt (Vasvani et al. 2017). Mit diesem Ansatz ist es gelungen, Züge mit Geschwindigkeiten bis zu 5 km/h stabil zu verfolgen (vgl. Abb. 5c).

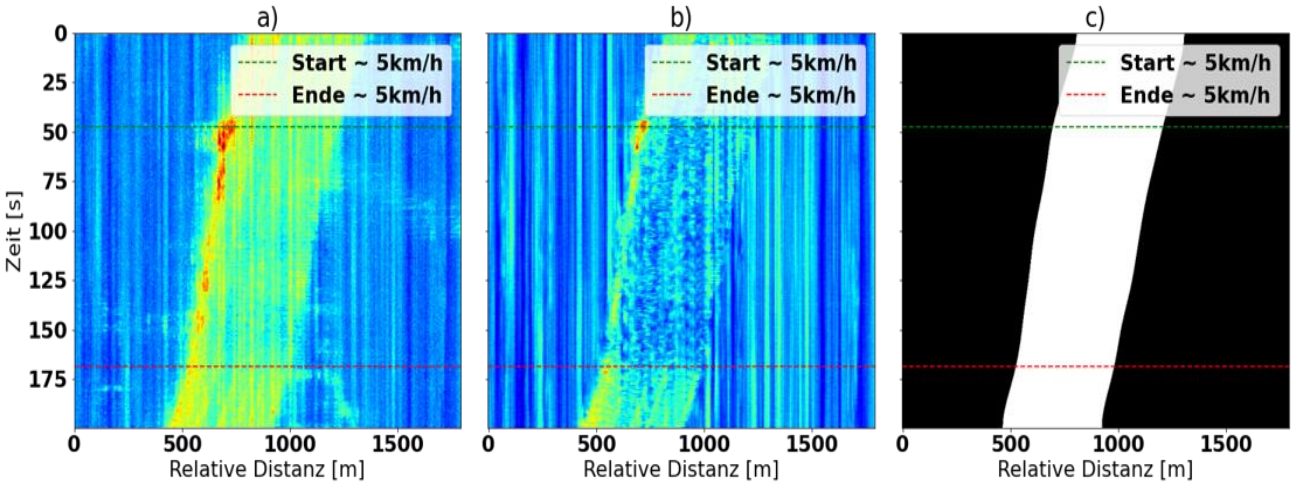

Abb. 5 Zug mit niedriger Geschwindigkeit. (a) Im Frequenzband 50 Hz – 100 Hz. (b) Im Frequenzband 100 Hz – 1000 Hz. (c) Zugerkennung des neuronalen Netzes. Die horizontalen Markierungen kennzeichnen den Abschnitt mit einer Durchschnittsgeschwindigkeit von 5km/h.

3.3 Zugkreuzungen

Aus Sicht der FOS-Technologie stellen Zugkreuzungen eine Herausforderung dar, da zumeist nur eine Glasfaser verfügbar ist und demzufolge während der Kreuzung das Zugsignal des weiter von der Faser entfernten Zuges von dem näheren Zug überlagert wird (vgl. Abb. 6a).

Die Extrapolation der Zugposition über den Zeitraum der Kreuzung hinweg hat sich in unseren Untersuchungen als fehleranfällig herausgestellt, da bei bestimmten, extremen Konstellationen (kreuzende Güterzüge mit niedriger Geschwindigkeit oder Beschleunigungs- beziehungsweise Bremsvorgänge während der Kreuzung) der Fehler in der Extrapolation signifikant werden kann:

Die Abb. 6b zeigt einen langsamen Güterzug mit einer Beschleunigung während der Zugkreuzung. Die Zugsignale überlagern sich zum Zeitpunkt t = 55 Sekunden und trennen sich erst wieder zum Zeitpunkt t = 125 Sekunden. Die Extrapolation über 70 Sekunden ergibt für die Positionsangabe einem maximalen Fehler von 250 Meter.

Eine mögliche Lösung nutzt den Umstand, dass zu Beginn des Kreuzungsvorgangs zumindest das Ende der jeweiligen Züge ohne Signalüberlagerung erkennbar ist (solange bis das Ende des einen Zuges den Anfang des anderen Zuges passiert), und dann später (nachdem der Anfang des einen Zuges das Ende des anderen Zuges passiert hat) der Anfang ohne Signalüberlagerung erkennbar ist.

Dies ist in Abb. 6c visualisiert: Man erkennt, dass zum Zeitpunkt bei t = 55 Sekunden der Anfang des ersten Zuges (rot markiert) vom zweiten Zug überlagert wird. Das Ende des ersten Zuges (blau markiert) ist allerdings noch bis t = 98 Sekunden sichtbar. Zum Zeitpunkt t=101 Sekunden ist dann der Anfang des ersten Zuges bereits wieder sichtbar. Die kritische Zeitspanne, in der extrapoliert werden muss, wurde in diesem Szenario damit von 70 Sekunden auf 3 Sekunden gesenkt (im Allgemeinen hängt sie von dem relativen Längenunterschied und der Geschwindigkeit der beteiligten Züge ab). Eine analoge Logik ist auf den zweiten Zug anwendbar.

Indem unabhängig voneinander Anfang und Ende der Züge detektiert werden, können also auch während einer Kreuzung Informationen über Geschwindigkeit und Position der beteiligten Züge erlangt werden.

