Robustness Analysis of Safety-Critical Systems

Gary Balas, Peter Seiler, *Andrew Packard†

1 Overview

Increased flight safety is key to reducing the frequency and severity of aircraft accidents. Flight safety system reliability and integrity requirements are typically on the order of 10^{-9} failures per flight hour or less [3, 2]. Next generation aircraft will have integrated vehicle health management, fault detection, envelope protection, flight control and crew interfaces to reduce loss of control events and ensure flight safety. These systems will include nonlinear and adaptive control laws, stochastic decision-based reasoning, fault accommodation logic, and learning algorithms. Validating that the individual algorithms and combined system are performing their intended function under all possible conditions is critical to achieving flight safety reliability and integrity requirements.

Validation of safety critical systems plays a similarly important role in other domains including automotive (e.g. autonomous full-authority braking and adaptive cruise control) and medical devices (e.g. inplantable infusion pumps, gastric simulators, and pacemakers). **The basic challenge facing the systems community is the lack of tools and unified process to carry out the validation of integrated safety critical systems.** Developing analytical tools and a rigorous validation process, applicable to a diverse set of adaptive algorithms, is a priority to ensure that aircraft safety (vehicle, medical device or similar safety critical system) requirements are satisfied during nominal and off-nominal operation [3, 8].

The following research questions form important sub-problems that address the validation challenge:

1. **Nonlinear Robustness Analysis:** Can nonlinear analysis techniques be developed which provide certification and validation of adaptive algorithms? Current certification and validation procedures for flight control systems involve analytical, simulation based and experimental techniques. This mainly consists of linearizing the aircraft dynamics around numerous trim conditions and using linear analysis tools to assess the stability and performance characteristics. The linear analysis results are supplemented with Monte Carlo simulations of the full nonlinear equations of motion to provide further confidence in the system performance and to uncover nonlinear dynamic characteristics, e.g. limit cycles. Hence, current practice involves extensive linear analysis at different trim conditions and probabilistic nonlinear simulation results. The gap between linear

*G. Balas and P. Seiler are with the Department of Aerospace Engineering and Mechanics, University of Minnesota, (balas@umn.edu and seiler@aem.umn.edu)

†A. Packard is with the Department of Mechanical Engineering, University of California, Berkeley, (apackard@berkeley.edu)

analysis and Monte Carlo simulations can cause significant nonlinear effects to go undetected [4, 5]. Nonlinear analysis tools need to be developed to fill this gap. We hypothesize that the combination of Integral Quadratic Constraints (IQCs) [6] and Sum of squares (SOS) optimization [7, 1] analysis techniques would expand the ability to theoretically validate nonlinear and adaptive systems.

2. **Computational Tools for Analysis of Nonlinear Systems:** How will theoretical advances in nonlinear analysis be transitioned to industry? For tools to be effective on real-world problems, they need to be scalable and readily available. Hence high quality nonlinear robustness analysis computational software tools which transition theory to practice are necessary. A merged IQC/SOS theory is one approach to nonlinear robustness analysis for validation that offers the benefit that computational tools can be developed to analyze nonlinear safety critical systems. Nonlinear robustness analysis tools for real-world safety critical systems would offer a significant advance of current state-of-the-art analysis tools

3. **Analysis of Large-scale Complex Systems:** Can accurate, reduced order models be developed for analysis which provide guarantees regarding the original large-scale complex system? The complexity of flight control problems (and other safety critical systems) often dictates a decomposition approach, [51], first representing the system as an interconnection of smaller subsystems. Individual analysis on the isolated subsystems establishes coarse properties of the subsystems. We hypothesize that a mixture of SOS and IQC analysis, with knowledge of only coarse properties subsystems and interconnection topology is adequate to verify the overall behavior. Any advances in this direction would dramatically close the gap between nonlinear analysis theory and real-world applications.

References Cited

[1] G.J. Balas, A. Packard, P. Seiler, and U. Topcu. Robustness analysis of nonlinear systems. http://aem.umn.edu/∼AerospaceControl/, 2009.

[2] R.J. Bleeg. Commercial jet transport fly-by-wire architecture considerations. In *AIAA/IEEE Digital Avionics Systems Conference*, pages 399–406, 1988.

[3] H. Buus, R. McLees, M. Orgun, E. Pasztor, and L. Schultz. 777 flight controls validation process. *IEEE Transactions on Aerospace and Electronic Systems*, 33(2):656–666, 1997.

[4] A. Chakraborty, P. Seiler, and G.J. Balas. Susceptibility of f/a-18 flight controllers to the falling-leaf mode: Linear analysis. *AIAA Journal of Guidance, Control, and Dynamics*, 34(1):57–72, 2011.

[5] A. Chakraborty, P. Seiler, and G.J. Balas. Susceptibility of f/a-18 flight controllers to the falling-leaf mode: Nonlinear analysis. *AIAA Journal of Guidance, Control, and Dynamics*, 34(1):73–85, 2011.

[6] A. Megretski and A. Rantzer. System analysis via integral quadratic constraints. *IEEE Trans. on Automatic Control*, 42(6):819–830, 1997.

[7] P. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming Ser. B*, 96(2):293–320, 2003.

[8] J. Wilborn and J. Foster. Defining commercial transport loss-of-control: A quantitative approach. Providence, RI, August 2004. AIAA-2004-4811.