BARRON ASSOCIATES

Runtime Assurance for Complex Autonomy

1. An Air Force Funded Program

- Air Force Research Laboratory (AFRL) funded program
  - Wright-Patterson Air Force Base
  - Three year effort
  - Matt Clark, Program Manager
- Barron Associates team
  - John Schierman, Principal Investigator
  - Michael DeVore, Nathan Richards

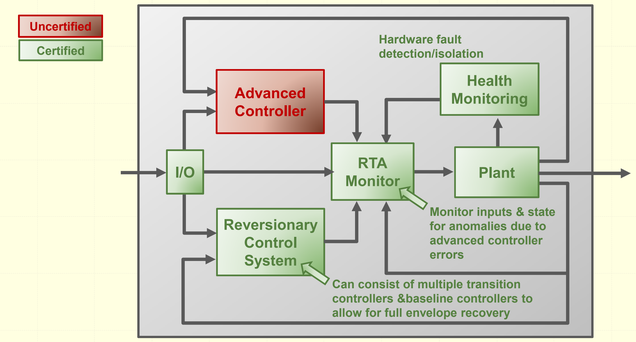
- Approved for Public Release, AFRL Case No. 88ABW-2014-3666

2. Runtime Assurance (RTA)

- Motivation
  - Aerospace systems require rigorous software certification for safety critical applications
  - Current V&V methods cannot achieve required certification levels for highly complex autonomous systems
  - Investigating application of Runtime Assurance (RTA) to solve this problem
- Started with Simplex Framework (90's-00's)
  - Carnegie Mellon: Lui Sha, Bruce Krogh, Danbing Seto
- Further developed approach
  - Multiple transition controllers/multiple recovery actions

3. RTA Framework – Protected System

- Protected system = fully certified system



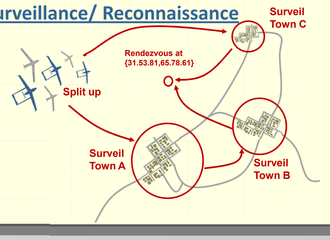
4. RTA Application to Complex Systems

- Multiple unmanned air systems
  - Heterogeneous fleets, including morphing wing vehicles
  - Performing complex, time sensitive missions
  - Decentralized/distributed command/control framework
  - Mixed-initiative: Full autonomy to human "on the loop" (supervisory/managerial role)

Morphing Wing

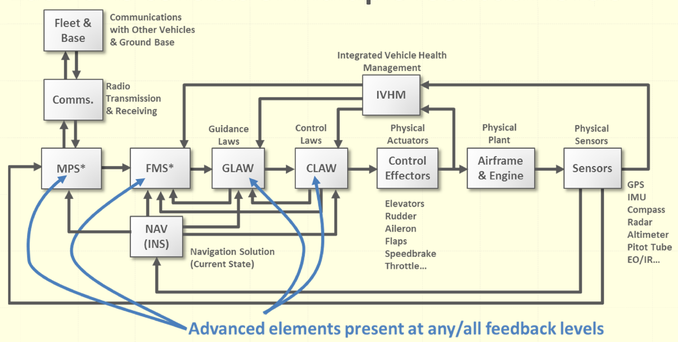
Urban Operations

Surveillance/ Reconnaissance



5. Complex System-of-Systems

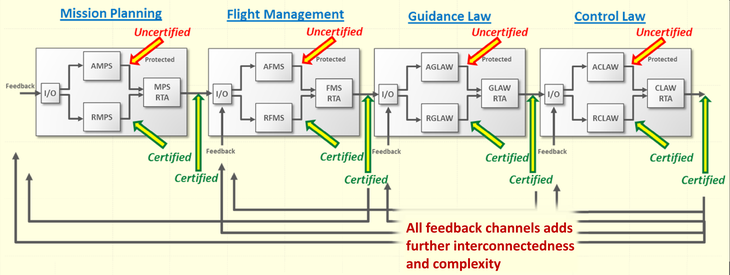
- Each UAS consists of multiple feedback levels



*MPS = Mission Planning System (plans out mission)
*FMS = Flight Management System (carries out mission)

6. Multiple Cascaded Protected Systems

- Advanced, uncertifiable elements at each feedback level
  - Result in multiple cascaded/interacting protected systems
  - *This is a highly complex RTA design!*

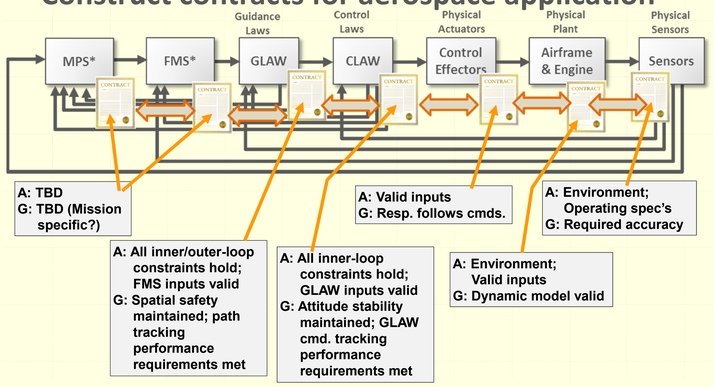


7. How Do We Handle All This Complexity?

- Compositional Reasoning Design Approach
  - Isolate analysis of design constraints/requirements at each subcomponent level to "modularize complexity"
  - Construct Assume-Guarantee (A-G) contracts for each subcomponent level
  - Analyze overall system in successively higher levels (children to parent elements)
  - Ensure contracts are met at each level and when connected to higher levels
- A-G contracts form the "checks" that are analyzed by the RTA monitor

8. New Application for A-G Contract Analysis

- Construct contracts for aerospace application



9. Next Steps

- Focus on A-G contracts for Mission Planning & Flight Management levels
  - May involve discrete decision making logic constructs
  - How do we analyze discrete logic contracts together with physics-based contracts at GLAW & CLAW levels?
- Employ Rockwell-Collins' AGREE tool (Assume-Guarantee REasoning Environment)
  - Can analyze over booleans, integers & real expressions*

*Cofer, Whalen, et al. S5, 2014, etc.

Interested in RTA? Contact:

John Schierman
Principal Research Scientist
BARRON ASSOCIATES, INC.
1410 Sachem Place, Suite 202
Charlottesville, VA 22901
Voice: 434-973-1215, Ext. 111
Fax: 434-973-4686
schierman@bainet.com
www.barron-associates.com