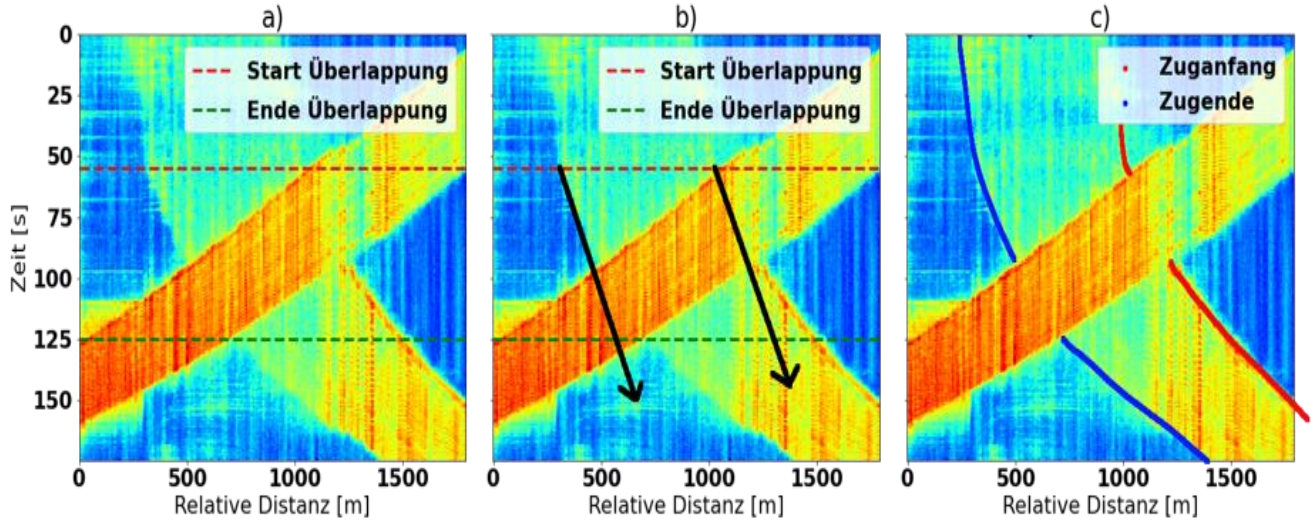

Abb. 6 (a) Zugkreuzung. (b) Extrapolation der Zugposition. (c) Lokalisierbarer Zuganfang bzw. -ende während der Kreuzung.

Diskussion

Es wurde ein Echtzeit-Algorithmus zur Zugortung basierend auf fiberoptischen Messdaten präsentiert. Der Algorithmus besteht aus den drei Teilschritten:

1. Der Vorverarbeitung der FOS-Daten zur Dimensionsreduktion und Erhöhung des Signal-Rausch-Verhältnisses.
2. Dem Erkennen der Züge ausgehend von den vorverarbeiteten Daten und dem Ausnutzen des zeitlichen und räumlichen Kontextes in den Eingangsdaten durch ein neuronales Netz (CNN).

3. Dem Herstellen von Zugidentitäten über die Zeit um Merkmale wie Geschwindigkeit, Beschleunigung und Zugintegrität aufstellen zu können.

Dabei wurde in allen Teilschritten auf eine effiziente Datenverarbeitung geachtet um den Echtzeit-Anforderungen gerecht zu werden. Konkret arbeitet der Algorithmus mit einer Latenz von 0,5 Sekunden und einem Abtastintervall von 0,25 Sekunden.

Während für nicht-sicherheitsrelevante Anwendungsfälle die Güte eines Algorithmus von der durchschnittlichen Leistung bestimmt wird, ist für sicherheitsrelevante Anwendungen insbesondere das Verhalten in seltenen beziehungsweise schwierigen Situationen relevant. Ausgehend von Messdaten, die an einer Strecke mit Personen- und Güterverkehr über ein Jahr hinweg erhoben wurden, sind drei, für eine automatische Auswertung schwierige, Situationen vorgestellt und entsprechende Lösungen präsentiert worden.

Es wurde gezeigt, dass multispektrale Informationen hilfreich für die robuste Zugverfolgung sind, da sie eine genauere Klassifikation der gemessenen akustischen Ereignisse erlauben. Die verschiedenen Frequenzbereiche besitzen außerdem komplementäre Eigenschaften bezüglich des Einflusses von Störgeräuschen und der Detektion von Zügen auch bei sehr niedriger Geschwindigkeit.

Des Weiteren wurde aufgezeigt, wie durch eine verbesserte Logik das Orten der Züge während Zugkreuzungen deutlich verbessert werden kann.

Die Kombination aus zeitlich und räumlicher Kontinuität der FOS-Technologie und der Unabhängigkeit von externen Einflussfaktoren wie Wetter oder Radio-Empfang prädestiniert FOS als zusätzliche Daten-Quelle zur Herstellung von Redundanz in der sicheren Zugortung und kann damit einen Beitrag zum „Betrieblichen Zielbildes 2.0“ der Deutschen Bahn leisten, welches ETCS Level 3 im Jahre 2035 vorsieht (Kopitzki et al. 2021, Seite 37).

4 Literaturverzeichnis

[1] ETCS-Spezifikation, Subset-026-3, Version 3.4.0 [online]. Available at: https://www.era.europa.eu/content/ccs-tsi-annex-mandatory-specifications (Accessed: 4. April 2022)

[2] Timofeev, A.V.; Egorov, D.V.; Denisov, V.M. TIMOFEEV, Andrey V.; EGOROV, Dmitry V.; DENISOV, Viktor M.: The rail traffic management with usage of C-OTDR monitoring systems. In: International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2015, 9. Jg., S. 1492-1495.

[3] Papp, Adam; Wiesmeyr, Christoph; Litzenberger, Martin; Garn, Heinrich; Kropatsch, Walter: Train Detection and Tracking in Optical Time Domain Reflectometry (OTDR) Signals. In: Rosenhahn, B., Andres, B. (eds) Pattern Recognition. GCPR 2016. Lecture Notes in Computer Science, vol 9796. Springer.

[4] Wiesmeyr, Christoph; Litzenberger, Martin; Waser, Markus; Papp, Adam; Garn, Heinrich, Neunteufel, Günther: Real-Time Tracking from Distributed Acoustic Sensing Data, Applied Sciences, 10(2) [online]. Available at: https://www.mdpi.com/2076-3417/10/2/448/htm (Accessed: 4. April 2022)

[5] Robl, Christian; Rubino, Eduardo; Capriotti, Daniele; Burschka, Darius; Pavlic, Marko; Rettinger, Angelika; Murray, Alasdair; Hall, Andrew; Molloy, Kevin; Jöckel, Lothar; Hofstetter, Albert; Brand, Alex; Ackermann, Urs; Ohrendorf-Weiss, Sebastian; Düsel; Thomas: smartrail 4.0: Technology Report PoC GLAT – Video/FOS [online]. Available at: www.voev.ch/de/Service/content_?download=18076 (Accessed: 4. April 2022)

[6] He, Kaiming; Zhang, Xiangyu; Ren, Shaoqing; Sun, Jian: Deep residual learning for image recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition. 2016. S. 770-778.

[7] Vaswani, Ashish; Shazeer, Noam; Parmar, Niki; Uszkoreit, Jakob; Jones, Llion; Gomez, Aidan N; Kaiser, Łukasz; Polosukhin, Illia: Attention is all you need. In: Advances in Neural Information Processing Systems, 2017, S. 5998—6008.

