SIL4 Data Center – eine neue Plattform-Architektur für sichere Bahnanwendungen

SIL4 Data Center – a new platform architecture for safety-relevant railway applications

Sonja Steffens | Tom Suess | Frank Eschmann | Patrick Marsch

Der Bahnsektor in Europa steht vor einem Technologiesprung in die digitale Zukunft: Die Sektorinitiative „Digitale Schiene Deutschland" nutzt diese Chance und bringt Zukunftstechnologien in das System Bahn. Das Fundament dafür wird mit der grundlegenden Modernisierung und Digitalisierung der Infrastruktur durch die konsequente Einführung der neuen Leit- und Sicherungstechnik (LST) European Train Control System (ETCS) und digitaler Stellwerke gelegt. Darüber hinaus arbeitet die Initiative an einer weitreichenden Digitalisierung des Bahnsystems. Dieses wird u. a. charakterisiert sein durch ein KI (Künstliche Intelligenz) -basiertes Verkehrsmanagementsystem, das Fahren im optimalen Abstand (im sogenannten ETCS Level 3 Moving Block-Ansatz), das vollautomatisierte Fahren in Kombination mit hochpräziser Zugortung und neuester Fahrzeugsensorik zur Umfeldwahrnehmung sowie ein automatisiertes Entstörungsmanagement. Insgesamt wird hiermit eine signifikante Verbesserung von Kapazität, Pünktlichkeit und Effizienz des Bahnsystems erreicht, allesamt Voraussetzungen für mehr Verkehr auf der Schiene und eine Stärkung der Bahn als CO_2-neutraler Verkehrsträger der Zukunft.

1 Einleitung

Die Umsetzung der genannten Technologien setzt voraus, dass neue Konnektivitäts- und IT-Plattformen eingeführt werden, wie z. B. das 5G-basierte Future Railway Mobile Communication System (FRMCS) [1] für die zukünftige Kommunikationsverbindung zwischen Zügen und Infrastruktur, oder IT-Infrastrukturen für datenintensive und teils KI-basierte Bahnapplikationen.

Gegenstand einer F&E-Kollaboration zwischen der Siemens Mobility GmbH (SMO) und der Deutschen Bahn AG (DB) war in diesem Kontext die Erarbeitung einer grundlegenden Architektur für SIL 4 Data Center, d. h. die Recheninfrastrukturen, auf denen sicherheitsrelevante Bahnanwendungen wie die weiterentwickelte LST oder unterstützende Funktionen für die Hochpräzisionsortung von Zügen in Zukunft laufen sollen.

Die Erwartungen an solche SIL4 Data Center sind hierbei sehr groß. Insbesondere sollen sie folgende Eigenschaften bieten:

- **Modularität**
  Die SIL4 Data Center sollen modular aufgebaut sein und insbesondere eine klare, standardisierte Trennung von Applikation, Ablaufumgebung (sog. Runtime Environment) und Hardware vornehmen, damit die sehr unterschiedlichen Lebenszyklen der verschiedenen Hardware- und Softwarekomponenten berücksichtigt und unterstützt werden.
- **Commercial-off-the-shelf (COTS) -Komponenten**
  Es sollen soweit wie möglich COTS-Komponenten genutzt werden, d. h. Komponenten, die nicht nur für den Bahnsektor ent-

The European railway sector is about to take a technological leap into the digital future: The "Digitale Schiene Deutschland" sector initiative exploits this opportunity to implement next-generation technologies in rail operations. The foundation for this process will be laid by the fundamental modernization and digitalization of the infrastructure by consistently introducing the European Train Control System (ETCS) and digital interlocking systems as new control and safety technology. In addition, the initiative is working on a far-reaching digitalization of rail operations, encompassing, for example, an AI (Artificial Intelligence) -based traffic and incident management system, an ETCS Level 3 moving block approach, fully automatic train operation combined with high-precision real time train localization and the latest vehicle sensor technology for environmental and automated incidence perception . Overall, this will significantly improve the capacity, reliability, and efficiency of rail operations, all of which are necessary for more transportation by rail and for strengthening the railway as a carbon-neutral mode of transportation of the future.

1 Introduction

For these technologies to be implemented, new connectivity and IT platforms will have to be established, such as the 5G-based Future Railway Mobile Communication System (FRMCS) [1] for future communications between trains and infrastructure, or IT infrastructures for data-intensive and partly AI-based railway applications.

In this context, an R&D collaboration project between Siemens Mobility GmbH (SMO) and Deutsche Bahn AG (DB) focused on developing a basic architecture for SIL4 Data Centers, i.e., the computing infrastructures in which safety-relevant railway applications such as advanced control command and signaling systems or support functions for high-precision train localization are to run in future.

The expectations placed on such SIL4 Data Centers are very high. In particular, they should have the following characteristics:

- **Modularity**
  The SIL4 Data Centers should be modular in design and, in particular, provide a clear and standardized separation of application, runtime environment and hardware, so that the very different lifecycles of the various hardware and software components are taken into account and supported.
- **Commercial-off-the-shelf (COTS) components**
  COTS components should be used as far as possible, i.e., components that are not exclusively developed for the rail sector and that are widely available. This approach cuts down on the

wickelt werden und breit verfügbar sind. Damit werden Kosten gesenkt und neueste Entwicklungen im IT-Cloud-Bereich für den Bahnsektor nutzbar gemacht.

- **Zentralisierung**
  Der SIL4 Data Center-Ansatz soll die Bündelung verschiedener sicherheitsrelevanter Anwendungen in wenigen Rechenzentren ermöglichen.
- **Skalierbarkeit**
  Die SIL4 Data Center sollen skalierbar sein, um für die geplante sukzessive Digitalisierung des Bahnsystems vorbereitet zu sein und auch zukünftige, rechenintensivere Anwendungen unterstützen zu können.
- **Flexibilität**
  Es soll möglich sein, Anwendungen bei Bedarf auf andere SIL 4 Data Center portieren zu können.

