

Newsletter

Issue 1 - September 2015

SAFURE

MAIN PROJECT INFORMATION

SAFURE targets the design of cyber-physical systems by implementing a methodology that ensures safety and security by construction. This methodology will be enabled by a framework developed to extend system capabilities so as to control the concurrent effects of security threats on the system behaviour. The current approach for security on safety-critical embedded systems is generally to keep subsystems separated, but this approach is now challenged by technological evolution towards openness, increased communication, and use of multi-core architectures. SAFURE addresses these problems and provides a holistic approach to design safe and secure dependable embedded systems by preventing and detecting potential attacks, and to empower designers and developers with analysis methods, development tools, and execution capabilities that jointly consider security and safety. The outcome of the SAFURE

project will be a framework with the capability to detect, prevent, and protect systems against security threats on safety, as well as the ability to monitor system integrity from the application level down to the hardware level including time, energy, temperature, and data integrity. A methodology will be developed that supports the joint design of safety and security of embedded systems, assisting the designers and developers with tools and modelling language extensions. The project is driven by three industrial use cases, which cover diverse application areas, ranging from embedded multi-core systems to telecommunication and automotive networking. SAFURE plans to release recommendations for extensions of standards to integrate security on safety-critical systems and to compile specifications to design and develop SAFURE-compliant products.

In this issue

- Main project information
- Message from the coordinator
- Project Progress
- Publications
- Submitted Deliverables
- Upcoming Deliverables & Milestones
- Upcoming Events

MESSAGE FROM THE COORDINATOR

The intention of this Newsletter is to open a new communication channel in order to provide news on the project progress and to discuss ongoing topics relevant to SAFURE for internal and external project partners, stakeholders, and all other interested bodies. For more detailed information about and around the project we warmly invite you to have a look on our project website, which is constantly kept up-to-date with the latest project related news: www.safure.eu.

The project has successfully started with the Kick-Off meeting in February 2015 and since then the project has been in its initial stages of formation. The use case specification and the requirements were being elaborated and defined to achieve a step towards a common SAFURE framework. Further, ground-forming discussions on modeling safety, security and timing, integrity algorithms, IT infrastructure, and the evaluation plan are ongoing. The SAFURE project has a well-balanced and focused consortium - comprising 12 partners from 6 countries - and brings together a European team of recognized organizations and respected universities with scientific and technological backgrounds. It is well-positioned intellectually and geographically to achieve its objectives.



Start date: 1 February 2015

End date: 31 January 2018

Duration: 36 months

Project reference: 644080

Project costs: € 5,702,631

Consortium: 12 partners (6 countries)

Project coordinator: Dr. Klaus-Michael Koch
coordinator@safure.eu

Technical leader: Andre Osterhues

andre.osterhues@escrypt.com



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.

Linked in



https://twitter.com/SAFURE_H2020

PROJECT PROGRESS

The SAFURE project has started successfully and the ongoing work is well on track.

In **WP1 "Specifications and requirements"** have been defined. This includes security, safety, and timing aspects for three use cases (Telecom, Automotive Multi-Core, and Automotive Network). Furthermore, the SAFURE Framework has been outlined.

Deliverables D1.1 (Use Cases Specifications) and D1.2 (Requirements Specification) were submitted as planned.

For D1.3, the consortium agreed on an extension of the deadline until October 2015.

WP2 "Architecture design & modelling" started soon after the beginning of the project. The initial part of WP2 is dedicated at finding state of the art references to models, standards, and research results for the description of timing, safety, and security, properties, standards, and mechanisms. This effort is documented in the current version of D2.1 (due in December). The state of the art analysis is almost completed and will be the basis for the second part of WP2 regarding the definition of a proposal for models according to the most popular and most adequate methodologies and formalisms.

In **WP3 "Timing, data & energy integrity algorithms"** partners are currently reviewing the requirements from WP1 with respect to their impact on timing and resource sharing integrity. SAFURE partners perform initial steps towards developing methods and algorithms to analyze and mitigate timing and thermal effects in particular, timing analysis of Ethernet, hierarchical scheduling, and covert channels (e.g. security and safety threats due to temperature) will be investigated.

In **WP4 "Run-time system & processor architecture"** HW boards candidates have been discussed. The WP4 plans have been refined with partner synchronising on plans and dependencies. Works on security aspects and scheduling on OS level have been started. The preparation for work on timing and energy assessments wrt the board candidates have been initiated.

