Erste Implementierung einer virtualisierten LST-Architektur bis SIL4

The first implementation of a virtualised railway signalling architecture up to SIL4

Jonas Rebstadt | Martin Mitzkus | Sonja Steffens | Patrick Marsch

Heutige digitale Leit- und Sicherungstechnik (DLST) basiert überwiegend auf spezialisierter Hardware und bahnspezifischen Lösungen. Dies führt zu erhöhten Kosten, Obsoleszenzrisiken und ineffizienter Instandhaltung. Eine Abstraktion von Hard- und Software durch Virtualisierung und der Einsatz von Commercial-Off-The-Shelf (COTS)-Komponenten verspricht erhebliche Vorteile. Im Projekt Cloud4Rail wurde nun erstmalig eine Safety-Integrity-Level 4 (SIL4)-Bahnanwendung über Virtualisierung und COTS-Komponenten umgesetzt und der Native Hardware Access (NHA) als notwendige sektorspezifische Komponente als Open Source implementiert.

1 Motivation und Einführung

Die europäischen Eisenbahninfrastrukturunternehmen (EIU), darunter auch die DB InfraGO AG (DB InfraGO), befinden sich in einem umfassenden Modernisierungsprozess ihrer Leit- und Sicherungstechnik (LST). Aufgrund der evolutionären Entwicklung der Systeme basieren diese heute (z. B. im Kontext der Umsetzung von Stellwerks-Zentraleinheiten in digitalen Technikzentralen, DTZ) aber noch in hohem Maße auf bahnspezifischer Spezialhardware und Legacy-Architekturen mit enger Verzahnung von Software und Hardware. Dies führt nicht nur zu hohem Platzbedarf in Rechenzentren (DTZ), sondern auch zu herstellerspezifischen Abhängigkeiten in Betrieb und Wartung sowie zu zunehmenden Herausforderungen durch Obsoleszenz.

Zur Bewältigung dieser Herausforderungen gehen zahlreiche LST-Hersteller dazu über, ihre Architekturen auf marktübliche, d. h. COTS-Hardware umzustellen. Bei SIL4-Systemen ist dies nur möglich, wenn die sicherheitsgerichteten Funktionen der Hardware softwareseitig ersetzt werden. Diese können in einem sogenannten Software-Safety-Layer (siehe Kapitel 3) gekapselt werden, der die funktionale Sicherheit der sicherheitskritischen Anwendungen bei potenziellen Fehlern in der Hardware oder in nicht sicherheitskritischer Software wie z. B. Open-Source-Betriebssystemen gewährleistet.

Der europäische Bahnsektor geht noch einen Schritt weiter und strebt eine vollständige Abstraktion der Software von der Hardware durch Virtualisierung an (siehe Zielbild in Bild 1). Dieser Schritt ist für die DB InfraGO und viele andere europäische EIU von zentraler Bedeutung, um einen generischen Hardwarepool zu ermöglichen, auf dem mehrere LST-Anwendungen mit unterschiedlichen SIL-Anforderungen und Betriebssystemen gemeinsam mit Basis-IT-Diensten wie z. B. einer Public Key Infrastructure (PKI) laufen können.

DB InfraGO erhofft sich hiervon u. a.:

Today's digital railway control, command and signalling (CCS) technology still largely relies on specialised hardware and railway-specific solutions. This leads to higher costs, significant obsolescence risks and inefficient maintenance processes. Virtualisation, the separation of software from hardware and the use of commercial-off-the-shelf (COTS) hardware promise substantial benefits. A safety integrity level 4 (SIL4) railway application has now been implemented using virtualisation and COTS hardware for the very first time in the Cloud4Rail project. A key sector-specific component required for this approach, known as Native Hardware Access (NHA), has been implemented and published as open-source software (OSS).

1 Motivation and introduction

European railway infrastructure managers (IMs), including DB InfraGO AG (DB InfraGO), are currently undertaking a major modernisation of their CCS systems. Their evolutionary development means that these systems (e.g. within the context of interlocking central units at Digital Technology Centres, DTZ) still depend heavily on railway-specific hardware and legacy architectures where software and hardware are tightly coupled. This results not only in large data centre (DTZ) footprints but also in vendor-specific operations and maintenance, as well as increasing obsolescence risks.

In order to address these issues, many signalling vendors are now moving toward COTS hardware. Hardware-based safety functions must be replaced with software equivalents in systems with the highest safety integrity level 4. These are typically encapsulated within a Software Safety Layer (see Chapter 3), which ensures safe operations even in the presence of hardware faults or non-safety-critical software such as open-source operating systems.

The European rail sector is taking this idea one step further and aiming for the full abstraction of software from hardware through virtualisation (the target image is shown in fig. 1). This is the key to enabling a shared hardware pool where multiple signalling applications with varying safety requirements and operating systems can operate alongside standard IT services such as public key infrastructure (PKI).

For DB InfraGO and other infrastructure operators, this approach promises:

- lower capital and operating costs
- strongly reduced obsolescence risks
- simplified and standardised maintenance

