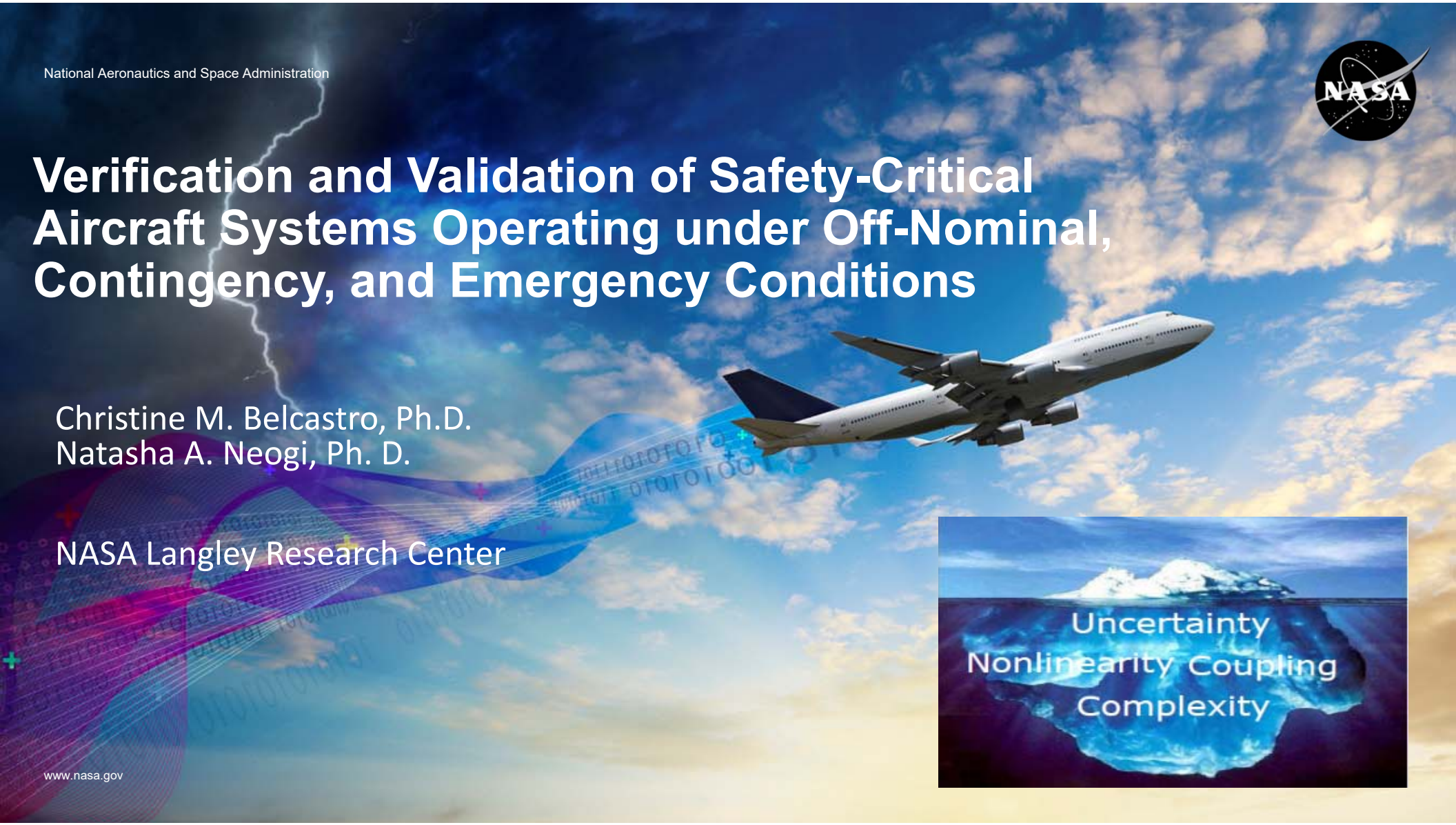
National Aeronautics and Space Administration



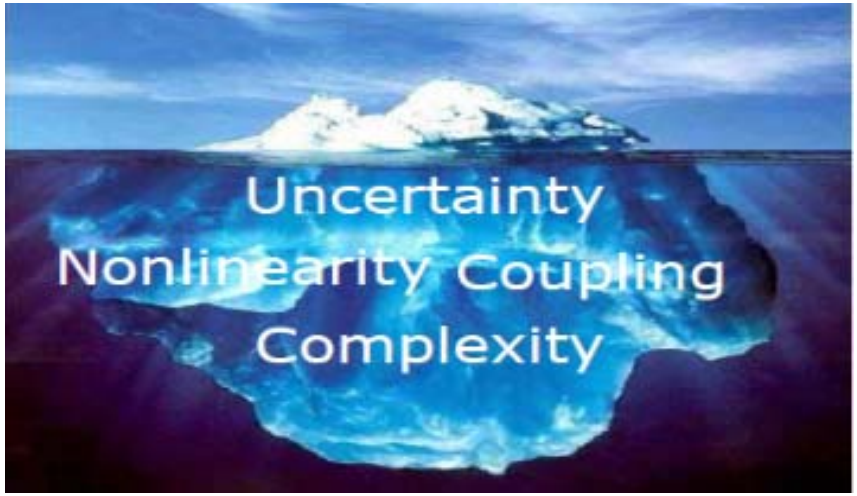
Verification and Validation of Safety-Critical Aircraft Systems Operating under Off-Nominal, Contingency, and Emergency Conditions

Christine M. Belcastro, Ph.D.
Natasha A. Neogi, Ph. D.

NASA Langley Research Center

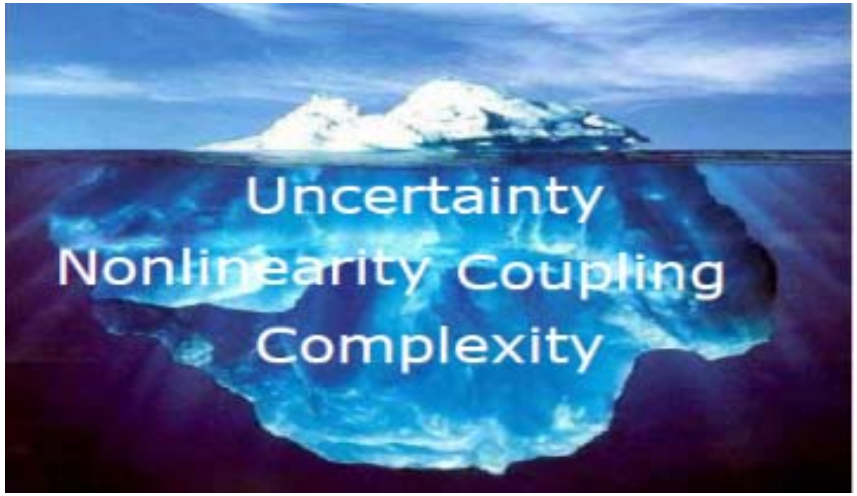
Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions

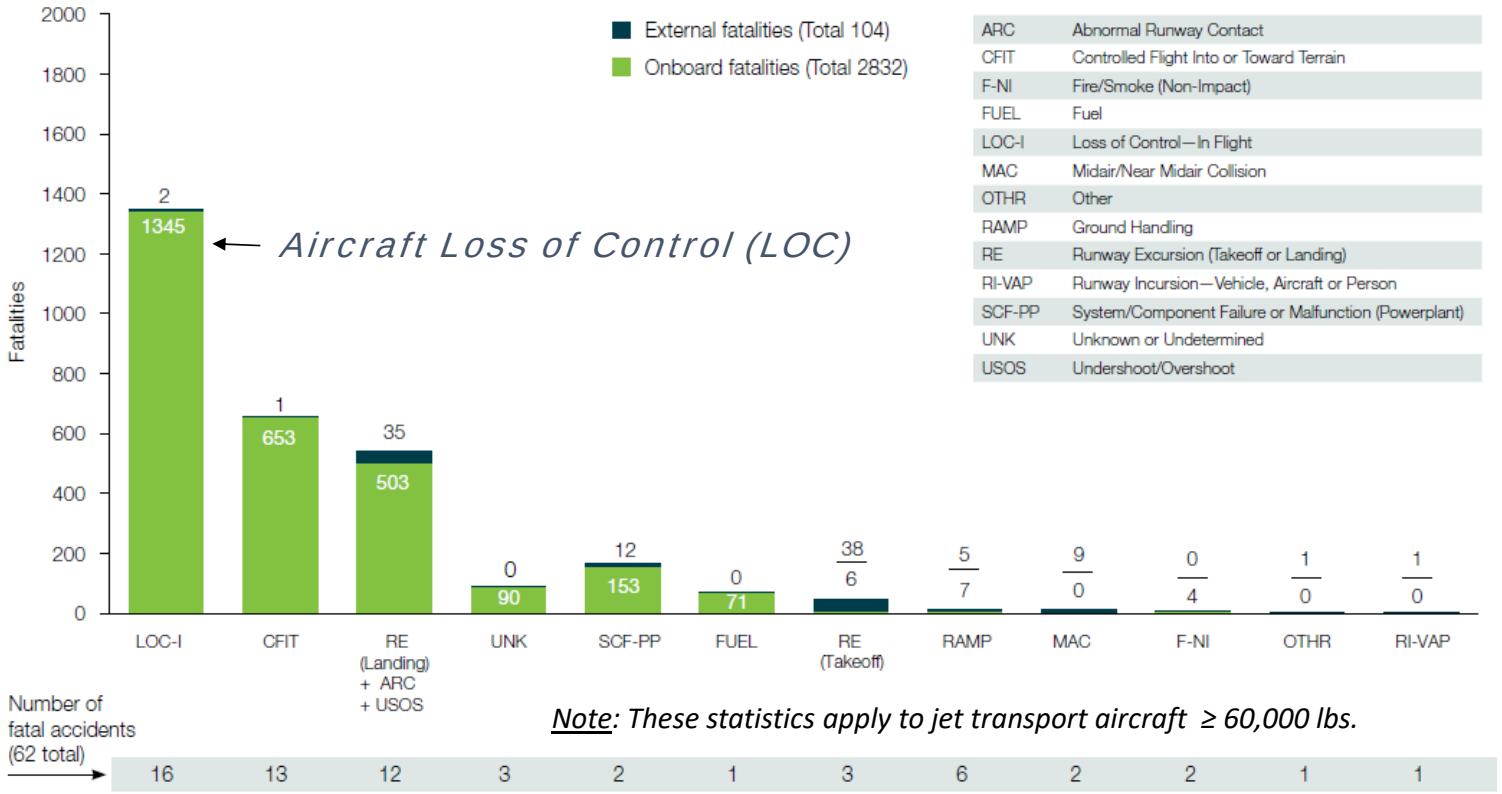


Definitions

- Validation
  - Confirmation that the system implementation (e.g., algorithms, etc.) is performing the intended function(s)
  - Affirmation of system effectiveness in these functions
- Verification
  - Confirmation that the system implementation in the software and hardware meets its (hopefully validated) specifications (e.g., correctly executes algorithms as designed)
- Certification
  - Formal procedure by which authorized agency assesses and verifies that products/procedures comply with established requirements or standards

Current Aviation Safety Issues

Fatal Accidents for Worldwide Commercial Jet Fleet (2007 – 2016)



ARC	Abnormal Runway Contact
CFIT	Controlled Flight Into or Toward Terrain
F-NI	Fire/Smoke (Non-Impact)
FUEL	Fuel
LOC-I	Loss of Control—In Flight
MAC	Midair/Near Midair Collision
OTHR	Other
RAMP	Ground Handling
RE	Runway Excursion (Takeoff or Landing)
RI-VAP	Runway Incursion—Vehicle, Aircraft or Person
SCF-PP	System/Component Failure or Malfunction (Powerplant)
UNK	Unknown or Undetermined
USOS	Undershoot/Overshoot

Note: These statistics apply to jet transport aircraft ≥ 60,000 lbs.

Ref: Boeing Statistical Summary of Commercial Jet Airplane Accidents, Worldwide Operations 1959 - 2016

Hazards Leading to Aircraft LOC

LOC Characteristics

Generally, LOC is described as motion that is: *

- outside normal envelopes
- not predictably altered by pilot control inputs
- characterized by nonlinear effects,
- disproportionately large responses to small state variable changes,
- oscillatory/divergent behavior
- likely to result in high angular rates / displacements,
- characterized by the inability to maintain heading, altitude, and wings-level flight

Primary Causes

1. Entry into vehicle upset condition (e.g., Stall)
2. Reduction or loss of control effectiveness
3. Changes to vehicle dynamic response and handling / flying qualities
4. Combinations of the above (1-3)

Causal & Contributing Factors

- **Adverse onboard conditions**:
  - **vehicle impairment**
    - » Inappropriate vehicle configuration, contaminated airfoil, improper loading, vehicle damage to airframe and engines
  - **system faults, failures, and errors**
    - » Control component, engine, sensor system, flight deck instrumentation, non-control component
  - **crew action / inaction**
    - » Loss of aircraft attitude, energy, or system state awareness, aggressive maneuver, abnormal control input, ineffective recovery, improper procedure, crew fatigue / impairment
- **External hazards and disturbances**:
  - **inclement weather & atmospheric disturbances**
    - » wind shear, turbulence, rain / thunderstorms, snow / icing, wake vortices
  - **poor visibility** (fog / haze, night)
  - **obstacle** (fixed or moving)
- **Abnormal dynamics & vehicle upsets**:
  - abnormal vehicle dynamics & control response
  - abnormal attitude, airspeed, angular rates, asymmetric forces, or flight trajectory
  - uncontrolled descent (including spiral dive)
  - stall/departure from controlled flight

* Wilborn, J. E. and Foster, J. V., "Defining Commercial Aircraft Loss-of-Control: a Quantitative Approach," *AIAA Atmospheric Flight Mechanics Conference and Exhibit, AIAA, Providence, Rhode Island, 16-19 August 2004.*

NASA Holistic Technical Approach to LOC

Prevent

- Improved Crew Training under LOC Precursor Conditions

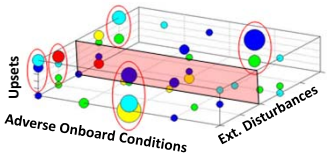
Detect | **Mitigate** | **Recover**

Normal Flight → **Vehicle Problem / External Hazard** → **Inappropriate Crew Response** → **Vehicle Upset** → Safe Flight

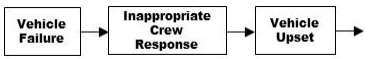
- Vehicle Impairment, Fault, Failure, Damage
- External Hazard / Disturbance
- Poor Situational Awareness / Distraction
- Spatial Disorientation (Poor Visibility)
- Mode Confusion (System Complexity)
- Abnormal Attitudes
- Abnormal Trajectory
- Stall/Departure

Problem Definition

LOC Hazards Analysis



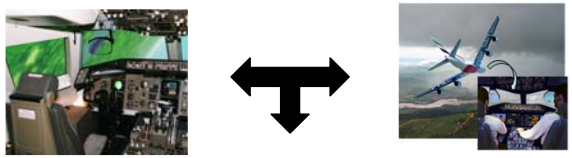
- **Crew Action / Inaction**
- **Vehicle / System**
- **Environmental / Atmospheric**
- **Vehicle Upsets**



New / Emergent Risks

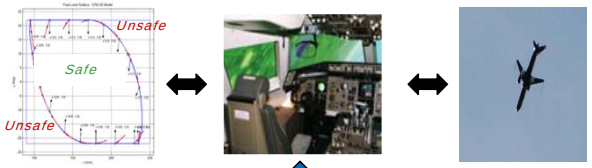
Technology Development & Evaluation

Vehicle Dynamics Modeling | **Guidance, Control & Systems**



Comprehensive Technology Validation

Analysis | ***Simulation*** | ***Testing***



LOC Test Scenarios ↕ ***Evaluation Requirements***

LOC RWG (Industry, Government, Academia)

Technology Products

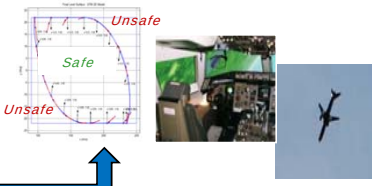
Improved Crew Training *under LOC Hazards*

Enhanced Representative Simulation Methods & Models

Improved Situational Awareness, Guidance & Control *under LOC Hazards*

Enhanced Onboard Systems Technologies

Improved Validation Methods & Tools for Safety-Critical Resilient Systems



Technology Transition

Emerging Aviation Safety Issues

- Increasing Levels of System Complexity & Autonomy
- Pilot-Optional Operations
- Bounding Behavior of Increasingly Autonomous Systems
- Trusted Autonomous Decision Making
- Human-Machine System Integration
- Non-Determinism and Uncertainty
- Security and Data Integrity
- Insufficient V&V Capabilities for Complex and Autonomous Systems
- Insufficient Evidence-Based Certification of Complex and Autonomous Systems

V&V Implications for Safety-Critical Systems (1)

- Current: *Aircraft Dynamics and Control Limitations under Hazardous Conditions can lead to LOC*
  - Until recently, crew training under LOC conditions is limited due to simulation model limitations for full stall conditions, failures and damage, and environmental hazards (Work by NASA and others enabled improved stall training for pilots)
  - Information currently provided to the crew does not clearly inform of impending LOC
  - Current autopilot systems are designed for nominal operations and often disengage under off-nominal conditions
  - Current envelope protection systems may provide limited capabilities and disengage under sensor failures or extreme upset conditions
  - Current validation methods are limited for evaluating advanced system technologies for resilience under hazards and under highly nonlinear flight conditions

- Future: *Potential Increase in LOC Accidents Resulting from*
  - Increasing demand on the National airspace requiring high-density operations
  - Increased demand on crew & automated systems
  - Potential for Increased external hazard encounters (wakes, weather)
  - New efficient vehicle configurations with higher flexibility
  - Increasing trend towards autonomous systems

