Managing Uncertainty in the Design of Safety-Critical Aviation Systems

Peter Seiler, Demoz Gebre-Egziabher*, Jason Rife, and Sam Guyer†

1 Overview

New methods for design, verification and validation of cyber-physical aviation systems are urgently needed, as exemplified by the development programs for a wide range of systems including the Boeing 787 Dreamliner and the FAA's ground based augmentation system (GBAS) for precision GPS landing. The 787 program has more than 50 suppliers spread across 135 global sites. The program was delayed multiple times due to many factors including issues with the supply chain, flight control software, and structural weaknesses in the fuselage [5, 7, 6]. The 787 certification process included 200,000 hours of review by FAA technical experts [4] and yet it had to be grounded shortly after entering service due to fire safety concerns associated with the novel design of its electrical system [1]. In the case of GBAS, the 1999 Federal Radionavigation Plan [2] stated that the FAA expected GBAS "Category II/III precision approach systems to be available for public use by 2003 at a few selected airports." Certification challenges delayed GBAS such that the system was first certified for limited use (Category I precision-approach) in 2009 [3], six years behind schedule. As of today, the effort to certify Category II/III GBAS continues.

Novel approaches are needed for designing and certifying safety critical aviation systems, and in particular systems consisting of tightly integrated components produced by a great many independent engineering organizations. The following research areas have the potential to reduce the inefficiencies and conservatism that exist in current design methods for complex, cyber-physical systems.

1. Use a probability-density-based method for converting system-level requirements to component-level requirements and create tools to bound the performance of dynamical components.

2. Develop a framework for the design and verification of software components for cyber-physical systems that uses recent work in runtime error detection and error tolerance to reduce programming effort, improve robustness, and provide a probabilistic model of software failure.

3. Apply techniques from Extreme Value Theory to develop adaptive verification and validation procedures that shorten the time required for certification of complex cyber-physical systems.

As shown in Figure 1, these three areas directly seek to reduce the costs and development time (horizontal and vertical axes of figure, respectively) throughout the entire design cycle. The first area is a novel method using probability density functions (PDFs) to decompose specifications in the early conceptual phases of the project. The methods of Area 1, by providing a distribution of allowable specifications rather than a single value, will effectively relax design constraints, thereby facilitating faster, cheaper product development in the detailed design phase. This approach requires new tools for detailed analysis and verification. Area 1 requires new tools to bound the stochastic performance of the system, thereby formalizing and streamlining certain debate-intensive verification procedures currently conducted by forming a consensus of expert opinions. Area 2 extends the concepts for probabilistic system-level modeling to apply more broadly to complex software components. Traditionally, the performance of software components has been modeled as deterministic for the purposes of system-level analysis (e.g., probability of failure is zero given thorough initial validation). For complex software systems paired with dynamic physical systems, it is increasingly difficult to perform a truly complete validation in advance. As such, two techniques are proposed for modifying safety-critical CPS: real-time monitoring of software performance and software design for probabilistic error-tolerance. Together these tools will both streamline validation requirements and enable a more formal, more representative means

*P. Seiler and D. Gebre-Egziabher are with the University of Minnesota, (seiler@aem.umn.edu and gebre@aem.umn.edu)
†J. Rife and S. Guyer are Tufts University, (jason.rife@tufts.edu and sguyer@cs.tufts.edu)

to account for probabilistic variations in the performance of software components that impact overall system-level performance. Finally, Area 3 focuses on the prototype validation and testing phase of design. Here we propose using tunable models, obtained from Extreme Value Theory (EVT), to estimate performance conservatively and thereby put products into service earlier. The use of EVT would enable early entry into service at first with limited functionality but adapting to more aggressive levels of performance as justified by continual logging of validation data from in-service products. This approach would transform today's binary certification process (product either meets or does not meet specifications) into a continual certification process. We hypothesize that these three novel approaches, taken together, will significantly reduce the time and cost required to design, certify, and maintain safety-critical CPS over the lifetime of the system.

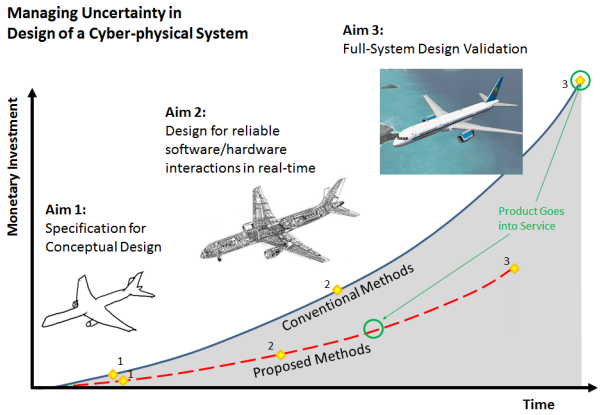

Figure 1: Comparison of anticipated development costs for complex cyber-physical systems using conventional and proposed methods.

