Validation and Verification (V&V) of Safety-Critical Systems Operating under Off-Nominal Conditions

Christine M. Belcastro

NASA Langley Research Center
Hampton, VA 23681-0001
e-mail: christine.m.belcastro@nasa.gov

Summary. *Loss of control* (LOC) remains one of the largest contributors to aircraft fatal accidents worldwide. Aircraft LOC 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. Research is underway at the *National Aeronautics and Space Administration* (NASA) in the development of advanced onboard system technologies for preventing or recovering from loss of vehicle control and for assuring safe operation under off-nominal conditions associated with aircraft LOC accidents. 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 highly significant technical challenges and is the subject of a parallel research effort at NASA. This chapter summarizes the V&V problem and presents a proposed process that could be applied to complex integrated safety-critical systems developed for preventing aircraft LOC accidents. A summary of recent research accomplishments in this effort is referenced.

1 Introduction: Motivation for Off-Nominal Conditions

Aircraft LOC accidents can result from numerous causal and contributing factors that are collectively referred to in this chapter as “off-nominal conditions”. “Off-nominal” conditions include adverse conditions occurring onboard the vehicle, such as system failures, external hazards, such as inclement weather, and abnormal flight conditions, such as stall/departure. A more detailed description of off-nominal conditions associated with aircraft LOC accidents is given in Sect. 1.1.

Current aircraft autopilot systems are primarily designed for operation under nominal conditions, and sometimes disengage and return control authority to the pilot under off-nominal conditions. Future aircraft control systems will be expected to provide resilience under off-nominal conditions and operate as a component of a larger resilient flight system. Control resilience will need to be designed into future systems 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 LOC accidents. The broader resilient flight system will include vehicle health management, flight safety management, and reliable crew interface management functions.

V&V becomes much more difficult for safety-critical resilient systems operating under off-nominal conditions. The objectives of this chapter are to address V&V issues associated with future safety-critical resilient flight systems operating under off-nominal conditions and to propose a comprehensive V&V research framework to address these issues. The remainder of Sect. 1 describes aircraft loss of control in more detail (Sect. 1.1) and presents a future resilient flight system concept (Sect. 1.2). Section 2 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 a research approach being taken at NASA. Section 3 presents a comprehensive V&V process that can serve as an initial research framework for addressing future integrated resilient flight systems. Section 4 briefly discusses the status of this research and references a detailed summary of research accomplishments made at NASA Langley. Section 5 provides a chapter summary and some concluding remarks. The primary emphasis of this chapter is on the validation component of V&V for advanced flight control systems.

1.1 Aircraft LOC

LOC remains one of the largest worldwide contributors to aircraft fatal accidents. For example, a summary of worldwide commercial jet airplane accidents from 2000 through 2009 [1] is shown in Fig. 1. As indicated in the figure, *inflight loss of control* (LOC-I) is the largest accident category for transport aircraft weighing more than 60,000 pounds, and resulted in 20 accidents and 1,848 total fatalities. The data in Fig. 1 show the number of fatalities for accident categories defined by the *Commercial Aviation Safety Team* (CAST) and the *International Civil Aviation Organization* (ICAO). A full definition of the CAST/ICAO accident categories is provided in Table 1.

Aircraft LOC is a highly complex event. Some contributors to aircraft LOC are denoted in Fig. 1. Although some LOC factors noted in Fig. 1 were not determined to be primary causal factors of any accidents in this class of vehicles (i.e., over 60,000 lbs.) during the stated time period, in general they have been found to contribute to LOC accidents and are therefore noted for completeness. Causal and contributing factors associated with aircraft LOC can occur individually, but more often occur in various combinations. A detailed analysis of 126 aircraft LOC accidents is presented in [2], in which worst case combinations of LOC accident precursors, i.e., causal and contributing factors, and their time sequences are identified. These factors, or “off-nominal

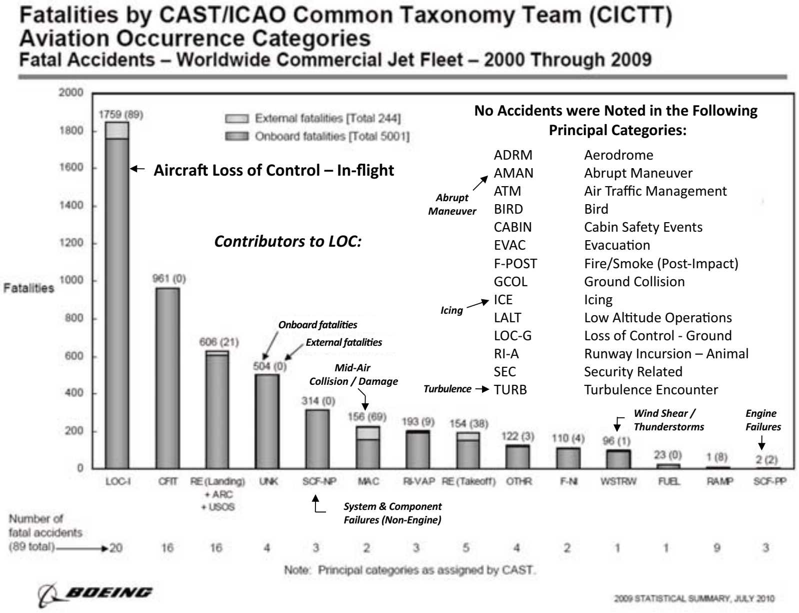

Fig. 1. Aircraft Accident Statistics for Worldwide Commercial Jet Fleet, 2000-2009 [1]

conditions," can be categorized as: adverse conditions occurring onboard the aircraft, including faults, failures, damage, crew error, etc.; external hazards and disturbances, including icing, wind shear, wake vortices, turbulence, terrain and obstacles, other aircraft, etc.; and abnormal flight or upset conditions, including unusual attitudes, stall, stall/departure, etc..

