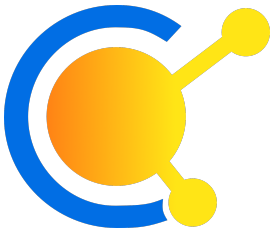

Kurzfassung zum Teilvorhaben

Mannheim CeCaS – Central Car Server: Supercomputing für Automotive

Teilvorhaben Universität zu Lübeck

Andrija Neskovic
Mladen Berekovic

November 2025

Projektname: Mannheim CeCaS – Central Car Server: Supercomputing für Automotive
Kurzbeschreibung: Automotive Supercomputing: Leichtgewichtige Memory Protection Unit, vertrauenswürdiger KI-Beschleuniger und virtuelle SoCEntwicklungsplattform
Verbundpartner: Universität zu Lübeck, Institut für Technische Informatik (ITI)

Projektleitung: Prof. Dr.-Ing. Mladen Berekovic
Projektlaufzeit: 01.12.2022 – 30.11.2025

Förderkennzeichen: 16ME0819

Einleitung

Das Mannheim-CeCaS-Projekt (Central Car Server – Supercomputing für Automotive) ist ein BMBF-gefördertes Verbundprojekt mit dem Ziel, die Hardware-Grundlagen für zukünftige zentrale Fahrzeugrechner zu schaffen. Das UzL-Teilvorhaben adressiert dabei die gleichzeitige Realisierung von **Sicherheit** (Speicherschutz, Seitenkanalresistenz) und **Höchstleistung** (KI-Inferenz, Sensordatenverarbeitung) unter strikten Automotive-Ressourcen-Budgets. Es umfasst drei aufeinander aufbauende Arbeitsbereiche: leichtgewichtige Memory Protection Unit (AP3), vertrauenswürdiger KI-Beschleuniger (AP4) und virtuelle SoC-Entwicklungsplattform für Pre-Silizium-Validierung (AP7).

Memory Protection Unit (MPU)

Bestehende Speicherschutzlösungen sind für HPC-Automotive entweder zu ressourcenintensiv oder nicht ausreichend gegen Seitenkanalangriffe gehärtet. Im Rahmen von AP3 wurde eine dedizierte Hardware-Einheit entwickelt, die zwischen CPU-L2-Cache und DRAM sitzt und auf Basis des Leichtgewichts-Algorithmus ASCON alle Speichertransfers in Echtzeit chiffriert. Dies ermöglicht sichere Speicherpartitionierung bei minimalem Overhead. Die vollständige Integration in eine RISC-V-CPU (RocketCore) wurde auf einem AMD/Xilinx ZCU104 FPGA verifikativ demonstriert: Hardware-Mehraufwand nur +0,32% LUT und +0,09% FF – alle übrigen Ressourcen unverändert. Sicherheit und Performance-Budgets schließen sich damit nicht aus.

Vertrauenswürdiger KI-Beschleuniger

Bisherige KI-Hardware adressiert Zuverlässigkeit oder Sicherheit – nicht beides. AP4 entwickelt eine Entwurfsraum-Explorations-Methodik (DSE), die Beschleuniger automatisiert für ganze Familien von KI-Modellen (ONNX-Format) optimiert, sowie systematische Fehlerinjektionen (Bit-Flips, Stuck-at-Fehler), die Hardware-Ausfallmodi vor Fertigung auf FPGA simulieren. Kernergebnisse: (1) **Compatibility Ratio** – neue Metrik zur familienweiten Beschleuniger-Bewertung; (2) **NAIL** – vom ITI entwickeltes, im Rahmen von CeCaS für KI-Beschleuniger weiterentwickeltes Open-Source-Fehlerinjektions-Framework. Ein vollständiges FPGA-System (RISC-V-CPU + KI-Beschleuniger + Coprozessor) wurde erprobt; Ergebnis: Kontrollpfad-Fehler verursachen verborgene, kritische KI-Fehlklassifikationen.

Virtuelle SoC-Entwicklungsplattform

Fehler in SoC-Designs werden heute meist erst nach der teuren Fertigung erkannt. AP7 entwickelt eine SystemC/TLM-basierte virtuelle Plattform, die ein vollständiges SoC – CPU, MPU, KI-Beschleuniger, Speicher, Busse – bereits vor Siliziumeinsatz simuliert. Damit sind HW/SW-Koentwicklung, Safety/Security-Analysen und Entwurfsraumexploration in frühen Designphasen möglich. Das Open-Source-Werkzeug SCA-WAL ermöglicht zudem Power-Seitenkanalanalysen auf RTL-Ebene. Der funktionsfähige Demonstrator integriert Komponenten aus AP3 und AP4 und wird bereits als Entwicklungsplattform am ITI und in Folgeprojekten eingesetzt.

Ergebnisse und Verwertung

Drei peer-reviewed Publikationen verbreiten die Projektergebnisse: SCA-WAL (IEEE Embedded Systems Letters, 2025), NAIL (Euromicro DSD, 2025), SystemC/TLM Survey (ACM TODAES, 2025). Alle Quellcodes sind öffentlich zugänglich.

SCA-WAL: `https://github.com/iti-luebeck/sca-wal`,

NAIL: `https://gitlab.iti.uni-luebeck.de/pubs/nail`.

Darüber hinaus wurde im Rahmen des Projekts ein Multi-Partner-Project-Paper bei der *Design, Automation and Test in Europe Conference (DATE) 2026* eingereicht und zur Veröffentlichung angenommen. Während der Projektlaufzeit wurden am Institut für Technische Informatik außerdem **3 Masterarbeiten** und **3 Bachelorarbeiten** zu projektbezogenen Themen herausgegeben. Die MPU-IP kann für zukünftige SoC-Designs benutzt werden; DSE-Methodik und NAIL sind auf andere KI-Beschleuniger und Domains direkt übertragbar. Mittelfristig fließen die Ergebnisse in die Lehre am ITI ein und bilden die Basis für Folgeprojekte (Horizon Europe, KDT JU) sowie ein mögliches Ausgründungsvorhaben. Langfristig trägt das Teilvorhaben zur technologischen Souveränität Deutschlands im Bereich sicherer KI-Systeme für automatisierte Fahrzeuge bei.

Fazit

Das UzL-Teilvorhaben demonstriert erfolgreich eine neuartige Kombination: **Sicherheit** (kryptografische MPU mit minimalem Overhead), **Leistung** (optimierter KI-Beschleuniger für Fahrzeug-KI) und **Validierbarkeit** (virtuelle Plattform für Pre-Silizium-Bewertung). Alle Meilensteine wurden erreicht und durch FPGA-Demonstratoren sowie Publikationen belegt. Mit diesen Ergebnissen trägt die Universität zu Lübeck wesentlich zur technologischen Souveränität Deutschlands im Autonomous Driving bei.