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

Newsletter Issue 3 (September 2016)

SAFURE

It's halftime – 18 months of the SAFURE project passed. Great progress, lots of reports and discussions characterized the first project period. Since the last newsletter in January 2016, major attention was drawn to the refinement of the use cases as well as to the architecture description. Many conference calls and a face-2-face meeting were dedicated to the technical progress of the project and discussions of suitable solutions and detailed concepts.

During the Advisory Board meeting in Vienna, hosted by TTT, in May 2016, the consortium received valuable comments and feedback from our external advisors from BMW, Qualcomm and NXP. These comments pose an exciting challenge and will serve as guidance for future poject work. The partners are now starting to prepare for the 1st Review Meeting which will take place in Brussels in September 2016. Overall, the project is well on track and in line with expectations.

MESSAGE FROM THE COORDINATOR

In this issue

- Message from the coordinator
- Submitted and upcoming Deliverables & Milestones
- Latest Publications
- Project Progress
- Advisory Board Meeting
- Upcoming Events

PUBLIC SUBMITTED DELIVERABLES AND MILESOTNES (since the last newsletter)

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

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

LASTEST PUBLICATIONS

- Davide B. Bartolini; Philipp Miedl; Lothar Thiele, **"On the Capacity of Thermal Covert Channels in Multicores"**, EuroSys'16, London, 18-21 April 2016
- Mischa Möstl; Daniel Thiele; Rolf Ernst, **"INVITED: Towards Fail-Operational Ethernet Based In-Vehicle Networks"**, Design Automation Conference (DAC)
- Marco di Natale; Alessandro Biondi; Youcheng Sun; Stefania Botta, **"Moving from single-core to multicore: initial findings on a fuel injection case study"**, SAE 2016 World Congress and Exhibition
- Gabriel Fernandez; Javier Jalle; Jaume Abella; Eduardo Quiñones; Tullio Vardanega; Francisco Cazorla, **"Computing Safe Contention Bounds for Multicore Resources with Round-Robin and FIFO Arbitration"**, IEEE Transactions on Computers
- Daniel Thiele; Rolf Ernst, **"Formal Worst-Case Performance Analysis of Time-Sensitive Ethernet with Frame Preemption"**, International Conference on Emerging Technologies and Factory Automation (ETFA)

Further information can be found following: https://safure.eu/publications-deliverables

SAFURE ensures Open Access to scientific publications: https://zenodo.org/collection/user-safure _h2020

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.

LinkedIn

https://twitter.com/SAFURE _H2020

Newsletter Issue 3 (September 2016) SAFURE

PROJECT PROGRESS / HIGHLIGHTS

WP1 “Specification & Requirements” was successfully completed with the submission of **D1.3 “SAFURE framework specifications”** in October 2015.

In **WP2 “Architecture design & modelling”** the **state of the art analysis** of the models for safe and secure CPS systems has been completed and so is the **analysis and definition of the abstract modelling concepts** that are required to support the desirable analysis in the domains of time, safety and security. The findings have been documented in the submitted deliverable **D2.1 “Architecture models and pattern for safety & security (Alpha)”.** In addition, the definition of the **extensions to commercial languages** that are required for the practical use of the abstract concepts is underway using the UML/SysML/AUTOSAR Rhapsody modelling tool as a demonstrator. D2.1 contains the early results of this activity.

WP3 “Timing, data & energy integrity algorithms” achieved outstanding results in many different research areas. **Thermal sensors in MPSoC platforms** were identified as a security risk as they may be used to establish a covert communication channel and the covert channel on x86 and ARM based platforms was characterised. Further, **cryptographic algorithms** to be used in the telecommunication use case were identified and implemented. The evaluation of their performance started with the goal to determine their feasibility for **deadline-constrained mixed-critical systems**. In the timing domain, **interferences in multicore platforms** and methods on mitigating those are investigated. Important sources of on-chip interferences were identified and a contention model was developed. Preliminary algorithms were proposed to mitigate these interferences.

In **WP4 “Run-time system & processor architecture”** Pike OS was configured to run on the ARM Juno and Qualcomm SnapDragon 810 with ARMv8. Joint solutions combining **real-time hypervisor Pike OS** and the **crypto library** CycurLIB have been successfully finalised. Extensions of AUTOSAR OS for time and memory protection have been defined and implemented. Further, an analysis approach was developed to **characterise the worst-case temperature** on a hardware platform executing a mixed-critical application.

In **WP5 “Predictable, Secure Communication Infrastructure”** the **prototype of the worst-case Ethernet analysis** using the SymTA/S analysis tool has been extended to consider FIFO and strict priority scheduling. A **formal timing analysis** of switched Ethernet by exploiting FIFO scheduling has been researched, as well as a **formal worst-case performance analysis** of time sensitive Ethernet with frame pre-emption. First experiments regarding the influence of cryptographic mechanisms on the performance of deterministic networks has taken place. A compilation of data integrity algorithms that could to be implemented in SAFURE has been conveyed in order to cover the anti-counterfeiting measures. Moreover, the security assessment document with focus on the telecommunication and automotive domains has been expanded.

