Integrierte Safety und Security durch softwarebasierte Segregation im EULYNX Object Controller

Integrated safety and security through software-based segregation in the EULYNX Object Controller

Stefanos Moumouris | Martin Zehnder

In einem Cross-Industry-Ansatz mit der Luftfahrt hat die Schweizerische Bundesbahnen AG (SBB AG) eine Plattform beschafft und integrieren lassen, mit welcher sie Proofs of Concept (PoC) für EULYNX Object Controller (OC) durchführen kann. Einer dieser PoC beweist, dass es mit heute verfügbaren Betriebssystemen möglich ist, Safety-relevante und nicht Safety-relevante Software gleichzeitig und unabhängig voneinander auf einem gemeinsamen Prozessorsystem auszuführen. Das EULYNX-OC-Verhalten wird anhand eines simulierten EULYNX-Stellwerks, eines realen Hauptsignals und weiterer, simulierter Außenanlagen demonstriert.

1 Einführung

Zur Umsetzung der ERMTS-Strategie des Bundesamts für Verkehr führt die SBB AG aktuell eine Ausschreibung für Bahnsicherungsanlagen durch. Ziel ist eine Beschaffung mittels langfristiger Rahmenverträge. Die Ausschreibung umfasst hauptsächlich Sicherungsanlagen mit Außensignalisierung, Führerstandssignalisierung sowie OC auf Basis von EULYNX / EU-Rail System Pillar Standard Baseline 4.1 oder höher. Der Begriff OC wird hier synonym zum offiziellen Begriff EULYNX field element Subsystem EfeS verwendet. Um Helvetismen zu vermeiden, hat die SBB in den vergangenen Jahren parallel zur Erstellung der OC-Lastenhefte an der EULYNX Baseline 4 mitgearbeitet. Sowohl Anforderungen im EULYNX-Standard als auch in den darauf basierenden Lastenheften lassen sich durch PoC schärfen und deren Machbarkeit untermauern. Ein neutraler, durch einen Infrastrukturbetreiber durchgeführter PoC kann herstellerunabhängig beweisen, dass eine Anforderung technisch umsetzbar ist. Aus diesem Grund hat die SBB AG in einem Cross-Industry-Ansatz mit der Luftfahrtindustrie COTS (Commercial Off The Shelf)- Hardware und ein käufliches Betriebssystem beschafft. Ein von der Bahnindustrie unabhängiger Embedded-Software-Entwicklungsdienstleister hat einen zulassungsfähigen RaSTA (Rail Safe Transport Application)- Protokollstack entwickelt und zur so entstehenden, SIL4 (Safety Integrity Level 4) fähigen sog. OC PoC Plattform integriert. Mit ihr lassen sich EULYNX-OC-Funktionen realisieren und testen.

Das RaSTA-Protokoll wird in EULYNX als Protokoll für die sichere (safe) Kommunikation verwendet. Mit dem EULYNX Standard

In a cross-industry approach with the aviation industry, Schweizerische Bundesbahnen AG (SBB AG) has procured and integrated a platform that allows SBB to perform proofs of concept (PoC) for the EULYNX Object Controller (OC). One of these PoC has demonstrated that it is possible to run both safety-relevant and non-safety-relevant software simultaneously and independently of each other on a common processor system using currently available operating systems. The EULYNX OC behaviour has been demonstrated using a simulated EULYNX interlocking, a real main signal and other simulated external equipment.

1 Introduction

SBB AG is currently issuing a call for tenders for railway safety systems in order to implement the ERMTS strategy of the Federal Office of Transport. The aim is to procure these systems on the basis of long-term framework agreements. The tender mainly covers safety systems with external signalling, driver's cab signalling and OC based on EULYNX/EU-Rail System Pillar Standard Baseline 4.1 or higher. The term OC is used here synonymously with the official term EULYNX EfeS field element subsystem. In order to avoid Helvetisms, SBB has been collaborating on EULYNX Baseline 4 over the past few years in parallel with the creation of the OC specifications. The requirements in both the EULYNX standard and the specifications based on it can be refined and their feasibility underpinned by means of PoC. A neutral PoC carried out by an infrastructure manager can prove that a requirement is technically feasible independently of the manufacturer. For this reason, SBB AG has procured COTS (Commercial Off The Shelf) hardware and a commercial operating system in a cross-industry approach with the aviation industry. An embedded software development service provider independent of the railway industry has developed a certifiable RaSTA protocol stack and integrated it into the resulting SIL4-capable, so-called OC PoC platform. It can be used to implement and test EULYNX OC functions.

The RaSTA protocol is used in EULYNX as a safe communication protocol. The EULYNX standard Baseline 4.1 has made it possible for several OC to use a common RaSTA connection to

Baseline 4.1 ist es möglich geworden, dass mehrere OC eine gemeinsame RaSTA-Verbindung zum Stellwerk verwenden können. Damit sind Multi-Element-Controller-Plattformen möglich. Die EULYNX Baseline 4.1 führt zudem Security ein und ermöglicht eine segregierte Safety und Security auf Applikationsebene. Als Verschlüsselungsprotokoll wird dabei Transport Layer Security V1.3 (TLS) verwendet.