In **WP5 "Predictable, Secure Communication Infrastructure"**, work on formal analysis methods for Ethernet TSN and software defined networking in the context of real-time systems started. Moreover, the selection of security network protocols is currently taking place, as well as the first steps towards their analysis.

WP6 "Integration and evaluation of Use Cases" 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 "Exploitation" will develop exploitation strategies to ensure the required impact of the project and promote the adoption of the SAFURE methodology (e.g. by recommendations to standardization bodies).

In **WP8 "Dissemination and Communication"**, external communication channels (website etc.) and internal communication infrastructure (common repository, mailing lists, etc.) have been set up. Project information has been released on the website and a project leaflet was created. Furthermore, first scientific results have been published.

In the course of **WP9 "Project-, Risk- and Innovation Management"** the project kick-off was successfully prepared and the ongoing work is on good track. Collaboration among partners is well functioning and quite efficient due to the effective implementation of project management structures, a well-established IT infrastructure and regular dedicated and focused conference calls.

PUBLICATIONS

- Gabriel Fernandez, Javier Jalle, Jaume Abella, Eduardo Quiñones, Tullio Vardanega, Francisco J. Cazorla, "**Resource Usage Templates and Signatures for COTS Multicore Processors**", 52nd Design Automation Conference (DAC), San Francisco (California), June 7-11 2015
- Gabriel Fernandez, Javier Jalle, Jaume Abella, Eduardo Quiñones, Tullio Vardanega, Francisco J. Cazorla, "**Increasing Confidence on Measurement-Based Contention Bounds for Real-Time Round-Robin Buses**", 52nd Design Automation Conference (DAC), San Francisco (California), June 7-11 2015
- M. Jakovljevic and M. Plankensteiner, "**Deterministic Ethernet - High-speed communications with real-time guarantees**", Forum Funktionale Sicherheit, Vienna, July 8-9 2015



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



SUBMITTED DELIVERABLES

- **D1.1 Use Cases Specifications:** The Use Cases Specifications deliverable consists of a description of the three use case scenarios (Telecom, Automotive Multi-Core, and Automotive Network). For each use case scenario, the motivation and objective is stated, followed by details about the respective use cases (including actors, goals, triggers as well as pre- and postconditions).
- **D1.2 Requirements Specification:** The Requirements Specification deliverable comprises a complete set of requirements for the SAFURE platform, which can be categorized into functional and non-functional (specific to security, safety, architecture design, real-time operating system, time analysis, temperature, mixed-critical, hardware platform, or other) requirements. The requirements have been assign to either the respective use case scenario or to common requirements for all scenarios.
- **D7.1 Data Management Plan:** SAFURE is taking part in the Horizon 2020 Open Research Data Pilot. This deliverable describes the data management lifecycle for all data sets within the project.
- **D8.1 Internal and external IT communication infrastructure and project website:** This briefly describes the website and its functionality. Further, it describes the tools provided within the IT infrastructure to facilitate cooperation and coordination.

UPCOMING DELIVERABLES AND MILESTONES

- **D1.3: SAFURE framework specification** - Framework specifications will be defined as input for the development in other WPs. (due date - October 2015, M09)
- **D2.1: Architecture models and patterns for safety and security** - Modelling languages and tools for automotive and telecommunication architectures will be selected. (due date - January 2016, M12)
- **D9.2: Risk assessment plan** - Critical Path Analysis will show potential threats to the project and identify risks and eventual mitigation plans. (due date - January 2016, M12)
- **MS1: Specification and requirements** (due date - October 2015, M09)

UPCOMING EVENTS

- **30th September - 1st October 2015:** Symtavision NewsConference: Project partner Symtavision will be hosting their annual conference on timing analysis in Braunschweig, Germany. The Symtavision NewsConference provides a forum to discuss trends and solutions for the development of reliable, safe, and efficient embedded real-time systems. Engineers, managers, technology experts, and researchers use this opportunity to share their experiences, visions, questions, and requirements.
See here for further information: <https://www.symtavision.com/events/9th-newsconference-2015/>
- **3rd - 5th November 2015:** First SAFURE technical meeting at Barcelona Supercomputing Center in Barcelona, Spain. As all technical work packages have started, this technical meeting will be used to discuss the technical progress of SAFURE and to synchronize efforts to reach the common goal of a safe and secure design methodology for interconnected mixed-critical cyber-physical systems.



Scuola Superiore Sant'Anna



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