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026

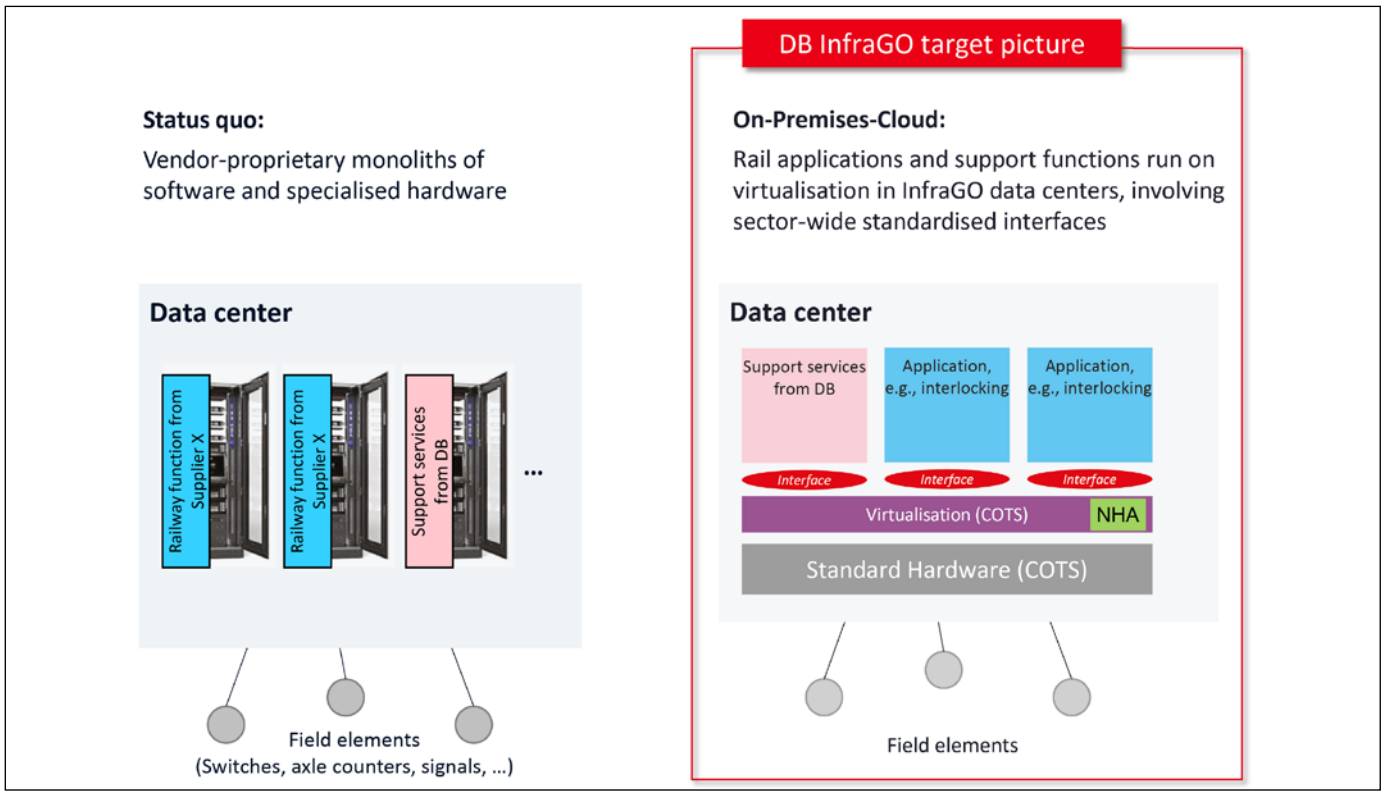


Bild 1: Vom Status Quo monolithischer Lösungen zur Zielarchitektur On-Premises-Cloud der DB InfraGO
Fig. 1: From the current state of monolithic solutions to the target architecture for an on-premises cloud at DB InfraGO
Quelle / *Source*: DB InfraGO

- reduzierte Invest- und Betriebskosten
- deutlich reduzierte Obsoleszenzrisiken
- vereinfachte, da standardisierte Instandhaltung
- mehr Flexibilität und dadurch Beschleunigung des LST-Rollouts.

Die hierbei für SIL4-Anwendungen notwendigen Architekturanpassungen wurden im Förderprogramm Europe's Rail gemeinsam mit anderen europäischen Bahnen und Herstellern grundlegend erarbeitet [1]. Im Förderprojekt Cloud4Rail ist nun erstmalig in einer F&E-Kollaboration zwischen DB InfraGO und Siemens Mobility eine Umsetzung der in Europe's Rail spezifizierten Architektur erfolgt und damit die Machbarkeit des Konzeptes bestätigt worden. Zudem wurde eine hierfür erforderliche Komponente „Native Hardware Access" erstmalig implementiert, welche nun dem Sektor als Open Source Software (OSS) zur Verfügung gestellt wird.
Aufsetzend auf einer kurzen Einleitung zu On-Premises-Clouds im Bahnsektor wird im Folgenden die grundlegende Architektur von IT-Plattformen für SIL4-Anwendungen wie Stellwerkskernen oder ETCS-Zentraleinheiten (Radio Block Centres, RBC) vorgestellt, um danach auf die Potenziale von Open-Source-Entwicklung im Bahnsektor einzugehen und den NHA als exemplarische initiale Open-Source-Komponente vorzustellen. Abgerundet wird der Beitrag durch ein Kapitel zur technischen Machbarkeit virtualisierter LST-Funktionen bis SIL4 sowie einem abschließenden Ausblick.

2 On-Premises-Cloud für Applikationen bis SIL4

Im Bahnsystem gibt es eine Vielzahl von Bahnanwendungen mit unterschiedlichen Anforderungen an die darunterliegenden IT-Plattformen, mit der Konsequenz, dass verschiedene Ausprägungen von Plattformen zum Einsatz kommen bzw. eingeführt werden. So macht es z. B. einen großen Unterschied, ob Bahnanwendungen sogenannte Basisintegrität oder z. B. SIL4 erfüllen und somit höheren

- greater flexibility and faster deployment of signalling systems.

The required SIL4 architecture principles have been developed collaboratively with other European railways and suppliers under the Europe's Rail program [1]. Within the Cloud-4Rail project, specifically in collaboration among DB InfraGO and Siemens Mobility, this architecture was now implemented for the first time, and its feasibility was demonstrated. A central component, the NHA, has also been implemented and made available as OSS.
The following sections introduce the concept of on-premises clouds in the rail sector, outline the architecture for SIL4 applications such as interlockings or Radio Block Centres (RBC), discuss the potential of open source in the rail sector and present the NHA component as a first example. The paper concludes with a chapter on the technical feasibility of virtualised LST functions up to SIL4, as well as an outlook.

2 An on-premises cloud for applications up to SIL4

There is a wide range of railway applications within the rail system, each with different requirements on the underlying IT platforms. As a result, multiple platform variants have been used or introduced. For example, it makes a significant difference whether applications only need to meet basic integrity requirements or must comply with higher functional safety standards such as SIL4. Approval and certification processes also vary depending on the application, as do the immediate consequences that a system failure may have on railway operations. Reference [2] identifies the key railway application characteristics, from which four distinct types of railway IT platforms can be derived.
It should be emphasised that DB InfraGO plans to implement all the dispositive and operational railway functions exclusive-

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026

Anforderungen an funktionale Sicherheit genügen müssen. Auch spielt es eine Rolle, welche Freigabe- und Zulassungsprozesse für die jeweiligen Anwendungen zu befolgen sind und welche unmittelbaren Auswirkungen der Ausfall einer Anwendung auf den Bahnbetrieb hat. In [2] wurden die wesentlichen Eigenschaften von Bahnanwendungen aufgelistet, aus denen sich vier Ausprägungen von bahnbetrieblichen IT-Plattformen ergeben.