Die F&E-Kollaboration berücksichtigte dabei die Vorarbeiten zur generischen „Safe Computing Platform" der Bahninitiativen Reference CCS Architecture (RCA) [2] und Open CCS Onboard Reference Architecture (OCORA) [3], insbesondere die Anforderungen, die in diesem Kontext bereits abgeleitet wurden [4, 5]. Ferner sind Security-Anforderungen aus den einschlägigen Normen und Shift2Rail [6] berücksichtigt worden, und es sind Anforderungen und Erfahrungen aus EULYNX [7] eingeflossen.

Während RCA und OCORA gleichermaßen Compute-Infrastrukturen auf Zugseite und Streckenseite betrachten, bestand der Fokus in der Arbeit von SMO und DB auf streckenseitigen Datenzentren. Ein wesentlicher Aspekt war hierbei, die verschiedenen Sichtweisen abzugleichen und die fachlichen, technischen sowie kommerziellen Herausforderungen für die Umsetzung frühzeitig zu identifizieren.

Hierbei wurde explizit berücksichtigt, wie bestehende Softwarekomponenten mit vertretbarem Aufwand migriert werden können. Zudem wurden die in [4] genannten Anforderungen ausführlich in Bezug auf Kritikalität, Wechselwirkungen und Implikationen auf die Architektur beleuchtet. Ergänzend zu den genannten Arbeiten in RCA und OCORA wurden zudem Konzepte erarbeitet, mit denen sicherheitsrelevante Applikationen über geografisch verteilte Standorte realisiert werden können, um eine höhere Robustheit des Gesamtsystems bei katastrophalen Ereignissen (z. B. Erdbeben oder Überflutungen) zu erreichen.

Im Rahmen der Zusammenarbeit ist ein umfassender Forschungsbericht [8] entstanden und veröffentlicht worden. Dessen Kerninformationen werden in diesem Beitrag beleuchtet.

2 Architektur

Die Architektur basiert auf einem modularen Layer-Ansatz, bei dem die verschiedenen Ebenen durch eindeutig beschriebene und standardisierte Softwareschnittstellen voneinander getrennt sind. Dadurch ist es möglich, dass die verschiedenen Hardware- und Softwarekomponenten nicht nur separat ausgeschrieben, entwickelt und eingesetzt werden können, sondern auch ihren eigenen Lebenszyklus besitzen dürfen. Somit ist es beispielsweise möglich, die Hardware in kürzeren Zyklen gegen aktuellere Hardwarekomponenten auszutauschen, ohne Auswirkungen auf die Sicherheitszulassung zu haben.

Die Architektur des SIL4 Data Centers ist in Bild 1 dargestellt und besteht aus den folgenden Komponenten:

- **COTS Hardware**
  Die Hardware wird grundsätzlich nicht als sicherheitsrelevant klassifiziert, damit die Hardware einfach austauschbar ist und keine sicherheitsrelevanten Abhängigkeiten zwischen den sicherheitsrelevanten Softwareebenen und der Hardware entste-

costs and ensures that the latest developments in IT cloud technology can be used for the rail sector.

- **Centralization**
  The SIL4 Data Center approach should enable the pooling of different safety-relevant applications in a small number of data centers.
- **Scalability**
  The SIL4 Data Centers should be scalable to be prepared for the intended gradual digitalization of rail operations and to be able to support future, computationally more intensive applications.
- **Flexibility**
  It should be possible to port applications to other SIL4 Data Centers, if required.

The R&D collaboration project took into account the preliminary work for the generic Safe Computing Platform of the Reference CCS Architecture (RCA) [2] and Open CCS Onboard Reference Architecture (OCORA) [3] rail initiatives, in particular the requirements already derived in this context [4, 5]. In addition, security requirements from the relevant standards and Shift2Rail [6] were considered and requirements and experience from EULYNX [7] were included.

While RCA and OCORA cover both the on-board and the trackside computing infrastructures, SMO and DB focused on trackside data centers. A key aspect was to align the various viewpoints and to identify the functional, technical, and commercial challenges for implementation at an early stage.

Explicit consideration was given to how existing software components can be migrated with a justifiable effort. Moreover, the requirements stated in [4] were analyzed in detail regarding their criticality, interactions, and implications for the architecture. In addition to the stated work performed in RCA and OCORA, concepts for implementing safety-relevant applications across geographically distributed sites were derived to achieve a more robust overall system in the event of catastrophic events (e.g., earthquakes or floods).

A comprehensive Research Report [8] was prepared and published as part of the collaboration project. The key information therein will be presented in this article.

2 Architecture

The architecture is based on a modular, multi-layered approach, in which the different layers are separated by clearly defined and standardized software interfaces. As a result, the various hardware and software components cannot only be tendered, developed, and used separately, but may also have their own lifecycle. In this way, it is possible, for example, to replace the hardware with more up-to-date hardware components at shorter intervals without having any impact on the safety approval.

