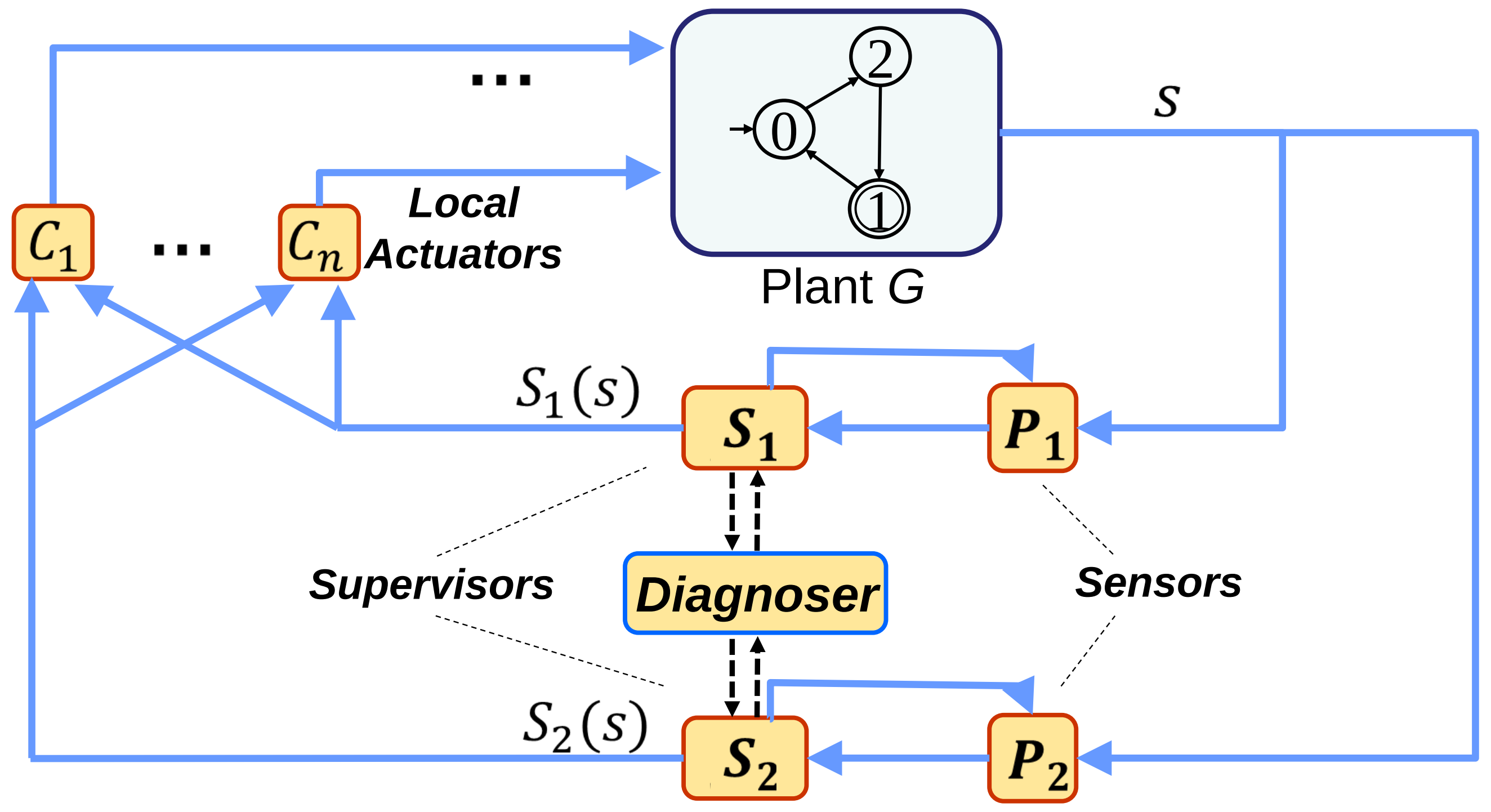
CPS – Breakthrough: Development of Novel Architectures for Control and Diagnosis of Safety-Critical Complex Cyber-Physical Systems

