Projekt AutomatedTrain

Einsatz von Open-Source-Software im Eisenbahnsektor

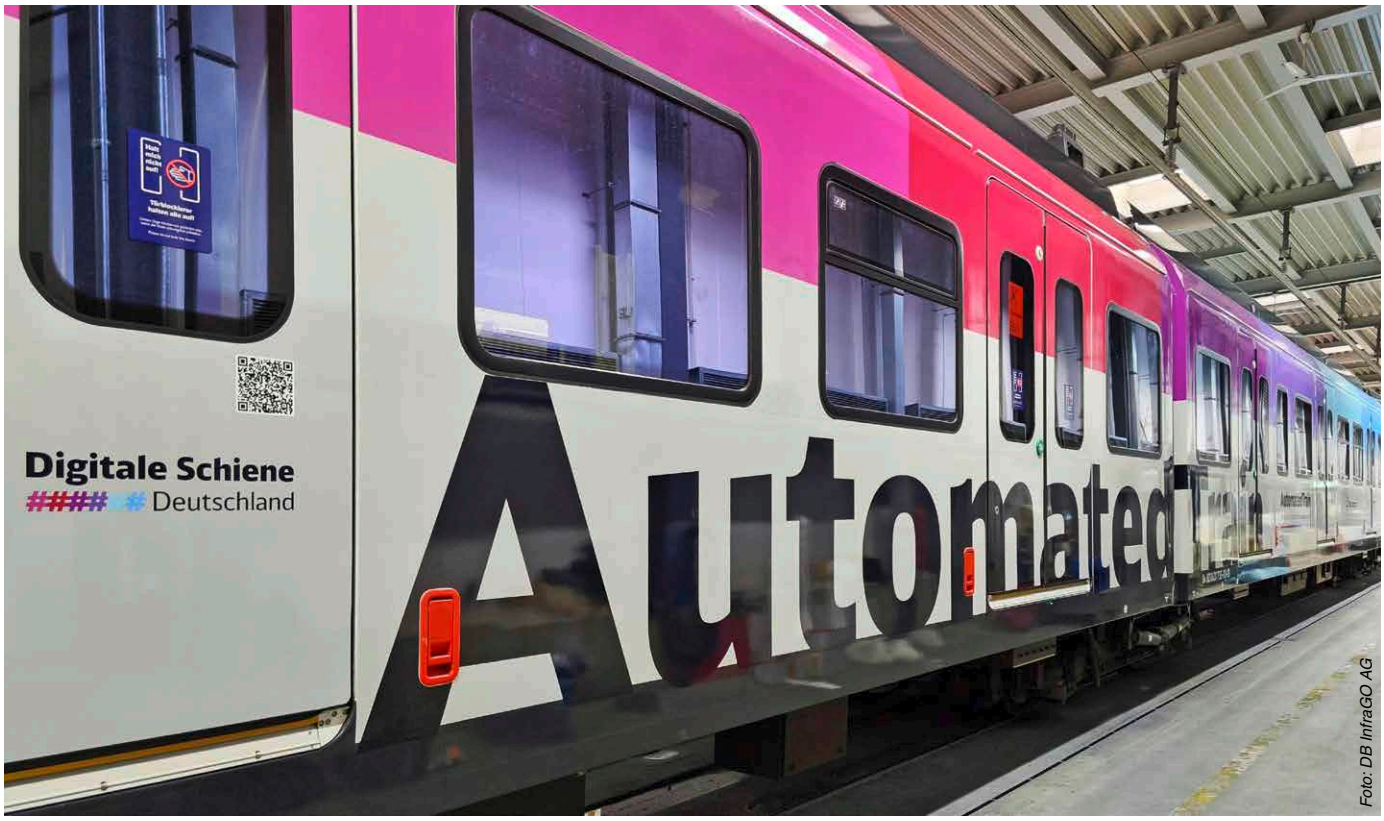

Foto: DB InfraGO AG

Dr. Jonas Rebstadt, IT Plattform Architekt, DB InfraGO AG, **Cornelius Schumacher**, Open Source Steward, DB Systel GmbH, und **Sebastian Hetze**, Principal Software Engineer, Red Hat, alle Berlin

Aufgrund ihrer grundlegenden Relevanz für den Einsatz von rechenintensiver Software zur Steuerung autonomer Züge werden im Zuge des Projektes AutomatedTrain auch die Potenziale sicherer und leistungsstarker Rechnerplattformen evaluiert. Der Einsatz von Open-Source-Software stärkt hierbei nicht nur die technologische Unabhängigkeit, sondern treibt auch nachhaltige und wirtschaftliche Innovationen im Eisenbahnsektor voran. Im Fokus steht die Frage, wie Open Source zuverlässig und langfristig im Bahnkontext etabliert werden kann.