[8] Kopitzki, Matthias; Braun, Wolfgang; Post, Sebastian: Betriebliches Zielbild für den digitalen Bahnbetrieb [online]. Available at:

[9] https://www.ews.tu-berlin.de/fileadmin/fg98/aushaenge/2021-wise/2021-11-15_EWS_Kopitzki_Braun_Post_DB_Netz_Zielbild_digitaler_Bahnbetrieb.pdf (Accessed: 4. April 2022)

BIM in der LST Planung

Volker Uminski

WSP Infrastructure Engineering GmbH

1 Einleitung

„Mehr Schiene – mehr Klimaschutz“ ist im Grunde eine einfache und erfolgreiche Gleichung. Sie setzt insbesondere voraus, dass die Planungs- und Realisierungsprozesse von eisenbahnbezogenen Infrastrukturprojekten möglichst effektiv und effizient sind, um den aktuell hohen Investitionsbedarf zeitnah zu decken. Deshalb setzt die Deutsche Bahn (DB) verstärkt auf neue Technologien im Kontext BIM und will damit eine „durchgehende digitale Datenhaltung“ in allen Projektphasen erreichen (Abbildung 1). Dabei ist die Aufgabe von standardisierten Datenströmen alle beteiligten Softwaresysteme zu vernetzen und das projektspezifische 3D-Koordinationsmodell, den sogenannten „Digitalen Zwilling“, mit den relevanten Fachobjekten aller Gewerke zu versorgen.

Die vorliegende Ausarbeitung wirft einen Blick auf die vorgenannten Aspekte aus Sicht der Leit- und Sicherungstechnik (LST) für elektronische und digitale Stellwerke (ESTW, DSTW).

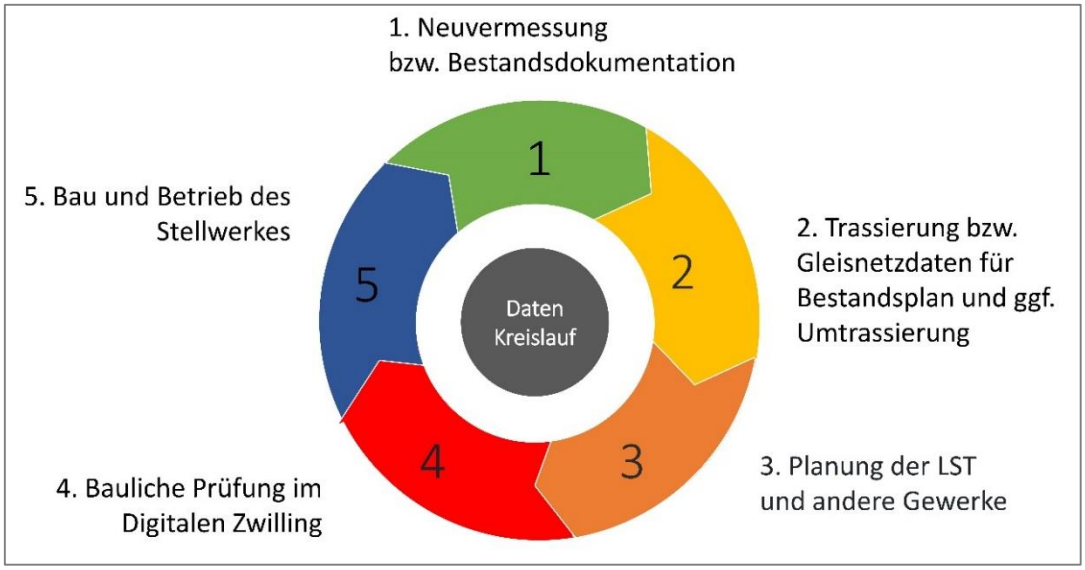

Abb. 1 Datenkreislauf in den Infrastrukturprojekten der DB. [1]

2 Grundlegende BIM-Anforderungen

Ungeachtet in welcher Industrie die Methode „BIM“ zum Einsatz kommt, gibt es mindestens die drei folgenden Anforderungen und deren wirkungsvollste Hebel:

- Durchgehender Datenstrom (Dataflow) durch standardisierte Datenschnittstellen.

- Reibungsloser Arbeitsablauf (Workflow) durch standardisierte Planungsprozesse in den Gewerken.
- Transparente Kollaboration durch standardisierte Koordinationsprozesse aller Gewerke anhand eines 3D-Koordinationsmodells (Digitaler Zwilling bzw. Digital Twin).

2.1 Durchgehender Datenstrom

Wie bei jeder IT-getriebenen Technologie, so sind auch bei BIM die digitalen Informationsströme das zentrale Medium, das die beteiligten Mensch-Maschine-Systeme miteinander vernetzt.

In dieser Vernetzung liegt das Hauptpotenzial von BIM: zeitlich und fachlich relevante Informationen über alle Anforderungen und Einflussgrößen für die Beteiligten und die Anspruchsgruppen eines Projektes (Stakeholder) zu erzeugen und bereitzustellen. Idealtypisch lassen sich Projektziele auf diese Weise effektiver und effizienter erreichen, insbesondere, weil Fehler und Irrtümer schon früh erkannt werden und somit die bauliche Umsetzung optimal vorbereitet und gesteuert werden kann.

Am Anfang dieses Mehrwertes stehen immer Informationspakete in digitaler Form, die als Datensatz erzeugt und dann als Datenstrom auf die Reise durch die Systemlandschaft eines Projektes geschickt werden. Der Datensatz ist dabei wohldefiniert, damit er von allen beteiligten Systemen in derselben Weise erkannt, interpretiert und weiterverarbeitet werden kann.

Hierfür wurde im Bereich der LST-Planung das Datenformat „PlanPro“ entwickelt, das alle relevanten Objekte und deren Eigenschaften detailliert erfasst und beschreibt.

Das PlanPro-Objektmodell wurde und wird bei der DB Netz in Zusammenarbeit mit Richtlinienautoren, Prüfern, Planern, Zeichnern, Signalbaufirmen und Softwareherstellern bereits seit 2008 entwickelt und erfährt fortlaufend Anpassungen für aktuelle Anforderungen aus der Praxis; so auch in der letzten Zeit im Kontext ETCS, DSTW/Verkabelung und aktuell zu BIM.