Aircraft LOC clearly involves operation under off-nominal conditions, which motivates the use of the term "off-nominal conditions" to designate the associated causal and contributing factors. LOC accidents occur across all vehicle classes, from small aircraft through large transports, and configuration types, from single to multiple engines, including both jet and propeller. LOC also occurs across all operational categories, scheduled and unscheduled, and flight phases, including takeoff, cruise, and approach.

Because of the scope and complexity of aircraft LOC events, i.e., accidents and incidents, there is no single intervention strategy for preventing them. Improved crew training and operational procedures for off-nominal conditions can enable improved crew response during LOC events. Advanced onboard systems that provide resilience to off-nominal conditions can enable improved situational awareness and vehicle response under LOC events. A holistic approach for preventing aircraft LOC accidents is presented in the next section.

Table 1. CAST/ICAO Accident Categories

AMAN	Abrupt Maneuver
ADRM	Aerodrome
ARC	Abnormal Runway Contact
ATM	Air Traffic Management/Communications, Navigation, Surveillance
CABIN	Cabin Safety Events
CFIT	Controlled Flight into or Toward Terrain
EVAC	Evacuation
F-NI	Fire/Smoke (Non-Impact)
F-POST	Fire/Smoke (Post-Impact)
FUEL	Fuel Related
GCOL	Ground Collision
ICE	Icing
LALT	Low Altitude Operations
LOC-G	Loss of Control – Ground
LOC-I	Loss of Control – In flight
MAC	Midair/Near Midair Collision
OTHR	Other
RAMP	Ground Handling
RE	Runway Excursion
RI-A	Runway Incursion – Animal
RI-VAP	Runway Incursion – Vehicle, Aircraft or Person
SEC	Security Related
SCF-NP	System/Component Failure or Malfunction (Non-Power Plant)
SCF-PP	System/Component Failure or Malfunction (Power Plant)
TURB	Turbulence Encounter
USOS	Undershoot/Overshoot
UNK	Unknown or Undetermined
WSTRW	Wind Shear or Thunderstorm

1.2 Future Advanced System Concept

Improved capabilities are needed for off-nominal conditions that enable effective crew training, enhanced situational awareness, and onboard resilience. Underlying technologies to achieve these capabilities have been the subject of research at NASA over the past decade, i.e., since the year 2000, within NASA's *Aviation Safety Program* (AvSP). Core technology areas of research include: 1.) dynamics modeling and simulation for off-nominal conditions; 2.) diagnostics and prognostics for detecting, identifying, and characterizing off-nominal conditions in real time or near real time; 3.) resilient control technologies for mitigation of off-nominal conditions and vehicle recovery; and 4.) crew interface technologies for improved situational awareness and decision support especially under off-nominal conditions.

These core technology areas must be coordinated during both development and operation. V&V technologies must also be developed and applied to these technology areas for an improved understanding of safe and unsafe regions of operation under off-nominal conditions, and for the ultimate certification of these technologies.

An integrated system concept can be developed based on these technologies for preventing aircraft LOC accidents in the future. One such future concept, called the *Aircraft Integrated Resilient Safety Assurance and Failsafe Enhancement* (AIRSAFE) System, is shown in Fig. 2.

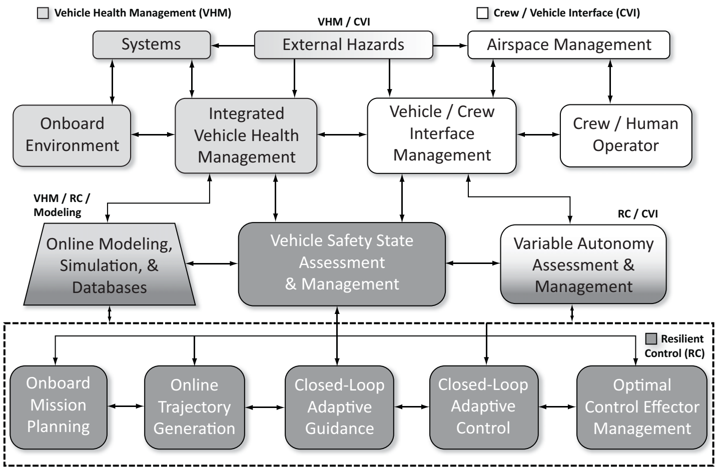
Vehicle Health Management (VHM)
VHM / CVI
Crew / Vehicle Interface (CVI)
Systems
External Hazards
Airspace Management
Onboard Environment
Integrated Vehicle Health Management
Vehicle / Crew Interface Management
Crew / Human Operator
VHM / RC / Modeling
RC / CVI
Online Modeling, Simulation, & Databases
Vehicle Safety State Assessment & Management
Variable Autonomy Assessment & Management
Resilient Control (RC)
Onboard Mission Planning
Online Trajectory Generation
Closed-Loop Adaptive Guidance
Closed-Loop Adaptive Control
Optimal Control Effector Management

Fig. 2. Aircraft Integrated Resilient Safety Assurance and Failsafe Enhancement (AIRSAFE) System Concept

The shading and block shapes of Fig. 2 designate the four core technology areas just discussed. Medium shading represents vehicle health management functions, no shading represents crew interface management functions, and dark shading represents flight safety management and resilient control functions. The trapezoidal shape represents modeling and simulation functions for off-nominal conditions. Multi-shaded blocks represent shared functions between multiple technology areas. A detailed description of the functional capabilities and interfaces associated with the AIRSAFE System concept is contained in [3, 4].

