RT-166: Formal Methods in Resilient Systems Design using a Flexible Contract Approach

PI: Prof. Azad M. Madni
Research Team: Prof. Dan Erwin, Dr. Ayesha Madni, Edwin Ordoukhanian, Parisa Pouya

SYSTEMS ENGINEERING RESEARCH CENTER

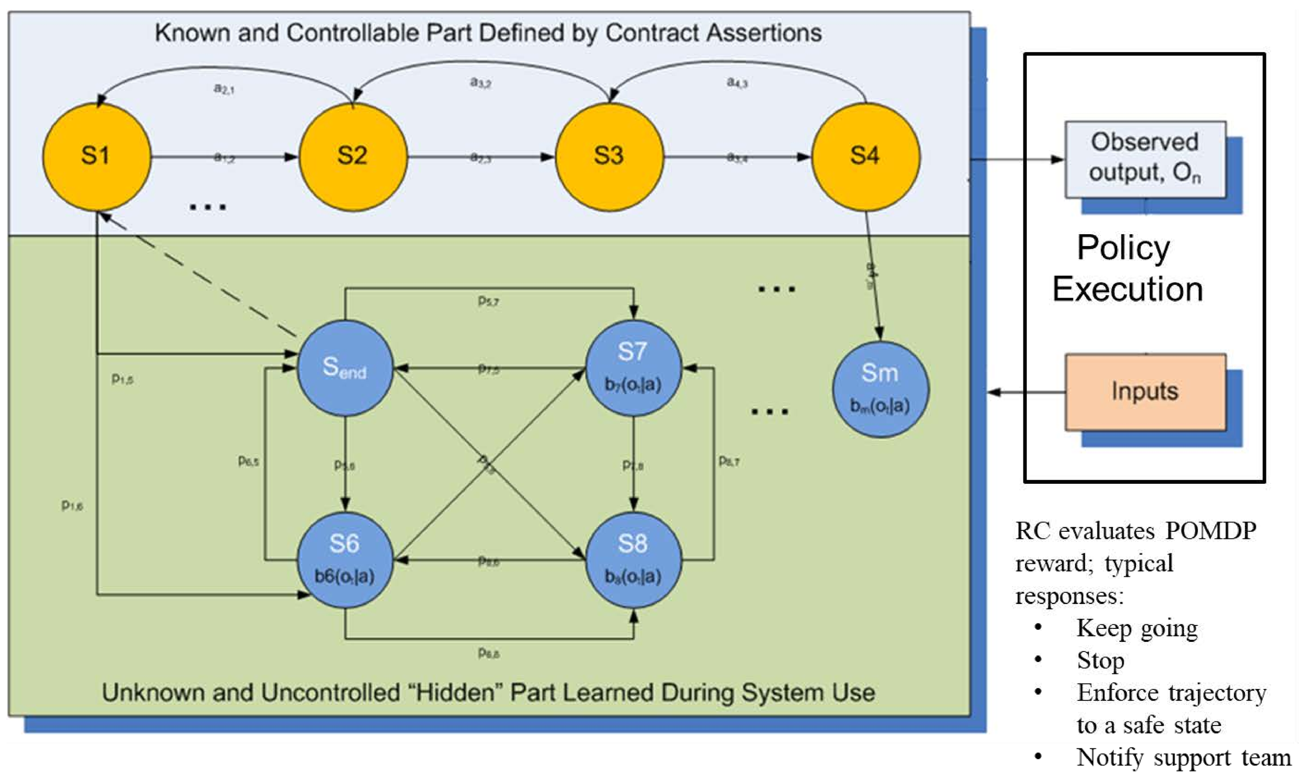
USC Viterbi School of Engineering
Systems Architecting and Engineering

