SAFURE - SAFety and secURity by design for interconnected mixed-critical cyber-physical systems

Newsletter Issue 7 (June 2018)

SAFURE

In this issue

- Message from the Coordinator
- Summary and objectives
- Final results
- Upcoming Events

MESSAGE FROM THE COORDINATOR

The **SAFURE** project has come to a **successful end**, with the completion of the SAFURE telecommunications prototype and well as the completion of the automotive prototype. Final specifications of the SAFURE framework and methodology were also completed. The consortium participated in the **final review meeting**, where the project partners were given the opportunity to show final prototypes and demonstrators. The meeting took place in Bologna, on the **5th of July 2018**.

Summary of the context and overall objectives of the SAFURE project

The SAFURE consortium, the project officer and reviewers at the final review meeting in Bologna, 5th July 2018.

SAFURE targets the design of cyber-physical systems by implementing a methodology that ensures safety and security "by construction". This methodology is enabled by a framework developed to extend system capabilities to control the concurrent effects of security threats on the system behaviour. **SAFURE** addressed the security of safety-critical cyber-physical systems by implementing a holistic approach to safety and security by construction, limiting the impact of security on safety when using common shared resources such as networks and processors, preserving the system from attacks that could affect the overall system safety. At the base of the **SAFURE** solution is the development **of a set of extensions of tools and system capabilities** (referred to as the reference SAFURE Framework) **able to prevent, detect and protect against possible vulnerabilities and attacks through efficient system configurations and reconfigurations, keeping critical subsystems within their safety and security boundaries, without inflicting performance impairments for best-effort applications.** This framework extends system capabilities to preserve the system integrity from time starvation, massive energy dissipation and data corruption, seamlessly integrating security requirements into safety systems in a way that has never been done before. These extensions are applicable from design and development stages to application deployment and execution on multi-core chips and high performance distributed systems. The extended analysis methods, development tools and execution capabilities provided by the framework are supported by a set of guidelines (referred to as the SAFURE Methodology) to assist the designer and the developer to:

- address security in a safety context,
- integrate heterogeneous security and safety requirements in the overall system architecture,
- open subsystems to resource sharing and communication,
- detect potential attacks on system integrity (timing, energy/temperature and data),
- prevent potential attacks through efficient system configuration (off-line),
- enhance mixed-criticality and reconfiguration capabilities (on-line and off-line), keeping security in mind, and
- enhance performance and resource usage on complex systems with safety and security constraints.

Start date:	1 February 2015	*Consortium:*	12 partners (6 countries)
End date:	31 May 2018	*Project coordinator:*	Dr. Klaus-Michael Koch coordination@safure.eu
Duration:	40 months		
Project reference:	644080	*Technical leader:*	Andre Osterhues andre.osterhues@escrypt.com
Project costs:	€ 5,702,631		
Project funding:	€ 5,231,375	*Project website:*	www.safure.eu

This project has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement No. 644080

This work was supported (also) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and agreements employed herein do not necessarily reflect the official views of the Swiss Government.

LinkedIn

https://twitter.com/SAFURE _H2020

SAFURE - SAFety and secURity by design for interconnected mixed-critical cyber-physical systems

