# Validation and Verification of Future Integrated Safety-Critical Systems Operating under Off-Nominal Conditions

Christine M. Belcastro*
*NASA Langley Research Center, Hampton, Virginia, 23681*

**Loss of control remains one of the largest contributors to aircraft fatal accidents worldwide. Aircraft loss-of-control accidents are highly complex in that they can result from numerous causal and contributing factors acting alone or (more often) in combination. Hence, there is no single intervention strategy to prevent these accidents and reducing them will require a holistic integrated intervention capability. Future onboard integrated system technologies developed for preventing loss of vehicle control accidents must be able to assure safe operation under the associated off-nominal conditions. The transition of these technologies into the commercial fleet will require their extensive validation and verification (V&V) and ultimate certification. The V&V of complex integrated systems poses major nontrivial technical challenges – particularly for safety-critical operation under highly off-nominal conditions associated with aircraft loss-of-control events. This paper summarizes the V&V problem and presents a proposed process that could be applied to complex integrated safety-critical systems developed for preventing aircraft loss-of-control accidents. A summary of recent research accomplishments in this effort is also provided.**

## Nomenclature

| | | |
|---|---|---|
| $\alpha$ | = | aircraft angle of attack |
| $\beta$ | = | aircraft angle of sideslip |
| AvSP | = | Aviation Safety Program |
| AIRSAFE | = | Aircraft Integrated Resilient Safety Assurance and Failsafe Enhancement |
| BRS | = | Base Research Station |
| CFD | = | Computational Fluid Dynamics |
| FAA | = | Federal Aviation Administration |
| FAR | = | Federal Aviation Regulation |
| FASTER | = | Full-Scale Aircraft Structural Test Evalutaion and Research |
| FUN3D | = | Fully Unstructured 3D |
| JAA | = | Joint Aviation Authorities in Europe |
| JAR | = | Joint Aviation Regulation in Europe |
| GTM | = | Generic Transport Model |
| HIRF | = | High Intensity Radiated Fields |
| INS/GPS | = | Inertial Navigation System / Global Positioning System |
| LANL | = | Los Alamos National Laboratory |
| LFR | = | Linear Fractional Representation |
| LOC | = | Loss of Control |
| LPV | = | Linear Parameter Varying |
| MOS | = | Mobile Operations Station |
| NASA | = | National Aeronautics and Space Administration |
| ONERA | = | French Aerosapce Laboratory |
| SAFETI | = | Systems and Airframe Failure Emulation, Testing, and Integration |
| USM3D | = | Unstructured Method 3D |
| V&V | = | Validation and Verification |

*Senior Researcher, Dynamic Systems and Control Branch, MS 308, E-Mail: christine.m.belcastro@nasa.gov; AIAA Senior Member.

## I. Introduction

Aircraft loss-of-control accidents can result from numerous causal and contributing factors that are collectively referred to in this paper as "off-nominal conditions". "Off-nominal" conditions include adverse conditions occurring onboard the vehicle, external hazards and disturbances, and abnormal flight conditions. Adverse onboard conditions include: vehicle impairment (including inappropriate vehicle configuration, contaminated airfoil, and improper vehicle loading); system faults, failures, and errors (resulting from design flaws, software errors, or improper maintenance actions); vehicle damage to airframe and engines (resulting from fatigue cracks, foreign objects, overstress during upsets or upset recovery); and inappropriate crew response (including pilot-induced oscillations, spatial disorientation, mode confusion, ineffective recoveries, and crew impairment). External hazards and disturbances include: poor visibility; wake vortices; wind shear, turbulence, and thunderstorms; snow and icing conditions; and obstacles requiring abrupt maneuvers or resulting in collisions. Vehicle upsets include: abnormal attitude; abnormal airspeed, angular rates, or asymmetric forces; abnormal flight trajectory; uncontrolled descent (including spiral dive); and stall/departure (including falling leaf and spin). Aircraft loss-of-control (LOC) accidents result from these off-nominal conditions occurring either individually or (more often) in combination. Worst case combinations and sequences associated with these LOC precursor conditions have recently been analyzed for 126 accidents that occurred between 1979 and 2009 and resulted in 6087 fatalities.[1]

Current aircraft autoflight systems are primarily designed for operation under nominal conditions, and often disengage (i.e., return control authority to the pilot) under off-nominal conditions. Future aircraft control systems will provide resilience under off-nominal conditions and operate as a component of a larger resilient flight system.[2] Control resilience will be designed to provide the capability to mitigate off-nominal conditions and provide recovery back to a stable operational mode (whenever possible). This capability will be developed as part of a holistic approach to reduce aircraft loss-of-control accidents. The broader resilient flight system will include vehicle health management, flight safety assurance, and safety-based crew interface functions.

Validation and verification (V&V) becomes much more difficult for safety-critical resilient systems operating under off-nominal conditions. The objectives of this paper are to address V&V issues associated with future safety-critical resilient flight systems operating under off-nominal conditions, to propose a comprehensive V&V research framework to address these issues, and to provide a summary of recent research in this area. In this paper, the term "validation" refers to a confirmation that the algorithms are performing their intended function as well as an affirmation of their effectiveness in these functions. "Verification" in this paper relates to a confirmation that the system implementation in software and hardware is correctly executing the algorithms as designed (and validated). Section II defines the V&V problem associated with future resilient flight systems, describes problem complexity and key technical challenges, identifies V&V process requirements, and summarizes the research approach being taken. Section III proposes a comprehensive V&V process that can serve as an initial research framework for addressing future integrated resilient flight systems. Section IV summarizes the status of this research and presents selected research accomplishments at NASA Langley. Finally, Section V provides a summary and some concluding remarks. It should be noted that the primary focus of this paper is on the validation component of V&V for advanced flight control systems.

## II. Validation & Verification (V&V) Problem

The validation and verification problem is discussed here relative to a future onboard system concept, called the Aircraft Integrated Resilient Safety Assurance and Failsafe Enhancement (AIRSAFE) System, that was presented in Ref. 2 for addressing aircraft loss-of-control. The AIRSAFE concept is shown in Figure 1.

The colors of Figure 1 designate the four core technology areas (or subsystems) needed to address aircraft loss of control. Green blocks represent vehicle health management functions, yellow blocks represent crew interface management functions, blue blocks represent resilient control and flight safety management functions, and purple represents modeling and simulation functions for off-nominal conditions. Multi-colored blocks represent shared functions between multiple technology areas. The validation and verification (V&V) of future integrated systems, such as the AIRSAFE System concept of Figure 1, poses numerous technical challenges. In particular, there is currently no comprehensive V&V process for complex integrated safety-critical systems operating under off-nominal conditions. Subsection A presents the certification requirements for transport aircraft onboard systems,

Subsection B discusses V&V problem complexity and technical challenges, Subsection C summarizes V&V process requirements, and Subsection D summarizes the research approach being taken to address this V&V problem.

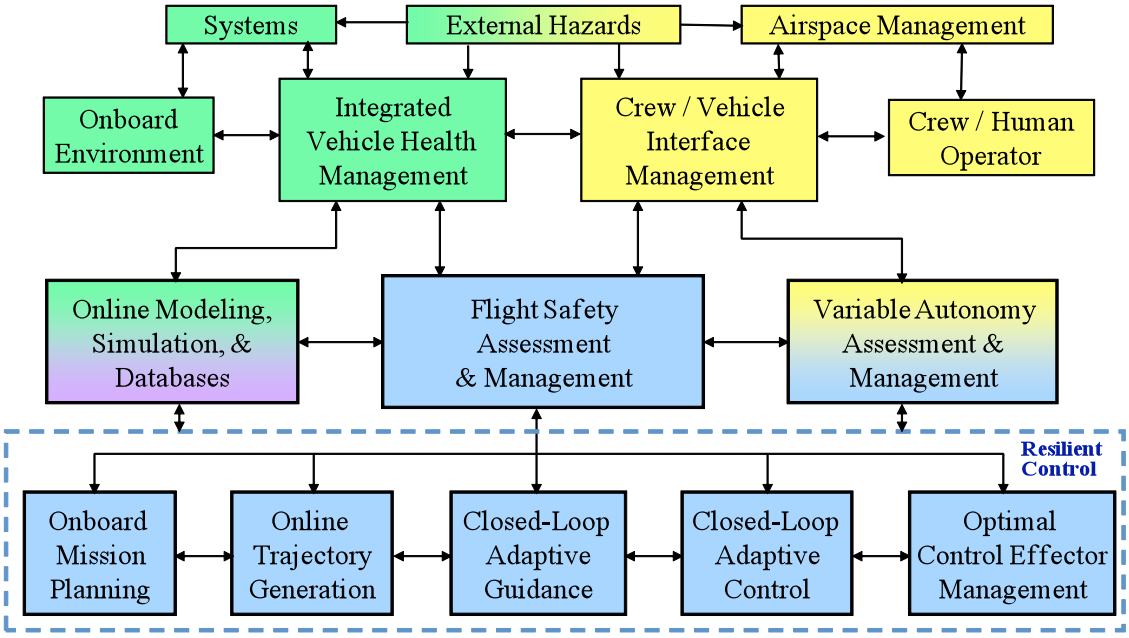


**Figure 1. Aircraft Integrated Resilient Safety Assurance & Failsafe Enhancement (AIRSAFE) System.**

### A. Certification Requirements

The V&V process must ultimately lead to system certification. The Federal Aviation Administration (FAA) in the United States and the Joint Aviation Authorities (JAA) in Europe have developed extensive (and compatible) certification specifications. The Federal Aviation Regulation (FAR) and Joint Aviation Regulation (JAR) Part 25 provides the certification specifications for transport category aircraft, and Section 1309 applies to equipment and systems installed onboard aircraft. An excerpt from FAR 25.1309 is provided below (and JAR 25.1309 is nearly identical).

*Part 25 AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES*

*Sec. **25.1309**: Equipment, systems, and installations.*

*(a) The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.*

*(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that—*
- *(1) The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and*
- *(2) The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.*

*(c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards.*

*(d) Compliance with the requirements of paragraph (b) of this section must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider—*
- *(1) Possible modes of failure, including malfunctions and damage from external sources.*
- *(2) The probability of multiple failures and undetected failures.*
- *(3) The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and*
- *(4) The crew warning cues, corrective action required, and the capability of detecting faults.*

In the above regulation, "extremely improbable" failures are those having a probability of $10^{-9}$ or less, and "improbable" failures have a probability of $10^{-5}$ or less. The development of a V&V process for demonstration of compliance to FAR/JAR 25.1309 is highly nontrivial for complex integrated systems designed for operation under off-nominal conditions, such as the AIRSAFE System concept of Figure 1. In fact, the V&V problem even for the core subsystems of AIRSAFE poses a key technology barrier to their implementation and transition into the fleet. For example, there are currently no comprehensive V&V processes for certifying advanced safety-critical control systems (commercial or military) for effective operation under off-nominal conditions, especially for adaptive and potentially non-deterministic systems. Similarly, there are no comprehensive V&V processes for diagnostic, prognostic, and reasoning systems or for variable autonomy systems. High-confidence V&V of these advanced systems is a complex problem with numerous technical challenges.

### B. V&V Problem Complexity and Technical Challenges

V&V problem complexity can be discussed in terms of system complexity, operational complexity, and V&V process complexity. System complexity arises from integrating vehicle health management functions, resilient control functions, flight safety assessment and prediction functions, and crew interface functions. Each of these functions is characterized by algorithmic diversity that must be addressed in the V&V 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 real-time residual-based adjustment of control parameters and/or hybrid system switching. Flight safety management may involve diagnostic and prognostic reasoning algorithms as well as controls-related algorithms. Crew interface functions involve displays that are human-factors-based and require information processing, and variable autonomy will require assessment and reasoning algorithms. All three core functions are software based and will involve various levels of logic and discrete mathematics-based algorithms. Subsystem integration may also involve significant implementation and functional complexity. As indicated in Ref. 2, the AIRSAFE System is a long-term research and technology development concept whose full functionality would be integrated using a phased implementation strategy over time. Implementation complexity may arise from the associated software and hardware complexity, such as the development of a modular system architecture that enables the integration of new or enhanced capabilities within each core subsystem over time. The associated functional integration complexity might arise from the integration (and validation) of new or enhanced subsystem features within the integrated system, as well as error propagation prevention and containment between subsystems.

The second aspect of V&V complexity arises from operational complexity. Normal operating conditions of the future may extend beyond current-day operational limits. Moreover, operation under off-nominal conditions that can cause loss-of-control events (i.e., accidents and incidents) 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 (e.g., current and future vehicle configurations as well as piloted and autonomous vehicles).

The third aspect of V&V complexity pertains to the V&V process itself. 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. Simulation methods will require the development of high-fidelity models that characterize off-nominal conditions and their multidisciplinary effects on the vehicle. The capability for multidisciplinary susbsystem integration must also be available in a simulation environment, as well as the inclusion of pilot-in-the-loop effects. Simulation capability must range from desk-top batch operation to hardware/pilot-in-the-loop fixed/motion-based cockpit evaluations. Experimental test capability must include ground and flight testing of hardware/software systems, allow for multidisciplinary subsystem integration, and enable realistic emulation of off-nominal conditions. The V&V process must itself be assessed for its predictive capability to effectively infer safe system operation under off-nominal conditions associated with aircraft loss-of-control events that cannot be fully replicated during V&V. The V&V process assessment must be able to quantify a level of confidence in this inference.

Operation under off-nominal conditions over a wide envelope of flight conditions results in a very large operational space with multidisciplinary coupled effects (such as vehicle damage and upsets). Vehicle damage conditions can affect the aerodynamics, airframe structure, propulsion system, and underlying vehicle systems, depending on the nature of the damage. Vehicle upset conditions can affect aerodynamics, airframe structures (due to abnormal loads), and propulsion system performance (due to changes in inlet flow). Due to the huge operational

space, there are too many conditions to fully analyze, simulate, and test. While there are numerous technical challenges associated with this problem, some key technical challenges are summarized below.