Research Task / Overview

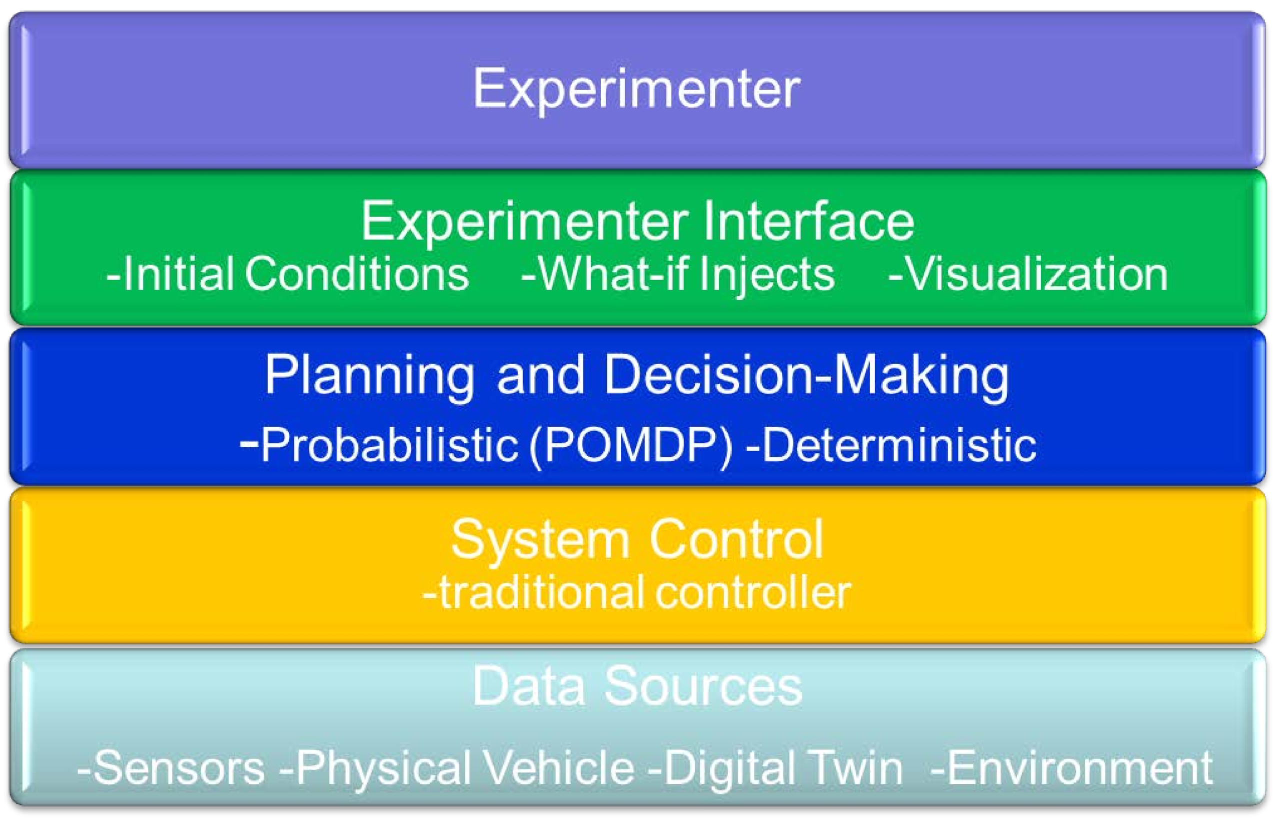
- Develop formal methods-based approach for resilient system and SoS design
- Support SERC's Systems Engineering and System Management Transformation Research Area

Data & Analysis

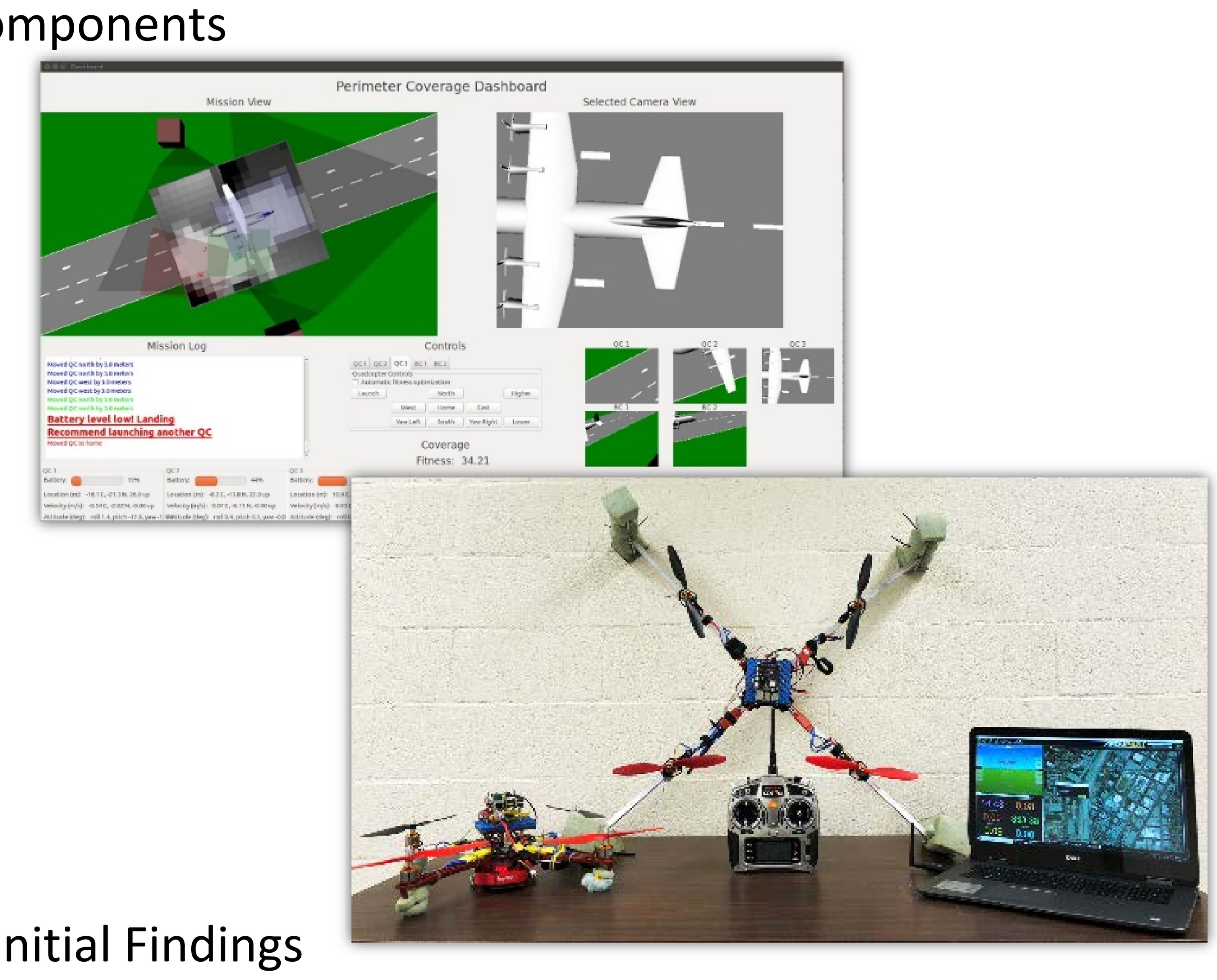
- Data Sources
  - Representative Multi-UAV mission
  - Exemplar scenarios
- Resilience Contract Formalism



