Entwicklung einer neuen Safety-Plattform DS3 – vom Forschungsprojekt bis zur Inbetriebnahme

The development of the new DS3 safety platform – from the research project to commissioning

Sonja Steffens | Walter Valvoda

Seit über zehn Jahren gestaltet und standardisiert der Bahnsektor die Streckenarchitektur im Rahmen der Projekte Neupro im nationalen und Eulynx im internationalen Kontext. Proprietäre Lösungen für eine Gesamtfunktionalität „Stellwerk" werden separiert in funktionale Stellwerkslogik und eigensichere Außenanlagensteuerung (z. B. Lichtsignale, Achszähler) mit standardisierten IP-basierten Kommunikationsschnittstellen. Dieser Architekturwandel zum „Digitalen Stellwerk" (DSTW) bietet die Möglichkeit der vollständigen Zentralisierung der sicherungstechnischen Bahnapplikationen wie Stellwerkslogik und RBC-Logik. Hieraus ergibt sich im nächsten Schritt der Digitalisierung die Anforderung zur Nutzung von industriellen Commercial-off-the-Shelf-(COTS)-Multicore-Rechnern, um die verfügbare Technologie für rechenzeitintensive Bahnapplikationen zu nutzen und die verwendete Hardware in zentralisierten Rechenzentren zu standardisieren. Hieraus resultiert die Option für eine vollständige Zentralisierung mit geographischer Redundanz für höchstmögliche Verfügbarkeit.

1 Forschungsprojekt (2013 bis 2015)

„Nutzung von COTS-Multicore-Technologie ohne jegliche spezifische Hardware" – dies ist eine gewaltige Anforderung für die

The rail sector has been designing and standardising track architecture as part of the Neupro project in Germany and the Eulynx project in an international context for more than ten years now. Proprietary solutions for overall "interlocking" functionality are subdivided into the functional interlocking logic and the intrinsically safe field element controllers (e.g. signals or axle counters) with standardised IP-based communication interfaces. This architectural change to a "digital interlocking" offers the possibility of completely centralising safety-related railway applications such as the interlocking logic and RBC logic. As such, the next step of digitalisation requires the use of industry-standard commercial off-the-shelf (COTS) multicore computers in order to use the available technology for computationally intensive railway applications and to standardise the hardware used in centralised data centres. This will result in the option of complete centralisation with geographic redundancy for the highest possible availability.

1 The research project (2013 to 2015)

"The usage of COTS multicore technology without any specific hardware" – this is a huge requirement for the signalling

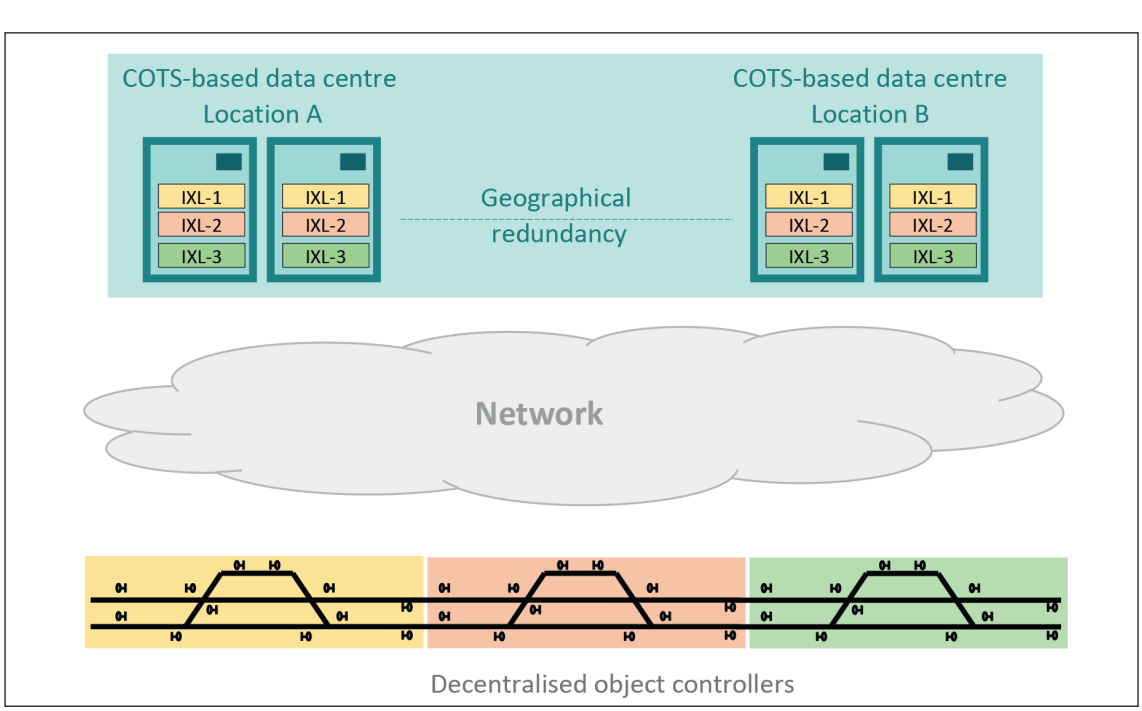

Bild 1: Zentralisierte DSTW (IXL-1/2/3) in COTS-basierten Rechenzentren mit geographischer Redundanz
Fig. 1: Centralised digital interlockings (IXL-1/2/3) in COTS-based data centres with geographical redundancy
Quelle aller Bilder / *Source all images*: Siemens Mobility

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

Sicherungstechnik, mit der sich Siemens Mobility seit mehreren Jahren beschäftigt.

Ende 2011 startete das vom BMBF geförderte und vom Forschungsverbund SafeTRANS organisierte Förderprojekt „Automotive Railway Avionics Multicore Systems“ (ARAMiS https://news.safetrans-de.org/ausgabe-2012-02/aramis.html) mit dem Ziel, den breiten Einsatz von Multicore-Rechnern, die hohe Anforderungen hinsichtlich Sicherheit, Zuverlässigkeit und Schutz gegen unbefugten Zugriff erfüllen müssen, vorzubereiten.

