Formal methods for Aerospace Applications

Eric Feron

Georgia Tech, USA

Abstract

Formal methods are being progressively incorporated in the aircraft and spacecraft software design and verification process and become commonplace elements of the aerospace industry. Five aerospace software system experts will present their views on this process and where it is headed.

Focusing first on design issues, PETE MANOLIOS (Northeastern University, USA) will discuss design aspects and costs of commercial air transport vehicles, including integrated modular avionics, verification costs, and system integration. He will then discuss how new verification technology is used to algorithmically synthesize an optimal architecture subject to high level constraints. This work will be illustrated by a case study involving the Boeing 787 Dreamliner.

MARC PANTEL (IRIT, France) will then discuss safety requirements as a key aspect of the development of embedded systems in avionics. He will discuss the current regulations linking safety requirements to software design guidelines. He will then discuss novel approaches to model driven software development, using formal models and verification activities at the various steps of the development cycle. Experiments conducted in relation with European avionics companies will be described.

Moving then towards analysis methods, GUILLAUME BRAT (NASA, USA) will discuss sound, complete, precise, and scalable static analysis of flight control systems. He will introduce the IKOS static analysis framework, whose intellectual foundation is abstract interpretation. He will insist on compositional verification, a necessary tool for to make formal methods scale up to real, avionics systems. He will address the component-based development approach of these systems.

ERIC FERON (Georgia Tech, USA), and PIERRE-LOIC GAROCHE will discuss the application of the methods introduced above to control software, a narrow, but essential component of any safety-critical software system. They will then describe a possible evolution of the current development process of aircraft control systems towards more formalism (through a combination of formal proof and proof replay). They will discuss the static analysis of the behavior of the controller (stability and other non linear properties), and the static analysis of the safety architecture of the controller.

978-0-9835678-2-0/12/$31.00 ©2012 FMCAD Inc.