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:

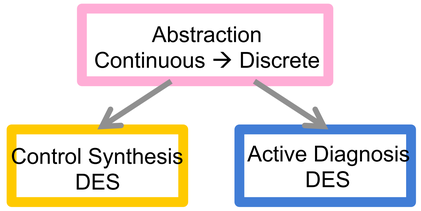
•Scalability of formal methods for synthesis of provably-correct controllers

•Development of abstraction techniques that lift CPS design problem to synthesis problem on discrete state system

•Combination of control and sensor activation

•Synthesis for resilience and adaptivity

•Consideration of the distributed features of the system at synthesis step and at implementation step



Project Duration:
January 2015 – December 2018

Project Website:
https://wiki.eecs.umich.edu/complexcps/

Participants:

• Graduate Students: Xiang Yin (PhD graduate 2017), Yun Jae Cho (MS graduate 2016), Yunus Sahin, Romulo Meira Goes, Yiding Ji, Glen Chou, Liren Yang

• Undergraduate Students: Hector Dominguez, Dylan Lawton, Nicholas Recker, Stanley Smith, Siyuan Shen, Andrew Wagenmaker, Gregory Willett, Ryan Wunderly, Andrew Bourgeois, Isaac Dubuque, William Vandini, Philip Sisk

Industrial Collaborators:

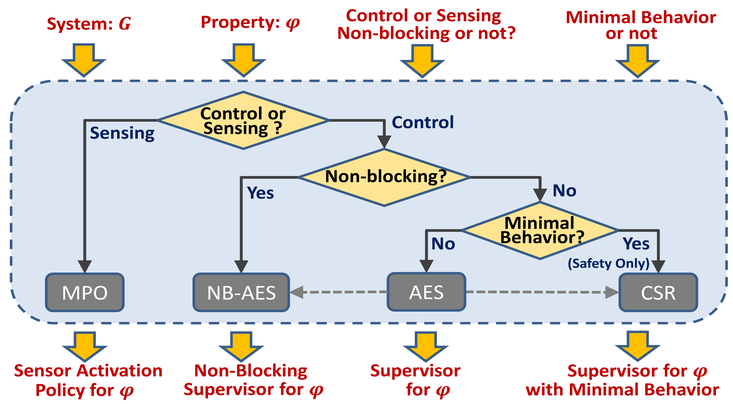
• UTC Aerospace Systems (UTAS)

• Ford Motor Company

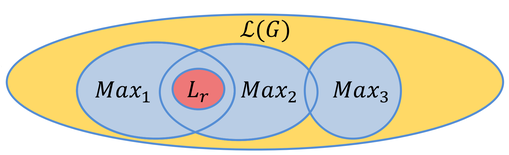
Key Results:

• Uniform Synthesis Methodology at the Discrete Level

- Controller synthesis: for safety, non-blockingness, maximal permissiveness, and minimal behavior
- Synthesis of sensor activation policies: for information-state based properties, such as diagnosability, opacity
- Solves synthesis problems that had remained open for a long time, using a game approach on suitable discrete transition structures: MPO and [NB-]AES
- Implemented in Software Tool: DPO-SYNT https://gitlab.eecs.umich.edu/M-DES-tools/DPO-SYNT
- PhD dissertation of Xiang Yin (2017)

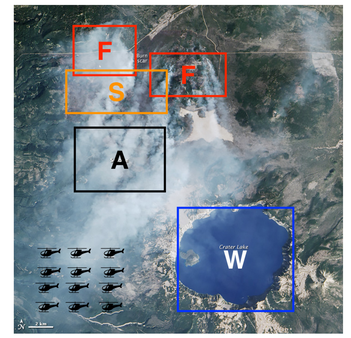


Use minimal required behavior at synthesis time to select local maximal solution



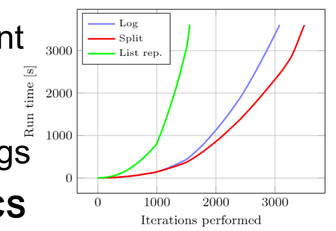
• Massively Scalable Multi-agent Coordination

- Structural properties:
  - large # of systems
  - small # of classes
  - counting constraints (sufficiently many/not too many)
  - identity of individual systems is not important



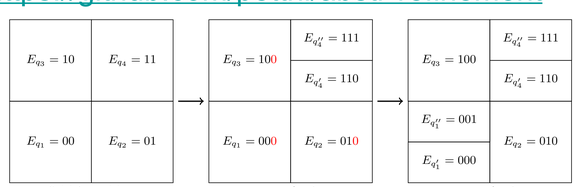
- Exploits symmetry (permutation invariance) for scalability with the number of agents
  - Two new logics (counting Linear Temporal Logic and counting Linear Temporal Logic Plus) to capture multi-agent coordination specifications
- Leverages hierarchical planning for scalability with respect to the individual agent dynamics
- Robustness to asynchrony

• Nonuniform **a**bstractions, **r**efinement and **c**ontroller **s**ynthesis with novel BDD encodings, called split encodings



- Implemented in Software Tool: **ARCS**

https://github.com/pettni/abstr-refinement



Split encodings automatically adapt to the topology of the refined partition.