Zunächst waren nur die Domänen Automotive und Avionics vertreten, um Hard- und Software-Architekturen sowie Methoden zu untersuchen, welche die Anwendung von Multicore-Systemen und Virtualisierung erlauben.

Anfang 2013 stieß ein Team von Siemens Mobility und TÜV Rheinland zu ARAMiS dazu. Im Rahmen der Untersuchungen konnte gezeigt werden, dass sich Multicore-Technologie grundsätzlich für sicherungstechnische Eisenbahnanwendungen eignet.

Die konkreten Anforderungen waren:

- Nutzung industrieller COTS-Multicore-Technologie
- Erreichen der Sicherheits- und Verfügbarkeitsziele für Bahnanwendungen mit Zentralisierung und geographischer Redundanz
- Skalierbarkeit für die Integration beliebiger Anwendungen beliebiger Sicherheitslevel („mixed SIL“) auf derselben COTS-Hardware
- Flexibilität in der Kommunikationsarchitektur für Kommunikationsteilnehmer beliebiger Sicherheitslevel.

Das Ergebnis des Forschungsprojekts war ein technisches Architektur- und Sicherheitskonzept zur Definition einer softwarebasierten Sicherheitsplattform „Distributed Smart Safe System“ (DS3®) für den Betrieb von SIL-4-Anwendungen auf beliebigen COTS-Multicore-Rechnern.

Das DS3-Konzept basiert auf einer Architektur mit folgenden wesentlichen Merkmalen:

- Eine sicherungstechnische Anwendung (z. B. Stellwerkslogik) läuft parallel zeitgleich in mehreren Instanzen = Replikanten (Rep) auf unterschiedlichen physikalischen CPU-Kernen.
- Jeder Replikant läuft als zyklische Task (z. B. 200-ms-Takt) getriggert von einer sicheren Uhr (CoarseClock).
- Die Ergebnisse (= Ausgaben) der einzelnen Replikanten werden von einem sicheren Voter geprüft.
- Das Ergebnis des Votings wird über ein sicheres Protokoll-Gateway an angeschlossene Systeme gesendet.
- Das Sicherheitskonzept betrachtet die physikalischen Kerne eines Multicore-Rechners als Hardware-Einheit. Sichere Anwendungen laufen in mindestens zwei physikalischen Kernen in diversitären = „colored“ Code-Emulatoren mit diversitär implementierten Sicherheitsmechanismen (z. B. zyklische Speicherprüfungen, Selbstprüfungen, Rechenoperationen, diversitäres Speichermanagement, Kanalbeteiligung).
- Als Redundanzkonzept kann die Anzahl der Replikanten auf einem Rechner erhöht und das System redundant, d. h. auf zwei Rechnern laufend, aufgebaut werden. Ausgefallene Replikanten oder Rechner werden neu gestartet und wieder mit den laufenden Replikanten synchronisiert.
- Jegliche Kommunikation zwischen den Komponenten erfolgt über ein neu definiertes IP-basiertes Kommunikationsprotokoll XDM mit Publish / Subscribe-Mechanismus über einen zentralen nicht sicherheitsrelevanten Message-Broker für die Nachrichtenverteilung.

Im Zuge des Forschungsprojekts wurde das grobe technische DS3-Konzept erarbeitet, es wurden Softwareanteile als Demonstratoren prototypisch entwickelt und die grundsätzliche Tauglichkeit des Konzepts wurde von einem Gutachter des TÜV Rheinland bestätigt.

and safety systems that Siemens Mobility has been working on for several years.

The “Automotive Railway Avionics Multicore Systems” funding project (ARAMiS https://news.safetrans-de.org/ausgabe-2012-02/aramis.html) funded by the Federal German Ministry of Education and Research (BMBF) and organised by the SafeTRANS research association was launched at the end of 2011 with the aim of preparing for the widespread use of multicore computers that have to meet high requirements in terms of safety, reliability and protection against unauthorised access.

Initially, only the automotive and avionics domains were represented in the investigation into hardware and software architectures and methods that allow the application of multicore systems and virtualisation.

A team from Siemens Mobility and TÜV Rheinland joined ARAMiS at the beginning of 2013. The investigations showed that multicore technology is basically suitable for safety-related railway applications.

The specific requirements were:

- the use of industry-standard COTS multicore technology
- the achievement of the safety and availability objectives for railway applications with centralisation and geographical redundancy
- scalability for the integration of applications at any safety level (“mixed SIL”) into the same COTS hardware
- a flexible communication architecture for communication partners of any safety level.

The research project resulted in a technical architecture and safety concept for the definition of a software-based “Distributed Smart Safe System” (DS3®) safety platform for running SIL 4 applications on any COTS multicore computers.

The DS3 concept is based on an architecture with the following characteristics:

- a safety-related application (e.g. interlocking logic) simultaneously runs in parallel in multiple instances = replicants (Rep) on different physical CPU cores.
- each replicant runs as a cyclic task (e.g. 200 ms clock) triggered by a safe clock (CoarseClock).
- the results (= outputs) of the individual replicants are checked by a safe voter.