2 Cross-Industry-Ansatz

In der Luftfahrt ist die Virtualisierung Safety-relevanter Systeme schon seit Jahren zugelassen. Diese wird im ARINC 653-Standard spezifiziert. Dabei laufen die Partitionen räumlich und zeitlich segregiert auf einer Microcontroller-Plattform. Das Betriebssystem weist jeder Partition einen definierten Speicherbereich und eine definierte Laufzeit zu. Damit laufen die Partitionen deterministisch in derselben Reihenfolge, in Echtzeit und immer im selben zyklischen Zeitintervall ab und werden vom Betriebssystem überwacht. Die Kommunikation zwischen den Partitionen und ihrer Umgebung erfolgt über konfigurierte Ports mittels hierfür im ARINC 653 API Standard spezifizierter Funktionen.
Mit dieser softwarebasierten Segregation ist es nun möglich, Partitionen mit unterschiedlichen SIL (SIL0 bis SIL4) auf einer Microcontroller-Plattform zu integrieren.
Dies ermöglicht darüber hinaus eine inkrementelle Zulassung des Systems. Bei Änderung einer Partition bleibt die Zulassung der anderen Partitionen auf dem System erhalten. Die Zulassung eines solchen Gesamtsystems wird dadurch stark vereinfacht. Als Beispiel sei hier das häufige Update der Security Partition genannt. Voraussetzung dafür ist, dass die partitionsübergreifenden Konfigurationsparameter wie z. B. die zugewiesene Rechenzeit und der Speicherplatz sowie die Schnittstellen identisch bleiben. Die noch zu wiederholenden System- und Abnahmetests beschränken sich dank der Segregation auf die geänderte Partition und deren Integration ins Gesamtsystem.
Entdeckt das Betriebssystem in einer Partition einen Fehler (z. B. eine Speicher- oder Laufzeitverletzung), startet es diese neu oder stellt sie ab. Die Fehlerreaktion ist abhängig vom spezifizierten Systemverhalten und kann konfiguriert werden. Dadurch wird eine Fehlerfortpflanzung im System verhindert.
Dieser Ansatz aus der Luftfahrt wurde auf eine Bahnanwendung übertragen. Speziell auf die OC PoC Plattform, einer Implementation des EULYNX Multi Element Controllers.

3 Aufbau der OC PoC Plattform

Die OC PoC Plattform besteht aus zwei Lanes, welche synchronisiert betrieben werden. Eine Lane entspricht einer unabhängigen Microcontroller-Einheit. Beide Microcontroller-Einheiten ergeben dabei ein 2-aus-2-System. Dies ist erforderlich, um die Safety-Anforderungen an ein SIL4-System zu erfüllen. Die beiden Microcontroller tauschen ihre Datenbasis aus und konsolidieren sie gegenseitig. Für eine Zustandsänderung müssen die Berechnungen beider Microcontroller nach jedem Zeitintervall übereinstimmen. Trifft das nicht zu, führt das Betriebssystem die vordefinierte Fehlerreaktion durch. Der eingesetzte Microcontroller ist der MPC5567@128MHz, und es stehen 4 Mbyte SRAM und 8 MByte Flash ROM zur Verfügung.
Das ARINC 653 Betriebssystem ist auf beiden Lanes installiert. Folgende Partitionen sind aktuell konfiguriert:

- 4 Weichen-Partitionen (beide Lanes)
- 8 Lichtsignal -Partitionen (beide Lanes)

an interlocking. This makes multi-element controller platforms possible. EULYNX Baseline 4.1 also introduces security and enables segregated safety and security at the application level. Transport Layer Security V1.3 (TLS) has been used as the encryption protocol.

2 A cross-industry approach

The virtualisation of safety-relevant systems has been certified for years in aviation. This is specified in the ARINC 653 standard. The partitions run on a microcontroller platform in a spatially and temporally segregated manner. The operating system assigns each partition a defined memory area and a defined runtime. Thus, the partitions run deterministically in the same order, in real time and always in the same cyclic time interval and are monitored by the operating system. Communication between the partitions and their environment takes place via configured ports using functions specified for this purpose in the ARINC 653 API standard.
This software-based segregation means that it is now possible to integrate partitions with different SIL (SIL0 to SIL4) onto a microcontroller platform.
This also enables the incremental certification of the system. If one partition is changed, the certification of the other partitions in the system is retained. The certification of this type of complete system is therefore significantly simplified. One example of this involves the frequent updating of the security partition. The prerequisite for this is that the cross-partition configuration parameters such as the allocated computing time and storage space as well as the interfaces remain identical. Thanks to this segregation, the system and acceptance tests that still have to be repeated are limited to the changed partition and its integration into the overall system.
If the operating system detects an error in a partition (e.g. a memory or runtime violation), it restarts it or shuts it down. The error response depends on the specified system behaviour and can be configured. This prevents error propagation in the system.
This aviation approach has been transferred to a railway application, specifically to the OC PoC platform, an implementation of the EULYNX Multi Element Controller.