Infrastrukturbetreiber und Eisenbahnverkehrsunternehmen werden durch den Fachkräftemangel bei Triebfahrzeugführenden und weiteren Bahnberufen vor große Herausforderungen gestellt. Um die vorhandenen Mitarbeitenden möglichst effizient einzusetzen, können Automatisierung und Digitalisierung geeignete Lösungen anbieten.

Eine vielversprechende Facette hiervon wird durch das vom Bundesministerium für Wirtschaft und Energie (BMWE) geförderte Forschungs- und Entwicklungsprojekt AutomatedTrain adressiert. In dem Projekt erprobt die DB InfraGO AG mit acht weiteren Partnern aus Industrie und Wissenschaft die technische Machbarkeit der vollautomatisierten, fahrerlosen Abstellungs- und Bereitstellungsfahrt im offenen Netz sowie das automatische Auf- und Abrüsten von Zügen. Das Projekt gibt damit wichtige Impulse in den Sektor und legt den Grundstein für die Entwicklung serienfähiger Produkte durch die Industrie.

Als Basis auch für zukünftige, datenintensive KI-Workloads wird im Zuge des Projektes eine hoch performante, modulare und funktional sichere Rechnerplattform spezifiziert und prototypisch evaluiert. Hierzu wird im Zusammenspiel mit weiteren Projekten sowohl DB-seitig [1] als auch im übergreifenden europäischen Kontext [2] auf einem einheitlichen Zielbild aufgesetzt.

Im Fokus dieses Zielbildes liegt die Entkopplung der Hardware von der durch einen Safety-Layer unterstützten Anwendungslogik. Um Entwicklungskosten zu reduzieren und Obsoleszenzrisiken zu minimieren, wird hierzu eine Virtualisierungsschicht eingefügt, welche physische IT-Ressourcen abstrahiert und als individuell provisionierbare, virtuelle Einheiten zur Verfügung stellt. Trotz differenzierter Anforderungen beim strecken- und zugseitigen Einsatz wird eine möglichst einheitliche Nutzung von marktgängiger Hardware und -Virtualisierungstechnologie verfolgt.

Die in Abbildung 1 (S. 43) dargestellte Plattformarchitektur ist nicht nur strecken- und zugseitig vergleichbar einsetzbar, sie stellt auch klar heraus, dass bereits durch den Einsatz von COTS-Komponenten (also marktüblicher Komponenten) – vor allem in den unteren beiden Schichten sowie im Bereich Maintenance und Diagnose zentrale Mehrwerte erzielt werden.

Gemeinsam von mehreren Unternehmen im Sektor entwickelte Open-Source-Komponenten können jedoch auch darüber hinaus als vielversprechende Enabler von Kosten-, Nachhaltigkeits- und Effizienzgewinnen dienen. Die folgenden Kapitel geben einen Einblick in das Thema Open Source und die Herausforderungen für die Etablierung, aber auch die Passgenauigkeit in den Bahnsektor.

Operational Technology

Herausforderungen im Bahnsektor

Der Einsatz von Open-Source-Software ist in der klassischen IT seit Jahren etabliert. Betriebssysteme, Datenbanken, Cloud-Plattformen und Entwicklungswerkzeuge werden heute selbstverständlich weitgehend als offene Komponenten entwickelt. In Domänen mit expliziten Safety-Anforderungen steht Open Source traditionell vor größeren Herausforderungen. Dennoch gibt es nicht nur mit dem Ingenuity Helicopter der NASA [3] sowie ELISA [4] Projekte und Initiativen, die das klare Potenzial von Open Source im Safety-Kontext erfolgreich demonstrieren. Vielmehr hat auch der Automobilsektor die Mehrwerte für sich erkannt und im Jahr 2025 eine groß angelegte Open-Source-Initiative [5] u. a. zur Entwicklung einer sicherheitskonformen, serviceorientierten Softwareplattform initiiert.

