

Sichere Software-Updates für sicherheitskritische Systeme und Komponenten

Secure software updates for safety critical systems and components

Andres Gonzalez Guilarte | Thomas Gehrke

Der Eisenbahnsektor durchläuft einen tiefgreifenden Wandel mit der Digitalisierung der streckenseitigen und fahrzeugseitigen Systeme, die für die Automatisierung, Datenanalyse, Konnektivität und gemeinsame Mobilität erforderlich sind. Gleichzeitig entwickelt sich die Schiene rasch zum Rückgrat der zukünftigen Mobilität. Sie ist der energieeffizienteste Verkehrsträger, der derzeit für 9 % des weltweiten motorisierten Personenverkehrs und 7 % des Güterverkehrs verantwortlich ist und dabei nur 3 % des gesamten Energieverbrauchs im Verkehrswesen benötigt [5]. In Anbetracht der weltweiten Ausdehnung unserer Städte wird sich die Passagiernachfrage in den nächsten 30 Jahren auf 122 Billionen Passagierkilometer verdreifachen, und der Bahnsektor wird wachsen und sich anpassen müssen, um den Großteil dieser neuen Passagierkilometer zu bewältigen. Siemens Mobility arbeitet an zahlreichen digitalen Lösungen, die es der Bahnindustrie ermöglichen, diese Herausforderung zu meistern. Eine dieser Lösungen ist die Einführung von ferngesteuerten oder zentralisierten Software-Updates, die es Betreibern und Infrastruktureigentümern ermöglichen, die Effizienz der Bahnsysteme kontinuierlich zu verbessern und ihren Lebenszyklus zu verlängern.

1 Einleitung

Um die wachsende Nachfrage nach schnellem, zuverlässigem und klimafreundlichem Transport zu befriedigen, werden sich die Bahnbetreiber in den nächsten Jahrzehnten auf drei Kernelemente konzentrieren: 1. Senkung des Energieverbrauchs, 2. Erhöhung der Kapazität und 3. Erhöhung der Verfügbarkeit der Infrastruktur durch Verringerung der Ausfallzeiten aufgrund ungeplanter Ausfälle oder geplanter Wartungsarbeiten.

Die Kapazität des Schienenverkehrs wird derzeit durch die Einführung des Europäischen Zugsicherungs- und Zugsteuerungssystems (ETCS) und des automatischen Zugbetriebs (ATO) optimiert, welche Daten aus der Infrastruktur, der Strecke und dem Fahrplan verwenden, um das ideale Geschwindigkeitsprofil für die aktuellen Bedingungen zu berechnen. Dies kann die Kapazität um bis zu 30 % erhöhen und bis zu 30 % Energie einsparen.

Die Umstellung auf eine digitale Infrastruktur macht eine Vielzahl von Geräten auf den Gleisen überflüssig und kann so Ausfälle verhindern. Beispielsweise gibt es in Deutschland heute 2800 Stellwerke, 160 000 Signale und 400 000 Kilometer Kabel entlang der Strecken. Dies sind alles Elemente, deren eventueller Ausfall zu Störungen führen kann. Durch eine Migration von Elementen in ein zentralisiertes System können Einsparungen von bis zu 50 % beim Platz- und Energieverbrauch erzielt werden. Weiterhin kön-

The railway sector is currently undergoing a profound transformation with the digitalisation of the trackside and onboard systems that are necessary to deliver automation, data analytics, connectivity and shared mobility. At the same time, rail is also rapidly becoming the backbone of future mobility, as it is the most energy-efficient transport mode that currently accounts for 9 % of global motorised passenger movements and 7 % of freight, while consuming only 3 % of all used transport energy [5]. The expansion of our cities means that passenger demand is set to triple to 122 trillion passenger kilometres in the next 30 years and rail is set to grow and adapt in order to master the majority of these new passenger kilometres. Siemens Mobility is currently working on many digital solutions to enable the rail industry to tackle this challenge, one of them being the introduction of remote or centralised software updates to enable operators and infrastructure owners to continuously improve the efficiency of the railway systems and extend their lifecycles.

1 Introduction

In order to meet the growing demand for fast, reliable and climate-friendly transportation, railway operators will need to focus on three core elements in the next decades: 1) the reduction of energy consumption, 2) increased capacity and 3) increased infrastructure availability achieved by reducing the downtimes caused by either unplanned failures or planned maintenance activities.

Rail capacity is currently being optimised by means of the implementation of the European Train Control System (ETCS) and Automatic Train Operation (ATO) that use data from the infrastructure and the track and train schedule information to calculate the ideal speed profile for the current conditions at any given time. This can increase capacity by up to 30 % and save up to 30 % of energy.