3 Setting up the OC PoC platform

The OC PoC platform consists of two lanes that are operated synchronously. Each lane corresponds to an independent microcontroller unit. Both microcontroller units result in a two out of two system. This is necessary in order to fulfil the safety requirements of a SIL4 system. The two microcontrollers mutually exchange and consolidate their databases. In the case of a change of state, both microcontrollers' calculations must match after each time interval. If this does not apply, the operating system will perform the predefined error response. The microcontroller in use is the MPC5567@128MHz and there are 4 Mbyte SRAM and 8 MByte flash ROM available.
The ARINC 653 operating system has been installed on both lanes. The following partitions are currently configured:

- 4 point partitions (both lanes)
- 8 light signal partitions (both lanes)
- 1 train detection system partition (both lanes)
- 1 RaSTA Safety and Redundancy Layer partition (both lanes)
- 1 RaSTA Retransmission Layer partition (both lanes)

- 1 Gleisfreimelder-Partition (beide Lanes)
- 1 RaSTA Safety und Redundancy Layer Partition (beide Lanes)
- 1 RaSTA Retransmission Layer Partition (beide Lanes)
- 1 TLS Partition (beide Lanes)
- 1 TCP/IP Partition (beide Lanes)
- 1 OPC UA für SDI Partition (Lane A)
- 1 OPC UA für SMI Partition (Lane B)
- 1 Security Services SSI Partition (Lane A)
- 2 System-Partitionen (beide Lanes)

Alle Partitionen außer TLS und OPC UA werden auf beiden Lanes synchron und immer zum selben Zeitpunkt und in derselben Reihenfolge aufgerufen und müssen ihre Berechnungen innerhalb des vordefinierten Zeitbudgets (Partition Slice) abgeschlossen haben (Deadline Monitoring).

Die TLS und OPC UA Partitionen laufen ohne Deadline Monitoring und können ihre Laufzeit über mehrere Partition Slices verteilen (Continuous Partitioning). So ist es möglich, nicht Safety-relevante Partitionen mit langer Rechenzeit auf einer deterministischen Plattform zu integrieren.

Der RaSTA-Protokollstack ist auf zwei Partitionen aufgeteilt, weil er aus einem Safety-relevanten und einem nicht Safety-relevanten Teil besteht. Diese sind der Safety and Retransmission Layer (SIL4) und der Redundancy Layer (Basic Integrity).

Die Weichen-/Lichtsignal-/Gleisfreimelder-Partitionen bezeichnen wir als OC-Partitionen. Diese verwenden einen gemeinsamen RaSTA-Kanal für die Kommunikation mit dem Stellwerk (EULYNX SCI-Schnittstelle). Durch den Heartbeat des RaSTA-Kanals wird kontinuierlich überprüft, ob die RaSTA-Verbindung zum Stellwerk aktiv ist.

Da einzelne OC-Partitionen den RaSTA-Kanal gemeinsam verwenden, muss sichergestellt werden, dass der OC dem Stellwerk signalisiert, wenn einzelne davon nicht zur Verfügung stehen. In einem Fehlerfall könnte beispielsweise das Betriebssystem eine oder mehrere OC-Partitionen abschalten. Ohne die Signalisierung würde das

- 1 TLS partition (both lanes)
- 1 TCP/IP partition (both lanes)
- 1 OPC UA for SDI partition (lane A)
- 1 OPC UA for SMI partition (lane B)
- 1 Security Services SSI partition (lane A)
- 2 System partitions (both lanes)

All the partitions, except the TLS and OPC UA, are invoked on both lanes synchronously, always at the same time and in the same order, and must have completed their calculations within the predefined time budget (partition slice) (deadline monitoring).

The TLS and OPC UA partitions run without any deadline monitoring and can distribute their runtime over several partition slices (continuous partitioning). This allows the integration of non-safety-relevant partitions with long computing times onto a deterministic platform.

The RaSTA protocol stack has been divided into two partitions, because it consists of a safety-relevant and a non-safety-relevant part. These are the Safety and Retransmission Layer (SIL4) and the Redundancy Layer (Basic Integrity).

The point/light signal/train detection system partitions are called OC partitions. These use a common RaSTA channel to communicate with the interlocking (EULYNX SCI interface). The heartbeat of the RaSTA channel continuously checks whether the RaSTA connection with the interlocking is active.

Since individual OC partitions share the RaSTA channel, it is necessary to ensure that the OC informs the interlocking, if any of them are not available. In the event of an error, for example, the operating system could switch off one or more OC partitions. Without indication, the interlocking would only notice that the faulty OC partitions are no longer available once they were addressed. Therefore, an internal heartbeat between the OC partitions and the SIL4 RaSTA partition has been introduced. The

