Safe4RAIL

SAFE architecture for Robust distributed Application Integration in roLling stock

Project reference: **730830**
Project website: **www.safe4rail.eu**
Start date: **1st October, 2016**
End date: **31st September, 2018**
Duration: **24 months**
Project cost: **€ 6,681,211.25**
Project funding: **€ 6,681,211.25**
Programme type: **Horizon 2020**
Programme acronym: **H2020-S2RJU-OC-2016-01-2**
Complementary project: **CONNECTA (Ref: 730539)**

This project has received funding from the Shift2Rail Joint Undertaking under grant agreement No. 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Germany, Czech Republic, Italy, France. The content of this document reflects only the author's view - the Joint Undertaking is not responsible for any use that may be made of the information it contains.

Mission:

Safe4RAIL (Safe architecture for Robust distributed Application Integration in roLling stock) targets to provide the baseline for a fundamentally simplified embedded computing and networked Train Control Monitoring System (TCMS) platform for modular integration and certification for distributed hard real-time controls, safety signals and functions up to the highest Safety Integrity Level (SIL).

Safe4RAIL will reinforce European competitiveness by offering fundamentally simplified electronic and train control and monitoring architectures required for the optimization of railway systems. The outcomes refer to the reduction of the number of on-board computing devices, improved reliability, shortening the integration and (re)commissioning times and thus life-cycle cost reduction, as well as the ability to implement the SIL4 functions in TCMS.

Concept:

The project Safe4RAIL aims to create safety concepts for mixed-critical Ethernet-based networking as well as a mixed-criticality application framework, including the brake-by-wire concept. The project will provide recommendations for standardization and certification of next generation TCMS embedded platform.

Objectives:

In order to define the networking and application framework safety concepts, Safe4RAIL starts from cross-industry best practices, models of computation and embedded platform (computing, networking and software) technologies. These inputs lead to the development of proof-of-concepts that demonstrate the core components of the technology and ensures sustainable design of integrated modular architectures and next generation TCMS. The technology is demonstrated in the context of electronic train brake control based on a novel fully electronic architectural concept based on drive-by-wire technology. As a whole Safe4RAIL targets the following objectives:

Objective 1: Configurable Mixed Criticality Networking "Drive-By-Data" Concept

- Analyse viability of existing standards from other transport sectors (SAE AS6802, IEEE Time-Sensitive Networking) and Avionics (ARINC 664) in a railway context
- Hosts all system function traffic with different timing and safety requirements, support the partitioning of network bandwidth for time-critical & safety-critical functions (up to SIL4)
- Design the concept and methodology for the railway network and the embedded platform integration

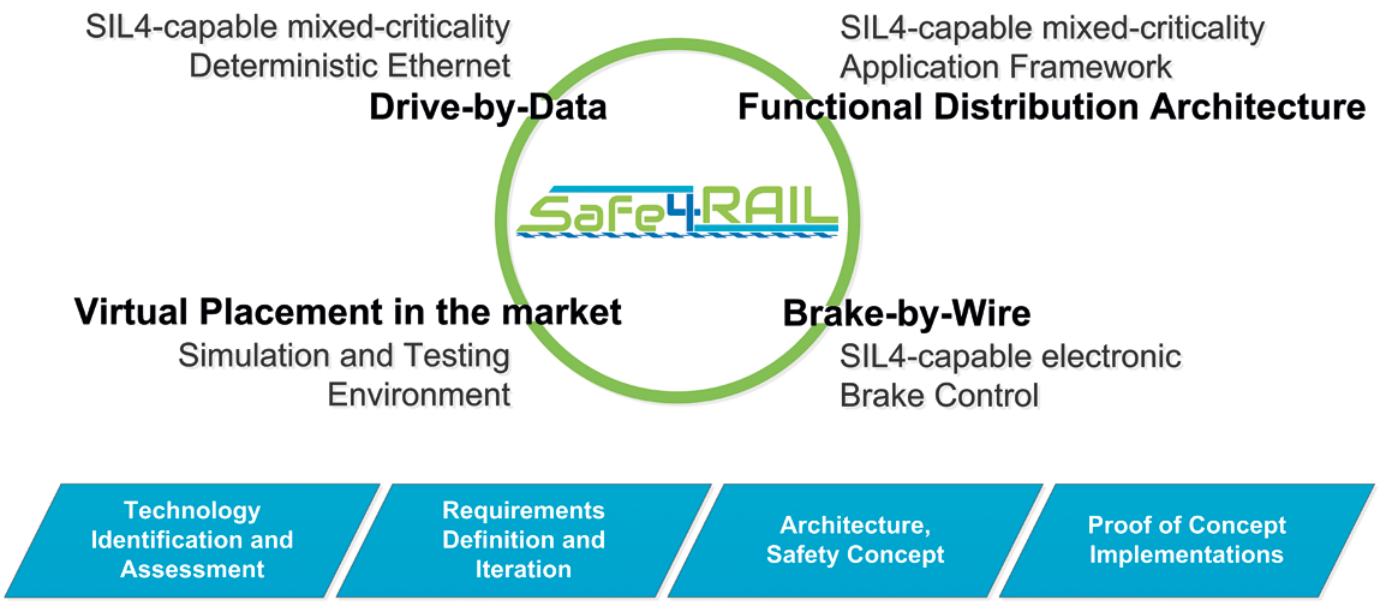
Objective 2: Mixed Criticality Application Framework Concept

- Provide solutions to fulfil functional safety-critical and non-critical requirements and non-functional requirements (including security)
- Analyse viability of existing embedded platform from transportation sectors such as automotive (AUTOSAR/MICROSAR) and avionics (ARINC 653) in TCMS context, together with TRDP application profiles
- Design the concept and methodology for the railway network and the embedded platform integration and provide proof-of-concept implementations

