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

Annual Program Review
27 Oct 08

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 plans for the coming year of research

Agenda

9:00	MURI overview (Murray)
9:30	Design of Cooperative Control Strategies (Klavins)
10:00	Automated Verification (Chandy)
10:30	Break
10:45	Fundamental Limits (Doyle)
11:15	Stochastic Behavior (Thorsley)
11:45	Game Theoretic Approaches (Parrilo)
12:15	Lunch
1:00	Implementation and Transition Plan (Murray)
1:15	Plans for years 3-5 (Murray)
1:30	Q&A
2:00	Poster session
3:00	Review team caucus
4:00	Review team feedback

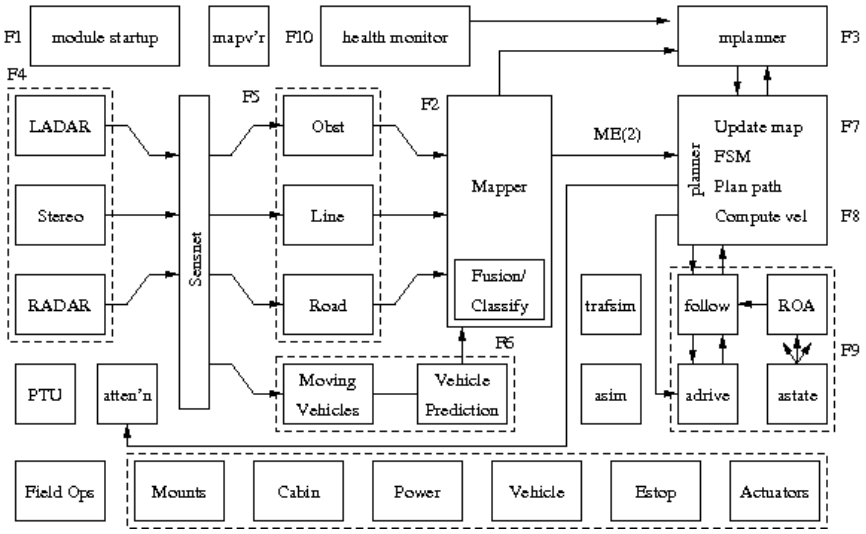
Motivating Example: Alice (DGC07)

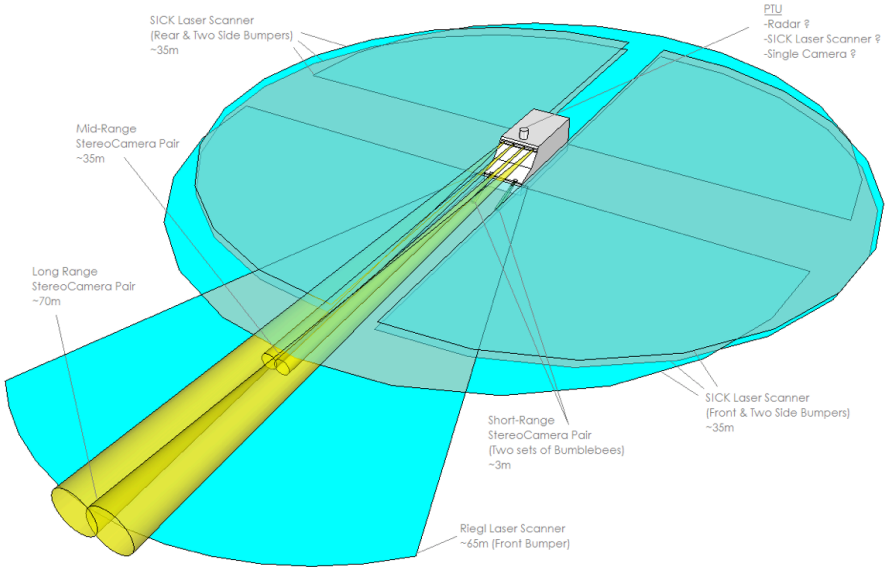
Alice

- 300+ miles of fully autonomous driving
- 8 cameras, 8 LADAR, 2 RADAR
- 12 Core 2 Duo CPUs + Quad Core
- ~75 person team over 18 months

Software

- 25 programs with ~200 exec threads
- 237,467 lines of executable code



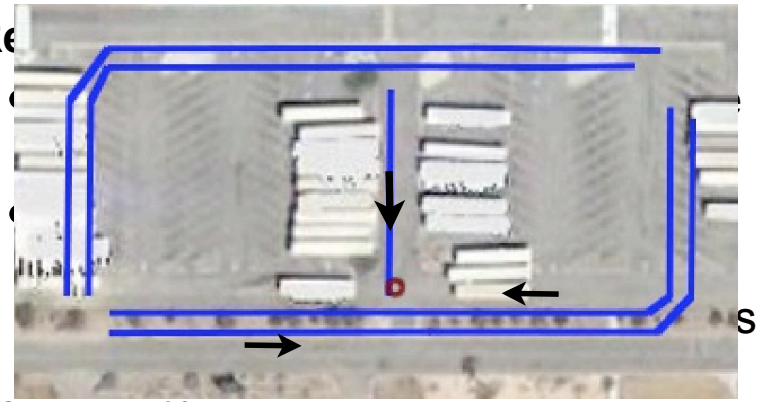


2007 National Qualifying Event

Merging test

- 10-12 cars circling past inters'n
- Count "perfect runs" in 30 min

Re



S

V&V MURI Team (Aug 06)

