Abstract

Formal methods are seen as a cheaper and more exhaustive solution to the current expensive testing process used in the aviation industry. However, aviation systems are getting more and more complex. So, formal methods have no hope to address these systems unless some compositional argument is being made. In this talk, I will present the results of the effort led by NASA to demonstrate the use of formal methods and compositional verification for the V&V of safety requirements of a flight critical system. The talk will show how the formal arguments made at the component level are being composed into a system-level argument. The study is done on Simulink models for a quad-redundant flight control system for a transport class airplane.