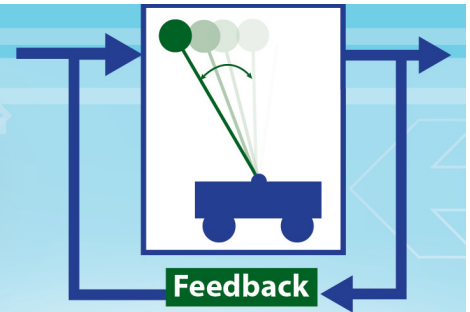


COLLEGE OF ENGINEERING

Control Seminar



Sponsored by: Bosch, Ford, and Toyota

Formal Verification of Aerospace Software



Jean-Baptiste Jeannin

University of Michigan
Department of Aerospace Engineering

Friday, November 17, 2017

3:30 – 4:30 pm • 1500 EECS

ABSTRACT: Software plays an ever-increasing role in the design and operation of all aircraft, from UAVs to airliners. On-board software is rigorously developed following the DO-178C norm. Going beyond this rigorous process, this talk shows how to mathematically prove formal guarantees about the correctness of aerospace software, through the example of an industrial aircraft collision avoidance system, ACAS X. ACAS X is an industrial system intended to be installed on all large aircraft to prevent mid-air collisions. A successor to TCAS, it is being developed by the Federal Aviation Administration. As part of a physical world, ACAS X is a hybrid system: its models are governed by both discrete program constructs as well as differential equations, making verification particularly challenging. I will first determine the geometric configurations under which the advice given by ACAS X is safe, and formally verify these configurations. I will then examine the ACAS X system and analyze some cases where our safe configurations conflict with the advisory given by ACAS X. The approach is general and can be applied to other collision avoidance systems, as well as cars, trains, robots and medical devices.

BIO: Jean-Baptiste Jeannin is a starting Assistant Professor in the Department of Aerospace Engineering at the University of Michigan, where his research focuses on formal verification and safety of cyber-physical systems, with a focus on aerospace software systems. His background is in programming languages, logic and security, whose techniques and ideas he applies to the aerospace domain. Before coming to Michigan, Jean-Baptiste was working on Javascript compilers and software security, as a Researcher at Samsung Research America in Mountain View, California. He also led the formal analysis of the Next-Generation Airborne Collision Avoidance System (ACAS X), as a Post Doctoral Fellow working with André Platzer at Carnegie Mellon University, and in collaboration with the Johns Hopkins Applied Physics Laboratory. He received a Ph.D. in Computer Science from Cornell University in 2013, where he was advised by Dexter Kozen. He also received a Master of Engineering in Computer Science from Cornell University in 2008, and a Diplôme d'Ingénieur from École Polytechnique, France in 2007. In his spare time, he likes to fly small airplanes.