The V&V of future integrated systems, such as the AIRSAFE System concept of Fig. 2, poses numerous technical challenges. In particular, there is no current V&V capability for complex integrated safety-critical systems operating under off-nominal conditions. This problem is the subject of Sect. 2.

2 V&V Problem

The V&V of integrated safety-critical systems that are designed for operation under off-nominal conditions is a complex problem. 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.*

The terminology “extremely improbable” in FAR 25.1309 translates to an average probability per flight hour for catastrophic failure conditions of 10^{-9}, and “improbable” failure conditions are those having a probability on the order of 10^{-5} or less per flight hour (but greater than 10^{-9}). The development of a V&V process for demonstration of compliance to FAR/JAR 25.1309 is extremely challenging for complex integrated systems designed for operation under off-nominal conditions, such as the AIRSAFE System concept of Fig. 2. In fact, the V&V problem for these systems poses a key technology barrier to their implementation and transition into the fleet. 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, or even for adaptive and potentially non-deterministic systems. The following subsections discuss V&V problem complexity and key technical challenges for the AIRSAFE future system concept, V&V process requirements for meeting those challenges, and a research approach being taken at NASA to address V&V of future safety-critical systems.

2.1 V&V Problem Complexity and Technical Challenges

V&V of safety-critical integrated systems operating under off-nominal conditions can be thought of and analyzed as a complex multidimensional problem [5]. 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 and variable autonomy 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 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-factor-based and require information processing, and variable autonomy will require assessment and reasoning algorithms. Onboard modeling functions will involve system identification algorithms and databases. All four core functions are software based and will involve various levels of logic and discrete mathematics-based abstractions and combinations. Subsystem integration will also involve significant software and possible hardware complexity.

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, safe operation under off-nominal conditions that could lead to LOC 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 [6] 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.

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 subsystem 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 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 LOC 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. 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 or easily obtained
  - Can involve multidisciplinary coupled effects
  - Cannot fully replicate in-flight LOC environment
- V&V of Adaptive Diagnostic, Prognostic, and Control Algorithms Operating under Off-Nominal Conditions
  - Involves a variety of nonlinear mathematical constructs (e.g., 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 and metrics for establishing off-nominal condition coverage, reliability, and accuracy for diverse algorithms and 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, as presented in Sect. 2.2.

2.2 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 a level of confidence in this compliance.

Key components of the V&V process include algorithm validation, system 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 LOC 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, 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 Fig. 3. 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 Fig. 3 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 subprocess 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 3 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, including parameter variations and unmodeled system dynamics, and disturbances, including 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. Crew interface and variable autonomy algorithms must be evaluated for handling qualities and interface effectiveness, and *aircraft-*

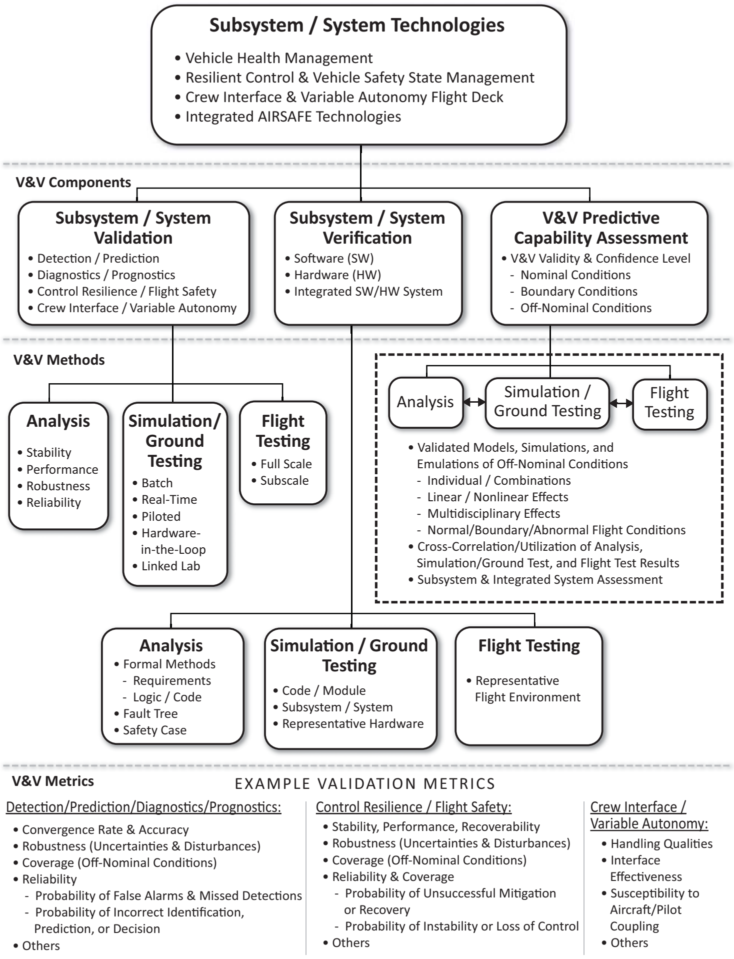
Subsystem / System Technologies
• Vehicle Health Management
• Resilient Control & Vehicle Safety State Management
• Crew Interface & Variable Autonomy Flight Deck
• Integrated AIRSAFE Technologies
V&V Components
Subsystem / System Validation
• Detection / Prediction
• Diagnostics / Prognostics
• Control Resilience / Flight Safety
• Crew Interface / Variable Autonomy
Subsystem / System Verification
• Software (SW)
• Hardware (HW)
• Integrated SW/HW System
V&V Predictive Capability Assessment
• V&V Validity & Confidence Level
- Nominal Conditions
- Boundary Conditions
- Off-Nominal Conditions
V&V Methods
Analysis
• Stability
• Performance
• Robustness
• Reliability
Simulation/ Ground Testing
• Batch
• Real-Time
• Piloted
• Hardware-in-the-Loop
• Linked Lab
Flight Testing
• Full Scale
• Subscale
Analysis
Simulation / Ground Testing
Flight Testing
• Validated Models, Simulations, and Emulations of Off-Nominal Conditions
- Individual / Combinations
- Linear / Nonlinear Effects
- Multidisciplinary Effects
- Normal/Boundary/Abnormal Flight Conditions
• Cross-Correlation/Utilization of Analysis, Simulation/Ground Test, and Flight Test Results
• Subsystem & Integrated System Assessment
Analysis
• Formal Methods
- Requirements
- Logic / Code
• Fault Tree
• Safety Case
Simulation / Ground Testing
• Code / Module
• Subsystem / System
• Representative Hardware
Flight Testing
• Representative Flight Environment
V&V Metrics
EXAMPLE VALIDATION METRICS
Detection/Prediction/Diagnostics/Prognostics:
• Convergence Rate & Accuracy
• Robustness (Uncertainties & Disturbances)
• Coverage (Off-Nominal Conditions)
• Reliability
- Probability of False Alarms & Missed Detections
- Probability of Incorrect Identification, Prediction, or Decision
• Others
Control Resilience / Flight Safety:
• Stability, Performance, Recoverability
• Robustness (Uncertainties & Disturbances)
• Coverage (Off-Nominal Conditions)
• Reliability & Coverage
- Probability of Unsuccessful Mitigation or Recovery
- Probability of Instability or Loss of Control
• Others
Crew Interface / Variable Autonomy:
• Handling Qualities
• Interface Effectiveness
• Susceptibility to Aircraft/Pilot Coupling
• Others