- Development and Validation of Physics-Based Off-Nominal Conditions and Effects Models
  - Requires modeling of
    - » adverse onboard conditions (e.g., faults, failures, damage)
    - » abnormal flight conditions (e.g., unusual attitudes, stall, stall/departure, other vehicle upset conditions)
    - » external hazards and disturbances (e.g., icing, wind shear, wake vortices, turbulence)
    - » Worst-Case Combinations (as Determined from LOC Accident/Incident Data)
  - Requires data and/or experimental methods for off-nominal conditions, which may not be available
  - Can involve multidisciplinary coupled effects
  - Cannot fully replicate in-flight loss-of-control environment
- V&V of Adaptive Diagnostic, Prognostic, and Control Algorithms Operating under Off-Nominal Conditions
  - Involves a variety of nonlinear mathematical constructs (inference engines, probabilistic methods, physics-based, neural networks, artificial intelligence, etc.)
  - May involve onboard adaptation that may result in stochastic system behavior
  - Involves fusion and reasoning algorithms for sensor data, information processing, and decisions
  - Requires methods for establishing probabilities of
    - » false alarms and missed detections
    - » incorrect identifications and decisions
    - » loss of stability, recoverability, and control
  - Requires methods & metrics for establishing off-nominal condition coverage, reliability, and accuracy for diverse algorithms & multiple objectives
  - Requires integrated multi-disciplinary system assessment methods
    - » performance assessment
    - » error propagation and effects assessment
    - » inter-operability effectiveness assessment
- System Verification and Safety Assurance
  - Involves large-scale complex interconnected software systems
  - Involves potentially fault tolerant and reconfigurable hardware
  - May involve adaptive and reasoning algorithms with stochastic behavior
  - Requires verification methods for a complex system of systems
- V&V Predictive Capability Assessment
  - Requires methods to demonstrate compliance to certification standards for an extensive set of off-nominal conditions (and their combinations) that cannot be fully replicated
  - Requires methods for determining (and quantifying) level of confidence in V&V process and results for demonstrating compliance

These technical challenges can be utilized in defining V&V process requirements.

### C. V&V Process Requirements

In carrying out V&V of complex integrated safety-critical systems operating under off-nominal conditions, it is necessary to expose system weaknesses and vulnerabilities, and to be able to identify safe and unsafe operational conditions, regions, and their boundaries. This is a key point. It is not sufficient, for example, to demonstrate that a system appears to work in a few selected flight regimes or under a small subset of off-nominal conditions. In fact, it is necessary to define a comprehensive integrated V&V process for these systems, and to utilize this process as a research framework to identify gaps in current V&V capabilities. Moreover, it is critical to define a V&V process that effectively and efficiently utilizes analysis, simulation, and experimental testing to assist in exposing system deficiencies and limitations over a very large operational space. The V&V process must clearly demonstrate compliance to certification specifications (such as FAR/JAR 25.1309), and quantify the level of confidence in this compliance.

Key components of the V&V process include system/subsystem validation, system/subsystem verification, and V&V predictive capability assessment. Each of these V&V components requires the development of methods, tools, and testbeds to perform analysis, simulation / ground testing, and flight testing. Moreover, each method, tool, and testbed must be developed to assess system operation under off-nominal conditions associated with aircraft loss-of-control accidents in order to reduce (or prevent) them in the future. V&V metrics must be defined for the diverse set of algorithms associated with the subsystems and integrated system, and new methods, tools, and testbeds developed (as needed) to assess these metrics. Based on an analysis of the V&V problem[3], the V&V process requirements for future systems designed for operation under off-nominal conditions (such as the AIRSAFE System concept) can be defined as depicted in Figure 2. This figure shows V&V process components, methods, and some example algorithm validation metrics that are required for AIRSAFE subsystem and integrated system technologies. The core V&V methods of analysis, simulation/ground testing, and flight testing are applicable to each of the core V&V components and take on different meanings for each. Metrics must be developed for assessment of each core component using the appropriate methods. Although Figure 2 shows some example metrics for algorithm validation, and illustrates that these are dependent on the algorithm type, metrics are needed for each core V&V component.

System validation is a confirmation that the algorithms are performing the intended function under all possible operating conditions. Validation is not merely a demonstration that the system works under the design condition and selected test conditions, but a comprehensive process that involves analytical, simulation / ground testing, and flight testing. The validation sub-process must be capable of identifying potentially problematic regions of operation (and their boundaries) and exposing system limitations – particularly for operation under off-nominal conditions. Figure 2 presents some of the methods and metrics needed for the analysis, simulation/ground testing, and flight testing of algorithms associated with AIRSAFE System technologies. New methods, tools, testbeds, and metrics must be established for algorithms that cannot be thoroughly evaluated using existing methods. For example, adaptive control systems may require new methods and metrics for their effective analysis. Moreover, methods and metrics may vary depending on the algorithm being considered. For example, stability of detection and prediction algorithms may imply convergence rate and accuracy rather than the traditional control-theoretic meaning of stability. Performance of diagnostic and prognostic algorithms may be characterized by probabilities associated with correct detection and diagnosis of system faults or failures, whereas performance of control systems may be characterized by tracking capability (or evaluation of some other control objective). Robustness for all algorithms must be evaluated relative to uncertainties (e.g., parameter variations and unmodeled system dynamics) and disturbances (e.g., signal and system noise and turbulence). Coverage of off-nominal conditions must also be clearly defined and evaluated for effectiveness in dealing with these conditions. Examples of reliability metrics are given in the figure for detection/prediction and control theoretic algorithms. Variable autonomy algorithms must be evaluated for handling qualities and interface effectiveness, and pilot-induced oscillation (PIO) susceptibility under off-nominal conditions. Moreover, real-time partitioning effectiveness between the human and automation (and the levels of automation that are engaged) must be evaluated under off-nominal (and emergency) conditions. Simulation and ground testing includes traditional batch, real-time, piloted, and hardware-in-the-loop methods, as well as a linked lab capability for the integration and simultaneous evaluation of multidisciplinary technologies. Flight testing includes traditional full-scale testing to evaluate pilot/system interactions, as well as sub-scale testing to evaluate algorithm effectiveness (and dynamics models) under off-nominal conditions that are too risky for full-scale testing.

Verification of the system is a confirmation that the validated algorithms have been correctly implemented in software (and hardware). This is also a nontrivial task. Formal methods are utilized for analytically verifying (with proofs) that the system requirements are fully defined and met by the implementation. Safety assurance of the system implementation must also be verified. Testing of code is performed at various levels of system build-up, including evaluation of the code on representative or actual hardware to be fielded. Flight testing also requires the use of actual hardware systems and flight environments under nominal and off-nominal conditions. Although none are given in Figure 2, verification metrics must be clearly defined and evaluated.

V&V predictive capability assessment is an evaluation of the validity and level of confidence that can be placed in the V&V 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 V&V, as well as interactions that have been neglected and assumptions that have been made. 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 V&V 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. Metrics for performing this evaluation are also needed.

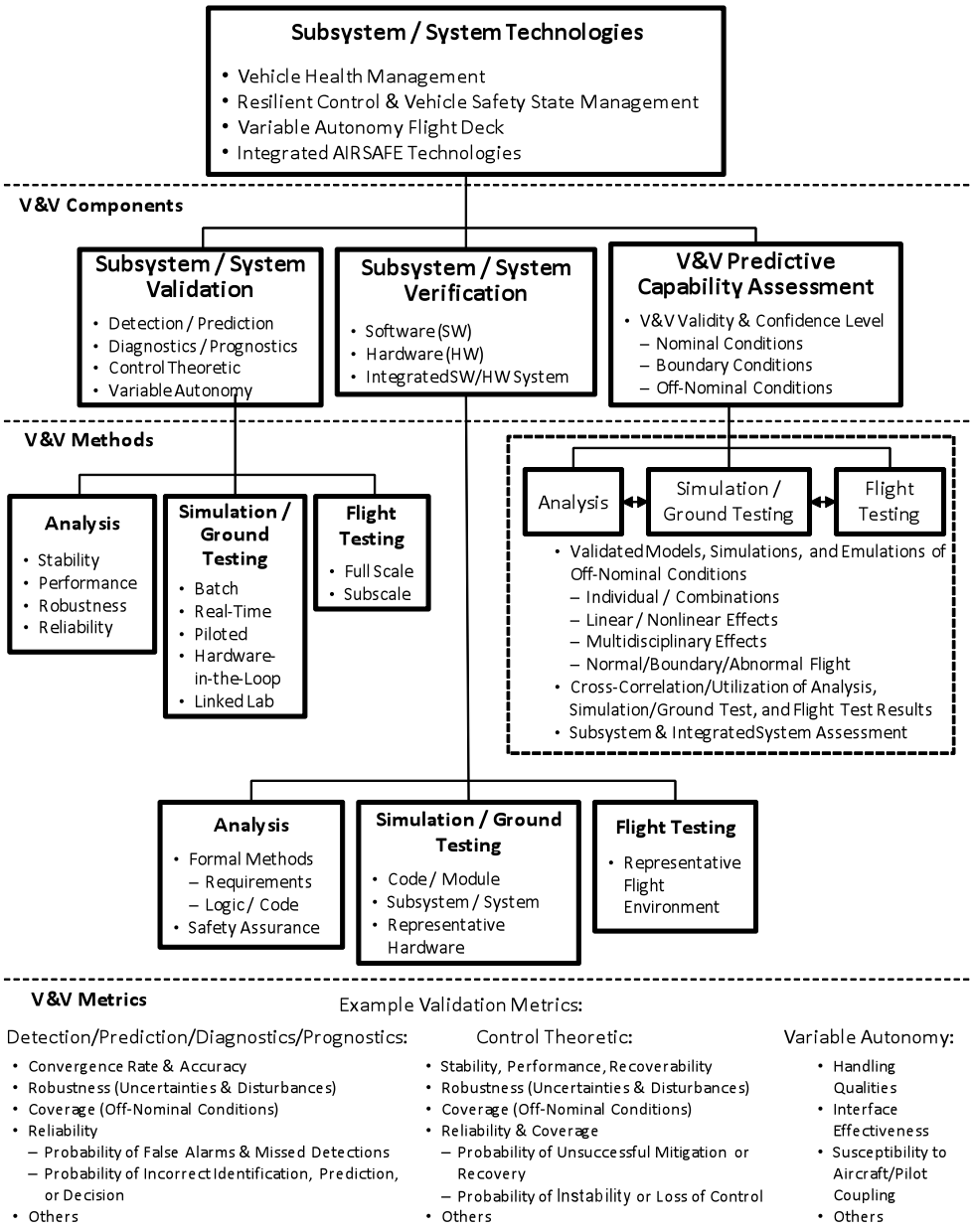


**Figure 2.** V&V Process Requirements for the AIRSAFE System Concept

### D. V&V Research Approach

The approach being taken within the vehicle health management and resilient control systems research and development components within NASA's Aviation Safety Program for addressing the validation and verification of safety-critical systems operating under off-nominal conditions is to develop metrics, methods, software tools, and testbeds that facilitate the evaluation of these systems. A high-level V&V concept has been developed, as described in Section III below, which integrates analytical, simulation, and experimental methods. Analytical methods are

being developed, with theoretical extensions where needed, as well as user-friendly software tools. Simulation methods are being developed to facilitate analysis-guided Monte Carlo and piloted evaluations under off-nominal conditions. In addition, advanced high-fidelity databases, models, and simulation enhancements are being developed to characterize off-nominal conditions and their impacts on vehicle dynamics. Experimental testbeds are being developed to facilitate testing under off-nominal conditions in ground-based laboratory tests as well as in-flight tests. The full integrated V&V process will ultimately be demonstrated, evaluated, and refined using realistic example problems and systems.

## III. Development of a Comprehensive Validation & Verification (V&V) Process

Based on the V&V process requirements of Figure 2, a detailed V&V process can be developed for complex integrated resilient systems, such as the AIRSAFE System concept of Figure 1. A high-level overview of the integrated V&V process is presented in Figure 3. The colors of the blocks correlate to the three primary AIRSAFE subsystem functions depicted in Figure 1 – that is, blue correlates to resilient control functions, green represents health management functions, and yellow is associated with crew interface functions. Multi-colored boxes in Figure 3 represent evaluation of the associated integrated subsystem functions. Analysis, simulation, and experimental V&V components are organized in the V&V process of Figure 3 moving from left to right, and system evaluation becomes more highly integrated moving to the center (from above and below) and to the right. Also as indicated in Figure 3, results from the V&V process are utilized as an iterative process for refining the algorithm design of each subsystem. The remainder of this section will present a more detailed description of the controls-related components of the V&V process (including methods and interfaces). This is depicted in Figure 3 by the dotted red box around the lower two rows of the process. Reference [3] provides a detailed description of the entire process.

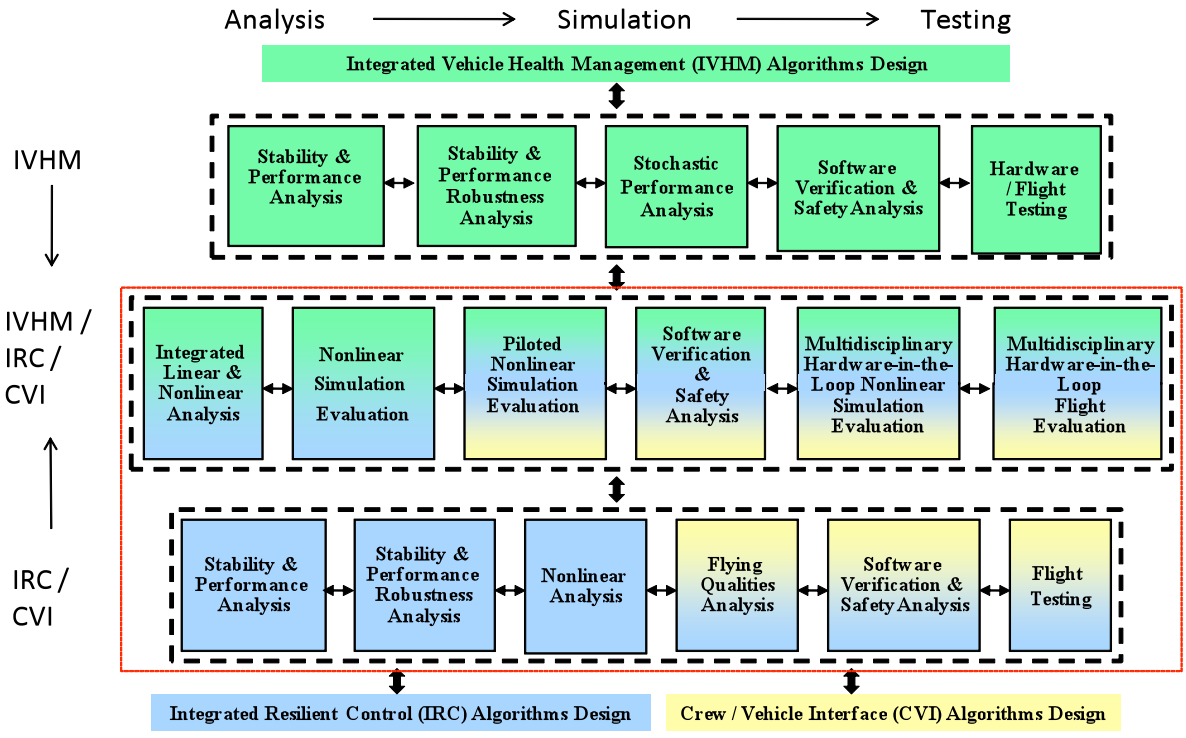


**Figure 3.** V&V Process Overview

A set of recommended V&V methods for resilient control system functions is presented in Figures 4 and 5, which depict analysis and simulation methods and simulation and experimental methods, respectively. The right-most blocks of Figure 4 (Piloted Nonlinear Simulation Evaluation and Flying Qualities Analysis) are repeated on the left side of Figure 5 for process continuity. The methods listed in each block include those that are currently well

understood and available as software tools, as well as some that are in need of further research. Moreover, additional methods can be identified and added to each block. In this way, new methods and tools can be identified.