Migrating to a digital infrastructure eliminates the need for a lot of trackside equipment and can thus prevent shutdowns. For example, Germany currently has 2800 interlocking locations, 160,000 signals and 400,000 kilometres of cables spread along its routes. These are all parts that can fail and lead to disruption. The migration of elements to a centralised system enables space and energy savings of up to 50 %. Shutdowns can also be prevented with georedundant centralised systems. Moreover, eliminating hardware obsolescence by moving towards digital infrastructure resolves the 40-year proprietary spare part supply and means that the software becomes the main element to be maintained throughout the lifecycle (fig. 1).

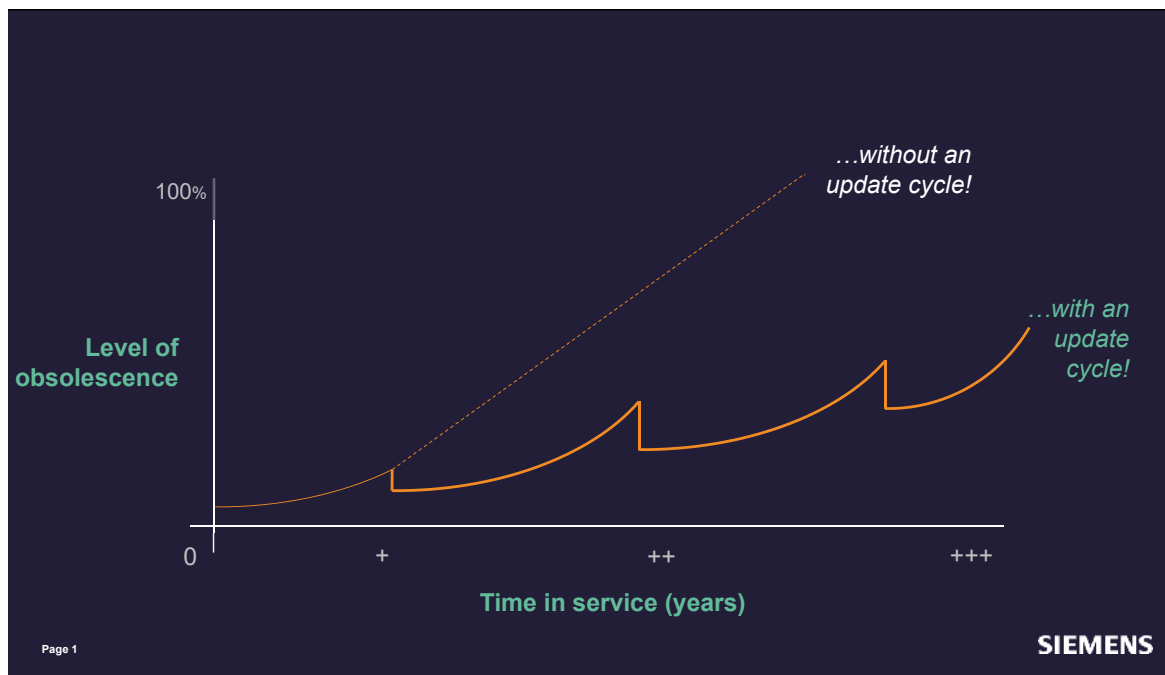


Bild 1: Auswirkung von Software-Updates auf das Lifecycle Management

Fig. 1: Impact of software updates on lifecycle management

nen durch Geo-Redundanz des zentralen Systems Abschaltungen verhindert werden. Außerdem wird durch die Umstellung auf digitale Infrastrukturen die Veralterung der Hardware verhindert, eine Ersatzteilversorgung über 40 Jahre ist nicht mehr erforderlich, und die Software wird zum wichtigsten Element, das während des Lebenszyklus gewartet werden muss (Bild 1).

2 Hauptinhalt

Mit dem CoreShield Remote Software Update (RSU) und dem Betriebssystem CoreShield Secure Long-life Linux (S2L2) setzt Siemens Mobility die Anforderungen nach Remote Software-Updates um.

Das CoreShield S2L2-Betriebssystem wurde entwickelt, um die IT-Sicherheit aller Komponenten und Systeme von Siemens Mobility zu erhöhen. Als wesentlicher Teil der Maßnahmen von Siemens Mobility, die Versionen und Typen von Linux- und Windows-Betriebssystemen bezüglich IT-Sicherheit zu harmonisieren, bietet S2L2 eine standardisierte Architektur für verschiedene Funktionen, die von den verschiedenen Signalisierungskomponenten und -systemen im Zusammenspiel mit IT-Sicherheitsfunktionen benötigt werden. Das zentrale Element für Software-Updates ist das Update Application Programmable Interface (API). Bild 2 präsentiert eine Übersicht über die hierfür von CoreShield S2L2 bereitgestellten API (Application Programmable Interface).