Es sollte betont werden, dass DB InfraGO plant, für dispositive und operative bahnbetriebliche Funktionen ausschließlich IT-Plattformen als DB-Eigentum und in der vollen rechtlichen und funktionalen Hoheit der DB umzusetzen – in der Form von On-Premises-Clouds im eigenen Hause, wie z. B. in den Betriebszentralen und DTZ der InfraGO. Dies rührt daher, dass regulatorische, normative und rechtliche Vorgaben im bahnbetrieblichen Kontext die Nutzung nicht-Bahn-eigener Cloud-Infrastruktur sehr einschränken bzw. die Wirtschaftlichkeit einer solchen Nutzung sehr fraglich erscheinen lassen. Hinzu kommen vergaberechtliche, strategische und auch geopolitische Gründe, die für On-Premises-Clouds sprechen.

In diesem Beitrag ist der Fokus auf bahnbetriebliche Anwendungen mit den stringentesten Anforderungen, nämlich Stellwerks- und ETCS-Zentraleinheiten, welche SIL4 erfordern, und welche, so wie alle dispositiven und operativen bahnbetrieblichen Funktionen, künftig in On-Premises-Clouds umgesetzt werden sollen.

3 Safety-Architektur für SIL4-Anwendungen in einer On-Premises-Cloud

Für die Verwendung einer On-Premises-Cloud für sicherungstechnische Applikationen – etwa Stellwerks- oder ETCS-Zentraleinheiten – sind eine neue Safety-Architektur und mehrere technologische Schritte erforderlich. In [3] ist ein Vergleich zweier grundsätzlich möglicher Ansätze erfolgt; in der hier beschriebenen Implementierung ist nun die dort genannte „Safety-Architektur 1" umgesetzt worden.

Zunächst bedarf es eines softwarebasierten Safety-Layers, der auf COTS-Hardware betrieben werden kann und die Einbindung nicht sicherheitsrelevanter Softwarekomponenten – beispielsweise eines handelsüblichen Betriebssystems (z. B. Linux) sowie eines Security-Stacks – ermöglicht. Ein solcher Safety-Layer basiert typischerweise auf etablierten Sicherheitsprinzipien:

- Mehrkanaligkeit auf separater Hardware,
- Diversität der Kanäle,
- sicherer Kanalvergleich sowie
- zusätzliche Redundanz zur Gewährleistung der Verfügbarkeit.

Der Safety-Layer stellt dabei nicht nur die sichere Ablaufumgebung für die sicherungstechnische Applikation bereit, sondern ist auch für deren zeitlich korrekten Ablauf verantwortlich. Er muss einen sicheren Systemtakt zur zeitlichen Steuerung der Applikation bereitstellen. Auch für diesen Systemtakt gelten die genannten Sicherheitsprinzipien – insbesondere Mehrkanaligkeit, separate Hardware und sicherer Vergleich. Konkret werden hierzu Systemtakte aus Quarzoszillatoren separater Hardwarekomponenten herangezogen und unter Berücksichtigung möglicher Drifts gegeneinander verglichen. Diese Prinzipien bilden die wesentliche Grundlage eines softwarebasierten Safety-Layers.

Soll ein solcher Safety-Layer in einer On-Premises-Cloud betrieben werden, sind im nächsten Schritt weitere Maßnahmen erforderlich, um die zusätzlichen Gefährdungen zu beherrschen, die sich aus der Verwendung nicht sicherungstechnisch qualifizierter Virtualisierungstechnologie ergeben:

a) **Hardwareseparation der Kanäle:** Der Ablauf der einzelnen Kanäle auf separater physikalischer Hardware ist nicht hinreichend sicher gewährleistet, da Virtualisierungsumgebungen Funktionen

ly on IT platforms that are owned by DB and fully under its legal and functional control, specifically in the form of on-premises clouds hosted within its own facilities, such as operations control centres and DTZ. This approach is driven by regulatory, normative and legal constraints in the railway domain, which significantly limit the use of non-railway-owned cloud infrastructure or render its economic viability questionable. In addition, procurement and strategic and geopolitical considerations further support the pursuit of on-premises cloud solutions.

This article focuses on the most demanding applications such as interlocking and ETCS central units, which require SIL4 and which, like all dispositive and operational railway functions, are to be implemented in on-premises clouds in the future.

3 The safety architecture for SIL4 applications in an on-premises cloud

A new safety architecture and several technological steps are required so as to enable the use of an on-premises-cloud for safety-critical applications, such as interlockings or ETCS central units. Reference [3] compares two fundamentally possible approaches; the implementation described here follows what is referred to therein as "Safety Architecture 1."

At its core, this approach requires a software-based safety layer that can run on COTS hardware and allows the integration of non-safety-critical software components, such as a standard operating system (e.g. Linux) and a security stack. Such a safety layer typically relies on well-established safety principles:

- multi-channel operations on separate hardware
- channel diversity
- secure channel output comparison
- additional redundancy so as to ensure availability.

The safety layer not only provides a secure execution environment for the safety-critical application but is also responsible for ensuring its correct behaviour. This must include a reliable system clock to control the application's execution. The system clock must also adhere to the same safety principles, particularly a multi-channel design, hardware separation and secure comparison. In practice, system clocks derived from quartz oscillators on separate hardware components are compared against each other while accounting for any potential drift. These principles form the foundation of a software-based safety layer.

When such a safety layer is operated within an on-premises cloud, additional measures are required to address any new risks introduced by virtualisation technologies that have not been inherently safety-certified:

a) **the hardware separation of the channels:** the reliable running of the channels on separate physical hardware cannot be fully guaranteed, as virtualisation platforms allow applications to be migrated between machines (e.g. live migration).
b) **the integrity of the system clock:** the use of the physical hardware clock cannot be fully trusted, since virtualisation environments can simulate or manipulate time information.
c) **hardware transparency:** any information about the underlying hardware or its use (required for the safety concept) is no longer directly accessible from within the virtualised environment.

A computing environment architecture that includes the NHA software component has been defined within the context of Europe's Rail Joint Undertaking [1] in order to address these challenges. This component runs natively at the host operating sys-

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026

zur Migration von Applikationen auf andere Hardware bereitstellen (z. B. Live-Migration).

b) **Integrität des Systemtakts:** Die Nutzung des Systemtakts der physikalischen Hardware ist nicht hinreichend sicher gewährleistet, da Virtualisierungsumgebungen Funktionen zur Simulation von Zeitinformationen bieten.

c) **Hardwaretransparenz:** Weitere für das Sicherheitskonzept notwendige Informationen über die zugrunde liegende Hardware bzw. deren Nutzung sind aus der virtualisierten Umgebung heraus nicht mehr direkt zugänglich.