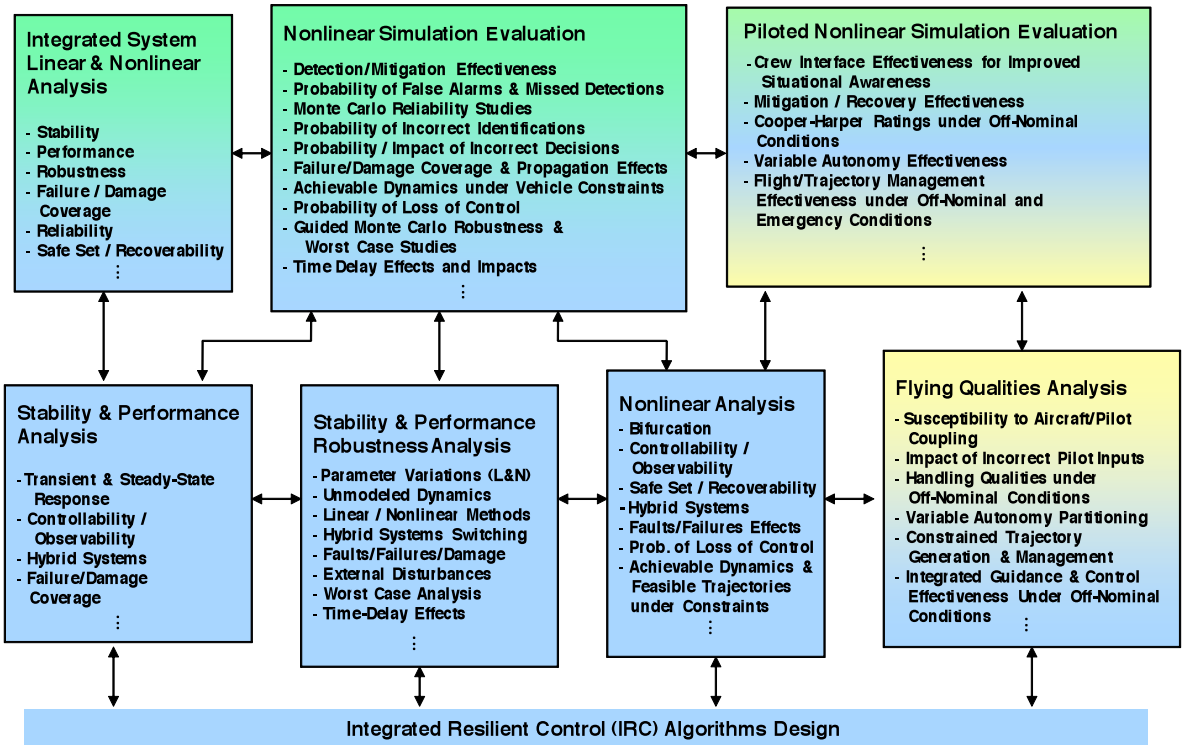


**Figure 4.** V&V Process for Resilient Control Functions – Analysis and Simulation Methods

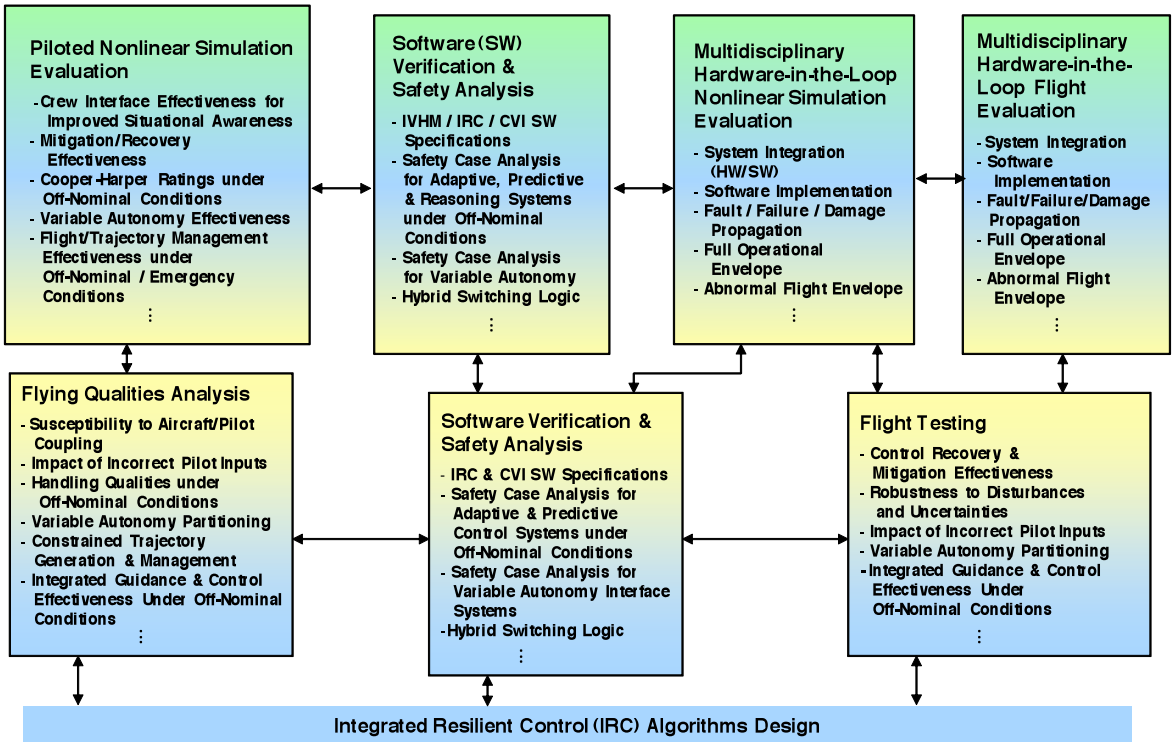


**Figure 5.** V&V Process for Resilient Control Functions – Simulation and Experimental Methods

The "Stability & Performance Analysis" block in the lower left of Figure 4 includes standard stability and performance linear analysis methods, including: eigenvalue and eigenvector analysis, transient and steady-state response, and controllability/observability analysis. These methods are well understood for standard linear time-invariant systems, but are not as well understood for nonlinear, hybrid, and adaptive systems. Failure and damage coverage must also be considered relative to stability and performance implications.

The "Robustness Analysis" block includes standard μ-Analysis methods as well as nonlinear extensions for analyzing stability and performance robustness to uncertainties. Uncertainty modeling methods that generate a Linear Fractional Representation (LFR) of the uncertain system must be utilized for characterizing linear and nonlinear parameter variations and unmodeled dynamics. Robustness methods that enable the evaluation of hybrid systems switching effects, adaptive systems, stochastic uncertainties, and time-delay effects must also be considered, as well as robustness and worst case analysis for fault / failure / damage conditions and external disturbances.

The "Nonlinear Analysis" block of Figure 4 includes bifurcation analysis of nonlinear dynamic and controlled systems, controllability and observability in a nonlinear sense (e.g., degree of controllability and observability as a function of changing parameters), and safe set and recoverability analysis. The safe set and recoverability analysis enables the determination of safe operating regions within which recovery to stable trim points can be achieved, as well as the identification of boundaries to unsafe regions from which recovery may not be guaranteed or even possible. Nonlinear analysis of hybrid and adaptive systems, fault and failure effects, and achievable dynamics of constrained (e.g., impaired) vehicles must also be considered. A method for analytically determining the probability of loss of control (in a nonlinear sense) must also be developed.

These analysis methods must then be applied to the integrated health management (e.g., failure detection and identification functions for critical control components) and resilient control system (e.g., failure mitigation functions), as indicated by the "Integrated System Linear & Nonlinear Analysis" block.

The "Flying Qualities Analysis" block evaluates resilient control system effectiveness relative to a pilot being in the loop, and may integrate pilot models and/or crew interface functions. This analysis includes methods to assess susceptibility to aircraft / pilot coupling (i.e., pilot induced oscillation, or PIO), impact of inappropriate pilot inputs, handling qualities under off-nominal conditions, effectiveness of variable autonomy partitioning between automatic control resilience functions and human-involved control, effectiveness of trajectory generation and management under vehicle constraints (e.g., impairment or damage), and integrated guidance and control effectiveness under off-nominal conditions.

Nonlinear simulation evaluations are performed to assess: the effectiveness of the detection and mitigation algorithms (and their integration); the probability and impact of false alarms, missed detections, incorrect identifications, and incorrect decisions; failure / damage coverage and propagation effects; achievable dynamics under vehicle constraints (e.g., failures, damage); and time delay effects (e.g., associated with failure detection, identification, and mitigation). Guided Monte Carlo studies (i.e., guided by analysis results to further explore potentially problematic operational regions) can be utilized to assess these and other reliability metrics, robustness under uncertainties, and worst-case combinations (e.g., flight and impairment conditions). Nonlinear simulations are used in evaluating the vehicle health management and resilient control subsystems individually and in combination. The crew interface subsystem is assessed in piloted simulation evaluations individually and as part of the integrated system to evaluate: crew interface effectiveness in improving situational awareness under off-nominal conditions; mitigation and recovery effectiveness (including variable levels of autonomy); handling qualities under off-nominal conditions (e.g., using Cooper-Harper metrics and extensions); variable autonomy interface effectiveness; and flight / trajectory management under off-nominal and emergency conditions.

Note that Figure 4 represents validation of the subsystem and integrated system algorithms prior to their implementation in flight-representative software and hardware. Figure 5 shows the progression to subsystem and integrated system evaluations that involve the software / hardware implementations (in final, or near-final, form). Formal verification and safety case analysis methods are utilized to assess system requirements and specifications, implementation integrity of adaptive and predictive/reasoning systems under off-nominal conditions, hybrid switching logic, and the variable autonomy interface. Various levels of system integration and implementation are evaluated through laboratory tests and flight tests (both full-scale and sub-scale vehicle flight tests). Ground and flight test methods are utilized to assess system integration, software implementation, fault / failure / damage mitigation effectiveness, and upset recovery effectiveness under off-nominal conditions throughout and beyond the normal flight envelope. Robustness to uncertainties, reliability and coverage, variable autonomy interface effectiveness, and impacts of inappropriate crew responses are also assessed. Subscale vehicle flight tests are utilized for high-risk conditions that would not be feasible in a manned vehicle, and full-scale flight tests are performed to evaluate the crew/vehicle interfaces in flight.

The V&V process depicted in Figures 4 and 5 is integrated across the various methods, with information being exchanged between each block. Information exchange is indicated with double-headed arrows. Reference [3] provides a detailed description of information exchange throughout the process. Figures 6 and 7 provide an example of information exchange based on a subset of methods in each block. Figure 6 focuses on analysis and simulation blocks, and Figure 7 depicts simulation and experimental methods. As in Figures 4 and 5, the right-most blocks of Figure 6 are repeated on the left side of Figure 7 for process continuity. Starting with the lower left block of Figure 6, failure/damage scenarios evaluated in the Stability and Performance Analysis block can be provided for use in the Robustness Analysis block to generate uncertainty models based on failure and damage profiles being considered, and for performing a worst case analysis. Using robustness analysis techniques, failure/damage coverage margins can be generated as well as worst case failure, damage, and uncertain parameters. These results can be utilized by the nonlinear analysis tools (e.g., bifurcation, safe set and recoverability, and failure effects analyses) to identify potentially problematic nonlinear operating regions. The nonlinear analysis results can be utilized in re-evaluating robustness in these regions and to evaluate flying qualities. Analysis results related to stability and performance (e.g., failure/damage coverage predictions), robustness (e.g., uncertainties, worst case scenarios, and predicted margins), and nonlinear properties (e.g., potentially problematic operating conditions) are utilized, corroborated, refined, or disputed during nonlinear simulation evaluations. Simulation results can then be utilized by the analysis components during re-evaluation. The flying qualities analysis methods might then be utilized to generate test scenarios for use in piloted simulation evaluations, as well as predicted flying qualities limitations and constraints.

Moving to Figure 7, analysis and simulation results might be used to generate software safety properties and performance requirements, and formal verification and safety analysis methods used to identify software errors and safety property violations for the subsystem implementations as well as various levels of integration. The verified software could then be used in ground and flight testing of the individual subsystems and each level of system integration. Subsystem flight test results might be used in generating test scenarios and identifying potentially problematic operating conditions and integration issues for use in ground and flight testing of the fully integrated system. Ground test results can also be used to generate flight test scenarios for flight testing. Moreover, flight test results associated with subsystems can generate test scenarios for consideration in evaluating various levels of integration.

As indicated in Figures 6 and 7, analysis, simulation, and experimental evaluation results are also utilized as part of an iterative design process. Each evaluation method provides a basis for improved system design. Although some of the blocks of Figures 6 and 7 depict various levels of system integration, the analysis, simulation, and test methods depicted can be applied to a single subsystem – which itself may integrate multiple functions and features. The process can also be refined through application experience and as research progresses in developing advanced methods, tools, and testbeds needed for advanced safety-critical systems V&V. Ultimately, this V&V process could be used as part of a certification process for technology transition to the aircraft fleet.

Recent NASA research that pertains to this V&V process is summarized in Section IV, and some key results are presented in greater detail. Some associated references are also provided for this work, although the reference list is certainly not exhaustive.