Advanced V&V Methods and Evidence-Based Certification Process Needed to Identify Problematic Conditions Up Front for Increasingly Complex Systems and under Potentially Hazardous (Expected and Unexpected) Conditions

V&V Implications for Safety-Critical Systems (2)

Example: F-18 Falling Leaf

- U.S. Navy F/A-18 Hornet (Early Versions with Baseline Control Law) Experienced Out-of-Control Falling Leaf Flight Departures
  - Numerous Mishaps
  - Loss of Airplane & Pilot
- NASA Participated in Analysis to Identify Cause of Problem (Starting in 1996)
  - Post-Stall Mode of Instability
    - » Sustained Out-of-Control Oscillatory Motion
    - » Nonlinear Instability Mode
    - » Lack of Directional Stability Causes In-Phase Roll / Yaw Rates
    - » Exacerbated by Centerline Tank & Aft C.G.
  - Difficult to Assess Control System for Susceptibility (Using Current Linear Methods)
    - » Baseline Control System was Extensively Tested Prior to Entry into Service
      - Susceptibility to Falling Leaf Mode Not Identified During Analysis
    - » Indicates Current V&V Capability Unable to Fully Capture Nonlinear Phenomena
- Revised Control System Successfully Suppressed Falling Leaf Motion (Introduced on the F/A-18E/F Super Hornet in 2001)

https://www.youtube.com/watch?v=pdftTMpXXCQ

Refs:

- Foster, John V.; "Investigation of the Susceptibility of Fighter Airplanes to the Out-of-Control Falling Leaf Mode", NASA/TP-2001-211048, August, 2001
- Chakraborty, A., Seiler, P., and Balas, G. J., "Susceptibility of F/A-18 Flight Controllers to the Falling-Leaf Mode: Linear Analysis," *Journal of Guidance, Control, and Dynamics*, Vol. 34, No. 1, Jan.–Feb. 2011

Current V&V Methods were Unable to Identify Susceptibility to Falling Leaf or Limitations of Baseline Control System

V&V Implications for Safety-Critical Systems (3)

Example: Maneuvering Characteristics Augmentation System (MCAS) for B737 MAX

Lion Air Flight 610 (10/29/2018, 189 Fatalities) and Ethiopian Airlines Flight 302 (3/10/2019, 157 Fatalities)

- Insufficient Redundancy and Guidance Requirements (Both Accidents Involved Incorrect Data from Faulty Sensor)
  - MCAS Relied on Input from a Single AOA Sensor Making it Susceptible to Single-Point Sensor Failure
  - Crew Bombarded by Multiple Alarms & Alerts In Cockpit
  - No Meaningful Guidance or Alerts Provided to Crew for Responding to Potential MCAS Issues
  - Absence of AOA Disagree Alert
- Worst-Case Test Scenarios Not Evaluated During the MCAS Safety / Functional Hazard Assessment
  - Key Failure Modes that Could Lead to Uncommanded MCAS Activation
    - » Erroneous High AOA Inputs to MCAS
    - » Crew Response Error (Even though Flight Crew was Assumed / Expected to Mitigate Failures)
  - Maximum Stabilizer MCAS Deflection Limit of 2.5 deg
  - Multiple MCAS Activations Resulting in Cumulative Mis-Trim and Increased Difficulty in Controlling Aircraft
    - » Attitude
    - » Flight Path
  - Combined Flight Crew Workload and Failure Effects
- Insufficient Crew Training
  - Procedures for Runaway Stabilizer Not Reintroduced, New Procedures Considered Unnecessary
  - Use of Stabilizer Cutout and Manual Trim Wheel to Control Stabilizer Position

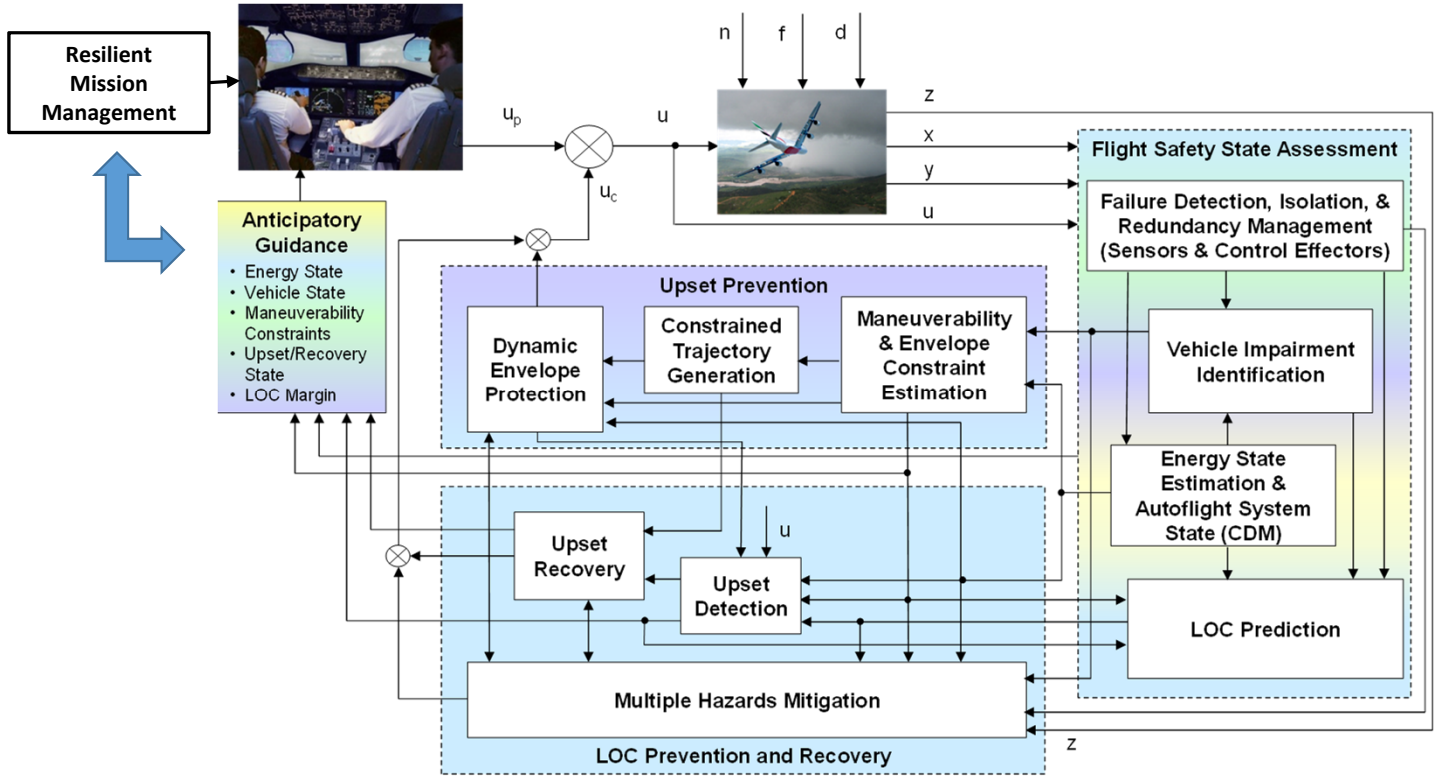
- **MCAS** is a feature on **Boeing** 737 MAX aircraft intended to **prevent stalls** in flaps-retracted, low-speed, nose-up flight
- **MCAS** uses airspeed and other sensor data to compute when a dangerous condition has developed and then trims the aircraft nose down

Accident Investigation Determined that the Design & Certification of MCAS Feature was Inadequate

Refs: Final Accident Investigation Report for Lion Air 610, Preliminary Accident Investigation Report for Ethiopian Airlines 302, NTSB Safety Recommendation Report

V&V Implications for Safety-Critical Systems (4)

Example Advanced Future Resilient System: LOC Prevention / Recovery



Focus of Validation Effort for Safety-Critical Aircraft Systems

System Certification Requirements

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.

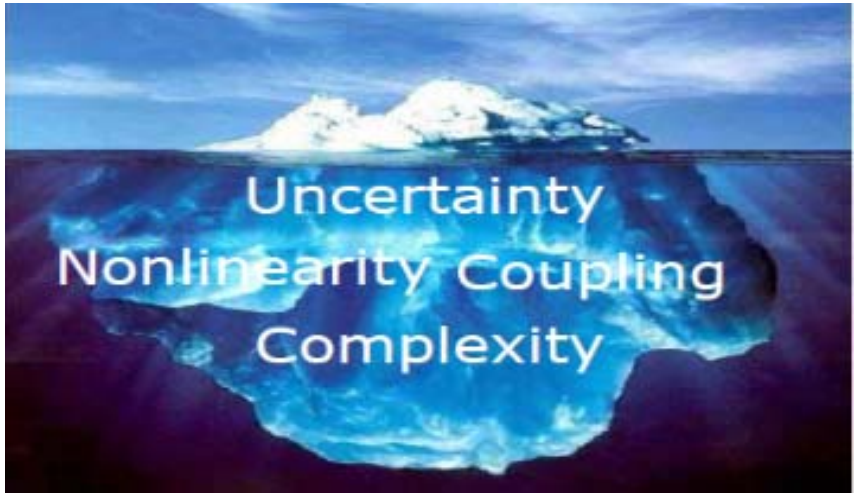
(2) The probability of multiple failures and undetected failures.