Zur Behandlung dieser Aspekte wurde im Rahmen von Europe's Rail Joint Undertaking eine Computing-Environment-Architektur mit einer NHA-Softwarekomponente definiert [1]. Diese Komponente wird unterhalb der Virtualisierungsschicht auf Ebene des Host-Betriebssystems nativ ausgeführt und stellt dem Safety-Layer (innerhalb der virtuellen Maschine) folgende erforderlichen Hardwareinformationen bereit:

a) eine eindeutige Identifikation der verwendeten physikalischen Hardware,

b) einen Systemtakt, der unmittelbar aus dem physikalischen Quarzoszillator der verwendeten Hardware abgeleitet wird, sowie

c) bei Bedarf weitere Informationen über die Hardware bzw. deren Nutzung.

Diese Informationen ergeben sich aus den herstellerspezifischen Sicherheitskonzept(en) der Safety-Layer.

4 Open Source im Bahnsektor

Wie zuvor beschrieben, ist eine wesentliche Prämisse der angestrebten Architektur eine weitestmögliche Nutzung von COTS-Komponenten. In manchen Fällen sind Bahnsektor-spezifische Lösungen wie die NHA-Komponente aber nicht vermeidbar. Es ist zu erwarten, dass auch das Management, Update und Konfiguration einer On-Premises-Cloud für den Bahnbetrieb, inkl. der automatisierten Reaktion auf Hardwareausfälle, bahnspezifische Aspekte beinhalten wird.

tem level, beneath the virtualisation layer, and provides the safety layer (within the virtual machine) with the following essential hardware-related information:

a) unique identification of the physical hardware in use,

b) a system clock derived directly from the hardware's physical quartz oscillator, and

c) additional hardware or usage information, if required.

These requirements stem from the manufacturer-specific safety concepts of the safety layer. Fig. 2 illustrates the general safety architecture for a two-channel system, where synchronisation between the channels is achieved via IP-based communication between the safety layer instances.

When selecting a virtualisation technology, it is essential to ensure that it supports the integration of an NHA component at the host operating system level. Moreover, the combined architecture, i.e. the virtualisation together with the NHA, must be reflected in the system-specific safety concepts defined by the manufacturers.

4 Open source in the railway sector

As described earlier, a key premise of the proposed architecture involves the extensive use of COTS components. However, in some cases, railway-specific solutions, such as the NHA component, are unavoidable. It can also be expected that the management, update and configuration of an on-premises cloud for railway operations, including any automated responses to hardware failures, will involve domain-specific requirements.

An OSS approach appears to be a highly suitable solution [4] to ensuring that any such railway-specific functions remain cost-efficient and sustainably available across the sector.

While OSS has been firmly established in traditional IT for many years, safety-critical domains have historically faced greater challenges in adopting it. In the railway sector, especially within operational technology (OT), systems control

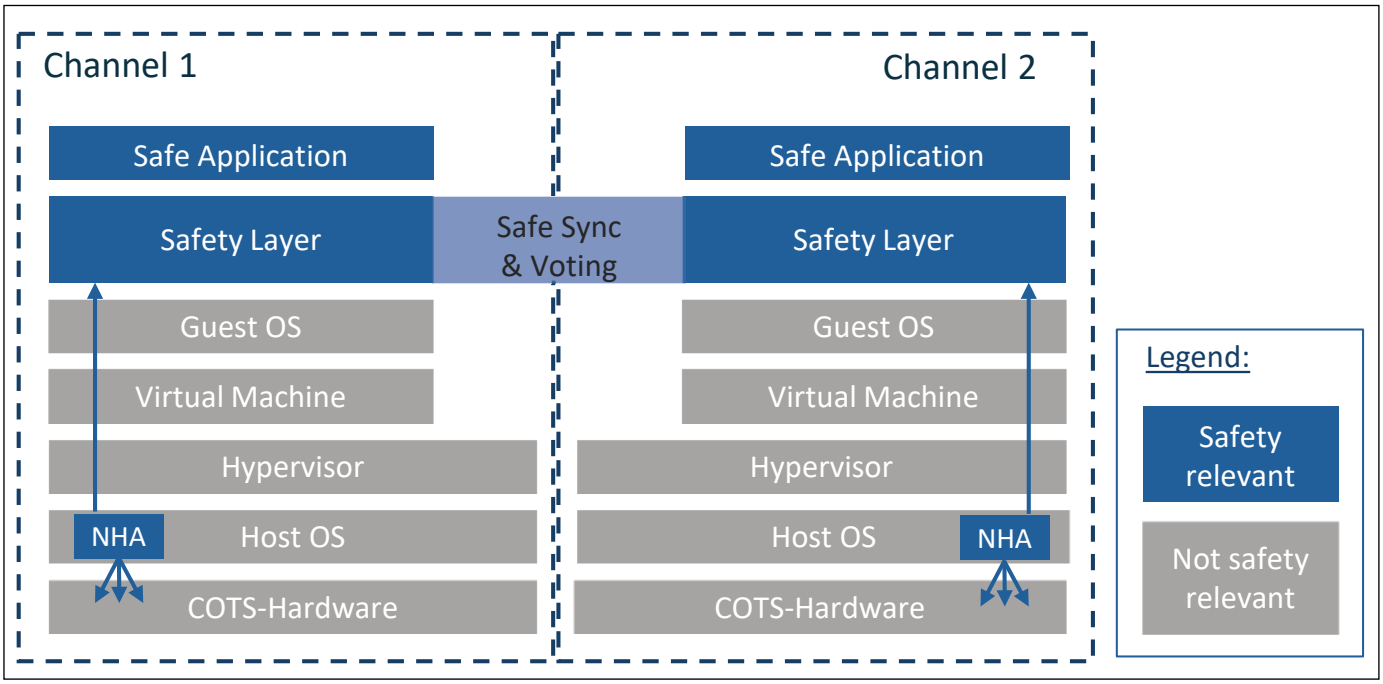


Bild 2: Darstellung eines zweikanaligen Systems mit Nutzung von Safety-Layer und NHA
Fig. 2: A representation of a two-channel system using a safety layer and NHA

Quelle / *Source*: Siemens Mobility

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026

Um sicherzustellen, dass auch diese bahnspezifischen Funktionen kostengünstig und nachhaltig im Sektor zur Verfügung stehen, erscheint ein OSS-Ansatz hier sinnvoll [4].