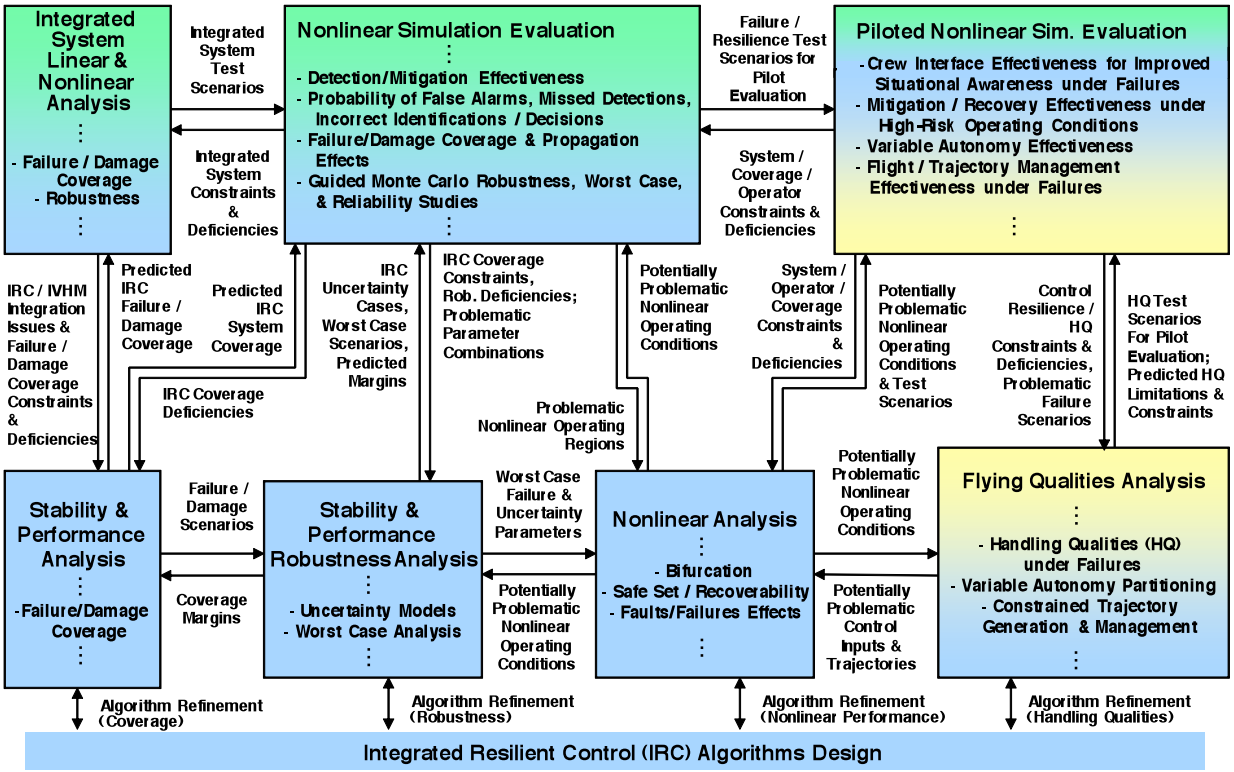


**Figure 6.** V&V Process for Resilient Control Functions – Analysis and Simulation Interface Example

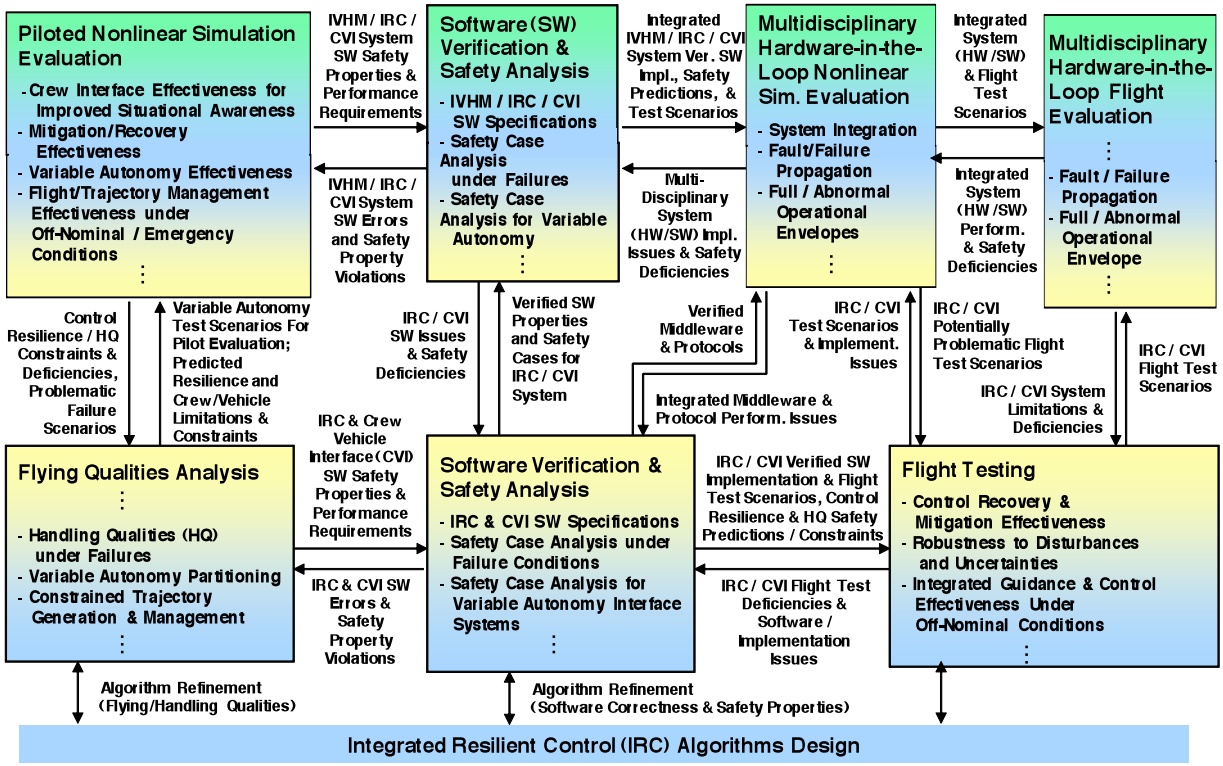


**Figure 7.** V&V Process for Resilient Control Functions – Simulation and Experimental Interface Example

## IV. V&V Research Status and Recent Accomplishments

Significant resources and effort have been invested by NASA in addressing the V&V of future advanced safety-critical systems. For the last decade, this work has largely been planned and funded by the systems research projects focused on vehicle health management, flight-critical system design, and resilient control technology development under the NASA Aviation Safety Program (AvSP). This research has resulted in the development of analytical methods and software tools, simulation-based methods, and experimental testbeds for the validation of safety-critical systems operating under off-nominal conditions related to aircraft loss of control.[4, 5] The methods, tools, and testbeds and some associated results will be described in the following subsections, with selected results presented in greater detail. Software verification methods and tools were also developed under this research effort, and a new effort under the AvSP is currently being planned to focus on the V&V of software-intensive systems. [6] This new effort will develop V&V methods that can be applied to the Next Generation Air Transportation System.

### A. Analytical Methods & Tools

Analytical methods and software tool development has focused on uncertainty modeling for robustness analysis, reliability analysis, stability analysis under actuator saturation, nonlinear robustness analysis extensions, nonlinear system analysis, the analysis of fixed-structure neural networks, and system malfunction effects analysis.

Uncertainty modeling methods and tools have been developed to generate linear parameter varying (LPV) models using orthogonal polynomial functions[7] and symbolic generation near bifurcation points[8], linear fractional representation (LFR) models of systems with parametric uncertainties[9, 10, 11, 12, 13, 14] and unmodeled dynamics (see [11] – [12]). Orthogonal function modeling is presented in Chapter 5 of Reference [7], and its application to LPV modeling is presented in References [11] (theoretical development) and [12] (application example). A method for generating LPV models at or near bifurcation points is presented in Reference [8], and application of this method to an F-16 modeling example near a stall bifurcation is given in Reference [14]. An overview of parametric uncertainty modeling is given in Reference [9], and a matrix-based computational approach to generating LFR models is given in References [10] – [14]. The full uncertainty modeling process consisting of formulation of the LPV model and generation of LFR models for systems involving parametric uncertainties and unmodeled dynamics is described and illustrated in References [11] and [12], respectively. In Reference [13], a framework is presented for representing parametric uncertainties, faults, and failures within an LFR model for use in performing robustness analyses of faulty uncertain systems and integrated failure detection and accommodation systems. Reference [14] describes a preliminary software tool for generating LFR models using the matrix-based computational approach, and provides a comparison for several examples with other LFR modeling methods (including methods developed by ONERA, and the method available in the Matlab Robust Control Toolbox[15]). Applications of LFR-based robustness analysis to aircraft control problems are presented in References [16] and [17] to illustrate the determination of reliable flight regimes for an integrated resilient aircraft control system[16] and a fault tolerant control system[17]. Stochastic uncertainty and robustness analysis methods are also under development. [18, 19]

Stability analysis of systems with saturating actuators is particularly relevant under failures, damage, upset conditions, and other off-nominal conditions related to loss of control. A combined analytic and simulation-based approach was developed for reconfigurable systems.[20] The method utilizes linearized plant dynamics, a linearized state-feedback description of the nonlinear controller dynamics, and a nonlinear actuator model, and provides an estimate of the domain of attraction. This estimate is then used to guide simulation-based stability analyses. An extension of these methods for nested saturations (i.e., involving simultaneous position and rate saturations) was developed for continuous[21] and discrete-time[22] linear systems.

Integrated analysis and simulation-based methods for robustness and worst case analysis were developed to facilitate evaluation under off-nominal conditions. [23] This tool utilizes linear-based analytical robustness results to generate and automatically execute a test-plan for further evaluation using a nonlinear simulation. Interim simulation results are also used in making adjustments to the test plan during implementation. Visualization of the results is facilitated through a graphical user interface. Using this tool, guided Monte Carlo evaluations are facilitated using analytical results in order to examine key regions in the very large space of operational, flight, and off-nominal conditions. Analysis methods that extend robustness analysis for application to nonlinear systems have also been the subject of research. These methods combine analytical and simulation-based techniques to estimate regions of attraction in a robustness analysis setting (i.e., in the presence of uncertainties). Work in this area that was partially or fully sponsored by NASA is reported in References [24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34].

Nonlinear analysis methods are also under development by NASA to perform bifurcation analysis of controlled systems and safe set analysis to identify recoverable regions in the operational envelope for various off-nominal conditions (such as system failures and vehicle damage).[35, 36] Bifurcation methods and software tools have been developed to examine equilibrium structure for aircraft in highly nonlinear upset conditions (i.e., at or near bifurcation points) and under failure/damage conditions. Figure 8 illustrates an example 3-D equilibrium surface computed for a subscale aircraft in terms of flight path angle ($\gamma$), airspeed (V), and elevator deflection ($\delta_e$).

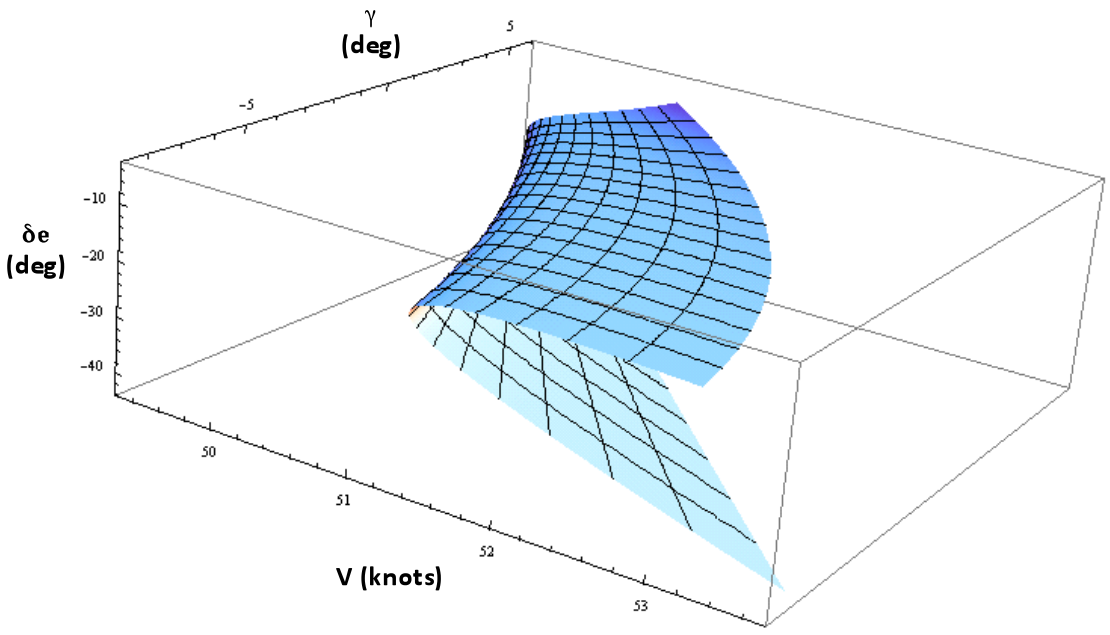


**Figure 8.** Example 3-Dimensional Equilibrium Surface for a Subscale Aircraft

Figure 9 illustrates departure from controlled flight near a stall bifurcation during a coordinated turn of a subscale transport aircraft. Three airspeed points are identified in the top plot along a portion of the coordinated turn equilibrium surface as airspeed approaches the stall speed of 84.8 ft/sec. At each of the three airspeeds of 90 ft/sec, 87 ft/sec, and 85 ft/sec, ground track (y-x) plots and adverse aerodynamics ($\alpha$-$\beta$) plots are shown. The $\alpha$-$\beta$ plot is one of five envelopes identified for use as an indication of loss of control.[37] At 90 ft/sec, the subscale transport exhibits a normal coordinated turn maneuver. At 87 ft/sec, the vehicle departs from trim and enters a well-formed, slowly descending, periodic motion, with violent attitude swings. At stall speed of 85 ft/sec, the vehicle departs from trim and enters a steeply descending, chaotic motion with increasingly violent attitude swings. Please see Reference [35] for a more detailed analysis of this example.

Nonlinear analysis methods are also being used to evaluate control properties near bifurcation points through the use of LPV models (see Reference [8]) to evaluate zero structure dynamics, stability, controllability, and observability. Degeneracy of the control structure can also be examined. Safe set analysis methods are being developed to identify safe regions in the flight envelope within which recovery can be guaranteed. The identification of safe set boundaries enables the clear identification of regions within which recovery may not be possible. Figure 10 shows some preliminary results in safe set computation for a subscale transport aircraft in wings level flight. The left plot shows the safe set calculated for the unimpaired vehicle relative to flight path angle and airspeed. The plots on the right show the changes to the safe set size and shape under elevator failures (stuck failures at +3 deg and -3 deg). Please see Reference [36] for additional results on safe set analysis and other nonlinear analysis techniques applied in the evaluation of aircraft loss of control.