(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.

Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions

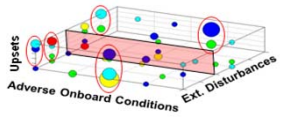


Validation Concept for Advanced Systems

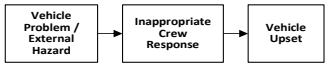
Enhanced Onboard Systems Technologies for Improved Situational Awareness, Guidance & Control *under LOC Hazards*

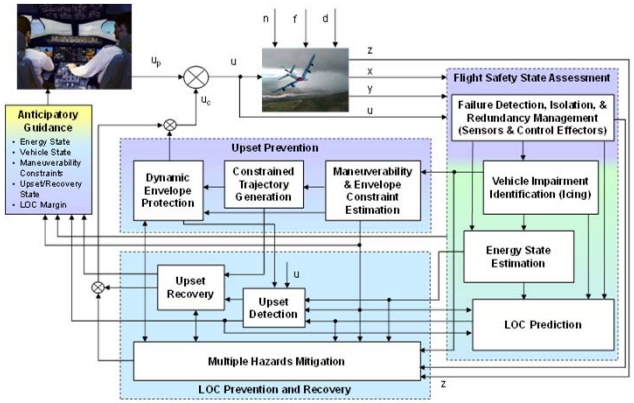
LOC Hazards Analysis

Worst-Case Hazards Combinations



Hazards Sequences





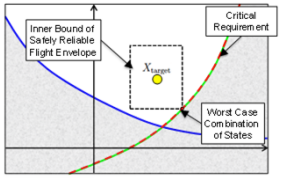
Integrated LOC Hazards Effects Simulation

Vehicle Upsets

Vehicle Impairment

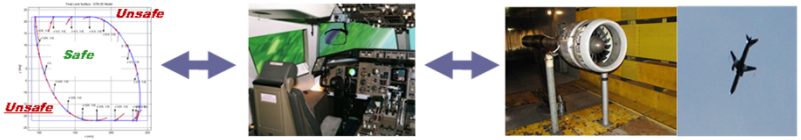
External Disturbances

Evaluation Methods, Tools, & Testbeds



ASC Technology Evaluation (CTE)

Analysis *Simulation* *Experimental Testing*



Test Scenarios Based on Accident / Incident Analysis & Future Risks

Level of Confidence in the Evaluation Results

Level of Hazards Coverage

Degree of Technology Effectiveness

Technology Limitations & Constraints

Validation Technology Approach

Comprehensive Technology Evaluation using Realistic Hazards Test Scenarios

Analysis

- Nonlinear & Uncertainty Effects Analysis
- Stability / Robustness Analysis
  - Nonlinear Estimation, FDI, & Control Systems
  - Human-in-the-Loop Systems
- Confidence Level Assessment (Models)

Identification of Potential Technology Problems

Simulation

- Vehicle Upsets
- Vehicle Impairment
- External Hazards

Guided Monte Carlo & Piloted Evaluations

Experimental Testing

- Ground-Based
- In-Flight

Integrated & High-Risk Evaluations

Real-Time Monitoring

- Real-Time Safety Monitoring under High-Risk Conditions
- Real-Time Safety Risk Assessment

Integrated System Evaluations under Multiple Hazards

Assess Effective Hazards Coverage, and Identify System Limitations & Weaknesses

NASA Partners: University of Minnesota, University of West Virginia, Georgia Institute of Technology (Bristol University and Drexel University)

Validation Methods & Tools (1)

- **Analysis**
  - Uncertainty Modeling for Robustness Analysis
    - » LPV Modeling Using Orthogonal Polynomials & Symbolic Build-Up
    - » Parametric
    - » Unmodeled Dynamics
  - Reliability Analysis
  - Stability Analysis for Actuator Saturation
  - Analysis of Fixed-Structure Neural Networks
  - System Malfunction Effects Analysis
  - **Nonlinear Dynamics and Control Analysis (Bifurcation Analysis, Safe Set Analysis)**
  - **Nonlinear Robustness Analysis**
  - Nonlinear Uncertainty Quantification (Briefing on December 15)
  - **Probabilistic Uncertainty Effects Analysis**
  - Analysis of Nonlinear Stochastic Estimation Filters
  - Analysis of Piloted Systems under LOC Conditions (e.g., PIO Prediction)
  - Analysis of Complex Integrated Systems

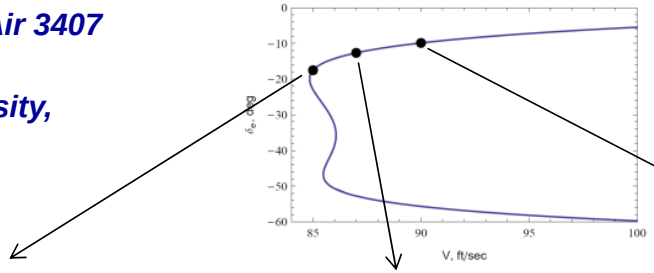
Research Partners: University of Minnesota, University of California at Berkeley, Barron Associates, Drexel University, Techno-Sciences, Georgia Institute of Technology, West Virginia University

Analysis Method: Nonlinear Dynamics & Control (1)

Bifurcation Analysis Example: Coordinated Turn Near Stall

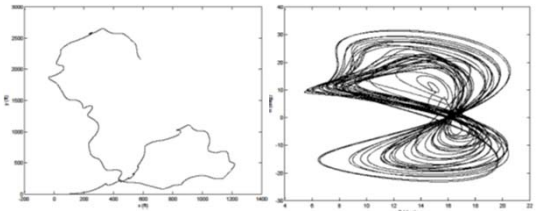
Motivated by LOC Accident: Colgan Air 3407 (2/12/2009)

Research Partners: Drexel University, Techno-Sciences, Inc.



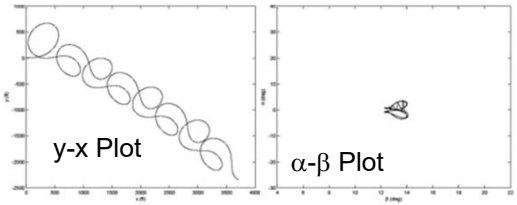
Bifurcation: Points in the state space (or flight envelope) which result in abnormal dynamic response and at which normal vehicle trim cannot be achieved

Coordinated turn @ 85 fps



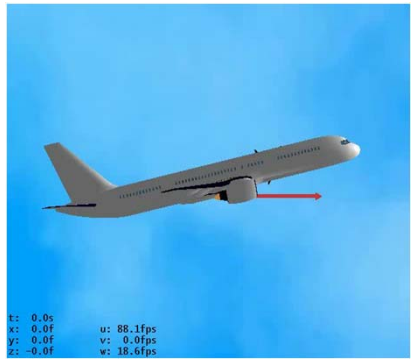
y-x Plot α-β Plot

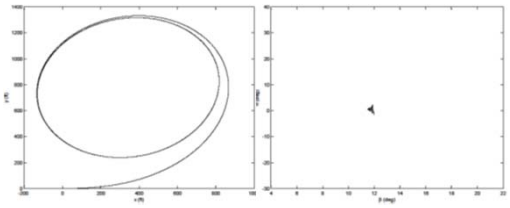
Coordinated turn @ 87 fps



y-x Plot α-β Plot

Coordinated turn @ 90 fps





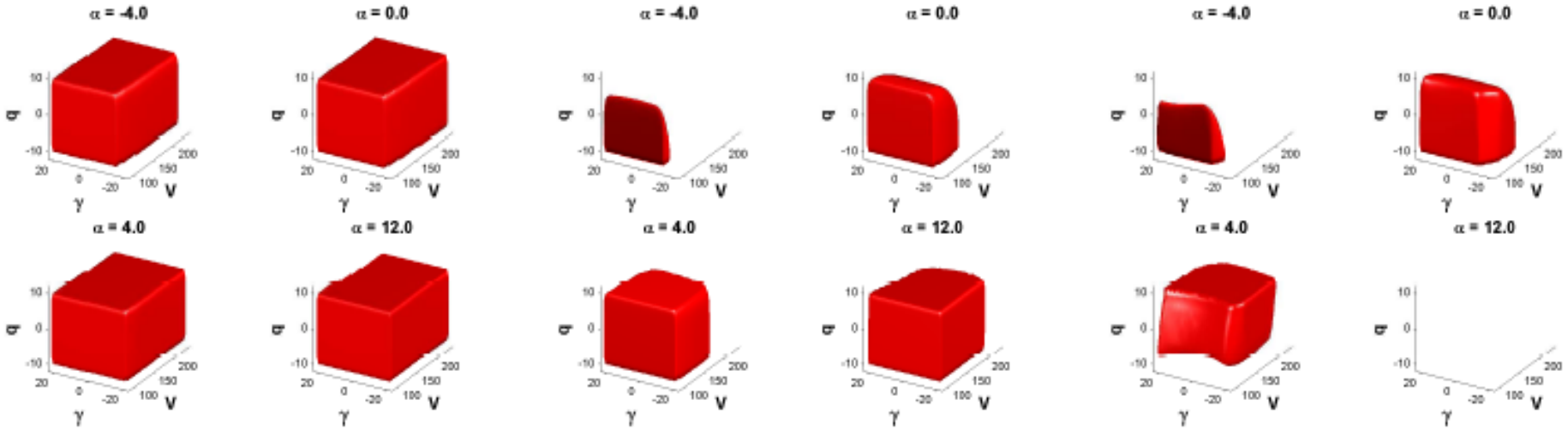
y-x Plot α-β Plot

See Backup for Alternate Bifurcation Example

Analysis Method: Nonlinear Dynamics & Control (2)