Während OSS in der klassischen IT bereits seit Jahren etabliert ist, stehen Domänen mit Safety-Anforderungen traditionell vor größeren Herausforderungen. Im Bahnsektor und vor allem im Kontext von Operational Technology (OT) existieren durch die Steuerung physischer Prozesse und erheblicher Auswirkungen von Fehlern auf Menschen, Umwelt und Infrastruktur Rahmenbedingungen, die sich merklich von klassischen IT-Systemen unterscheiden [4]. Entsprechend unterliegen sicherungstechnische Applikationen – etwa Stellwerks- oder RBC-Logik – langen Lebenszyklen, strengen Zulassungsverfahren und höchsten Anforderungen an Nachvollziehbarkeit und Sicherheit.

Trotz dieser Herausforderungen zeigen sich bereits in Domänen wie der Raumfahrt (Ingenuity Helicopter der NASA [5]) oder dem Automotive Sektor (z. B. Eclipse S-CORE [6]) erste Erfolgsgeschichten hin zur kollaborativen, offenen Entwicklung von Software. Offener Quellcode kann hierbei Transparenz, unabhängige Prüfung und gemeinschaftliche Weiterentwicklung ermöglichen, wodurch neue Ansätze zur Risikokontrolle und Sicherheits-Governance entstehen können [4]. Gerade in Zeiten geopolitischer Anspannungen kann die kollaborative Open-Source-Entwicklung zudem die Souveränität der (IT-)Infrastruktur und der Lieferketten stärken.

Um diese Schritte auch im Bahnsektor erfolgreich gehen zu können, müssen monolithische Systemarchitekturen modularisiert und muss eine saubere Trennung von Komponenten mit hohem eigenem Wertschöpfungsanteil und Basiskomponenten ohne zentrale Intellectual Property (IP) vorgenommen werden. Während Erstere auch in anderen Sektoren in der individuellen Entwicklung der jeweiligen Hersteller verbleiben, bieten gerade grundlegende Plattformtechnologien ein großes Potenzial für Kosteneinsparungen durch kollaborative Entwicklung und Pflege. Hierdurch können Innovationszyklen beschleunigt, Wartbarkeit verbessert und Sicherheitsargumentationen langfristig stabilisiert werden. Gleichzeitig erfordert der nachhaltige Einsatz von Open Source aber auch klare Verantwortlichkeiten einer Mindestzahl von Kontributoren, geeignete Governance-Strukturen und langfristige Pflege.

physical processes and failures can have significant consequences for people, the environment and infrastructure. As a result, the underlying conditions differ significantly from those in classic IT systems [4]. Accordingly, safety-critical applications, such as interlocking or RBC logic, are subject to long lifecycles, strict certification processes and the highest traceability and safety requirements.

Despite these challenges, successful examples of collaborative and open software development are already emerging in domains such as aerospace (e.g. NASA's Ingenuity helicopter [5]) and the automotive sector (e.g. Eclipse S-CORE [6]). Open source can enhance transparency, enable independent verification and foster collective development, thereby creating new approaches to risk control and safety governance [4]. Particularly in times of geopolitical tension, collaborative open-source development can also strengthen the sovereignty of IT infrastructure and supply chains.

Monolithic system architectures must first be modularised and a clear separation must be established between those components with high proprietary value creation and foundational components without any critical intellectual property (IP) in order to achieve similar progress in the railway sector. While the former typically remain within the responsibility of individual manufacturers, core platform technologies offer significant potential for cost savings through collaborative development and maintenance. This can accelerate innovation cycles, improve maintainability and stabilise safety arguments over the long term. At the same time, the sustainable use of OSS requires clear responsibilities among a core group of contributors, appropriate governance structures and long-term maintenance commitments.

A key factor for successfully establishing open source in OT environments is precisely this separation between competitively differentiating components and fundamentally standardised system components. The ongoing sector-wide standardisation efforts and central role played by safety cases, in-

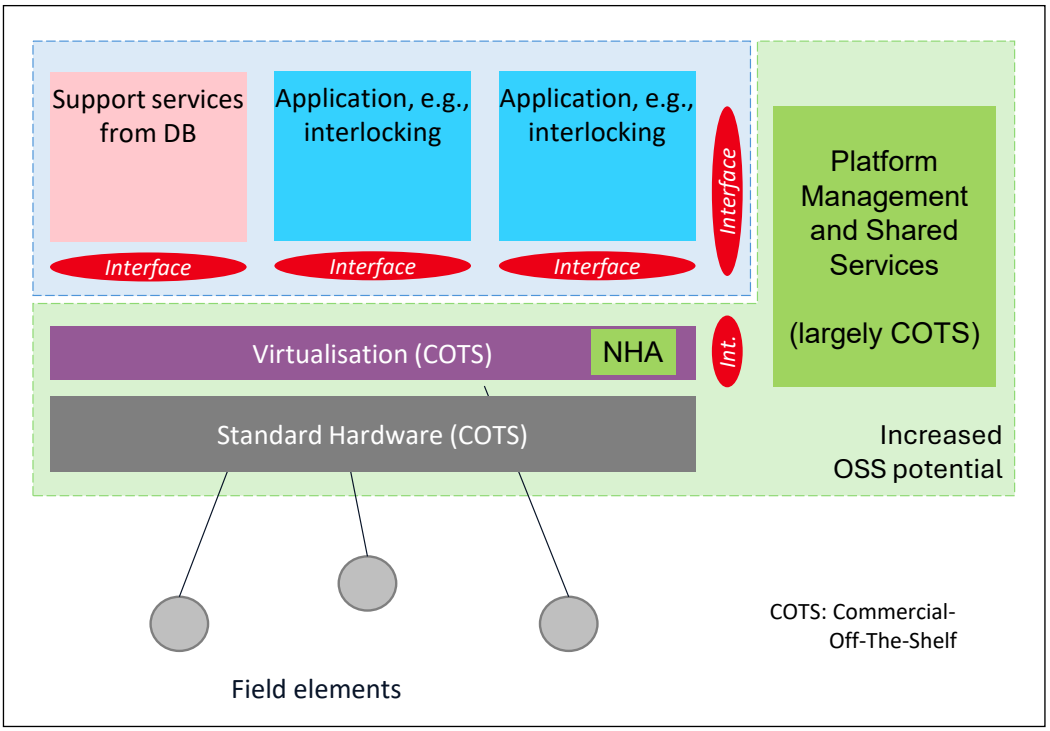


Bild 3: Virtualisierte DLST-Architektur inklusive OSS-Potenzialen in grün
Fig. 3: A virtualised digital signalling architecture (DLST), including the OSS potential highlighted in green
Quelle / *Source*: DB InfraGO

