SAFEDMI

Safe Driver Machine Interface (DMI) for ERTMS Automatic Train Control

Funding: European (6th RTD Framework Programme)
Duration: Sep 2006 - Aug 2008
Status: Complete with results
Total project cost: €2,022,666
EU contribution: €1,234,999

Call for proposal: FP6-2005-TRANSPORT-4
CORDIS RCN: 79979

Background & policy context:

Automatic Train Control (ATC) systems are based both on railway trackside and on-board systems. The increasing level of train traffic and the growing network of high-speed rail lines are now demanding an increase in safety levels of ATC systems. In order to ensure compatibility and interoperability between the ATC systems produced in Europe, the European Rail Traffic Management System (ERTMS) programme has been set up to provide unique functional and non-functional standard requirements.

The ERTMS architecture for on-board ATC encompasses a Driver Machine Interface (DMI) component whose functions and ergonomic requirements are defined so as to satisfy all the related requirements of CENELEC (the European Committee for Electrotechnical Standardisation).

Such requirements do not, as yet, include safety, despite the fact the DMI is required to operate (as a slave) in a critical context, due to the increasing complexity of ATC on-board systems, generated by an increasingly demanding environment and railway line capacities. Therefore, many railway operators have started requiring from their providers DMIs which satisfy being a safe Man Machine Interface reaching at least SIL2 (Safety Integrity Level 2) CENELEC specifications, while avoiding possible loss of driver attention caused by the amount of information displayed.

Objectives:

The objective of the SAFEDMI project was to design and develop a DMI system that distinguishes itself from other train-borne DMIs currently available on the market by being able to satisfy at least SIL2 (safety integrity level 2) according to CENELEC specifications (with all the related implications), and to integrate safe wireless communication interfaces for configuration, software and firmware downloading and diagnostic purposes.

The detailed objectives are:

1. To design and develop a safe DMI integrated with the current onboard ERTMS systems and developed according to ERTMS interface specifications.
2. To study and develop all the hardware and software solutions in order to properly address the safety and fault tolerance issues generated by the SIL 2 requirements.
3. To integrate secure wireless communication interfaces in the DMI for configuration, software and firmware downloading and diagnostic purposes.
4. To design and develop a hardware and software tool infrastructure to support automatic test execution, simulating a driver's actions.

Furthermore, the safety issues at stake are related to:

- Visualisation:
  If an error occurs during the visualisation process, DMI must allow drivers to classify the displayed information as erroneous in the applicable context.
Driver input data acquisition:
In addition to the visualisation issue, some DMI data acquisition from the driver's keyboard must be secure.

Data communication between on-board system components:
The DMI is a slave unit of the onboard vital computer. A secure communication protocol stack has therefore to be provided for connecting safety-related peer agents as part of the architectural design.

Data processing:
In order to satisfy the previous issues, it is evident that the whole data processing has to be secure.

Wireless communication interface:
DMI must be secure. Consequently also DMI configuration (e.g. change of the DMI language set, icons, timeouts, etc.), SW/firmware download, and the wireless communication interfaces also have to be secure.

Methodology:
The project was carried out following five technical steps:

Phase 1: This first step was an analysis of the railway scenarios that will serve as a source of requirements for the project, identifying the technical challenges, threats and resilience requirements that will be addressed by the design, evaluation and testing solutions to be developed in the project. This phase will also assess the risks to be considered while being SIL2 - CENELEC compliant.

Phase 2: focused on the design of hardware and software architectures and fault tolerance mechanisms.

Phase 3: developed secure and non-secure protocols for wireless communication.

Phase 4: developed a comprehensive a comprehensive quantitative evaluation methodology encompassing analytical modelling, simulation and experimental techniques, aimed at assessing the dependability and resilience of applications. Further, a testing framework targeted at the removal of design and malicious faults is built in order to evaluate the technical solutions developed in 2 and 3 above and analyse their efficiency.

Lastly, Phase 5: designed and built an experimental prototype integrating building blocks from the previous phases, together with a suitable application, to illustrate the feasibility of the technical solutions developed in SAFEDMI and analyse their efficiency using controlled experiments.

Parent Programmes:
FP6-SUSTDEV-3 - Global Change and Ecosystems

Institute type: Public institution
Institute name: European Commission
Funding type: Public (EU)

Lead Organisation:

Ansaldo Sts S.p.a.

Address:
Via Paolo Mantovani 3-5
16151 Genova
Italy

Organisation Website:
http://www.ansaldo-sts.com

EU Contribution: €0

Partner Organisations:

Azd Praha Sro

Address:
ZIROVNIKA 3146/2, ZABEHLICE
106 00 PRAHA
Key Results:

The expected results of SAFEDMI were:

- the requirements and constraints to be considered to be compliant with SIL2;
- the SAFEDMI architecture, a preliminary hardware and software specification, the selected wireless communication technology, the communication architecture and a preliminary quantitative evaluation methodology;
- the SIL2-compliant final prototype to be evaluated and validated.

SAFEDMI would directly contribute to the CENELEC Technical Body CLC/SC 9XA ‘Communication, signalling and processing systems’ and in particular to the standardisation activities dealing with ‘Railway applications – Communication, signalling and processing systems – European Rail Traffic Management System – Driver-Machine Interface’.

SAFEDMI would also contribute to CENELEC TC9X-WG12 ‘Electrical and electronic applications for railways’, in the Working Group 12 (WG12) dealing with ‘Communication means between safety equipment and Man Machine Interface (MMI)’.

Documents:

- Design and Evaluation of a Safe Driver Machine Interface.pdf (Other relevant documents)

STRIA Roadmaps:
Cooperative, connected and automated transport, Network and traffic management systems

**Transport mode:** Rail transport

**Transport sectors:** Passenger transport, Freight transport

**Transport policies:** Digitalisation, Safety/Security

**Geo-spatial type:** Network corridors