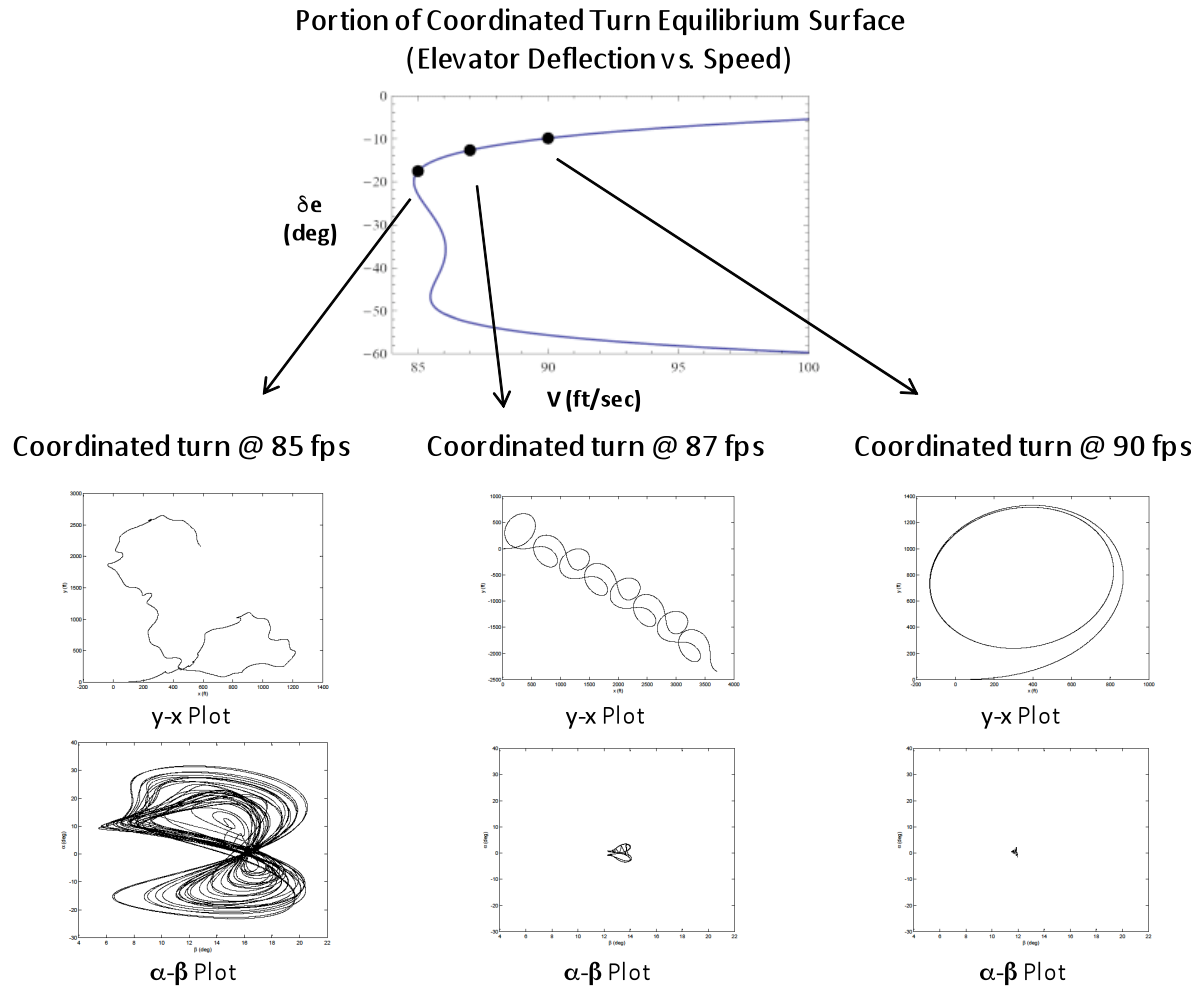


**Figure 9.** Bifurcation Analysis of a Coordinated Turn for a Subscale Transport Aircraft

Reliability analysis methods were developed for the evaluation of control redundancy and reconfigurability [38], to quantitatively delineate the relationship between reliability and fault tolerant control using Markov models [39], to model and assess fault/failure coverage [40, 41], and to establish reliability-based modeling and analysis methods for safety-critical systems[42]. A study was also performed to assess the applicability to flight control systems of Markov-based reliability tools developed for digital systems using an F-16 Self-Repairing Flight Control System as a test case for the reliability analysis [43]. More recent research in this area is based on failure domain bounding. [44]

Analysis methods for fixed-structure neural networks and system malfunction effects are described in References [4] and [5]. The fixed structure neural networks were evaluated as a replacement for aero data tables.[45] Control system malfunction effects are being considered relative to flight control computer closed-loop operation in an adverse electromagnetic environment, and methods for modeling and analytically characterizing closed-loop system stability under digital system upsets are being developed. [46, 47, 48]

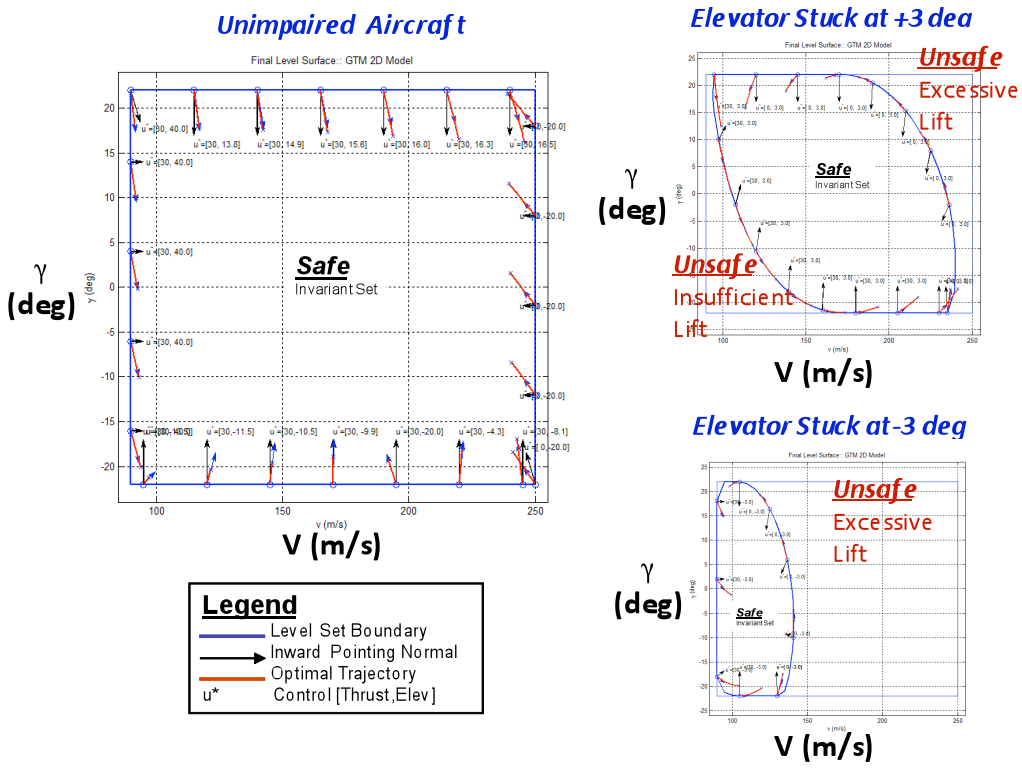


**Figure 10.** Safe Set Analysis of a Subscale Transport Aircraft in Wings Level Flight

### B. Modeling & Simulation Methods for Off-Nominal Conditions

The development of simulation capability for off-nominal conditions has largely focused on the development of enhanced simulation models and databases for characterizing vehicle dynamics under upset conditions, failures, and damage.

Upset conditions are flight conditions that exceed normal operation (i.e., the normal flight envelope). They include unusual or extreme aircraft attitudes, abnormal velocities and angular rates, loss of stability, stall and/or departure from controlled flight, uncommanded motions due to failures or asymmetric thrust, and out-of-control flight motions (such as falling leaf, stall-spin, or uncontrolled descent). Figure 11 illustrates the extreme flight conditions that can occur during a loss-of-control event (i.e., accident or incident). This figure depicts the angle of attack ($\alpha$) versus sideslip angle ($\beta$) for a transport aircraft, and shows the normal flight envelope as compared to loss-of-control accident data (shown in red).

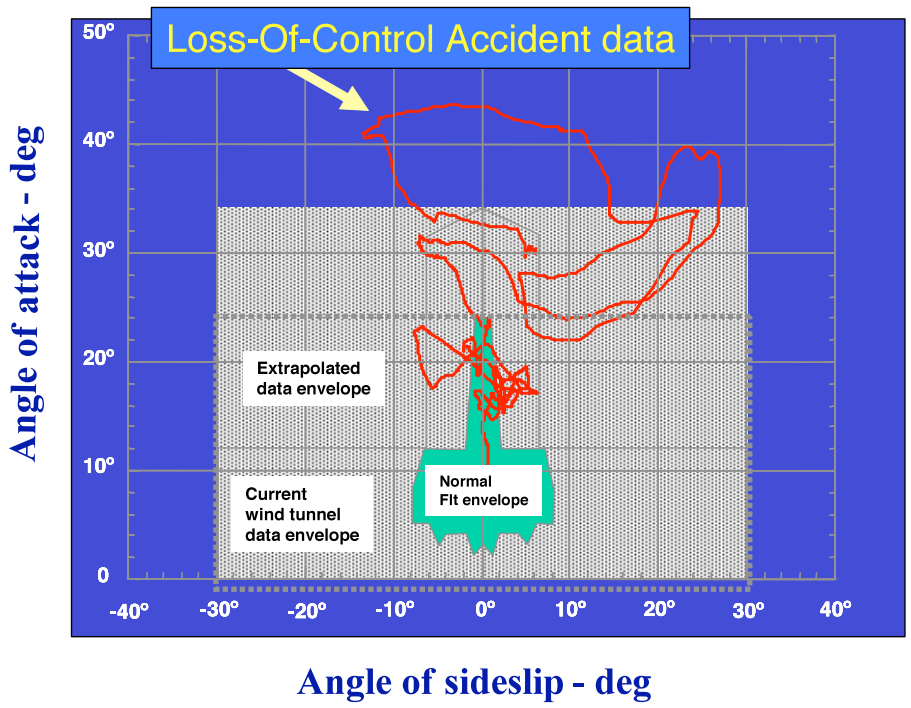


**Figure 11.** Transport Simulation Assessment for Loss-of-Control Characterization

The dashed box of Figure 11 shows the simulator envelope used in current transport simulations. The green region depicts flight-validated data, and the gray hatched region depicts wind tunnel data used in current transport simulators. As indicated in the figure, current transport simulators use data extrapolation techniques when the simulator gets into flight conditions within the regions devoid of wind tunnel data. Characterization of upset conditions therefore required extensive wind tunnel testing (static and dynamic) to obtain additional data.[49] Figure 12 depicts the wind tunnel tests conducted at NASA Langley in collaboration with The Boeing Company. Static and dynamic tests were conducted in three wind tunnels using several wind tunnel transport models, and flow visualization tests were conducted to visualize turbulent flow under extreme flight conditions. Forced oscillation tests were performed in each axis with varying amplitudes and frequencies. Rotary balance tests were performed at varying angles and angular rates. The resulting enhanced database was used to develop enhanced simulation models. Figure 13 shows an example result for pitching moment and elevator control power. The red curves represent results using the enhanced database, and the white curves represent the current standard baseline database. As indicated in the figure, a higher pitching moment effect is predicted by the enhanced simulation at angles of attack beyond approximately 22 degrees than that predicted by the baseline simulator database (which holds a constant value for angle-of-attack values greater than 22 degrees). Moreover, elevator control power is significantly lower at higher angles of attack than the values provided by the baseline simulation.

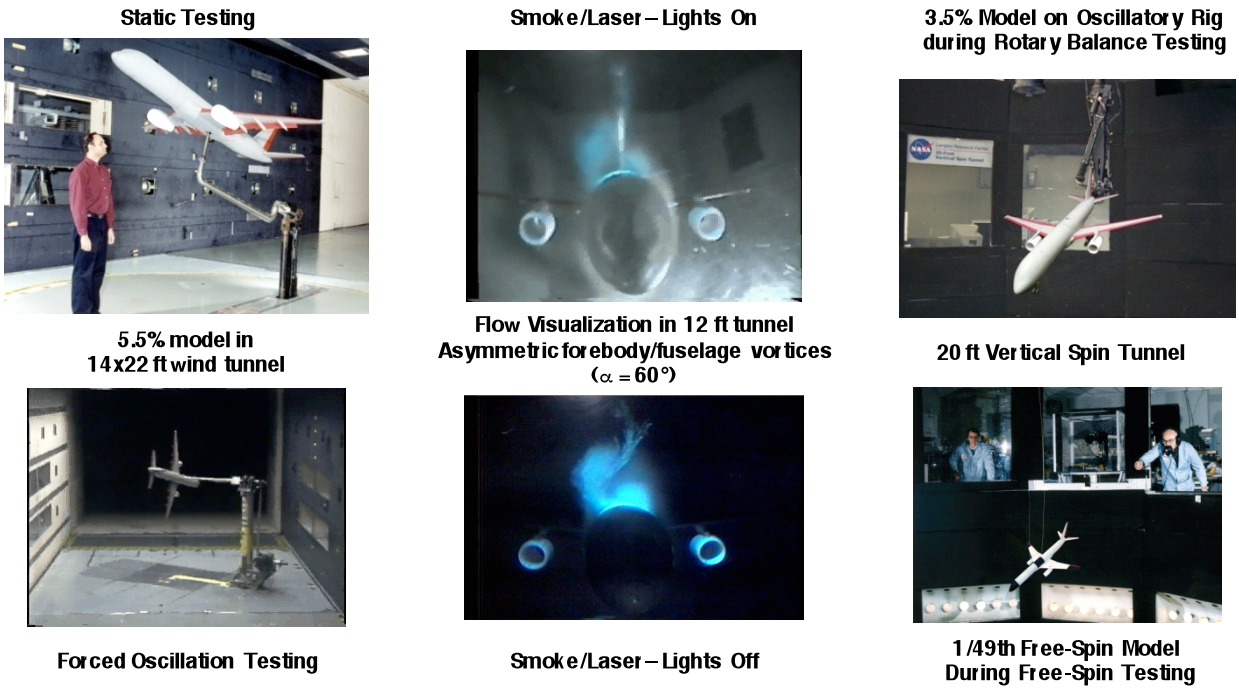


**Figure 12.** Wind Tunnel Testing at NASA Langley for Upset Characterization

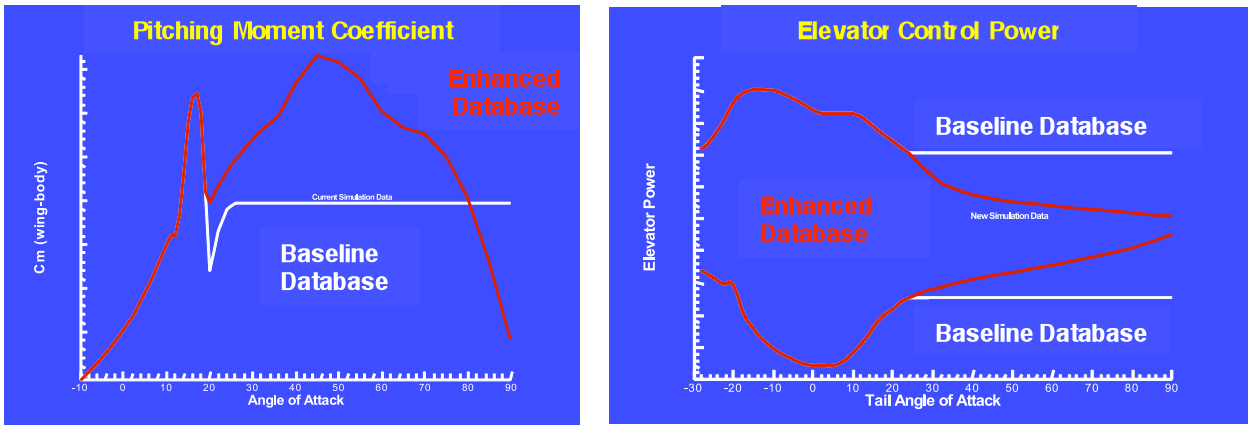


**Figure 13.** Example Result Comparing Pitching Moment and Elevator Control Power Using the Current and Enhanced Databases

The upset enhanced simulation was tested in piloted simulation evaluations,[50, 51] and flight test stall data, provided by Boeing, was used to evaluate the effectiveness of the enhancements. [52] Figure 14 shows some example flight test stall results. The green trace in each plot represents flight test data, the red trace represents baseline simulation data, and the orange trace represents enhanced simulation data. As highlighted in the figure with dashed green ovals, the enhanced simulation produced much better agreement in pitching moment with the flight data (relative to the baseline simulation), and some improvement in roll, yaw, and drag. Further model validation is being performed using a subscale flight test vehicle, which is described in Subsection C.