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026

Zentral für die erfolgreiche Etablierung von Open Source im Bereich der OT ist wie genannt eine saubere Abgrenzung der wettbewerblich differenzierenden Komponenten von den grundlegend einheitlichen Komponenten des Systems. Bedingt durch die sektorweit vorangetriebene Standardisierung und die – auch im Hinblick auf die IP – zentralen Safety-Cases ergibt sich hierbei für bahnbetriebliche IT-Plattformen im OT-Kontext die in Bild 3 dargestellte Aufteilung. Während der hellblaue Teil oben sowohl die funktionalen Bestandteile inkl. der herstellerspezifischen Safety-Logik enthält, baut der hellgrüne Anteil inklusive Plattformmanagement und Shared Services weitestgehend auf auch in anderen Sektoren verbreiteten Komponenten auf.

Entsprechend existiert bei den Komponenten unterhalb des Safety-Layers ein hohes Potenzial zur Nutzung von COTS-Komponenten oder – bei Sektorspezifika – der sektorweiten OSS-Entwicklung.

Unter Letztere fällt auch die NHA-Komponente, die in Cloud4Rail erstmalig implementiert wurde. Auch wenn diese ggf. abhängig von der Umsetzung des Safety-Layers unterschiedliche Informationen bereitstellen muss, ist eine unternehmensübergreifende Nutzung und Weiterentwicklung aufgrund der überschaubaren Komplexität sehr vielversprechend.

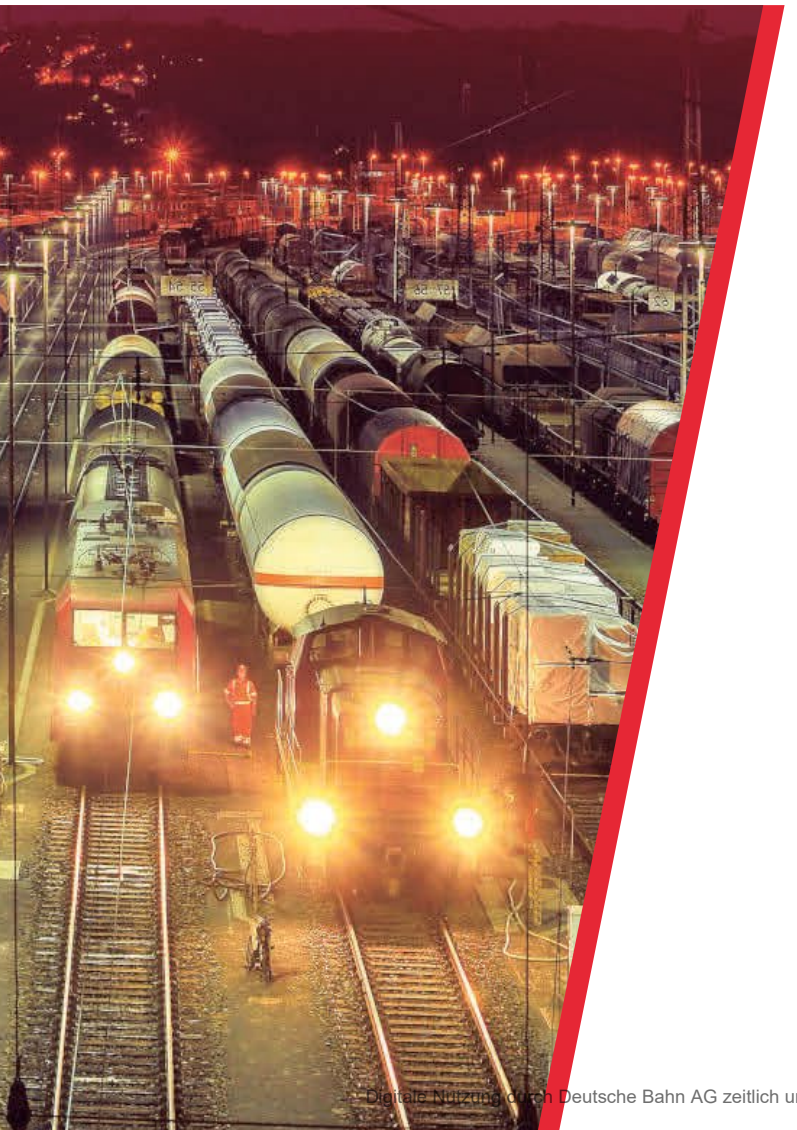
In einem ersten Schritt wurde die implementierte NHA-Komponente über den GitHub-Account der DB-InfraGO unter einer permissiven Lizenz dem Sektor zur Verfügung gestellt [7]. Im Anschluss soll gemeinsam mit interessierten Unternehmen z. B. innerhalb der Open Rail Association [8] eine auf die Bedürfnisse des Sektors ausgerichtete Governance-Struktur etabliert werden, um die Nachhaltigkeit, Planbarkeit und gemeinsame Entwicklungsmöglichkeiten für teilnehmende Organisationen langfristig zu sichern.

cluding considerations of intellectual property, mean that railway IT platforms within the OT context can be structured as shown in fig. 3. The upper (light blue) layer here contains the functional elements, including the manufacturer-specific safety logic, while the lower (light green) layer, including the platform management and shared services, relies largely on components that are also widely used in other industries.

Accordingly, there is significant potential below the safety layer to use COTS components or, where sector-specific adaptations are required, to develop them collaboratively as open-source solutions.

The NHA component, initially implemented in the Cloud4Rail project, is one such example. Although it may need to provide different types of information depending on the specific safety layer implementation, its relatively low complexity renders cross-company use and collaborative development highly promising.

The implemented NHA component has been made publicly available to the sector under a permissive licence via the DB InfraGO GitHub account [7] as an initial step. Going forward, a governance structure tailored to the sector's needs is planned in collaboration with interested stakeholders, for example within the Open Rail Association [8], so as to ensure long-term sustainability, predictability and joint development opportunities for participating organisations.