The architecture of the SIL4 Data Center is shown in fig. 1 and comprises the following components:

- **COTS hardware**
  The hardware is generally classified as non-safety-relevant so that the hardware can be easily replaced, and no safety-relevant dependencies arise between the safety-relevant software layers and the hardware. Therefore, COTS hardware can be used, the only requirement being that the hardware is sufficiently dimensioned, e.g., with regard to the number of CPU cores, computing power, and memory.
- **Load operating system (load OS)**
  The load OS is used for standardized and vendor-independent spare parts management of the COTS hardware. In particular,

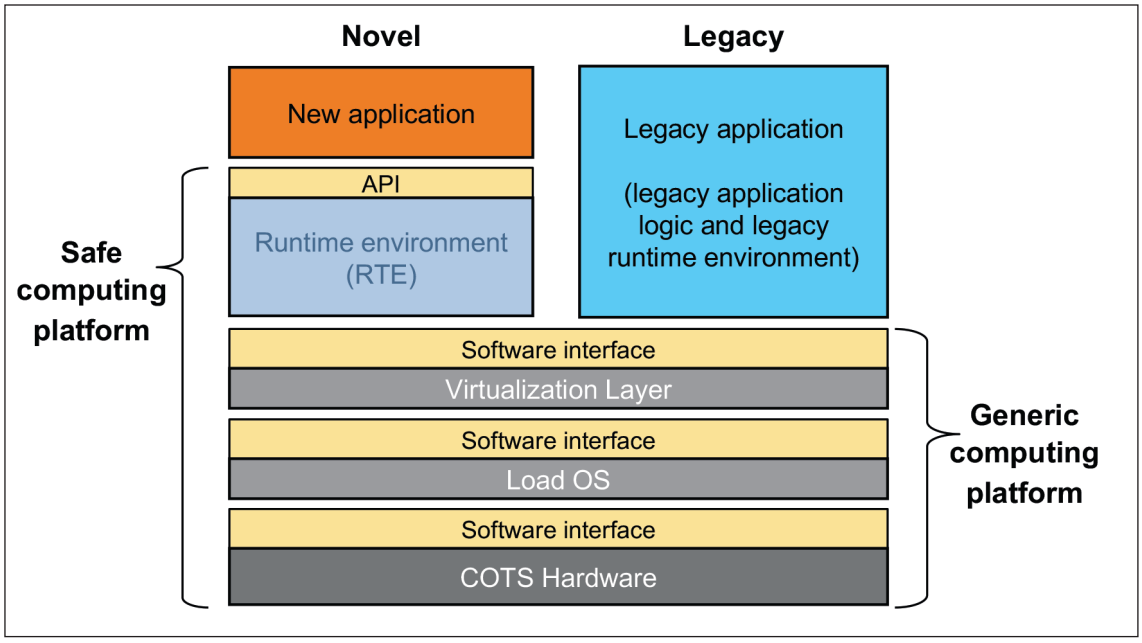

Bild 1: Grundlegende Architektur des SIL4 Data Centers
Fig. 1: Basic architecture of the SIL4 Data Center
Quelle (alle Bilder) / *Source (all fig.)*: eigene Darstellung / *own illustration*

hen. Damit ist der Einsatz von COTS Hardware möglich. Die einzige Anforderung ist, dass die Hardware ausreichend dimensioniert ist, u. a. in Bezug auf Anzahl Prozessorkerne, Rechenleistung und Speicher.

- **Load Operating System (Load OS)**
  Das Load OS dient einem einheitlichen und herstellerunabhängigen Ersatzteil-Management der COTS Hardware. Insbesondere ermöglicht es die Ferninstallation und -aktualisierung aller Software und Daten auf der jeweiligen COTS Hardware.
- **Virtualisierung**
  Die Virtualisierung ist ein Mittel, um die im SIL4 Data Center zu betreibende Software von der Hardwarekonfiguration unabhängig zu halten. Gleichzeitig kapselt sie die verschiedenen Applikationen voneinander und schützt sie vor gegenseitiger Beeinflussung.
  Die Virtualisierungslösung muss für die Verwendung seitens SIL 4 Applikationen auf COTS Hardware geeignet sein. Hierbei geht es im Wesentlichen um die Sicherheitsnachweisführung bzgl. der Verteilung der sicherheitsrelevanten Software auf verschiedene COTS-Hardware-Einheiten und um das grundsätzliche echtzeitnahe Zeitverhalten.
- **Runtime Environment für sicherheitsrelevante Anwendungen (RTE)**
  Das RTE trennt die sicherheitsrelevante Applikation von den nicht-sicherheitsrelevanten unteren Schichten. Es ist verantwortlich für die Composite Fail Safety, d. h. für die sichere, zeitlich korrekte Ausführung der Anwendungen in redundanten Replikas und die funktional sichere Kommunikation zwischen den verschiedenen Anwendungen sowie zu den externen Systemen.
- **Applikation**
  Die Applikation stellt die funktionale Anwendung dar. Neu zu entwickelnde sicherheitsrelevante Applikationen profitieren von den funktional sicheren und standardisierten Services des RTE wie beispielsweise der Verteilung der Replikas, dem Voting und der sicheren Kommunikation. Damit kann die Applikation auf die eigentliche Anwendungslogik fokussieren.
- **Legacy-Applikation**
  Durch die große Menge an vorhandenen Installationen der heute existierenden Applikationen im Feld (z. B. digitale Stellwerke) ist es wichtig, ein Migrationskonzept für die Bestandsapplikationen

it enables the remote installation and updating of all software and data on the respective COTS hardware.

- **Virtualization**
  Virtualization is a means of keeping the software to be run in the SIL4 Data Center independent of the hardware configuration. Simultaneously, it encapsulates the different applications and protects them against mutual interference.
  The virtualization solution must be suitable for running SIL 4 applications on COTS hardware. This essentially involves demonstrating technical safety regarding the distribution of the safety-relevant software to different COTS hardware units and the basic real-time response.
- **Runtime environment for safety-relevant applications (RTE)**
  The RTE separates the safety-relevant applications from the non-safety-relevant lower layers. It is responsible for composite fail-safety, i.e., for safe execution of the applications at the correct time in redundant replicas and for functionally safe communications between the various applications and with the external systems.
- **Application**
  The application implements its actual logic functionality. New safety-relevant applications to be developed benefit from the functionally safe and standardized services of the RTE, such as the distribution of the replicas, voting, and safe communications. This enables the application to focus on the actual application logic.
- **Legacy applications**
  Due to the large number of existing installations of the currently existing applications in the field (e.g., digital interlockings), it is important to support a migration concept for the legacy applications. Such legacy applications should be executable directly on the virtualization layer and continue to be responsible for their functionally safe execution. Therefore, legacy applications do not need to be adapted to the interfaces of the RTE. However, newly developed applications should be implemented in accordance with the new overall architecture, i.e., with a standardized separation of application and RTE.