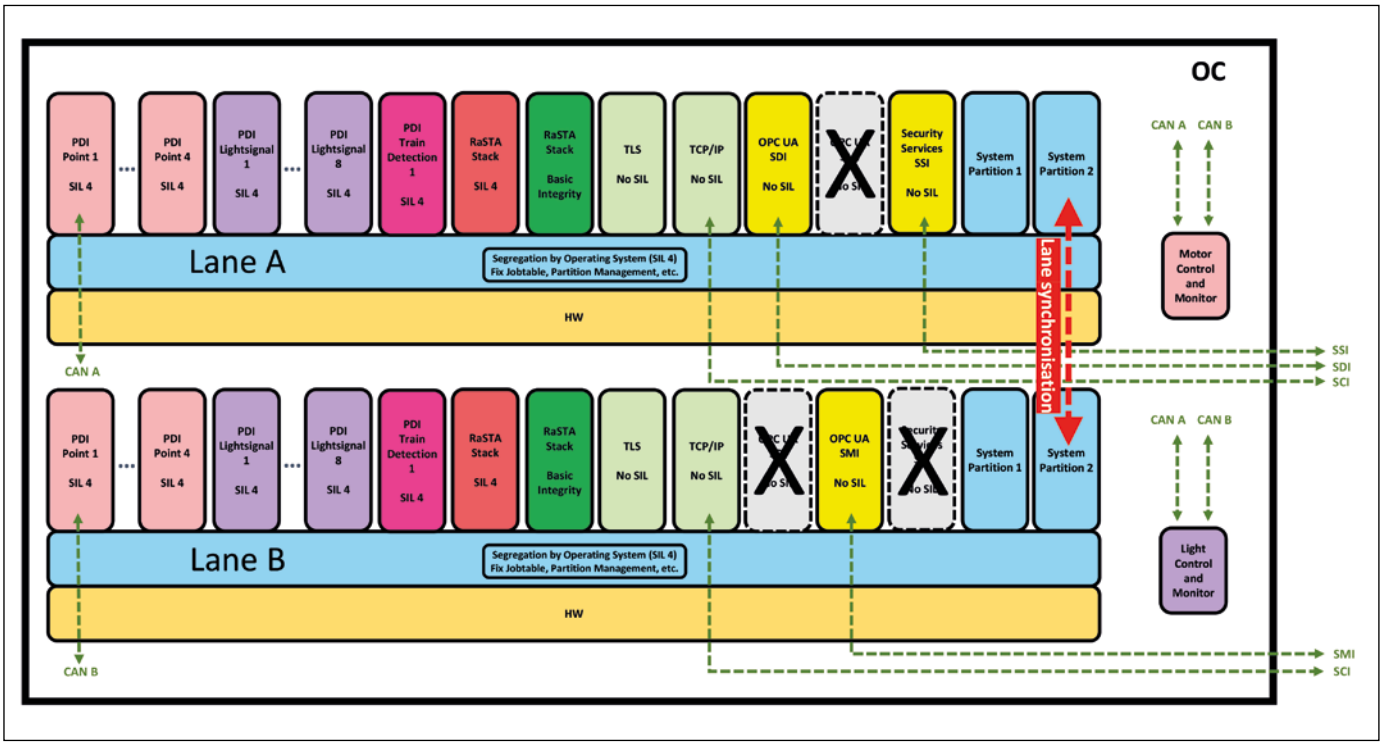


Bild 1: OC PoC Plattform
Fig. 1: OC PoC Platform

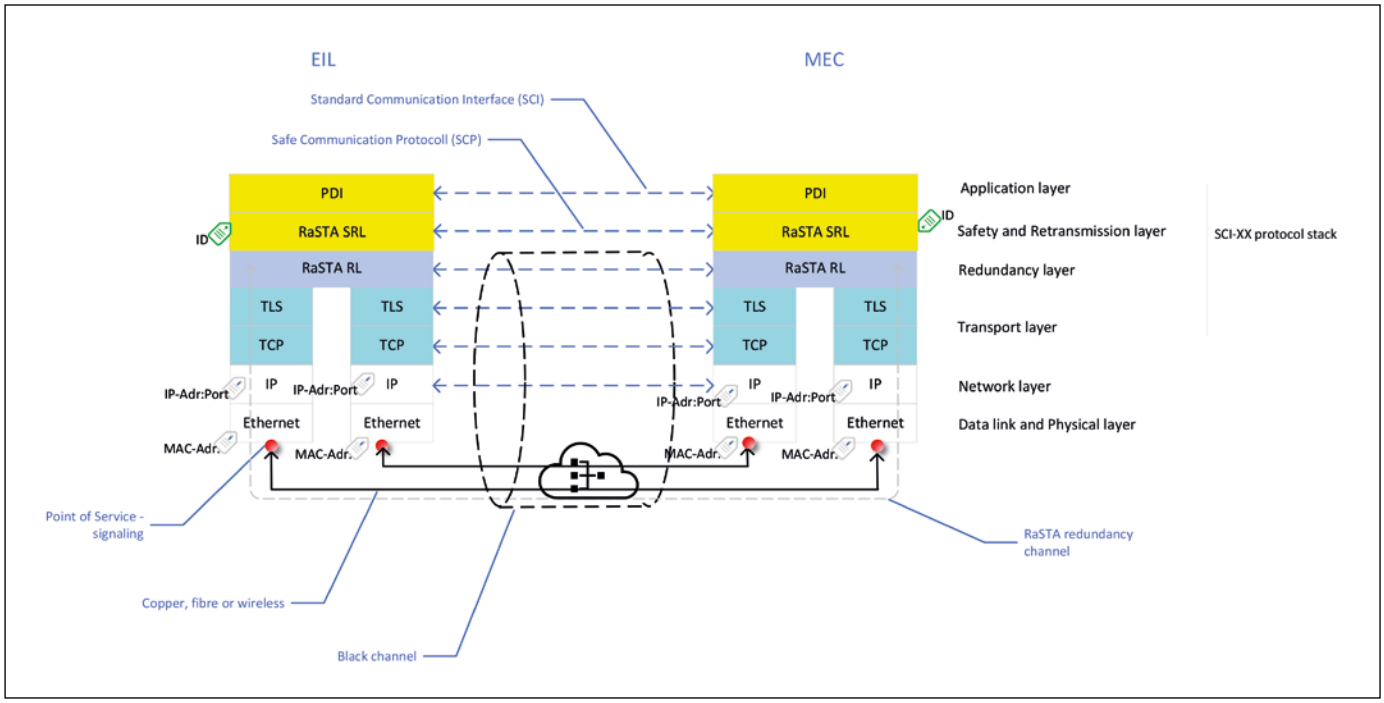


Bild 2: OSI-Kommunikation – EULYNX Eu.Doc.16 Systemarchitektur, Eu.SAS.736
Fig. 2: OSI Communication – EULYNX Eu.Doc.16 System Architecture, Eu.SAS.736

Quelle / *Source*: erweitert durch SBB AG / *enhanced by SBB AG*

Stellwerk erst beim Ansprechen der fehlerhaften OC-Partitionen feststellen, dass diese nicht mehr zur Verfügung stehen. Deswegen wurde ein interner Heartbeat zwischen den OC-Partitionen und der SIL4 RaSTA-Partition eingeführt. Die SIL4 RaSTA-Partition überprüft in jedem Zyklus mittels Heartbeat, ob die angeschlossenen OC-Partitionen aktiv sind. Wenn dies nicht der Fall ist, wird die entsprechende OC-Partition beim Stellwerk abgemeldet.
Jede Lane verfügt über eine Ethernet-Schnittstelle. Die SCI-Schnittstelle zum Stellwerk ist dabei redundant vorhanden (Redundantes SCI auf Lane A und Lane B). Die SDI / SMI / SSI-Schnittstellen sind auf die beiden Lanes aufgeteilt und nicht redundant vorhanden.
Die PDI-Schnittstelle der OC-Partitionen sind nach dem EULYNX Standard Baseline 4.1 implementiert.