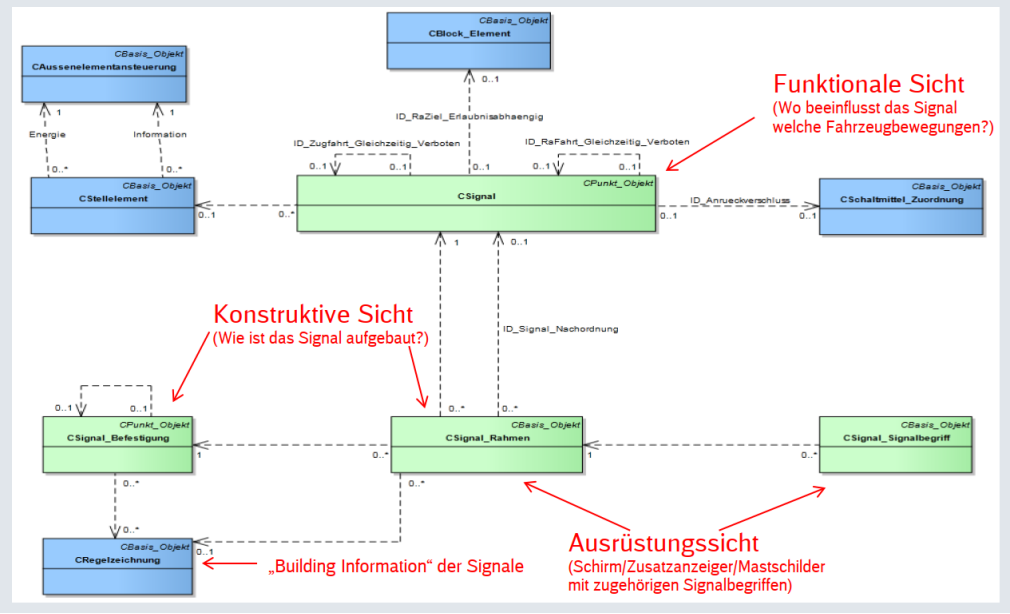

Abb. 2 Verschiedene Sichten auf das PlanPro-Objektmodell am Beispiel des Signals. [2]

Um das Datenmodell für alle relevanten Planung- und Realisierungsprozesse zu ertüchtigen, muss es auch verschiedene Sichten auf die Daten zulassen. Am Beispiel des Signals (Abbildung 2) kann man den Zusammenhang zwischen funktionaler, konstruktiver, ausrüstungstechnischer und baulicher Sicht

erkennen. Diese z.T. sehr komplexen Zusammenhänge müssen nun in Softwaresystemen wie ProSig (Kapitel 2.2) derart abgebildet werden, dass die Nutzer in der Lage sind, eben diese komplexen Informationen bzw. Daten in das System möglichst effizient und komfortabel einbringen zu können.

2.2 Reibungsloser Arbeitsablauf

Der optimale Arbeitsablauf ist etwas, nach dem in jeder Produktion und in jedem Projekt kontinuierlich gesucht und gerungen wird. BIM kann dafür zwar kein fachspezifisches Patentrezept liefern, wohl aber einen schlüssigen Handlungsrahmen, der insbesondere auf ein optimales Miteinander innerhalb von Werkschöpfungssystemen setzt. Tatsächlich meint „reibungsloser Arbeitsablauf“ in diesem Kontext „ohne überflüssige oder redundante Tätigkeiten“, jedoch nicht unbedingt „fehler- oder problemfrei“. Eine „offene Fehlerkultur“ ist sogar elementarer Bestandteil einer transparenten Kommunikation bzw. Kollaboration (Kapitel 2.3).

Ein hierfür entscheidender Hebel im Bereich der LST sind standardisierte Planungsprozesse, die bereits in der Entwurfsplanung der Stellwerke bzw. Bahnhöfe zum Einsatz kommen und dessen Ergebnisse in der Ausführungsplanung medienbruchfrei weiter detailliert werden, um sie schließlich über die PlanPro-Datenschnittstelle in Format XML und IFC in Richtung 3D-Koordinationsmodell ausleiten zu können.

Die Planungssoftware ProSig ist seit 1998 als Standardsoftware im Bereich der LST-Planung im landesweiten Einsatz und hat zusammen mit der Entwicklung des o.g. PlanPro-Objektmodells die dafür notwendigen Erweiterungen erfahren, sodass alle LST-relevanten Fachdaten mit weitreichend standardisierten und automatisierten Planungsprozessen erzeugt, validiert, geändert und weitergegeben werden können.

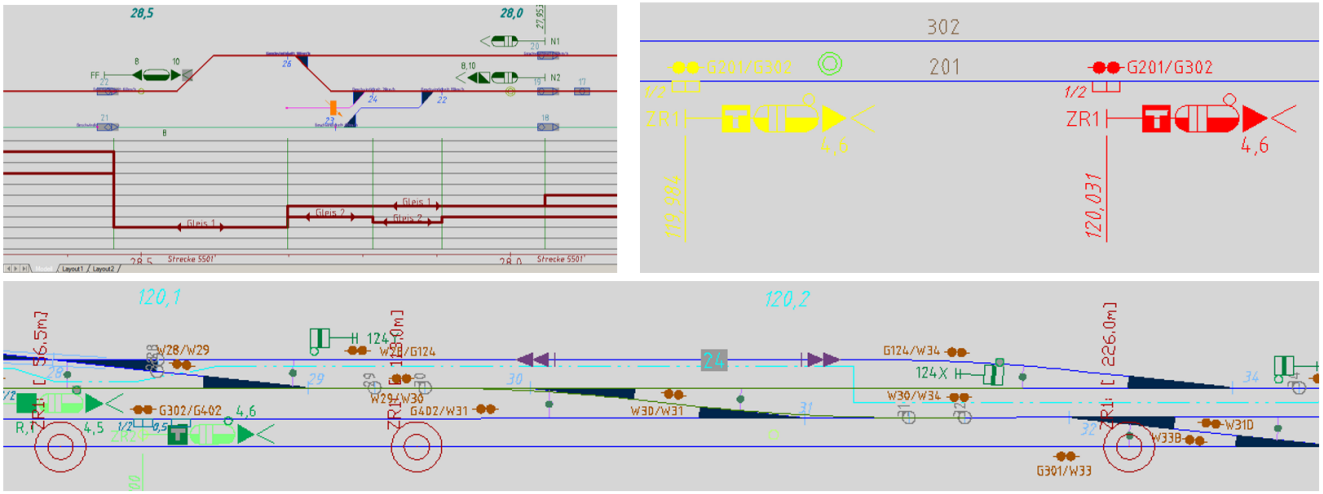

Abb. 3 Beispiele für automatisierte Planungsunterstützung in ProSig: ETCS L2 Geschwindigkeitsband, Bauzustandsplanung und neigungsabhängige Standortermittlung. [3]

Somit steht passend zum verstärkten Ausrollen von BIM-Anforderungen in den ESTW/DSTW-Projekten bei der DB ein zentrales Werkzeug in der LST Planungslandschaft zu Verfügung, dass die Anwender mithilfe von datenbasierten Algorithmen bei Analysen, Berechnungen, Entscheidungen und Planerstellung unterstützt (siehe Beispiele in Abbildung 3).