In the remainder of this paper, the bundle of COTS hardware, load OS and virtualization is referred to as **Generic Computing**

("Legacy") zu unterstützen. Solche Legacy-Applikationen sollen direkt auf dem Virtualisierungs-Layer ausführbar sein und sind weiterhin selbst verantwortlich für ihre funktional sichere Ausführung. Damit ist kein Anpassungsaufwand der Legacy-Applikation an die Schnittstellen des RTE erforderlich. Neu entwickelte Applikationen sollten jedoch nach der neuen Gesamtarchitektur umgesetzt werden, d. h. mit standardisierter Trennung von Applikation und RTE.

Im Folgenden wird das Bündel aus COTS Hardware, Load OS und Virtualisierung als **Generic Computing Platform** bezeichnet. In Kombination mit dem RTE ergibt diese die in [4] definierte **Safe Computing Platform**, die innerhalb der F&E-Kollaboration detaillierter ausgearbeitet wurde.

Um bei einer modularen Systemarchitektur mit verschiedenen Herstellern ein einheitliches SIL4 Data Center zu erreichen, wurden folgende wesentliche Schnittstellen und Aspekte zur Vereinheitlichung oder Standardisierung identifiziert. Hierbei ist eine maßgebende Prämisse, so weit wie möglich bestehende Standards zu nutzen.

- **COTS Hardware (1)**
  Die Eigenschaften und das User Interface der zu verwendenden COTS Hardware müssen mindestens innerhalb eines Data Centers vereinheitlicht sein. Darüber hinaus wäre die Erarbeitung einer internationalen Referenz empfehlenswert.
- **Load OS (2)**
  Das Load OS sollte einheitlich auf den Servern aller SIL4 Data Center eines Eisenbahninfrastrukturunternehmens (EIU) laufen, damit die COTS Hardware austauschbar ist und die Softwarekomponenten einheitlich installiert, aktualisiert und geladen werden können. Die Funktionen und Schnittstellen des Load OS sollten darüber hinaus auch international harmonisiert werden.
- **Infrastruktur für Installation und Update (3)**
  Die Schnittstelle zur Infrastruktur bzgl. Remote-Installation und -Update und dazugehörige Prozesse müssen als Standard definiert sein, z. B. auf Basis des Standard Maintenance Interface (SMI*) [7].
  Prozess-relevant ist hierbei der Umgang mit den zu ladenden Softwarepaketen (Programme und Daten) und die Handhabung von Systemzuständen wie z. B. Stopp und Neustart von Systemteilen.
- **Virtualization-Layer (4)**
  Der Virtualization-Layer benötigt aus Sicht von RTE und Legacy-Applikation ein standardisiertes User Interface. Zusätzlich muss er seitens der RTE bzw. Legacy-Applikation als nicht-sicherheitsrelevant klassifiziert sein, um sicherheitsrelevante Abhängigkeiten zwischen RTE oder Legacy-Applikation und Virtualization-Layer zu vermeiden.
  Der Virtualization-Layer sollte zudem innerhalb eines SIL4 Data Centers aus einer einheitlichen Softwarelösung bestehen, um eine hardwareübergreifende einheitliche Virtualisierung zu erreichen.
- **Infrastruktur IT Security (5)**
  Die Schnittstelle zur Infrastruktur bzgl. IT-Security und dazugehörige Prozesse müssen als Standard definiert sein.
  Hierbei ist insbesondere der Aspekt des kurzen Lebenszyklus der IT-Security-relevanten Softwareanteile zu berücksichtigen, d. h. die von IT-Security-Patches betroffenen nicht sicherheitsrelevanten Softwareanteile der RTE bzw. Legacy-Applikationen müssen einfach austauschbar sein, ohne dass sicherheitsrelevante Gutachten betroffen sind.
- **Zentrale Diagnose (6)**
  Die Schnittstelle zum zentralen Diagnosesystem muss als Standard definiert sein, z. B. auf Basis des Standard Diagnostic Interface (SDI*) [7].
  Hierbei sind insbesondere die für die Diagnose der unterlagerten Schichten wie Virtualisierung und COTS Hardware relevanten Daten zu berücksichtigen.

Platform. Together with the RTE, it forms the **Safe Computing Platform** defined in [4], which was elaborated in greater detail in the R&D collaboration project.

To achieve a standardized SIL4 Data Center with a modular system architecture involving different vendors, the following key interfaces and aspects have been identified for standardization. In general, it is assumed that existing standards are reused as far as possible.