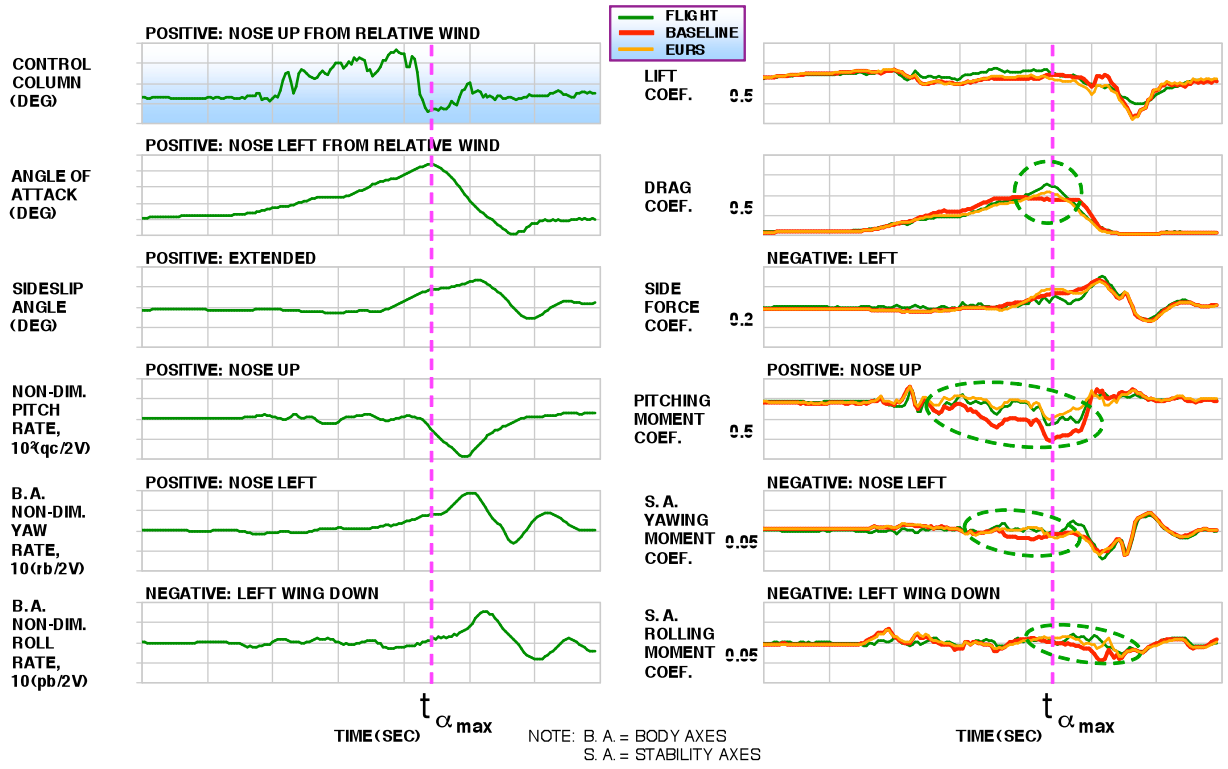


**Figure 14.** Example Result Comparing the Enhanced Simulation and Baseline Simulation to Flight Test Stall Data

Failure and damage modeling research is currently underway at NASA to characterize aerodynamic and structural impacts. Damage components for one of the previously developed transport wind tunnel models were developed, and extensive wind tunnel testing is being performed similar to that describe above for upset modeling. Figures 15a and 15b depict the damage model used in the wind tunnel tests. The damage components are representative of damage in the lifting surfaces (holes of varying sizes and tip loss of varying percentages), control surfaces (missing surface), and engine (nacelle/pylon loss). Tests to date have focused on individual damage conditions, as opposed to simultaneous multiple damage conditions (e.g., wing tip loss combined with a hole).

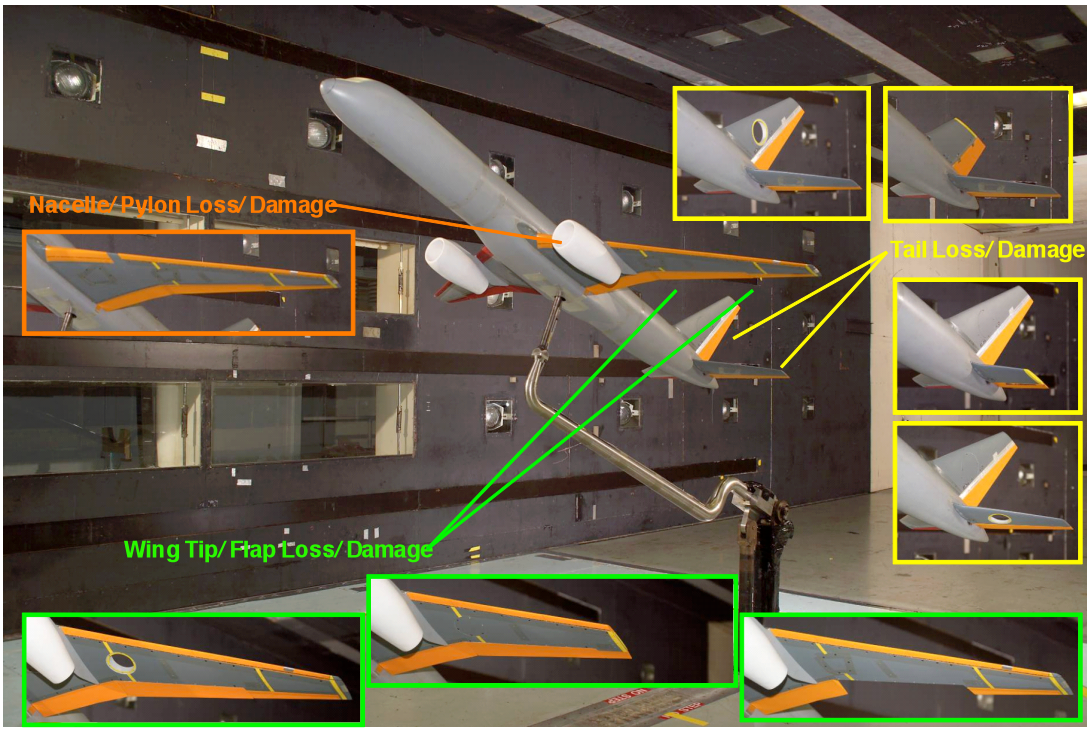


**Figure 15a.** Transport Configuration with Representative Damage Conditions in the NASA Langley 14'x22' Tunnel

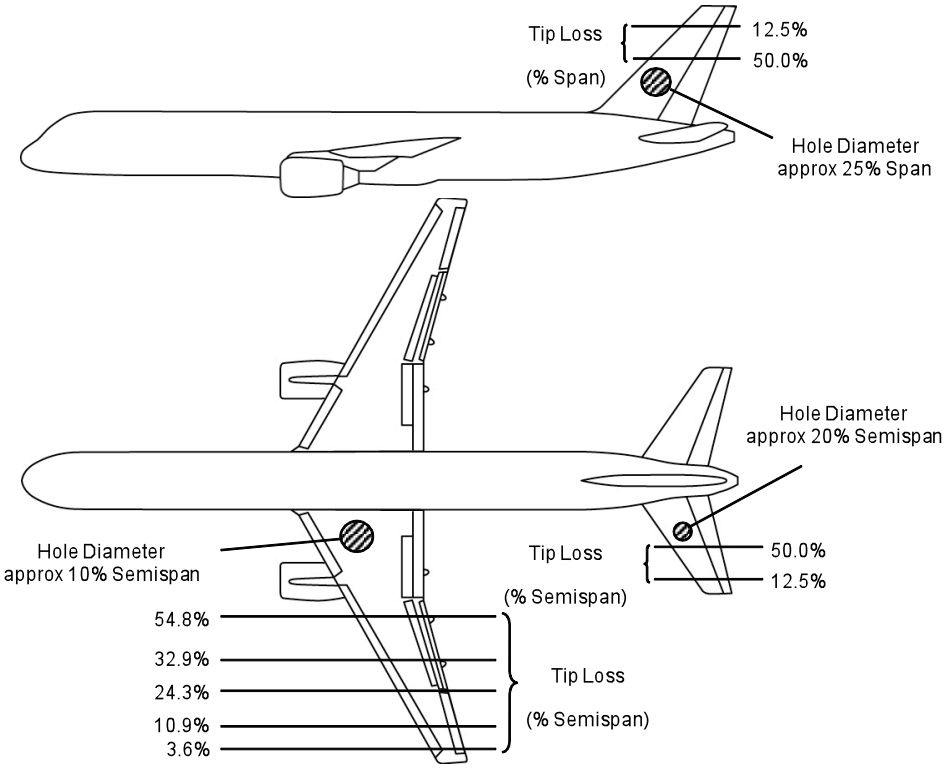


**Figure 15b.** Schematic Diagram of Damage Scenarios Tested

The damage scenarios characterized by the wind tunnel components of Figures 15a and 15b are "clean" damage configurations (i.e., round holes, straight-cut surface tip loss, etc.). They are intended for use in obtaining gross aerodynamic characteristics associated with damage. Aerodynamic characteristics associated with more realistic damage shapes are being obtained using computational fluid dynamics (CFD) models and modeling methods. The first step in accomplishing this goal is to replicate the wind tunnel damage scenarios and use wind tunnel data for CFD model validation. Figure 16a depicts the wing damage models used to generate CFD data for comparison to wind tunnel data. Figure 16b shows plots of the lift coeffecient versus angle-of attack and the rolling moment coefficient versus sideslip for the CFD data (symbols) and wind tunnel data (solid and dashed lines). Although these results are shown for wing damage comparisons, horizontal and vertical tail damage was also evaluated.[53] As indicated in the figure, good agreement between the CFD models and wind tunnel data was achieved for lifting and rolling moment trends, with less agreement in actual magnitudes. These modeling methods will ultimately be used in generalizing vehicle damage shapes, and in capturing ice shapes for characterizing aerodynamic effects under icing conditions.

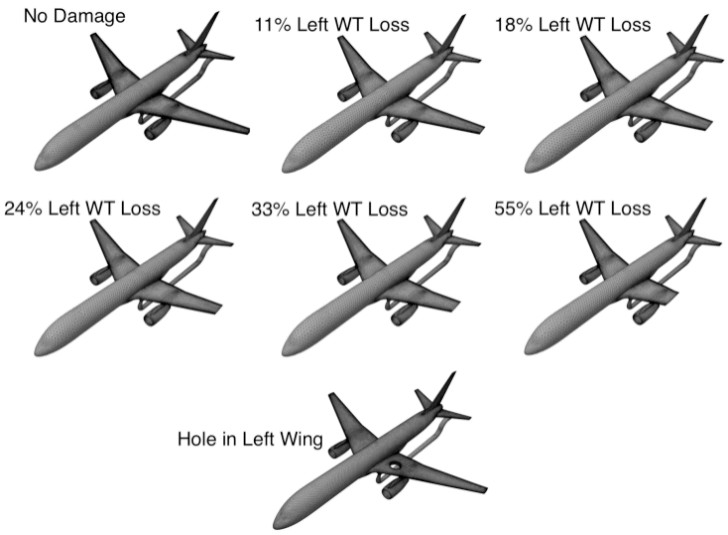


**Figure 16a.** CFD Models of Wing Damage Used to Generate CFD Data for Comparison to Wind Tunnel Data

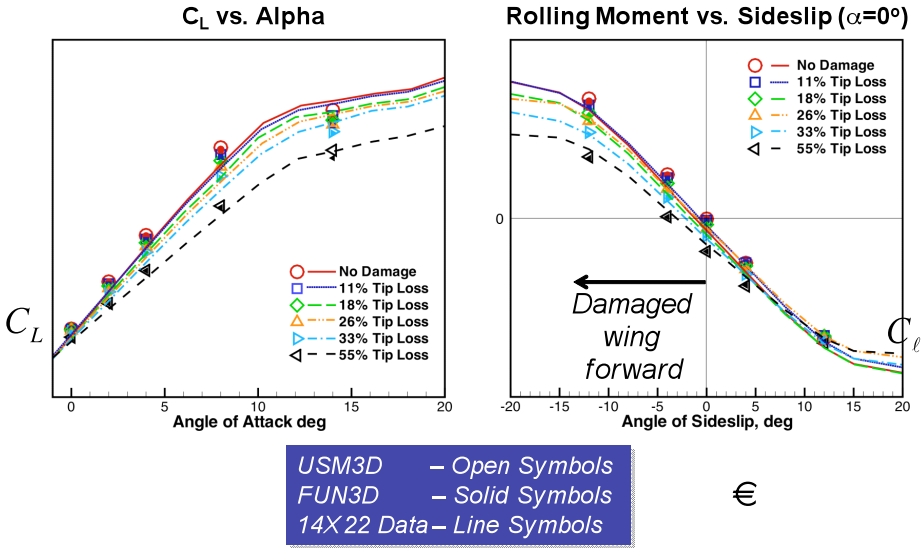


**Figure 16b.** Example CFD Data Comparison to Wind Tunnel Data for Varying Degrees of Wing Tip Loss

Structural dynamics modeling methods and tools are also under development at NASA to characterize damage effects. Research in this area focuses on impact dynamics modeling,[54] damage propagation modeling,[55] and aeroelastic effects modeling[56, 57, 58] of discrete source damage. Examples of discrete source damage are given in Figure 17. The ultimate goal of this research is to develop damage models and databases that can be used in real-time simulation to characterize structural damage effects (e.g., in terms of residual strength and aeroelastic characteristics) based on the size, shape, and location of the damage.