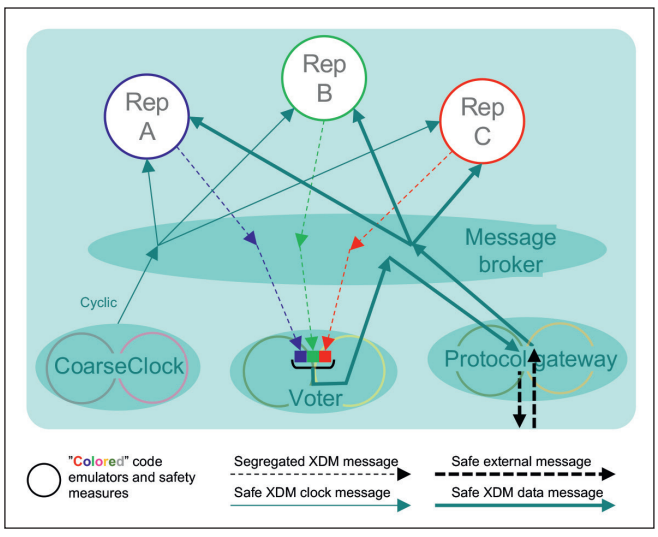

Bild 2: Prinzipielle Architektur der DS3-Plattform
Fig. 2: Basic architecture of the DS3 platform

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

Auf der InnoTrans 2014 wurde von Siemens Mobility eine Demonstration „Stellwerkslogik läuft auf mehreren CPU-Kernen geographisch redundant verteilt in Berlin und München“ ausgestellt. Damals wurden die Tragweite und das Potenzial eines solchen Konzepts von der Fachöffentlichkeit jedoch noch nicht voll erkannt.
Bei Abschluss des Forschungsprojekts 2015 stellte sich die Frage: Wie geht es weiter?

2 Machbarkeitsuntersuchung (2016 bis 2017)

Da 2015 Siemens-Mobility-intern das Potenzial dieses Konzepts zwar erkannt wurde, aber noch nicht alle von der tatsächlichen Machbarkeit und Zulassungsfähigkeit des DS3-Konzepts überzeugt waren, folgte eine Machbarkeitsuntersuchung mit den Zielen:

- Klärung offener, nicht zu Ende gedachter Punkte (z. B. softwarebasiertes sicheres Voting und sichere CoarseClock)
- Definition eines Migrationskonzepts für existierende Bahnanwendungen
- Berücksichtigung der Kommunikationsprotokolle für Eulynx / NeuPro
- Sicherheitsbetrachtung und gutachterliche Bewertung bzgl. der Zulassungsfähigkeit von Bahnanwendungen
- Praktische Bestätigung der Machbarkeit durch prototypische Umsetzung und Migration einer ganz konkreten Stellwerksanwendung.

2.1 Stellwerksprodukt Trackguard Simis AT als Proband

Bei der Auswahl des Probanden für die praktische Machbarkeitsuntersuchung fiel die Entscheidung auf das Stellwerksprodukt Trackguard Simis AT.
Dieses basiert auf der Rechnerplattform Trackguard Simis ECC, beinhaltet im Stellwerksrechner (STWR) eine SIL-4-Stellwerksanwendung für österreichische Bahnen und hat IP-basierte Kommunikationsschnittstellen zu den Ein- / Ausgabe-Rechnern (EAR), zum Nachbarstellwerk (NSTW), zur Leittechnik (OCS) und zur Diagnose.
Für die Migration der STWR-Anwendung auf die DS3-Plattform ergab sich folgende Konfiguration:

- Der zentrale STWR läuft mit der Software-Plattform DS3 auf zwei COTS-Multicore-Rechnern.
- Die beiden STWR synchronisieren sich kontinuierlich; bei Ausfall eines STWR läuft der andere STWR als sicheres System weiter.
- Jegliche Kommunikation zu angeschlossenen Rechnern ([X25]-Protokoll und [Sahara]-Protokoll) erfolgt zweikanalig; hierbei sind die beiden Transportkanäle (A/B) auf die beiden STWR verteilt.
- Die Kommunikationsschnittstellen des STWR sind von dem Plattformwechsel ECC -> DS3 unberührt, d. h., der Plattformwechsel ist rückwirkungsfrei auf die angeschlossenen Systeme.

Der STWR war ein idealer Proband für diese Machbarkeitsuntersuchung, weil damit nicht nur die grundsätzliche Machbarkeit der neuen DS3-Plattform, sondern insbesondere auch der Aspekt „Migration einer existierenden ECC-basierten Bahnapplikation auf die neue DS3-Plattform“ betrachtet werden konnte.

2.2 Portierung des ECC-Betriebssystems

Bei der Migration des STWR sollten die grundsätzlichen Dienste des ECC-Betriebssystems (Basic ECC OS) mit auf die neue DS3-Plattform portiert werden, um die Auswirkungen auf die existierende zugelassene STWR-Applikation auf ein Minimum zu reduzieren.
Dieser Aspekt war von großer Bedeutung, weil damit der Weg für die Migration weiterer ECC-basierter Bahnapplikationen (z. B. andere Stellwerksprodukte, RBC) vorbereitet werden sollte.

- the results of the voting process are sent to the connected systems via a safe protocol gateway.
- the safety concept considers a multicore computer's physical cores to constitute a hardware unit. Safety-related applications run on at least two physical cores in diverse (= “coloured”) code emulators with diversely implemented safety mechanisms (e.g. cyclic memory tests, self-tests, arithmetic operations, diverse memory management and channel involvement).
- the number of replicants on a computer can be increased as a redundancy concept and the system can be designed redundantly, i.e. running on two computers. Failed replicants or computers are restarted and re-synchronised with the running replicants.
- All communication between the components is done via a newly defined IP-based communication protocol, XDM, with a publish/subscribe mechanism via a central non-safety-related message broker for message distribution.

During the research project, the rough DS3 technical concept was developed, software components were prototyped as demonstrators and the basic suitability of the concept was confirmed by an assessor from TÜV Rheinland.
Siemens Mobility exhibited a demonstration of an interlocking logic running on multiple CPU cores with redundant geographical distribution across Berlin and Munich at InnoTrans 2014. At that time, however, the scope and potential for such a concept was yet to have been fully recognised by the professional public. When the research project ended in 2015, the question was “What's next?”

