Design Automation for Automotive Cyber-Physical Systems

PI: Samarjit Chakraborty (UNC) **Co-PIs: James Anderson (UNC), Parasara Sridhar Duggirala (UNC), Prachi Joshi (GM)**

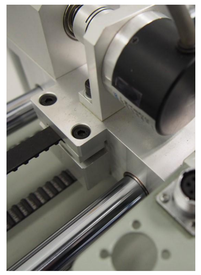
Graduate Students: Bineet Ghosh, Clara Hobbs, Shengjie Xu

https://tarheels.live/designautocps/

Motivation

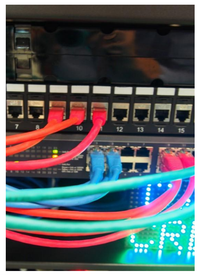
- Methods for incorporating implementation artifacts like delays, numerical errors, and side-effects introduced by software have been studied in the control technology literature (e.g., starting with Computer-Controlled Systems by Åström and Wittenmark)
- But modern automotive electrical/electronic (E/E) architectures have hundreds of electronic control units (ECUs) connected by a complex communication architecture with buses like CAN, FlexRay, LIN and automotive Ethernet
- Such highly distributed and heterogeneous architectures offer *many* different controller implementation options

Variety of Control Software

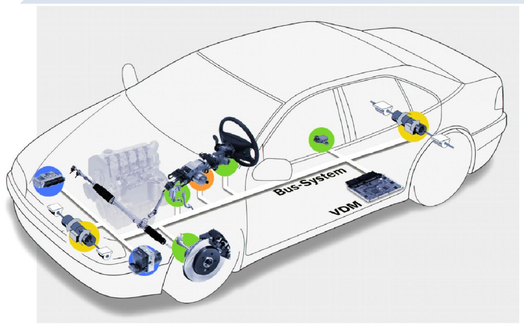


Distributed E/E Architecture

Different Communication Buses



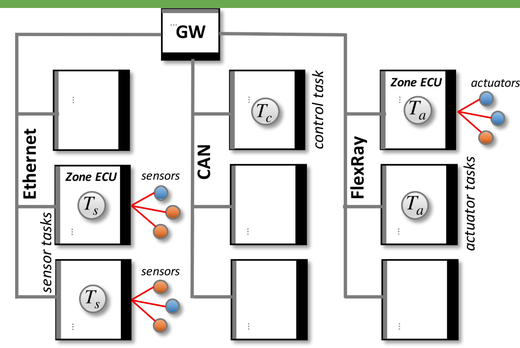
Modern Automotive Hardware/Software Architectures



Driving Problem

Basic problem: How to implement feedback controllers on distributed embedded systems?

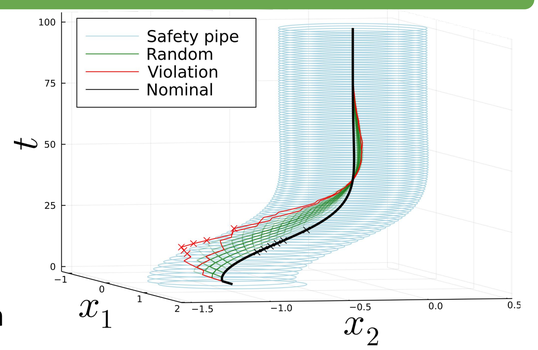
- Modern cars are equipped with a variety of sensors such as cameras, radars and lidars, which involve computationally expensive processing
- There are many ways in which such processing may be organized or structured, each associated with different delays or timing behaviors
- How can we automatically explore these different implementation options and the associated modifications to the controllers? What kind of tool support is necessary to support this design flow and control/architecture co-design?



Heterogeneous Automotive Architecture

Recent Results

- Scalable safety analysis techniques for control software under timing uncertainties
- Tool integration for automated controller synthesis on FlexRay-based distributed embedded systems
- Using statistical hypothesis testing to check safety properties in controller implementations in the presence of timing uncertainties
- Scheduling controllers with weakly-hard constraints to meet plant safety properties
- Using combinations of model checking and fuzzing for test case generation
- Extension of dynamics-aware schedule synthesis to the industrial automation domain
- ML techniques for intrusion detection in CAN-based automotive architectures



Safety Analysis Under Timing Uncertainties

Highlights

- Clara Hobbs completed a summer internship at GM in 2022
- Clara Hobbs and Shengjie Xu offered summer internships by GM for Summer 2023
- New research contract from General Motors to study timing analysis of service-oriented automotive architectures
- RTCSA 2022 paper nominated for Best Paper Award
- Bineet Ghosh received Best Presentation Award at ACM SIGBED SRC 2022
- Bineet Ghosh selected for 2022 SRI Summer School on Formal Techniques
- Bineet Ghosh received the Chateaubriand Fellowship 2021
- Academic collaboration with TU Munich, LORIA (France), UT Austin, University of Verona, Tata Innovation Labs Pune
- Broadening participation: mentoring undergraduate students

Selected Recent Publications

- Xu et al., "Safety-aware Flexible Schedule Synthesis for Cyber-Physical Systems using Weakly-Hard Constraints," ASP-DAC 2023
- Hobbs et al. "Safety Analysis of Embedded Controllers under Implementation Platform Timing Uncertainties," EMSOFT 2022
- Ghosh et al., "Statistical Hypothesis Testing of Controller Implementations Under Timing Uncertainties," RTCSA 2022
- Yeolekar et al., "Checking Scheduling-induced Violations of Control Safety Properties," ATVA 2022
- Balszun et al., "Process Dynamics-Aware Flexible Manufacturing for Industry 4.0," CASE 2022
- Balszun et al., "Exploiting Process Dynamics in Multi-Stage Schedule Optimization for Flexible Manufacturing," ETFA 2022

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Award ID#: 2038960