Signalisierungskomponenten, die CoreShield S2L2 als Betriebssystem verwenden, werden als Secure Components bezeichnet und können zu einem System der Sicherheitsstufe (Security Level, SL) 3 gemäß der Norm IEC 62443-3-3 integriert werden.

CoreShield RSU ist ein Produkt, das das Fernladen von Software für Signalisierungskomponenten und -systeme ermöglicht, und zwar sowohl für streckenseitige als auch für fahrzeugseitige Anwendungen, indem es die Aktualisierung von Software, Firmware, Konfigurations- und Lizenzdateien von einer zentralen Stelle aus in einer Anlage ermöglicht. CoreShield RSU unterstützt dabei die von EULYNX [3] definierten Update-Mechanismen in Bezug auf die Software-Update-Schnittstelle, das Datenmodell und die Arbeitsabläufe.

2 The core text

Siemens Mobility has addressed the challenge of software updates with the CoreShield Remote Software Update (RSU) and the CoreShield Secure Long-life Linux operating system (S2L2).

The CoreShield S2L2 operating system has been designed to standardise and increase the security of all Siemens Mobility components and systems. As an essential part of Siemens Mobility efforts to standardise and harmonise the versions and types of Linux and Windows operating systems with regard to security, S2L2 provides a standardised architecture for the different functions required by the various signalling components and systems in conjunction with the security functions. The enabling element in the case of software updates is the Update Application Programmable Interface (API). Fig. 2 provides an overview of the APIs provided by CoreShield S2L2.

Signalling components that use CoreShield S2L2 as their operating system are called Secure Components and can be integrated into a Security Level (SL) 3 compliant system according to the IEC 62443-3-3 standard.

The CoreShield RSU is a product used to remotely update software in signalling components and trackside and onboard applications. It provides a central point for updating software, firmware, configuration data and license files. The CoreShield RSU has also been designed to support the update mechanisms defined by EULYNX [3] with regard to the software update interface, data model and workflows.

The CoreShield RSU consists of the following three core elements in order to achieve a high level of security and the modularity required to carry out the software updates (fig. 3):

1. the Preparation System (a Siemens site)
2. the Deployment System (the infrastructure owner's site)
3. the Update API (the target component or system).

The RSU Preparation System imports software from an internal repository containing software packages provided by Siemens Product Management using project-specific asset management tools. It performs additional measures to create an update package,

