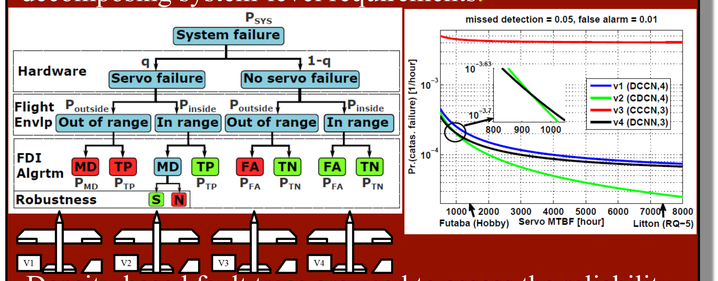
CPS: Synergy: Collaborative Research: Managing Uncertainty in the Design of Safety-Critical Aviation Systems

NSF/CNS-1329390
Peter Seiler and Demoz Gebre-Egziabher
University of Minnesota

NSF/CNS-1329341
Jason Rife and Sam Guyer
Tufts University

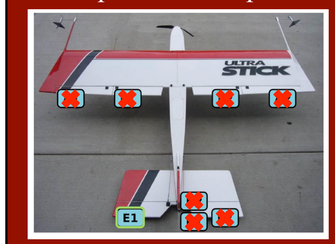
Aim 1: Convert system requirements to component-level requirements using a probability density function approach.

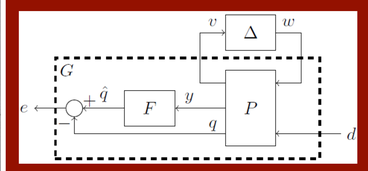
Task 1.A - Derive density-function methodology for decomposing system-level requirements.



Density-based fault trees are used to assess the reliability of actuator architectures for unmanned aircraft.

Task 1.B - Investigate techniques for computing bounds on the probabilistic performance of a system.





Integral quadratic constraints provide a framework to design and analyze fault estimators for uncertain systems.

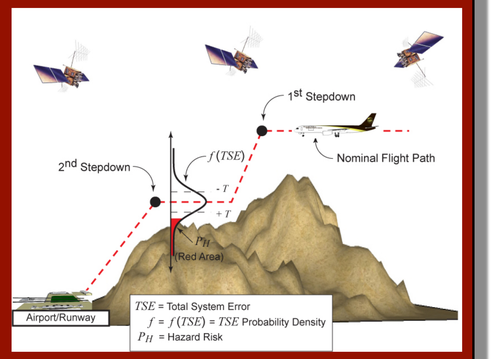
[1] R. Venkataraman and P. Seiler, "Safe Flight Using One Aerodynamic Control Surface," AIAA SciTech, 2016, Paper No. AIAA-2016-0634.

[2] R. Venkataraman and P. Seiler, "Robust LPV estimator synthesis using integral quadratic constraints," 2016 American Control Conference (ACC), Boston, MA, 2016, pp. 4611-4616.

Overview

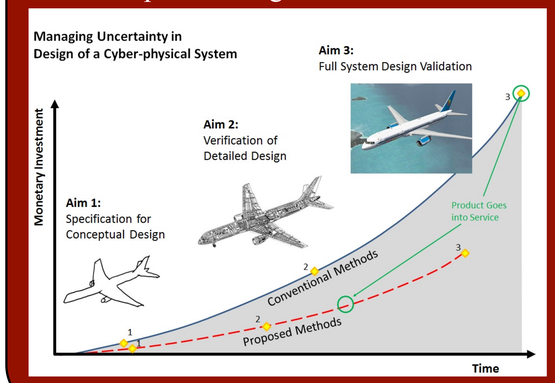
Issue: Aviation systems require hardware (physical) and software (cyber) components designed by many engineering teams to be safely integrated.

Objective: Create tools to manage uncertainty in the design and certification process of safety-critical aviation systems, e.g. NextGen.



Typical Profile for a Precision Landing

Development Costs for Conventional and Proposed Design Methods



Impacts:

Significant reduction in the costs and time required for fielding new aviation systems.

Applications to other complex systems including smart power grids and automated highways.

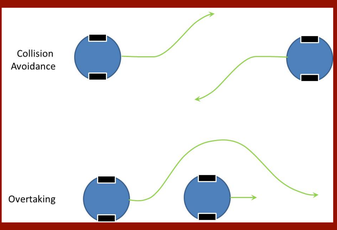
Outreach and Education: Engage engineering students in hands-on, CPS-centric projects.

Robotic Snowplow Competition

Student competition to design, build and operate an autonomous snow plow. Competition rules are now being modified to incorporate a CPS-challenge starting with the 2015 competition cycle.

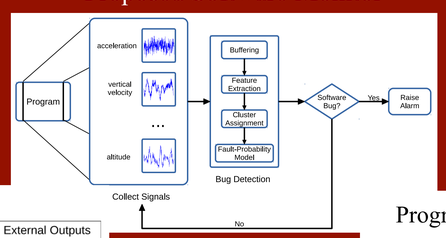
CPS Curriculum Development

Use sim. and hardware experiments in intro. control course to explore hybrid controls (as example CPS application).

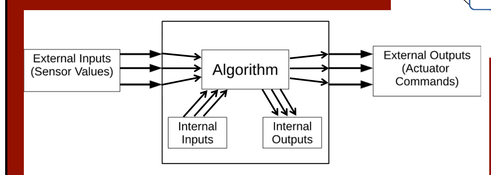


Aim 2: Develop a framework for software design and verification that incorporates probabilistic software failure models.

Proposed Software Monitor

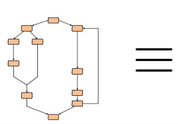


What Variables to Monitor?

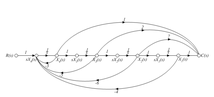


Slicing Provides an Answer

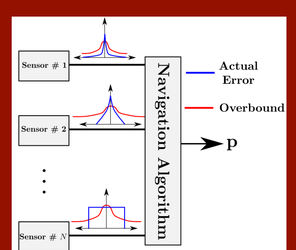
Program Slice



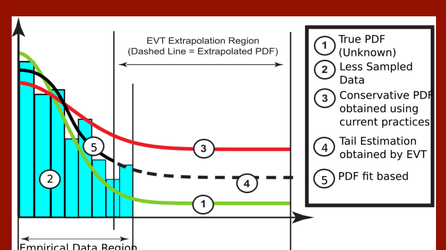
Signal Flow-Graph



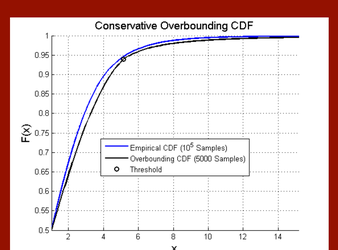
Aim 3: Apply techniques from Extreme Value Theory (EVT) to develop adaptive verification and validation procedures that shorten the time required for certification of complex cyber-physical systems.



Current V&V methods use Gaussian distributions to overbound actual sensor errors and thereby overbound the overall system uncertainty.



EVT offers a more data-efficient way to overbound the tails of unknown distributions by leveraging a different statistical model.



Combining EVT tail overbounding and Gaussian core overbounding could potentially provide conservative CDFs using 95% less data.

[3] J. Larson and D. Gebre-Egziabher, "Conservatism Assessment of Extreme Value Theory Overbounds," IEEE Transactions on Aerospace Electronic Systems, *Under Review*