Für die „Nachbargewerke“ der LST sind entsprechend standardisierte Planungsprozesse und BIM-konforme Datenschnittstellen vorzusehen, um für die gewerkeübergreifenden Kollaborationsprozesse

(Kapitel 2.3) eine gemeinsame Datenbasis zu schaffen; insbesondere über die projektspezifischen Grundlagen wie Trassierung, Gleislage, Gelände, Umgebung, und Bestandsobjekte.

2.3 Transparente Kollaboration

In den vorangegangenen Kapiteln ging es insbesondere um die Voraussetzungen optimaler Kommunikations- und Arbeitsprozesse innerhalb der Gewerke am Beispiel der LST. Nun wird eine größere „Umlaufbahn“ angesteuert, um das Zusammenspiel der an einem Infrastrukturprojekt beteiligten Gewerke zu realisieren. Da dies naturgemäß sehr viele sein können (siehe Abbildung 4), steigt die Komplexität der Koordination entsprechend stark an, auch weil diese Abstimmungen regelmäßig über die Grenzen der beteiligten Unternehmen hinaus erfolgen müssen.

Zu den gewerkeübergreifenden Datenschnittstellen und klar definierten Arbeitsprozessen kommt nun noch die explizite Forderung nach „Transparenter Kommunikation“ hinzu. Der Grund dafür liegt in der (bisherigen) Markt- und Unternehmenskultur, das Knowhow und die Leistungen gegenüber Dritten zu schützten und den eigenen Vorsprung auszubauen. Das führt zu einem sehr vorsichtigen und gleichsam verschlossenen Miteinander in den Projekten, das schon in der Ausschreibungsphase beginnt und sich meist bis zur finalen Auslieferung durchzieht.

Genau das kann und will BIM überwinden, um sein Potential maximal auszuschöpfen; hier nur zwei Beispiele aus dem Kontext LST:

- Es ist sinnvoll schon in frühen Planungsphasen eine große Datentiefe und somit einen hohen Informationsgehalt in den Plänen bzw. in den entsprechenden Softwaredateien zu generieren und an die Bearbeiter der Folgephasen weiterzugeben. Wird diese Leistung aber nicht dezidiert gefordert bzw. entlohnt, was nach HOAI oft der Fall ist, so wird schlimmstenfalls nur Papier oder eine entsprechende PDF weitergegeben. Damit bleibt das Wissen in den Dateien ungenutzt und muss mehrfach bzw. erneut generiert werden. BIM ermöglicht und erfordert hierfür eine kollaborative Mentalität aller Beteiligten, um den Wissensverlust an Firmen- und Mediengrenzen zu vermeiden.
- Fehler, Irrtümer, unvorhergesehene Probleme und Verzögerungen sind täglicher Bestandteil menschlichen Handelns und jedweder Kommunikation in gemeinsamen Projekten. Dennoch wird aus Angst vor unangenehmen Konsequenzen „traditionell“ mehr Aufwand auf Beschwichtigung und Schuldzuweisung verwendet als auf transparente Darstellung und schnelle gemeinsame Lösungen. Hierfür wird eine grundlegend neue „Fehlerkultur“ in den BIM-Projekten propagiert, die schon bei der Formulierung der Verträge beginnen muss, derart: „Mehr Fördern statt Fordern“ und „Lieber ein Fehler jetzt als eine Katastrophe später“.

Ohne Anspruch auf wissenschaftlich korrekte Bewertung, kann man sich sehr gut vorstellen, wieviel ungenutztes Potential bzw. teure Verluste allein aus den vorgenannten Beispielen erwachsen. Gelingt es, nur einen Teil dessen zur vermeiden, setzen die Effekte schnell und nachhaltig ein, und rechtfertigen den initial hohen Aufwand bei der Einführung von BIM in den Unternehmen.

Aus diesem Grund sollen bei der DB in den aktuellen und künftigen Infrastrukturprojekten immer mehr übergreifende Prozesse in den Handlungsrahmen aufgenommen werden. Aus Sicht der LST, die insbesondere in den DSD-Projekten das führende Gewerk ist, bietet sich das grüne Cluster in Abbildung 4 an: Vermessung, Trassierung, Oberbau/Fahrbahn, LST-Planung (inkl. ZN/ZL, BÜSA) mit Verkabelung und der dazu nötigen Kabeltrasse des Kabeltiefbaus (KTB). Sowie im erweiterten Fokus

das Zusammenspiel mit der Fahrleitung/Oberleitung (OLA) sowie mit den Verkehrsstationen (VST) und dem bahnbezogenen Hochbau, siehe oranges Cluster. Das blaue Cluster ist insbesondere bei der Dimensionierung und Koordinierung der Kabeltrassen im Kabeltiefbau (KTB) zusammen mit der LST-Verkabelung zu berücksichtigen. Schließlich beschreibt das graue Cluster, die bauliche Umgebung eines Infrastrukturprojektes, v.a. der konstruktive Ingenieurbau (KIB) mit seinen Tunneln und Brücken.

