SAFURE

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

Project number: **644080**
Project website: **www.safure.eu**
Project start: **1st February, 2015**
Project duration: **3 years**
Total costs: **EUR 5.702.631**
EC contribution: **EUR 5.231.375**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 644039.

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

SAFURE

Mission of SAFURE:

SAFURE's mission is to design a cyber-physical system 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.

Motivation:

The current approach for security on safety-critical embedded systems is generally to keep subsystems separated, but this approach is now being challenged by technological evolution towards openness, increased communications 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.

Objectives:

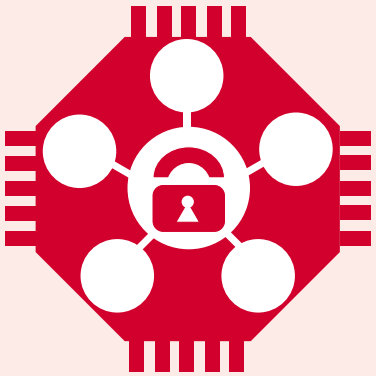
The project SAFURE aims at addressing the security of safety-critical cyber-physical systems by implementing a holistic approach to safety and security by construction. For this purpose, extensions of tools and system capabilities are developed to prevent, detect and protect against possible vulnerabilities and attacks. Efficient system configurations and reconfigurations, keep critical subsystems within their safety and security boundaries without inflicting performance impairments for best-effort applications. Thus, the SAFURE Framework will extend system capabilities to preserve the system integrity from time starvation, massive energy dissipation and data corruption, seamlessly integrating security requirements into safety systems from a new point of view.

The specific objectives of the SAFURE project are:

- **Objective 1: Holistic approach to safety and security by construction**
  One objective of SAFURE is to implement a holistic approach to safety and security by construction of embedded dependable systems, preventing and detecting potential attacks and increasing end-to-end system performance for security and safety-critical domains.

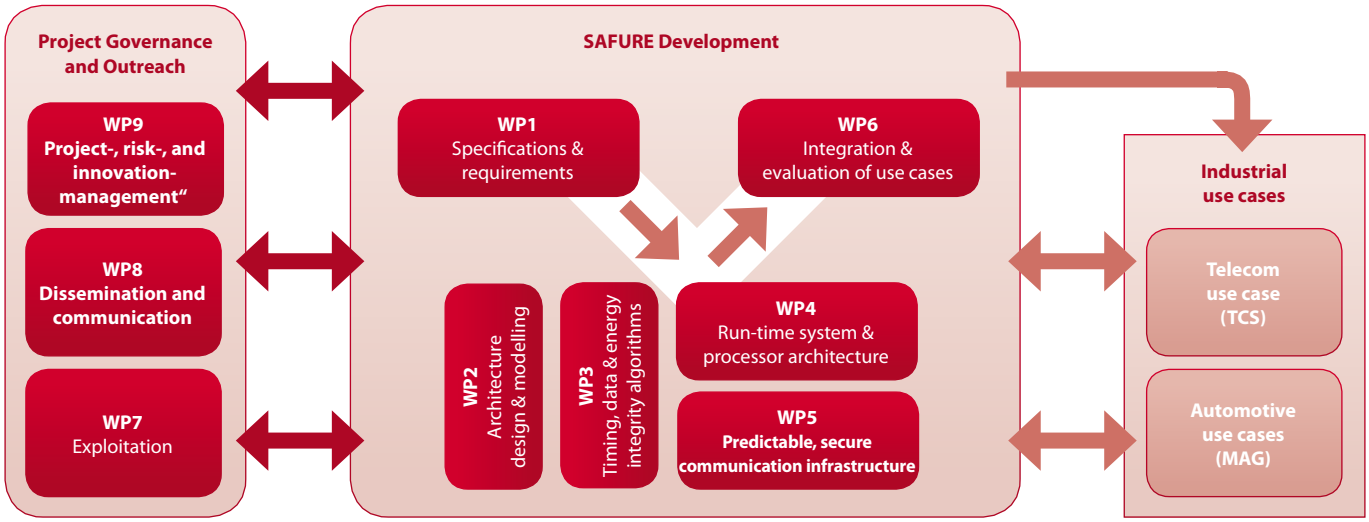
- **Objective 2: Empowering designers and developers**
  Objective 2 is about empowering designers and developers with analysis methods, development tools and execution capabilities that jointly consider security and safety, communications and runtime system support requirements.

- **Objective 3: Opportunity to extend current standards**
  The third specific objective aims at providing extensions to current safety-related standards that will set the ground for the development of SAFURE-compliant safe and secure mixed-critical embedded products.



SAFURE

SAFURE structure of the work plan



Technical Approach:

The SAFURE project activities are organized considering the three industrial use cases that guide the development of the SAFURE Framework and Methodology. They will be processed within 36 months and are structured in the following nine work packages.