Um auch im Bahnsektor die vorhandenen Potenziale nutzen zu können, muss einerseits die strategische Bedeutung herausgestellt werden. Es müssen andererseits aber auch die Besonderheiten des Sektors explizit adressiert werden, die sich im Kontext von OT (Operational Technology) und insbesondere dort, wo funktionale Sicherheit gefordert ist, zwangsläufig ergeben.

OT ist nicht IT – und Sicherheit ist nicht verhandelbar

OT steuert physische Prozesse. Fehler führen nicht etwa zu Datenverlust oder temporären Ausfällen, sondern potenziell zu Gefährdungen von Leben, Umwelt und Infrastruktur. Systeme der Leit- und Sicherungstechnik, Onboard-Steuerungen oder Automatisierungsfunktionen sind über Jahrzehnte im Einsatz, unterliegen staatlichen Zulassungsverfahren und müssen Risiken auf extrem niedrige, gesellschaftlich akzeptierte Niveaus reduzieren.

Diese Rahmenbedingungen verändern den Blick auf Software grundlegend. In sicherheitskritischer OT ist Software kein Produkt im klassischen Sinn, sondern Teil eines regulierten Gesamtsystems, dessen Verhalten nachweisbar, nachvollziehbar und langfristig beherrschbar sein muss. Genau an dieser Stelle verschieben sich zwar die Maßstäbe für Open Source, strukturell ergeben sich jedoch klare Vorteile.

Offener Quellcode bei ausreichend großer Community ermöglicht Transparenz, unabhängige Bewertung und kollektive Lernprozesse. Anders als proprietäre Black-Box-Software erlaubt Open Source eine gesellschaftlich kontrollierbare Sicherheitsbasis.

Damit wird Open Source in sicherheitskritischer OT nicht nur zu einem Innovations- oder Kostenthema, es kann sich sogar zu einem Governance-Instrument für Risikokontrolle entwickeln.

Entkopplung von Lebenszyklen als Sicherheitsvorteil

Historisch sind viele OT-Systeme – insbesondere im Bahnsektor – monolithisch aufgebaut: Applikation, Middleware, Betriebssystem und Hardware sind eng gekoppelt und gemeinsam zertifiziert. Das erschwert nicht nur Innovation, sondern erhöht langfristig auch Sicherheitsrisiken, etwa durch veraltete Software oder fehlende Updates.

Open-Source-Software, die in gemeinsamer Verantwortung entwickelt wird, wirkt hier als Enabler für die Entkopplung der einzelnen Softwarearchitektur-Layer. Offene Komponenten, wie Betriebssysteme, Middleware-Stacks oder Anwendungsschnittstellen erlauben es, Lebenszyklen zu entkoppeln und Sicherheitsargumente gezielt auf stabile Basiskomponenten aufzubauen.

Änderungen werden nachvollziehbar, Updates kontrollierbar und Zertifizierungsartefakte wiederverwendbar. Damit wird Open Source zu einem Mittel, Sicherheit über lange Zeiträume aktiv zu erhalten, statt sie einmalig nachzuweisen.

Der offene Quellcode entbindet dabei niemanden von Verantwortung, vielmehr erzwingt er klare Rollen:

- Communities entwickeln und pflegen generische Komponenten
- Integratoren prägen Architekturentscheidungen und übergreifende Safety Cases
- Betreiber verantworten den sicheren Betrieb über den Lebenszyklus

Diese Entkopplung ist kein Nachteil, sondern eine Voraussetzung für skalierbare, herstellerunabhängige Systeme. Sie ermöglicht es, sicherheitsrelevante Argumente stabil zu halten, auch wenn sich Lieferanten, Hardwareplattformen oder Wartungsverträge ändern.

Das Paradox der Nachhaltigkeit: Öffentlich genutzt, aber nicht öffentlich gepflegt

Gerade in sicherheitskritischer OT zeigt sich jedoch auch die Kehrseite: Open Source ist ein öffentliches Gut, aber kein selbsttragendes. Wartung, Security-Fixes, Dokumentation und Community-Arbeit sind ressourcenintensiv. Werden offene Komponenten lediglich konsumiert, ohne dass Industrie, Betreiber oder öffentliche Hand Verantwortung übernehmen, entsteht ein strukturelles Risiko.