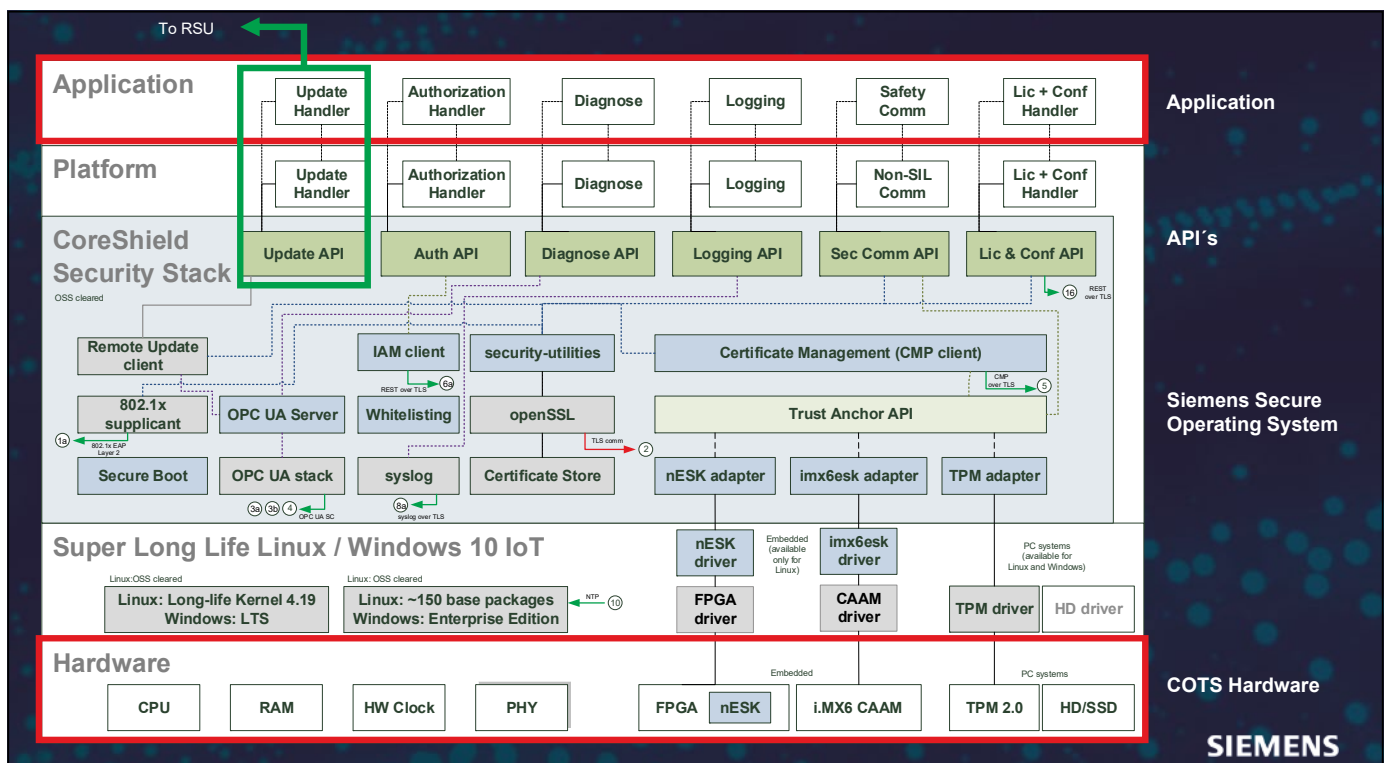


Bild 2: CoreShield S2L2-Komponenten und interne API

Fig. 2: The CoreShield S2L2 building blocks and internal APIs

CoreShield RSU besteht aus den folgenden drei Kernelementen, um ein hohes Maß an Sicherheit und Modularität zu erreichen, das für die Durchführung von Software-Updates erforderlich ist (Bild 3):

1. Vorbereitungssystem (Preparation System, Standort Siemens)
2. Verteilungssystem (Deployment-System, Standort des Infrastrukturbetreibers)
3. Update-API (in Zielkomponente oder -system).

Das RSU-Vorbereitungssystem importiert Software aus einem internen Repository, das die Software-Pakete enthält, die vom Siemens-Produktmanagement mittels projektspezifischer Asset-Management-Tools bereitgestellt wird. Es führt zusätzliche Maßnahmen zur Erstellung eines Update-Pakets durch, z. B. die Signierung des Pakets und die Verschlüsselung seines Inhalts. Das erstellte Aktualisierungspaket wird dann zum Kunden übertragen. Dies kann manuell geschehen, z. B. mithilfe von Massenspeichern oder per Fernübertragung über ein sicheres Netzwerk, wenn eine Netzwerkverbindung vorhanden ist und sichere Gateways implementiert sind. Nach dem Transport wird das Softwarepaket von Siemens überprüft und validiert, um sicherzustellen, dass das Paket, das der Verteilungsserver erhalten hat, gültig ist. Anschließend kann der Betreiber oder Infrastruktureigentümer mit der Einleitung der Verteilung der Software gemäß den jeweiligen Betriebsvorschriften fortfahren (Bild 4).

Am Standort des Infrastrukturbetreibers wird das Aktualisierungspaket im RSU-Verteilungssystem gespeichert. Das Verteilungssystem prüft den Inhalt des Pakets bezüglich Vollständigkeit und Integrität und erstellt einzelne Pakete für die Geräte, die aktualisiert werden sollen. Anschließend überträgt es die einzelnen Pakete über eine standardisierte Schnittstelle auf Basis der OPC-UA-Schnittstellentechnologie [6] an die Geräte. Nachdem das Laden der Software auf die Geräte abgeschlossen ist, orchestriert das Verteilungssystem die Aktivierung der zuvor geladenen Software

such as signing the package and encrypting its contents. The created update package is then transferred to the customer's site. This can either be done manually, e.g. using mass storage devices, or remotely using a secure network transport if a network connection has been established and secure gateways have been implemented. Once it has been transported, the software package is validated and tested by Siemens in order to ensure that the package the deployment server has received is valid. The operator or infrastructure owner can then proceed to initiate the distribution of the software according to their specific operating rules (fig. 4).

The update package is stored in the RSU Deployment System at the infrastructure owner's site. The Deployment System checks the contents of the package with regard to its completeness and integrity and creates individual packages for the devices that are to be updated. It then transfers the individual packages to the devices using a standardised interface based on OPC UA interface technology [6]. Once the software deployment has been completed, the Deployment System orchestrates the activation of the previously deployed software at the devices. If the deployment and activation of a software package fails, the Deployment System can initiate a rollback to any previous software version, as it stores the history and all the previous software and configuration versions.

Many update operations require more than one device to be updated in a single update step, e.g. all devices of a certain type or all devices in a specific geographical area should be updated. The CoreShield RSU provides the concept of stages for this purpose. The updating of all the devices belonging to a stage is handled as a transaction. The devices are updated in parallel. The transaction is only completed and the devices can only become operational if all the devices in the stage have been successfully updated. Otherwise, a rollback can be performed for the devices.

