RailChain – Anwendung von Distributed-Ledger-Technologien im Bahnbetrieb

RailChain – the application of distributed ledger technologies in railway operations

Jens Braband | Rüdiger Kapitza | Andreas Polze | Ingo Schwarzer

Im Projekt „RailChain" wurde ein verteilter Juridical Recorder entworfen, der auf einem echtzeitfähigen verteilten Konsensprotokoll basiert und als „Distributed Ledger" (Softwareimplementierung eines verteilten Kassenbuches) an Bord des „Advanced TrainLab" von DB Systemtechnik (ICE-TD 605 017) umgesetzt wurde. Neben Details zur Architektur und zum Konsensprotokoll werden hier auch zusätzliche Einsatzfälle besprochen, die weit über das Fahrzeug hinausgehen und dank EULYNX und RCA auch Zustandsinformationen von Feldelementen und Systemkomponenten aufzeichnen. So lässt sich nachvollziehbar und unveränderlich das Zusammenspiel von ortsfesten ETCS-Komponenten (European Train Control System – ETCS) wie Balisen, GSM-R/FRMCS-Nachrichten und Radio Block Center (RBC) ebenso dokumentieren wie die Verarbeitung von ETCS-Befehlen auf der Fahrzeugseite. Letztlich wird damit die Grundlage für eine vertrauenswürdige Datenwirtschaft sowie für Schritte hin zum automatisierten Bahnbetrieb (Automatic Train Operation – ATO) gelegt.

1 Motivation

In der europäischen EULYNX-Initiative arbeiten 13 Eisenbahninfrastrukturunternehmen mit dem Ziel zusammen, Schnittstellen und Feldelemente des digitalen Leit- und Sicherungssystems zu standardisieren. Die ersten EULYNX-Projekte laufen seit 2014. Die Veröffentlichung der ersten vollständigen Versionen der Schnittstellenstandards erfolgte im Dezember 2017 (Baseline 2). Dem folgten Aktualisierungen (Baseline 3) in 2018 und 2019. EULYNX setzt konsequent auf die Prinzipien der modellbasierten Systementwicklung.

Über die EULYNX-Schnittstellenbeschreibungen hinaus geht der RCA-Ansatz. RCA steht dabei für Reference CCS Architecture – und beschreibt einen Ansatz, die Command, Control & Signaling (CCS, Leit- und Sicherungstechnik – LST)-Architekturen verschiedener Infrastrukturbetreiber zu vereinheitlichen. RCA legt die Grundlagen für den automatischen Zugbetrieb (Automatic Train Operation – ATO) basierend auf den CCS-Architekturen. RCA enthält Konzepte für die Migration, Adaption und Weiterentwicklung (Versionierung) von CCS-Systemen. Dabei werden aktuelle Techniken aus dem Feld der Betriebssysteme und des Rechnerbetriebs eingesetzt, wie Hardware Abstraction Layers (HAL), adaptive Kommunikationsprotokolle oder kontext-basierende Protokolle.

Mit dem Ansatz, Schnittstellen für zukünftige CCS-Systeme zu definieren und zu vereinheitlichen geht der Wunsch einher, das Management von CCS-Systemen über ihre gesamte Lebensdauer zu vereinfachen und dabei Kosten zu senken. Anders als bei Hardwarekomponenten, die eine Lebensdauer im Feld von 25 - 60 Jah-

A distributed juridical recorder has been designed in the "RailChain" project based on a real-time distributed consensus protocol and has been implemented as a distributed ledger (the software implementation of a distributed cash book) on board DB Systemtechnik's "Advanced TrainLab" (ICE-TD 605 017). In addition to any details on the architecture and the consensus protocol, additional use cases that go far beyond the vehicle and, thanks to EULYNX and RCA, also record the status information of the field elements and system components are discussed here. In this way, the interaction of ETCS (European Train Control System) trackside components, such as balises, GSM-R/FRMCS messages and Radio Block Centre (RBC), can be documented comprehensibly and unalterably, as can the processing of any ETCS commands on the vehicle side. Ultimately, this will lay the foundation for a trustworthy data economy and for the steps towards automatic train operations (ATO).

1 Motivation

13 rail infrastructure companies are working together in the European EULYNX initiative with the aim of standardising the interfaces and field elements of the digital control and safety system. The first EULYNX projects have been running since 2014. The publication of the first complete versions of the interface standards took place in December 2017 (Baseline 2). This was followed by updates (Baseline 3) in 2018 and 2019. EULYNX consistently relies on the principles of model-based system development.

The RCA approach goes beyond the EULYNX interface descriptions. RCA stands for Reference CCS Architecture and it describes an approach to standardising the command, control & signalling (CCS) architectures of different infrastructure managers. RCA lays the foundations for automatic train operation (ATO) based on CCS architectures. RCA contains concepts for the migration, adaptation and further development (versioning) of CCS systems. Current techniques from the field of operating systems and computer operation are being used, such as hardware abstraction layers (HAL), adaptive communication protocols or context-based protocols.

The approach to defining and standardising the interfaces for future CCS systems is accompanied by the desire to simplify the management of CCS systems over their entire service life and to reduce the costs in the process. Unlike hardware components, which can have a service life of 25–60 years,

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

ren erreichen können, sind Softwarekomponenten in einem CCS-System nach fünf Jahren veraltet und nach 15 Jahren nicht mehr wartbar. Einheitliche Schnittstellen zu Komponenten vermeiden Herstellerabhängigkeiten und – viel wichtiger noch im Sinne politischer Initiativen wie der „Starken Schiene" – bieten das Potenzial, in den kommenden Jahren das Tempo der Digitalisierung signifikant zu erhöhen.

Die Anwendung von Ansätzen aus der Softwaretechnik, wie kontinuierliche Integration und Versionierung, bietet die Chance, über die gesamte Lebensdauer von Komponenten ein nachvollziehbares Monitoring des Systemzustandes zu implementieren und von einer zeitbasierten Wartung auf zustandsbasierte Wartung zu wechseln. Dies verspricht Kostensenkungen.