Objective 3: Simulation and Testing Environment for distributed embedded railway systems

- Develop a network-centric system-level simulation providing a timing-accurate simulation of heterogeneous in-train communication networks
- Support Software In the Loop and Hardware In the Loop testing, while supporting the secure coupling of simulators and physical systems at different sites connected via internal Local Area Networks or the Internet (co-simulation with remote subsystems)
- Develop simulations of the wireless interfaces to ground systems

Safe4RAIL technical approach



Objective 4: Architecture and Safety Concept for Brake-by-Wire (SIL4) utilizing the Networking- and Application Framework Concepts

- Move train brake controls from pneumatic or mixed pneumatic electronic architectures to a fully electronic one (brake-by-wire)
- Define safety communication requirements for brake-by-wire
- Develop hardware/software safety-architecture, redundancy in critical sensors and signals , technical concepts and implement proof of concept
- Define verification and validation process, concept of test activities, and assessment criteria to be taken as future reference point

Objective 5: Modular Certification capability enabled by the distributed embedded railway platform and systems

- Ease partition-level development, migration, certification and re-certification
- Provide evidences for interference-freeness provided by the safe " functional distribution" architecture
- Assessment of modular certification strategy by certification experts

Objective 6: Contribution to safety- and technology standards for future European uptake

- Identify open technologies and capabilities required, identify gaps or issues
- Provide recommendations for embedded platform and networking capabilities or requirements which are not included in existing technology and safety standards (e.g. IEC 61375, EN 5012x and EN 50657)

Project Phases:

Phase 1 – State of the Art

The Safe4RAIL project starts with an exploratory inventory of technology and solutions from the aerospace, automotive and railway domains with regards to system-level, embedded platform with networking, computing, functional distribution, safety and security analyses.

Phase 2 – Requirements and Technology Assessment

The traceability of requirements is a baseline essential for the knowledge transfer, future system development and system platform demonstration activities. The concepts and methodology for the design, configuration, integration, analysis, simulation and verification of subsystems are as essential as the set of principles, components, and networking capabilities enabling the definition of advanced integrated systems, so that they can be certified and commissioned by railway authorities.

Phase 3 – Proof of Concepts and SIL4 Brake Use Case

The outcome of the activities will be validated by means of proof-of-concept demonstrators. The proof-of-concepts show the viability of the defined networks and embedded platforms for "drive-by-data" systems to host SIL4 functions and have all properties required for the TCMS system certification. The Brake-by-Wire activities and design concepts for electronics brake-by-wire system as an exemplary SIL4 can be placed and hosted on the same Safe4RAIL TCMS platform.

Contact:

Project coordinator:
Arjan Geven
TTTech Computertechnik AG
Schönbrunner Straße 7
1040 Vienna
Austria
E-Mail: arjan.geven@tttech.com
Web: www.safe4rail.eu

Safe4RAIL

Project Partners:

1 TTTech Computertechnik AG, Vienna, Austria

2 IK4-Ikerlan, Mondragón, Spain

3 Universität Siegen, Siegen, Germany

4 Technikon Forschungs- und Planungsgesellschaft mbH, Villach, Austria

5 Unicontrols A.S., Prague, Czech Republic

6 NewTec GmbH System-Entwicklung und Beratung, Pfaffenhofen/Roth, Germany

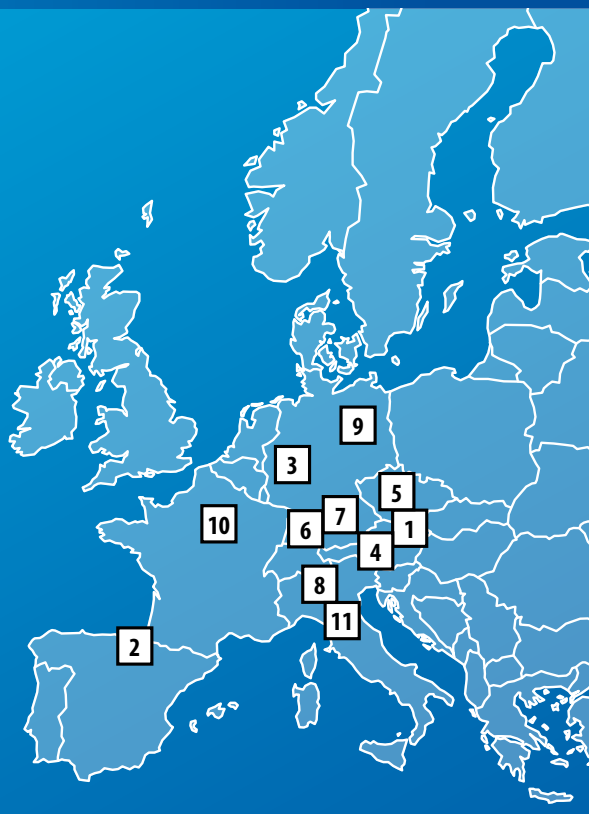
7 TÜV SÜD Rail GmbH, Munich, Germany

8 Eletech S.r.l. – Innovation in electronics, Lomagna, Italy

9 IAV GmbH Ingenieur-gesellschaft Auto und Verkehr, Berlin, Germany

10 Institut français des sciences et technologies des transports, de l'aménagement et des réseaux, Marne la Vallée Cedex 2, France

11 NIER Ingegneria SpA, Castel Maggiore, Bologna, Italy



Consortium:

Safe4RAIL is driven by a cross-industry consortium, with automotive, aerospace, and railway industry experts with proven leadership in advanced networking technologies and design of deterministic embedded computing and networking platforms, modules and components for advanced integrated architectures and by-wire systems.