NASA SBIR 2011 Phase I Solicitation

A1.16 Validation Methods for Safety-Critical Systems Operating under LOC Conditions

Lead Center: LaRC

Participating Center(s): AFRC, ARC, GRC

Validation of future complex integrated systems designed to ensure flight safety under off-nominal conditions associated with aircraft loss of control is a significant challenge. Future systems will ensure vehicle flight safety by integrating vehicle health management functions, resilient control functions, flight safety assessment and prediction functions, and crew interface and variable autonomy functions. Each of these functions is characterized by algorithmic diversity that must be addressed in the validation process. Vehicle health management involves diagnostic and prognostic algorithms that utilize stochastic decision-based reasoning and extensive information processing and data fusion. Resilient control functions can involve adaptive control algorithms that utilize time-varying parameters and/or hybrid system switching. Flight safety management may involve diagnostic and prognostic reasoning algorithms as well as control theoretic algorithms. Crew interface functions involve displays that are human-factors-based and require information processing and reasoning, and variable autonomy will require assessment and reasoning algorithms. Onboard modeling functions will involve system identification algorithms and databases. Normal operating conditions of the future may extend beyond current-day operational limits. Moreover, safe operation under off-nominal conditions that could lead to loss-of-control events will be a focus of the system design. In particular, operation under abnormal flight conditions, external hazards and disturbances, adverse onboard conditions, and key combinations of these conditions will be a major part of the operational complexity required for future safety-critical systems. Future air transportation systems must also be considered under operational complexity, such as requirements for dense all-weather operations, self separation of aircraft, and mixed capabilities of aircraft operating in the same airspace, including current and future vehicle configurations as well as piloted and autonomous vehicles.

System validation is a confirmation that the algorithms are performing the intended function under all possible operating conditions. The validation process must be capable of identifying potentially problematic regions of operation (and their boundaries) and exposing system limitations - particularly for operation under off-nominal and hazardous conditions related to loss of control. New methods, metrics, and software tools must be established for algorithms that cannot be thoroughly evaluated using existing methods. Innovative research proposals are sought to address any of the following areas:

- Analytical Validation Methods.
- Predictive Capability Assessment Methods.

- Real-Time (or Run-Time) Validation Methods.

Analytical validation methods are comprised of a set of analytical methods and tools that facilitate the accurate prediction of system properties under various operating and off-nominal conditions. A wide variety of analytical methods will be needed to evaluate stability and performance of various and dissimilar system functions, robustness to adverse and abnormal conditions, and reliability under errors, faults, failures, and damage. These methods and software tools will be utilized offline and prior to implementation in representative avionics system software and hardware. These methods will enable analysis under a wide range of conditions, and be used to facilitate nonlinear simulation-based and experimental evaluations under selected potentially problematic conditions in order to expose system deficiencies and limitations over a very large operational space. Analytical methods and tools applicable to determining stability, performance, robustness, and reliability of nonlinear, time-varying, and/or hybrid systems involving control theoretic, diagnostic/prognostic, and/or reasoning systems are sought.

Predictive capability assessment is an evaluation of the validity and level of confidence that can be placed in the validation process and results under nominal and off-nominal conditions (and their associated boundaries). The need for this evaluation arises from the inability to fully evaluate these technologies under actual loss-of-control conditions. A detailed disclosure is required of model, simulation, and emulation validity for the off-nominal conditions being considered in the validation, interactions that have been neglected, assumptions that have been made, and uncertainties associated with the models and data. Cross-correlations should be utilized between analytical, simulation and ground test, and flight test results in order to corroborate the results and promote efficiency in covering the very large space of operational and off-nominal conditions being evaluated. The level of confidence in the validation process and results must be established for subsystem technologies as well as the fully integrated system. This includes an evaluation of error propagation effects across subsystems, and an evaluation of integrated system effectiveness in mitigating off-nominal conditions and preventing cascading errors, faults, and failures across subsystems. Metrics for performing this evaluation are also needed. Uncertainty-based and/or statistical-based methods and tools that enable the determination of level of confidence in the validation of uncertain systems operating under extreme conditions are sought.

Real-time (or run-time) validation methods are needed for the onboard monitoring of crucial system properties whose violation could compromise safety of flight. These properties might include closed-loop stability, robustness margins, or underlying theoretical assumptions that must not be violated. This information could be used as part of a real-time safety-of-flight assessment system for the vehicle. Real-time methods and software tools are sought that enable onboard validation of nonlinear, time-varying, and reasoning systems.