Nach dem initialen Proof-of-Concept eines Digitalen Stellwerks (DSTW) in Annaberg-Buchholz, das Anfang 2018 in Betrieb ging und noch nicht EULYNX-konform ausgelegt ist, gibt es derzeit bei der Deutschen Bahn AG (DB) vier Vorserienprojekte, die bis 2022 in Betrieb gehen sollen. Dies sind die digitalen Stellwerke in Warnemünde (Siemens Mobility, in Betrieb), Meitingen-Mertingen (Thales), Harz-Weser-Netz / Braunschweig Süd / Südharz und Koblenz-Trier. Die ersten beiden Vorserienprojekte setzen dabei durchgängig auf Komponenten eines Herstellers. Der Nachweis, dass LST-Projekte auf Basis von EULYNX herstellerübergreifend implementiert werden können, steht derzeit noch aus.

In der OCORA-Initiative (Open CCS On-board Reference Architecture) unternehmen die europäischen Eisenbahnverkehrsunternehmen DB, SNCF, NS, ÖBB und SBB den Versuch, Architektur und Schnittstellen für die nächste Generation der ETCS-Fahrzeugausrüstung zu standardisieren. OCORA beschreibt ein fahrzeugseitiges, komponentenbasiertes und verteiltes IT-System mit wohldefinierten Anforderungen an die Zuverlässigkeit und Nachvollziehbarkeit von Komponenten.

EULYNX und OCORA skizzieren herstellerübergreifende, heterogene IT-Systeme. Solche Systeme bergen eine neue Herausforderung, die bislang im Kontext der zugelassenen, sicherheitsrelevanten LST der Bahn weder strecken- noch fahrzeugseitig adressiert werden musste: Logbuch-Implementierungen, wie der gängige Juridical Recorder (Juridical Recorder Unit – JRU; wie die Blackbox im Flugzeug) auf Fahrzeugen, können nicht mehr als zentrale Systemkomponente eines einzigen Herstellers umgesetzt werden. Vielmehr bieten sich verteilte Konsensprotokolle als probates Mittel an, um unveränderliche (gerichtsfeste) Zustandsinformationen über eine Vielzahl von Systemkomponenten herstellerübergreifend speichern zu können. Gleichzeitig existiert mit OCORA und EULYNX ein fahrzeug- und streckenseitiger Architekturentwurf, auf den Implementierungen verteilter Konsensprotokolle aufsetzen können.

2 Grundlagen zur Distributed Ledger Technology

Distributed Ledger-Technologien (DLT) – dazu zählt auch die Blockchain – definieren verteilte Datenbanken und stellen ein digitales Protokoll für Transaktionen zwischen Geschäftspartnern dar, ohne dass ein Mittelsmann wie etwa eine Bank oder ein Bezahlsystem wie PayPal beteiligt sein müsste. Überall dort, wo der Transfer von Daten oder Werten erfasst werden muss, könnte die DLT z. B. durch computerüberwachte Verträge (Smart Contracts) Prozesse vereinfachen, automatisieren und sicherer machen. Drei mathematische Fachrichtungen sind hier auf neue und elegante Weise verknüpft: Kryptografie, verteilte Systeme und Spieltheorie. In einer Blockchain ist die zeitliche Abfolge von Transaktionen exakt und jederzeit öffentlich nachvollziehbar.

software components in a CCS system become obsolete after five years and unmaintainable after 15 years. Uniform interfaces to components avoid manufacturer dependencies and – much more importantly in terms of political initiatives such as "Strong Rail" – offer the potential to significantly increase the pace of digitalisation in the coming years.

The application of approaches from software engineering, such as continuous integration and versioning, offers the opportunity to implement the traceable monitoring of the system status over the entire service life of the components and to switch from time-based maintenance to condition-based maintenance. This promises cost reductions.

After the initial proof-of-concept of a digital rail signalling system in Annaberg-Buchholz, which went into operation at the beginning of 2018 and is not yet designed to be EULYNX-compliant, Deutsche Bahn AG (DB) currently has four pre-series projects that are scheduled to go into operation by 2022. These are the digital rail signalling systems in Warnemünde (Siemens Mobility, in operation), Meitingen-Mertingen (Thales), Harz-Weser-Netz / Braunschweig Süd / Südharz and Koblenz-Trier. The first two pre-series projects are based entirely on components from one manufacturer. Proof that CCS projects based on EULYNX can be implemented across manufacturers is currently still pending.

The DB, SNCF, NS, ÖBB and SBB European railway undertakings are attempting to standardise the architecture and interfaces for the next generation of ETCS on-board equipment in the OCORA initiative (Open CCS On-board Reference Architecture). OCORA describes an on-board, component-based distributed IT system with well-defined requirements for component reliability and traceability.

EULYNX and OCORA outline multi-vendor, heterogeneous IT systems. Such systems pose a new challenge, which to date has not had to be addressed on either the track side or on-board within the context of the approved, safety-relevant railway CCS systems: logbook implementations, such as the common juridical recording unit (JRU: similar to a black box in an aircraft) on vehicles, can no longer be implemented as a central system component from a single manufacturer. Instead, distributed consensus protocols are an effective means of storing unchangeable (court-proof) status information about a large number of system components across manufacturers. At the same time, OCORA and EULYNX provide an on-board and trackside architecture design, on which implementations of distributed consensus protocols can be based.

2 The fundamentals of distributed ledger technology

Distributed ledger technologies (DLT) (which include Blockchain) define distributed databases and provide a digital protocol for transactions between business partners without the need for an intermediary such as a bank or a payment system like PayPal. Wherever the transfer of data or values needs to be recorded, DLT could simplify, automate and make the processes more secure, for example through computer-monitored contracts (smart contracts). Three mathematical disciplines are linked here in a new and elegant way: cryptography, distributed systems and game theory. The chronological sequence of the transactions in a blockchain is exact and publicly traceable at any time.