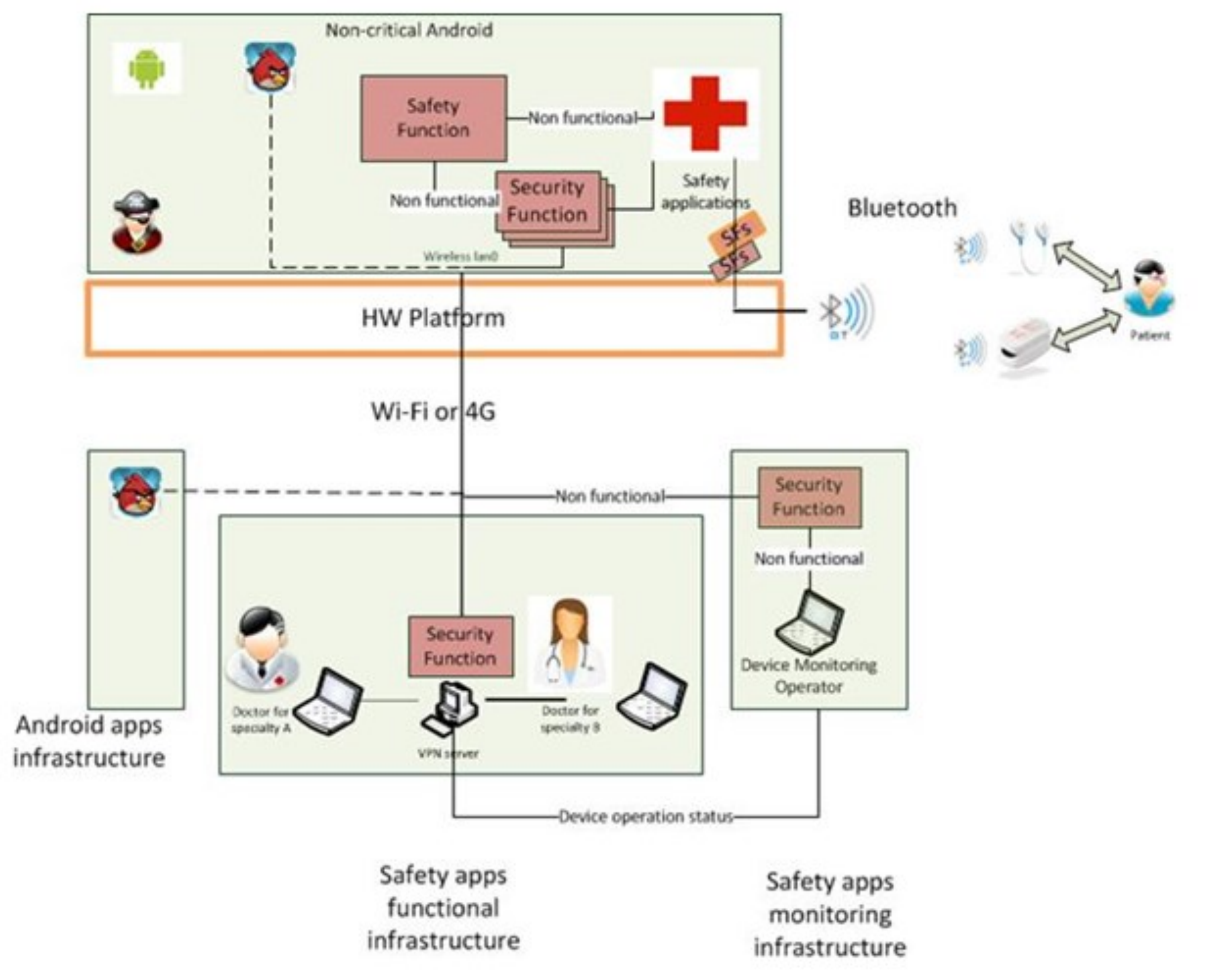
Newsletter Issue 7 (June 2018)

SAFURE

Telecommunications use-case:

A confidential document describing the **telecommunication use-case** has been finalised in M40 of the project. It presents the choices and reasonings for selecting the platform and technologies from a technological and business perspective. It also presents **safety** and **security** features and gives an introduction to SAFURE technologies, which can be applied to the demonstrator. Two Architectures were proposed: An initial architecture with PikeOS and Android, as well as a revised architecture with Android only.