**Figure 17.** Examples of Aircraft Discrete Source Damage

The ultimate objective of this research is to establish simulation capability that characterizes a variety of off-nominal LOC conditions (including, upsets, failures and damage, impairment under icing conditions, and external disturbances) occurring either individually or in combination. [59] Capturing the resulting multidisciplinary effects of these conditions for the V&V of safety-critical systems is a major and complex task.

### C. Experimental Testbeds

Experimental testing of safety-critical systems operating under off-nominal LOC conditions poses significant technical challenges. Ground testing requires the simulation and/or emulation of a wide variety of conditions for which data is either nonexistent or difficult to obtain. Flight testing under these conditions can pose significant safety risks, especially for full-scale aircraft. In fact, some LOC conditions render full-scale flight testing infeasible due to the high safety risk to the vehicle and those onboard. Experimental testbeds for ground and flight testing under off-nominal conditions are therefore being developed.

A multidisciplinary linked-lab hardware-in-the-loop ground facility, the Systems and Airframe Failure Emulation, Testing, and Integration (SAFETI) Laboratory (see Reference [5]), is being developed at NASA Langley to enable closed-loop safety-critical system testing under a large variety of simulated/emulated LOC conditions. Vehicle upsets, failures, and damage effects are simulated using the modeling and simulation methods described in Section 20.4.2. Structural damage can also be emulated using an airframe test article in one of the structures labs at NASA Langley (or elsewhere), and linked into the closed-loop experiment. High energy radiating electromagnetic fields are emulated in the High Intensity Radiated Fields (HIRF) Lab at NASA Langley, [60, 61] in order to study their effects on safety-critical avionics and electronic systems. The SAFETI Lab is being developed to provide modular hardware-in-the-loop capability, including advanced programmable avionics systems, actuators, and sensors. The linked-lab capability enables the interconnection of laboratories within NASA Langley, NASA, or elsewhere. The distributed multidisciplinary test capability of the SAFETI Lab will enable the closed-loop evaluation of error propagation and containment between integrated safety-critical subsystems, including the effects of missed detections, incorrect decisions, and inappropriate control actions. Figures 18 and 19 depict envisioned SAFETI Lab capabilities and links, respectively.

The HIRF Lab at NASA Langley has been linked into the SAFETI Lab, and links to the Structures Labs, Landing Dynamics Facility, and Cockpit Motion Facility at NASA Langley are in progress. Planned links include key facilities at the other NASA Centers, including Ames Research Center, Dryden Flight Research Center, Glenn Research Center, and Wallops Flight Facility. Other potential links being considered include the Federal Aviation Administration (FAA) Full-Scale Aircraft Structural Test Evaluation and Research (FASTER) Facility, the Los Alamos National Laboratory (LANL) Neutron Science Center, and an engine test facility at Pratt & Whitney or General Electric (GE).

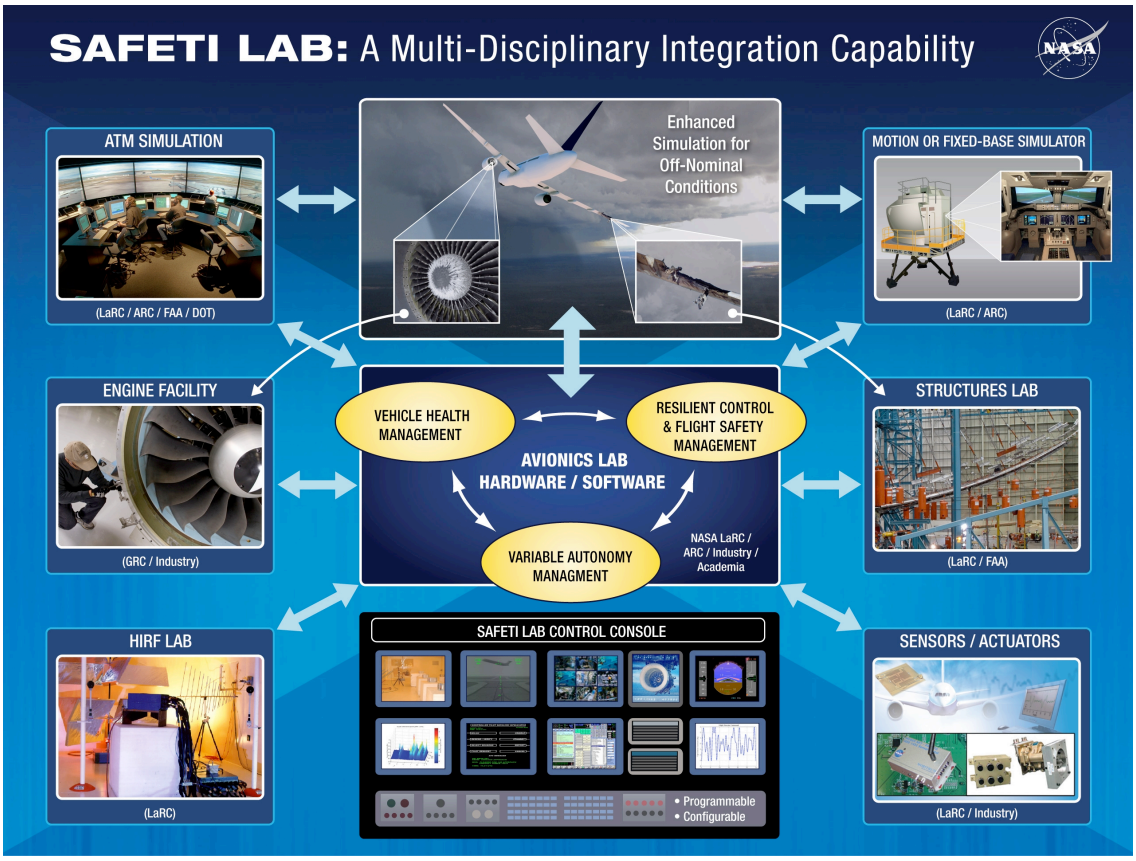


**Figure 18.** Potential SAFETI Lab Capabilities

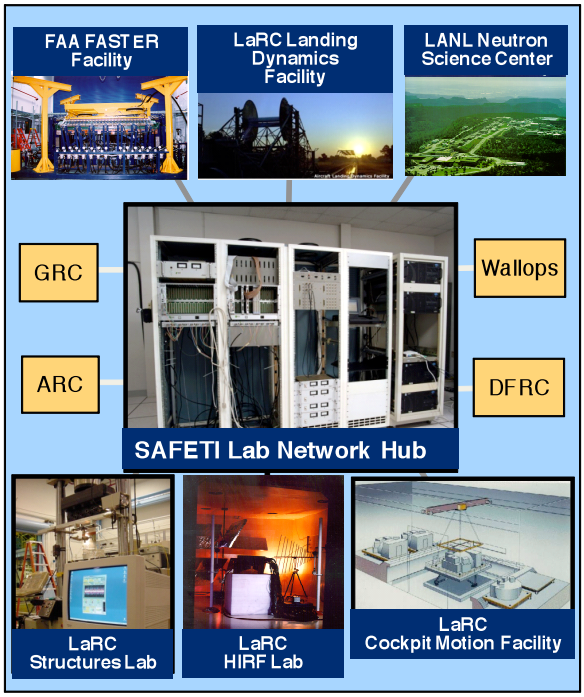


**Figure 19.** Potential SAFETI Lab Links

The Airborne Subscale Transport Aircraft Research (AirSTAR) Testbed has been developed at NASA Langley to provide a flight test capability for off-nominal conditions associated with LOC. Figure 20 shows some photographs of some key components of the AirSTAR Testbed.


**Figure 20.** AirSTAR Testbed

The testbed consists of dynamically scaled transport aircraft models [62] developed for pilot training and instrumented for research, less expensive commercial aircraft models for use in preliminary testing, and ground facilities (laboratory and mobile)[63] to support flight experiments. The Base Research Station (BRS) is a laboratory ground facility that enables pre-experiment testing using a high-fidelity nonlinear simulation that includes upset and aerodynamic damage effects data. The instrumentation in the BRS is duplicated in the Mobile Operations Station (MOS), which is deployed with the aircraft to support flight test experiments. The research aircraft is a 5.5% dynamically scaled generic transport model (GTM), has split control surfaces for failure and damage emulation, and is instrumented with onboard sensors and a data system that provides measurements of angle of attack ($\alpha$), angle of sideslip ($\beta$), airspeed, altitude, rates and accelerations (analog), control surface positions, and inertial navigation system / global positioning system (INS/GPS) solutions. The aircraft weighs 56 lbs., has an 82" wingspan, and has twin wing-mounted turbine engines. Data is telemetered to/from the MOS during research flight operations, and the control architecture has been developed to enable the activation of the standard aircraft control system, research control laws, and failure/damage emulation. [64, 65, 66] Research experiments are conducted from a pilot station inside the MOS that utilizes synthetic vision displays generated from a terrain database of the flight test site. Researcher stations within the MOS enable real-time data monitoring during flight experiments. A safety pilot located outside the MOS conducts flight operations during takeoff and landing using a handheld remote control (RC) transmitter. The safety pilot can also take over flight operations should the need arise (e.g., loss of telemetry from the MOS). This testbed enables flight testing under LOC conditions that would be infeasible in a full-scale manned aircraft.

### D. Real-Time Onboard V&V Methods

Several onboard methods for monitoring system behavior have been developed by NASA. A run-time stability margin estimation method and tool have been developed for monitoring control law stability margins online in quasi-real-time, and a preliminary evaluation of this method was performed using the AirSTAR Testbed. [67] A distributed detection and data fusion method has also been developed for flight control computer malfunction monitoring. [68, 69] This approach can be used for the detection and mitigation of flight control computer errors due to digital system upset. Preliminary evaluations were performed using data collected during closed-loop HIRF testing in the NASA Langley HIRF Lab. [70]

## V. Concluding Remarks

Aircraft loss of control is the largest aircraft accident category, and results in the highest number of fatalities among the worldwide commercial jet fleet. It is also the most complex accident category, resulting from numerous causal and contributing factors that act individually or (more often) combine to result in a loss of control event (accident or incident). These factors are off-nominal conditions that occur onboard the aircraft, as external disturbances, or as abnormal flight conditions. To address aircraft loss of control, NASA is developing onboard systems technologies to: prevent and detect faults, failures, and damage through the development of vehicle health management technologies; provide improved situational awareness to the crew through the development of advanced crew interface technologies; and to provide the capability to mitigate and recover from off-nominal conditions through the development of resilient aircraft control technologies. A future technology vision, called the AIRSAFE System, has been developed as a research framework for integrating these technologies and providing onboard flight safety assurance. These technologies are being developed for safety-critical operation under off-nominal conditions, and their validation and verification (V&V) poses significant technical challenges. This paper has provided an analysis of this V&V problem, and has described the research approach being taken to address it. A high-level V&V concept was presented, which integrates analytical, simulation, and experimental methods, software tools, and testbeds. A detailed V&V process was defined for application to the AIRSAFE System concept, and a detailed description provided of the methods and some example interfaces involved in the controls-related components. Research progress in the development of analytical, simulation, and experimental methods was summarized, with some key accomplishments presented in greater detail. Some references for this work have been provided for obtaining additional information and technical details.


## Acknowledgments

The V&V research process, some of the analytical methods and software tools, the AirSTAR Testbed, and the SAFETI Lab concept presented in this paper were developed in collaboration with Dr. Celeste M. Belcastro of NASA Langley Research Center, who lost her courageous and selfless battle with cancer and passed from this life on August 22, 2008. Continued work in this area is dedicated to her memory.


## References


[1] Belcastro, Christine M., "Aircraft Loss-of-Control Accident and Incident Analysis", AIAA Guidance, Navigation, and Control Conference, Toronto, 2010.

[2] Belcastro, Christine M., and Jacobson, Steven R., "Future Concepts for Preventing Aircraft Loss-of-Control Accidents", AIAA Guidance, Navigation, and Control Conference, Toronto, 2010.

[3] Belcastro, Christine M., and Belcastro, Celeste M.: Future Research Directions for the Development of Integrated Resilient Flight Systems to Prevent Aircraft Loss-of-Control Accidents, Part II: Validation and Verification; NASA TM (in final preparation for review).

[4] Belcastro, Christine M., and Belcastro, Celeste M., "On the Validation of Safety Critical Aircraft Systems, Part I: An Overview of Analytical & Simulation Methods, AIAA Conference on Guidance, Navigation, and Control, 2003.

[5] Belcastro, Celeste M., and Belcastro, Christine M., "On the Validation of Safety Critical Aircraft Systems, Part II: An Overview of Experimental Methods", AIAA Conference on Guidance, Navigation, and Control, 2003.

[6] Validation and Verification for Flight-Critical Systems Assessment of Critical Research Activities, NASA Aeronautics Research Mission Directorate, Aviation Safety Program, November 25, 2009.