2 Motivation

This position statement addresses the basic challenge of managing uncertainty in the design of safety-critical aviation systems. The proposed research areas are motivated by the cyber-physical systems envisioned for the next generation airspace system, known as NextGen. If successful, NextGen will double or triple the capacity of the national airspace with no reduction in safety. In order to achieve this goal, new CPS design and verification methods are needed. To appreciate the key challenges associated with the design of this cyber-physical system, consider one aspect of flight operations that will be important in NextGen. This is the precision approach to landing operation depicted graphically in Figure 2. Precision approach systems provide lateral (distance from airport) and vertical (height above the ground) information to allow safe landing of aircraft in inclement weather conditions, which may obscure from view the destination airport, the approach path, and obstacles along the approach path. In such conditions, most of the flying along the approach path is accomplished by the on-board automatic control system. A typical approach lasts less than 10 minutes during which the *Total System Error* (TSE) is required to be less than some threshold value T. This threshold is selected such that the probability of a hazard P_H during approach is below a required value such as 10^{-6} to 10^{-9}. In the simple approach depicted in Figure 2 the risk is that of collision with the terrain below. TSE is a stochastic quantity whose value is estimated in real-time and compared to the threshold value T. If $|TSE| > T$ at any point in time then an alarm is issued and the approach is discontinued. The threshold value T is selected to balance the probability of a missed detection against the false alarm rate.

The TSE is the key performance metric for the design of the cyber-physical system for precision landing. It is a complex function of the *Path Definition Error* or PDE (guidance system errors); the *Navigation System Error* or NSE (estimation error of navigation sensor fusion algorithms); and *Flight Technical Error* or FTE (control system tracking error). The PDE, NSE and FTE are, in turn, complex functions of measurements from an array of sensors, information from databases, software implementations of the estimation/guidance/control algorithms and hardware devices. For example, the control system hardware consists of multiple and redundant actuators and sensors. These are coupled with controls system software

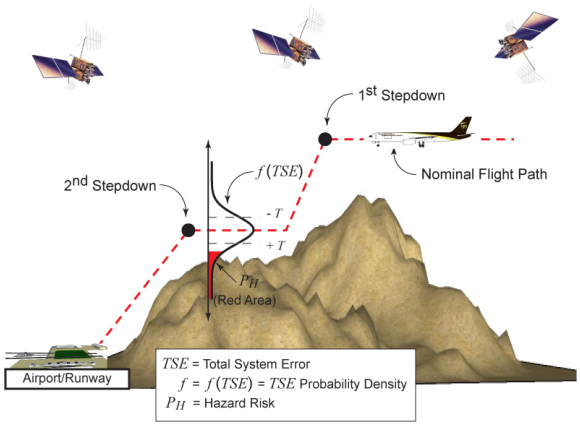

Figure 2: Typical Profile for a Precision Landing.

and algorithms hosted on multiple flight computers. The automatic control system is driven by inputs from a navigation system. The navigation system, in turn, consists of a large number of heterogeneous sensors which are integrated via a complex sensor fusion algorithm. Navigation sensors can be located both on- and off-board the aircraft. For example, off-board sensors include ground based navigation reference stations, communication radio transmitters for relaying time-sensitive navigation information to the aircraft and a satellite-based navigation system broadcasting navigation signals. Underlying all of this is a web of software processes. These various systems must interact to enable a safe landing of an aircraft.

Current design practice involves dividing and allocating portions of the hazard risk to each sub-system. Thus, the control sub-system design must keep FTE below some threshold and will issue an alarm when it cannot satisfy this requirement. Similarly, the guidance and navigation sub-systems will issue alarms when PDE and NSE exceed threshold values. Such decompositions and allocations are a convenient way to design these systems especially when we consider the fact that each system is designed by a different manufacturer. However, this approach is conservative because it assumes that a fault in any one sub-system is automatically hazardous. In fact, a single fault may not be hazardous, as in the example of precision approach into mountainous airports requiring several step-downs as shown in Figure 2. At each step-down point, the control system must change the airplane configuration. When changing configuration at the step-downs the FTE may exceed the threshold values allocated to it. Suppose, however, NSE and PDE are small such that the composite TSE is smaller than its threshold value even if FTE is not. While this is a safe condition, under current design practices the system would raise an alarm forcing the aircraft to abort the approach, an unnecessary and even dangerous procedure (given that FTE is less than its threshold value).

References Cited

[1] Federal Aviation Administration. Emergency Airworthiness Directive 2013-02-51. Technical Report AD 2013-02-51, Federal Aviation Administration, Washington D.C, January 2013.

[2] 1999 federal radionavigation plan. U.S. Department of Transportation and U.S. Department of Defense Report DOD-4650.5/DOT-VNTSC-RSPA-98-1, December 1999.

[3] FAA approves 1st u.s. ground based augmentation system. FAA Press Release, September 2009.

[4] FAA will review Boeing 787 design and production. FAA Press Release, January 2013.

[5] J. Gunsalus. Delays 787's first flight to November-December. Bloomberg, September 2007.

[6] T. Kelly. Dreamliner carries its first passengers and boeing's hopes. Reuters, October 2011.

[7] J. Ostrower. Boeing 787 dreamliner lifts off on maiden flight. *Flightglobal*, December 2009.