One well-known blockchain application is the Bitcoin digital currency. The public focus at the moment is mainly on finan-

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

Eine bekannte Blockchain-Anwendung ist etwa die digitale Währung Bitcoin. Im öffentlichen Fokus stehen derzeit vor allem finanzielle und rechtliche Transaktionen, wo die Vorteile von dezentralen Datenbanken mit Peer-to-Peer-Ansätzen über Unternehmensgrenzen hinweg zum Tragen kommen.

Die Implementierung einer Blockchain für das lokale Netzwerk einer Eisenbahnanlage (z. B. Stellwerk oder Zug) erlaubt es, die im verteilten System entstehenden Daten nachweislich in Echtzeit zu protokollieren. Dabei können eisenbahnspezifische Randbedingungen ausgenutzt werden, um anwendungsspezifische Anpassungen an Standard-Blockchains vorzunehmen. Dies können Änderungen bei den sogenannten Einigungsprotokollen (Konsensprotokolle) sein. Einigungsprotokolle dienen dem Zweck, eine Wahrheit über die Daten unter Übereinstimmung aller Teilnehmer zu gewährleisten, sind in vielfältigen Ausprägungen verfügbar (z. B. die Verwendung von Einigungsprotokollen wie Proof of Authority, Proof of Kernel Work oder Proof of Stake) und haben Einfluss auf verschiedene Faktoren, wie beispielsweise Datensicherheit, Skalierbarkeit oder Geschwindigkeit in der Verarbeitung.

Das Ziel des mFUND-geförderten Projektes "RailChain" (siehe „Förderhinweis" am Ende des Beitrags) ist in erster Linie die Spezifikation und Implementierung eines Blockchain-Demonstrators für das Eisenbahnwesen, der eine Basis-Funktionalität umsetzt, auf der Echtzeitanwendungen ablaufen können, sowie dessen Erprobung in einem geeigneten Testfeld. Das RailChain-Konsortium vereint die Partner DB (DB Systel, DB Netze, DB Erzgebirgsbahn), Siemens Mobility GmbH, Siemens AG, Technische Universität Braunschweig, Hasso-Plattner-Institut für Digital Engineering GmbH (HPI) / Universität Potsdam, TÜV Rheinland InterTraffic GmbH und Spherity GmbH.

RailChain demonstriert, wie ein – bislang obligatorischer – physischer Juridical Recorder eingespart und durch einen verteilten,

cial and legal transactions, where the advantages of decentralised databases with peer-to-peer approaches across company boundaries come into play.

The implementation of a blockchain for the local network of a railway installation (e.g. a signal box or train) allows the data generated in the distributed system to be verifiably logged in real time. Railway-specific boundary conditions can be exploited to make application-specific adaptations to standard blockchains. These can involve changes in the so-called agreement protocols (consensus protocols). Agreement protocols serve the purpose of guaranteeing a truth about the data with the agreement of all the participants. They are available in many forms (e.g. the use of agreement protocols such as Proof of Authority, Proof of Kernel Work or Proof of Stake) and influence various factors, such as data security, scalability or processing speed.

The aim of the "RailChain" mFUND-funded project (see "Funding reference" at the end of the article) is primarily to specify and implement a blockchain demonstrator for the railway sector that implements a basic functionality, on which real-time applications can run, and to test it in a suitable test field. The RailChain consortium has brought together the partners DB (DB Systel, DB Netze, DB Erzgebirgsbahn), Siemens Mobility GmbH, Siemens AG, the Braunschweig University of Technology, Hasso-Plattner-Institut für Digital Engineering GmbH (HPI) / Universität Potsdam, TÜV Rheinland InterTraffic GmbH and Spherity GmbH.

RailChain demonstrates how a – previously mandatory – physical juridical recorder can be dispensed with and replaced with a distributed, software-based juridical blockchain recorder (JBR). The effectiveness of the railway is increased by using or adapting standard components to a large extent. In addition to the technical transferability to railway technology,

Bild 1: Das Advanced TrainLab
Fig. 1: The Advanced TrainLab

Quelle / *Source*: Andreas Polze

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

softwarebasierten Juridical Blockchain Recorder (JBR) ersetzt werden kann. Durch weitgehenden Einsatz bzw. Anpassung von Standardkomponenten wird damit die Effektivität der Eisenbahn erhöht. Neben der technischen Übertragbarkeit in die Bahntechnik soll auch die Wirtschaftlichkeit gezeigt und in Use Cases weiter konkretisiert werden.

Folgende Use Cases sind geplant:

- Use Case 1: Asset Identity inklusive Asset Tracking
- Use Case 2: Daten-Logger ohne Echtzeitanforderungen
- Use Case 3: JBR mit Echtzeitanforderungen für die Eisenbahnfahrzeuge, das ETCS, das DSTW und die Betriebszentralen (BZ)

Die Funktionalität der Blockchain-Technologie entspricht den Kernkonzepten:

- Peer-to-Peer-Netzwerk (in einem zukünftigen Railway Internet of Things)
- Shared Recording
- Consensus Validation
- Immutable Storage

Daher sollen im Projekt erste Anwendungsfälle für diese Technik auch in Eisenbahnanwendungen realisiert, z. B. auf dem Advanced TrainLab (Bild 1), und durch Mitwirkung in branchenspezifischen Gremien die Einsatzmöglichkeit der Technologie für den Eisenbahnbereich sichergestellt werden. Es ist zu erwarten, dass die hier untersuchten neuartigen Ansätze für verteilte Datenbanken und die Verarbeitung der erfassten Daten völlig neue Verkehrs- und Mobilitätskonzepte entstehen lassen werden. Neben der technischen Übertragbarkeit in die Bahntechnik soll zudem auch die Wirtschaftlichkeit der DLT gezeigt werden.