Der verwendete Security-Ansatz implementiert die Variante C, welche im EULYNX-Standard im Security Concept, Eu.Doc.15, Baseline 4.1 spezifiziert ist. Die Variante C spezifiziert eine Segregation von Safety und Security auf Anwendungsebene.
Die OC PoC Plattform verfügt pro Lane über eine Echtzeit und online Debugging-Schnittstelle. Diese verwendet jeweils die Ethernet-Schnittstelle der entsprechenden Lane, über die interne Zustände ausgelesen oder Fehler stimuliert werden. Für das Auslesen und Stimulieren der Fehlerzustände wird ein echtzeitfähiger Integrations- und Test-Computer auf Linux-Basis eingesetzt. Dieser kann zusätzlich über eine RS232-Schnittstelle ein Relais-Board ansteuern. Im aktuellen Set-up der OC PoC Plattform können 13 Außenelemente angesteuert werden.
Die Firma Aviotech GmbH hat im Rahmen des PoC folgende Komponenten geliefert:

- Dual Lane Hardware und das ARINC 653 Betriebssystem SCORPOS
- Konfiguration der OC PoC Plattform
- Simulation der Außenelemente
- Entwicklungs-, Integrations- und Testumgebung

Die Firma CSA Engineering AG hat im Rahmen des PoC folgende Komponenten geliefert:

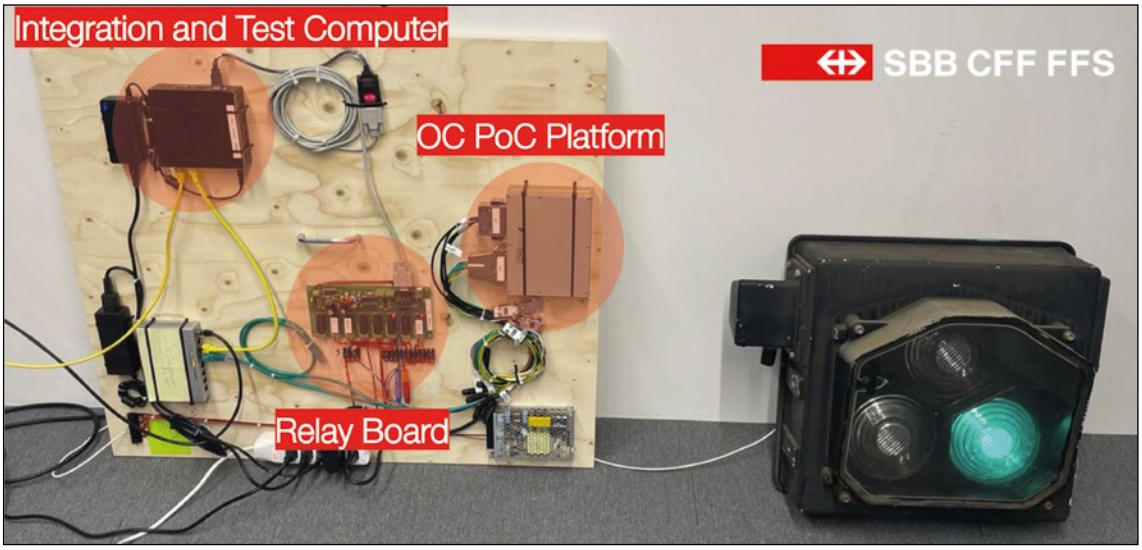
SIL4 RaSTA partition checks that the connected OC partitions are active in every cycle by means of a heartbeat. If this is not the case, the corresponding OC partition is de-registered at the interlocking.
Each lane has an Ethernet interface. The SCI interface to the interlocking is redundant (redundant SCI on lane A and lane B). The SDI / SMI / SSI interfaces have been divided between the two lanes and are not redundant.
The OC partitions' PDI interface has been implemented according to the EULYNX standard Baseline 4.1.
The used security approach implements variant C, which is specified in the EULYNX standard (in Security Concept, Eu.Doc.15, Baseline 4.1). Variant C specifies the segregation of safety and security at the application level.
The OC PoC platform provides a real-time, online debugging interface for each lane. This uses the corresponding lane's Ethernet interface, via which internal states are read out or errors are stimulated. A Linux-based real-time integration and test computer is used for reading out and stimulating the error states. This computer can also control a relay board via an RS232 interface.
13 external elements can be controlled in the current OC PoC platform setup.
Aviotech GmbH has supplied the following components as part of the PoC:

- the Dual Lane hardware and the SCORPOS ARINC 653 operating system.
- the OC PoC platform configuration
- the simulation of external elements
- the development, integration and test environment

CSA Engineering AG has supplied the following components as part of the PoC:

- the implementation of a RaSTA protocol stack according SIL4, which has been assessed by TÜV Nord. This should be made available in the EULYNX framework as an open source reference implementation, including the certification kit.

Bild 3:
Foto PoC Set-up
Fig. 3: Photo PoC Setup



- Implementation eines RaSTA-Protokollstacks nach SIL4, welcher vom TÜV Nord begutachtet wird. Dieser soll im EULYNX-Rahmen als Open-Source-Referenzimplementation inklusive Zertifikationskit zur Verfügung gestellt werden.
- Implementation der OC-Partitionen nach dem EULYNX Standard Baseline 4.1
- Implementation und Integration der Port Kommunikation
- Integration und Adaption der verwendeten TLS, TCP/IP und OPC UA Stacks auf die OC PoC Plattform
- Integration eines physischen Lichtsignals und mehrerer anderer simulierter Außenanlagen
- Gesamtintegration der OC PoC Plattform

Die Firma Systems Lab 21 GmbH hat die EULYNX-Stellwerkssimulation entwickelt und in die PoC-Umgebung integriert.

4 Beschreibung der PoC

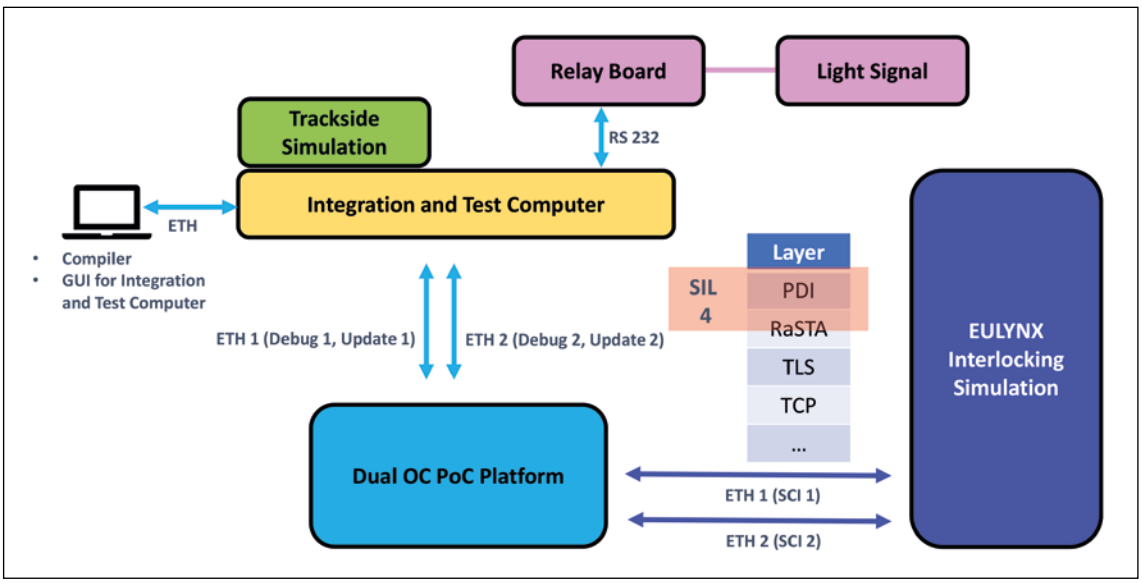
Im ersten Schritt wurde für den PoC eine OC PoC Plattform mit nur einer Lane verwendet (kein 2-aus-2-System). Um die Plattform anzusteuern, wurde ein simuliertes EULYNX-Stellwerk mit einer TLS-verschlüsselten SCI-Schnittstelle verwendet.

