Specification, Design and Verification of Distributed Embedded Systems

Mani Chandy John Doyle Richard Murray (PI)
California Institute of Technology

Eric Klavins
U. Washington

Pablo Parrilo
MIT

Project Overview
September 2009

Goals and Agenda

Goals

- Provide a review of the goals and objectives of the MURI
- Summarize activities over last year and accomplishments to date
- Describe open areas of research and opportunities for follow-on research

Agenda

1:00 Introduction and welcome

1:10 MURI overview (Murray)

1:30 Verifying Distributed Systems: Examples, Tools, Limitations (Chandy)

2:00 Specification of Networked Embedded Systems (Klavins)

2:30 Break

3:00 Fundamental Limits (Doyle)

3:30 LTL-based specifications and planning for autonomous systems (Murray)

4:00 Future Directions (Murray)

4:15 Review team caucus

4:45 Review team feedback (review team + PIs)

5:00 Adjourn

V&V MURI Team

Principal Investigators

- Mani Chandy (Caltech CS)
- John Doyle (Caltech CDS)
- Gerard Holzmann (JPL CS)*
- Eric Klavins (U. Washington, EE/CS)
- Richard Murray (Caltech CDS)
- Pablo Parrilo (MIT EE)






Partners

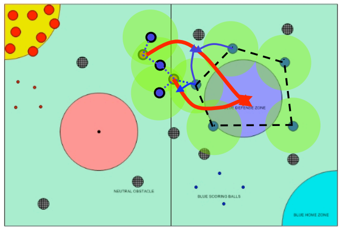
- Air Force Research Laboratory: (IF), MN, VA, VS
- Boeing Corporation - Systems of Systems Integration
- Honeywell Corporation - Guidance and Control [Glavaski -> Easton]
- Jet Propulsion Laboratory (JPL) - Laboratory for Reliable Software (LARS)
- Julia Braman -> NASA Johnson Space Center

Problem Scope

Overall Goal:

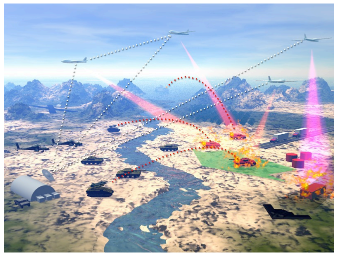
Develop methods and tools for designing control policies, specifying the properties of the resulting distributed embedded system and the physical environment, and proving that the specifications are met

Specification



- How does the user specify---in a single formalism---continuous and discrete control policies, communications protocols and environment models (including faults)?

Design and reasoning



- How can engineers reason that their designs satisfy the specifications?
- In particular, can engineers reason about the performance of computations and communication, and incorporate real-time constraints, dynamics, and uncertainty into that reasoning?

Implementation

- What are the best ways of mapping detailed designs to hardware artifacts, running on specific operating systems? What languages are suitable for specifying systems so that the specifications can be verified more easily?

Program Thrusts

Specification and Reasoning Using Graph Grammars

- Build on Klavins' Computation and Control Language (CCL) & SPIN (Holzmann)
- Graph grammars to define & reason about interaction rules
- Temporal specifications using linear temporal logic (LTL)

Sum of Squares [Lyapunov] Techniques (SOS)

- Unified framework for finding invariants and proof certificates for nonlinear and hybrid systems

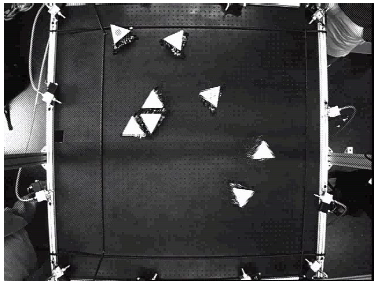
- Allow temporal logic statements and verification of semi-algebraic conditions to coexist
- Develop design specification and design language plus reasoning tools

Extensions

- Probabilistic techniques (specification + algorithms)
- Adversarial settings (including security issues)

Testbeds

- U. Washington Programmable Parts testbed -> factory floor
- ~~Caltech Multi-Vehicle Wireless Testbed (hardware + sims)~~
- Alice: 2005 and 2007 DARPA Grand Challenge entry



Cooperative Control Systems Framework

Agent dynamics

$$\dot{x}^i = f^i(x^i, u^i) \quad x^i \in \mathbb{R}^n, u^i \in \mathbb{R}^m$$
$$y^i = h^i(x^i) \qquad y^i \in \mathbb{R}^q$$

Vehicle "role"

- $\alpha \in \mathcal{A}$ encodes internal state + relationship to current task
- Transition $\alpha' = r(x, \alpha)$

Communications graph $\mathcal{G}$

- Encodes the system information flow
- Neighbor set $\mathcal{N}^i(x, \quad)$

Communications channel

- Communicated information can be lost, delayed, reordered; rate constraints

$$y^i_j[k] = \gamma y^i(t_k - \tau_j) \quad t_{k+1} - t_k > T_r$$

- γ = binary random process (packet loss)

Task

- Encode as finite horizon optimal control

$$J = \int_0^T L(x, \alpha, \mathcal{E}(t), u)\, dt + V(x(T), \alpha(T)),$$

- Assume task is *coupled,* env't estimated

Strategy

- Control action for individual agents

$$u^i = k^i(x, \alpha) \qquad \{g^i_j(x, \alpha) : r^i_j(x, \alpha)\}$$

$$\alpha^{i\,\prime} = \begin{cases} r^i_j(x, \alpha) & g(x, \alpha) = \text{true} \\ \text{unchanged} & \text{otherwise.} \end{cases}$$