[7] Klein, V. and Morelli, E.A. *Aircraft System Identification - Theory and Practice*, AIAA Education Series, Reston, VA, August 2006.
[8] Kwatny, H. G., and Chang, B.-C.: Constructing Linear Families from Parameter-Dependent Nonlinear Dynamics, *IEEE Transactions on Automatic Control*, vol. 43, pp. 1143-1147, 1998.
[9] Belcastro, Christine M.: Parametric Uncertainty Modeling: An Overview; Proceedings of the American Control Conference, Philadelphia, 1998.
[10] Belcastro, Christine M. and Chang, B.-C.: LFT Formulation for Multivariate Polynomial Problems; Proceedings of the American Control Conference, Philadelphia, 1998.
[11] Belcastro, Christine M., Lim, Kyong B., and Morelli, Eugene A.: Computer-Aided Uncertainty Modeling of Nonlinear Parameter-Dependent Systems, Part I: Theoretical Overview; Proceedings of the Computer-Aided Control System Design Conference, Hawaii, 1999.
[12] Belcastro, Christine M., Lim, Kyong B., and Morelli, Eugene A.: Computer-Aided Uncertainty Modeling of Nonlinear Parameter-Dependent Systems, Part II: F-16 Example; Proceedings of the Computer-Aided Control System Design Conference, Hawaii, 1999.
[13] Belcastro, Christine M. and Chang, B.-C.: Uncertainty Modeling for Robustness Analysis of Failure Detection & Accommodation Systems; Proceedings of the American Control Conference, Anchorage, Alaska, 2002.
[14] Belcastro, Christine M., Khong, Thuan H., Shin, Jong-Yeob, Kwatny, Harry, Chang, Bor-Chin, and Balas, Gary J.: Uncertainty Modeling for Robustness Analysis of Aircraft Control Upset Prevention and Recovery Systems; Proceedings of the Guidance, Navigation, and Control Conference, San Francisco, 2005.
[15] Matlab Robust Control Toolbox, The Mathworks Inc., Natick MA, 2002-2010.
[16] Shin, J-Y. and Belcastro, C.: Robustness Analysis and Reliable Flight Regime Estimation of an Integrated Resilient Control System for a Transport Aircraft, *AIAA Guidance, Navigation and Control Conference*, Honolulu, Hawaii, 2008, AIAA-2008-6656.
[17] Shin, J-Y., Belcastro, C., and Khong, T. : "Closed-Loop Evaluation of An Integrated Failure Identification and Fault Tolerant Control System for a Transport Aircraft", *AIAA Guidance, Navigation and Control Conference and Exhibit*, Keystone, CO, AIAA-2006-6310, 2006.
[18] Kenny, S., Crespo, L., Giesy, D., "Dimensionality Reduction for Uncertain Dynamic Systems", International Journal of Numerical Methods in Engineering, accepted for publication.
[19] Crespo, L., Kenny, S., Giesy, D., "An Optimization-based Approach to the Verification of Control Robustness", AIAA Journal of Guidance, Control, and Dynamics, in review
[20] Bateman, A.J., D.G Ward, J.F. Monaco, and Z. Lin "Stability Analysis for Reconfigurable Systems with Actuator Saturation," Proc. American Control Conf., Anchorage, AK, May 8-10, 2002.
[21] Bateman, A. and Z. Lin: "An Analysis and Design Method for Linear Systems under Nested Saturation"; *Systems & Control Letters*, Vol. 48, No. 1, pp. 41-52, 2002.
[22] Bateman, A. and Z. Lin: "An Analysis and Design Method for Discrete Time Linear Systems under Nested Saturation"; *IEEE Trans. Automatic Control,* Vol. 47, No. 8, Aug. 2002, pp. 1305-1310.
[23] Bateman, Alec J., Ward, David G., and Balas, Gary: Robust / Worst Case Analysis and Simulation Tools; AIAA Conference on Guidance, Navigation, and Control, 2005.
[24] Topcu, U. , Packard, A.K. , Seiler, P. , and Balas, G.J.: "Local stability analysis for uncertain nonlinear systems using a branch-and-bound algorithm", American Control Conference, June 2008, pp. 3428 - 3433.
[25] Tan, W. , Topcu, U. , Seiler, P. , Balas, G.J. , and Packard, A.K.: "Simulation-aided Reachability and Local Gain Analysis for Nonlinear Dynamical Systems", 47th IEEE Conference on Decision and Control, December 2008, pp. 4097-4102.
[26] Seiler, P. , Balas, G.J. , Packard, A.K. , and Topcu, U.: "Analytical Validation Tools for Safety Critical Systems", AIAA Infotech@aerospace Conference, April 2009, AIAA 2009-1991.
[27] Chakraborty, A. , Seiler, P. , and Balas, G.J.: "Applications of Linear and Nonlinear Robustness Analysis Techniques to the F/A-18 Flight Control Laws", AIAA Guidance, Navigation, and Control Conference, August 2009, AIAA 2009-5675.
[28] Topcu, U., Packard, A.K. , Seiler, P. , and Balas, G.J.: "Stability region estimation for systems with unmodeled dynamics", European Control Conference, August 2009.
[29] Topcu, U. and Packard, A.: "Local Stability Analysis for Uncertain Nonlinear Systems", IEEE Transactions on Automatic Control, Vol. 54, No. 5, pp. 1042 - 1047, May 2009.
[30] Topcu, U. , Packard, A.K. , and Seiler, P.: "Local stability analysis using simulations and sum-of-squares programming", Automatica, Vol. 44, pp. 2669-2675, September 2008.

[31] Seiler, P. , Topcu, U. , Packard, A. , and Balas, G.: "Parameter-Dependent Lyapunov Functions for Linear Systems With Constant Uncertainties", IEEE Transactions on Automatic Control, Vol. 54, No. 10, pp. 2410-2416, October 2009.
[32] Lu, L. , Lin, Z. , and Bateman, A.: "Decentralized state feedback design for large-scale linear systems subject to input saturation", IET Control Theory and Applications, to appear.
[33] Seiler, P. , Packard, A. , and Balas, G.J.: "A gain-based lower bound algorithm for real and mixed mu problems", accepted for publication, *Automatica*.
[34] Topcu, U. , Packard, A.K. , Seiler, P. , and Balas, G.J.: "Robust Region-of-Attraction Estimation", accepted for publication, *IEEE Transactions on Automatic Control*.
[35] Kwatny, Harry G., Dongmo, Jean-Etienne T., Chang, Bor-Chin, Bajpai, Guarav, Yasar, Murat, and Belcastro, Christine M.: Aircraft Accident Prevention: Loss-of-Control Analysis; Proceedings of the AIAA Conference on Guidance, Navigation, and Control, Chicago, 2009.
[36] Kwatny, Harry G., Dongmo, Jean-Etienne T., Allen, Robert, Chang, Bor-Chin, and Bajpai, Guarav: Loss-of-Control: Perspectives on Flight Dynamics and Control of Impaired Aircraft; AIAA Conference on Guidance, Navigation, and Control, Toronto, 2010.
[37] Wilborn, James E., Foster, John V.: Defining Commercial Transport Loss-of-Control: A Quantitative Approach; AIAA Atmospheric Flight Mechanics Conference and Exhibit, 2004, AIAA Paper No. 2004-4811.
[38] Wu, N. Eva , Zhou, Kemin , and Salomon, Gregory : Control reconfigurability of linear time-invariant systems; Automatica, vol.36, pp17670-1771, 2000.
[39] Wu, N. Eva: Reliability of fault-tolerant control systems: Part I; Proc. IEEE Conference on Decision and Control, 2001.
[40] Wu, N. Eva: Reliability of fault-tolerant control systems: Part II; Proc. IEEE Conference on Decision and Control, 2001.
[41] Wu, N. Eva: Coverage in fault-tolerant control; Automatica, vol.40, pp. 537-548, 2004.
[42] Wu, N. Eva and Aydin, Oguz A.: Reliability-based modeling and analysis of fault-tolerant flight control systems; Proc. AIAA-GNC 2005.
[43] Wu, N. Eva: Reliability analysis for AFTI-F16 SRFCS using ASSIST and SURE, Proc. American Control Conference, 2002.
[44] Crespo, L., Giesy, D., Kenny, S., "Reliability-Based Analysis and Design via Failure Domain Bounding", Journal of Safety Systems, accepted for publication.
[45] Hull, J.R., D.G. Ward, "Verification and Validation of Neural Networks for Safety-Critical Applications," Proceedings of the American Control Conference, Anchorage, AK, May 8-10, 2002.
[46] Gray, W. S., Wang, R. , and González, O. R.: `A Performance Model for a Distributed Flight Control System Subject to Random Upsets,' Proc. 2008 IEEE Conference on Control Applications, San Antonio, Texas, 2008, pp. 918-923.
[47] Tejada, A., O. R. González, and Gray, W. S.: `Stability of Digital Control Systems Implemented in Error-Recoverable Computers,' International Journal of Control, vol. 81, no. 11, November 2008, pp. 1665-1681.
[48] W. S. Gray, R. Wang, O. R. González, and J. R. Chávez-Fuentes, `Tracking Performance Analysis of a Distributed Recoverable Boeing 747 Flight Control System Subject to Digital Upsets,' Proc. 2010 American Control Conference, Baltimore, Maryland, 2010, to appear.
[49] Shah, Gautam H., Cunningham, Kevin, Foster, John V., Fremaux, C. Michael, Stewart, Eric C., Wilborn, James E., Gato, William, and Pratt, Derek W.: Wind-Tunnel Investigation of Commercial Transport Aircraft Aerodynamics at Extreme Flight Conditions; World Aviation Congress & Display, Phoenix, Arizona, November 5-7, 2002, SAE Technical Paper 2002-01-2912.
[50] Cunningham, Kevin, Foster, John V., Shah, Gautam H., Stewart, Eric C., Rivers, Robert A., Wilborn, James E., and Gato, William: Simulation Study of a Commercial Transport Airplane During Stall and Post-Stall Flight; World Aviation Congress, Reno, Nevada, 2004, SAE Technical Paper 2004-01-3100.
[51] Cunningham, Kevin, Foster, John V., Shah, Gautam H., Stewart, Eric C., Ventura, Robin N., Rivers, Robert A., Wilborn, James E., and Gato, William: Simulation Study of Flap Effects on a Commercial Transport Airplane in Upset Conditions; AIAA Atmospheric Flight Mechanics Conference, 2005.
[52] Foster, John V., Cunningham, Kevin, Fremaux, Charles M., Shah, Gautam H., Stewart, Eric C., Rivers, Robert A., Wilborn, James E., and Gato, William: Dynamics Modeling and Simulation of Large Transport Airplanes in Upset Conditions; AIAA Guidance, Navigation, and Control Conference, 2005.

[53] Frink, Neal T., Pirzadeh, Shahyar Z., Atkins, Harold L., Viken, Sally A., and Morrison, Joseph H.: CFD Assessment of Aerodynamic Degradation of a Subsonic Transport Due to Airframe Damage; AIAA 2010-0500, January 2010.
[54] Hinrichsen, Ronald L., Kurtz, Alex G., Wang, John T., Belcastro, Christine M., and Parks, Jeffrey L.: Modeling Projectile Damage in Transport Aircraft Wing Structures; AIAA Journal, Vol. 46, No. 2, pp. 328 – 335, AIAA-26374-357, February, 2008.
[55] Ransom, J. B., Glaessgen, E. H., Raju, I. S., and Harris, C. E.: Recent Advances in Durability and Damage Tolerance Methodology at NASA Langley Research Center; AIAA Structures, Structural Dynamics and Mechanics Conference, 2007.
[56] Krishnamurthy,T., and Brian H. Mason, "Equivalent Plate Analysis of Aircraft wing with discrete Source Damage," AIAA-2006-2218, Presented at 47th AIAA/ASME/ASCE /AHS/ASC Structures, Structural Dynamics and Materials Conference 13th AIAA/ASME /AHS Adaptive Structures Conference, Newport, Rhode Island, May 1-4, 2006.
[57] Krishnamurthy,T., Eldred, B. Lloyd, "Frequency Response of an Aircraft Wing with Discrete Source Damage Using Equivalent Plate Analysis, " AIAA-2007-2144, Presented at 48th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference, Honolulu, Hawaii, Apr. 23-26, 2007.
[58] Krishnamurthy,T. and Tsai, Frank J., "Static and Dynamic Structural Response of an Aircraft Wing with Damage Using Equivalent Plate Analysis, " AIAA-2008-1967, Presented at 49th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference, Schaumburg, IL, Apr. 07-10, 2008.
[59] Shah, Gautam H., Foster, John V., Cunningham, Kevin: Simulation Modeling for Off-Nominal Conditions – Where Are We Today?; AIAA Modeling and Simulation Technologies Conference, Toronto, 2010.
[60] Williams, R. A.: The NASA High Intensity Radiated Fields Laboratory"; AIAA/IEEE Digital Avionics Systems Conference, 1997.
[61] Koppen, Sandra V., Nguyen, Truong X., and Mielnik, John: Reverberation Chamber Uniformity Validation and Radiated Susceptibility Test Procedures for the NASA High Intensity Radiated Fields Laboratory; NASA TM-2010-216181, 2010.
[62] Jordan, Thomas L., Langford, William M., and Hill, Jeffrey S.: Airborne Subscale Transport Aircraft Research Testbed – Aircraft Model Development; AIAA Guidance, Navigation, and Control Conference, 2005.
[63] Bailey, Roger M., Hostetler, Robert W., Barnes, Kevin N., Belcastro, Celeste M., and Belcastro, Christine M.: Experiment Validation: Subscale Aircraft Ground Facilities and Integrated Test Capability; AIAA Guidance, Navigation, and Control Conference, 2005.
[64] Murch, Austin M.: A Flight Control System Architecture for the NASA AirSTAR Test Infrastructure; AIAA Guidance, Navigation, and Control Conference, 2008.
[65] Cunningham, Kevin, Foster, John V., Morelli, Eugene A. and Murch, Austin M.; Practical Application of a Subscale Transport Aircraft for Flight Research in Control Upset and Failure Conditions, AIAA-2008-6200, AIAA Atmospheric Flight Mechanics Conference, Honolulu, HI, 2008.
[66] Jordan, Thomas L., Bailey, Roger M.; NASA Langleys AirSTAR Testbed A Subscale Flight Test Capability for Flight Dynamics and Control System Experiments, AIAA-2008-6660, AIAA Guidance, Navigation and Control Conference, Honolulu, HI, 2008.
[67] Lichter, Matthew D., Bateman, Alec J., and Balas, Gary J.: Flight Test Evaluation of a Run-time Stability Margin Estimation Tool; AIAA Guidance, Navigation, and Control Conference, 2009.
[68] Belcastro, Celeste M., "Ensuring Control Integrity of Critical Systems Subjected to Electromagnetic Disturbances: Problem Overview", Proceedings of the American Control Conference, Philadelphia PA, June 1998
[69] Belcastro, Celeste M., and Weinstein, B.: Sistributed Detection with Data Fusion for Malfunction Detection and Isolation in Fault Tolerant Flight Control Computers; Proceedings of the American Control Conference, Anchorage, Alaska, June 2002.
[70] Belcastro, Celeste M., Chowdhury, Fahmida, Cheng, Qi, Michels, James H., and Varshney, Pramod K.: Distributed Detection with Data Fusion for Aircraft Flight Control Computer Malfunction Monitoring; AIAA Guidance, Navigation, and Control Conference, San Francisco, CA, AIAA-2005-6358, 2005.