- the implementation of the OC partitions according to the EULYNX standard Baseline 4.1
- the implementation and integration of the port communication
- the integration and adaptation of the used TLS, TCP/IP and OPC UA stacks to the OC PoC platform
- the integration of a physical light signal and several other simulated external systems
- the overall integration of the OC PoC platform
- Systems Lab 21 GmbH has developed the EULYNX interlocking simulation and integrated it into the PoC environment.

4 A description of the PoC

Initially, an OC PoC platform with only one lane was used (no two out of two system). A simulated EULYNX interlocking with a TLS encrypted SCI interface was used in order to control the platform. The platform was successfully integrated and tested using the debugging interface and the integration and test computer. A real light signal was controlled (but not monitored) using a relay board. The other external elements used were simulated by the integration and test computer.

Bild 4: PoC set-up
Fig. 4: PoC setup



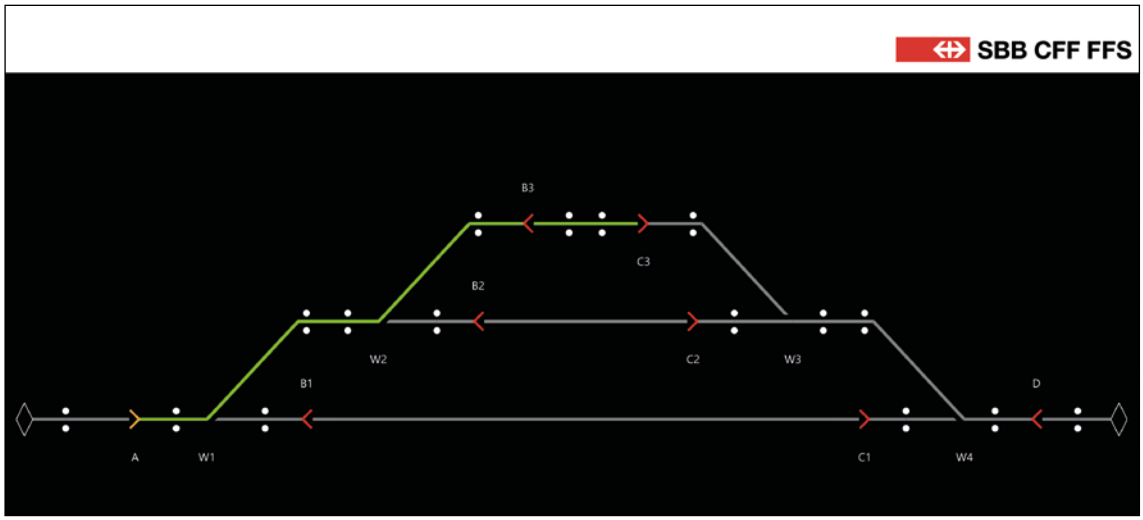


Bild 5: EULYNX-Stellwerkssimulation
Fig. 5: EULYNX interlocking simulation

Über die Debugging-Schnittstelle und mit dem Integrations- und Test-Computer wurde die Plattform erfolgreich integriert und getestet. Ein reales Lichtsignal wurde mittels Relais-Board angesteuert (aber nicht überwacht). Die anderen verwendeten Außenelemente wurden vom Integrations- und Test-Computer simuliert.
Der erste PoC sah zwei Szenarien vor. In beiden Szenarien wurden mittels der Stellwerkssimulation Fahrstraßen gestellt. Im ersten Szenario wurde ein Fehler in der Lichtsignal Partition stimuliert. Als Fehlerreaktion wurde nachgewiesen, dass das Betriebssystem die entsprechende Lichtsignal-Partition abgeschaltet hatte und das Lichtsignal auf rot (Fail Safe) gestellt wurde. Die RaSTA-Verbindung zum simulierten EULYNX-Stellwerk blieb bestehen, und die anderen simulierten Außenelemente konnten vom Stellwerk weiterhin angesteuert werden. Lediglich das fehlerhafte Lichtsignal war nicht mehr verfügbar. Im zweiten Szenario wurde ein Fehler in der RaSTA-Partition stimuliert. Als Fehlerreaktion wurde nachgewiesen, dass die RaSTA-Verbindung beendet wird und alle Außenelemente den Fail-Safe-Zustand einnehmen, sofern sie über einen solchen verfügen. Das simulierte Stellwerk konnte in diesem Szenario keine Außenelemente mehr ansteuern.
Mit diesem PoC konnten die Segregation von Partitionen, die Verhinderung der Fehlerfortpflanzung im System und die segregierte Safety und Security auf Anwendungsebene nachgewiesen werden. Die Kommunikation zum Stellwerk ist dabei mit TLS verschlüsselt. Dies wurde alles auf einem Microcontroller.System mit softwarebasierter Segregation umgesetzt. Die Zulassbarkeit einer solchen Multi-Element-Controller-Plattform wurde ebenfalls nachgewiesen. Diese ist inkrementell möglich. Die Performance der Plattform reicht aus, um aktuell eine Zykluszeit von 100 ms zu realisieren. Eine aktive Kühlung der Plattform ist dabei nicht notwendig.

