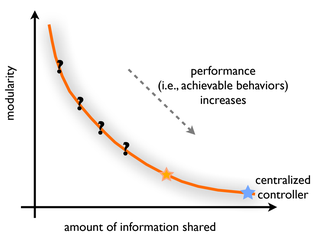
CAREER: A Compositional Approach to Modular Cyber-Physical Control System Design

Necmiye Ozay, Department of EECS, University of Michigan

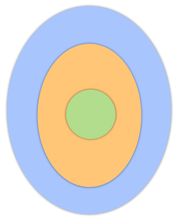
Overall Objective:

- Modularity to manage complexity during both design- and life-cycles for CPSs
- At the discrete-level: computing local assume-guarantee specifications per subsystem from a global specification
- At the continuous-level: decomposing a system into possibly uncertain subsystems
- Developing correct-by-construction control synthesis techniques that can handle uncertainty and partial information
- Understanding structural system properties that facilitate composition and decomposition



★ decentralized control where local controllers use models of all other subsystems and all other local controllers

? compositional control where local controllers only use some assumptions summarizing the behavior of other subsystems



Project Start Date: January 2016

Industry Interactions:

Toyota Research Institute, Ford, Mathworks

Participants:

- Graduate Students

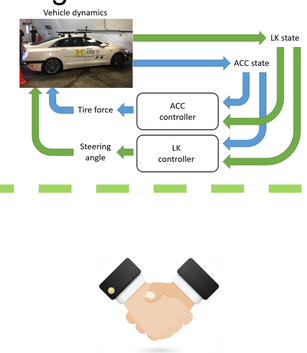
Yunus E. Sahin, Petter Nilsson, Kwesi Rutledge

- Undergraduate Students

Stanley W. Smith, Andrew Wagenmaker, Ryan Wunderly

Results-to-date:

- Compositional Invariant Synthesis via Contracts
  - Main idea: separately synthesize controllers for interdependent subsystems with guarantees on composition
  - Interdependence quantification via convex over-approximation
  - Ability to handle nonlinear terms in uncertain system dynamics exploiting mono-tonicity or convexity

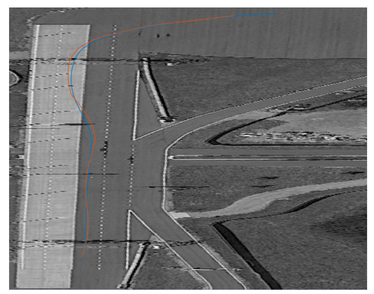


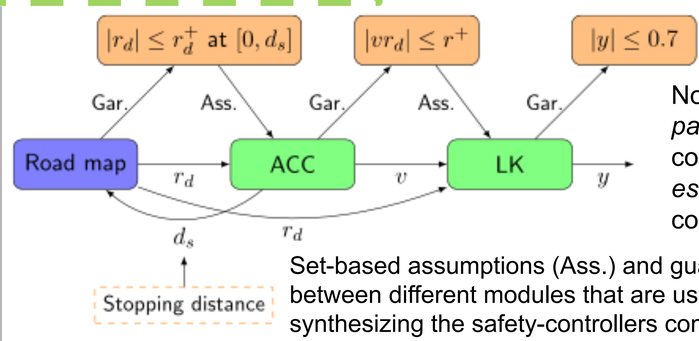
LK: $\frac{d}{dt}\begin{bmatrix} y \\ \nu \\ \Delta\Psi \\ r \end{bmatrix} = \left(A_{LK,0} + A_{LK,1}\frac{1}{v} + A_{LK,2}v\right)\cdot\begin{bmatrix} y \\ \nu \\ \Delta\Psi \\ r \end{bmatrix} + B_{LK}\delta_f + E_{LK}v\, r_d$

ACC: $\frac{d}{dt}\begin{bmatrix} v \\ h \end{bmatrix} = A_{ACC}(\nu r)\begin{bmatrix} v \\ h \end{bmatrix}$

  - Two methods for computing separable invariant sets:
    - Iterative decoupled computation
    - LMI-based centralized computation
  - Handles input and state constraints, external disturbances
  - Takes advantage of disturbances that can be measured at run-time
  - Handles *arbitrary information sharing patterns* (e.g., which subsystem has access to which other subsystems' states)
  - Allows trading off between online vs offline computation

- Correct-by-construction Controllers in Mcity
  - Setup for quick deployment
  - Synthesized code is automatically integrated to Simulink (enables C code generation)
  - Collaboration with Mathworks to build a bridge: same code runs with high fidelity simulators (e.g., Carsim) and on the real car with Polysync as middleware





Novel *parameterized* contracts and *estimation* contracts

Set-based assumptions (Ass.) and guarantees (Gar.) between different modules that are used in synthesizing the safety-controllers compositionally.

UNIVERSITY OF MICHIGAN

NSF