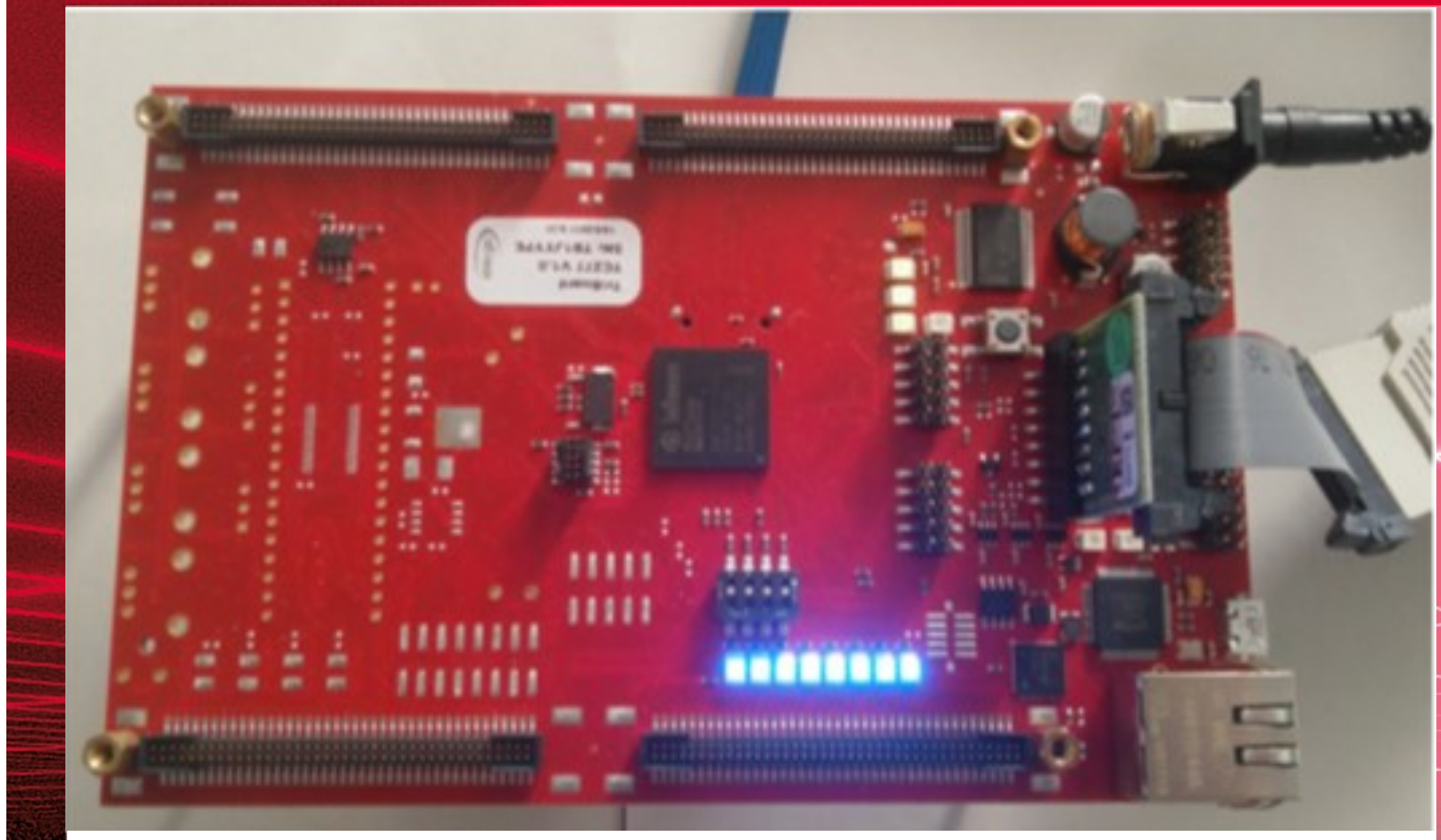
The **telecommunication use-case** demonstrator is based on an Android smartphone connected to a smartband and is providing safety and security capabilities. The evaluation covers the modelling of tasks and resources using the SymTA/S tool, the description of the test methodology, tests of the elements to be evaluated in the systems, and a synthesis of the requirements compliance according to the structure previously defined in "SAFURE Framework Specifications". It is possible to extend the security features in Android by using additional security components such as Cycurlib, in order to ensure better control of health-related data. The addition of safety capabilities is presently quite difficult, considering the lack of control of the Android platform by applications. Hence, safety functionalities are limited to application monitoring and alert propagation whenever degraded conditions can be detected.