5 Zulassung

In der Luftfahrt wird Software nach dem DO178C-Standard entwickelt. In der Bahnindustrie ist das die EN 50128. Beide Standards sind sich im Grundsatz ähnlich, da sie auf denselben Prinzipien der Functional Safety aufbauen. Das ARINC 653 Betriebssystem ist in der Luftfahrt seit 2007 zugelassen und wird erfolgreich und zuverlässig eingesetzt. Eine Zulassung in der Bahnindustrie ist mit den entsprechenden Nachweisen möglich. Ziel des PoC war es, eine mögliche Zulassung aufzuzeigen, die Zulassung aber nicht umzusetzen.

The first PoC included two scenarios. Routes were set in both scenarios using the interlocking simulation. In the first scenario, a fault was stimulated in the light signal partition. The error response was proven when the operating system switched off the corresponding light signal partition and set the light signal to red (the failsafe). The RaSTA connection to the simulated EULYNX interlocking was preserved and the other simulated external elements were still able to be controlled by the interlocking. Only the faulty light signal was no longer available. In the second scenario, a fault was stimulated in the RaSTA partition. The error response was demonstrated when the RaSTA connection was terminated and all the external elements assumed their failsafe state, where available. The simulated interlocking could no longer control any of the outdoor elements in this scenario.
The segregation of the partitions, the prevention of error propagation in the system and the segregated safety and security at the application level were able to be demonstrated by means of this PoC. The communication with the interlocking is encrypted with TLS. This was all implemented on a microcontroller system with software-based segregation. The certifiability of such a multi-element controller platform has also been proven. This is possible incrementally. The performance of the platform is currently sufficient to realise a cycle time of 100 ms. No active cooling of the platform is necessary.

5 Certification

In aviation, software is developed according to the DO178C standard. In the railway industry, the standard is EN 50128. Both standards are similar in essence, as they are based on the same principles of functional safety. The ARINC 653 operating system was certified in aviation in 2007 and has been used successfully and reliably since then. Certification in the railway industry is possible with the appropriate evidence. The aim of the PoC was to demonstrate the possibility of certification, but not to implement it.

6 Outlook

The PoC was carried out on a single lane OC PoC platform in 2022.The plan is to use a dual lane OC PoC platform (two out of two system) with redundant SCI interfaces in 2023. This was implemented in Q1 2023 and is operational. The simulated EULYNX interlocking now controls the Dual OC PoC platform via

6 Ausblick

Der PoC wurde 2022 auf einer Single Lane OC PoC Plattform durchgeführt. Für das Jahr 2023 ist geplant, eine Dual Lane OC PoC Plattform (2-aus 2-System) mit redundanten SCI-Schnittstellen zu verwenden. Diese wurde im Q1 2023 umgesetzt und ist betriebsbereit. Das simulierte EULYNX-Stellwerk steuert nun über zwei redundante SCI-Verbindungen die Dual OC PoC Plattform an. Weiterhin sind für 2023 folgende Punkte geplant:

- Optimierung der Laufzeit des Systems. Damit sollen Zykluszeiten unter 100 ms erreicht werden.
- Implementierung der SMI / SSI-Schnittstellen
- Ansteuerung und Überwachung realer Außenelemente wie Weichen und Lichtsignale über zwei CAN-Schnittstellen von Lane A und Lane B. ■

two redundant SCI connections. Furthermore, the following items have also been planned for 2023:

- optimisation of the system runtime. The aim is to achieve cycle times of less than 100 ms
- the implementation of the SMI / SSI interfaces
- the control and monitoring of real external elements such as points and light signals via two CAN channels from Lane A and Lane B. ■

LITERATUR | LITERATURE

[1] ARINC 653: https://de.wikipedia.org/wiki/ARINC_653
[2] SCORPOS Plattform: https://www.aviotech.de/scorpos-arinc653-betriebssystem.html
[3] EULYNX Standard, Baseline 4.1

AUTOREN | AUTHORS

Dipl. El.-Ing. (FH) Stefanos Moumouris
Systemingenieur Object Controller / Teilprojektleiter OC PoC Plattform / *System Engineer Object Controller / Sub-Project Manager OC PoC Plattform*
E-Mail: stefanos.moumouris@sbb.ch

Dipl. El.-Ing (ETH, EMBA) Martin Zehnder
Projektleiter Object Controller / *Project Manager Object Controller*
E-Mail: martin.zehnder@sbb.ch

Beide Autoren / *both authors*:
SBB AG
Anschrift / *Address*: Trüsselstraße 2, CH-3000 Bern 65