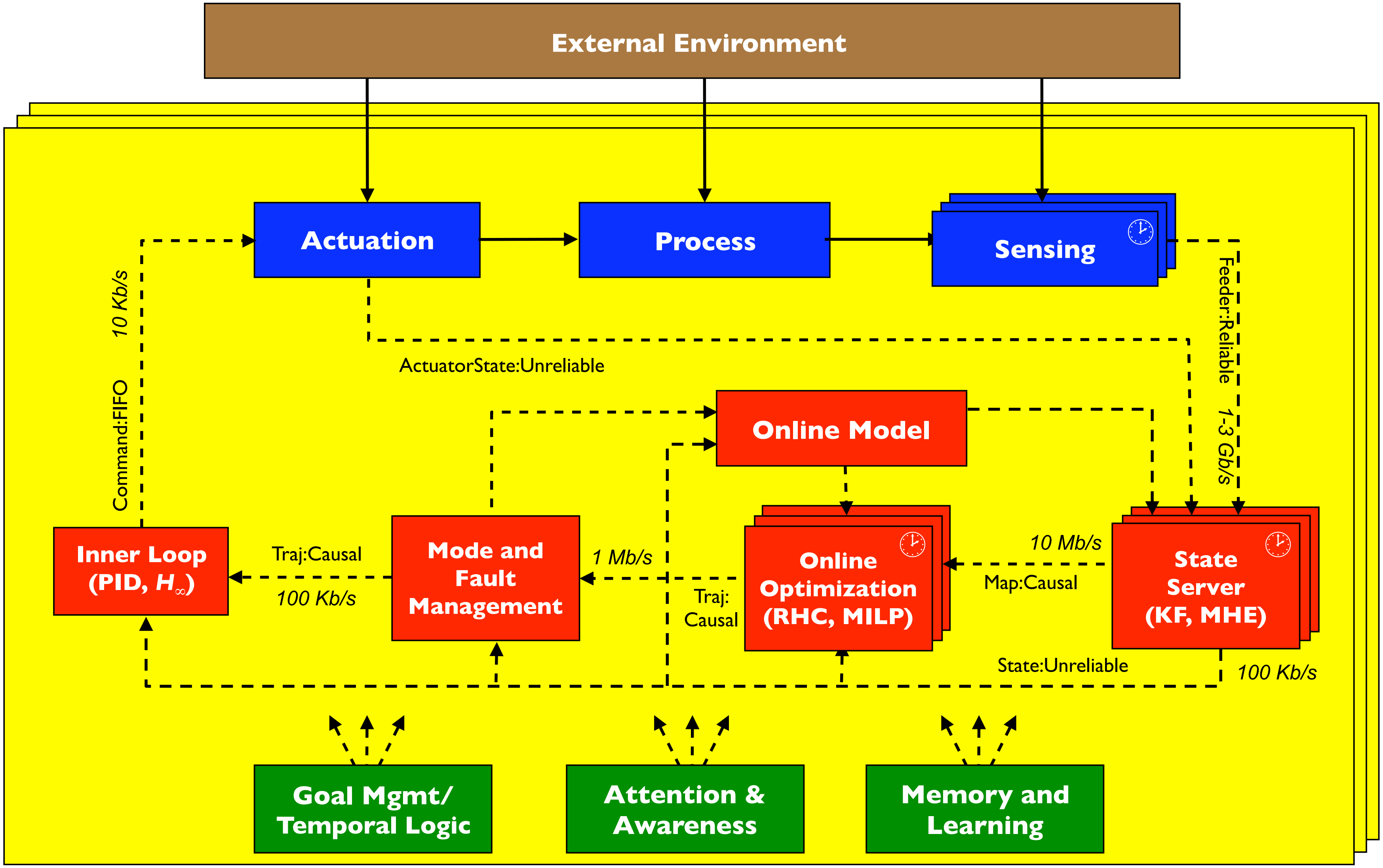
***Decentralized* strategy**

$$u^i(x, \alpha) = u^i(x^i, \alpha^i, y^{-i}, \alpha^{-i}, \hat{\mathcal{E}})$$
$$y^{-i} = \{y^{j_1}, \ldots, y^{j_{m_i}}\}$$
$$j_k \in \mathcal{N}^i \quad m_i = |\mathcal{N}^i|$$

- Similar structure for role update

Networked Control Systems

(following P. R. Kumar)



Goals and Agenda

Goals

- Provide a review of the goals and objectives of the MURI
- Summarize activities over last year and accomplishments to date
- Describe open areas of research and opportunities for follow-on research

Agenda

1:00 Introduction and welcome

1:10 MURI overview (Murray)

1:30 Verifying Distributed Systems: Examples, Tools, Limitations (Chandy)

2:00 Specification of Networked Embedded Systems (Klavins)

2:30 Break

3:00 Fundamental Limits (Doyle)

3:30 LTL-based specifications and planning for autonomous systems (Murray)

4:00 Future Directions (Murray)

4:15 Review team caucus

4:45 Review team feedback (review team + PIs)

5:00 Adjourn