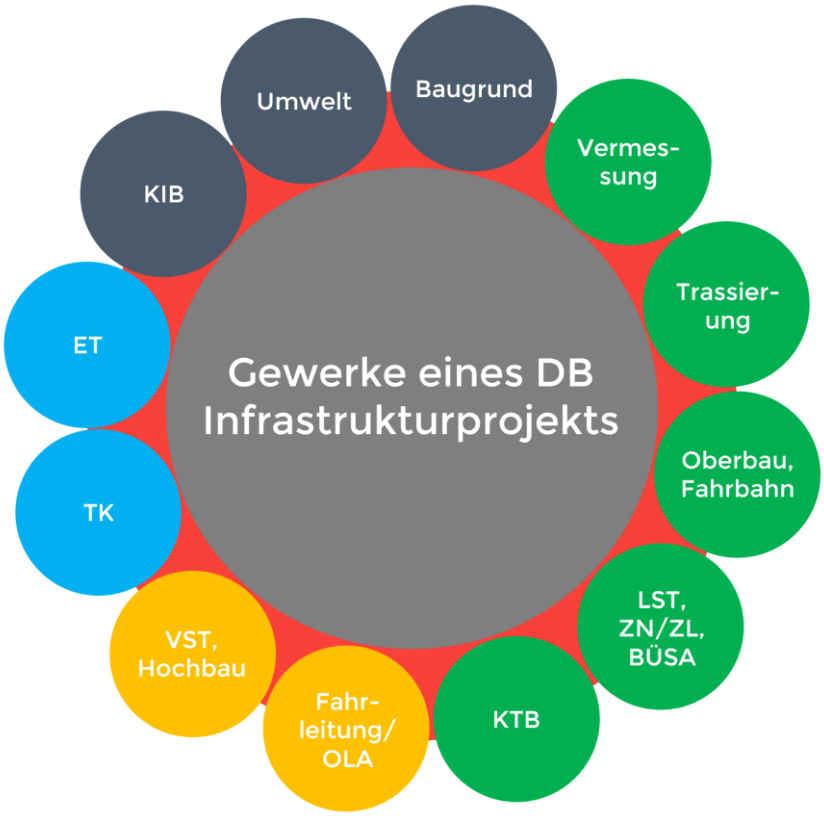

Abb. 4 Gewerke von Planung und Bau, die an einem Infrastrukturprojekt der DB beteiligt sein können.

3 Digitaler Zwilling im Kontext LST

Wenn man den bisherigen Argumentationen der vorliegenden Ausarbeitung folgt, dann ist die Einführung eines projektweiten, gemeinsamen und gesamtheitlichen 3D-Koordinationsmodells (Digitaler Zwilling) sofort schlüssig. Dabei spricht die Literatur auch von „big BIM“, ganz im Gegensatz zu der aktuell meist noch üblichen „Little BIM“-Praxis, die lediglich ein separates 3D-Modell für einzelne Gewerke als Teil der Auslieferung zur Leitungserbringung vorsieht. (Bormann et al. 2021, S. 409).

Das Koordinationsmodell ist die zentrale virtuelle Baustelle der Infrastrukturprojekte mit BIM, ähnlich wie die reale Baustelle in den klassischen Projekten, aber mit dem wichtigen Unterschied, dass alle Fehler und Irrtümer schon an dem Koordinationsmodell erkannt, analysiert und behoben werden können, noch bevor sie die echte Baustelle erreichen und dort zu immensen Problemen und Verzögerungen führen kann. In BIM wird dieses Prinzip sodann mit „Erst virtuell, dann real bauen“ (Bundesregierung, Homepage) zusammengefasst.

Tatsächlich ist dieses Prinzip aber viel älter als die BIM-Methode und hat seine partiellen Vorläufer auch im Zusammenhang der Stellwerksplanung mit dem sogenannten „Koordinierten Kabellageplan“. Dabei werden alle Verkabelungsanforderungen der verschiedenen Gewerke (v.a. LST, TK und ET) in einem 2D-Kabeltrassen- bzw. Kabellageplan zusammengeführt, um die Kabeltrasse passend zu konstruieren und die Kabelgefäße ausreichend groß zu dimensionieren.

Im 3D-Koordinationsmodell wäre eine solche Abstimmung bezüglich der Verkabelung bzw. der Kabeltrasse ein Anwendungsfall von vielen. Auch wenn die meisten Anwendungsfälle in einem Koordinationsmodell noch nicht im Fokus oder gar formal definiert sind, so gibt es aus Sicht der LST einige, die man bereits kennt und in aktuellen BIM-Projekten z.T. auch schon berücksichtigt:

- Bauliche Kollisionsdetektion, die aufzeigt, wo es bauliche Engpässe oder Zusammenstöße gibt, z.B. ein identischer Standort eines Signals und eines Oberleitungsmasts, oder die Kollision eines Signalbestandteils mit der Bahnsteigüberdachung.
- Signalsichtweitenprüfung, die klärt, ob ein Signalbild aus einer bestimmten Entfernung vom Fahrzeugführer ausreichend gesehen werden kann oder nicht.
- Detektion von Kollisionen mit Lichtraumprofilen, die zeigen, ob der Zug die Gleise ohne hineinragende Hindernisse (wie z.B. Bauten, Signalbestandteile oder Oberleitungsausleger) befahren kann.

Neben den baulichen Aspekten (in 2D bzw. 3D) spielen auch die zeitlichen Aspekte (4D) und die wirtschaftlichen Aspekte (5D) der BIM-Methodik eine wichtige Rolle bei der Analyse bzw. Auswertung eines Koordinationsmodells. Idealtypisch liefern hierzu die speziellen Softwaresysteme der Gewerke die grundlegenden Daten. Im Fall der LST macht das die Software ProSig wie folgt:

- 2D: Planung der LST im Kontext ESTW/DSTW und ETCS (Abbildung 3, oben links) und Ausleitung der fachlichen Daten in Form der PlanPro-XML.
- 3D: Ausleitung der baulichen Informationen mittels 3D-Objektkatalog in eine „PlanPro-IFC“; siehe beispielhafte BIM-Signalobjekte in Abbildung 6.
- 4D: Planung der Bauzustände für die zeitliche Abfolge der betriebssicheren Realisierung, siehe Bauzustandsplan in Abbildung 3 oben rechts.
- 5D: Mengengerüste und Ausrüstungsinformationen für die Kostenermittlung.

In Abbildung 5 ist der Übergang anhand eines gleichbleibenden Projektausschnitts vom 2D-Plan in ProSig (1) in das automatisch daraus abgeleitete 3D-Modell der LST in Navisworks (2) und schließlich in das Gesamtmodell in KorFin (3) erkennbar. Die zentrale Datenschnittstelle hierfür ist der 3D-Objektkatalog im IFC-Format, der bei der DB Netz seit etwa einem Jahr in Zusammenarbeit mit der WSP sukzessive erstellt und erweitert wird. In einer komplexen BIM-Software wie KorFin laufen alle Informationen der beteiligten Gewerke zusammen und können, wie oben beschrieben, dargestellt und ausgewertet werden. Ein solches 3D-Koordinationsmodel wurde aktuell im DB-Projekt „Hauptbahnhof Dortmund“ erstellt, das bereits sehr viele der in Kapitel 2.3 genannten Gewerke berücksichtigt, inklusive aller vorhandenen und geplanten Leitungen und deren Trassen, siehe Abbildung 7.