- **COTS hardware (1)**
  The characteristics and the user interface of the COTS hardware to be used must be standardized at least within one SIL 4 Data Center. It would also be advisable to derive an international reference.
- **Load OS (2)**
  The load OS should run in a standardized manner on the servers of all SIL4 Data Centers of a rail infrastructure company, so that the COTS hardware can be replaced, and the software components can be installed, updated and loaded in a standardized manner. The functions and interfaces of the load OS should also be harmonized on an international level.
- **Installation and update infrastructure (3)**
  The interface to the remote installation and update infrastructure and the associated processes must be standardized, e.g., based on the Standard Maintenance Interface (SMI*) [7].
  The handling of the software packages to be loaded (programs and data) and the handling of system states such as stop and restart of system parts are relevant to these processes.
- **Virtualization layer (4)**
  From the point of view of the RTE and the legacy application, the virtualization layer requires a standardized user interface. In addition, it must be classified as non-safety-relevant regarding the RTE and the legacy application to prevent safety-relevant dependencies between the RTE or legacy application and the virtualization layer.
  Moreover, the virtualization layer should consist of a standard software solution within a SIL4 Data Center to achieve a standardized virtualization across all hardware components.
- **IT security infrastructure (5)**
  The interface to the IT security infrastructure and the associated processes must be standardized.
  In particular, the aspect of the short lifecycle of the IT security-relevant software parts must be considered, i.e., the non-safety-relevant software parts of the RTE or legacy applications affected by IT security patches must be easily replaceable without safety assessments being impaired.
- **Central diagnostic system (6)**
  The interface to the central diagnostic system must be standardized, e.g., based on the Standard Diagnostic Interface (SDI*) [7].
  In particular, the data relevant to diagnostics of the underlying layers such as virtualization and COTS hardware must be taken into account.
  For this purpose, a suitable diagnostic software must be considered as a data source.
- **Other rail products outside the SIL4 Data Center (7)**
  The operative interfaces to other rail products have already been defined as Standard Communication Interfaces (SCI*) [7].
  It is not relevant here whether rail products are installed at the same SIL4 Data Center or at a different location.
- **Generic API of the RTE and application bundling (8)**
  A generic API (Application Programming Interface) of the RTE must be standardized for the development of new applications. It should be noted that process-related SRACs (safe-

Hierzu ist als Datenquelle eine geeignete Diagnosesoftware zu betrachten.

- **Andere Bahnprodukte außerhalb des SIL4 Data Centers (7)**
  Die operativen Schnittstellen zu anderen Bahnprodukten sind heute bereits als Standard Communication Interface (SCI*) [7] definiert.
  Hierbei ist es nicht relevant, ob Bahnprodukte im gleichen SIL 4 Data Center installiert sind oder an anderer Stelle.
- **Generische API des RTE und Applikations-Bündelung (8)**
  Für neu zu entwickelnde Applikationen muss eine generische API (Application Programming Interface) des RTE als Standard definiert werden. Hierbei ist hervorzuheben, dass prozessrelevante SRACs (Safety Related Application Conditions) der Safe Computing Platform von den Details des RTE-eigenen Sicherheitskonzepts abhängen und deshalb voraussichtlich nicht generisch definierbar sind. Insbesondere ist anzunehmen, dass für jede verwendete RTE-Lösung eine Applikation neu kompiliert, integriert und validiert werden muss.
  Als besondere Anforderung an RTE wurde die zeitkritische Kommunikation zwischen Applikationen identifiziert. Falls Applikationen mit sehr geringen Latenzen direkt miteinander kommunizieren müssen, ist das „Bündeln" dieser Applikationen zusammen in einer Replika notwendig, um Verzögerungszeiten durch Nachrichtenverteilung in zyklisch arbeitenden Systemen zu vermeiden.
  Das Bündeln von Applikationen bedingt besondere Mechanismen und Services seitens des RTE für die Datenflusssteuerung zwischen den gebündelten Applikationen. Diese sind wesentlicher Input für die RTE-Entwicklung und müssen somit ebenfalls standardisiert werden.
- **Sichere Kommunikationsprotokolle (9)**
  Wenn innerhalb einer Installation (z. B. in einem Stellwerk) die einzelnen Applikationen auf eigenen RTE-Instanzen betrieben werden, dann muss ein sicherungstechnisches Kommunikationsprotokoll für die Kommunikation zwischen diesen Applikationen definiert werden.
  Dieses Kommunikationsprotokoll muss standardisiert werden, falls die RTE von unterschiedlichen Herstellern stammen.
  Die heute existierenden Kommunikationsprotokolle wie z. B. RaSTA sind als Punkt-zu-Punkt-Kommunikation für diese Zwecke nur sehr eingeschränkt geeignet.
- **Prozesse und Tools (10)**
  Für automatisiertes herstellerunabhängiges Testen im Zuge der Integration der modularen Systemteile zu einem Gesamtsystem sind die notwendigen Prozesse und Tools bzw. Schnittstellen zu Tools zu standardisieren. Dies betrifft sowohl Tools für das Erstellen und Ausführen von Testfällen als auch für die Generierung von topologiebezogenen Anlagendaten.

Obige Festlegungen (1)...(7) sind übergreifend für bereits existierende und neu zu entwickelnde Software zu treffen, damit sowohl heute existierende Applikationen (Legacy) als auch neu entwickelte Applikationen (z. B. neue in RCA spezifizierte Leit- und Sicherungsfunktionen [2]) im selben SIL4 Data Center laufen können. Die Festlegungen (8)...(10) sind nur für das RTE und die neu zu entwickelnden Applikationen relevant.

Bild 2 zeigt die grundsätzliche Systemarchitektur des SIL4 Data Centers, sowohl für neu entwickelte Applikationen APP-x, z. B. RCA, als auch für portierte existierende Applikationen (Legacy). Die dargestellte Modularität entspricht der möglichen Herstellervielfalt, die zu standardisierenden Aspekte sind mit (1)...(10) gekennzeichnet.

Diese Architektur erlaubt einerseits den Betrieb mehrerer Safety-Applikationen innerhalb eines SIL4 Data Centers, andererseits lassen sich mehrere SIL4 Data Center mit der gleichen Architektur auf dem Gebiet eines EIU aufbauen.

ty-related application conditions) of the Safe Computing Platform may depend on the details of the RTE's safety concept and can therefore probably not be generically defined. In particular, it can be assumed that an application has to be recompiled, reintegrated and revalidated for each RTE solution used.

Time-critical communications between applications have been identified as a special requirement for the RTE. If applications with very low latency requirements need to communicate directly with one another, these applications must be "bundled" together in one replica to avoid time delays due to message switching in cyclic systems.

When bundling applications, special mechanisms and services are required regarding the RTE for data flow control between the bundled applications. These are an essential input for RTE development and should also be standardized.