Stéphane Lafortune and Necmiye Ozay   Department of EECS, University of Michigan

Overall Objective:

- Scalability of formal methods for synthesis of provably-correct controllers
- Development of abstraction techniques that lift CPS design problem to synthesis problem on discrete state system
- Combination of control and fault diagnosis to ensure resilience and adaptivity
- Consideration of the distributed features of the system at synthesis step and at implementation step



Project Start Date: January 2015

Participants:

- Graduate Students

Xiang Yin, Yun Jae Cho, Yunus Sahin

- Undergraduate Students

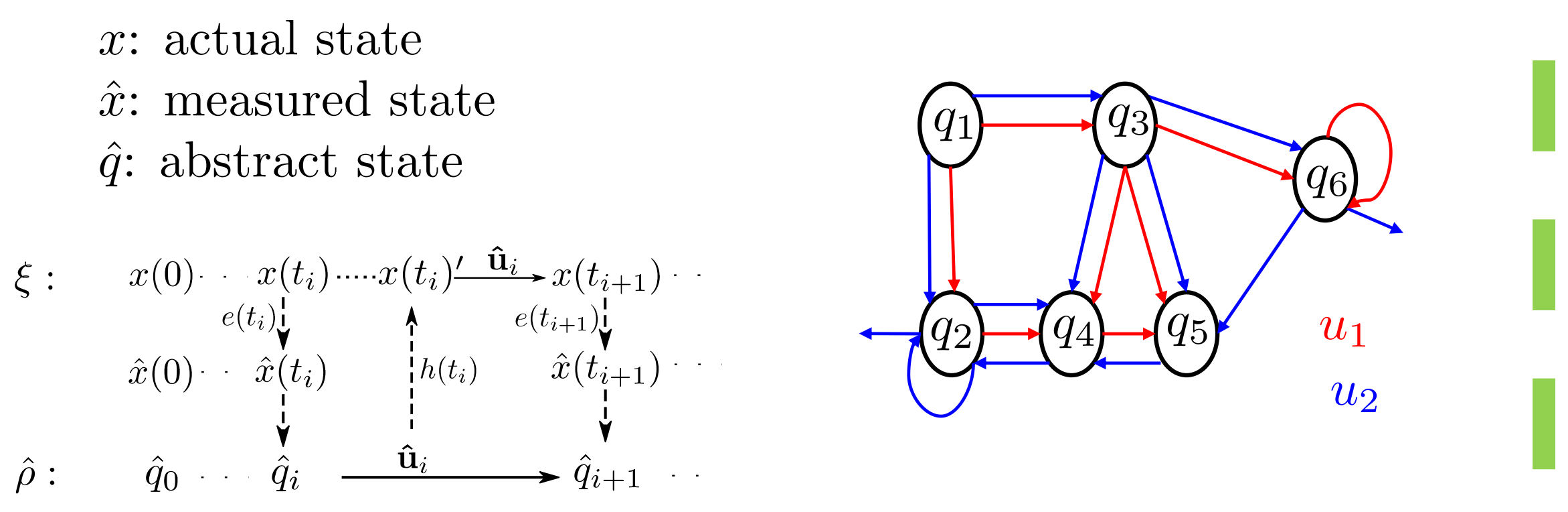
Stanley Smith, Maxwell Morrison, Mercedes Modet Benjumea

Industrial Collaborators:

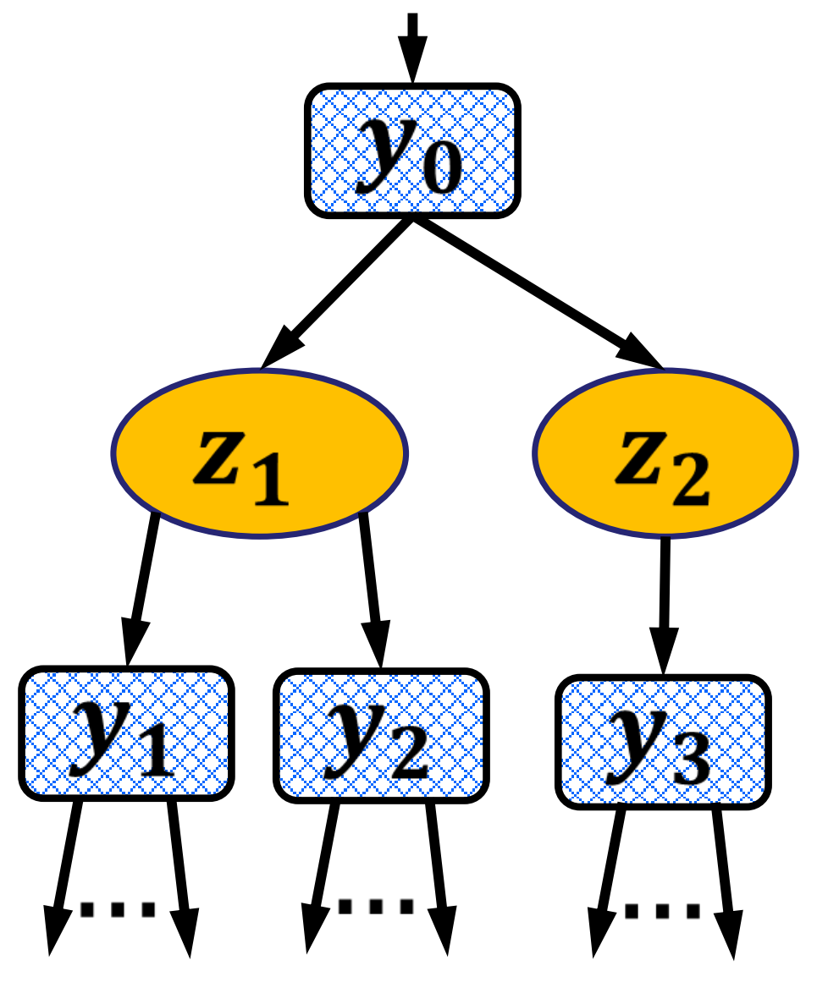
- UTC Aerospace Systems (UTAS)
- Ford Motor Company

Results-to-date:

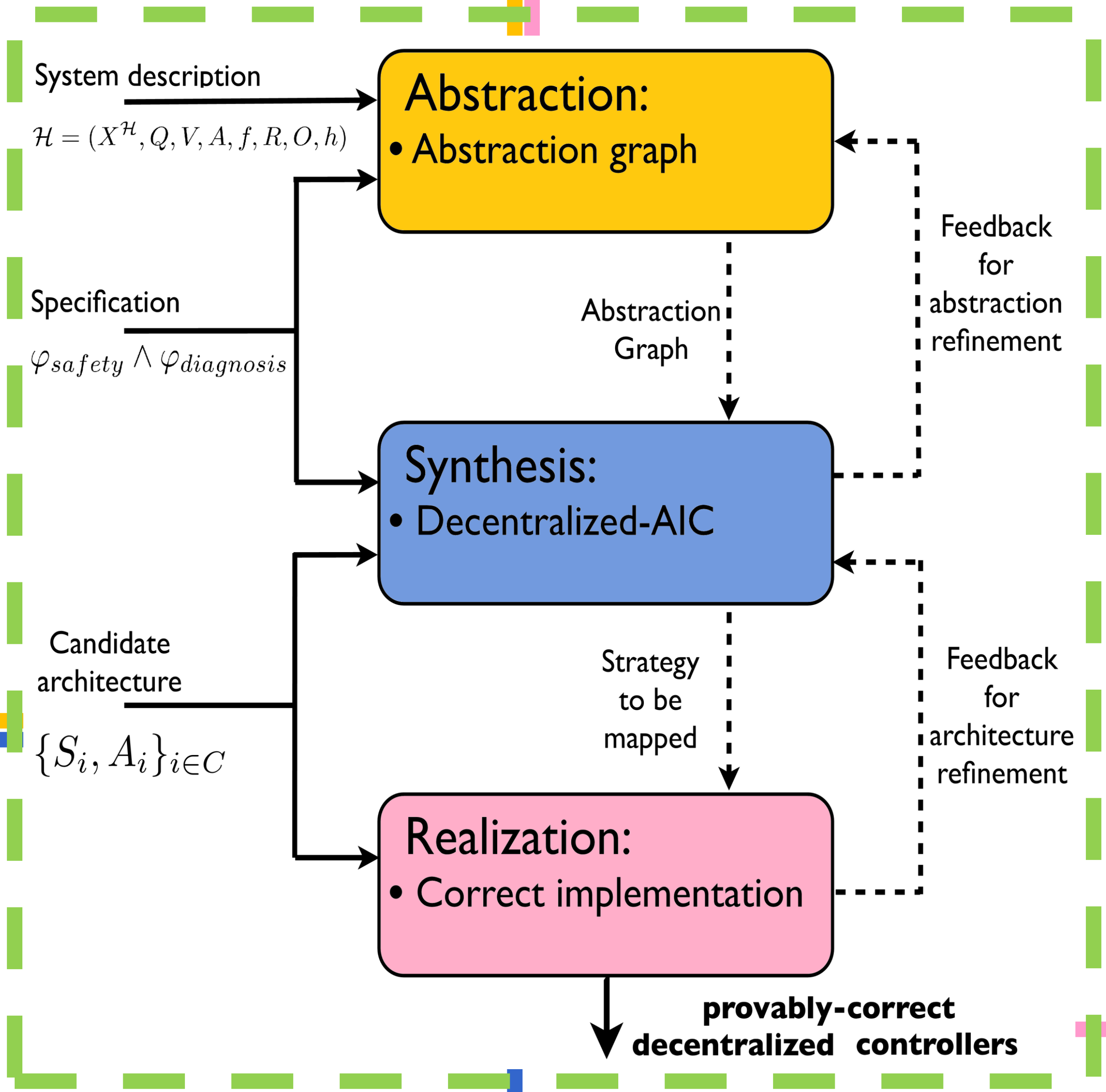
- Abstraction
  - A general abstraction method for nonlinear systems via linearization and local reachable set over-approximation
  - Quantifiable robustness margins to account for delays, uncertainties in the models, imperfect measurement
  - Extension to networked setting with abstraction graphs in progress


x: actual state
$\hat{x}$: measured state
$\hat{q}$: abstract state

- Synthesis
  - A uniform information-state-based approach: synthesis based on two-player game; bipartite transition systems (BTS)
  - Properties Considered: safety, opacity, diagnosability, attractability, etc.
  - Two stages when solving game: first enforce IS-based property, then enforce non-blockingness
  - We leverage the IS-based approach to solve the sensor activation problem
  - Decentralized synthesis in progress