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
- Jet Propulsion Laboratory (JPL) - Laboratory for Reliable Software (LARS)

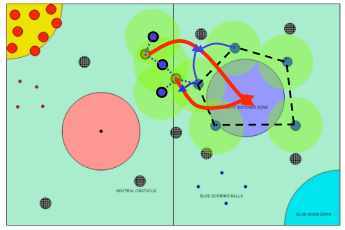
Problem Scope (Aug 06)

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

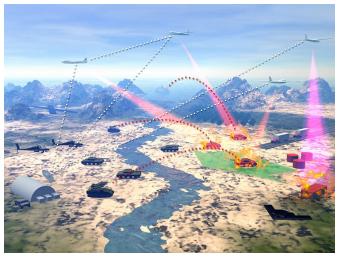
Specification

- 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 (Aug 06)

Specification and Reasoning Using Graph Grammars

- Build on Klavins' Computation and Control Language (CCL) & SPIN (Holzmann)
- Use graph grammars to define interaction rules and reason about them

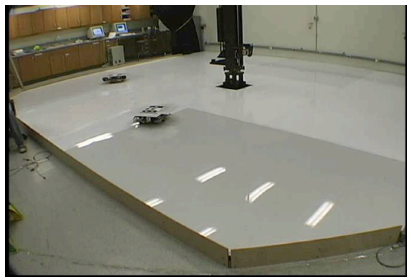
Sum of Squares Techniques (SOS)

- 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)
- Computational techniques (with JPL/CACR)



Testbeds

- Caltech Multi-Vehicle Wireless Testbed (hardware + sims)
- Alice: 2005 and 2007 DARPA Grand Challenge entry

Transition Strategy (Aug 06)

Toolbox development

- Develop and disseminate algorithms via publicly available toolboxes (DESTOOLS)

Annual workshops/short courses

- Model after mutools workshops developed by Balas, Doyle and Packard
- Provide opportunity for researchers to learn about the toolboxes developed under the MURI and apply the design tools to simple problems
- Provide forum for feedback to MURI team and discussion of needed tools
- Develop new courses and new course materials that can be used to teach students the required background to be effective practitioners and researchers in distributed embedded systems

Personnel exchange

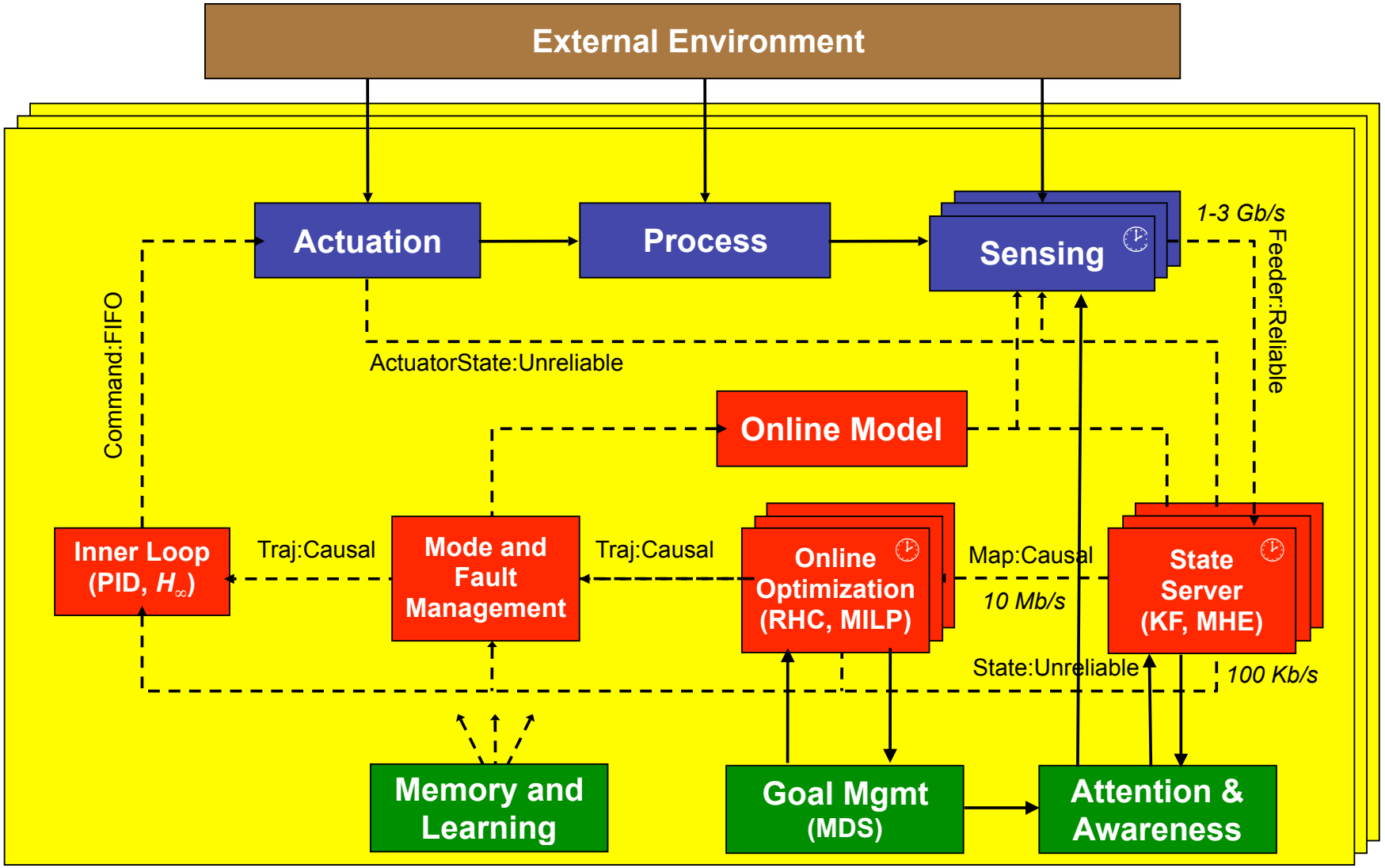
- Student internships at AFRL labs and industry
- Industry visitors: eg, Sonja Glavaski from Honeywell spending 1 month at Caltech