In **WP6 “Integration and evaluation of Use Cases”**, partners started to work on the **three industrial use cases**: telecommunication, automotive multi-core and automotive network. In particular, the **architectures of the prototypes** have been defined according to the requirements and use cases defined in WP1 as well as modelling features provided in WP2. Furthermore, the implementation of the use cases was fostered, in order to efficiently integrate technologies produced by WP4, thermal, data and timing integrity algorithms from WP3 as well as the communication prototype for Ethernet delivered in WP5.

In **WP7 “Exploitation”**, **D7.2 “Intermediate business plan, technology and market watch and updated exploitation plan”** presents **an intermediate business plan, a technology and market watch and an exploitation plan** to ensure the adoption of the SAFURE Framework methodology to build safe and secure solutions on multi-core platforms for mixed-criticality markets. Important elements of this deliverable include: a business model canvas, an external environmental analysis (PEST), a SWOT analysis, a continuous technology and market watch strategy as well as a brief summary regarding standards and guidelines related to security and safety.

In **WP8 “Dissemination and Communication”** the SAFURE consortium is working on the project’s **dissemination activities**. This includes presenting the project at the DATE 2016 conference in Dresden with a booth, as well as a technical meeting with the advisory board in Vienna. In April 2016 and June 2016, the project was presented at the Road2CPS in Vienna and the DAC in Austin, Texas, respectively.

In July the first official project period (18 months) of SAFURE ended, which brought the **reporting process** including templates, structure, inputs etc., for both technical and financial issues, to the centre of attention in **WP9 “Project-, Risk-, and Innovation Management”**. Further, the work progress has been monitored and opportunities as well as threats have successfully been addressed.

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

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

Newsletter Issue 3 (September 2016)

SAFURE

ADVISORY BOARD MEETING

In May 2016 the first advisory board meeting was hosted by TTT in Vienna, Austria. The advisory board of SAFURE consists of three independent external advisors from the companies BMW, Qualcomm and NXP. The progress and the main intermediate results of the project were presented to the AB members, who in turn provided their feedback to the consortium. In general, the presentations were very well conceived by the AB members which was reflected in their feedback: "During the AB meeting, it was evident that the consortium has high competence in both fields (safety and security), which was demonstrated in insightful technical talks presenting novel research. The project is a great chance to bring safety and security aspects together to talk about the coexistence and interplay between the two."

UPCOMING DELIVERABLES AND MILESTONES

- **D2.2: Architecture models and patterns for safety & security -** Presents a final and complete description of the selected modelling languages and definitions of possible extensions of existing standard languages (due date - September 2016, M20)
- **D4.2 Analysis of runtime and software applications on multi-core** - Includes a methodology description and application results (due date - January 2017, M24)
- **MS4: Final architectures and models defined** (due date - September 2016, M20)

UPCOMING EVENTS

- **20th - 21st September 2016: Preparation & Review Meeting, Brussels/Belgium**

During a half-day meeting, the SAFURE consortium will internally discuss, prepare and harmonize the presentations for the upcoming review meeting. On the second day the review meeting will take place at European Commission's premises in Brussels. In the course of this meeting the consortium members will present the project progess to the officer and the reviewers who in turn will provide their feedback.

- **17th - 19th January 2016: Technical & AB/GA meeting of SAFURE consortium, Paris/France**

In the course of a two-day meeting, the project members will discuss the work plan for the upcoming months as well as upcoming challenges, align and arrange collaboration and take decisions during a General Assembly session if required. Half a day will be dedicated to receive feedback on the project progress and market feasability of the expected results, from external industry experts who are part of the SAFURE Advisory Board.

- **6th - 9th September 2016: ETFA Conference, Berlin/Germany**

Project partner TUBS will have a keynote talk on opportunities and pitfalls of Automotive Ethernet, thereby discussing the use of Switched Ethernet in time and safety critical applications before describing potential shortcomings and mitigation strategies. For more information visit: http://www.etfa2016.org/

TTTech Ensuring Reliable Networks

THALES

MAGNETI MARELLI

INSTITUTE OF COMMUNICATION, INFORMATION AND PERCEPTION TECHNOLOGIES

Scuola Superiore Sant'Anna

SYSGO EMBEDDING INNOVATIONS

SYMTA VISION

escrypt Embedded Security by ETAS

Technische Universität Braunschweig

BSC Barcelona Supercomputing Center Centro Nacional de Supercomputación

ETH zürich

TECHNIKON

THALES

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