The RSU Deployment System can also have more than one instance running within a railway system. This redundancy increases

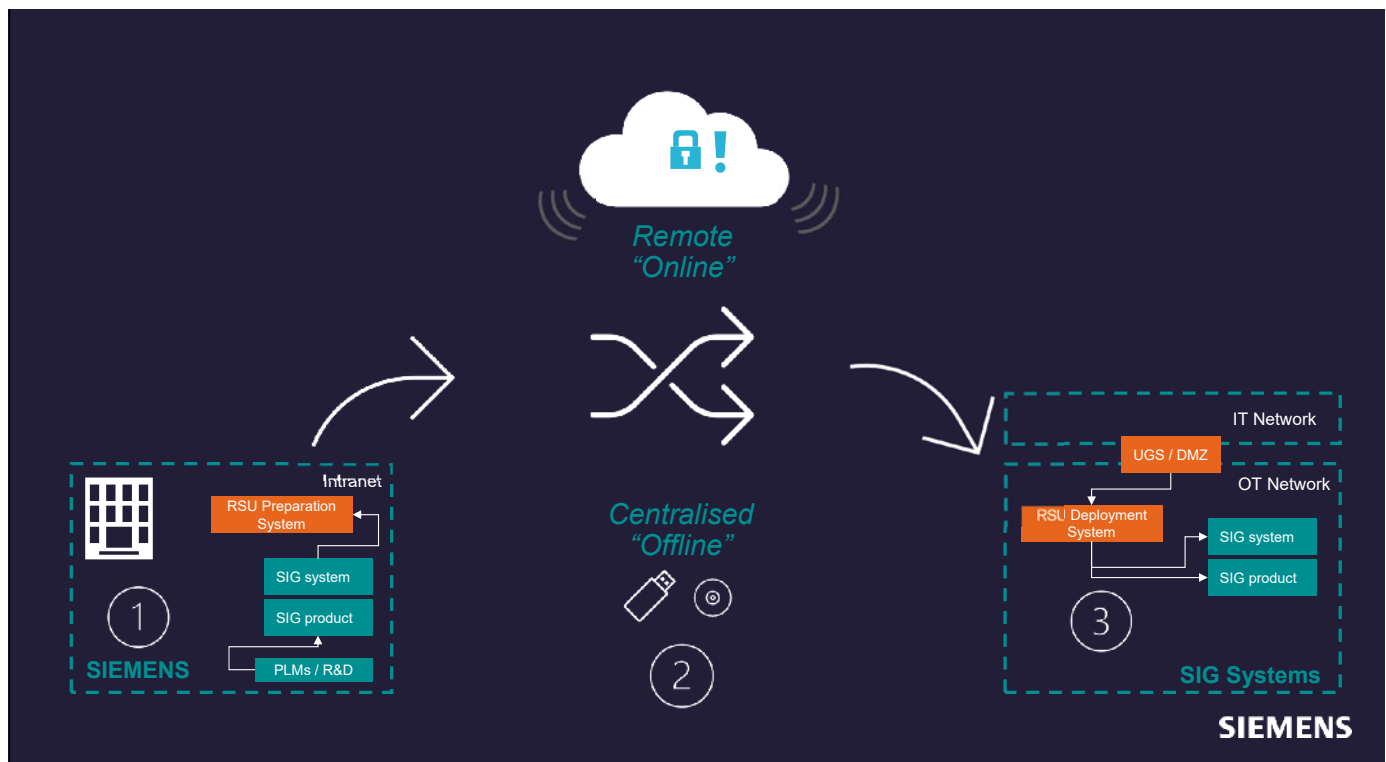


Bild 3: CoreShield RSU High-level-Architektur

Fig. 3: CoreShield RSU high-level architecture

auf den Geräten. Wenn das Laden und die Aktivierung eines Softwarepakets fehlschlagen, kann das Verteilungssystem ein Roll-back zu den vorherigen Softwareversionen einleiten, da es die Historie und alle vorherigen Software- und Konfigurationsversionen speichert.

Bei vielen Aktualisierungsvorgängen ist es erwünscht, mehr als ein Gerät in einem einzigen Aktualisierungsschritt zu aktualisieren. Beispielsweise sollen alle Geräte eines bestimmten Typs oder alle Geräte in einem bestimmten geographischen Gebiet aktualisiert werden. Hierfür bietet CoreShield RSU das Konzept der Stufen. Die Aktualisierung aller Geräte, die zu einer Stufe gehören, wird als eine Transaktion behandelt. Die Geräte werden parallel aktualisiert. Erst wenn alle Geräte der Stufe erfolgreich aktualisiert wurden, ist die Transaktion abgeschlossen und die Geräte können in Betrieb genommen werden. Andernfalls kann ein Roll-back für die Geräte durchgeführt werden.