Safe Set Analysis Example: Full Longitudinal Dynamics under Vehicle Constraints (4 Dimensional State Space)

Safe Set: Region of the State Space (or Flight Envelope) from which Departure Trajectories can be Prevented



(a) Unimpaired (b) Restricted Elevator (c) Jammed Elevator

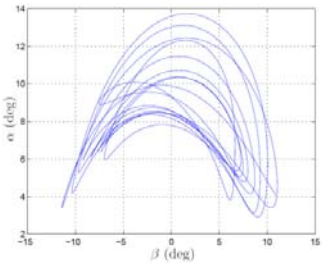
Fig. 5. The figure shows the four dimensional safe sets for slices of constant α=(-4,0,4,12) for an unimpaired and two levels of elevator impairment. The figure on the left shows the safe set for the unimpaired aircraft in which case the elevator position ranges from -40 deg to +20 deg. In the center figure, the elevator motion is restricted in the positive direction to + 3 deg, and in the rightmost figure the elevator is stuck at + 3 deg.

Research Partners: Drexel University, Techno-Sciences, Inc.

Analysis Method: Nonlinear Robustness (1)

Example: F-18 Falling Leaf Mode

Many F/A-18 aircraft lost due to an out-of-control departure phenomenon, "falling leaf" mode



Revised control law uses ailerons to damp sideslip
Is *revised* better?

•Yes, several years service confirm – but can this be ascertained with a model-based validation?

•*Baseline* underwent "validation", yet ...

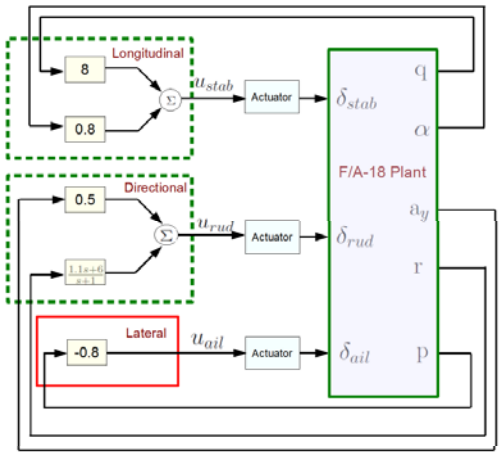
Linearized Analysis: at equilibrium and several steady turn rates

- Classical loop-at-a-time margins
- Disk margin analysis (Nichols)
- Multivariable input disk-margin
- Diagonal, full-block input multiplicative uncertainty
- Parametric stability margin (μ) using physically motivated uncertainty in 8 aero coefficients

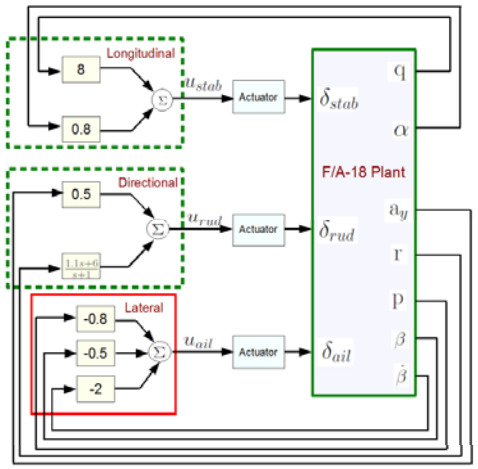
<u>Conclusion: Both designs have excellent (and nearly identical) linearized robustness margins trimmed across envelope…</u>

- Objectives
  - Extend Robustness Analysis Methods Based on Linearized Models to Broader Regions of Nonlinearity
  - Retain Capability to Consider Multiple Uncertainties and Perform Worst-Case Analyses
- Research Partners
  - University of Minnesota, UC-Berkeley, Barron Associates

Baseline



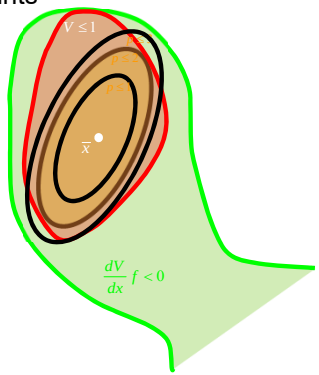
Revised



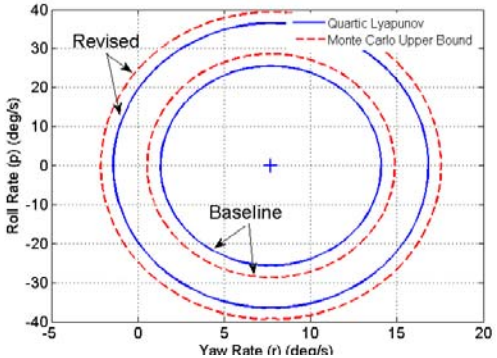
Analysis Method: Nonlinear Robustness (2)

Example: F-18 Falling Leaf Mode (cont.)

- Approach
  - Enforce Lyapunov/Dissipation inequalities locally, on sublevel sets
    - » Set containments via S-procedure and SOS constraints
  - Bilinear semidefinite programs
    - » "Always" feasible
    - » Simulation aids nonconvex proof/certificate search
- Address model uncertainty
  - Parametric Uncertainty
    - » Parameter-independent Lyapunov/Storage Funct.
    - » Branch-&-Bound
  - Dynamic Uncertainty
    - » Local small-gain theorems



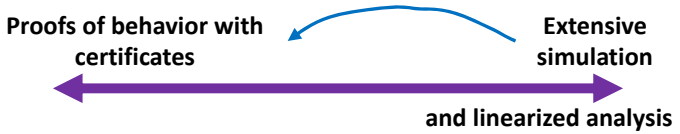
Example: F-18 Baseline and Revised Control System Analysis



Ellipsoidal shape factor, aligned w/ states, appropriately scaled

- *5 hours for quartic Lyapunov function certificate*
- *100 hours for divergent sims with "small" initial conditions*

- Status
  - –Tools (Multipoly, SOSOPT, SeDuMi) that handle (cubic, in *x*, vector field)
    - 15 states, 3 parameters, unmodeled dynamics, analyze with *∂(V)*=2
    - 7 states, 3 parameters, unmodeled dynamics, analyze with *∂(V)*=4
    - 4 states, 3 parameters, unmodeled dynamics, analyze with *∂(V)*=6-8
    - Certified answers, however, not clear that these are appropriate for design choices
  - –*S*-procedure/SOS/Dissipative Inequalities Locally are more quantitative than linearization
    - Linearized analysis: *quadratic storage functions, infinitesimal sublevel sets*
    - SOS/S-procedure always works
  - –Working to scale up to large, complex systems analysis (e.g., adaptive flight controls) where "certificates" are desired.
  - –Work to scale up to large, complex systems analysis (e.g., adaptive flight controls) where "certificates"



- Benefits / Payoffs
  - –Enables Robustness Analysis in Broader Regions of Nonlinearity
  - –In F-18 Example, Provided Significant Benefit over Standard Linear Robustness Methods

Nonlinear Robustness Analysis Method Confirms Robustness Benefit of the F-18 Control System Revision

Analysis Method: Nonlinear Robustness (3)

Thrust 1: Certification of Analytically Redundant Systems

- B. Hu and P. Seiler, “A Probabilistic Method for Certification of Analytically Redundant Systems”, submitted to the International Journal of Applied Mathematics and Computer Science, 2014.
- B. Hu and P. Seiler, “Worst-Case False Alarm Analysis of Aerospace Fault Detection Systems”, accepted to the 2014 American Control Conference.
- B. Hu and P. Seiler, “Certification Analysis for a Model-Based UAV Fault Detection System”, AIAA Guidance, Navigation and Control Conference, AIAA-2014-0610, 2014.
- B. Hu and P. Seiler, “A Probabilistic Method for Certification of Analytically Redundant Systems”, IEEE Conference on Control and Fault-Tolerant Systems (SysTol'13), p.13-18, 2013.

Thrust 2: Robustness Analysis of Uncertain LPV Systems

- H. Pfifer and P. Seiler, “Robustness Analysis of Linear Parameter Varying Systems Using Integral Quadratic Constraints”, submitted to the International Journal of Robust and Nonlinear Control, 2014.
- H. Pfifer and P. Seiler, “Integral Quadratic Constraints for Delayed Nonlinear and Parameter-Varying Systems”, submitted to Automatica, 2014.
- H. Pfifer and P. Seiler, “Robustness Analysis of Linear Parameter Varying Systems Using Integral Quadratic Constraints”, accepted to the American Control Conference, 2014.