Fig. 3. V&V Process Requirements for the AIRSAFE System Concept

pilot coupling (APC), or *pilot-induced oscillation* (PIO), susceptibility under off-nominal conditions. Moreover, real-time partitioning effectiveness between the human and automation 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 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. Fault-tree and safety case analyses of the system implementation must also be performed. 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 representative avionics hardware systems and flight environments under nominal and off-nominal conditions. Although none are given in Fig. 3, verification metrics must be clearly defined and evaluated.

V&V predictive capability assessment is an evaluation of the validity and a level of confidence that can be placed in the V&V process and its results for operation under nominal and off-nominal conditions. The need for this evaluation arises from the inability to fully evaluate these technologies under actual LOC 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 during design. 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.

2.3 Research Approach

An approach taken at NASA for addressing V&V has been in the development of metrics, methods, software tools, and testbeds that facilitate the evaluation of safety-critical systems operating under off-nominal conditions. A high-level V&V concept was developed which integrates analytical, simulation, and experimental methods. Analytical methods must be developed, with theoretical extensions where needed, as well as user-friendly software tools to assess algorithm stability, performance, robustness, and reliability under off-nominal conditions. Simulation methods must be developed to facilitate Monte Carlo analysis and piloted evaluations under off-nominal conditions. In addition, advanced high-fidelity databases, models, and simulation enhancements must be developed to characterize off-nominal conditions and their impacts on vehicle dynamics and control. Experimental testbeds must be 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 must also be demonstrated, evaluated, and refined using realistic LOC test scenarios, subsystems, and systems. The following sections present a V&V research framework developed at NASA Langley and a brief summary of recent accomplishments in this research.

3 V&V Process and Research Framework

Based on the V&V process requirements of Fig. 3, a detailed V&V process can be developed for complex integrated resilient systems, such as the AIRSAFE System concept of Fig. 2. A high-level overview of the integrated V&V process is presented in Fig. 4. The shading of the blocks correlates to core AIRSAFE subsystem functions depicted in Fig. 2 – that is, dark gray correlates to resilient control functions, light gray represents health management functions, and white is associated with crew interface functions. Multi-shaded boxes in Fig. 4 represent evaluation of the associated integrated subsystem functions. Analysis, simulation, and experimental V&V components are organized in the V&V process of Fig. 4 moving from left to right, and system evaluation becomes more highly integrated moving to the center and to the right. Also as indicated in Fig. 4, 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 control-related components of the V&V process, including methods and interfaces. This is depicted in Fig. 4 by the dotted box around the lower two rows of the process. Reference [5] provides a detailed description of the entire process.

A set of recommended V&V methods for resilient control system functions is presented in Figs. 5 and 6, which depict analysis and simulation methods and simulation and experimental methods, respectively. For process continuity, the right-most blocks of Fig. 5 are repeated as the left-most blocks of Fig. 6. 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.