Das RSU-Verteilungssystem kann innerhalb eines Bahnsystems auch in mehreren Instanzen vorhanden sein. Diese Redundanz erhöht die Verfügbarkeit der Software-Update-Infrastruktur. Darüber hinaus wird die Leistung bei der Aktualisierung großer Mengen von Geräten durch Lastverteilung erhöht. Bei sicherheitskritischen Systemen bis zum Safety Integrity Level 4 (SIL4) garantiert CoreShield RSU, dass der Aktualisierungsprozess die Sicherheitseigenschaften von Sicherheitskomponenten oder -systemen nicht beeinträchtigt. Es wird sichergestellt, dass die neuen Softwarepakete vollständig und unverändert an die richtigen Komponenten geliefert und installiert werden. Weiterhin wird verhindert, dass ein Gerät mit einer falschen Softwareversion in Betrieb geht. Dies ist insbesondere für sicherheitskritische Geräte von zentraler Bedeutung. Für dieses Szenario beinhaltet das Verfahren Maßnahmen, die sicherstellen, dass die richtige Softwareversion auf den Geräten installiert wird. Einige Maßnahmen werden von CoreShield RSU durchgeführt, andere werden von den Secure Components selbst realisiert. Die Integrität und

es the availability of the software update infrastructure. Moreover, it also increases the performance when updating large sets of devices due to load-balancing. In the case of safety-critical systems up to Safety Integrity Level 4 (SIL4), the CoreShield RSU guarantees that the update process does not compromise the safety characteristics of any safety components or systems. It is necessary to ensure that the new software packages are delivered to and installed in the correct components in a complete and unchanged form. Furthermore, it is also necessary to prevent devices with a false software version becoming operational. This is especially important for safety-critical systems. In this scenario, the CoreShield RSU includes several measures to ensure that the correct software version has been installed. Some measures are performed by the CoreShield RSU and others are performed by the safety components themselves. The integrity and completeness of an update package is ensured by the specific encoding of the package and by the verification of checksums that include device-specific information. To this end, the RSU Preparation System generates the necessary information and performs the corresponding modifications to the update packages. The verification of the checksums is either performed automatically or involves interaction with the operator at the RSU Deployment System, depending on the checksum type. The RSU Deployment System will then communicate with a Secure Component using S2L2 or with a legacy component using a so-called SDS agent (fig. 5).

The measures and processes for safety updates are implemented as modules in the update process and can therefore be omitted if so desired or if they are unnecessary. As such, they do not complicate the updating of any non-safety-critical components. It is possible to update a complete software image or individual software layers, such as the operating system or individual applications, depending on the complexity of the device being updated. Updates of individual applications are especially impor-