2 The feasibility study (2016 to 2017)

Siemens Mobility had internally recognised the potential of this concept since 2015, but not everyone was yet convinced of the actual feasibility and approvability of this DS3 concept. As such, a feasibility study followed with the following objectives:

- clarification of any open points that had not yet been well thought through (e.g. the software-based safe voting and safe CoarseClock)
- the definition of a migration concept for existing railway applications
- consideration of the communication protocols for Eulynx/ NeuPro
- a safety investigation and assessment regarding the approvability of railway applications
- practical confirmation of the feasibility through the implementation of a prototype and the migration of a specific interlocking application.

2.1 The Trackguard Simis AT interlocking product as the pilot application

When selecting the pilot application for the practical feasibility test, a decision was made in favour of the Trackguard Simis AT interlocking product.
This product is based on the Trackguard Simis ECC computer platform, contains a SIL 4 interlocking application for railway lines in Austria in the interlocking computer (STWR) and has IP-based communication interfaces to the input/ output computers (EAR), adjacent interlocking (NSTW), operations control system (OCS) and diagnostics.
The following configuration was used to migrate the interlocking computer application to the DS3 platform:

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

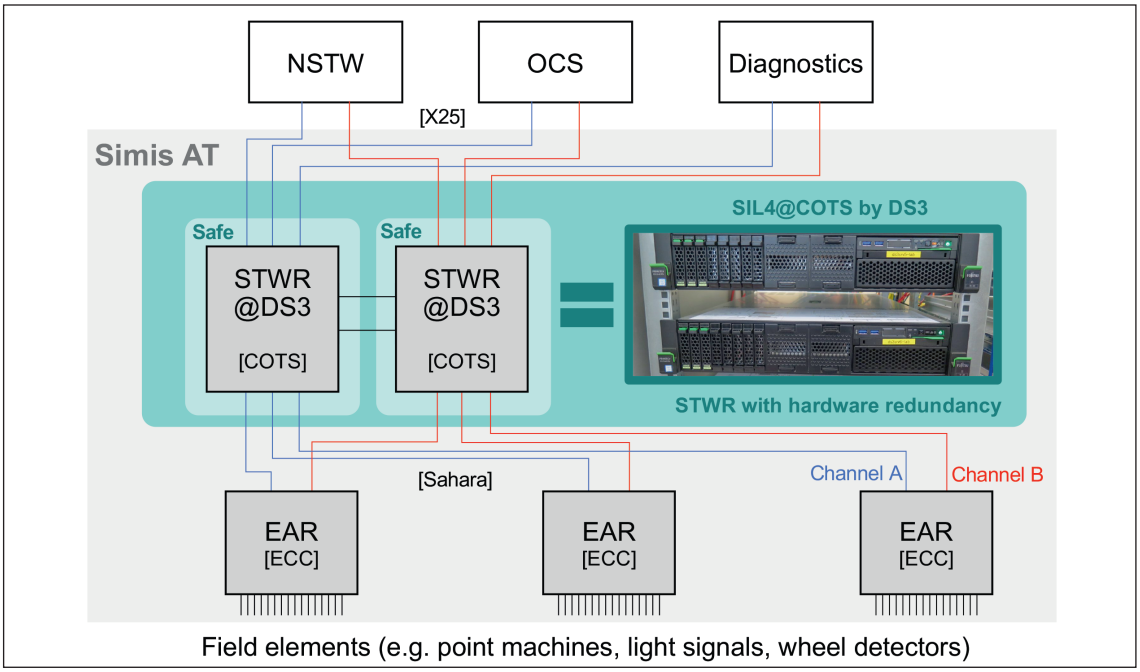

Bild 3: Architektur Trackguard Simis AT mit STWR@DS3
Fig. 3: Trackguard Simis AT with an STWR@DS3 architecture

In der Machbarkeitsuntersuchung wurden Softwarekomponenten der DS3-Plattform (z. B. Code-Emulator, Message-Broker, rudimentäres Voting) prototypisch entwickelt und die ECC-Betriebssystemanteile provisorisch für den Betrieb mit DS3 angepasst.
Dadurch konnte die STWR-Applikation direkt – ohne jegliche Anpassung – eingebettet in das neue ECC-Betriebssystem und DS3 auf COTS-Hardware zum Laufen gebracht werden, und das war die praktische Bestätigung, dass das grundsätzliche DS3-Konzept funktioniert.
Zugleich war das für die über 30 Jahre lang evolutionär weiterentwickelte STWR-Applikation des Trackguard Simis AT die dritte Plattform-Generation: 1990 mit Plattform SCM86, 2000 mit Plattform ECC, 2018 mit Plattform DS3.

2.3 Preliminary Hazard Analysis

Parallel zu den prototypischen Entwicklungen wurden architektonische Verfeinerungen des technischen Konzepts erarbeitet und die Sicherheitsbetrachtungen mittels einer Preliminary Hazard Analysis erstellt und begutachtet mit dem Ergebnis: „Mit DS3 kann der Betrieb von SIL-4-Applikationen auf COTS-Hardware erreicht werden".
Damit waren die Weichen für den Start des Entwicklungsprojekts für das erste Release der DS3-Plattform gestellt.

3 Entwicklungsprojekt (2017 bis 2020)

Das Entwicklungsprojekt startete mit der Aufgabe, etwas komplett Neuartiges von Anfang an zu entwickeln mit folgenden Herausforderungen.

3.1 „Mixed SIL" innerhalb der DS3-Plattform

Die komponentenorientierte DS3-Architektur definierte sowohl sicherheitsrelevante Anteile (Ablaufumgebung für Replikanten, Voting, CoarseClock, Protokoll-Gateway) als auch nicht sicherheitsrelevante Anteile (Message-Broker, Diagnose, Start-up), die gemeinsam auf einem nicht sicherheitsrelevanten Betriebssystem (Windows, Linux) ablauffähig sind.
Dieser Aspekt der unterschiedlichen SIL-Level innerhalb von DS3 musste sowohl bei der Definition des plattforminternen Kommunikations-

- the central interlocking computer runs with the DS3 software platform on two COTS multicore computers.
- the two interlocking computers synchronise continuously; if one interlocking computer fails, the other interlocking computer continues to run as a safe system.
- all communication with the connected computers (the X25 and Sahara protocols) takes place in dual-channel mode with the two transport channels (A/B) distributed between the two interlocking computers.
- the communication interfaces of the interlocking computer are unaffected by the ECC -> DS3 platform change, i.e. the platform change has no effect on the connected systems.