The "Stability and Performance Analysis" block in the lower left of Fig. 5 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 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 (see Chap. **??**) as well as nonlinear extensions (see Chap. **??**) for analyzing stability and performance robustness to uncertainties. Uncertainty modeling

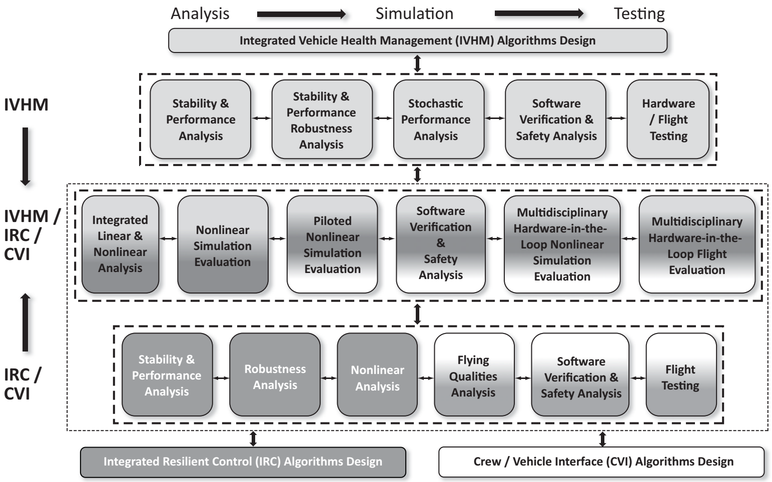
Analysis
Simulation
Testing
Integrated Vehicle Health Management (IVHM) Algorithms Design
IVHM
Stability & Performance Analysis
Stability & Performance Robustness Analysis
Stochastic Performance Analysis
Software Verification & Safety Analysis
Hardware / Flight Testing
IVHM / IRC / CVI
Integrated Linear & Nonlinear Analysis
Nonlinear Simulation Evaluation
Piloted Nonlinear Simulation Evaluation
Software Verification & Safety Analysis
Multidisciplinary Hardware-in-the-Loop Nonlinear Simulation Evaluation
Multidisciplinary Hardware-in-the-Loop Flight Evaluation
IRC / CVI
Stability & Performance Analysis
Robustness Analysis
Nonlinear Analysis
Flying Qualities Analysis
Software Verification & Safety Analysis
Flight Testing
Integrated Resilient Control (IRC) Algorithms Design
Crew / Vehicle Interface (CVI) Algorithms Design

Fig. 4. V&V Process Overview

methods that generate a *Linear Fractional Representation* (LFR) of the uncertain system must be utilized for characterizing linear and nonlinear parameter variations (see Chaps. **??**–**??**) 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 Fig. 5 includes bifurcation analysis of nonlinear dynamic and controlled systems, controllability and observability in a nonlinear sense, such as degree of controllability and observability as a function of the changing parameters, and safe set and recoverability analysis. 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 or impaired vehicles must also be considered. A method for analytically determining the Probability of LOC in a nonlinear sense must also be developed.

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

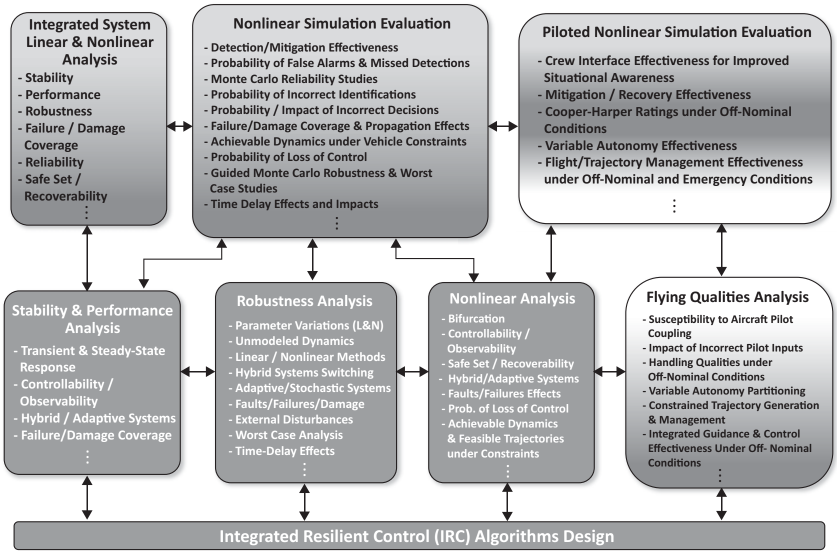
Integrated System Linear & Nonlinear Analysis
- Stability
- Performance
- Robustness
- Failure / Damage Coverage
- Reliability
- Safe Set / Recoverability
Nonlinear Simulation Evaluation
- Detection/Mitigation Effectiveness
- Probability of False Alarms & Missed Detections
- Monte Carlo Reliability Studies
- Probability of Incorrect Identifications
- Probability / Impact of Incorrect Decisions
- Failure/Damage Coverage & Propagation Effects
- Achievable Dynamics under Vehicle Constraints
- Probability of Loss of Control
- Guided Monte Carlo Robustness & Worst Case Studies
- Time Delay Effects and Impacts
Piloted Nonlinear Simulation Evaluation
- Crew Interface Effectiveness for Improved Situational Awareness
- Mitigation / Recovery Effectiveness
- Cooper-Harper Ratings under Off-Nominal Conditions
- Variable Autonomy Effectiveness
- Flight/Trajectory Management Effectiveness under Off-Nominal and Emergency Conditions
Stability & Performance Analysis
- Transient & Steady-State Response
- Controllability / Observability
- Hybrid / Adaptive Systems
- Failure/Damage Coverage
Robustness Analysis
- Parameter Variations (L&N)
- Unmodeled Dynamics
- Linear / Nonlinear Methods
- Hybrid Systems Switching
- Adaptive/Stochastic Systems
- Faults/Failures/Damage
- External Disturbances
- Worst Case Analysis
- Time-Delay Effects
Nonlinear Analysis
- Bifurcation
- Controllability / Observability
- Safe Set / Recoverability
- Hybrid/Adaptive Systems
- Faults/Failures Effects
- Prob. of Loss of Control
- Achievable Dynamics & Feasible Trajectories under Constraints
Flying Qualities Analysis
- Susceptibility to Aircraft Pilot Coupling
- Impact of Incorrect Pilot Inputs
- Handling Qualities under Off-Nominal Conditions
- Variable Autonomy Partitioning
- Constrained Trajectory Generation & Management
- Integrated Guidance & Control Effectiveness Under Off- Nominal Conditions
Integrated Resilient Control (IRC) Algorithms Design