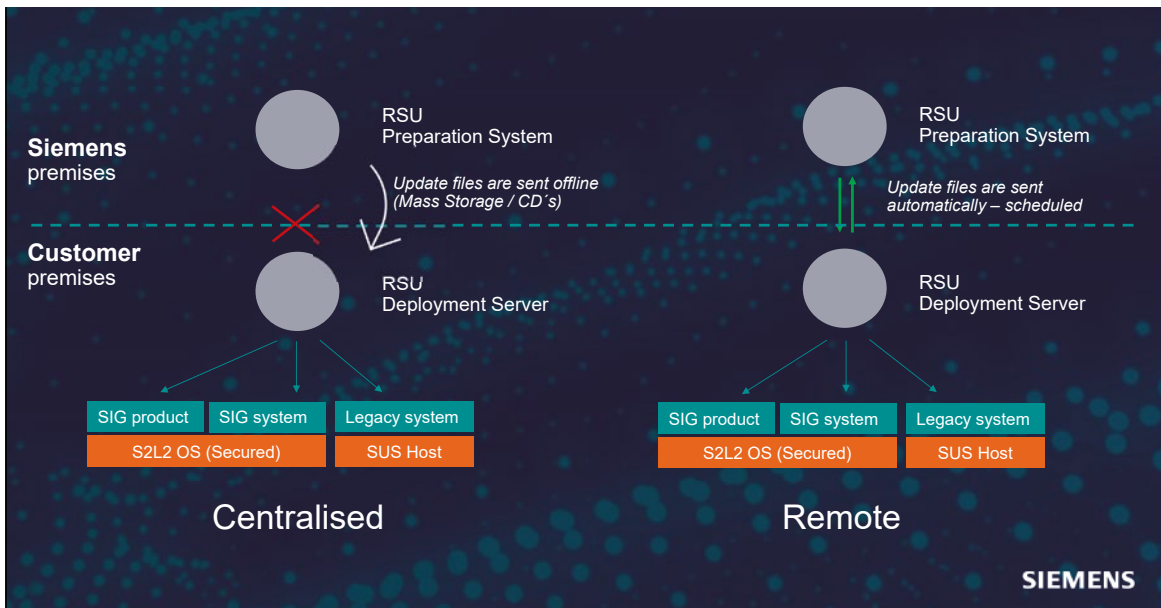


Bild 4: Betriebsarten von CoreShield RSU
Fig. 4: CoreShield RSU operating modes

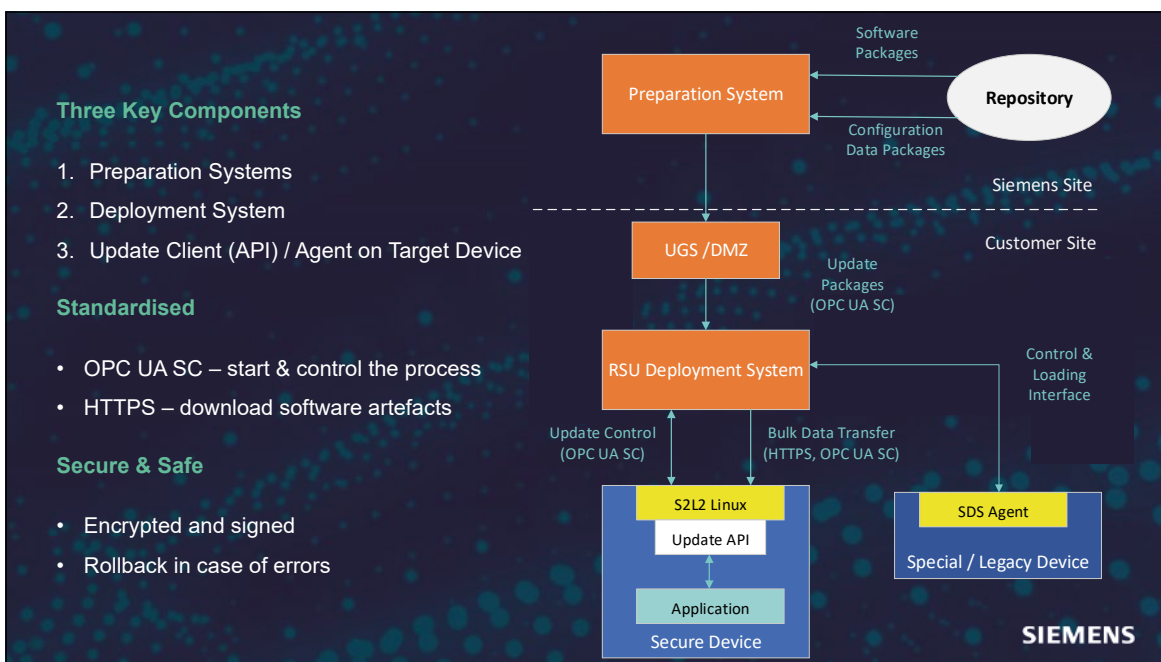


Bild 5: CoreShield RSU-Komponenten
Fig. 5: CoreShield RSU components

Vollständigkeit eines Updatepakets wird durch eine spezielle Kodierung des Pakets und durch die Überprüfung von Prüfsummen, die gerätespezifische Informationen enthalten, sichergestellt. Dazu generiert das RSU-Vorbereitungssystem die notwendigen Informationen und nimmt die entsprechenden Änderungen an den Update-Paketen vor. Die Überprüfung der Prüfsummen erfolgt je nach Prüfsummentyp entweder automatisch oder durch Interaktion mit dem Betreiber am RSU-Verteilungssystem. Das RSU-Verteilungssystem interagiert dann mit einer Secure Component über von S2L2 bereitgestellte Mechanismen oder mit einer Altkomponente über einen sogenannten SDS-Agenten (Bild 5).

Die Maßnahmen und Prozesse für Sicherheitsupdates sind als Module im Updateprozess implementiert und können, wenn gewünscht oder nicht notwendig, weggelassen werden. Sie erschweren somit nicht das Update von nicht-sicherheitskritischen Komponenten und Systemen.

tant for SIL4 Data Centres that host virtualised safety-critical applications [4]. This enables a virtualised device to be updated without influencing the other devices that are still operational at the same Data Centre.

The CoreShield RSU is part of the CoreShield product family and it has therefore been designed to seamlessly integrate with other security systems, such as CoreShield Identity & Access Management (IAM) for checking roles and permissions or the CoreShield Shared Security Infrastructure (SSI) for certificate management and other functions ensuring compliance with the system level requirements for SL3 according to IEC 62443-3-3. When required, the CoreShield RSU can also run as a stand-alone or even be integrated with an existing IT security infrastructure. As a CoreShield system, the CoreShield RSU fulfils the requirements for SL3 in accordance with IEC 62443-4-2 [2]. Moreover, the CoreShield RSU has been developed in accord-

Je nach Komplexität eines zu aktualisierenden Gerätes ist es möglich, das komplette Software-Image oder einzelne Software-schichten wie das Betriebssystem oder einzelne Anwendungen zu aktualisieren. Die Aktualisierung einzelner Anwendungen ist besonders wichtig für SIL4-Rechenzentren, die virtualisierte sicherheitskritische Anwendungen hosten [4]. Dies ermöglicht die Aktualisierung eines virtualisierten Geräts, ohne die anderen Geräte, die im selben Rechenzentrum noch in Betrieb sind, zu beeinflussen.