Architecture of the SAFURE telecommunications demonstrator.

Automotive use-case:

A deliverable describing the realization of the automotive prototype, according to the architecture previously described in **"Architecture of automotive prototype"** has been released. In particular, the automotive prototype incorporates both the **automotive multi-core** and **network prototype.** For these reasons, the deliverable is organized in three main parts: the automotive multicore prototype, the network automotive prototype, and the integration of automotive network and multicore prototype. The multicore automotive prototype is mainly characterized by a control unit with an **Aurix Tri-core microcontroller.** The powertrain control unit integrated the SAFURE framework to guarantee "freedom from interferences", secure communication over a CAN-bus and to exploit from one hand the new patterns and from the other the new multicore mechanisms provided by the SAFURE framework. The network automotive prototype is focused on safety and security requirements required to enable mixed-critical communication in future in-vehicle Ethernet networks. These two prototypes will be combined together introducing a hardware gateway, which inserts CAN-messages into an Ethernet network. Evluative details of the SAFURE automotive prototype were also provided in a public deliverable „Evaluation of Automotive Demonstrator".



The LEDs of the Triboard indicate ocurring timing faults.

This project has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement No. 644080

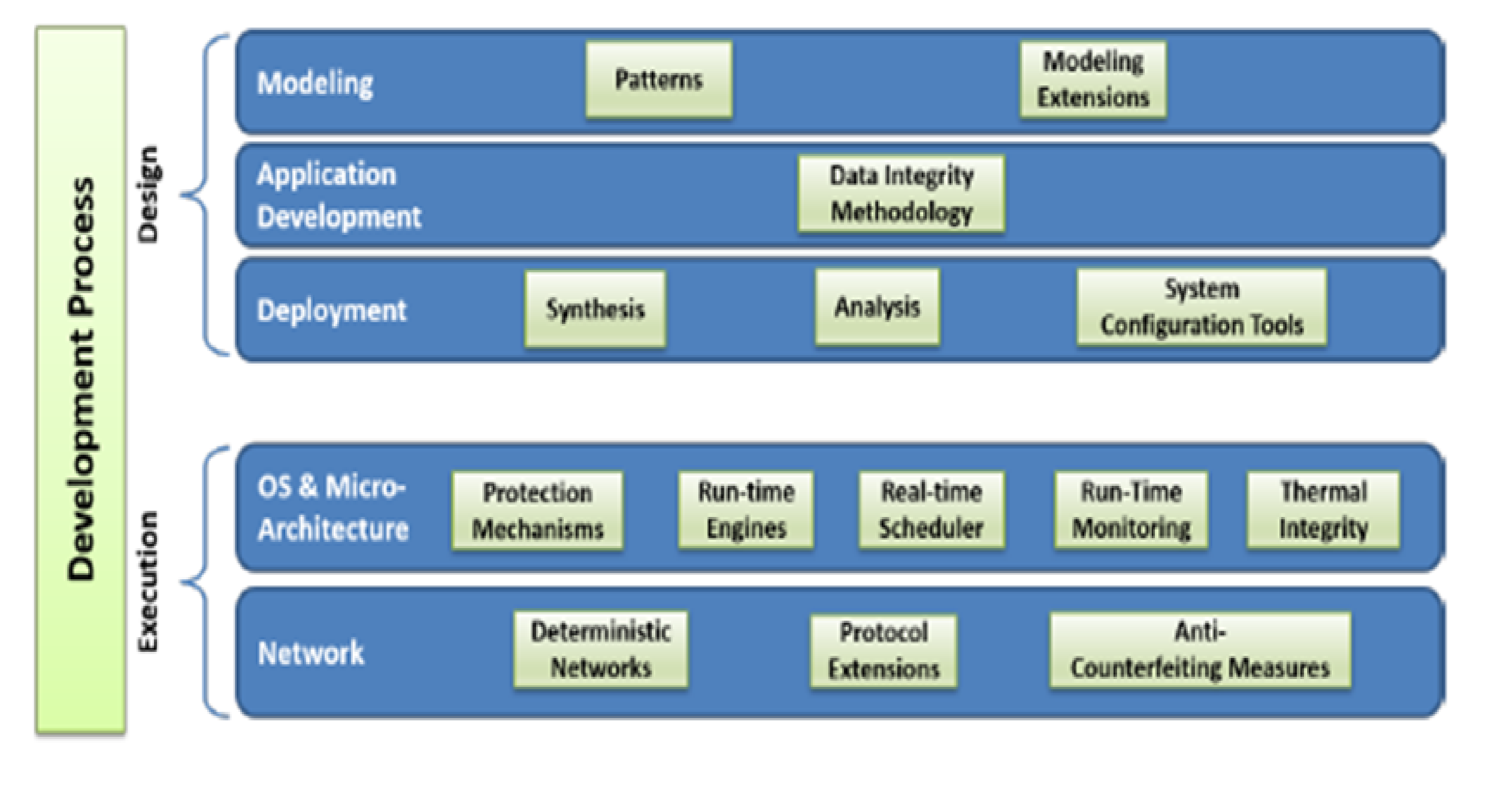
This work was supported (also) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and agreements employed herein do not necessarily reflect the official views of the Swiss Government