The interlocking computer was the ideal pilot application for this feasibility study, because both the basic feasibility of the new DS3 platform and "migration of an existing ECC-based railway application to the new DS3 platform" could be examined.

2.2 Porting the ECC operating system

When migrating the interlocking computer, the basic ECC operating system services (basic ECC OS) were also supposed to be ported to the new DS3 platform in order to minimise the impact on the existing approved interlocking computer application.
This aspect was of great importance, because it was intended to pave the way for the migration of other ECC-based railway applications (e.g. other interlocking products, RBC).
The software components of the DS3 platform (e.g. the code emulator, message broker and rudimentary voting) were prototyped and the ECC operating system components were provisionally adapted for operation with DS3 in the feasibility study.
This allowed the interlocking computer application to run directly – without any customisation – embedded in the new ECC operating system and DS3 on COTS hardware and confirmed that the basic DS3 concept works in practical terms.
At the same time, this was the third platform generation for the Trackguard Simis AT interlocking computer application, which has been undergoing evolutionary development for over 30 years: in 1990 with an SCM86 platform, in 2000 with an ECC platform and in 2018 with a DS3 platform.

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

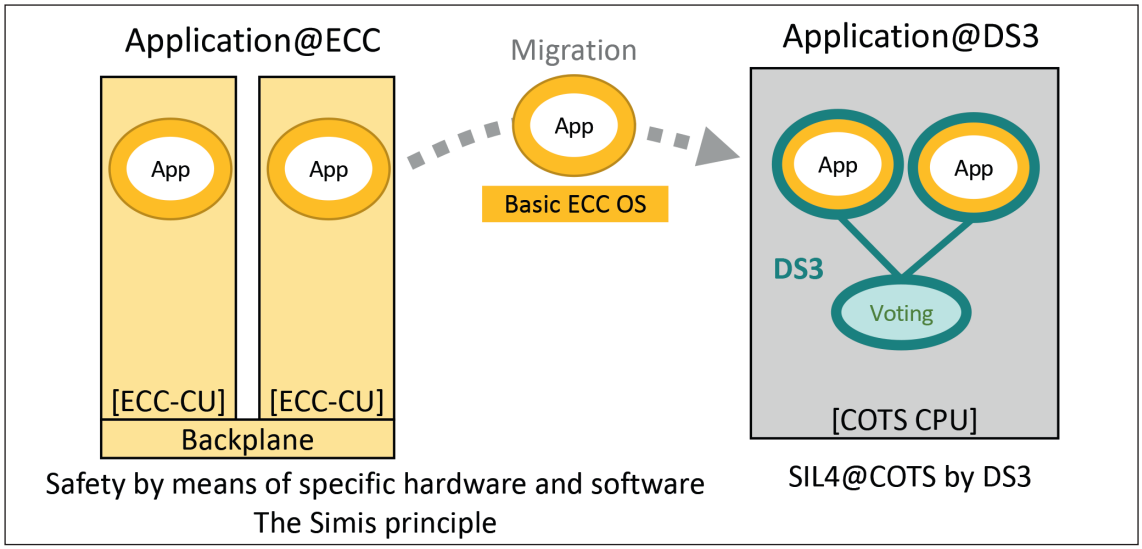

Bild 4: Portierung des ECC-Betriebssystems zu DS3
Fig. 4: Porting the ECC operating system to DS3

protokolls XDM als auch bei der funktionalen Architektur der DS3-Softwarekomponenten berücksichtigt werden.

3.2 Sicheres Kommunikationsprotokoll XDM mit Publish / Subscribe-Prinzip

Ein Grundpfeiler der kommunikationsorientierten Plattformarchitektur war das neue Kommunikationsprotokoll XDM.
Dieses bot durch das Publish / Subscribe-Prinzip bestmögliche Flexibilität und erforderte ein grundsätzliches Umdenken in der Gestaltung der funktionalen und redundanten Datenflüsse zwischen den DS3-Komponenten (Replikanten, Voter usw.).
Zusätzlich mussten die Sicherheitsmechanismen im XDM-Protokoll so definiert werden, dass auch nicht sichere Kommunikationspartner an der XDM-Kommunikation teilnehmen können.
Das XDM-Protokoll wurde bereits im Forschungsprojekt grob definiert, während des Entwicklungsprojekts im Zuge der Sicherheitsbetrachtungen verfeinert und auch noch während der Entwicklung und Integration durch neue Erkenntnisse verbessert.
XDM bedeutet für die sichere Kommunikation nach DIN EN 50159 einen Paradigmenwechsel, da bisher auf verbindungsorientierte Kommunikationsprotokolle wie z. B. RaSTA gesetzt wurde. Die Sicherungsprinzipien der DIN EN 50159 lassen sich auch auf das Broadcast-Protokoll XDM übertragen.

3.3 Sicherheit und Verfügbarkeit

3.3.1 DS3-Plattform

Für die Sicherheit der DS3-Plattform selbst (Voting, CoarseClock, Protokoll-Gateway) musste ein „Safety Pattern" definiert und realisiert werden.
Zusätzlich braucht es ein komponentenorientiertes Redundanzkonzept, d. h., alle DS3-Komponenten müssen auf beiden COTS-Rechnern redundant vorhanden sein und ihre Funktionalität für beide Rechner zur Verfügung stellen.
Jeder Ausfall einer DS3-Komponente muss erkannt werden und zur „Reparatur" (= Neustart) der Komponente führen. Während des Komponentenausfalls muss die redundante Komponente auf dem anderen Rechner die gesamte Funktionalität übernehmen.
Beispiel:
Bei Ausfall der CoarseClock auf Rechner 1 wird durch die CoarseClock des Rechners 2 die volle CoarseClock-Funktionalität für beide Rechner zur Verfügung gestellt.