Additional workshops and tutorials

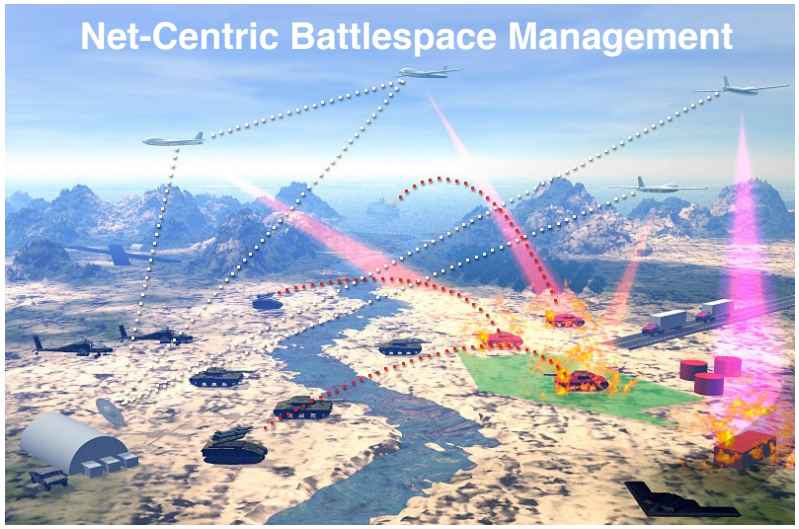
- Connections II: Foundations of Network Science, 14-18 Aug @ Caltech
- CDC 2006: High Confidence Embedded Systems (Klavins and Murray)

Networked Control Systems

(following P. R. Kumar)



Specification, Design and Verification of Distributed Embedded Systems
Caltech/MIT/UW, Murray (PI)/Chandy/Doyle/Klavins/Parrilo



Long-Term PAYOFF: Rigorous methods for design and verification of distributed systems-of-systems in dynamic, uncertain, adversarial environments

OBJECTIVES

- Specification language for continuous & discrete control policies, communications protocols and environment models (including faults)
- Analysis tools to reason about designs and provide proof certificates for correct operation
- Implementation on representative testbeds

APPROACH/TECHNICAL CHALLENGES

- Specification and reasoning using graph grammars
- Sum of squares analysis for certificates, invariants
- Extensions to probabalistic, adversarial and networked operations

ACCOMPLISHMENTS/RESULTS

- Embedded graph grammars for cooperative control
- Lyapunov-based verification of temporal properties
- Stochastic games using semidefinite programming
- Tools for converting goal networks to hybrid FSM
- Applications examples with DARPA GC + JPL

FUNDING ($K)—Show all funding contributing to this project

	FY06	FY07	FY08	FY09	FY10
AFOSR Funds	417	1000	1000	1000	1000
Boeing	310	390	390	390	[390]
DARPA GC		1200			

TRANSITIONS

- Application to autonomous driving (DGC07)

STUDENTS, POST-DOCS

2006-08: 12 graduate students, 4 postdocs, 4 undergraduates

LABORATORY POINT OF CONTACT

Dr. Siva Banda, AFRL/RBCA, WPAFB, OH

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 plans for the coming year of research

Agenda

9:00	MURI overview (Murray)
9:30	Design of Cooperative Control Strategies (Klavins)
10:00	Automated Verification (Chandy)
10:30	Break
10:45	Fundamental Limits (Doyle)
11:15	Stochastic Behavior (Thorsley)
11:45	Game Theoretic Approaches (Parrilo)
12:15	Lunch
1:00	Implementation and Transition Plan (Murray)
1:15	Plans for years 3-5 (Murray)
1:30	Q&A
2:00	Poster session
3:00	Review team caucus
4:00	Review team feedback