PINTSCH
Safety for Rail

Systemlösungen
für die Bahninfrastruktur

PINPROTEGIO. Bahnübergangstechnik.
PINCLIRIO. Achszähltechnik.
PINMOVIO. Stellwerks- und Rangiertechnik.
PINMOVIO. Weichenantrieb.
PINLUXON. Signale.
PINPOSITON. Fördertechnik.
PINCALIO. Weichenheizungen.
PINDIAGON. Diagnose.

InnoTrans
VISIT US
22.-25.9.26
HALLE 27
STAND 710

pintsch.net

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026

nance-Struktur aufgesetzt werden, um damit auch eine langfristigere Planbarkeit sowie eine potenzielle gemeinsame Weiterentwicklung für die beteiligten Unternehmen sicher zu stellen.

5 Nachweis technischer Machbarkeit

Im Projekt Cloud4Rail erfolgte der Nachweis der technischen Machbarkeit mit Fokus auf der technischen Integration in die Umgebungsbedingungen des Betreibers. Die Machbarkeit wurde hierbei auf der technischen Ebene ohne die Übernahme von sicherungstechnischen Aufgaben und ohne Zulassungen gezeigt, und dies erfolgte in drei Schritten:

- **Funktionale Integration:** Hierbei wurde sichergestellt, dass die Funktionalität der RBC auf der COTS-Hardware und im Zusammenspiel mit der Siemens Software-Safety-Plattform unter dem Produktnamen „Distributed Smart Safe System, DS3," die vorhandene Funktionalität bereitstellt. Anschließend wurde die RBC-Anwendung mit der DS3-Plattform in eine virtuelle Maschine integriert, um die Trennung von Hardware und Software zu vervollständigen. In diesem Schritt wurde auch die Funktionalität der NHA-Komponente integriert, welche Voraussetzung für eine zukünftige Anwendung mit Sicherheitsverantwortung ist.
- **Technische Integration in die On-Premises-Cloud der DB InfraGO:** Ein wesentliches Ziel der Forschungskooperation war die Implementierung einer sektorweit nutzbaren NHA-Komponente. Diese Komponente wurde in der Cloud der DB InfraGO mit einer Standard-Virtualisierungslösung installiert, um eine SIL4-fähige Rechnerinfrastruktur zu erzeugen. Wichtig war dabei, dass in dieser Infrastruktur die Rahmenbedingungen zum Betrieb von SIL4-Anwendungen geschaffen wurden, allerdings keine Sicherheitsnachweise oder Begutachtungen der Hardware- und Softwarekomponenten erforderlich sind. Ebenso können in dieser Infrastruktur virtuelle Anwendungen mit unterschiedlichen SIL-Anforderungen genauso wie Anwendungen ohne Sicherheitsbezug betrieben werden. Die Integration der NHA-Komponente in die Virtualisierung schafft die Voraussetzungen, um SIL4-Anwendungen zu betreiben, behindert aber keine Anwendungen, die diese Anforderungen nicht stellen. Anschließend wurde die virtualisierte RBC-Anwendung in dieser SIL4-fähigen Rechnerinfrastruktur betrieben. Ziel war dabei, verschiedene Hardwareausfälle und Recovery-Mechanismen zu erproben, um die Betriebsführung einer virtualisierten SIL4-Anwendung zu testen.
- **Betrieblicher Test in praktischer Umgebung:** Nach der Integration in die SIL4-fähige Infrastruktur der DB InfraGO wurde das RBC im Digitalen Testfeld Bahn im Erzgebirge in eine reale Bahnumgebung gebracht. In diesem Testschritt ging es darum, die Integration einer virtuellen RBC-Anwendung im Zusammenspiel mit den Komponenten der Streckeninfrastruktur (z. B. der Funkausrüstung) und der Züge zu erproben und zu demonstrieren. Das Ziel dieser technischen Machbarkeitsstudien war es, Erfahrungen zu sammeln, um On-Premises-Cloud-Lösungen in zukünftigen Technikgenerationen der DB InfraGO als Referenzarchitektur für die zentralen Systeme der LST festzulegen. Dabei lag der Fokus darauf, Erfahrungen mit den grundlegenden Fragen zur Wartung und Instandhaltbarkeit von virtualisierten SIL4-Anwendungen zu sammeln. Das Ziel dieses Projekts war die Schaffung einer Referenz, die im gesamten Sektor genutzt werden kann.

6 Zusammenfassung und Ausblick

Die Einführung einer standardisierten Trennung von Bahnanwendungen und IT-Plattformen mithilfe von Virtualisierung und der Aufbau moderner (On-Premises-)Cloud-Infrastruktur sind essenziell für den effizienten Rollout und Betrieb digitalisierter LST, mit

5 Proof of technical feasibility

Technical feasibility has been demonstrated in the Cloud4Rail project with a focus on the integration into the operator's existing environment. This feasibility was proven purely at a technical level, i.e. without taking on any safety responsibilities or obtaining any formal certifications, and undertaken in three steps:

- **Functional integration:** this step ensured that the RBC functionality could run on COTS hardware in combination with the Siemens' software safety platform, the "Distributed Smart Safe System" (DS3), while delivering the existing functionality. The RBC application, together with the DS3 platform, was then integrated into a virtual machine in order to complete the separation of hardware and software. The functionality of the NHA component, which is a prerequisite for future safety-critical deployment, was also integrated at this stage.
- **Technical integration into DB InfraGO's on-premises cloud:** a key objective of the research collaboration was to implement an NHA component that can be used across the entire sector. This component was deployed in the DB InfraGO cloud using a standard virtualisation solution to create a SIL4 capable computing infrastructure. Importantly, this infrastructure provides the necessary conditions for operating SIL4 applications but does not require any formal safety certification or an assessment of the underlying hardware and software components. At the same time, it also supports the operation of virtual applications with different safety integrity levels, as well as applications without any safety requirements. The integration of the NHA component into the virtualisation environment enables the use of SIL4 applications while not posing any burden to non-safety-critical applications. The virtualised RBC application was then operated within this SIL4 capable infrastructure. The objective was to test various hardware failure scenarios and recovery mechanisms in order to evaluate the operation of a virtualised SIL4 application.
- **Operational testing in a real-world environment:** following the integration into the SIL4 capable infrastructure, the RBC was deployed in DB's Digital Test Field in the Erzgebirge region, i.e. in a real operating environment. This testing phase focused on validating and demonstrating the interaction of the virtualised RBC with the trackside infrastructure components (such as the radio equipment) and trains. The goal of these technical feasibility studies was to gather experience that would enable on-premises cloud solutions to become the standard platform for central signalling systems in future generations of DB InfraGO technology. In particular, the focus was on gaining insights into the maintenance and serviceability aspects of the virtualised SIL4 applications. Ultimately, the project aimed to establish a reference architecture that could be adopted and utilised across the railway sector.

