Partners & Project Data

fortiss

STI

TTTech

Virtual Open Systems

T.E.I. of Crete

ENERGICA

Fondazione Centro San Raffaele

actility

Third party

RIA
TAPPS Goals

Architecture designed for open Cyber-Physical Systems
enabling new services and customization features

Open: Extensible at run-time
by instantly adding or updating functionality on demand
through apps (also provided by 3rd parties) like in the mobile domain

Pros:
- enables products to keep pace with user expectations and latest technologies

Cons:
- use of apps imply safety, privacy and security risks

www.tapps-project.eu
TAPPS Approach:
Multiple Layers of Security
TAPPS Approach: Multiple Layers of Security

1. Verified Apps
   • to ensure correct and secure behavior
   • by model-checking, model-based development, trusted toolchain

2. Tailored Execution Environments (EEs)
   • to ensure spatial & temporal isolation of apps
   • through virtualization and a safety integration layer

3. Fine-grained access control to resources of the CPS devices
   • to ensure safety and privacy
   • by communication with critical interfaces

4. Hardware equipped with security mechanisms
   • to ensure real time execution of critical apps
   • by ARM TrustZone technology, a tailored network on chip

5. Trusted network
   • to ensure secure and safe transfer of mixed-critical content
   • by virtual end-to-end channels and firewalls
Key Issues of the TAPPS Architecture

End-to-end solution

Application Model ➔ Apps Application Container ➔ App Market Place

Execution Environments

Rich EE ➔ Trusted EE ➔ Critical EE

Trusted HW & Networks

Normal World ➔ Secure World

sCAN ➔ Deterministic Ethernet
Validation
Automotive Domain

TAPPSS trusted apps platform will enable the possibility to add new features into produced vehicles

- check trip capability based on traffic conditions and battery status
- activate optional traction control module
- braking adjustment depending on environment conditions

Electric Motorcycles
Validation Healthcare Domain

TAPPS trusted apps platform will guarantee a secure therapy preparation and administration

- safe drug management through patient ID check and automatic drawers
- patient data management with access to electronic health records (EHR)
- monitoring of vital signs

Smart Trolley
Main Achievements so far

- Architecture for open CPS including three execution environments (EEs) and a Safety Integration Layer
- Tool Chain for trusted Apps with symbolic model-checking of IEC 61499 sub-applications
- Market place with roles for users, distributors and OEMs
- Running real-time OS in ARM TrustZone’s secure world
- Efficient virtualization for EEs and secure inter-EE communication
- Secure real-time networking with deterministic Ethernet and secure CAN bus

Implemented and validated in the two use cases: drug administration trolley and trusted dashboard for the electronic motorbike

Presentations of TAPPS results in 12 events, 6 main publications, and organization of the workshops Future Therapy @Politecnico di Milano and Cyber Security for Cyber Physical Systems @Modena
TAPPS Planned Outcomes

Open platform for CPS with

• Multiple layers of security
• Execution environments with different protection level
• Integrated security, safety, RT over all layers
• From HW, NW, virtualization to SW
• End-to-end security, boot, installation, operation
• Adaptation under real-time

Validation in several domains: Automotive, Healthcare, Industry4.0

Next TAPPS workshop at JRC, May 2017