3 Anforderungen

In Bild 2 ist am Beispiel eines heute verbauten Juridical Recorders [2] erkennbar, welche weiteren Vorteile ein JBR bringen könnte. Besonders hervorgehoben ist der Bereich, in dem sich der besonders geschützte Speicher befindet. Derzeit ist ein Datenexport nur über eine RS232-Schnittstelle [2] spezifiziert. Mit einem JBR könnte ein vereinfachter Zugriff auf die Daten ermöglicht sowie eine höhere Vertrauenswürdigkeit der Daten erreicht werden, da die Daten in einem JBR unveränderlich und kryptographisch gesichert abgelegt werden. Dies könnte auch den Wert der Daten steigern sowie den Einstieg in eine wirtschaftliche Verwertung der Daten ebnen.

Die Echtzeitfähigkeit (<1 Sekunde Block-Zyklus-Zeit) ist eine der Kernanforderungen für einen Juridical Recorder. Mit den üblichen DLT-Anwendungen, vgl. zum Beispiel BitCoin oder Ethereum, sind solche Anforderungen nicht realisierbar, da deren Performance im Bereich von mehreren Minuten bzw. vielen Sekunden liegt und auch architekturbedingt nicht wesentlich beschleunigt werden kann. Hinzu kommt noch, dass bei normalen DLT-Anwendungen die Finalität nur stochastisch, aber nicht deterministisch garantiert werden kann. Dies bedeutet praktisch, dass es Teilnehmer geben könnte, die auch nach einer längeren Zeit vom allgemeinen Konsens des Netzwerks abweichen könnten, wenn auch nur mit einer geringen Wahrscheinlichkeit. Für eine JBR-Anwendung sollte die Finalität aber deterministisch sein. Dies macht die Entwicklung eines spezifischen JBR-Protokolls unumgänglich.

Eine wichtige Anforderung ist die Zuverlässigkeit. Nach dem Lastenheft der DB [4] wird für eine JRU eine mittlere Zeit zwischen Ausfällen (Mean Time between Failures – MTBF) von 180 000 Stunden gefordert bei einer mittleren Fehlerbehebungszeit (Mean Time to Repair – MTTR) von 18 Stunden, dies entspricht ei-

the economic efficiency will also be demonstrated and further concretised in use cases.

The following use cases are planned:

- Use case 1: Asset identity, including asset tracking
- Use case 2: A data logger without any real-time requirements
- Use case 3: A JBR with real-time requirements for the railway vehicles, the ETCS, the DSTW, and the operations centres (OC)

The functionality of blockchain technology corresponds to the core concepts:

- a peer-to-peer network (in a future Railway Internet of Things)
- shared recording
- consensus validation
- immutable storage

Therefore, the first use cases for this technology will also be realised in railway applications in the project, e.g. on the Advanced TrainLab (fig. 1), and the possibility of using the technology in the railway sector will be ensured through participation in industry-specific committees. It is to be expected that the novel approaches to distributed databases and the processing of the collected data being investigated here will give rise to completely new traffic and mobility concepts. The economic viability of DLT should also be demonstrated in addition to its technical transferability to railway technology.

3 Requirements

Fig. 2 shows the further advantages that a JBR could bring, using the example of a currently installed juridical recorder [2]. The area where the specially protected memory is located is highlighted in particular. Currently, data export is only specified via an RS232 interface [2]. With a JBR, data access could be simplified and data trustworthiness could be enhanced, since the data is stored unchangeably and is cryptographically secured in the JBR. This could also increase the value of the data and pave the way for its commercial utilisation.

Real-time capability (<1 second block cycle time) is one of the core requirements for a juridical recorder. Such requirements cannot be met by the usual DLT applications, for example BitCoin or Ethereum, since their performance falls within the range of several minutes or many seconds and also cannot be significantly accelerated for architectural reasons. In addition, finality can only be guaranteed stochastically in normal DLT applications, but not deterministically. In practice this means that there could be participants who could deviate from the network's general consensus even after a longer period of time, albeit with only a low probability. However, the finality for a JBR application should be deterministic. This makes the development of a specific JBR protocol inevitable.

Reliability is an important requirement. According to the DB specifications [4], a JRU is required to have a mean time between failures (MTBF) of 180,000 h with a mean time to repair (MTTR) of 18 h, which corresponds to an availability A of approx. 0.9999. In the event of an accident, the JRU is particularly protected against shock and fire, e.g. against fire up to 700 °C for 5 minutes, due to its special hardware.

Thus, reliability is a core requirement, if one wants to replace a traditional JRU in special hardware (the especially hardened module is highlighted in fig. 2) with a distributed solution (JBR) in standard hardware. Redundancy is to be achieved

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

ner Verfügbarkeit A von ca. 0,9999. Im Fall eines Unfalls ist die JRU aufgrund ihrer Spezialhardware z. B. besonders vor Schock und Brand geschützt, z. B. gegen Feuer bis zu 700 °C über 5 Minuten.
Wenn man also eine herkömmliche JRU in Spezialhardware (in Bild 2 ist das speziell gehärtete Modul hervorgehoben) durch eine verteilte Lösung (JBR) in Standardhardware ersetzen will, ist die Zuverlässigkeit eine Kernanforderung. Dabei soll mit der Verteilung im Zug (z. B. vorne, mittig und hinten) eine Redundanz erreicht werden, sodass die Anforderungen an die Verlässlichkeit der einzelnen Hardwarekomponenten verringert werden können. Der Vorteil der redundanten Lösung besteht darin, dass es im Normalbetrieb quasi 100 % Verfügbarkeit gibt, aber es bei Unfällen in seltenen Fällen dazu kommen kann, dass die Daten in allen Replikaten unbrauchbar sind. Dass man mit dem JBR auf eine mindestens gleiche Zuverlässigkeit kommt, wurde bereits in einer eigenen Fachveröffentlichung nachgewiesen [4]. Beim JBR reicht aber die Bergung nur eines intakten Replikaten für eine rechtssichere Aufzeichnung.
Da auf dem Zug aufgrund der Zuverlässigkeitsanforderungen drei oder vier Replikaten notwendig werden, lassen sich auch anspruchsvolle Security-Anforderungen fast ohne Mehraufwand erfüllen, z. B. dass einer der Replikaten gehackt werden könnte, sollte die JBR-Funktionalität auf den anderen Replikaten nicht beeinträchtigt werden. Gleichzeitig soll es zur Erhöhung der Zuverlässigkeit möglich sein, die JBR-Aufzeichnungen zyklisch oder ereignisgesteuert an die Streckenseite zu übertragen, damit die Daten dort auch für andere Zwecke zeitnah weiterverarbeitet werden können.
Eine weitere wichtige Anforderung besteht darin, dass die JBR-Funktionalität ohne zusätzliche Hardware realisiert werden soll. Die Realisierung erfolgt in Software, die bisher verwendete JRU wird obsolet. D. h. es handelt sich um ein echtes Digitalisierungsprojekt. Dies wird insbesondere durch neue Architekturen wie OCORA oder EULYNX möglich.