- **Safe communication protocols (9)**
  If the individual applications within an installation (e.g., an interlocking) are run on their own RTE instances, a safe communication protocol must be defined for communications between these applications.
  This communication protocol must be standardized if the involved RTEs are provided by different vendors.
  As point-to-point communication protocols, today's communication protocols such as RaSTA are only suitable to a very limited extent for these purposes.
- **Processes and tools (10)**
  The processes and tools and the interfaces to the tools must be standardized to be able to run automatic and vendor-independent tests when integrating the modular system parts to form an overall system. This applies to both tools for creating and executing test cases and tools for generating topology-related installation data.

Specifications (1) to (7) must generally be applied for existing software and new software to be developed so that both legacy applications and newly developed applications, such as new Control, Command and Signaling (CCS) functions specified by RCA [2], can be run in the same SIL4 Data Center. Specifications (8) to (10) are only relevant to the RTE and new applications to be developed.

Fig. 2 shows the basic system architecture of the SIL4 Data Center, both for newly developed applications APP-x (e.g., specified by RCA) and for ported legacy applications. The modularity shown corresponds to the possible vendor multiplicity; the aspects to be standardized are identified as (1) to (10).

On one hand, this architecture permits the operation of multiple safety-relevant applications within one SIL4 Data Center; on the other hand, several SIL4 Data Centers with the same architecture can be set up in the operational area of a railway infrastructure company.

In addition to the architecture shown, detailed concepts for the geographically redundant implementation of applications were developed as part of the collaboration project [8]. An important aspect is here that both the individual replicas of an application and the RTE are distributed geographically.

The security concepts defined in the X2Rail-3 research project [6] are compatible with the presented system architecture and appear to be directly applicable.

3 Integration and testing

Besides the design of the SIL4 Data Center architecture, the implications of the architecture for integration and testing were

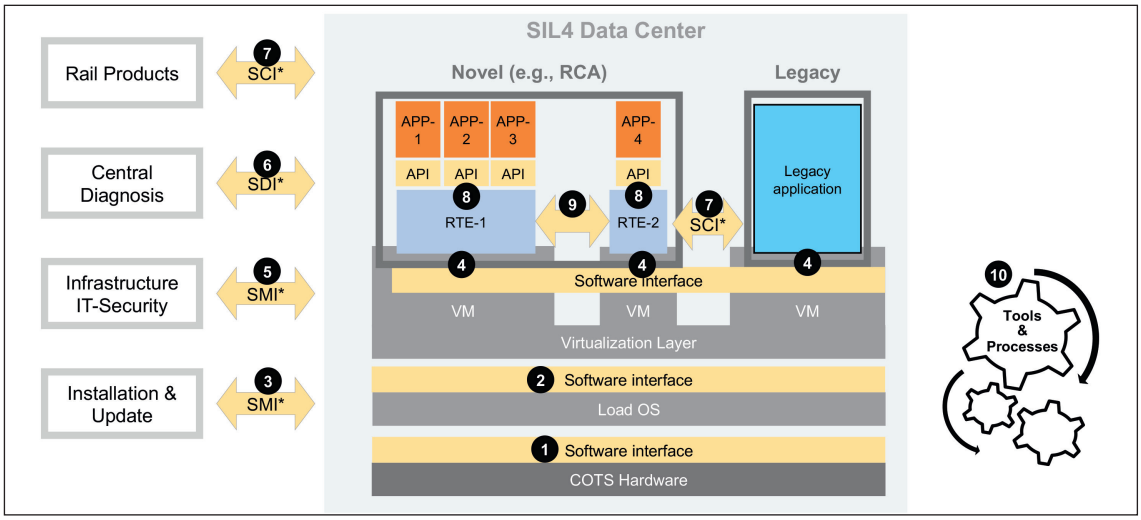

Bild 2: Schnittstellen zwischen den Komponenten eines SIL4 Data Centers
Fig. 2: Interfaces between the components of a SIL4 Data Center

Über die dargestellte Architektur hinaus wurden im Rahmen der Kollaboration detaillierte Konzepte zur georedundanten Umsetzung von Applikationen entwickelt [8]. Ein wichtiger Bestandteil ist dabei, dass sowohl die einzelnen Replikas einer Applikation als auch die RTE geographisch verteilt werden.
Die im Forschungsprojekt X2Rail-3 definierten Security-Konzepte [6] sind kompatibel zu der vorgestellten Systemarchitektur und scheinen sich direkt anwenden zu lassen.

3 Integration und Test

Neben dem Entwurf der Architektur des SIL4 Data Centers wurde in der F&E-Kollaboration auch im Detail beleuchtet, welche Implikationen die Architektur auf Integration und Test hat. Hier war es zunächst einmal recht offensichtlich, dass durch die Vielfalt an Einzelkomponenten verschiedener Hersteller ein deutlicher Anstieg der Aufwände und Komplexität bei der Integration zu erwarten ist.
Die mit Abstand wichtigste Feststellung stellt jedoch die erforderliche Verschiebung der Verantwortlichkeiten im Bereich Integration und Test dar. Um Integrität und Sicherheit des Gesamtsystems auch mit mehreren Teillieferanten sicherstellen und nachweisen zu können, wird eine Verlagerung der Verantwortung für die Systemintegration von den Herstellern hin zu den Betreibern eines Systems (i. d. R. EIU) erforderlich.
Damit aus modularen Systemteilen von verschiedenen Herstellern ein komplexes Gesamtsystem erstellt werden kann, sind weitere geeignete Instrumente erforderlich. Dazu zählt insbesondere ein solides Integrationskonzept, welches die Umsetzung standardisierter Prozesse, Schnittstellen, Tools und hochgradig automatisierter Testfälle ermöglicht. Dieses sollte idealerweise umfassen:

- Standardisierte Datenschnittstellen und -formate (für Konfigurations- und Engineering-Daten), die herstellerunabhängige Testumgebungen ermöglichen (sogenannte „Testbahnhöfe“)
- harmonisierte Engineering-Tools für die Erstellung der Testumgebungen
- standardisierte Testfälle für alle im vorherigen Abschnitt genannten Schnittstellen
- harmonisierte Simulationsumgebungen für externen Komponenten (z. B. Object Controller, Onboard-Einheiten) mit definierten Schnittstellen für eine Manipulation ihres Verhaltens entsprechend der zuvor genannten Testfälle
- ein Testsystem zum Erstellen und automatisierten Durchführen der Testfälle sowie der Überprüfung der Testergebnisse

investigated in detail as part of the R&D collaboration project. First of all, it was very obvious that the variety of individual components from different vendors will cause a significant increase in the expenditure and complexity of integration.
However, the most important finding by far was the necessary shift in responsibilities in integration and testing. To ensure integrity and safety of the overall system across multiple vendors and to provide the necessary evidence, a shift in responsibilities from the vendors to the system operators (usually railway infrastructure companies) is necessary.
Additional suitable concepts and tools are required so that a complex overall system can be created out of modular system parts from different vendors. These include, in particular, a solid integration concept that enables the implementation of standardized processes, interfaces, tools, and highly automated test cases. This concept should ideally include the following:

- standardized data interfaces and formats (for configuration and engineering data) that enable vendor-independent test environments (known as test stations)
- harmonized engineering tools for creating the test environments
- standardized test cases for all interfaces mentioned in the section above
- harmonized simulation environments for external components (e.g., object controllers or on-board units) with defined interfaces for manipulating their behavior in accordance with the test cases mentioned above
- a test system for creating and automatically executing the test cases and checking the test results

In addition to standardized processes and tools, it should be emphasized that an overall system consisting of components from different vendors definitely also needs defined mechanisms for logging all standardized interfaces to be able to verify the cause of a fault in a legally compliant manner (known as juridical recording). In particular, internal system interfaces (e.g., between an application and the RTE or between the RTE and the virtualization layer) present new challenges for juridical recording.

4 Approval

The modular architecture of the SIL4 Data Center is also expected to lead to a significantly higher expenditure for validation and assessment. When using multiple implementations

Über standardisierte Prozesse und Tools hinaus ist zu betonen, dass ein Gesamtsystem bestehend aus Komponenten verschiedener Hersteller natürlich auch definierte Mechanismen der Protokollierung aller standardisierten Schnittstellen benötigt, um im Fehlerfall auch rechtswirksam die Fehlerursache nachweisen zu können. Hierbei stellen insbesondere systeminterne Schnittstellen (z. B. zwischen Applikation und RTE, zwischen RTE und Virtualisierung) neue Herausforderungen an die rechtssichere Protokollierung dar.

4 Zulassung

Auch für den Bereich Validierung und Gutachten wird erwartet, dass die modulare Architektur des SIL4 Data Centers zu deutlich höherem Aufwand führen kann. Beim Einsatz mehrerer Implementierungen einzelner Softwarekomponenten (z. B. RTE) muss beispielsweise jede einzelne Kombination in einem SIL4 Data Center validiert werden. Daher ist eine sinnvolle Abwägung zwischen der gewünschten Flexibilität im System und dem dafür erforderlichen Aufwand notwendig. Im Research Report [8] wird genauer darauf eingegangen, welche Aspekte hierbei zu berücksichtigen sind.
Eine wesentliche Randbedingung für eine effiziente Evolution eines bereits zugelassenen Gesamtsystems ist, dass etwaige Änderungen in einzelnen Komponenten (z. B. die Aufrüstung mit neuer Hardware, Einspielen von Patches oder andere Upgrades von RTE-Lösungen) entweder keine erneute E2E-Zulassung erfordern oder dass diese zumindest nicht das Mitwirken der anderen Hersteller erfordert. Hierzu ist ein modulares Zertifizierungskonzept notwendig, welches auch im Research Report [8] näher beleuchtet wird.

5 Betriebs- und Kostenaspekte

Standardisierung, Modularisierung und Zentralisierung sind grundlegende neue Paradigmen, die das SIL4 Data Center einführt, mit entsprechenden wirtschaftlichen Implikationen. Im Research Report [8] wird eine Betrachtung aller erforderlichen Investitionen und erwarteter monetären Vorteile vorgenommen, wobei explizit der

of individual software components (e.g., RTEs), for example, each single component in a SIL4 Data Center must be validated. For this reason, it is necessary to balance the desired flexibility in the system and the necessary expenditure. The Research Report [8] explains in greater detail the aspects that need to be considered.
An essential boundary condition to efficiently evolve an already approved overall system is that any changes to individual components (e.g., upgrading with new hardware, loading patches, or other upgrades of RTE solutions) do neither require E2E reapproval nor, at least, involvement of the other vendors in the reapproval process. For this purpose, a modular approval concept is necessary, which is also described in more detail in the Research Report [8].

5 Operational and cost-related aspects

Standardization, modularization, and centralization are new basic paradigms coming with the SIL4 Data Center, with the corresponding economic implications. In the Research Report [8], all necessary investments and expected cost benefits are analyzed, explicitly considering the entire technology lifecycle from planning through to operation and maintenance. It becomes clear that considerable investments are required on the route to implementation, but the long-term business case appears positive.
In this context, it should be emphasized that the SIL4 Data Center is already advantageous for existing railway applications (e.g., digital interlockings) and is also an essential basis for boosting the digitalization of rail operations, such as fully automated rail operation or moving block operation. In addition, standardization is expected to increase flexibility and reduce the operating costs.

