AUTOMOTIVE CYBERSECURITY

This competency focuses on cybersecurity testing and hardening of embedded systems in vehicles and critical infrastructure. It applies expertise in automotive IT architectures, communication protocols, and embedded platforms to perform vulnerability analysis and secure-system design. The activity supports partners in strengthening cyber resilience for next-generation mobility, defence, and industrial platforms, aligned with dual-use and regulatory requirements.

ACHIEVEMENTS

- Cybersecurity risk assessments and threat modelling for connected and autonomous vehicle systems.
- Development and validation of secure in-vehicle communication (CAN, LIN, Ethernet-based).
- Research aligned with ISO/SAE 21434 and UNECE WP.29 vehicle cybersecurity standards.
- Design and simulation of attack scenarios and penetration-testing frameworks for ECUs.

INFRASTRUCTURE

- Embedded cybersecurity testing environments.
- Automotive protocol simulators (CAN, LIN, V2V).
- 5G vulnerability testing tools.
- Cyber range support for embedded and automotive scenarios.
- Collaboration framework with national security and defence stakeholders.

REFERENCES

- Embedded software security validation with Bosch Engineering Center Hungary.
- Automotive cybersecurity testing with Continental Automotive Hungary.
- Secure electric bus control systems engagement with Ikarus Electric.
- Cybersecurity co-design insights applied with Magnus Aircraft Zrt..

Initium Venture Labs Zrt.
Email: initium@uni-obuda.hu
Web: www.initium.uni-obuda.hu
www.linkedin.com/company/initium-venture-labs
Tel: +36302128861