4 Verteiltes Einigungsprotokoll als Basis für den JBR

Für die Umsetzung des JBR wurde wie zuvor begründet ein Einigungsprotokoll entwickelt, welches auf die Tolerierung von beliebigen, auch als Byzantinisch bezeichnete, Fehler ausgelegt ist. Dies ermöglicht es, JBR-Replikate kolloziert mit anderer für den Betrieb relevanter Software auf bereits vorhandenen Systemen zu betreiben. Selbst wenn einzelne Replikate durch einen Software- oder Hardwarefehler sich nicht mehr protokollkonform verhalten, werden weiterhin Nachrichten zuverlässig durch den Verbund des JBR aufgezeichnet. Weiterhin wird lediglich ein schwach echtzeitfähiges Kommunikationssystem benötigt. Im Falle des entwickelten Prototyps wurde hierzu auf Ethernet und TCP / IP zurückgegriffen. Dies ermöglicht es beispielsweise, wie im Testaufbau nachgewiesen, Nachrichten eines Multifunction Vehicle Bus (MVB) zu protokollieren, ohne eine Änderung an dessen Kommunikationsplan vorzunehmen. Auch eine Einspeisung von Nachrichten anderer Kommunikationssysteme wird unterstützt.
Die Architektur des JBR setzt sich aus drei Kernkomponenten zusammen:

- Verteilte Annahme der Nachrichten des Kommunikationssystems
- Einigung und Aufzeichnung der zu protokollierenden Nachrichten
- Transfer der protokollierten Daten in streckenseitige sichere Datenzentren

Im Rahmen des Empfangs der Nachrichten durch die einzelnen Replikate des JBR kann es zu Verfälschungen oder Verlust von Nachrichten kommen. Dies bedeutet, dass nicht alle Nachrichten jedem

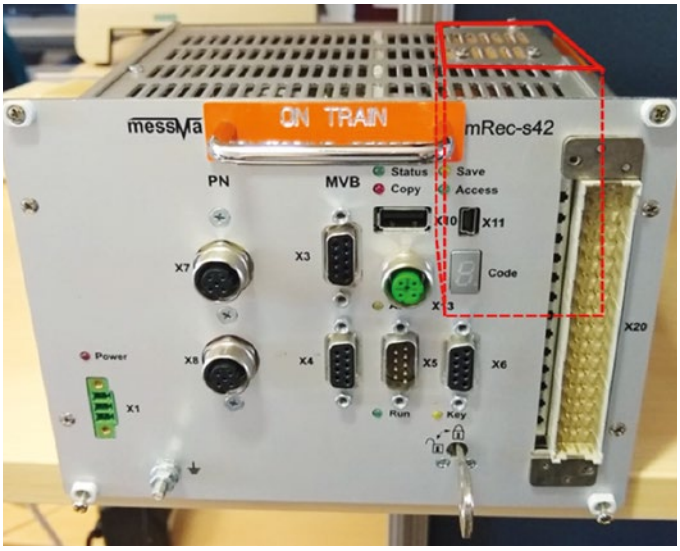

Bild 2: Beispiel für einen Juridical Recorder
Fig. 2: An example of a juridical recorder
Quelle / *Source*: Siemens Mobility

with the distribution in the train (e.g. front, centre and rear) so that the reliability requirements for the individual hardware components can be reduced. The advantage of the redundant solution is that there is quasi 100 % availability under normal operations, but the data in all the replicas may become unusable in rare cases in the event of any accidents. The fact that at least the same reliability can be achieved with the JBR has already been demonstrated in a separate technical publication [4]. With the JBR, however, the recovery of only one intact replica is sufficient for a legally compliant record.
Since three or four replicas are necessary on the train due to the reliability requirements, even the most demanding security requirements can be fulfilled almost without any additional effort, e.g. if one of the replicas is hacked, the JBR functionality on the other replicas should not be affected. At the same time, in order to increase reliability, it should be possible to transmit the JBR recordings to the trackside cyclically or in an event-controlled manner, so that the data can also be promptly further processed there for other purposes.
Another important requirement involves the fact that the JBR functionality should be realised without any additional hardware. The realisation is performed in the software and the JRU used to date thus becomes obsolete. In other words, it is a genuine digitalisation project. This has particularly been made possible by new architectures such as OCORA or EULYNX.

4 A distributed agreement protocol as the basis for the JBR

An agreement protocol, which is designed to tolerate any errors and is also referred to as Byzantine, has been developed for the implementation of the JBR as previously substantiated. This allows JBR replicas to run on existing systems, collocated with other software relevant to the operation. Even if individual replicas no longer behave in accordance with the protocol due to a software or hardware error, messages will continue to be reliably recorded by the JBR network. Furthermore, only a weakly real-time capable communication system is required. The Ethernet and TCP/IP were used for this purpose in the case of the developed prototype. This makes it possible, for example, to log messages from a Multifunction Vehicle Bus

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

Replikat direkt nach Abnahme vom Bussystem zur Verfügung stehen. Ziel ist es aber, dass alle Nachrichten, welche von fehlerfreien Replikaten empfangen werden, auch verteilt aufgezeichnet werden. Entsprechend haben alle Replikate das Vorschlagsrecht für die zu protokollierenden Daten. Davon machen Replikate Gebrauch, wenn eine Nachricht, die sie über den Bus empfangen haben, nicht im Rahmen einer gewissen Zeitspanne zur Einigung vorgeschlagen wird.