CoreShield RSU ist Teil der CoreShield-Produktfamilie und daher für eine nahtlose Integration mit anderen Sicherheitssystemen ausgelegt. Hierzu gehören beispielsweise CoreShield Identity & Access Management (IAM) für die Überprüfung von Rollen und Berechtigungen sowie die CoreShield Shared Security Infrastructure (SSI) für das Zertifikatsmanagement und andere Funktionen, um die Anforderungen auf Systemebene für IT-SIL3 gemäß IEC 62443-3-3 zu erfüllen. CoreShield RSU kann bei Bedarf auch eigenständig betrieben oder in eine bestehende IT-Sicherheitsinfrastruktur integriert werden. Als CoreShield-System erfüllt CoreShield RSU die Anforderungen des SIL3 gemäß IEC 62443-4-2 [2]. Darüber hinaus wurde die CoreShield RSU nach dem GUIDE-Entwicklungsprozess von Siemens Mobility entwickelt, der nach IEC 62443-4-1 [1] für die Entwicklung von SIL3-Komponenten zertifiziert wurde.

3 Zusammenfassung

In Anbetracht des aktuellen Umfelds von Bahnsystemen und der Herausforderungen, die das zukünftige Wachstum mit sich bringt, müssen ferngesteuerte und zentralisierte Software-Updates als eine Kernfunktion bei der Migration zu einer digitalen Infrastruktur betrachtet werden, da Software durch ihre zunehmende Bedeutung der wesentliche Bestandteil ist, der während des Lebenszyklus eines jeden digitalen Bahnsystems zu warten ist.

Software-Updates für sicherheitskritische Systeme sind aufgrund ihrer Auswirkungen auf die Sicherheitssysteme und der Vielzahl der heute existierenden Schnittstellen sehr komplex. Daher investiert Siemens Mobility kontinuierlich in die Förderung und die Weiterentwicklung von Software-Update-Funktionen und ihre Standardisierung in der Bahnindustrie. Daher sind die Funktionalität und die Implementierung von CoreShield RSU eng mit EULYNX und dem SIL 4-Data-Center-Ansatz von Siemens Mobility und der Deutschen Bahn AG abgestimmt [4]. ■

ance with the GUIDE development process at Siemens Mobility that has been certified for the development of SIL3 components in accordance with IEC 62443-4-1 [1].

3 Conclusion

Considering the current environment for railway systems and the challenges that come with future growth, remote or centralised software updates must be considered as a core function when migrating to a digital infrastructure, because the role of software has become prevalent and it is now the main element to be maintained during the lifecycle of any digital railway system. Software updates for safety critical systems are highly complex due to their implications for safety systems and the variety of interfaces that exists today. As such, Siemens Mobility is continuously investing in supporting and further developing these types of functions and their standardisation in the railway industry. This means that the functionality of the CoreShield RSU and its implementation are closely aligned with EULYNX and the SIL 4 Data Centre approach of Siemens Mobility and Deutsche Bahn AG [4]. ■

LITERATUR | LITERATURE

- [1] IEC 62443-4-1:2018. "Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements"
- [2] IEC 62443-4-2:2019. "Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components"
- [3] EULYNX, [Online]. Available: <https://www.eulynx.eu>
- [4] Steffens, S.; Suess, T.; Eschmann, F.; Marsch, P.: SIL4 Data Center – eine neue Plattform-Architektur für sichere Bahnanwendungen, SIGNAL+DRAHT (113) 10/2021
- [5] IEA [Online]. Available: <https://www.iea.org/reports/rail>
- [6] OPC UA [Online]. Available: <https://opcfoundation.org/about/opc-technologies/opc-ua/>

AUTOREN | AUTHORS

Andres Gonzalez Guilarte

Leiter des Cybersecurity Center of Excellence /
Head of Cybersecurity Center of Excellence
E-Mail: andres.guilarte@siemens.com

Dr. Thomas Gehrke

Principal Key Expert für Digitalisierung und Diagnose /
Principal Key Expert for Digitalization and Diagnostics
E-Mail: gehrke.thomas@siemens.com

Beide Autoren / both authors:

Siemens Mobility GmbH

Anschrift / Address: Ackerstraße 22, D-38126 Braunschweig