Thrust 3: Confidence Levels: Gap Metric

- A. Dorobantu, P. Seiler, and G.J. Balas, “Validating Uncertain Aircraft Simulation Models Using Flight Test Data,” AIAA Atmospheric Flight Mechanics Conference, AIAA 2013-4984, 2013.
- A. Dorobantu, G.J. Balas, and T.T. Georgiou, ``Validating Aircraft Models in the Gap Metric,'' to appear, AIAA Journal of Aircraft, January 2014.

Thrust 4: Large-scale nonlinear interconnected systems

- C. Meissen, L. Lessard and AK Packard, “Performance Certification of Interconnected Systems using Decomposition Techniques,” American Control Conference, Portland, OR, 2014.
- C. Meissen, L. Lessard, M Arcak, and AK Packard, “Performance Certification of Interconnected Nonlinear Systems using ADMM,” IEEE Control and Decision Conference, Los Angeles, CA, 2014.

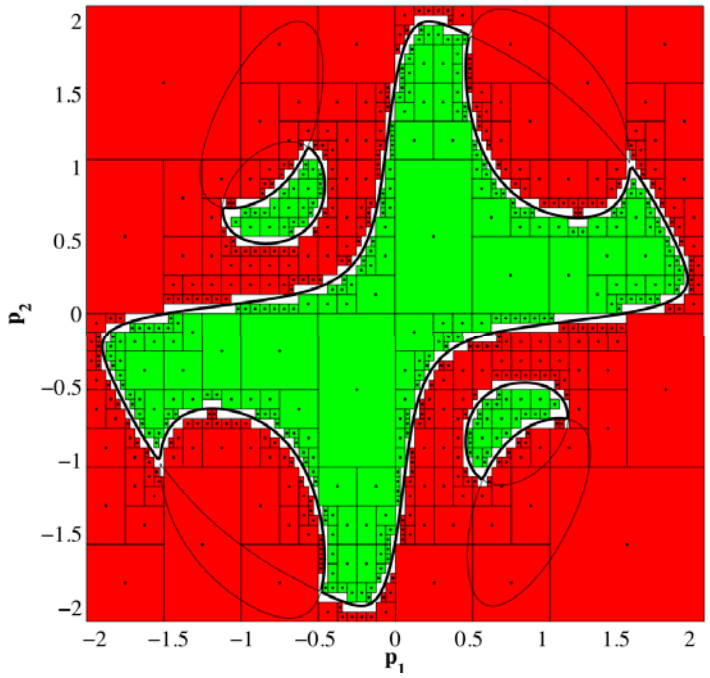
Thrust 5: UMN Flight Research Platform

- F.A. Lie, A. Dorobantu, B. Taylor, D. Gebre-Egziabher, P. Seiler, and G. Balas, “An Airborne Experimental Test Platform, Inside GNSS, p.44-58, March/April 2014.
- A. Dorobantu, W. Johnson, FAP. Lie, A. Murch, YC. Paw, D. Gebre-Egziabher, and G.J. Balas, ``An Airborne Experimental Test Platform: From Theory to Flight,'' 2013 American Control Conference}, Washington DC, June 2013.

Research Partners: University of Minnesota, University of California at Berkeley

Analysis Method: Uncertainty Quantification

- Builds upon the research in homothetic deformations
- Yields high fidelity characterizations of complex nonlinear failure domains
- Utilizes theory of Bernstein polynomials
- Desensitizes the analysis from assumptions used to model the uncertainty
- UQTools
  - Software Toolbox, Developed under Aviation Safety in 2010
  - Available via Software Release, that Implements Analytic Techniques
- Example Problems Addressed for Aviation Safety
  - Accuracy Requirement for Aero Coefficients to Retain Adequate Closed-Loop Performance
  - UQ Challenge Problem for GTM



Efficient "Failure Domain" Characterization to Identify Regions of Constraint Violation

Technical POCs: Dr. Sean P. Kenny and Dr. Luis G. Crespo, NASA Langley

To be Presented on December 15

Analysis Method: Probabilistic Uncertainty Effects

Algorithms for Uncertainty Representation and Analysis (AURA)

- **Motivation**: Understanding the range of possible system behaviors in response to uncertainties is critical for V&V and certification of safety-critical systems
- **AURA Probabilistic Analysis Toolset**
  - Enables designers to directly model uncertainties associated with design, implementation, and operation of complex systems
  - Propagates these uncertainties through system components and around feedback loops
  - Computes the resulting variability in system behavior
- **AURA Capabilities**
  - Highly efficient C++ library, with seamless integration to both Matlab and Simulink, that:
    - » Adds new datatypes and functions for manipulating random quantities
    - » Can interact with previously constructed models and code bases
  - Works with complete characterizations of random quantities, and can compute:
    - » Mean, variance, higher-order moments, and sensitivity indices
    - » Marginal and joint PDFs and CDFs of arbitrary variable combinations
    - » Probabilities of arbitrary events
  - Based on generalized polynomial chaos theory
    - » Has a rigorous and well-developed theoretical foundation
    - » Can represent arbitrary probability distributions
    - » Handles arbitrary dependencies between random quantities in a system

Validation of Autonomous Path Planning Algorithms for UAS

- Produce efficient global models of path planning algorithm performance
- Enable analysis and visualization of algorithm performance
  - What is the worst-case value of a metric?
  - What is the likelihood of a metric exceeding a specified limit?
  - What is the likelihood of a metric falling in a specified range?
  - What values/combinations of operating space parameters lead to worst case behavior?

- Develop tools to integrate into existing infrastructure and workflow
- Minimize human analyst interaction during gPC model generation
- Proof-of-concept demonstrations with representative path planners have shown these features

Many Other AURA Applications

- See Backup for Examples

Research Partner: Barron Associates

Validation Methods & Tools (2)

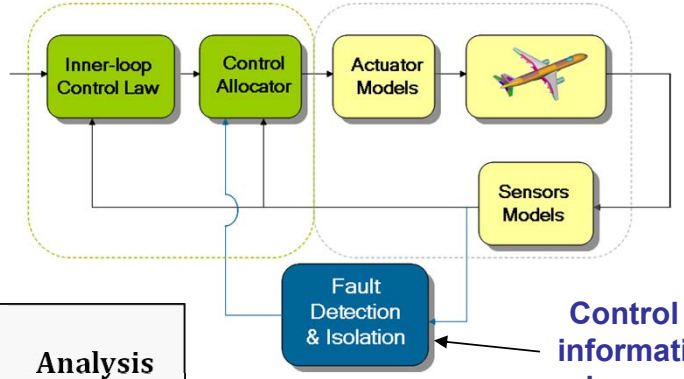
- **Simulation Utilizing Enhanced Multidisciplinary Vehicle Dynamics Models and Data**
  - Simulation Databases and Models for Off-Nominal Conditions
    - » Vehicle Dynamics Database & Models under Upset Conditions
    - » Aerodynamic Database & Models under Impairment Conditions (Damage, Icing)
    - » Simulation Models for Failure Conditions
    - » Simulation Models for External Disturbances (Wind Shear, Turbulence)
  - Simulation-Based Robustness Analysis
    - » **Guided Monte Carlo Simulation Evaluations**
    - » Automatic Test Matrix Generation for Piloted Simulation & Experimental Test Evaluations
  - Real-Time Piloted Simulation Evaluations
    - » Fixed Base
    - » Motion Base

Technical POCs: Gautam Shah, John Foster, and Kevin Cunningham, NASA Langley
Research Partner: Boeing

See Backup for Simulation Videos

Simulation Method: Guided Monte Carlo Evaluations

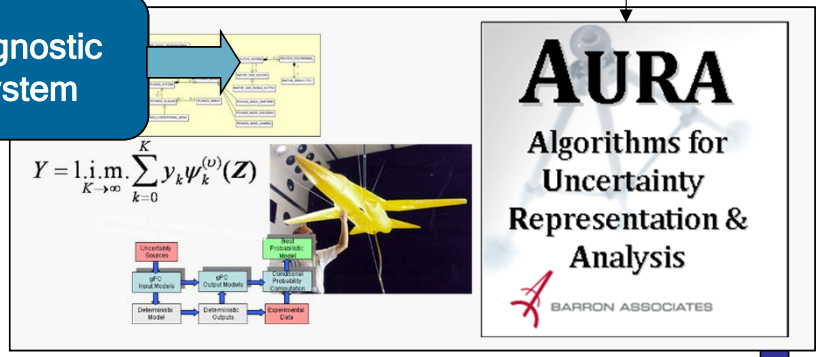
Analysis of Integrated Diagnostic & Control Systems