2.3 Preliminary hazard analysis

Architectural refinements to the technical concept were made in parallel with the prototypical developments and safety investigations were prepared and assessed using a preliminary hazard analysis with the result that "SIL 4 applications can be operated on COTS hardware with DS3".
This set the course for the start of the development project for the first release of the DS3 platform.

3 The development project (2017 to 2020)

The development project started with the task of developing something completely new from scratch with the following challenges.

3.1 "Mixed SIL" within the DS3 platform

The component-oriented DS3 architecture defined both safety-relevant parts (the runtime environment for the replicants, voting, the CoarseClock and the protocol gateway) and non-safety-relevant parts (the message broker, diagnostics and start-up) which are either executable together or on a non-safety-related operating system (Windows, Linux).
This aspect of the different SIL levels within DS3 had to be considered both in the definition of the platform-internal XDM communication protocol and in the functional architecture of the DS3 software components.

3.2 A safe XDM communication protocol with the publish / subscribe principle

The new XDM communication protocol was the cornerstone of the communication-oriented platform architecture.
This offered the best possible flexibility through the publish/subscribe principle and required fundamental rethinking in the design of the functional and redundant data flows between the DS3 components (replicants, voters, etc.).
In addition, the safety mechanisms in the XDM protocol had to be defined in such a way that any non-safety-related communication partners could also participate in XDM communication.
The XDM protocol had already been roughly defined in the research project, refined during the development project as part of the safety investigations and further improved during development and integration as a result of the new findings.

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

3.3.2 Applikation

Für die Sicherheit und Verfügbarkeit der Anwendungsapplikation musste ein Pattern für die parallele und sichere Ausführung der Replikanten mit einem sicheren Voting definiert und realisiert werden. Erkannte Fehler in Replikanten mussten identifiziert, der als fehlerhaft identifizierte Replikant gestoppt, neu gestartet und synchronisiert werden.
Hierzu war ein intelligentes Mehrheits-Voting notwendig, das sich an die Menge der aktiv laufenden, gestoppten und neu gestarteten Replikanten der beiden beteiligten Rechner anpasst.

3.4 Automatisiertes kommunikationsorientiertes Testsystem

Für die Komponenten- und Integrationstests der DS3-Plattform war ein neues Testsystem erforderlich, welches das Ansprechen und Auswerten der neu definierten XDM-Schnittstellen der Testobjekte unterstützt, sowohl für den Test einzelner DS3-Komponenten als auch für die Integration mehrerer DS3-Komponenten. Dies sollte mit höchstmöglicher Automatisierung der Testläufe in unterschiedlichsten Testkonfigurationen erfolgen.

4 Integration im Produkt Simis AT

Durch die Portierung des ECC-Betriebssystems auf die DS3-Plattform konnte die STWR-Applikation ohne jegliche Anpassung auf die DS3-Plattform migrieren, hierbei vollkommen rückwirkungsfrei auf die angeschlossenen Systeme wie EAR, OCS und NSTW.
Die Anforderung, die STWR-Applikation nicht anzufassen, war ein sehr wichtiger und hilfreicher Faktor bei jeglicher Integrationstätigkeit.
Die Integration der DS3-Plattform im Produkt Simis AT wurde seit der Machbarkeitsuntersuchung begleitend durchgeführt, und bei Problemen an der Simis-AT-Testanlage war immer klar: Die Ursache des Problems liegt in der neuen DS3-Plattform. Es gab keine Irritationen zwischen STWR-Applikation und DS3-Plattform hinsichtlich „Wer hat was warum geändert und weshalb funktioniert jetzt nichts mehr".

4.1 DS3-Konfiguration für den STWR

Für den Anwendungsfall der DS3-Plattform im Produkt Simis AT wurde das System wie folgt konfiguriert:

- Die STWR-Applikation läuft auf zwei COTS-Multicore-Rechnern mit jeweils vier, d. h. insgesamt acht, Replikanten.
- Der Bearbeitungszyklus der STWR-Applikation ist 200 ms.
- Die Kommunikationsprotokolle zu angeschlossenen Rechnern sind Sahara und X25.
- Als COTS-Plattform (CPU und Betriebssystem) wird auf bewährte industrielle Multicore-Rechner mit gehärtetem Windows-Betriebssystem zurückgegriffen, die schon bei SIL-2-Leittechnikanwendungen Verwendung finden.

4.2 Begutachtung und Zulassung

Begleitend zur DS3-Integration wurden auch Begutachtung und Zulassung des Produkts Trackguard Simis AT sehr frühzeitig gestartet.
Die Grundbausteine der Sicherheitsarchitektur von DS3 einschließlich der Portierung des ECC-Betriebssystems wurden entwicklungsbegleitend mit Gutachtern und Zulassern durchgesprochen und erläutert.
Auch hier war die Anforderung, die STWR-Applikation nicht anzufassen, von großem Vorteil, denn man konnte sich auf die Sicherheitsarchitektur der DS3-Plattform fokussieren und des Weiteren bei Regressionstests existierender Testfälle das identische Verhalten derselben STWR-Applikation auf ECC (bisher) und DS3 (neu) zeigen.

XDM represents a paradigm shift for safety-related communication in accordance with DIN EN 50159, since connection-oriented communication protocols such as RaSTA were used previously. The safety principles of DIN EN 50159 can also be transferred to the XDM broadcast protocol.