Die Eignung der vorgeschlagenen Nachrichten erfolgt dabei unter Verwendung einer ergänzten Variante des in „Practical Byzantine Fault Tolerance" veröffentlichten dreiphasingen Einigungsprotokolls. Spezifisch wird hierbei die Variante verwendet, welche Nachrichten mittels asymmetrischer Kryptographie signiert. Diese Vorgehensweise ist sinnvoll, da sie erfordert, dass ein Quorum der Replikate des JBR die Nachricht signiert. Wie für den Algorithmus vorgesehen, müssen hierzu N = 3f+1 Replikate vorhanden sein, von denen nur f beliebig fehlerhaft sein dürfen. D. h. wenn nicht genügend Replikate am Protokoll teilnehmen, kann keine Nachricht mehr aufgezeichnet werden. Dieser Fakt schützt die JBR vor nachträglicher Veränderung auch im Kontext eines Unfalls. Selbst unter der Annahme, dass nur noch ein Replikat geborgen werden kann, können keine Nachrichten im Nachhinein verändert werden. Einzig und allein eine Löschung von Ereignissen ist möglich.

Als dritte und letzte Komponente ist eine Übertragung der protokollierten Daten in Form der Blocks der Blockchain in gesicherte Datenzentren notwendig. Dies hat prinzipiell zwei Gründe: Freigabe von Speicherplatz der beteiligten Systeme im Zug und eine zeitnahe Analyse der Daten im Datenzentrum. Durch das entwickelte Transferprotokoll erfolgt eine sichere bestätigte Annahme der Daten durch mehrere Datenzentren, bevor eine Löschung auf den Replikaten im Zug vorgenommen werden kann.

Techniken der Verschlüsselung und Pseudonymisierung werden eingesetzt, um sicherzustellen, dass personenbezogene Daten

(MVB) without changing its communication plan, as demonstrated in the test setup. Feeding in messages from other communication systems is also supported.

The architecture of the JBR is made up of three core components:

- the distributed acceptance of the communication system's messages
- the agreement and recording of the messages to be logged
- the transfer of the logged data to secure trackside data centres

Messages may be corrupted or lost during the course of the message reception by the individual JBR replicas. This means that not all the messages will be available to every replica immediately after acceptance from the bus system. However, the aim is for all the messages received from the error-free replicas to also be recorded in a distributed manner. Accordingly, all the replicas have the right to propose the data to be logged. The replicas make use of this when a message received via the bus is not proposed for agreement within a certain period of time.

The suitability of the proposed messages is assessed using a modified version of the three-phase agreement protocol published in "Practical Byzantine Fault Tolerance". Specifically, the variant that signs the messages using asymmetric cryptography is used. This approach makes sense as it requires a quorum of the JBR replicas to sign the message. As intended for the algorithm, there must be N = 3f+1 replicates for this, of which only f may be faulty in any way. This means that no more messages can be recorded, if an insufficient number of replicas participate in the protocol. This fact protects the JBR from subsequent modification even within the context of an accident. Even assuming that only one replica can be recovered, no messages can be changed afterwards. Only the deletion of events is possible.