Part of BTS

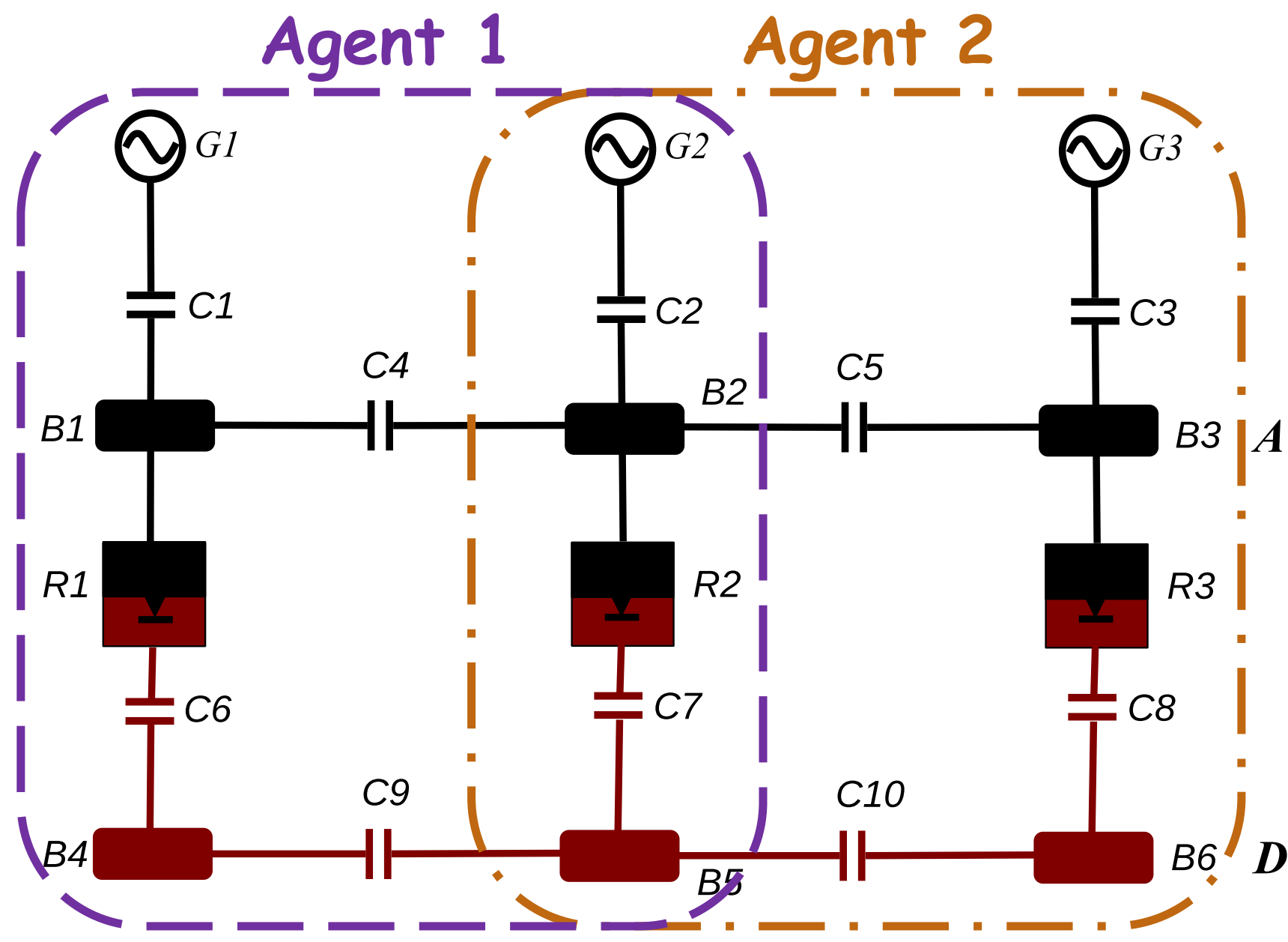

System description
$\mathcal{H} = (X^{\mathcal{H}}, Q, V, A, f, R, O, h)$
Specification
$\varphi_{safety} \wedge \varphi_{diagnosis}$
Candidate architecture
$\{S_i, A_i\}_{i \in C}$
Abstraction:
- Abstraction graph

