

# Dependable Vehicle Security

Enabling Predictable and **Secure Mobility**

With funding from the:



## Comprehensive **Security Platform**

Within this project we implemented a security platform examining various aspects:

- Protection of **intra-vehicle** and **external communication** [1, 3].
- **PKI integration (INCYDE)** for automotive ecosystems.
- Lightweight **DDS security** via a central **Security Platform** and adoption of the DDS Security Standard.
- A **Security Gateway** enabling **secure V2X**.

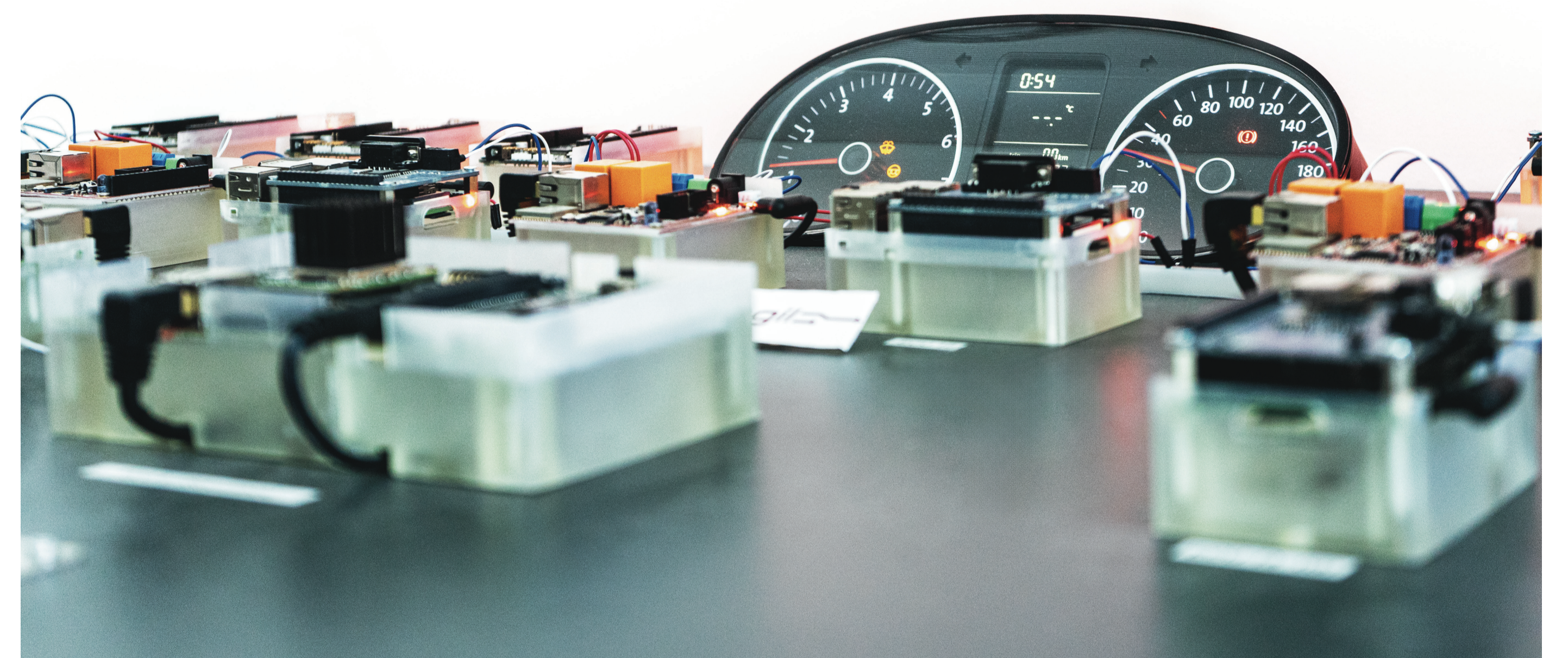


## Universal Vehicular Security **Demonstrator**

The demonstrator simulates modern heterogeneous vehicle architectures, enabling:

- **Intra-vehicle traffic** between resource-constrained ECUs and high-performance platforms.
- Supports Legacy (e.g. CAN) and **automotive Ethernet** communication via **service-oriented protocols**
- Simulation environment for **security solutions** and **demonstration of cyberattacks** within the network.