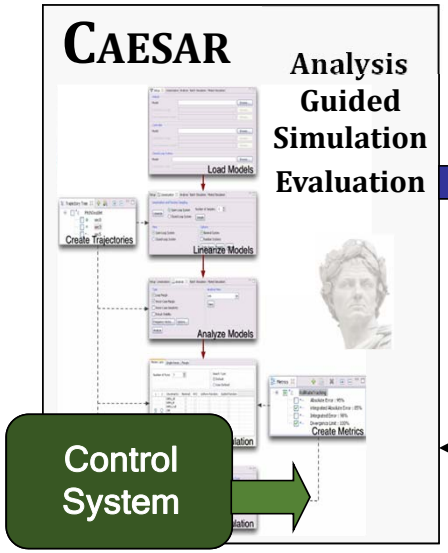
Control system uses FDI information to reconfigure in response to failures

AURA Software Developed by Barron Associates

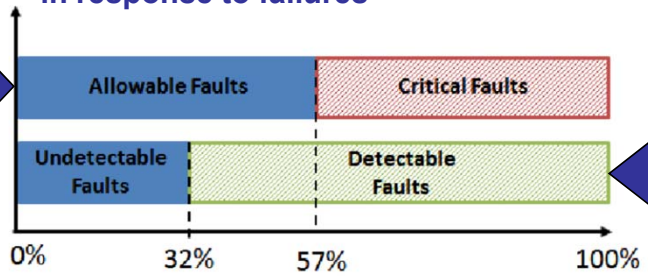
Diagnostic System



AURA quantifies level at which loss of surface effectiveness can be reliably detected by diagnostic system



CAESAR quantifies faults the system can tolerate without reconfiguration



GTM Example:
Longitudinal dynamics destabilized for demonstration purposes

Control System

CAESAR Capability Incorporated into the Robust Control Toolbox

Research Partners: Barron Associates and MUSYN

Validation Methods & Tools (3)

- **Experimental Methods**
  - Model & Algorithm Testing using Existing Data
    - » Flight/Accident/Incident Data
    - » Flight data from previous experiments
    - » Faulty component test data
  - Multidisciplinary Integrated System Testing (SAFETI Lab Concept Definition and Preliminary Development)
    - » Faults / Failures on actual sensor/actuator hardware components
    - » Simulated / Emulated vehicle/surface damage & atmospheric disturbances
    - » Simulated / Emulated environmental effects (e.g., electromagnetic)
    - » Piloted Evaluations
  - **Flight Testing**
    - » **Subscale Vehicle Flight Testing (Within and Beyond Visual Range)**
    - » Full-Scale Vehicle Testing (See Backup for Example)

See Backup for Subscale Flight Test Conducted Beyond Visual Range and SAFETI Lab Concept

Experimental: Subscale Flight Testing

Airborne Subscale Transport Aircraft Research (AirSTAR) Testbed

Research Aircraft

Low-Risk Test Vehicle

Base Research Station

Mobile Operations Station

Researcher Station

Research Pilot Station

Objective: Provide an In-Flight Test Capability for High-Risk Conditions Leading to Aircraft Loss-of-Control

- **RESEARCH AIRCRAFT**
  - Current: 5.5% Dynamically Scaled Generic Transport Model (GTM); 16% Generic Modular Aircraft with T-Tail (GMA-TT)
  - Future: Unconstrained
  - Split Control Surfaces (Failures / Damage)
  - Research Quality Instrumentation
- **GROUND FACILITIES**
  - Base Research Station (BRS)
  - Mobile Operations Station (MOS)
    - » Research Pilot cockpit with synthetic vision
    - » Multiple researcher stations
    - » Data telemetry to / from aircraft
- **UNIQUE CAPABILITIES**
  - Research Quality Data under High-Risk Test Conditions
  - Supports Wide Range of Research
    - » Vehicle Dynamics Modeling
    - » LOC Prevention / Recovery Systems
    - » UAS Operations / Safety / Autonomy
  - Supports Within and Beyond Visual Range Testing

Technical POCs: Dr. Christine Belcastro and Dr. David Cox, NASA Langley

AirSTAR: Adaptive Flight Control

Example Result: Offset Landing with Emulated Destabilizing Failure:

- Initial offset: 90 ft. lateral, 1800 ft. downrange, 100 ft. above the runway
- Pitch Stability degraded by 2 inboard elevator segments → 50% reduction in pitch control effectiveness
- Roll Damping Stability degraded by spoilers
- Flying qualities ratings taken for nominal, neutrally stable, unstable airplane

Note: Subscale Test Vehicle Response is 4.25X Faster than Full-Scale Aircraft

September 2010 Deployment, Ft. Pickett, VA

Open-Loop Aircraft

L1 Adaptive Control System

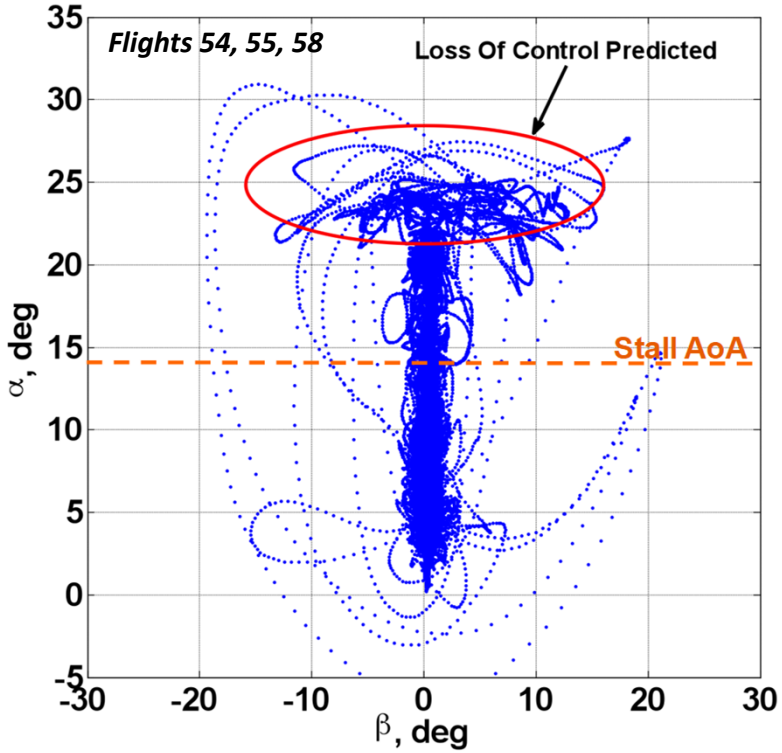
Nominal	CHR 4 (FQ L2)	CHR 3 (FQ L1)
Neutrally Stable	CHR 10 (Uncontrollable)	CHR 5 (FQ L2)
Unstable		CHR 7 (FQ L3)

Technical POC: Dr. Irene Gregory, NASA Langley
Research Partner: UIUC

AirSTAR: System Identification

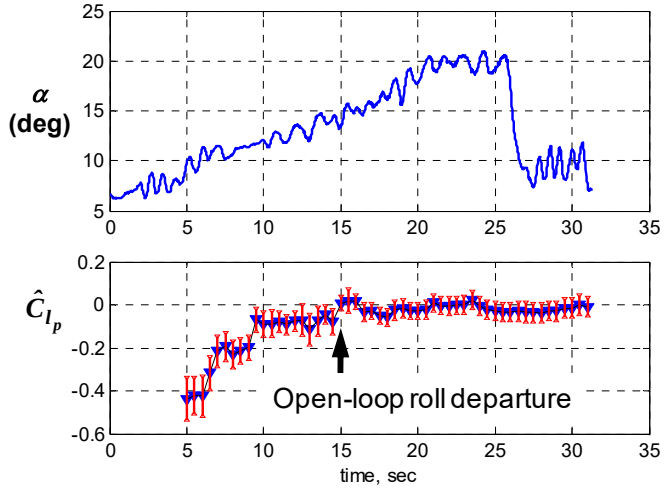
Example Result: Upset Test Condition - Stall / Departure (Pilot + Advanced Control System)

May 2011 Deployment, Ft. Pickett, VA



Demonstrated real-time stability and control characterization during approach to stall, through departure and recovery.