In OT-Systemen ist dieses Risiko besonders kritisch. Angriffe auf die Lieferkette, verwaiste Projekte oder fehlende Pflege sind nicht nur technische Probleme, sondern potenzielle Sicherheitslücken mit gesellschaftlicher Relevanz. Nachhaltiger Open-Source-Einsatz erfordert daher institutionelle Antworten: Konsortien, Foundations, langfristige Finanzierungsmodelle und klare Governance-Strukturen.

Open Source wird Teil der Sicherheitsarchitektur

Die eigentliche Besonderheit von Open Source in sicherheitskritischer OT liegt somit nicht im Code selbst, sondern in seiner Rolle. Open Source wird Teil der Sicherheitsarchitektur: organisatorisch, regulatorisch und technisch. Um die Vorteile von Open Source zu nutzen, muss es in einen Rahmen eingebunden werden, der Sicherheit und Stabilität gewährleistet.

Die entscheidende Frage muss daher nicht lauten: „Dürfen wir Open Source in sicherheitskritischen Systemen einsetzen?“, sondern: „Wie organisieren wir Open Source so, dass sie langfristig Sicherheit, Souveränität und Nachhaltigkeit unterstützt?“

Als zentrale Faktoren für die Etablierung von Open-Source-Software haben sich unter anderem eine breite Community und saubere Governance-Strukturen herauskristallisiert. Non-Profit-Organisationen wie die Linux Foundation oder die Eclipse Foundation können hierfür aufgrund ihrer Erfahrung und etablierten Strukturen ein ideales Dach bieten.

Seit Anfang 2024 gibt es mit der OpenRail Association[6] (OpenRail) auch formal eine explizit auf den Bahnsektor ausgerichtete Foundation, gegründet durch deutsche, französische und Schweizerische Bahnen (DB, SNCF, SBB) und den internationalen Eisenbahnverband UIC. OpenRail hat sich das Ziel gesetzt, die Zusammenarbeit zwischen den Organisationen des Sektors, vor allem in Europa, zu erleichtern, um die großen Herausforderungen des Sektors gemeinsam, effektiv und effizient anzugehen.

Konkret haben sich vor allem auf Plattformebene sowohl im Kontext von AutomatedTrain als auch

darüber hinaus Komponenten herauskristallisiert, die sich für eine offene gemeinsame Entwicklung – vergleichbar zum Automotive Sektor – sehr gut eignen würden. Aktuell werden sie noch mit vergleichsweise hohen Kosten individuell umgesetzt. Bei einer Beteiligung genügender Akteure innerhalb und außerhalb des Sektors könnten nennenswerte Kosten-, Nachhaltigkeits- und Effizienzgewinne realisiert werden.

Auch aus diesem Grund war die Betrachtung des Open-Source-Ökosystems im Sektor ein expliziter Bestandteil des AutomatedTrain-Projektes, welcher primär durch Red Hat als im Open-Source-Ökosystem stark verankertes Unternehmen vorangetrieben wurde.

Hierbei erfolgte zum einen eine Analyse des bereits existierenden Ökosystems, es wurden aber auch Empfehlungen für die weitere Ausgestaltung erarbeitet. Zuletzt lag der Fokus auf der Differenzierung hersteller- und benutzergeführter Konsortien sowie sinnvoll einsetzbarer Governance-Strukturen. Diese werden aktuell finalisiert und sollen dem Sektor im Anschluss zur Verfügung gestellt werden.

Zusammenfassung und Handlungsaufruf

Die kollaborative Entwicklung von Software als Open Source steht vor allem im Safety-Kontext vor Herausforderungen, verspricht jedoch auch weitreichende Mehrwerte. Vergleichbar mit dem Automotive-Sektor bietet auch im Bahn-Umfeld eine kartellrechtlich konforme kollaborative Entwicklung von nicht differenzierenden Komponenten ein hohes Potenzial für die beteiligten Unternehmen individuell aber auch für den Sektor insgesamt.