Fig. 5. V&V Process for Resilient Control Functions – Analysis and Simulation Methods

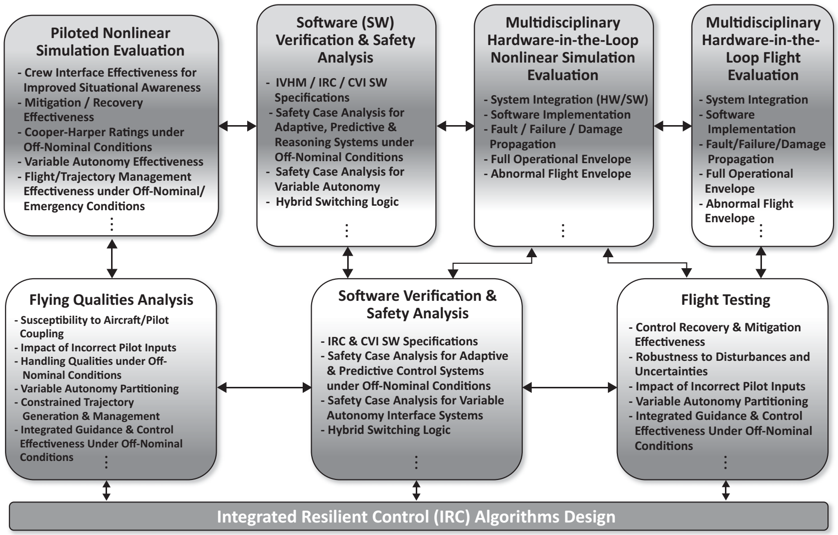
Piloted Nonlinear Simulation Evaluation
- Crew Interface Effectiveness for Improved Situational Awareness
- Mitigation / Recovery Effectiveness
- Cooper-Harper Ratings under Off-Nominal Conditions
- Variable Autonomy Effectiveness
- Flight/Trajectory Management Effectiveness under Off-Nominal/ Emergency Conditions
Software (SW) Verification & Safety Analysis
- IVHM / IRC / CVI SW Specifications
- Safety Case Analysis for Adaptive, Predictive & Reasoning Systems under Off-Nominal Conditions
- Safety Case Analysis for Variable Autonomy
- Hybrid Switching Logic
Multidisciplinary Hardware-in-the-Loop Nonlinear Simulation Evaluation
- System Integration (HW/SW)
- Software Implementation
- Fault / Failure / Damage Propagation
- Full Operational Envelope
- Abnormal Flight Envelope
Multidisciplinary Hardware-in-the-Loop Flight Evaluation
- System Integration
- Software Implementation
- Fault/Failure/Damage Propagation
- Full Operational Envelope
- Abnormal Flight Envelope
Flying Qualities Analysis
- Susceptibility to Aircraft/Pilot Coupling
- Impact of Incorrect Pilot Inputs
- Handling Qualities under Off-Nominal Conditions
- Variable Autonomy Partitioning
- Constrained Trajectory Generation & Management
- Integrated Guidance & Control Effectiveness Under Off-Nominal Conditions
Software Verification & Safety Analysis
- IRC & CVI SW Specifications
- Safety Case Analysis for Adaptive & Predictive Control Systems under Off-Nominal Conditions
- Safety Case Analysis for Variable Autonomy Interface Systems
- Hybrid Switching Logic
Flight Testing
- Control Recovery & Mitigation Effectiveness
- Robustness to Disturbances and Uncertainties
- Impact of Incorrect Pilot Inputs
- Variable Autonomy Partitioning
- Integrated Guidance & Control Effectiveness Under Off-Nominal Conditions
Integrated Resilient Control (IRC) Algorithms Design

Fig. 6. V&V Process for Resilient Control Functions – Simulation and Experimental Methods

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 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 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 failures or damage; and time delay effects associated with failure detection, identification, and mitigation. Guided Monte Carlo studies, 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 of 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, using Cooper-Harper metrics and extensions; variable autonomy interface effectiveness; and flight/trajectory management under off-nominal and emergency conditions.

Fig. 6 shows the progression to subsystem and integrated system evaluations that involve the software/hardware implementations. 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, using both full-scale and sub-scale vehicles. 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. Sub-scale 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* (CVI) in flight while using the appropriate timescale.

The V&V process depicted in Figs. 5 and 6 is integrated across the various methods, with information being exchanged between each block. Information exchange is indicated with double-headed arrows. Reference [5] provides a detailed description of information exchange throughout the process. As an example, consider a subset of the process shown in Fig. 5 and depicted below in Fig. 7.