6 Summary

The completed R&D collaboration project examined many aspects that are necessary for implementing and operating a SIL 4

gesamte Technologielebenszyklus von der Planung bis hin zu Betrieb und Wartung beleuchtet wird. Hierbei wird deutlich, dass erhebliche Investitionen bis zur Realisierung unabdingbar sind, der langfristige Business Case jedoch als positiv betrachtet wird.
In diesem Kontext ist zu betonen, dass das SIL4 Data Center bereits vorteilhaft für bestehende Bahnapplikationen ist (z. B. digitale Stellwerke) und zudem auch eine wesentliche Grundlage für einen weiter steigenden Digitalisierungsgrad des Bahnbetriebes darstellt, wie z. B. des vollautomatisierten Fahrens oder des Fahrens mit minimalem Abstand. Zusätzlich werden durch die Standardisierung eine höhere Flexibilität und eine Reduzierung der Betriebskosten erwartet.

6 Zusammenfassung

Die abgeschlossene F&E-Kollaboration hat viele Aspekte, die für die Realisierung und den Betrieb eines SIL4 Data Centers notwendig sind, sowohl aus Hersteller- als auch Betreibersicht untersucht. Hierbei konnte bestätigt werden, dass die zu Beginn dieses Beitrags genannten Ambitionen und Erwartungen an SIL4 Data Center grundsätzlich realistisch und erfüllbar sind.
In dem Zuge wurden auch Themen und Herausforderungen identifiziert, die nicht in dem gegebenen Zeitrahmen behandelt werden konnten und noch zu lösen sind. Die detaillierten Ergebnisse dieser Zusammenarbeit sind in dem Research Report [8] dokumentiert. Die Autoren danken allen Mitwirkenden der Kollaboration für die produktive Zusammenarbeit und freuen sich über Rückmeldung der Leser zu den Ergebnissen. ■

Dieser Artikel entstand im Rahmen einer Forschungskooperation zwischen der Siemens Mobility GmbH (SMO) und der Deutschen Bahn AG (DB), die sich mit der Entwicklung einer Basisarchitektur für SIL4 Data Center beschäftigte. Der umfassende Forschungsbericht kann auf den Homepages von Digitale Schiene Deutschland und Siemens Mobility heruntergeladen werden:
https://digitale-schiene-deutschland.de/en/downloads
https://siemens.com/SIL4-data-center

LITERATUR | LITERATURE

[1] „Future Railway Mobile Communication System (FRMCS)," [Online]. Available: https://uic.org/rail-system/frmcs/
[2] Reference CCS Architecture (RCA), [Online]: https://ertms.be/work-groups/ccs_architecture/
[3] Open CCS On-board Reference Architecture (OCORA), [Online]. Available: https://github.com/OCORA-Public/Publication/
[4] RCA and OCORA, „An Approach for a Generic Safe Computing Platform for Railway Applications," 2020: https://github.com/OCORA-Public/Publication/blob/master/00_Archive%20earlier%20Publications/01_OCORA%20Gamma%20Release/40_Technical%20Documentation/OCORA-40-004-Gamma_Computing-Platform-Whitepaper.pdf (Note: recent update available under: https://github.com/OCORA-Public/Publication/blob/master/04_OCORA%20Delta%20Release/OCORA-TWS03-010_Computing-Platform-Whitepaper.pdf)
[5] RCA and OCORA, „Generic Safe Computing Platform High-level Requirements," 12 2020: https://github.com/OCORA-Public/Publication/blob/master/00_Archive%20earlier%20Publications/01_OCORA%20Gamma%20Release/40_Technical%20Documentation/OCORA-40-013-Gamma_Computing-Platform-Requirements.pdf (Note: recent update available under: https://github.com/OCORA-Public/Publication/blob/master/04_OCORA%20Delta%20Release/OCORA-TWS03-020_Computing-Platform-Requirements.pdf)
[6] Shift2Rail, [Online]. Available: https://shift2rail.org/
[7] EULYNX, [Online]. Available: https://www.eulynx.eu/
[8] Deutsche Bahn, Siemens Mobility, „Research Report - SIL4 Data Center," 2021. [Online]. Available: https://digitale-schiene-deutschland.de/en/downloads; https://siemens.com/SIL4-data-center

Data Center, both from the vendor's and the system operator's perspective. It could be confirmed that the ambitions and expectations placed on SIL4 Data Centers and stated at the beginning of this article are basically realistic and can be met.
In this context, topics and challenges were identified that could not be dealt with within the given timeframe and still need to be resolved. The detailed results of this collaboration project are documented in the Research Report [8]. The authors wish to thank all those involved in the collaboration project for their productive cooperation and look forward to receiving feedback from readers on the results. ■

This article has been written as part of a research collaboration between Siemens Mobility GmbH (SMO) and Deutsche Bahn AG (DB), which focused on developing a basic architecture for SIL4 Data Centers. The comprehensive Research Report can be downloaded from the homepages of Digitale Schiene Deutschland and Siemens Mobility:
https://digitale-schiene-deutschland.de/en/downloads
https://siemens.com/SIL4-data-center

AUTOREN | AUTHORS

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

Tom Suess
Produktmanager für Sicherheitsplattformen / *Product Manager for Safety Platforms*
Siemens Mobility GmbH
Anschrift / *Address*: Nonnendammallee 101, D-13629 Berlin
E-Mail: tom.suess@siemens.com

Dr. Frank Eschmann
Chefarchitekt / *Chief Architect*
DB Systel GmbH
Anschrift / *Address*: Weilburger Straße 26-30, D-60326 Frankfurt a. M.
E-Mail: frank.eschmann@deutschebahn.com

Dr. Patrick Marsch
Leitung Plattformentwicklung / *Lead Platform Development*
Digitale Schiene Deutschland
DB Netz AG
Anschrift / *Address*: Stresemannstraße 123, D-10963 Berlin
E-Mail: patrick.marsch@deutschebahn.com