6 Summary and outlook

The introduction of a standardised separation between railway applications and IT platforms through virtualisation, together with the deployment of modern (on-premises) cloud infrastructure, is essential for the efficient rollout and operation of digital signalling systems. This approach offers significant cost advantages, increased flexibility and consequently faster deployment.

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026

erheblichen Kostenvorteilen sowie einem Zugewinn an Flexibilität und damit Geschwindigkeit im Rollout.
Im Projekt Cloud4Rail wurde erstmals, aufbauend auf dem Sektorkonsens in Europe's Rail, die avisierte Gesamtarchitektur aus Bahnanwendung, Safety-Layer, Virtualisierung und Hardware umgesetzt und damit die technische Machbarkeit einer virtualisierten SIL4-Applikation nachgewiesen. Hierzu erfolgte auch erstmalig die Umsetzung einer sogenannten NHA-Komponente, die nun permissiv dem Sektor zur Verfügung gestellt wird und einen initialen Schritt in Richtung einer kollaborativen OSS-Entwicklung für unvermeidbare bahnspezifische Komponenten darstellt.
Die Arbeiten in Cloud4Rail dienen nun als Grundlage für die geplante Pilotierung eines ersten Stellwerkskerns in einer On-Premises-Cloud der DB InfraGO. Ergänzt werden sollen die Arbeiten durch die weitere Spezifikation und Implementierung von Diensten, die für das automatisierte Deployment, Konfiguration und Update von bahnbetrieblichen Funktionen und der darunterliegenden Cloud benötigt werden: Es ist geplant, den OSS-Gedanken im Förderprojekt FP2 R2DATO-2 ab Oktober 2026 in Partnerschaft mehrerer Bahnen und Bahnhersteller fortzuführen. ■

Danksagung
Die vorliegende Publikation sowie zugrundeliegende Arbeiten sind im Rahmen des im IPCEI-CIS geförderten Projekts Cloud4Rail entstanden. Das Projekt ist gefördert vom Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages sowie finanziert von der Europäischen Union.

The target architecture (comprising the railway application, safety layer, virtualisation and hardware) has been implemented for the first time within the Cloud4Rail project building on the sector-wide consensus established in Europe's Rail. This has successfully demonstrated the technical feasibility of a virtualised SIL4 application. As part of this work, a so-called Native Hardware Access component was also implemented for the first time. It has now been made available to the sector under a permissive license, representing an initial step toward collaborative open-source development for unavoidable railway-specific components.
The work carried out in Cloud4Rail is now serving as the foundation for the planned pilot deployment of an initial interlocking core within an on-premises cloud environment at DB InfraGO. These efforts will be supplemented by the further specification and implementation of the services required for the automated deployment, configuration and update of railway operations functions and the underlying cloud infrastructure. This follow-up work is scheduled to begin in October 2026 within the FP2 R2DATO-2 funding project, in partnership with multiple railway operators and industry manufacturers and will continue to embrace the aforementioned open-source approach. ■

Acknowledgement
This publication and the underlying work have been carried out within the framework of the Cloud4Rail project, funded under the IPCEI-CIS initiative. The project is supported by the German Federal Ministry for Economic Affairs and Energy following a resolution of the German Bundestag and is co-financed by the European Union.

AUTOREN | AUTHORS

Dr. Jonas Rebstadt
IT Platform Architect
DB InfraGO AG
Anschrift / *Address*: EUREF-Campus 17, D-10829 Berlin
E-Mail: jonas.rebstadt@deutschebahn.com

Sonja Steffens
Product Manager Safety Platforms
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: sonja.steffens@siemens.com

Dr. Martin Mitzkus
System Manager DLST
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: martin.mitzkus@siemens.com

Dr. Patrick Marsch
Head of Technical System Architecture,
Technology Foundations and IT Platforms
DB InfraGO AG
Anschrift / *Address*: EUREF-Campus 17, D-10829 Berlin
E-Mail: patrick.marsch@deutschebahn.com

LITERATUR | LITERATURE

[1] Fox, M.; Mayer-Buschmann, O.; Marsch, P.; Wissmann, J.; König, N.; Ventas, I. A.; Venturi, G.; Inzirillo, F.; Rozijn, P.; Martin, T.; Steffens, S.; Bernburg, T.: „D26.3 – Final Modular Platform requirements, architecture and specification," 25.07.2025. [Online]. Available: 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]
[2] Heine, A.; Marsch, P.; Rebstadt, J.: „Die Migration der Leit- und Sicherungstechnik in ein modernes IT- und Cloud-System," SIGNAL+DRAHT 11/2025, S. 45-53
[3] Ansar, Z.; Wissmann, J.: „Virtualisierte Safety-Architekturen in der Leit- und Sicherungstechnik," SIGNAL+DRAHT 4/2026, S. 14-20
[4] Rebstadt, J.; Schumacher, C.; Hetze, S.: „Einsatz von Open-Source-Software im Eisenbahnsektor," Deine Bahn 05/2026
[5] Finley, K.: „github.com," 14.04.2021. [Online]. Available: https://github.com/readme/featured/nasa-ingenuity-helicopter. [Zugriff am 02.06.2026]
[6] VDA, „Pressemitteilung VDA," 07.01.2026. [Online]. Available: https://www.vda.de/de/presse/Pressemeldungen/2026/260107_PM_Innovation-im-Automotive-Sektor-durch-offene-Zusammenarbeit. [Zugriff am 06.02.2026]
[7] DB InfraGO AG, „Official GitHub organisation of DB InfraGO AG," [Online]. Available: https://github.com/dbinfrago. [Zugriff am 26.05.2026].
[8] OpenRail Association, [Online]. Available: https://openrailassociation.org/. [Zugriff am 06.02.2026]

Digitale Nutzung durch Deutsche Bahn AG zeitlich unbefristet genehmigt durch DVV Media Group, 2026