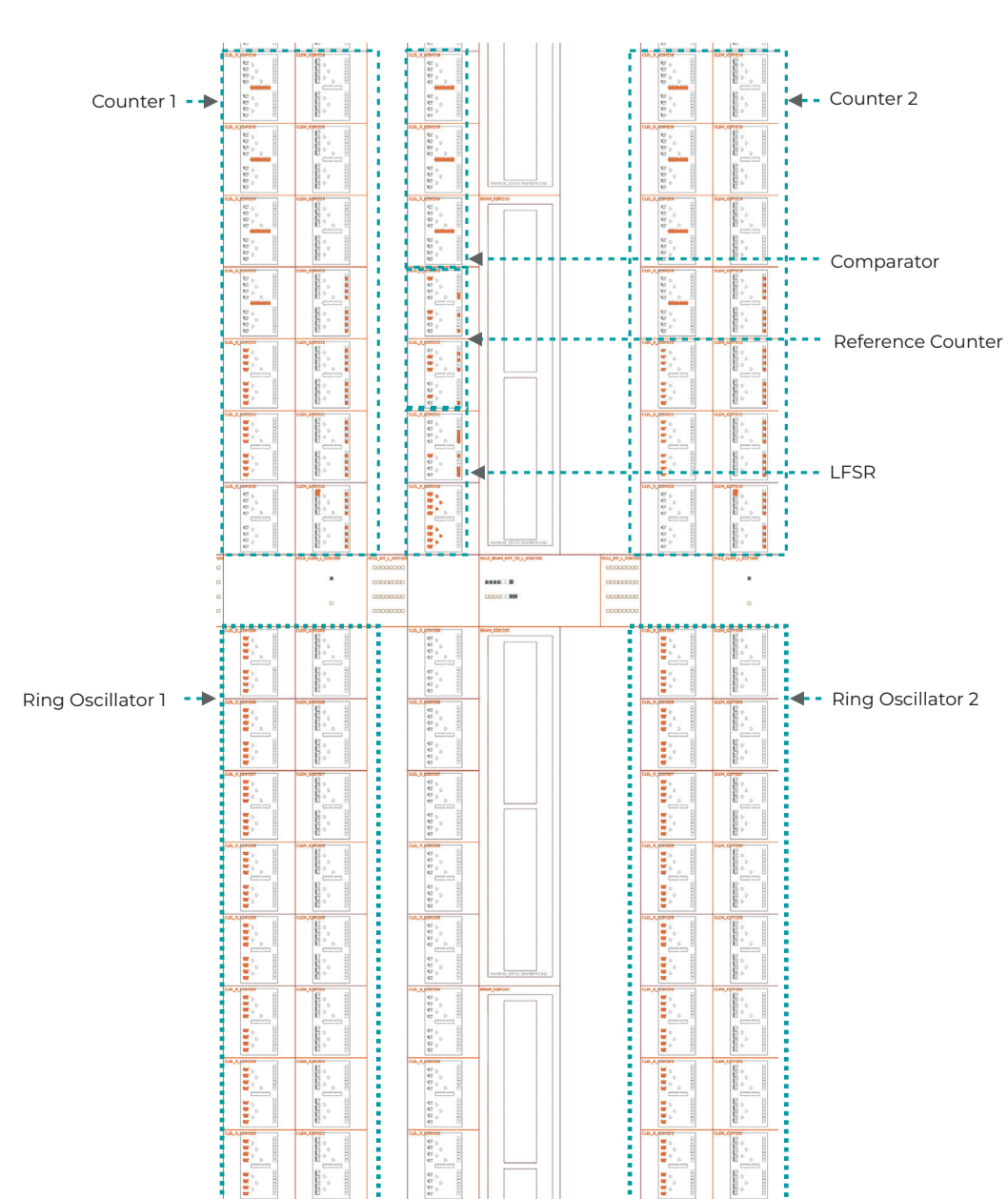
Our demonstration showcases attacks and mitigations like inception and replay, enabling the injection of false velocity data visualized on the speedometer.