3.3 Safety and availability

3.3.1 The DS3 platform

A safety pattern had to be defined and implemented for the safety of the DS3 platform itself (voting, the CoarseClock, the protocol gateway).
In addition, a component-oriented redundancy concept is also required, i.e. all DS3 components must be redundantly present on both COTS computers and provide their functionality for both computers.
Any failure of a DS3 component must be detected and lead to the "repair" (= restart) of the component. During a component failure, the redundant component on the other computer must take over all functionality.
Example:
If the CoarseClock on computer 1 fails, the CoarseClock on computer 2 will provide the full CoarseClock functionality for both computers.

3.3.2 The application

A pattern for the parallel and safe execution of the replicants with safe voting had to be defined and implemented for the safety and availability of the application.
Any errors detected in the replicants had to be identified and the replicant identified as being faulty had to be stopped, restarted and synchronised.
This required intelligent majority voting that adjusts to the number of actively running, stopped and restarted replicants on the two computers involved.

3.4 The automated communication-oriented test system

A new test system was required for the component and integration tests on the DS3 platform that supports addressing and evaluating the newly defined XDM interfaces of the test objects, both for testing individual DS3 components and for integrating multiple DS3 components.
This was meant to be done with the highest test run automation possible in a wide variety of test configurations.

4 Integration into the Simis AT product

Porting the ECC operating system to the DS3 platform meant the interlocking computer application could be migrated to the DS3 platform without any customisation and without any retroactive effects on the connected systems such as the input / output computers, the operations control system and the adjacent interlocking.
The requirement not to touch the interlocking computer application was a very important and helpful factor in all the integration activities.
The integration of the DS3 platform into the Simis AT product had been carried out in parallel since the time of the feasibility study and, if any problems occurred at the Simis AT test facility, it was always clear that the cause of the problem lay in the new DS3 platform. There were no irritations between the interlocking computer application and the DS3 platform regarding "who changed what why and why is nothing working now".

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

5 Pilotprojekt „Simis AT@DS3 Stellwerk Achau bei den ÖBB“

Aus Sicht des Siemens-Mobility-Portfolios war Trackguard Simis AT das ausgewählte DS3-Pilotprodukt mit einer Stellwerksanwendung für österreichische Bahnen, und demzufolge war es naheliegend, zur Erprobung und Einführung der neuen DS3-Plattform ein Pilotprojekt im Heimatmarkt Österreich bei den Österreichischen Bundesbahnen (ÖBB) zu finden.
Für die Pilotierung dieses innovativen Themas konnte Siemens Mobility die ÖBB Infrastruktur AG mit dem Projekt „Stellwerk Achau“ gewinnen und hatte hierfür den optimalen Partner.
Bei der Auswahl der Pilotanlage Achau wurde bereits in der Planung berücksichtigt, dass weder bei der Errichtung, Inbetriebnahme noch im Betrieb Einschränkungen zu erwarten sind und sich die Anlage für Bediener und Instandhaltung voll entsprechend den geltenden Lastenheften verhält.
Die Zusammenarbeit mit der ÖBB Infrastruktur AG und deren weisungsunabhängigem Gutachter (freigebende Person nach § 40 EisbG) ging Hand in Hand, sowohl hinsichtlich der theoretischen Betrachtungen für die Produktzulassung Trackguard Simis AT als auch der praktischen Testaktivitäten wie z. B. eine Testfahrt und Kundentests vor Ort an der Realanlage mit den entsprechenden betrieblichen Maßnahmen sowie an der Testanlage bei Siemens Mobility in Wien.
Bei der InnoTrans 2018 wurde das Pilotprojekt „Stellwerk Achau“ mit prototypischer DS3-Software und Originalkonfiguration Stellwerk Achau ausgestellt und hat damit – im Gegensatz zu 2014 – bei den Messebesuchern auch sehr großes Interesse geweckt.
Während der DS3-Entwicklung wurden sämtliche Simis-AT-seitigen Tests sowohl mit der Konfiguration des Simis-AT-Testbahnhofs als auch mit der Konfiguration der Kundenanlage Achau durchgeführt.
Für Vor-Ort-Tests in Achau wurden die COTS-Rechner des STWR direkt neben dem in Betrieb befindlichen ECC-Rechner aufgestellt. Damit waren Vor-Ort-Tests (z. B. in Betriebspausen) relativ einfach möglich; es wurden für die Umschaltung lediglich die LAN-Kabel umgesteckt. Bei diesen Tests wurden unter anderem auch realistische betriebliche Stresstests mit der realen Außenanlage durch ÖBB-Experten durchgeführt, welche auch zusätzliche Erfahrungen und Vertrauen in die neue Plattform lieferten.

6 Inbetriebnahme des Pilotprojekts Achau bei den ÖBB

Am 14. November 2020 war es endlich soweit – nach insgesamt fast sieben Jahren Forschung / Machbarkeit / Entwicklung von DS3 wurden in Achau die LAN-Kabel vom ECC-Rechner auf die DS3-COTS-Rechner umgesteckt und der STWR mit DS3 in Betrieb genommen – zunächst für eine viertägige Test- und Prüfungsphase mit eingeschränkter Sicherheitsverantwortung (Zugverkehr mit aufgehobener Signalabhängigkeit und den entsprechenden betrieblichen Maßnahmen) und ab dem 18. November 2020 dann mit uneingeschränkter Sicherheitsverantwortung der Anlage im regulären Bahnbetrieb.
Seitdem steht das Pilotprojekt Achau unter täglicher Beobachtung durch Fernzugriff auf den Service-Rechner und durch das ÖBB-Instandhaltungspersonal. Die tägliche Datenauswertung zeigte bis zum Redaktionsschluss keine Unregelmäßigkeiten – der STWR@DS3 läuft ohne jegliche Auffälligkeiten.
Für die ÖBB ist DS3 ein wichtiger Schritt in Richtung Digitalisierung und ein maßgeblicher Grundstein für die Stellwerksarchitektur von morgen.

