



Safety and Security for Embedded Software Systems



University of Peloponnese
Greece

German Aerospace Center
Germany



Project Coordination

Prof. Dr.-Ing. Dr. h. c. Jürgen Becker
Karlsruher Institut für Technologie (KIT)
Institut für Technik der Informationsverarbeitung (ITIV)
Engesserstr. 5
76131 Karlsruhe



XANDAR X-by-Construction Design framework for Engineering Autonomous & Distributed Real-time Embedded Software Systems. All rights reserved.
XANDAR has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 957210

www.xandar-project.eu

Key Facts

The next generation of networked embedded systems necessitates rapid prototyping and high performance while maintaining key qualities like trustworthiness and safety.

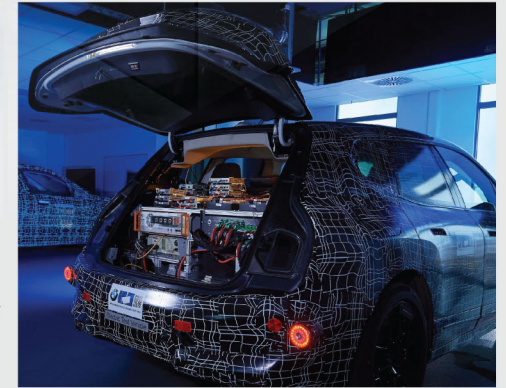
However, deployment of safety-critical embedded systems suffers from complex software toolchains and engineering processes.

Moreover, the current trend in autonomous systems relying on Machine Learning and AI applications in combination with fail-operational requirements renders the Verification and Validation of these new systems a challenging endeavor.



Objectives

- Provide holistic design methods and architectures that guarantee non-functional properties “by construction” throughout all phases of the software and system development lifecycle
- Improve development productivity and software quality with a reusable library of safety and security patterns, trusted HW/SW templates, and monitoring mechanisms
- Enable model-based design automation for trustworthy embedded software in critical environments
- Provide an interoperable, trustworthy and adaptive embedded HW/SW platform architecture that supports runtime platform health monitoring and self-healing capabilities
- Verification and validation of functional and non-functional requirements to show the effectiveness of the X-by-Construction paradigm
- Prototyping comprehensive avionics and automotive use-case application



Approach

XANDAR will deliver a **mature software toolchain** that fulfills the needs of the industry for rapid **prototyping of interoperable and autonomous embedded systems**.

Starting from a model-based system architecture, XANDAR will leverage **novel automatic model synthesis and software parallelization techniques** to achieve **specific non-functional requirements** setting the foundation for a novel **real-time, safety-, and security-by-Construction** (X-by-Construction) paradigm.