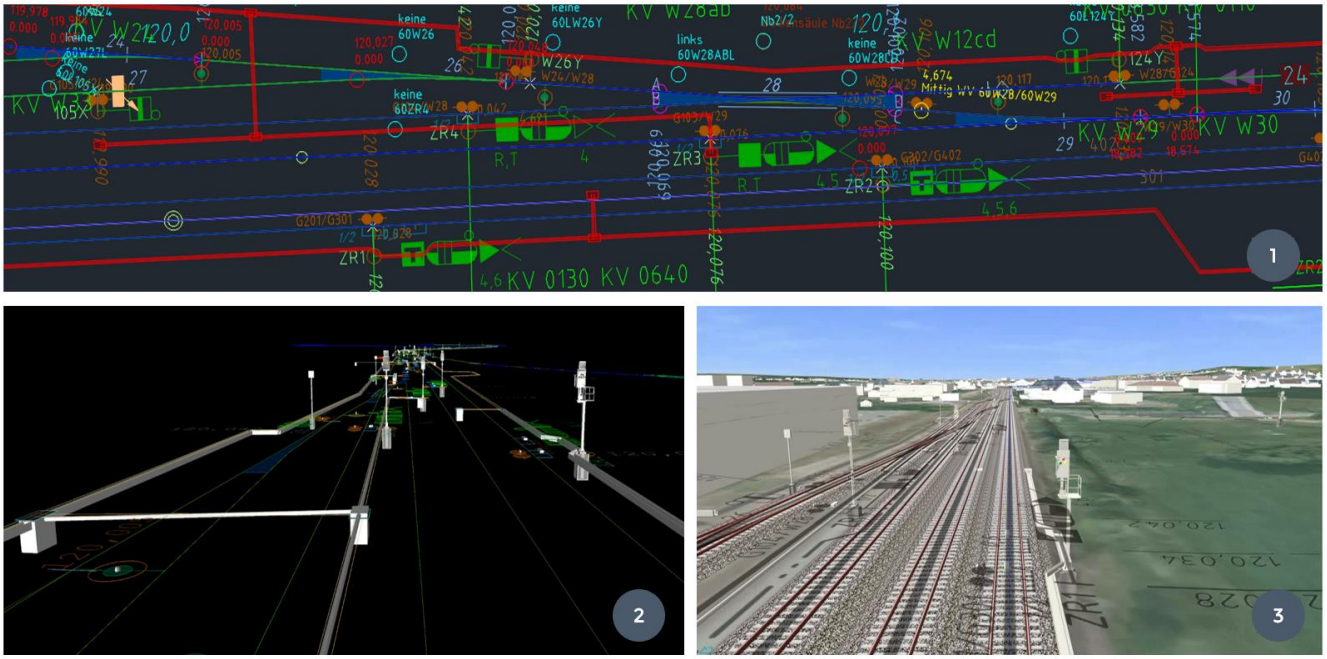

Abb. 5 Ausschnitt aus dem DB-Musterprojekt „P-Hausen“ bezüglich LST- und KTB-Objekte. [4]

In diesem Zusammenhang ist wichtig zu erwähnen, dass ein Digitaler Zwilling, der ein brauchbares Koordinationsmodel ist, nicht nur ein rein optisches 3D-Abbild der realen bzw. geplanten Situation ist, sondern auch alle fachlichen Informationen bzw. fach-logischen Zusammenhänge der relevanten Objekte in seiner Datenbasis hinterlegt hat.

Für den Bereich der LST müssen demnach die fachlichen Informationen aus der PlanPro-XML mit den baulichen Informationen der PlanPro-IFC datentechnisch zusammengebracht werden. Das geschieht über eine Objekt-ID, also einen Objektanfasser, der in beiden Dateien für ein instanziiertes Objekt (z.B. ein Hauptsignal) identisch ist. In einer BIM-Software, die in der Lage ist, beide o.g. PlanPro-Formate einzulesen, kann dann mit Hilfe der Objekt-IDs jedes sichtbare 3D-Objekt in seinen fachlichen Kontext eingebettet werden. Daraus ergeben sich erst fachlich-baulich kombinierte Analysemöglichkeiten, wie z.B. die o.g. „Detektion von Kollisionen mit Lichtraumprofilen“, die an den baulichen (!) Objekten entlang der fachlichen (!) Zufahrtsstraßen erfolgt.

Abb. 6 Eine von DB Netz definierte Signalanordnung wird je nach Detailierungsgrad (LOD) unterschiedlich genau in 3D dargestellt

4 Fazit und Ausblick

BIM ist als Arbeitsmethode und technologischer Rahmen für die künftige Abwicklung von komplexen Infrastrukturprojekten bei der DB und darüber hinaus gesetzt und weitgehend auch gewollt. Derzeit findet der Übergang von den klassischen Prozessen zu den BIM-relevanten Prozessen statt, was naturgemäß nicht reibungs- und problemlos verläuft. Bei allen Beteiligten wird durch Information und Schulung die Transitionsphase so gut wie möglich gestaltet und allmählich ist ein Umdenken und ein grundlegendes Verständnis für BIM in der Fläche und auf allen Unternehmensebenen erkennbar. Auch wenn aktuelle Projekte die neuen Verfahren und Organisationsstrukturen bereits in Form der BIM-Dokumente AIA und BAP vorgeben und einüben, so sind viele technische, vertragliche und rechtliche Details noch unklar. Das gilt sowohl speziell in den einzelnen Gewerken als auch in den gewerkeübergreifenden Prozessen und insbesondere in der Verwendung des 3D-Koordinationsmodells. Hier ist zu erwarten, dass die DB Netz die nötigen Vorgaben in einer Vielzahl von Richtlinien und technischen Mitteilungen definieren und entsprechend einfordern werden, so wie sie es im Kontext der PlanPro-Datenschnittstelle bereits getan hat.

Allerdings ist bei der Verwendung des 3D-Koordinationsmodells das Ende der Möglichkeiten bzw. der Anwendungsfälle noch nicht einmal in Sicht. Man kann zwar vermuten, dass mindestens alle realen Anwendungsfälle einer Baustelle auch ihr Pendant im Digitalen Zwilling finden, aber das virtuelle Modell macht auch Darstellungen und Aktivitäten möglich, die in der realen Welt nicht gehen. Hier sei als Beispiel das virtuelle Darstellen von Zufahrtsstraßen genannt, anhand derer man sich die Situationen in den verschiedenen Bauphasen vorlegt und etwaige Fahrstraßenausschlüsse erkennt und diskutiert.