https://twitter.com/SAFURE_H2020

SAFURE - SAFety and secURity by design for interconnected mixed-critical cyber-physical systems

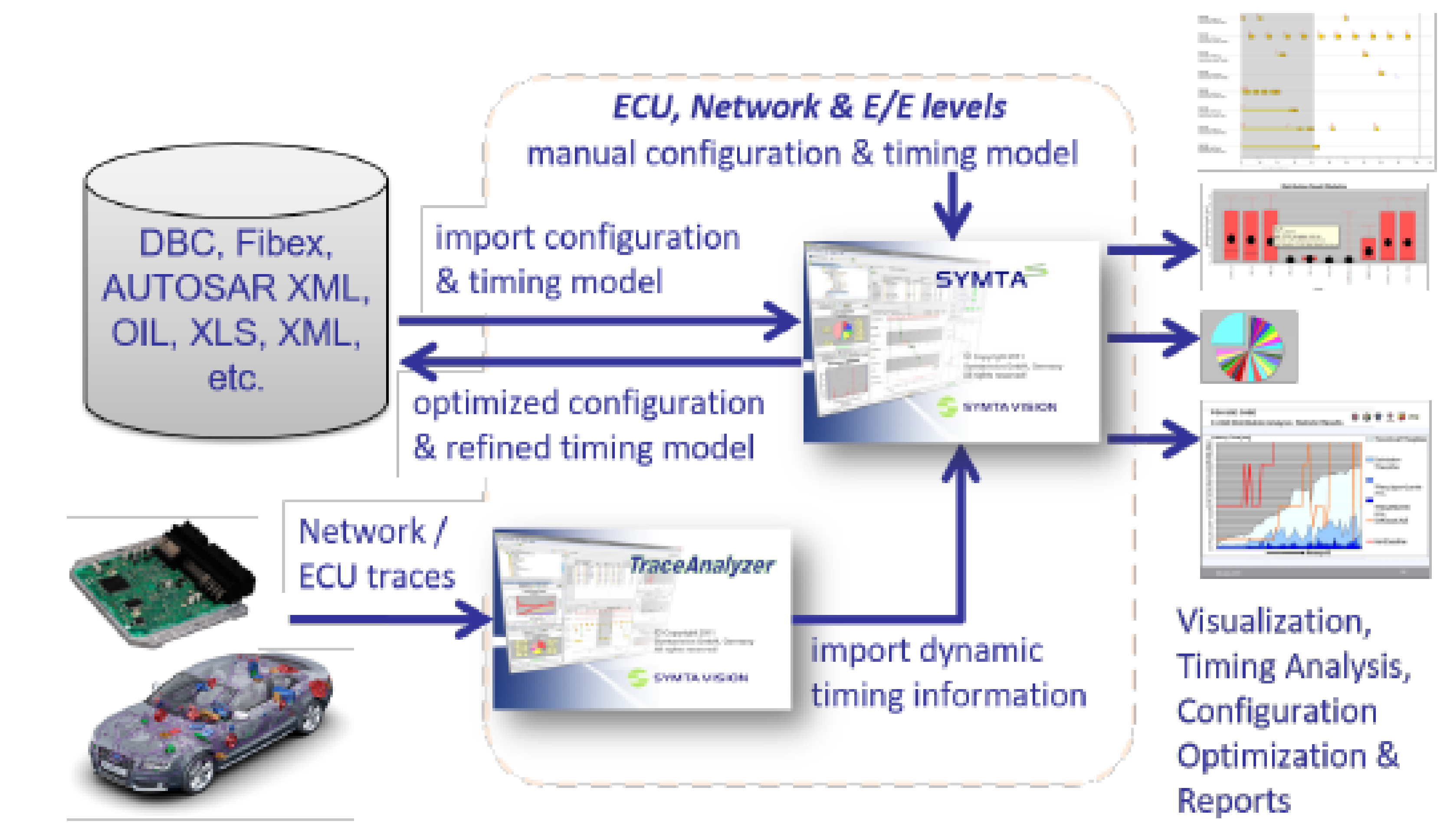
Newsletter Issue 7 (June 2018) SAFURE

SAFURE Framework and Methodology

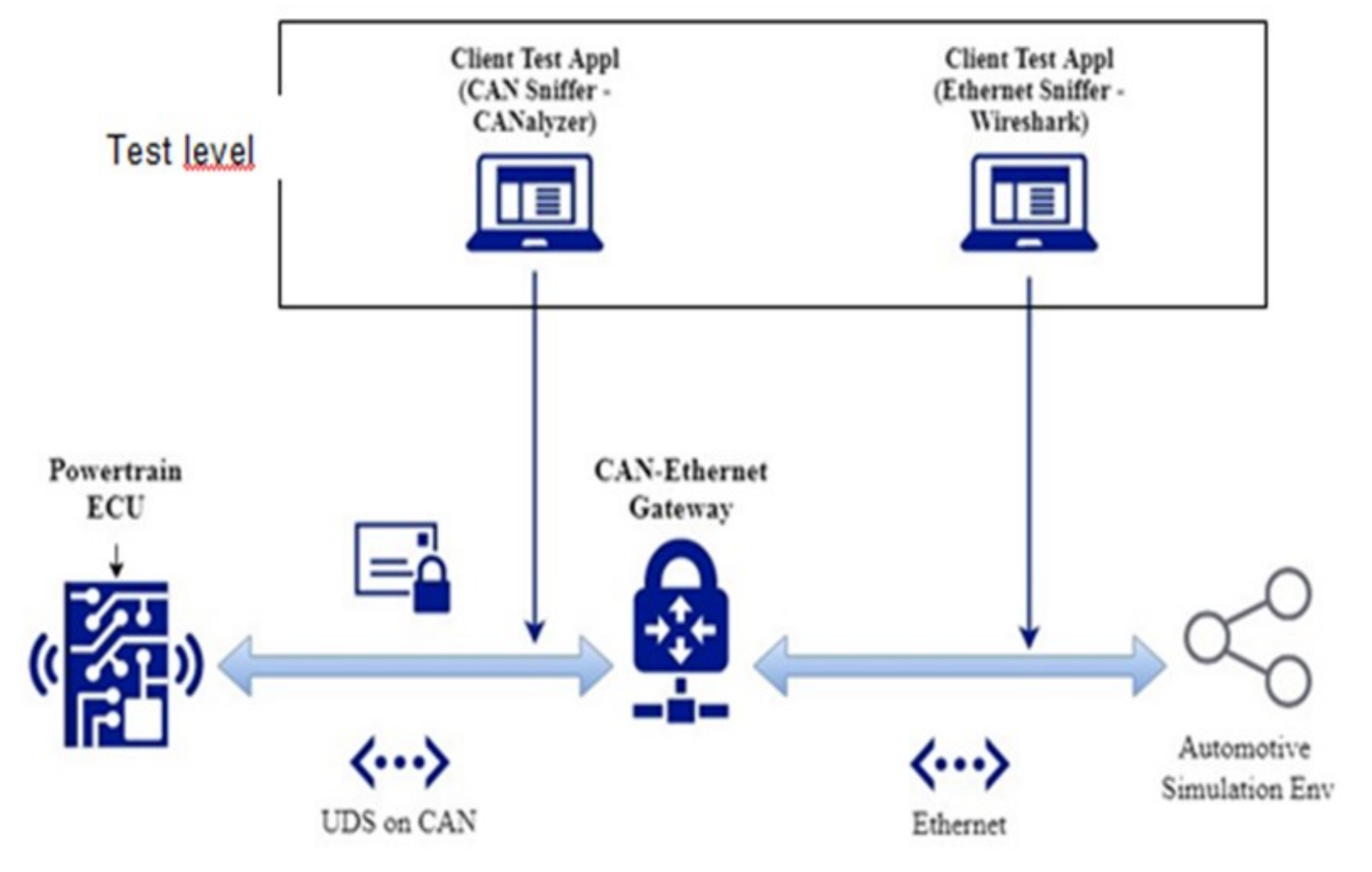


Overview of the SAFURE framework.

Embedded systems are much more complex nowadays than they were a few years ago. As a result, it is becoming increasingly necessary to develop appropriate strategies during the design phase, allowing aspects such as **data integrity,** timing or temperature to be less critical to the system. Not only in the design phase, but also in the verification phase, appropriate tools are necessary to measure and check such aspects in order to optimize the system in a later stage. In „Final Specifications of the SAFURE framework and Methodology" SAFURE partners present strategies, methodologies and tools for each phase to **make embedded systems safe** in this respect. The methodologies