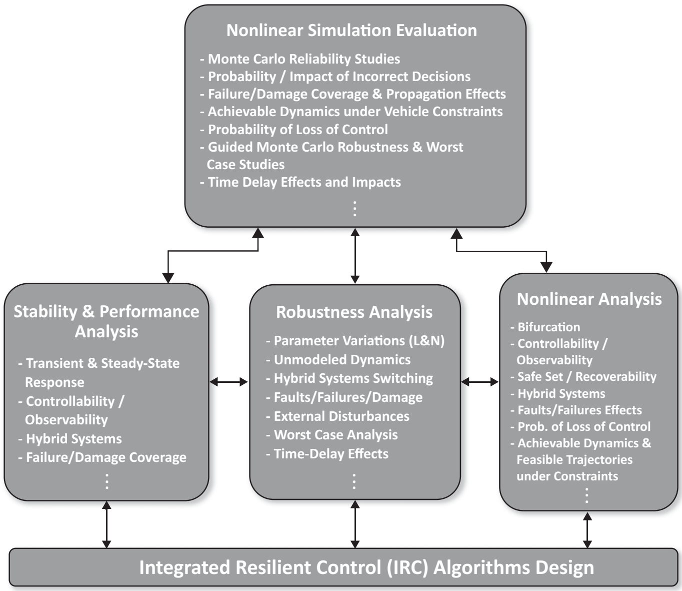
Nonlinear Simulation Evaluation
- Monte Carlo Reliability Studies
- Probability / Impact of Incorrect Decisions
- Failure/Damage Coverage & Propagation Effects
- Achievable Dynamics under Vehicle Constraints
- Probability of Loss of Control
- Guided Monte Carlo Robustness & Worst Case Studies
- Time Delay Effects and Impacts
⋮
Stability & Performance Analysis
- Transient & Steady-State Response
- Controllability / Observability
- Hybrid Systems
- Failure/Damage Coverage
⋮
Robustness Analysis
- Parameter Variations (L&N)
- Unmodeled Dynamics
- Hybrid Systems Switching
- Faults/Failures/Damage
- External Disturbances
- Worst Case Analysis
- Time-Delay Effects
⋮
Nonlinear Analysis
- Bifurcation
- Controllability / Observability
- Safe Set / Recoverability
- Hybrid Systems
- Faults/Failures Effects
- Prob. of Loss of Control
- Achievable Dynamics & Feasible Trajectories under Constraints
⋮
Integrated Resilient Control (IRC) Algorithms Design

Fig. 7. V&V Subprocess for Resilient Control Functions – Analysis and Simulation Methods

This figure contains analysis and simulation methods that are applied to the resilient control functions. To illustrate information exchange between subprocess components, consider a subset of these methods as presented in Fig. 8.

Starting with the lower left block of Fig. 8, failure/damage scenarios are evaluated in the "Stability and Performance Analysis" block based on the failure and damage profiles being mitigated in the resilient control design. The stability and performance analysis results define the effective coverage of these failure/damage scenarios. This information can be provided for use in the "Robustness Analysis" block to generate parametric and non-parametric uncertainty models, 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 uncertainty combinations. These results can be utilized by the nonlinear analysis tools, such as bifurcation,

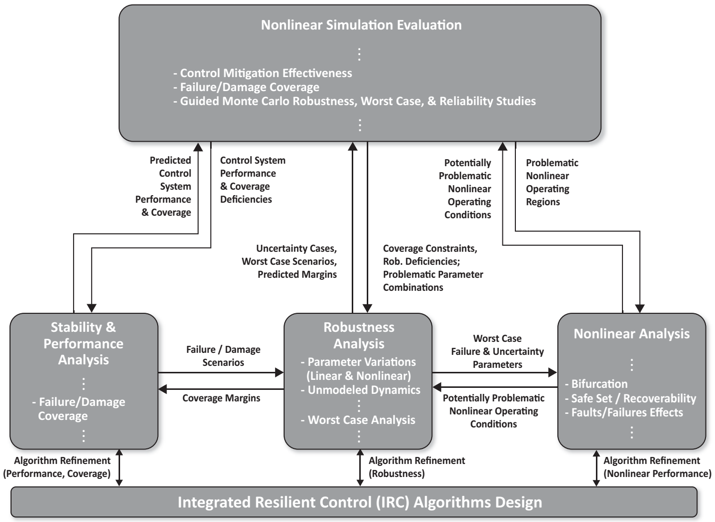
Nonlinear Simulation Evaluation
- Control Mitigation Effectiveness
- Failure/Damage Coverage
- Guided Monte Carlo Robustness, Worst Case, & Reliability Studies
Predicted Control System Performance & Coverage
Control System Performance & Coverage Deficiencies
Uncertainty Cases, Worst Case Scenarios, Predicted Margins
Coverage Constraints, Rob. Deficiencies; Problematic Parameter Combinations
Potentially Problematic Nonlinear Operating Conditions
Problematic Nonlinear Operating Regions
Stability & Performance Analysis
- Failure/Damage Coverage
Failure / Damage Scenarios
Coverage Margins
Robustness Analysis
- Parameter Variations (Linear & Nonlinear)
- Unmodeled Dynamics
- Worst Case Analysis
Worst Case Failure & Uncertainty Parameters
Potentially Problematic Nonlinear Operating Conditions
Nonlinear Analysis
- Bifurcation
- Safe Set / Recoverability
- Faults/Failures Effects
Algorithm Refinement (Performance, Coverage)
Algorithm Refinement (Robustness)
Algorithm Refinement (Nonlinear Performance)
Integrated Resilient Control (IRC) Algorithms Design

Fig. 8. Example V&V Subprocess Interfaces for Resilient Control Functions – Analysis and Simulation Methods

safe set and recoverability, and failure effect analyses, to identify potentially problematic nonlinear operating regions. The nonlinear analysis results can be utilized in re-evaluating robustness in these regions. Analysis results related to stability and performance, such as failure/damage coverage predictions, robustness, including uncertainties, worst case scenarios, and predicted margins, and nonlinear properties, such as potentially problematic operating conditions, are utilized, corroborated, or disputed during nonlinear simulation evaluations. Simulation results are then utilized by the analysis components during re-evaluation. The analysis and simulation results are also utilized as part of an iterative design process. Each evaluation method provides a basis for improved system design, as depicted in Fig. 8. The subsequent analysis and simulation results might then be utilized to generate test scenarios for use in piloted simulation evaluations (not shown in Fig. 8). It is conjectured that the use of analytical, simulation, and experimental results in a coordinated manner will provide a means to effectively and efficiently identify problematic flight conditions, off-nominal conditions, uncertainties, and combinations of these without having to perform exhaustive testing.