Generell erscheinen aus den bisherigen BIM-Erfahrungen die folgenden Aspekte wichtig und erfolgsrelevant:

- Letztlich produziert der Mensch immer den Mehrwert, die Maschinen können nur unterstützen.
- Mit einer flexiblen und transparenten Kollaboration muss auch eine vertragliche Transparenz und Fairness einhergehen. Das erfordert insbesondere die Überwindung von statischen Honorarmodellen wie z.B. die der HOAI zugunsten von flexibler und leistungsgerechter Entlohnung.
- Infolgedessen erscheint der statische Werksvertrag und die damit einhergehende Bieterbewertung „Der Billigste gewinnt“ deutlich überkommen und wenig zielführend im Kontext BIM.

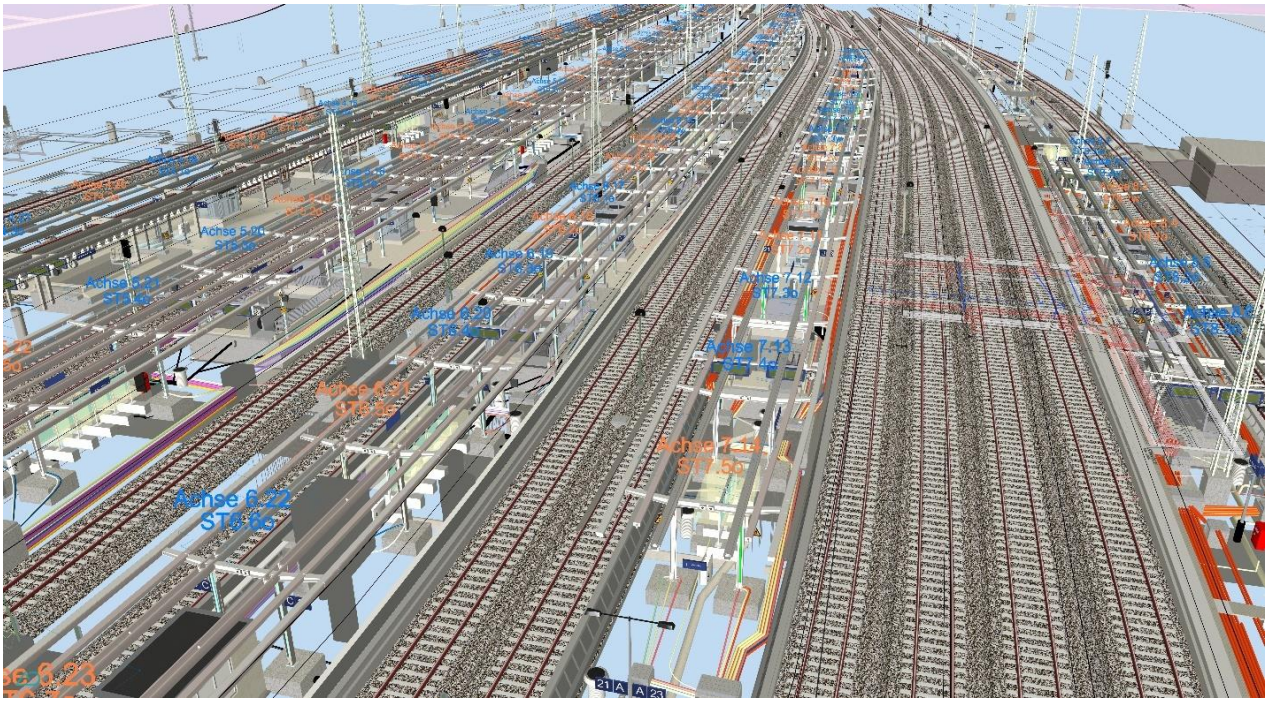

Abb. 7 Gesamtmodell des Hauptbahnhofs Dortmund in der BIM-Software KorFin. [5]

5 Abkürzungen

Tab. 1 Abkürzungen

Abkürzung	Bedeutung
AIA	Auftraggeberinformationsanforderungen
BAP	BIM Abwicklungsplan
BIM	Building Information Modeling
BÜSA	Bahnübergangssicherungsanlage
D3iP	Digitale durchgehende Datenhaltung in der Planung
DB	Deutsche Bahn
DSD	Digitale Schiene Deutschland
DSTW	Digitales Stellwerk
ESTW	Elektronisches Stellwerk
ET	Elektrotechnik
ETCS	European Train Control System
HOAI	Honorarabrechnung für Architekten und Ingenieure
IFC	Industry Foundation Classes
KIB	Konstruktiver Ingenieurbau
KTB	Kabeltiefbau
LOD	Level of Detail
LST	Leit- und Sicherungstechnik
OLA	Oberleitung
PDF	Portable Document Format
TK	Telekommunikation
VST	Verkehrsstationen
XLM	Extensible Markup Language
ZN/ZL	Zugnummern/Zuglenkung

6 Quellenangaben und Literaturverzeichnis

[1] Bildquelle: Uminski, Klaus, EI November 2021, S. 12

[2] Bildquelle: DB Netz Projekt D3iP

[3] Bildquelle: WSP Software ProSig

[4] WSP Software ProSig, DB Netz Projekt D3iP und A+S Software KorFin

[5] Bildquelle: A+S Software KorFin

[6] Bormann, A., König, M., Koch, C., Beetz, J. Hrsg. (2021), Building Information Modeling, Technologische Grundlagen und industrielle Praxis. Verlag: Springer Vieweg.

[7] Bundesregierung Homepage, Bundesverkehrsminister Alexander Dobrindt stellte in Berlin einen Stufenplan zur schrittweisen Einführung dieser digitalen Planungsmethode bei Infrastrukturprojekten und großen Bauvorhaben vor. Available at (accessed 12.04.2022): https://www.bundesregierung.de/breg-de/aktuelles/erst-virtuell-dann-real-bauen-454736

[8] Uminski, V., Klaus, C., Fachartikel im „Der Eisenbahningenieur “(EI November 2021). Digitale LST-Planung im Kontext Digitale Schiene Deutschland und BIM. Available at (accessed 12.04.2022):http://www.prosig.de/fileadmin/user_upload/202111_El_LST_im_Kontext_Digitale_Schiene_und_BIM.pdf