and tools developed were tested using so-called demonstrators , which are previously described. Adequate conclusions or, „lessons learned" from the demonstrators should be used as guidelines for future, similar projects from research and industry and provide a framework for such developments.


ECU, Network & E/E levels
manual configuration & timing model
DBC, Fibex, AUTOSAR XML, OIL, XLS, XML, etc.
import configuration & timing model
optimized configuration & refined timing model
SYMTA
Network / ECU traces
TraceAnalyzer
import dynamic timing information
Visualization, Timing Analysis, Configuration Optimization & Reports

Symtavision Tool Suite integrated in automotive developing workflow.


Test level
Client Test Appl (CAN Sniffer - CANalyzer)
Client Test Appl (Ethernet Sniffer - Wireshark)
Powertrain ECU
CAN-Ethernet Gateway
UDS on CAN
Ethernet
Automotive Simulation Env

Combine automotive scenario.

Past Events

Since the previous edition of the SAFURE newsletter in March 2018, The SAFURE project partners has been involved in two activities:

Design Automation Conference

24th - 28th of June 2018, San Francisco, USA

BSC has submitted a paper to the conference, which has been accepted.

The Security Track at the ACM Symposium on Applied Computing

9th - 13th of April 2018, Pau, France

A paper presented by TRT : "METrICS: a Measurement Environment for Multi-Core Time Critical Systems" has won the Best paper award, at the European Congress on Embedded Real-Time Software and Systems (ERTS2018).

All project results (scientific publications and deliverables) are accessible on our project website: https://safure.eu

This project has received funding from the European Union´s Horizon 2020 research and innovation programme under grant agreement No. 644080

This work was supported (also) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and agreements employed herein do not necessarily reflect the official views of the Swiss Government

https://twitter.com/SAFURE_H2020