Ph.D. Defense

Kerianne Hobbs

(Advisors: Eric Feron and Glenn Lightsey)

"Elicitation and Formal Specification of Run Time Assurance Requirements for Aerospace Collision Avoidance Systems"

Friday, March 13 at 1:00 p.m.
Montgomery Knight Building, Room 317

Abstract:
One of the greatest challenges preventing use of advanced controllers in aerospace is developing methods to verify, validate, and certify them with high assurance. Traditional test and simulation-based approaches evaluate system behavior at design time in a subset of the total state space. Results from simulation and testing cannot be interpolated over systems with large state spaces, systems with nonlinear dynamics, systems that learn or degrade over time, systems operating under high uncertainty, or systems in complex and adversarial environments.

Run Time Assurance (RTA) systems are proposed as a complementary verification approach to facilitate near-term certification of advanced aerospace decision and control systems. RTA systems monitor the state of a cyber-physical system (CPS) online for violations of predetermined boundaries that trigger a switch to a simple, safety remediation controller. For example, automatic collision avoidance systems are RTA systems that monitor the CPS state for violations of proximity constraints and switch to a backup controller that assures safe separation. Design of RTA systems is generally ad hoc and specific to application, although common design elements and requirements of RTA systems cross applications and domains.

This research elicits, formally specifies, and analyzes RTA-based collision avoidance system requirements for a conceptual spacecraft conducting autonomous close-proximity operations. First, the Automatic Ground Collision Avoidance System developed for aircraft is studied to identify common design elements and requirements of RTA last-instant collision avoidance systems that cross the air and space domains. Second, formal requirements specification templates are developed for a generalized RTA architecture that extends the simplex architecture by accounting for human interaction, system faults, and safety interlocks. Third, formal requirements are elicited through the process of formal specification as well as from common design elements and requirements, spacecraft guidance constraints in the literature, and a structured hazard assessment. Finally, the requirements are analyzed using compositional reasoning and formal model checking verification techniques.

Committee:

- Prof. Eric M. Feron, School of Aerospace Engineering, Georgia Institute of Technology
- Prof. Glenn Lightsey, School of Aerospace Engineering, Georgia Institute of Technology
- Dr. Moriba K. Jah, School of Aerospace Engineering and Engineering Mechanics, University of Texas at Austin
- Prof. Joseph H. Saleh, School of Aerospace Engineering, Georgia Institute of Technology
- Dr. Alwyn E. Goodloe, Safety Critical Avionics Systems Branch, National Aeronautics and Space Administration