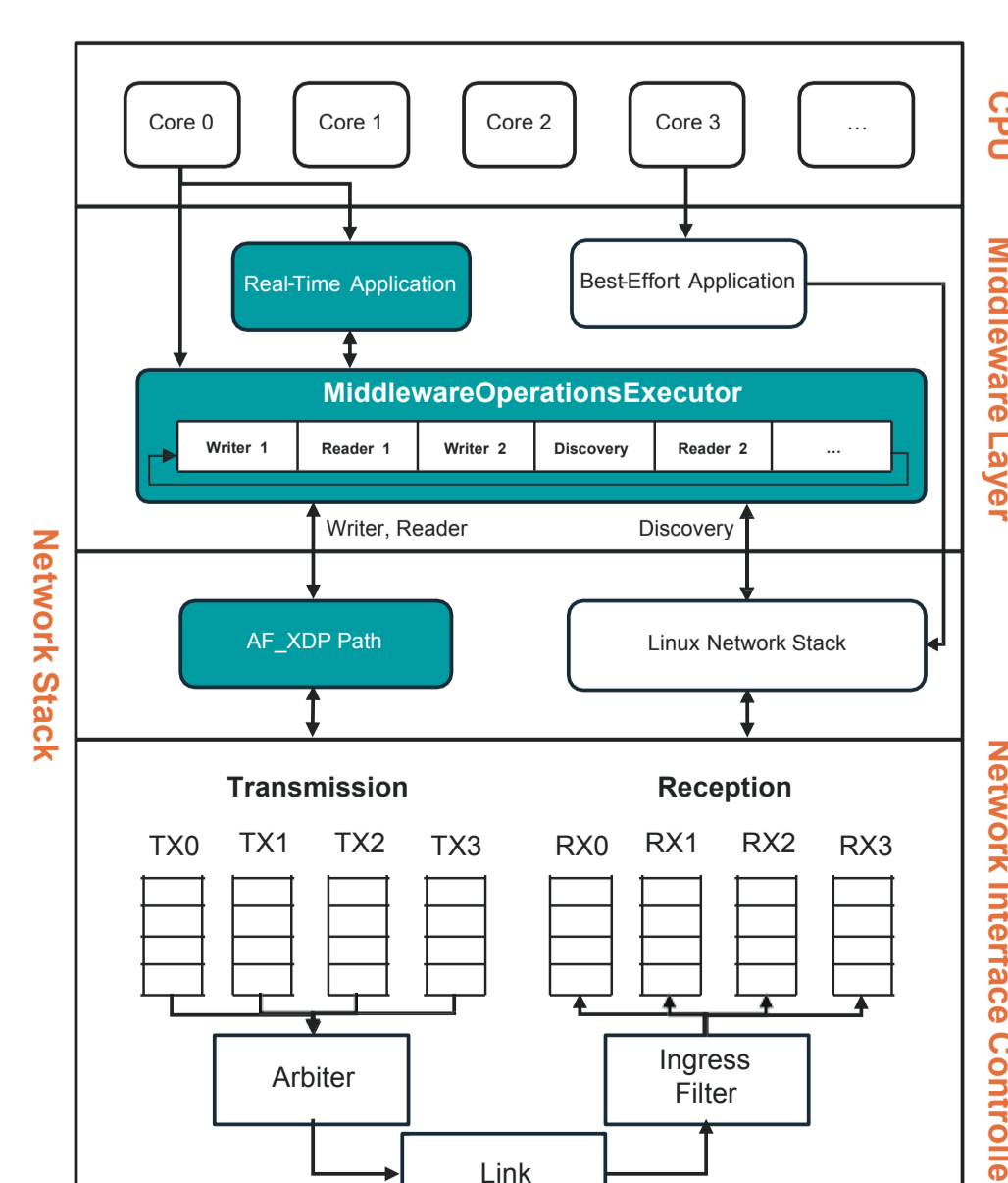
## Security meets **Timing Determinism**

We explored how to combine security with real-time guarantees essential for automated driving—without compromising timing determinism:

- Prioritization and acceleration of DDS traffic using a **dynamic prioritization TSN time-aware shaper** on MPSoCs [4].
- Security on FPGAs using a **ring-oscillator-based key derivation** and **ciphers implemented in hardware** [2, 4].
- Kernel bypass via AF\_XDP for time-critical traffic [5].



Ring oscillator hardware design allowing the derivation of secure cryptographic keys.



AF\_XDP kernel bypass architecture.

## Transferring **Research to Industry**

**EXIST Research Transfer** in cooperation with RWTH Aachen.

**Goal:** Founding a company to commercialize secure and certifiable open-source middleware.

The DDS library embeddedRTPS has already been extensively developed into the platform managedDDS.



## Publications

- [1] D. Püllen, F. Klement, A. Vinel, and S. Katzenbeisser, "Ensuring Trustworthy Automated Road Vehicles: A Software Integrity Validation Approach," Proceedings of the 2023 IEEE International Automated Vehicle Validation Conference (IAVVC), 2023.
- [2] F. Frank, M. Schmid, F. Klement, P. Palani, A. Weber, E. B. Kavun, W. Xiong, T. Arul, and S. Katzenbeisser, "Secure Data-Binding in FPGA-based Hardware Architectures Utilizing PUFs," Proceedings of the 19th ACM Asia Conference on Computer and Communications Security, 2024.
- [3] Y. Qendah, D. Püllen, and S. Katzenbeisser, "Real-Time Risk Assessment of Security Incidents for Autonomous Vehicles," Proc. of the 2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall), 2024.
- [4] F. Frank, D. Püllen, A. Kampmann, and S. Katzenbeisser, "Towards Deterministic DDS Communication for Secure Service-Oriented Software-Defined Vehicles," Proceedings of the 20th International Conference on Availability, Reliability and Security (ARES), 2025. (Accepted for presentation)
- [5] L. Meszlényi, J. Kahle, D. Püllen, S. Kowalewski, S. Katzenbeisser, and A. Kampmann, "Towards Timing Isolation for Mixed-Criticality Communication in Software-Defined Vehicles," Proceedings of the 2025 IEEE International Automated Vehicle Validation Conference (IAVVC), IEEE, 2025. (Accepted for presentation)