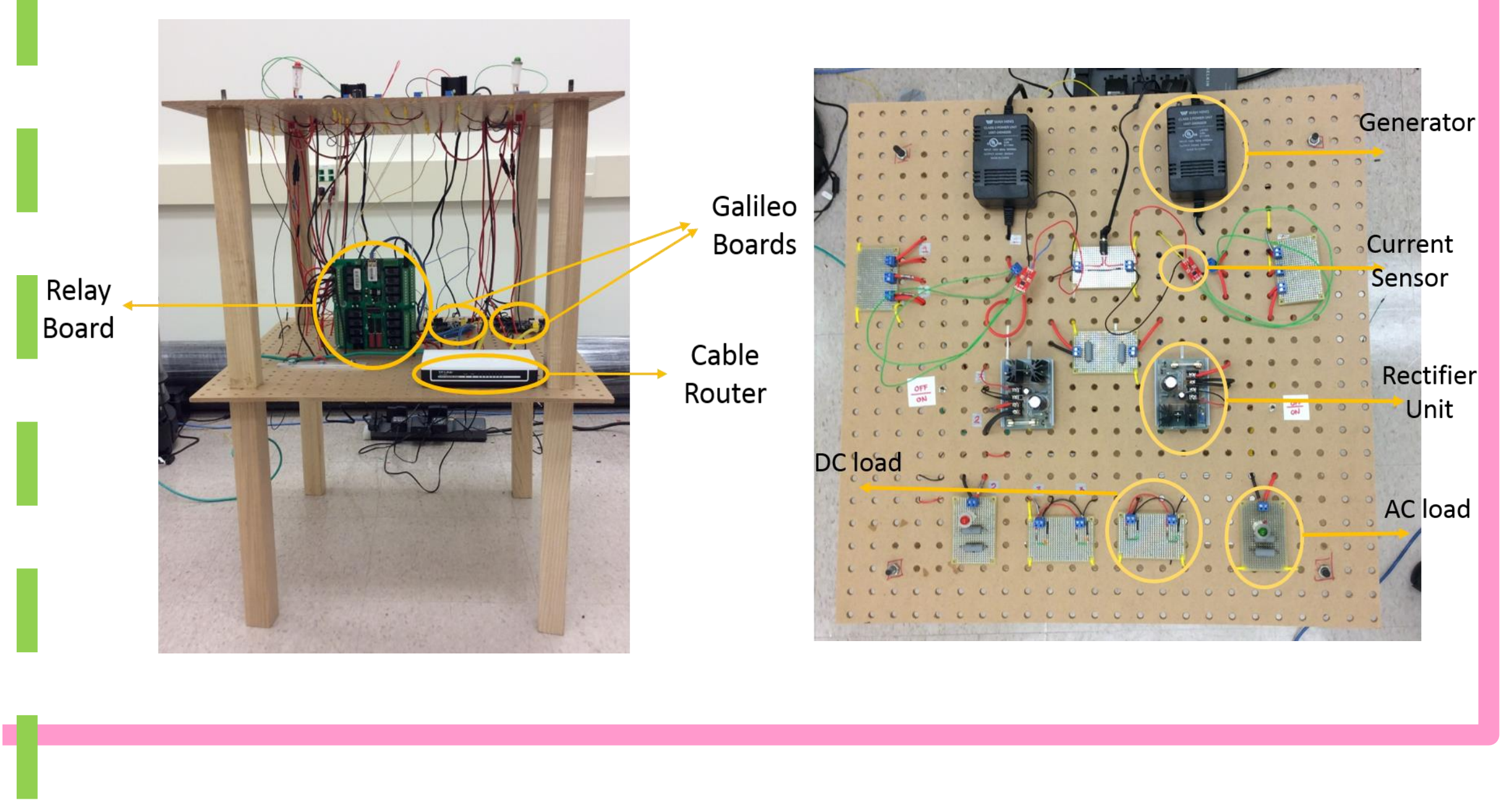
Abstraction Graph
Feedback for abstraction refinement
Synthesis:
- Decentralized-AIC

Strategy to be mapped
Feedback for architecture refinement
Realization:
- Correct implementation

provably-correct decentralized controllers

- *Simulation* model and *Test bed*
  - A university-scale test bed that captures some of the key features of an aircraft electric power system
  - Distributed sensing and control built on Robot Operating System (ROS)





References:

1.X. Yin and S. Lafortune. "A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems," *IEEE Transactions on Automatic Control*, to appear in August 2016.

2.X. Yin and S. Lafortune. "Synthesis of maximally permissive supervisors for partially observed discrete event systems," *IEEE Transactions on Automatic Control*, to appear in June 2016.

3.Y. Li, J. Liu, and N. Ozay, “Computing finite abstractions with robustness margins via local reachable set over-approximation”, Proc. 5th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS), Atlanta, GA, October 2015.

4.X. Xu, N. Ozay, and V. Gupta, “Passivity Degradation In Discrete Control Implementations: An Approximate Bisimulation Approach”, Proc. 54th IEEE Conference on Decision and Control (CDC), Osaka, Japan, December 2015.

UNIVERSITY OF MICHIGAN

D E S DISCRETE EVENT SYSTEMS GROUP
UNIVERSITY OF MICHIGAN

NSF