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

Newsletter ISSUE 4 (MAY 2017)

SAFURE

MESSAGE FROM THE COORDINATOR

The H2020 project SAFURE is currently in its final project year. All in all **15 deliverables** have been submitted and **4 milestones** have been reached so far. The first review meeting in September 2016 was very successful. According to the reviewers, SAFURE is an **excellently up-to-date project** with a top level consortium. In January 2017 the partners met for a technical / Advisory Board meeting in Paris/France where the team discussed the current project status and the plans for the upcoming months. At the beginning of May there was an intermediate review conference call in order to inform the EC about the platform / board decisions. For a more detailed project overview, please visit our project website: www.safure.eu.

In this issue

ADVISORY BOARD MEETING

In January 2017, the second Advisory Board meeting was hosted by TCS in Paris. Two Advisory Board members were present, Roberto Avanzi (ARM) and Christian Herber (NXP), and discussed the progress and intermediate results with the SAFURE consortium. The consortium thanks the AB members for the very valuable feedback and fruitful discussions during this meeting.

SUBMITTED PUBLIC DELIVERABLES

since the last newsletter

- **D2.2: Architecture models and patterns for safety and security** This deliverable is a 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 or the synthesis of mechanisms that guarantee the required levels of timing, safety and security.

The public deliverable D2.2 has been submitted on 31st January 2017 to the European Commission.

UPCOMING PUBLIC DELIVERABLES

- **D3.2 Final Analysis of run-time and software applications on multicore -** includes a report describing the integrity methods and protection mechanisms related to data management, timing and thermal analysis for safe and secure systems as developed in WP3 (in July 2017).
- **D3.3 Integration Methodology** - Includes a report which provides the design guidelines for ensuring the integrity of safe and secure systems based on the analysis methods and protection mechanisms developed in WP3 (in July 2017).
- **D7.3 Technology watch report** - This document is a public extract of the D7.2 business plan, technology watch and exploitation report, covering only technology aspects (in July 2017).

All finalized public deliverables are accessible on the SAFURE website.

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

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

Newsletter ISSUE 4 (MAY 2017)

SAFURE

PROJECT PROGRESS / HIGHLIGHTS

WP2 "Architecture design & modelling" has been completed in January 2017 with the final deliverable D2.2. Analysis and synthesis methods of the proposed methodology are described in D2.2 and were presented in several workshops. These presentations have been at the MESAS (Modelling and Simulation for Autonomous Systems) Workshop in 2016 in Rome, at the FORSE (FORmal methods for Security Engineering) Workshop in 2017 in Porto. The MESAS contribution has been extended and has been published as part of a Springer series book. In **WP3 "Timing, data & energy integrity algorithms",** the first analysis of the frequency covert channel has been conducted. Cryptographic libraries, including data integrity algorithms, have been ported to the real-time operating system PikeOS. Current work includes improving the robustness of thermal covert channels and corresponding thermal protection mechanisms, as well as timing analysis algorithms for Ethernet. Methods for analyses of systems in overload conditions have been developed and this work has been submitted to a conference for publication. Mixed criticality thermal protection mechanism has been developed and has been submitted to EMSOFT for publication. Preliminary analysis of a covert communication channel based on operating frequency has been completed and has been submitted to IEEE MICRO for publication. In **WP4 "Run-time system & processor architecture"**, memory protection drivers for ERIKA OS have been implemented and thermal protection mechanisms have been completed and evaluated. Furthermore, partners have decided to change the hardware platform from the DragonBoard to the ARM Juno board. **WP5 "Predictable, Secure Communication Infrastructure"** aims at studying and enhancing Ethernet technologies. The formal worst-case analysis for Ethernet AVB has been completed and integrated into the commercial tool SymTA/S. For the Metadata Stream Cipher for TTEthernet a randomness test has been performed and final results regarding the network performance for encrypted best-effort traffic have been provided. Formal analyses for Ethernet TSN traffic shaping have been finished and presented with ongoing work on additional TSN standards.

