Managing Uncertainty in the Design of Safety-Critical Aviation Systems

Submitted by pjseiler on Sun, 01/31/2016 - 1:22am. Contributors:
Peter SeilerDemoz Gebre-EgziabherJason RifeSam Guyer

Abstract:

The objective of this research is to create tools to manage uncertainty in the design and certification process of safety-critical aviation systems. The research focuses on three innovative ideas to support this objective. First, probabilistic techniques will be introduced to specify system-level requirements and bound the performance of dynamical components. These will reduce the design costs associated with complex aviation systems consisting of tightly integrated components produced by many independent engineering organizations. Second, a framework will be created for developing software components that use probabilistic execution to model and manage the risk of software failure. These techniques will make software more robust, lower the cost of validating code changes, and allow software quality to be integrated smoothly into overall system-level analysis. Third, techniques from Extreme Value Theory will be applied to develop adaptive verification and validation procedures. This will enable early introduction of new and advanced aviation systems. These systems will initially have restricted capabilities, but these restrictions will be gradually relaxed as justified by continual logging of data from in-service products. The three main research aims will lead to a significant reduction in the costs and time required for fielding new aviation systems. This will enable, for example, the safe and rapid implementation of next generation air traffic control systems that have the potential of tripling airspace capacity with no reduction in safety. The proposed methods are also applicable to other complex systems including smart power grids and automated highways. Integrated into the research is an education plan for developing a highly skilled workforce capable of designing safety critical systems. This plan centers around two main activities: (a) creation of undergraduate labs focusing on safety-critical systems, and (b) integration of safety-critical concepts into a national robotic snowplow competition. These activities will provide inspirational, real-world applications to motivate student learning.

Peter Seiler | Demoz Gebre-Egziabher | Jason Rife | Sam Guyer

Other available formats:

Managing Uncertainty in the Design of Safety-Critical Aviation Systems
Switch to normal viewerSwitch to experimental viewer

Aerospace Automotive Certification CPS Domains Avionics Smart Grid Control Defense Energy Robotics Transportation Validation and Verification Foundations safety critical systems Tufts University University of Minnesota National CPS PI Meeting 2015 2015 Abstract Poster Academia 2015 CPS PI MTG Videos, Posters, and Abstracts