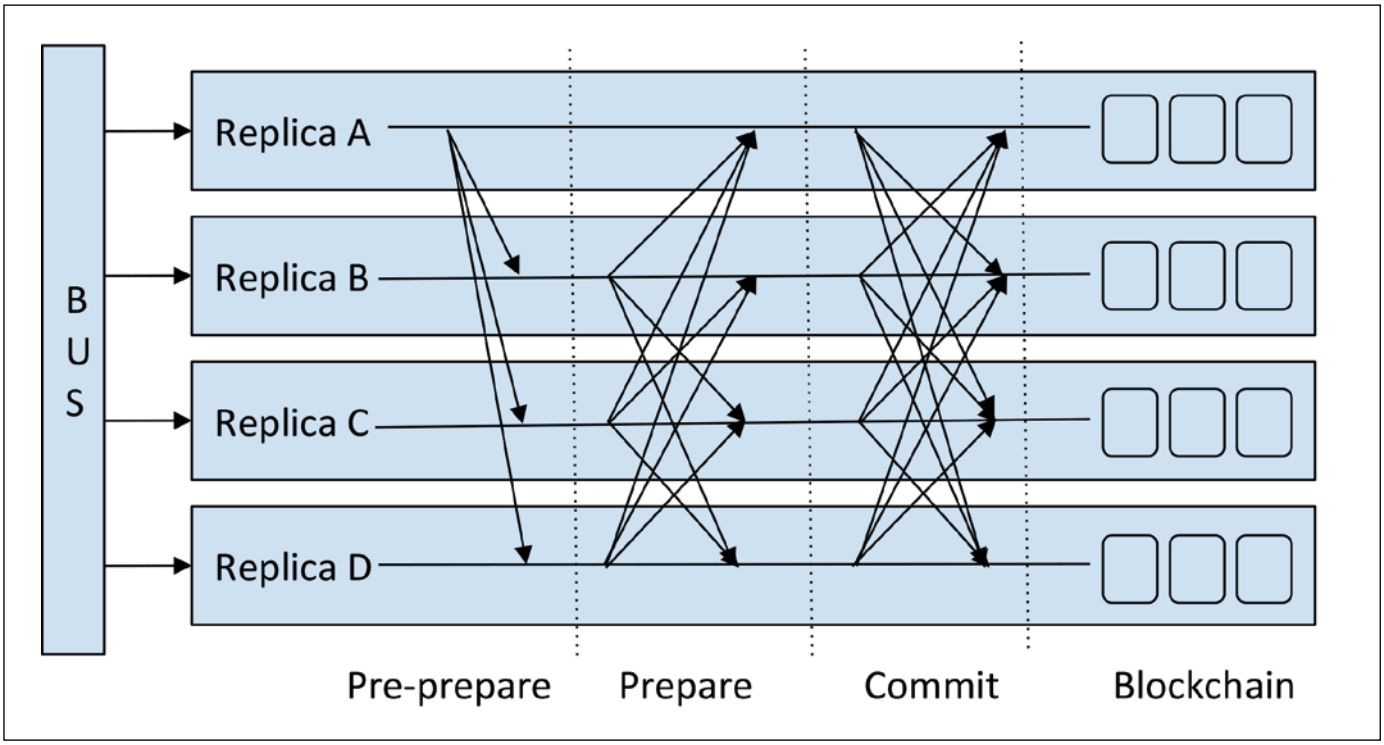

Bild 3: Vier unabhängige Rechner einigen sich auf die über einen Bus empfangenen Nachrichten und zeichnen diese in Form einer Blockchain auf.
Fig. 3: Four independent computers agree on the messages received via a bus and record them in the form of a blockchain Quelle / *Source*: TU Braunschweig

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

(bspw. Aufzeichnungen von Bedienhandlungen) unter Berücksichtigung der geltenden Regularien des Datenschutzes im Langzeitspeicher im Datenzentrum verwahrt werden.
Bild 4 zeigt das entwickelte mobile Testbed, welches über einen MVB Signale vermittelt, die durch die vier Systeme aufgezeichnet werden. Die Knoten führen dabei die entwickelte JBR-Software aus und können zusätzlich Funktionalitäten beheimaten. Unter Last sind die Knoten durch den JBR zu 30 % ausgelastet. Zur Kontrolle ist ebenfalls eine konventionelle JRU in den Aufbau integriert. Das Testbed ermöglicht mithilfe eines Steuerungsrechners (Raspberry Pi) verschiedene Last und Ausfallszenarien zu evaluieren. Zu Demonstrationszwecken wurde auf eine kompakte und transportable Integration Wert gelegt.

5 Ausblick: Daten werden vertrauenswürdiger

EULYNX und OCORA sind Bestandteile einer zukünftigen europäischen Referenzarchitektur für das Leit- und Sicherungssystem (RCA – Reference CCS Architecture; CCS – Command, Control, Signaling). Beide Architekturkonzepte skizzieren herstellerübergreifende, komponentenbasierende heterogene IT-Systeme. Solche Systeme bergen neue Herausforderungen, die bislang im Kontext der zugelassenen, sicherheitsrelevanten LST der Bahn weder strecken- noch fahrzeugseitig adressiert werden mussten.
Logbuch-Implementierungen, wie der gängige Juridical Recorder auf Fahrzeugen, können nicht mehr als zentrale Systemkomponente eines einzigen Herstellers umgesetzt werden. Alle zentralisierten Lösungsansätze sind in Frage gestellt. Diese Erfahrung hat die IT-Industrie in anderen Kontexten (bspw. Finanzindustrie, internationaler Handel) in den vergangenen 30 Jahren schmerzhaft machen müssen.
Das mFUND-geförderte Forschungsprojekt "RailChain" erbringt den praktischen Nachweis, dass verteilte Konsensprotokolle ein probates Mittel sind, um unveränderliche (gerichtsfeste) Zustandsinformationen über eine Vielzahl von Systemkomponenten herstellerübergreifend zu speichern.

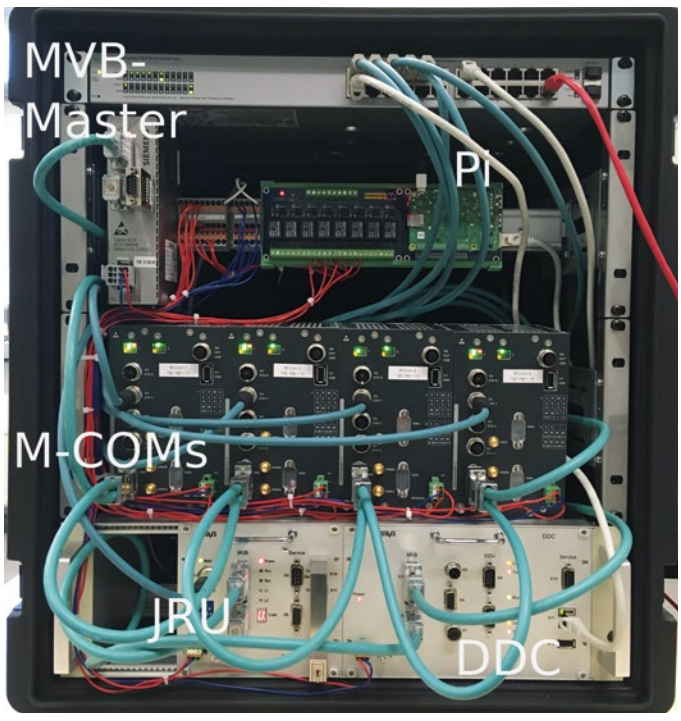

Bild 4: JBR Testbed
Fig. 4: The JBR testbed
Quelle / *Source*: TU Braunschweig

The third and final required component is the transfer of the logged data in the form of blocks of the blockchain to secure data centres. In principle, there are two reasons for this: the release of storage space in the train's systems and the prompt analysis of the data at the data centre. The developed transfer protocol ensures the secure confirmed acceptance of the data by several data centres before a deletion can be made on the replicas in the train.
Encryption and pseudonymisation techniques are used to ensure that personal data (e.g. recordings of the operator's actions) are stored in the data centre's long-term memory in compliance with the applicable data protection regulations.
Fig. 4 shows the developed mobile testbed which transmits the signals recorded by the four systems via an MVB. The nodes run the developed JBR software and can also host additional functionalities. When under load, the nodes are utilised by the JBR to 30 %. A conventional JRU is also integrated into the set-up for control purposes. The testbed enables different load and failure scenarios to be evaluated with the help of a control computer (Raspberry Pi). For demonstration purposes, emphasis has been placed on compact and transportable integration.

