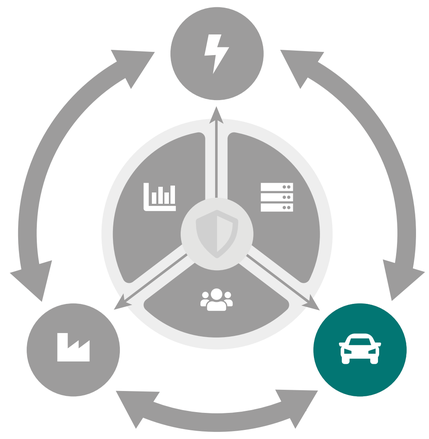
Karlsruhe Institute of Technology

P1T3

Design & Development Methods for Secure Automotive Software Systems

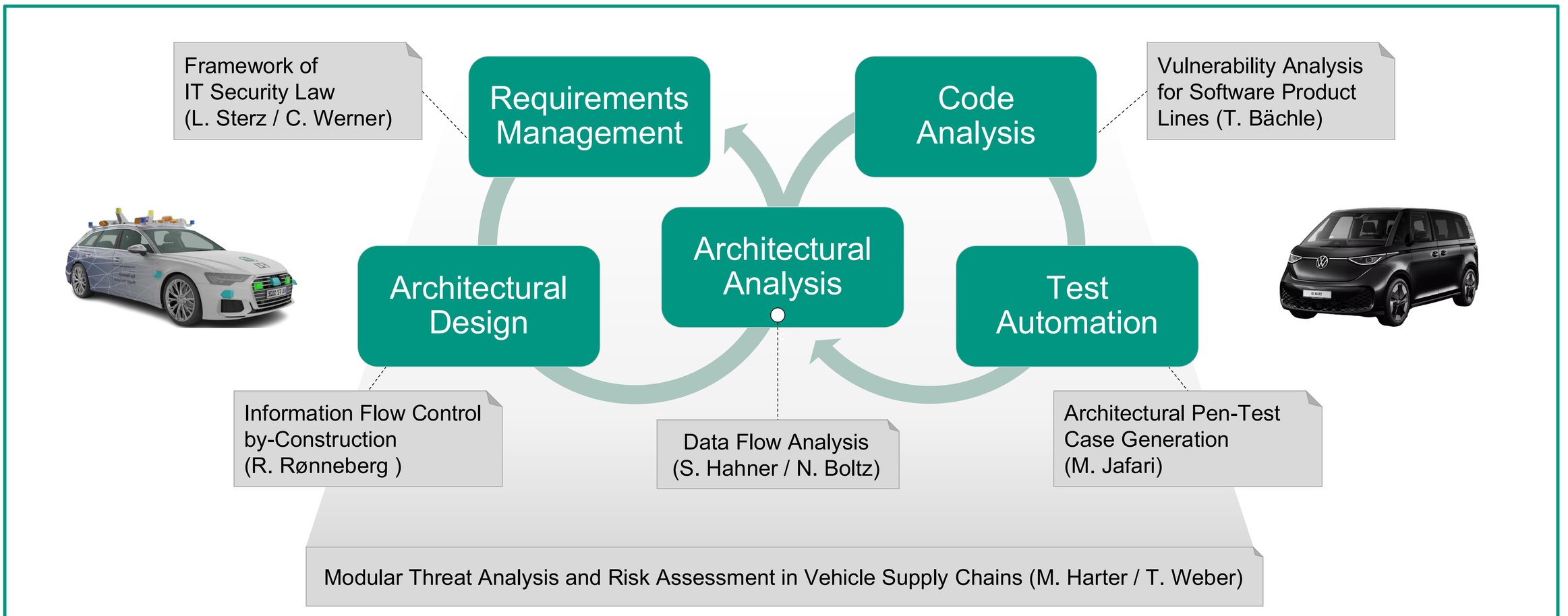


I. Schaefer, T. Bächle, M. Harter, R. Rønneberg, R. Reussner, N. Boltz, C. Gerking,
S. Hahner, M. Jafari Sarvejahani, T. Weber, O. Raabe, L. Sterz, C. Werner
(Dependability, Legal Informatics, Mobility Systems Security)

Motivation

- Automotive software engineering provides dedicated development methods for mobility systems.
- Methods for secure software gain in importance due to larger attack surface and legal obligations.
- Methods help to detect vulnerabilities or ensure their prevention from the ground up.
- Methods must cover the whole development lifecycle (including early phases: security by design)
- Methods need to address domain-specific characteristics of mobility systems.
- The legal framework must be considered as a basis for decision-making during development.

Research Activities and Results



Publications

- Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen. In: Recht der Datenverarbeitung 2022, 2023.
- Quantitative Information Flow Control by Construction for Component-based Systems. In: ECSA-C 2023.
- An Extensible Framework for Architecture-based Data Flow Analysis for Information Security. In: ECSA 2023.
- Towards Architectural Pen Test Case Generation and Attack Surface Analysis. In: ICSA-C 2025 (accepted).
- Model Everything but with Intellectual Property Protection. In: MODELS 2024.

links to:

Methods for Privacy-Preserving and Fair Ticketing for Europe-Scale Mobility-as-a-Service

Analysis of EVerest Modular Framework for EV-Charging

KASTEL