WP1: Specifications & requirements
Based on the specifications of the industrial use cases, WP1 will define the combined safety and security requirements that will be used to validate the solutions developed during the project. Furthermore, it will produce the first release of the Framework specifications.

WP2: Architecture design & modelling
WP2 will combine state of the art solutions to model safety requirements and extend them with the security concerns that the applications require. It will also consider the architecture design and the modelling methodology which these solutions will provide for the SAFURE Framework.

WP3: Timing, data & energy integrity algorithms
SAFURE will investigate three different integrity aspects: timing, energy/temperature and data. Their corresponding algorithms will be developed and integrated into the SAFURE Framework in the WP3. Timing and data integrity results will then be used to develop the tools and libraries for the Deployment Layer and also serve as inputs for the infrastructure studies (WP4 and WP5). Last, energy/temperature integrity studies will provide the means to consider the effect of energy/temperature on the behaviour of processors that could change the applications performance, thus affecting the timing integrity. The energy/temperature integrity considerations will be combined with the timing integrity solutions and provide inputs for the processing infrastructure (WP4).

WP4: Run-time system & processor architecture
The so-called COTS multi-cores and the operating systems will be considered in WP4. Hereto, solutions will be implemented in the SAFURE Framework – OS & Micro-Architecture Infrastructure. Studies to master the effect of interferences that occur on multi-cores when running multiple applications (or threads) will provide enhanced used in WP3 to improve timing integrity results, e.g. providing more accurate and performance-wise scheduling. Extensions to current operating systems such as required in automotive or telecommunications will be developed.

WP5: Predictable, secure communication infrastructure
In WP5 safety-oriented switched Ethernet technologies will be studied to enhance their performance and address security requirements. Extensions to protocols and network switches will be implemented to address the impact of security on safety in the SAFURE. The data and timing integrity studies conducted in WP3 will impact the development of these extensions and conversely these extensions will impact data and timing integrity solutions.

WP6: Integration and evaluation of use cases
WP6 will synthesize the specifications for the conception of new systems with safety and security requirements and ensure that the solutions provided for each of the SAFURE Framework Layers are interoperable. The different tools, methods and infrastructure solutions will be evaluated on three different use cases, designed to stress the security aspects while ensuring compliance with the safety and performance requirements. The use cases will serve as demonstrators of the applicability of the SAFURE Framework to industry.

WP7: Exploitation
Guided by specifications and solutions in the technical WPs (WP2, WP3, WP4 and WP5), the use cases (WP1) and the demonstrators results (WP6), WP7 will identify exploitation directions and propose standards evolutions for the development of systems with better resource usage through better integration of mixed-critical applications.

WP8: Dissemination and communication
WP8 will assess the potential of SAFURE solutions to build on top of the proven concept, acting as a catalyst for an early adoption program diffusing the new practices, disseminating the proof-of-concept to the scientific, technical, and industrial communities, exploiting the communication channels and technology transfer facilities of the partners' networks.

WP9: Project-, risk-, and innovation-management
WP9 monitors and guides other WPs in order to ensure a successful project lifetime with respect to risk- and innovation management. The management WP shows dependencies to all other WPs as it coordinates and ensures that the tasks are in line with the project work plan in order to reach the common goal of SAFURE.

SAFURE

Contact:

Project Coordinator:
Dr. Klaus-Michael Koch
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55
E-Mail: coordination@safure.eu
Web: www.safure.eu

Technical Leader:
André Osterhues
ESCRYPT GmbH – Embedded Security
Leopoldstrasse 244
80807 Munich
Germany
Tel.: +49 234 43870 208
E-Mail: andre.osterhues@escrypt.com

Consortium:

The SAFURE consortium brings together a team of recognized partners to achieve the project's objectives.

12 SAFURE partners, consisting of 7 industrial manufacturers, 4 leading universities and research centres, and 1 SME, are spread over 6 European countries and comprise basic research and service design with applied research and end-user oriented service.

Project Partners:

1 **Technikon Forschungs- und Planungsgesellschaft mbH, Austria**

2 **Escrypt GmbH – Embedded Security, Germany**

3 **Magneti Marelli S.P.A., Italy**

4 **TTTech Computertechnik AG, Austria**

5 **Sysgo AG, Germany**

6 **Symtavision GmbH, Germany**

7 **Thales SA, France**

8 **Technische Universität Braunschweig, Germany**

9 **Barcelona Supercomputing Center – Centro Nacional De Supercomputacion, Spain**

10 **Scuola Superiore di Studi Universitari e di Prefezionamento Sant'Anna, Italy**

11 **Eidgenössische Technische Hochschule Zürich, Switzerland**

12 **Thales Communications & Security, France**