4.1 The DS3 configuration for the interlocking computer

The system was configured as follows for the use case of the DS3 platform in the Simis AT product:

- the interlocking computer application runs on two COTS multicore computers with four replicants each, i.e. a total of eight replicants.
- the processing cycle of the interlocking computer application is 200 ms.
- the communication protocols for the connected computers are Sahara and X25.
- the COTS platform (the CPU and the operating system) is based on proven industry-standard multicore computers with a hardened Windows operating system, both of which are already being used in SIL 2 control system applications.

4.2 Assessment and approval

The assessment and approval of the Trackguard Simis AT product also started very early in parallel to the DS3 integration.
The basic modules of the DS3 safety architecture, including porting the ECC operating system, were discussed with and explained to the assessors and approvers during development.
Here, too, the requirement not to touch the interlocking computer application was a great advantage, because it was possible to focus on the DS3 platform's safety architecture and, in addition, to show the identical behaviour of the same interlocking computer application on ECC (previously) and DS3 (new) during regression tests of the existing test cases.

5 The “Achau Simis AT@DS3 interlocking at ÖBB” pilot project

From the perspective of the Siemens Mobility portfolio, Trackguard Simis AT was the selected DS3 pilot product with an interlocking application for railway lines in Austria. Consequently, it was an obvious step to move to find a pilot project in the Austrian home market at Österreichische Bundesbahnen (ÖBB) to test and introduce the new DS3 platform.
Siemens Mobility was able to win over ÖBB Infrastruktur AG with the Achau interlocking project for piloting this innovative topic and had the ideal partner for this.
When selecting the Achau pilot interlocking, it was already considered during the planning stage that no restrictions were to be expected in construction, commissioning and operations and that the interlocking would behave fully in accordance with the applicable specifications for operating and maintenance staff.
The cooperation with ÖBB Infrastruktur AG and the independent assessor (releasing § 40 EisbG person[AL1]) went hand in hand, both with regard to the theoretical considerations for the Trackguard Simis AT product approval and the practical test activities, such as a test run and on-site customer tests on a real-life system with the appropriate operational measures and at the test facility at Siemens Mobility in Vienna.
The Achau interlocking pilot project with the prototypical DS3 software and original Achau interlocking configuration was exhibited at InnoTrans 2018 and – in contrast to 2014 – aroused a great deal of interest among trade fair visitors.
During the DS3 development, all the Simis AT tests were performed with both the Simis AT test station configuration and the Achau customer system configuration.
The interlocking computer's COTS computers were set up right next to the operational ECC computer for on-site testing in Achau. This made on-site tests (e.g. during out-of-service periods) relatively easy; only the LAN cables had to be reconnected for

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH

7 Ausblick

Die DS3-Pilotierung mit Trackguard Simis AT war für sicherungstechnische Bahnanwendungen der erste und wichtigste Schritt auf dem Weg zu COTS-basierten Rechenzentren: die Definition, Umsetzung und Begutachtung der neuen DS3-Sicherheitsplattform für den Betrieb von SIL-4-Anwendungen auf nicht sicherer COTS-Multicore-Technologie.
Nun folgen schrittweise funktionale Weiterentwicklungen der DS3-Plattform wie z. B.

- IT-Security
- Betrieb in Virtualisierung
- Intelligente Außenanlagenelemente
- Mehr-Server-Betrieb mit verteilten Rechnern für geographische Redundanz.

Außerdem werden nächste Anwendungen (z. B. Radio Block Center / RBC) auf die DS3-Plattform portiert.
Der allererste Schritt auf einem langen Weg ist vollbracht – und nun geht es weiter. ■

the switchover. Among other things, these tests also included realistic operational stress tests with real-life outdoor equipment conducted by ÖBB experts, which also provided additional experience and confidence in the new platform.

6 Commissioning the Achau pilot interlocking at ÖBB

On November 14, 2020, the time had finally come – after a total of almost seven years of the research/ feasibility study/ development of DS3, the LAN cables were reconnected from the ECC computer to the DS3 COTS computers in Achau and the interlocking computer was started up with DS3; initially, for a four-day testing and trial phase with limited safety responsibility (non-signal-interlocked train operations with the appropriate operational measures) and then with unrestricted safety responsibility in regular rail operations from November 18, 2020.
Since then, the Achau pilot project has been under daily observation through remote access to the service computer and by the ÖBB maintenance staff. As of the editorial deadline, the daily data evaluation had been without any findings – STWR@DS3 is running without any irregularities.
DS3 is an important step towards digitalisation for ÖBB and a key cornerstone of the interlocking architecture of tomorrow.

7 Outlook

DS3 piloting with Trackguard Simis AT was the first and most important step towards COTS-based data centres for safety-related railway applications: the definition, implementation and assessment of the new DS3 safety platform for the operation of SIL 4 applications on non-safety-related COTS multicore technology.
Step-by-step functional enhancements of the DS3 platform will now follow, such as:

- IT security
- virtualisation operations
- intelligent outdoor elements
- multiple-server operation with distributed computers for geographical redundancy.

Moreover, further applications (e.g. Radio Block Center / RBC) will also be ported to the DS3 platform.
The very first step on a long road has been taken – and now the journey continues. ■

AUTOREN | AUTHORS

Sonja Steffens
Produktmanagerin DS3-Plattform / *Product Manager DS3-platform*
Siemens Mobility GmbH
Anschrift / *Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: sonja.steffens@siemens.com

Walter Valvoda
Produktmanager Simis AT / *Product Manager Simis AT*
Siemens Mobility Austria GmbH
Anschrift / *Address*: Siemensstraße 90, A-1210 Wien
E-Mail: walter.valvoda@siemens.com

Homepageveröffentlichung unbefristet genehmigt für Siemens Mobility GmbH / Rechte für einzelne Downloads und Ausdrucke für Besucher der Seiten genehmigt / © DVV Media Group GmbH