Recent NASA research that pertains to the V&V process thus described is briefly summarized and referenced in Sect. 4.

4 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 system 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 [7, 8]. These results are summarized in [9]. 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 [10]. This new effort will develop V&V methods that can be applied to the Next Generation Air Transportation System.

5 Summary and Concluding Remarks

Aircraft loss of control is a significant contributor to accidents and fatalities, resulting 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 occur individually or more often combine to result in a loss of control 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 flight deck technologies; and to provide the capability to mitigate off-nominal conditions through the development of resilient aircraft control technologies. A future technology concept, called the AIRSAFE System, for integrating these technologies and providing onboard flight safety assurance is envisioned. These technologies are being developed for safety-critical operation under off-nominal conditions.

The V&V of safety-critical systems operating under off-nominal conditions poses significant technical challenges. This chapter has provided an analysis of this V&V problem, and has described a research approach being taken at NASA to address it. High-level V&V process requirements were defined, which integrate 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 was provided of the methods and some example interfaces involved in the controls-related components. Research progress at NASA in the development of analytical, simulation, and experimental methods was briefly discussed and referenced.

Acknowledgement and Dedication The V&V research process, methods and software tools, and the AIRSAFE System concept presented in this chapter were developed in collaboration with Dr. Celeste M. Belcastro of NASA Langley Research Center, who lost her selfless and courageous battle with cancer and passed from this life on August 22, 2008. This chapter and continued work in this area are dedicated to her memory.

References

1. "Statistical Summary of Commercial Jet Airplane Accidents, Worldwide Operations, 1959-2009". Boeing Commercial Airplanes, July 2010. URL: `http://www.boeing.com/news/techissues/pdf/statsum.pdf`
2. C. M. Belcastro and J. V. Foster. Aircraft Loss-of-Control Accident Analysis. *AIAA Guidance, Navigation and Control Conference, Toronto, Canada*, 2010.
3. C. M. Belcastro and C. M. Belcastro. Future Research Directions for the Development of Integrated Resilient Flight Systems to Prevent Aircraft Loss-of-Control Accidents, Part I: System Technologies. NASA TM. (Under final preparation)
4. C. M. Belcastro and S. Jacobson. Future Integrated Systems Concept for Preventing Aircraft Loss-of-Control Accidents. AIAA Guidance, Navigation and Control Conference, Toronto, August 2-5, 2010.
5. C. M. Belcastro and C. M. Belcastro. 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. (Under preparation)
6. Joint Planning and Development Office, Concept of Operations for the Next Generation Air Transportation System, Version 3, October 2009. URL: `http://www.jpdo.gov/library.asp`
7. C. M. Belcastro and C. M. Belcastro. On the Validation of Safety Critical Aircraft Systems, Part I: An Overview of Analytical & Simulation Methods. *AIAA Guidance, Navigation and Control Conference, Austin, Texas, USA*, 2003.
8. C. M. Belcastro and C. M. Belcastro. On the Validation of Safety Critical Aircraft Systems, Part II: An Overview of Experimental Methods. *AIAA Guidance, Navigation and Control Conference, Austin, Texas, USA*, 2003.
9. C. M. Belcastro. Validation and Verification of Future Integrated Safety-Critical Systems Operating under Off-Nominal Conditions. *AIAA Guidance, Navigation and Control Conference, Toronto, Canada*, 2010.
10. Validation and Verification for Flight-Critical Systems Assessment of Critical Research Activities. NASA Aeronautics Research Mission Directorate, Aviation Safety Program, November 25, 2009.

Table 2. Abbreviations and acronyms

ADRM	Aerodrome
AIRSAFE	Aviation Integrated Resilient Safety Assurance and Failsafe Enhancement
AMAN	Abrupt Maneuver
ARC	Abnormal Runway Contact
ATM	Air Traffic Management
AvSP	Aviation Safety Program
CAST	Commercial Aviation Safety Team
CFIT	Controlled Flight Into or Toward Terrain
CVI	Crew/Vehicle Interface
EVAC	Evacuation
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
F-NI	Fire/Smoke (Non-Impact)
F-POST	Fire/Smoke (Post-Impact)
GCOL	Ground Collision
HW	Hardware
ICAO	International Civil Aviation Organization
ICE	Icing
IRC	Integrated Resilient Control
IVHM	Integrated Vehicle Health Management
JAA	Joint Aviation Authorities
LFR	Linear Fractional Representation
LOC	loss of control
LOC-G	Loss of Control - Ground
LOC-I	Loss of Control - In flight
LALT	Low Altitude Operations
L&N	Linear and Nonlinear
NASA	National Aeronautics and Space Administration
MAC	Midair/Near Midair Collision
OTHR	Other
PIO	Pilot-Induced Oscillation
RAMP	Ground Handling
RC	Resilient Control
RE	Runway Excursion
RI-A	Runway Incursion - Animal
RI-VAP	Runway Incursion - Vehicle, Aircraft or Person
SEC	Security
SCF-NP	System/Component Failure or Malfunction (Non-Power Plant)
SCF-PP	System/Component Failure or Malfunction (Power Plant)
SW	Software
TURB	Turbulence Encounter
USOS	Undershoot/Overshoot
UNK	Unknown or Undetermined
VHM	Vehicle Health Management
V&V	Validation and Verification
WSTRW	Wind Shear or Thunderstorm

Index