- Experimentation Testbed Architecture



- Execution Monitoring Dashboard and Hardware Testbed Components



- Initial Findings
  - Key problem: resolving mismatch between decision-making layer & vehicle control layer
  - POMDP and vehicle controller execute on different time scales
  - Concurrent creation of experimentation testbed facilitates experimentation and data collection
  - Monitoring and execution dashboard facilitated both understanding and debugging of vehicle behaviors

Goals & Objectives

- Enable a capability for verifiable and flexible complex system behaviors
- Exemplar Application: multi-UAV mission
- Exploit Formal and Flexible System Representation
  - deterministic + probabilistic modeling
  - patterns of disruptions
  - pattern-driven responses

Methodology

- Combines formal and probabilistic modeling with heuristics
- Architecture Characteristics:
  - Layered: planning and decision making; control
  - Decisions and information flow from planning and decision making (top layer) to control (bottom layer)
  - Execution constraints flow from control layer to planning and decision making layer
  - In case of conflicts, global swarm objectives have priority over local AV goals
- Defined Resilience Contract formalism to balance system verifiability and system flexibility requirements
  - Relaxes assertions in traditional contract to introduce flexibility ("belief-reward")
  - Partially Observable Markow Decision Process (uncertainty handling)
  - In-use reinforcement learning (hidden states, transitions, emissions)
  - Heuristics/patterns (complexity reduction)

Future Research

- Develop multi-UAV high-level probabilistic decision-making using POMDP
- Expand capability of experimentation testbed
- Collect and analyze data for more complex scenarios
- Transition capability to designated site(s)
- Develop measurable utility function (i.e., Reward Function) to evaluate candidate options
- Refine reward value assignment method
- Employ experimental testbed to refine transition probabilities among vehicle states

References

- Madni, A.M., Sievers, M., Erwin, D., Madni, A., Ordoukhanian, E., Pouya, P., "Formal Modeling of Complex Resilient Networked Systems", accepted for publication in AIAA SciTech 2019.
- Madni, A.M. Formal and Probabilistic Modeling in the Engineering of Resilient Multi-UAV Swarms, 21st Annual Systems and Mission Engineering Conference, Tampa, FL, October 22-25, 2018.
- Madni AM, Sievers M, Ordoukhanian E, Madni A, Pouya P. Extending Formal Modeling for Resilient Systems Design. INCOSE International Symposium 2018 Jul (Vol. 28, No. 1, pp. 1138-1152).
- Madni AM, Sievers MW, Humann J, Ordoukhanian E, Boehm B, Lucero S. "Formal methods in resilient systems design: application to multi-UAV system-of-systems control," Disciplinary Convergence in Systems Engineering Research 2018 (pp. 407-418). Springer, 2018.