UxAS Verification

September 25, 2018
Presented by Jen Davis

Rockwell Collins
Building trust every day

Introduction

- UxAS is the experimental platform for CASE
- The next few charts provide an overview of some of the UxAS verification work to date and where you can find artifacts which may (or may not) be helpful to you

AFRL Summer of Innovation (2017)

- ~50 participants from government, industry, and academia
  - AFRL, NASA Ames, SEI
  - Dependable Computing, Galois, GE Research, Lockheed Martin, Rockwell Collins
  - ASU, ISU, U of Cincinnati, CU-Boulder, UT-Austin, Vanderbilt, Wright State
- Challenge problem: Apply formal methods to UxAS, a system developed without formal verification in mind
- Subdivided into about ten teams to tackle various aspects of verification
- Results presented during Day 3 of AFRL’s Safe and Secure Systems and Software Symposium (S5)
  - Links to slides available here: http://mys5.org/index.php?id=30

AFRL Summer of Innovation (2017) Teams/Topics

- Argument
- Requirements
  - Link to top-down requirements spreadsheet (Google Sheet)
- System Safety
- Architecture
  - AADL/AGREE models are on the architecture branch of OpenUxAS under AADL_project
- Real-time/Middleware
- Hybrid Systems
- Cyber-Resilient Task/Service Planning (UxAS on seL4)
  - Embedded UxAS demo and presentation in the other session today
- Memory Safety of UxAS Tasks/Retrofitting UxAS with Rust
- Mission Planning
- Testing

Decentralized Perimeter Surveillance Systems (DPSS) Verification

- DPSS is a multi-agent (multi-UAV) protocol for perimeter surveillance
- It is part of UxAS (under src/DPSS), but the implementation doesn’t work yet
- Original paper on the algorithm published in 2008
- Formal verification (2017-present)
  - AADL/AGREE DPSS models on the architecture branch: link to DPSS-3-AlgB-for-paper project
  - Found a critical error in a lemma used in the proof of Theorem 2 in the paper
  - Recent paper summarizing the models and findings: http://loonwerks.com/publications/davis2018.html