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

Newsletter Issue 2 (March 2016)

SAFURE

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 so as to control the concurrent effects of security threats on the system behaviour. With this in mind, the project aims at allowing European suppliers of safety-critical embedded products to develop more cost and energy-aware solutions.

Mission

The current approach for security of safety-critical embedded systems is generally to keep subsystems separated, but this approach is now being challenged by technological evolution towards openness, increased communication and use of multi-core architectures. SAFURE will push forward the limits of current approaches on safety and security mixed-critical systems in a way that has never been done before.

Motivation

In this issue

MESSAGE FROM THE COORDINATOR

Since the beginning of the project several conference calls and events dedicated to the project development took place. From 3rd to 5th November 2015 the consortium met for the 1st Technical Meeting in Barcelona, hosted by BSC. The main focus of the meeting was the technical progress of each work package and of the project status in general. First ideas on the work plans of the demonstrators were presented. The meeting brought lively discussions on current and upcoming project objectives.

The partners are now starting to prepare for the 1st Technical & General Assembly as well as Advisory Board Meeting, including external advisors from BMW, Qualcomm or NXP, which will take place in Vienna/Austria in May 2016. Overall, the project is well on track.

SUBMITTED DELIVERABLES (since the project start)

- **D1.1 Use Case specifications** - This deliverable includes the specification of the Use Cases for each of the targeted industry domains, as well as the platforms that will be used for the development of typical embedded applications in each of the domains.
- **D1.2: Use Case requirements** - Deliverable D1.2 categorizes, groups and prioritizes the requirements in order to guide development in other SAFURE work packages. It illustrates the mapping between requirements and how they are reflected in the detailed Use Cases.
- **D1.3: SAFURE framework specification** - This deliverable defines the initial specifications for the SAFURE Framework and delivers the basis for the developments in other WPs. A final version of the specifications will be released at the end of the project.
- **D2.1: Architecture models and patterns for safety and security** - This deliverable is a preliminary document describing the selection of the modelling languages and tools for the definition of the automotive and telecommunication architectures of interest and the constraints that must be addressed to specify safety and security requirements (including timing constraints) and enable their automatic analysis.
- **MS1: Specification and requirements are available**

Public submitted deliverables are available online on the SAFURE website: https://safure.eu/publications-deliverables

Start date:	1 February 2015	*Consortium:*	12 partners (6 countries)
End date:	31 January 2018	*Project coordinator:*	Dr. Klaus-Michael Koch
Duration:	36 months		coordinaton@safure.eu
Project reference:	644080	*Technical leader:*	Andre Osterhues
Project costs:	€ 5,702,631		andre.osterhues@escrypt.com
Project funding:	€ 5,231,375	*Project website:*	www.safure.eu

This project has recieved funding from the European Union´s Horison 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.

Linked in

https://twitter.com/SAFURE _H2020

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

Newsletter Issue 2 (March 2016)

SAFURE

PROJECT PROGRESS

In **WP1**, the **specifications and requirements** have been defined, based on the three industrial use cases. This includes security, safety, and timing aspects. Furthermore, the first version of the SAFURE Framework has been specified. Deliverables **D1.1 "Use Cases specifications"** and **D1.2 "Use Cases requirements"** were submitted as planned in July, deliverable **D1.3 "SAFURE Framework specifications"** was submitted in October 2015.

The purpose of **WP2** is to study and **define models** for the representation of **safety and security related constraints and properties**, considering standards and needs of the automotive domain and the Use Cases. The activities of WP2 are coming close to the completion of the first deliverable (including the preliminary version of the models). The state-of-the art **research and analysis and the gap analysis has been completed** and the definition of the abstract models reached its first release.

WP3 covers the **algorithms for thermal, data and timing integrity for safe and secure systems**. We have had several important results in this WP. Specifically, we have **identified and characterized temperature** as a covert communication channel. Furthermore, we have performed **worst case Ethernet timing analysis**. We have also evaluated the **feasibility/timing analysis of CAN-to-Ethernet gateway.**

In **WP4** two boards have been chosen as a **HW platform**. These are the **Juno Board** and the **DragonBoard 810.** Partners have started work on the **implementation of algorithms and benchmarks** defined in WP3 on the respective platform. Partners are also working on definition of the framework for a coherent presentation of **mixed-critical characteristics**. Works on security aspects and scheduling on OS level are continuing.

WP5 aims to study and enhance existing **Ethernet standard technologies** in terms of performance, safety and security requirements. During the first year of the project, the partners of WP5 have achieved various results, including a **formal analysis for basic SDN timing** as well as a first prototype of a **worst-case analysis** based on compositional performance analysis in SymTA/S. In the context of deterministic network technologies (TTEthernet), a first prototype of the **METADAT Stream Cypher encryption algorithm** has been realised. Further security and anti-counterfeiting aspects are being considered in a security assessment document, which will provide the guidelines for future implementation.