Eine Berücksichtigung von Open Source nicht nur durch Entwickelnde und Einkaufende kann somit seinen Anteil zu einem langfristig sicheren und wirtschaftlichen Sektor liefern. Um diese Potenziale zu heben, stehen sowohl Foundations wie OpenRail, aber auch die Open-Source-Ansprechpartner der DB [7] gerne unterstützend zur Verfügung. ■

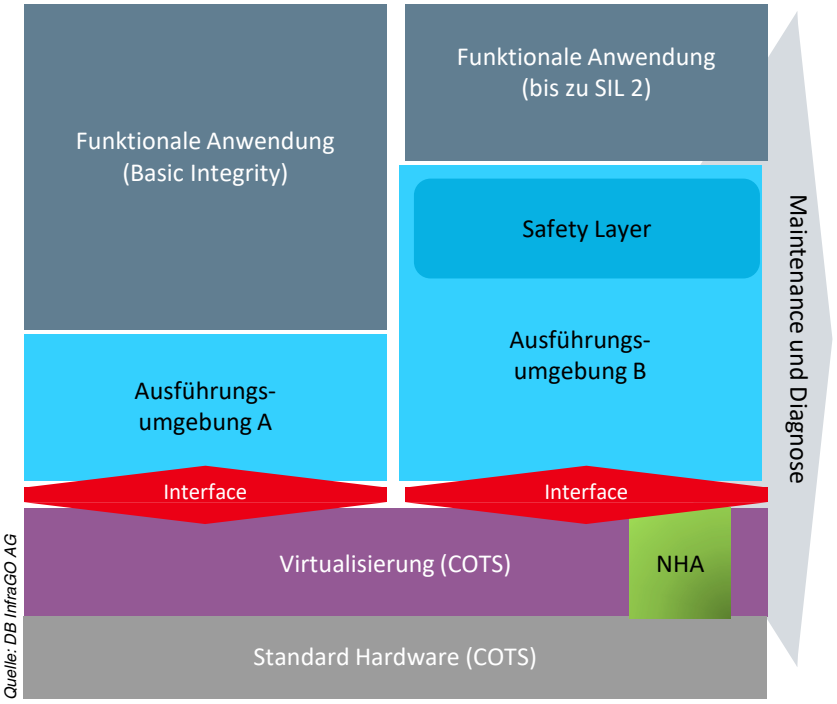

Abbildung 1:
Grundlegende Plattformarchitektur für Mixed-SiL-Anwendungsfällen basierend auf [1]

COTS = commercial off-the-shelf
NAH = native Hardware Acess
SIL = Sicherheitsanforderungsstufen (Safety Integrity Level)

Lesen Sie auch

Projekt AutomatedTrain: Betriebskonzept und Systemarchitektur
Deine Bahn 11/2024

Quellen

[1] A. Heine, P. Marsch und J. Rebstadt: Die Migration der Leit- und Sicherungstechnik in ein modernes IT- und Cloud-System, Signal+Draht 11/2025, S. 45-53.

[2] M. Fox, O. Mayer-Buschmann, P. Marsch, J. Wissmann, N. König, I. A. Ventas, G. Venturi, F. Inzirillo, P. Rozijn, T. Martin, S. Steffens und T. Bernburg: D26.3 – Final Modular Platform requirements, architecture and specification (25.07.2025). Online unter: https://rail-research.europa.eu/wp-content/uploads/2025/04/D26.3-%E2%80%93-Final-Modular-Platform-requirements-architecture-and-specification.pdf [Zugriff am 06.02.2026].

[3] K. Finley: Community powers NASA's Ingenuity Helicopter, github.com (14.04.2021). Online unter: https://github.com/readme/featured/nasa-ingenuity-helicopter [Zugriff am 02.06.2026].

[4] Foundation®, The Linux: ELISA Enabling Linux in Safety Applications. Online unter: https://elisa.tech [Zugriff am 06.02.2026].

[5] VDA: Innovation im Automotive-Sektor durch offene Zusammenarbeit (07.01.2026). Online unter: www.vda.de/de/presse/Pressemeldungen/2026/260107_PM_Innovation-im-Automotive-Sektor-durch-offene-Zusammenarbeit [Zugriff am 06.02.2026].

[6] OpenRail Association: https://openrailassociation.org [Zugriff am 06.02.2026].

[7] DB Systel GmbH: Open Source @ Deutsche Bahn. Online unter: https://opensource.deutschebahn.com/opensource [Zugriff am 06 02 2026].