CAREER: SOISTICe: Software Synthesis with Timing Contracts for Cyber-Physical Systems

Qi Zhu (Northwestern)

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting

Timing Challenges in Software Synthesis

- Timing behavior affects functionality and design metrics.
- Synthesis of CPS software faces timing-related challenges:
  - ✧ Diversity of timing requirements
  - ✧ Complexity of timing analysis
  - ✧ Uncertainty of timing behavior
- Timing constraints are often set in an ad-hoc fashion.

SOISTICe Framework

Theme A: Co-design & Refinement with Timing Contracts

A1. Multi-metric Co-design with Horizontal Timing Contracts

- Explore timing constraints while trading off design metrics.

A2. Hierarchical Refinement with Vertical Timing Contracts

- Assign timing budget for lower-level components for design refinement across system hierarchy.

Theme B: Timing-centric Task Generation and Mapping

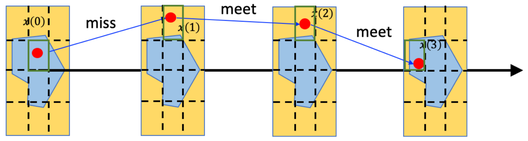
- Develop interactive task synthesis approaches.
- Task synthesis of heterogeneous functional models.

Theme C: Co-simulation with Contracts

- Timing contracts monitoring during co-simulation.
- Integration of simulation and analytical algorithms.

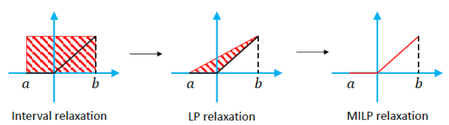
- CPS Software Synthesis and Verification under Disturbances

Safety Verification under Weakly-hard Constraints



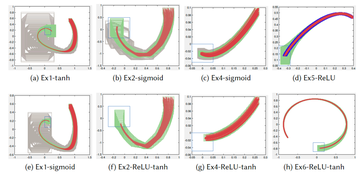
Verify control safety under bounded timing and functional disturbances. Tool **SAW** released (CAV20, ICCAD20, HSCC19).

Adversarial Robustness of Neural Networks



Quantify local robustness of neural networks via output range analysis. Tool **LayR** to be released (EMSOFT20).

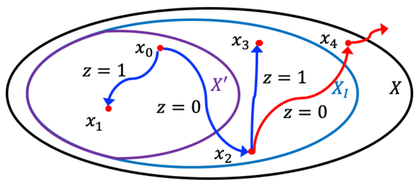
Safety Verification of Neural Network Controlled System

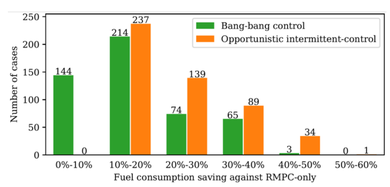


Tool **ReachNN*** released (ATVA20, EMSOFT19).

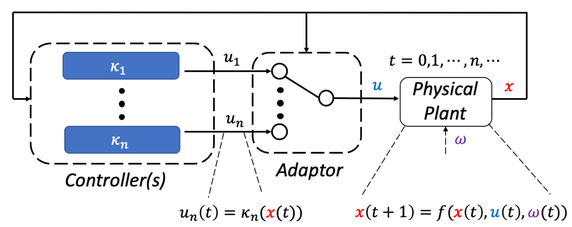
Verify safety of NNCS via reachability analysis leveraging Bernstein polynomial approximation.

- Safety-assured Design and Adaptation for LE-CPSs



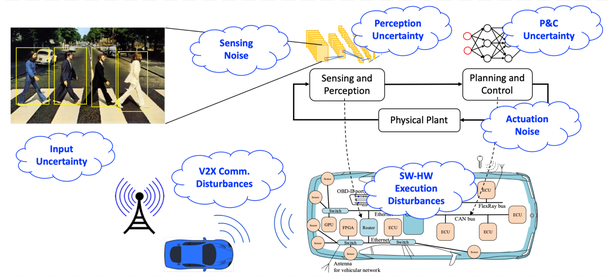


Opportunistically skip control to save energy with safety assurance. Derive invariant sets for safety assurance. Use RL for energy saving. ACC case study. (DAC20)



Switch among multiple controllers (including neural network based) to address adaptation needs. (ICCAD20 best paper candidate)

- Application in Connected and Autonomous Vehicles
  - Address uncertainties and disturbances throughout the autonomous driving pipeline. (ICCAD20, ASPDAC21, DATE21)
  - Quantify adversarial robustness in perception neural network. (EMSOFT20)
  - Verify safety of planning and control module. (EMSOFT19, ATVA20)
  - Address software/hardware execution disturbances. (HSCC19, DAC20, ICCAD20)
  - Address communication disturbances in connected vehicle applications. (TCPS19, RAID19, Autosec21, IV21)



Scientific Impacts

- Explore timing constraints to produce correct, efficient, and predictable CPS software.
- Develop new methodologies for timing contracts definition and exploration, and novel algorithms for timing-centric task generation and mapping.
- Target automotive and transportation systems as primary case studies.

Broader Impacts and Education

- Enable fundamental advances in design automation methods and tools for cyber-physical systems.
- Establish close industry collaborations.
- Outreach to K-12 schools with Lego Mindstorm.
- Extend undergrad embedded systems course and develop new graduate course on CPS.
- Write a textbook in collaboration with industry.

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: 1834701