5 Outlook: the data will become more trustworthy

EULYNX and OCORA are components of a future European reference architecture for the control-command and signalling system (RCA – Reference CCS Architecture; CCS – Command, Control, Signalling). Both architecture concepts outline multi-vendor, component-based heterogeneous IT systems. Such systems pose new challenges that previously did not have to be addressed either trackside or on-board within the context of the railway's approved, safety-relevant control-command and signalling system.
Logbook implementations, such as the common juridical recorder on vehicles, can no longer be implemented as a central system component from a single manufacturer. All centralised approaches to solutions are in question. This has been the painful experience of the IT industry in other contexts (e.g. the financial industry, international trade) over the past 30 years.
The "RailChain" mFUND-funded research project provides practical proof that distributed consensus protocols are an effective means of storing unchangeable (court-proof) status information about a large number of system components across manufacturers. The results of "RailChain" will be published, prototypically implemented in the IoT lab at HPI and TU Braunschweig and experimentally evaluated in a large field test on DB Systemtechnik's Advanced TrainLab. At the same time, OCORA and EULYNX mean that an on-board and trackside architecture design exists, on which future implementations of distributed consensus protocols can be based.
The data can thus be evaluated more promptly and at the same time its trustworthiness is increased. Among other things, this enables traceable condition-based maintenance, because it is possible to ensure at all times that the data is authentic and has not been changed. ■

Funding reference
The "RailChain" project is funded by the Federal Ministry of Transport and Digital Infrastructure as part of the mFUND innovation initiative. The Federal Ministry of Transport and

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

übergreifend speichern zu können. Ergebnisse von "RailChain" werden publiziert, im IoT-Labor am HPI und der TU Braunschweig prototypisch implementiert und im Rahmen eines großen Feldtests auf dem Advanced TrainLab der DB Systemtechnik experimentell evaluiert. Gleichzeitig existiert mit OCORA und EULYNX ein fahrzeug- und streckenseitiger Architekturentwurf, auf dem zukünftige Implementierungen verteilter Konsensprotokolle aufsetzen können.
Die Daten können dadurch zeitnaher ausgewertet werden, und gleichzeitig wird ihre Vertrauenswürdigkeit erhöht. Dies ermöglich u. a. nachvollziehbare zustandsorientierte Wartung, denn es kann jederzeit sichergestellt werden, dass die Daten authentisch sind und auch nicht verändert wurden. ■

Förderhinweis
Das Projekt „RailChain" wird im Rahmen der Innovationsinitiative mFUND durch das Bundesministerium für Verkehr und digitale Infrastruktur gefördert. Im Rahmen der Innovationsinitiative mFUND fördert das BMVI seit 2016 Forschungs- und Entwicklungsprojekte rund um datenbasierte digitale Anwendungen für die Mobilität 4.0. Neben der finanziellen Förderung unterstützt der mFUND mit verschiedenen Veranstaltungsformaten die Vernetzung zwischen Akteuren aus Politik, Wirtschaft und Forschung sowie den Zugang zum Datenportal mCLOUD.

Digital Infrastructure has been funding research and development projects relating to databased digital applications for Mobility 4.0 as part of the mFUND innovation initiative since 2016. In addition to financial funding, mFUND also supports networking between stakeholders from politics, industry and research with various event formats and access to the mCLOUD data portal.

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH, TU Braunschweig, Universität Potsdam, DB Systel GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

LITERATUR | LITERATURE

[1] UNISIG: FFFIS Juridical Recorder-Downloading tool, SUBSET-027, Issue 2.3.0, 2009
[2] messMa: Datenrecorder mRec-s42, Datenblatt, Ausgabe V.02, 2012
[3] Deutsche Bahn AG: Teillastenheft 4 ETCS Fahrzeug-Ausrüstung, Anhang 2 – Juridical Recording Unit (JRU) Version 2.0, 08.07.2011
[4] Braband, J.; Schäbe, H.: Zuverlässigkeit von Verteiltem Juridical Recording, SIGNAL+DRAHT, 9/2021
[5] Mühlemann, R.: OCORA – Die europäische Initiative zur ETCS-Fahrzeugausrüstung der Zukunft, SIGNAL+DRAHT, 9/2020
[6] Blockchain- bzw. Distributed Ledger Technologien im Bahnbetrieb – RailChain; FKZ: 19F2093X; https://railchain.berlin; https://www.bmvi.de/SharedDocs/DE/Artikel/DG/mfund-projekte/railchain.html
[7] Eulynx.eu – Baseline Set 3; https://eulynx.eu/index.php/documents/published-documents/open-availability/baseline-set-3

AUTOREN | AUTHORS

Prof. Dr. Jens Braband
Principal Key Expert
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38023 Braunschweig
E-Mail: jens.braband@siemens.com

Prof. Dr. Rüdiger Kapitza
Professor of Distributed Systems
Technische Universität Braunschweig
Anschrift / *Address*: Mühlenpfordtstraße 23, D-38106 Braunschweig
E-Mail: rrkapitz@ibr.cs.tu-bs.de

Prof. Dr. rer. nat. habil. Andreas Polze
Professor Operating Systems and Middleware
Hasso-Plattner-Institut für Digital Engineering GmbH
Universität Potsdam
Anschrift / *Address*: Prof.-Dr.-Helmert-Straße 2-3, D-14482 Potsdam
E-Mail: andreas.polze@hpi.de

Ingo Schwarzer
Fellow
DB Systel GmbH
Anschrift / *Address*: Kynaststraße 1, D-10317 Berlin
E-Mail: ingo.schwarzer@deutschebahn.com