WP6 will start in February 2016. It will develop **industrial applications** according to the Use Cases defined in WP1 and aims to integrate and evaluate the safety and security solutions of SAFURE. During the course of WP6, the SAFURE Framework specifications and methodology will be refined.

WP7 has been successfully kicked-off and headed towards submission of Deliverable **D7.1 "Data Management Plan (DMP)"**, focusing on providing an analysis of the main elements of the data management policy that will be used by the applications with regard to all the datasets that will be generated by the project. **Questionnaires** for DMP have been developed, distributed between the project partners and finally delivered central information for the DMP Deliverable, which was submitted in due time in M06.

In **WP8** SAFURE will start its active **dissemination** phase. SAFURE partners will have a booth at **DATE'16** to present the project and its first results to a wider audience. Additionally, a special session at the upcoming **DAC'16** has been organized to engage representatives from both industry and academia in a discussion about safety and security in future **automotive networks**. Furthermore, additional research results were presented at international conferences and published in international journals.

WP9 assured a smooth project collaboration by applying the initially established project structure as well as internal and external controlling tools. The work progress has been monitored and opportunities as well as threats have successfully been addressed. WP9 further focused on **risk management.** The risk management structure has been described in "**D9.2 – Risk Assessment Plan**", which also includes detailed evaluation of risks and mitigation plans by the WP leaders.

UPCOMING DELIVERABLES AND MILESTONES

- **D3.1: Interim analysis of integrity algorithms -** Overview of existing methods on data management, timing analysis and thermal analysis, together with first results on specific extensions of these methods to secure systems. (due date - April 2016 M15)
- **D4.1: Alpha OS & RTE prototypes** - Mixed-critical real-time scheduler integrated into PikeOS and AUTOSAR OS kernel RTEs are defined and integration strategies are worked out (due date - July 2016 M18)
- **MS2: Prototype architectures and models defined** (due date - April 2016 M15)
- **MS3: Architecture of Use Case demonstrators available** (due date - July 2016 M18)

This project has recieved funding from the European Union´s Horison 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 2 (March 2016)

LASTEST PUBLICATIONS

- Daniel Thiele, Rolf Ernst, **"Formal Analysis Based Evaluation of Software Defined Networking for Time-Sensitive Ethernet"**, DATE 2016, Dresden (Germany), March 14-18 2016
- Daniel Thiele, Rolf Ernst, **"Formal Worst-Case Timing Analysis of Ethernet TSN ’s Burst-Limiting Shaper"**, DATE 2016, Dresden (Germany), March 14-18 2016
- Daniel Thiele, Rolf Ernst, Jonas Diemer, **"Formal Worst-Case Timing Analysis of Ethernet TSN ’s Time-Aware and Peristaltic Shapers"**, Vehicular Networking Conference (VNC), Kyoto (Japan), December 16-18 2015
- Daniel Thiele, Johannes Schlatow, Philip Axer, Rolf Ernst, **"Formal timing analysis of CAN-to-Ethernet gateway strategies in automotive networks"**, Real-Time Systems Journal, Braunschweig (Germany), October 7 2015
- Sylvain Girbal, Xavier Jean, Jimmy Le Rhun,Daniel Gracia Pérez, Marc Gatti, **"Deterministic Platform Software for Hard Real-Time systems using Multi-core COTS"**, Digital Avionics System Conference (DASC 2015) Best Paper Award, Prague (Czech Republic), September 13-17 2015
- M. Jakovljevic and M. Plankensteiner, **"Deterministic Ethernet - High-speed communications with real-time guarantees"**, Forum Funktionale Sicherheit, Vienna (Austria), July 8-9 2015

All publications can be downloaded following: https://safure.eu/publications-deliverables

UPCOMING EVENTS

- **15th - 17th March 2016: Design Automation and Test in Europe (DATE), Dresden/Germany**

The SAFURE project will have a booth at the conference in section of the Proceedings dedicated to European Projects. DATE conference combines the world´s favorite electronic systems design and test conference with an international exhibition for electronic design, automation and test, from system-level hardware and software implementation right down to integrated circuit design. For more information visit: http://www.date-conference.com/

- **24th - 25th May 2016: Technical & AB/GA meeting of SAFURE consortium, Vienna/Austria**

During a two-day meeting, the consortium will internally discuss the work plan for the upcoming months, discuss upcoming challenges, arrange collaboration and if necessary, take decisions during a General Assembly session. The second day will be dedicated to receive external feedback on the project progress and market feasability of the expected results, from industry experts who are taking part in the SAFURE Advisory Board.

- **5th - 9th June 2016: Design Automation Conference (DAC), Austin/USA**

Project partner TUBS organizes the special session "Future Vehicular Networks - Safety and Security" featuring talks about the challenges of safe fail-operational in-vehicle Ethernet communication, secure updates of automotive ECUs, and V2X communication. For more information visit: https://dac.com/

This project has recieved funding from the European Union´s Horison 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