WP6 "Integration and evaluation of Use Cases": The first iterations of the telecommunication, automotive multi-core and automotive network demonstrators were presented. Algorithms and scheduling schemes developed in WP3 have been integrated into the commercial tool SymTA/S. Work on the integrated use-case for combining the automotive multi-core and network use-case, focusing on network and security constraints, has begun. In automotive multi-core use case, the Performance Monitoring Counter (PMC) infrastructure developed by BSC is successfully tested. For the telecommunication use-case, secure Bluetooth based communication between several devices on different physical architectures was developed. In **WP7 "Exploitation"**, the team worked on the identification of actual industrial-grade telecom technologies compliant with safety and security aspects in SAFURE. Furthermore, the consortium is working on business cases for privacy and trust third parties in the telecom domain as well as on the upcoming D7.3 "Technology watch report". In **WP8 "Dissemination and Communication"** the consortium is working on the project's dissemination activities. The latest public activities include participation at the HiPEAC 2017 Workshop and the SCIS Results 2016. An Advisory Board meeting was held in Paris in January 2017. **WP9 "Project-, Risk-, and Innovation Management"** main focus was on the creation of the first periodic report, the intermediate review report and the organisation of several meetings and telephone conferences.

PAST AND UPCOMING EVENTS & CONFERENCES

- **24th of January 2017: SCIS Results, Palaiseau / France**

  Presentation of the Budget Based RunTime Engine developed as part of SAFURE.
- **19th of February 2017: FORSE Workshop, Porto / Portugal**

  Presentations of results of D2.2.
- **6th of April 2017: SAC conference, Marrakesh / Morocco.**

  Presentation of results of the code generations from models of D2.2.
- **27th of June 2017: 17th International Workshop on Worst-Case Execution Time Analysis (WCET 2017), Dubrovnik / Croatia**
- **9th – 11th of October 2017: Technical & GA meeting of SAFURE consortium, Barcelona / Spain**

  In the course of the 2.5 days meeting, the SAFURE consortium will discuss the work plan for the next months as well challenges, align and arrange collaboration and take decisions during a General Assembly meeting if required.
- **15th – 20th of October 2017: Embedded Systems Week 2017 (EMSOFT 2017), Seoul / South Korea**
- **5th – 8th of December 2017: IEEE Real-Time Systems Symposium – RTSS 2017, Paris / France**

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 4 (MAY 2017)

SAFURE

PLATFORM - ALTERNATIVE BOARDS

One of the ambitious objectives of the SAFURE project is the integration of a large number of technologies developed in WP3/WP4 onto one single hardware platform along with the Telecom use case. This objective has shown to be not viable due to the limitations of the different hardware platforms available. The issues originate from the inability to access the required platform documentations which are required to integrate the developed technologies. The SAFURE team presented its contingency plans and mitigation actions to the consortium, including how the main project goal of the SAFURE framework can be achieved and remaining objectives fulfilled.

All in all, although the **DragonBoard** seemed to be the platform fitting everybody's needs, it failed to fulfil the requirements for its use in SAFURE. In the light of this, a number of actions have been taken. The evaluation, mostly led by SYSGO, brought onto the table a number of candidate platforms, which the partners assessed against their needs and constraints. This analysis required purchasing some additional boards to speed up technical assessments. The result is that no single board satisfies all partners' needs. SAFURE has elaborated a plan to use internal prototypes to evaluate WP4 technologies as preparation for the SAFURE Framework in WP6:

ARM Juno board: This board has been used to integrate PikeOS from SYSGO, TRT RTE scheduling and the WP4 mixed critical prototype. Also, some (limited) technology from BSC will be integrated. This approach will allow integrating SYS, TRT, BSC and ETHZ technologies onto a single board and obtain results in an industrial (avionics) prototype. TRT, on its side will be able to perform all the planned research on the Juno board as it is the only platform where PikeOS is available right now. Results from this experiment will be extrapolated to the Telecom use case by a smart selection of the telecom use case platform.

Sony Xperia: This platform, by being industrial, is of the interest of TCS and they have started porting their use case onto this platform as part of WP6. PikeOS porting is also possible (although difficult) and has just started. Given that documentation available is very limited and some features such as hardware virtualization are disabled, PikeOS porting is progressing slowly and a complete and successful porting cannot be guaranteed at this stage. ESCR will port its security algorithms to this platform for the Telecom use case.

Infineon AURIX TC27x:

Partner BSC is familiar with this board and its technology developed in WP3 already accounts for all the features needed for porting it to the AURIX platform. BSC provided first sets of tests to MAG as a preliminary step towards integration in the automotive use case. ESCR will use the Infineon AURIX platform as a basis for the Automotive multi-core demonstrator.

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