The IoT4CPS Project

IoT-based cyber-physical systems (CPS) are becoming increasingly common in industrial environments. When connecting the digital with the real world, however, new challenges regarding to the safety and security arise. This is particularly important for vehicles and in industrial production processes.
To tackle these challenges new concepts are required, that not only ensure security for particular components, but that increase the reliability and trustworthiness of the overall product / system.

IoT4CPS addresses the safety, security, reliability and resilience of IoT-based CPS systems which become increasingly important in IoT application in critical environments (production, driving). To ensure these qualities in largely heterogeneous, distributed and dynamic environments, IoT4CPS starts with an analysis of the industrial needs in these domains and provides methods and tools to address them through the whole integration stack and over the system lifecycle.

Areas of Research

	Design & Methods	Verification and Analysis	IoT Lifecycle Management
Issues	• Shift towards **combined safety & security** approach • Need for **ready-to-use** solutions • Need for easily applicable **crypto** solutions	• Proliferation of IoT and autonomous driving will dictate **higher-secured** approaches • Broad adoption of IoT requires adaption of **on-line counter-measures** • **Scalable testing** systems to ensure security, safety and dependability	• **Effective access and usage** of information by the stakeholders in the product life cycle. • Standardized and secure open APIs for accessing and integrating **life cycle data** • Secure **configuration management** support throughout the life cycle
Innovation	• **combined safety & security** design approach • **resilient system architecture** patterns and concepts • hardware based **unclonable functions** to ensure trustworthiness of CPS • secure **light-weight public-key cryptography** • secure and **reliable key distribution**	• Automotive **Ethernet protection profile** • Functional and formal **IoT security checks** for devices and protocols • Machine learning-based **anomaly detection** • **Threat Intelligence framework** • **Detection of HW-based and side-channel attacks** on IoT systems • Automated, **model-based testing**	• **Life cycle data management** across corporate boundaries and across platform boundaries • Avoidance of vendor lock in effects by using open source technology and open APIs • IOT4CPS's life cycle management will specifically adapt to the requirements of **integrated hardware- and software configuration management**

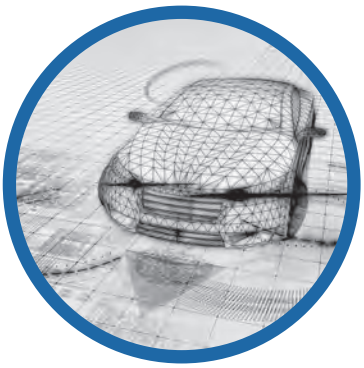
Based on concrete industrial requirements from the two use-cases connected vehicles and smart manufacturing, IoT4CPS will investigate tools and methods, addressing the design of secure IoT systems, the validation and runtime-analysis of IoT systems, and an integrated IoT lifecycle management.

IoT4CPS

Trustworthy IoT for CPS

The IoT4CPS Use-Cases

The IoT4CPS project develops guidelines, methods and tools for secure IoT-based applications in the areas of **Connected & Autonomous Vehicles and Industry 4.0**.



IoT for Connected Vehicles

The automation and interconnectivity of vehicles has become one of the international megatrends of automotive development. **IoT4CPS** provides a basis for the next generation of automated driving platform which integrates all three required characteristics: high-performance, (fail-operational) safety, and high security. **IoT4CPS** examines secure and reliable V2X and in-car connectivity solutions and provides example implementations of specific automated driving functions and components in automotive testing environments.

IoT for Smart Manufacturing

IoT4CPS aims to answer on secure Industry 4.0 demands by developing a design framework for IoT elements and a whole set of security tools and methods in order to improve system resilience. Lifecycle management aspects are addressed through conceptual models and the development of a prototype data management infrastructure. These results are integrated into an Industry 4.0 use-case that focus on three main aspects of a smart manufacturing environment, namely, secure connectivity, lifecycle traceability of components and systems and security by isolation.

Contact:
Dr. Mario Drobics (Project Coordinator)
AIT Austrian Institute of Technology
mario.drobics@ait.ac.at
More Information at https://iot4cps.at/

The IoT4CPS project is partially funded by the “ICT of the Future” Program of the FFG and the BMVIT.

Partners:

AIT Austrian Institute of Technology, Wien | Druck: druck.at | Grafik: transmitterdesign.com