Example Result: T2 FLT 58 C14 WT02a



Applied L1 adaptive control to lengthen time on condition with stabilization that allowed slow transition through stall boundary and improved stall/departure recovery

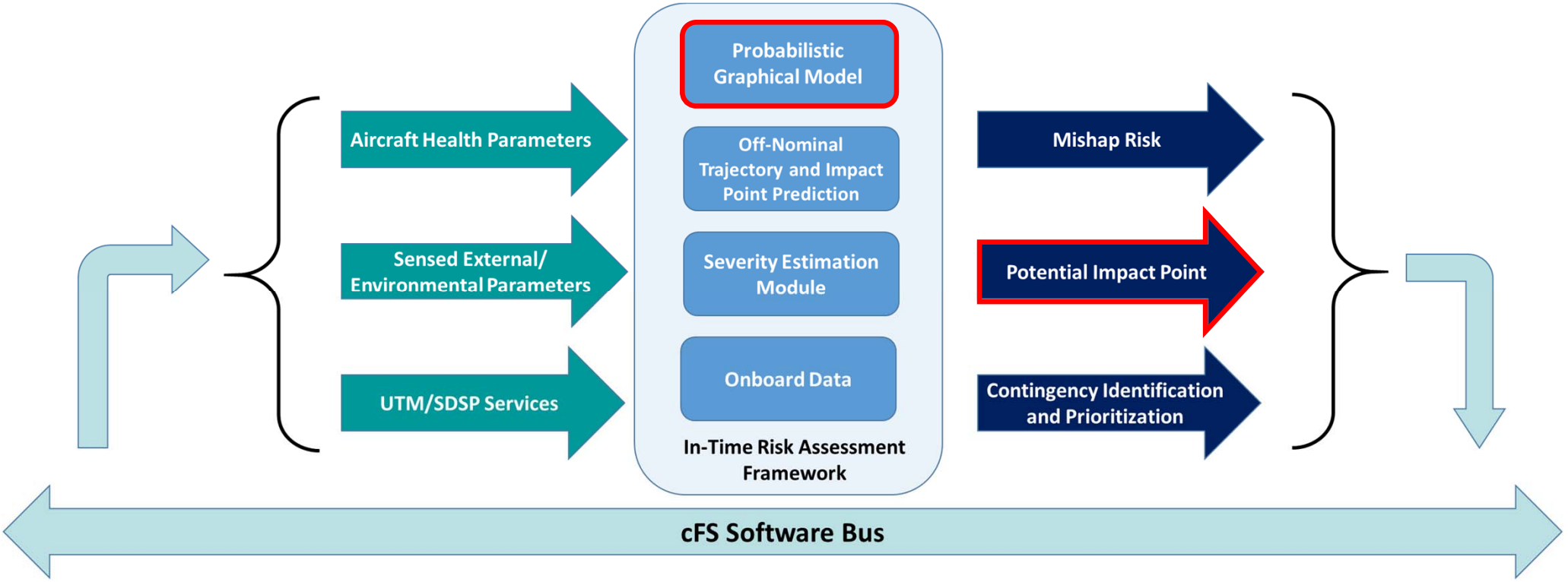
Technical POCs: Dr. Gene Morelli and Dr. Irene Gregory, NASA Langley

Validation Methods & Tools (4)

- **Real-Time/Onboard Validation Methods**
  - Estimation of Stability/Performance Margins
  - Critical Function Monitoring (Predictive Control Algorithms, Fault Detection)
  - Envelope Estimation and LOC Prediction
  - **Real-Time Risk Assessment**

Onboard Monitoring: Real-Time Risk Assessment (1)

Onboard In-Time Risk Assessment for Unmanned Aircraft Systems (UAS)

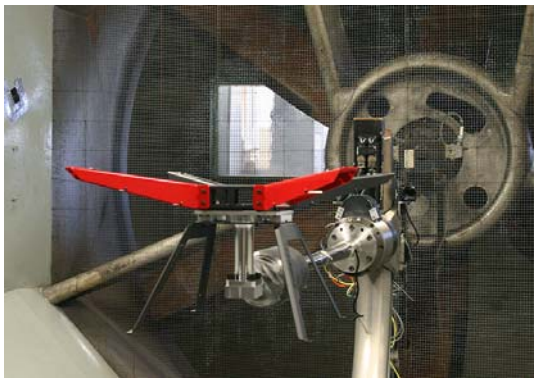


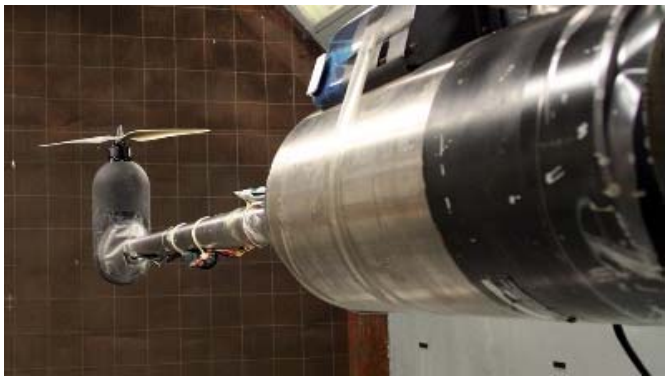
Technical POC: Dr. Ersin Ancel, NASA Langley

Onboard Monitoring: Real-Time Risk Assessment (2)

Off-Nominal Trajectory & Impact Point Prediction

- Prediction of flight trajectory and impact point following a severe off-nominal event is crucial for adequate casualty estimation
- 6-DoF flight dynamics simulation was proposed to help predict partial loss-of-control situations in erratic and/or extended trajectories
- Leveraged recent NASA wind-tunnel research that established an aerodynamic database for wide-range flow incidence angles and vehicular angular rates for *n*-rotor platforms

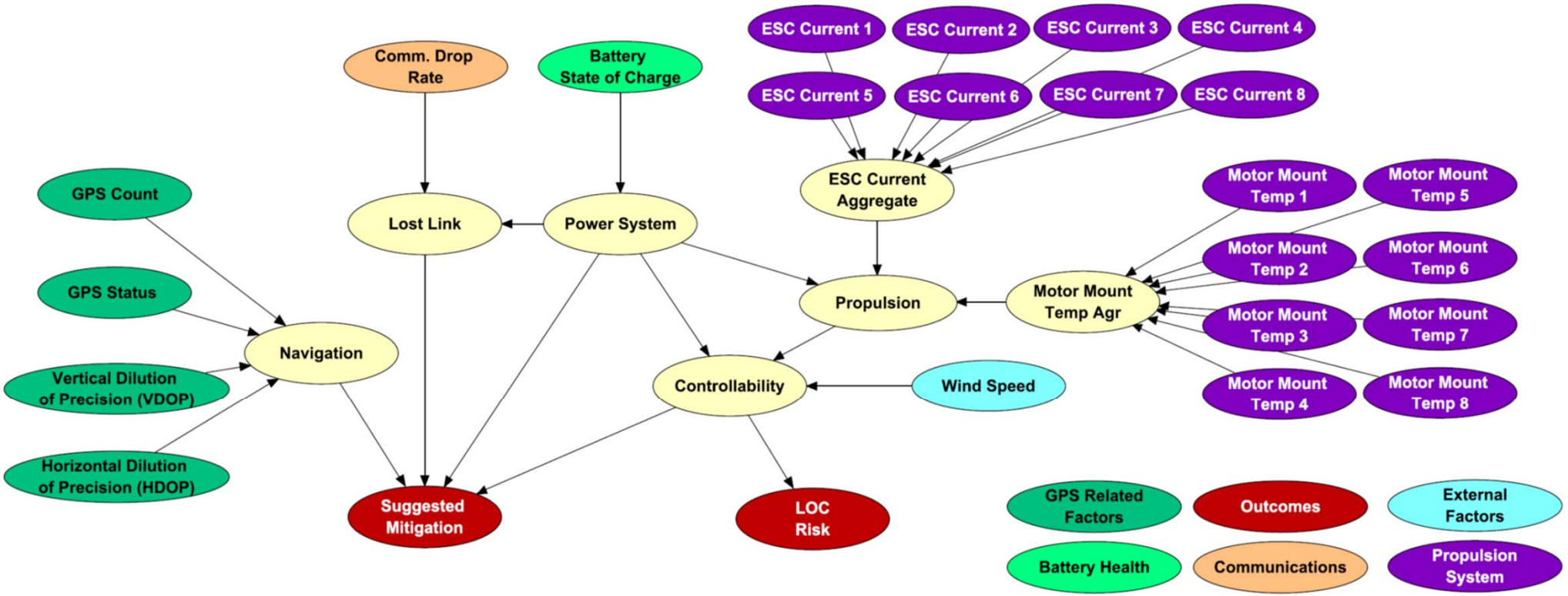




Technical POCs: Dr. Ersin Ancel and John Foster, NASA Langley

Onboard Monitoring: Real-Time Risk Assessment (3)

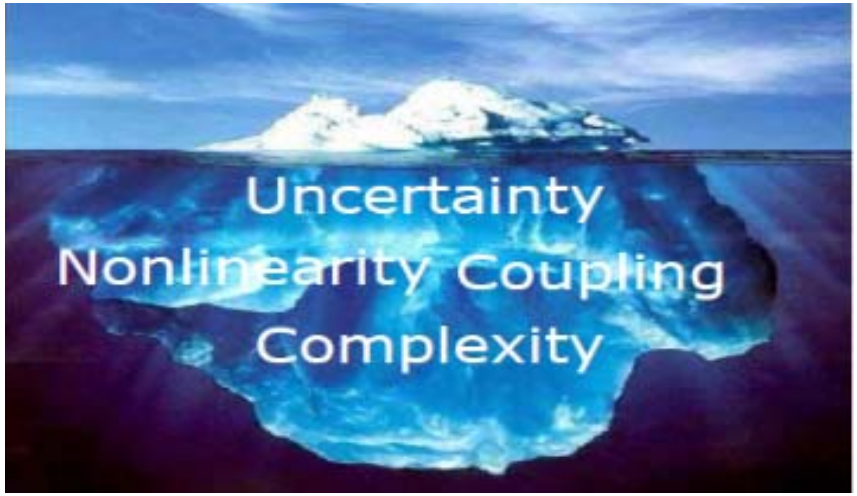
Probabilistic Graphical Model (Based on Bayesian Belief Networks)



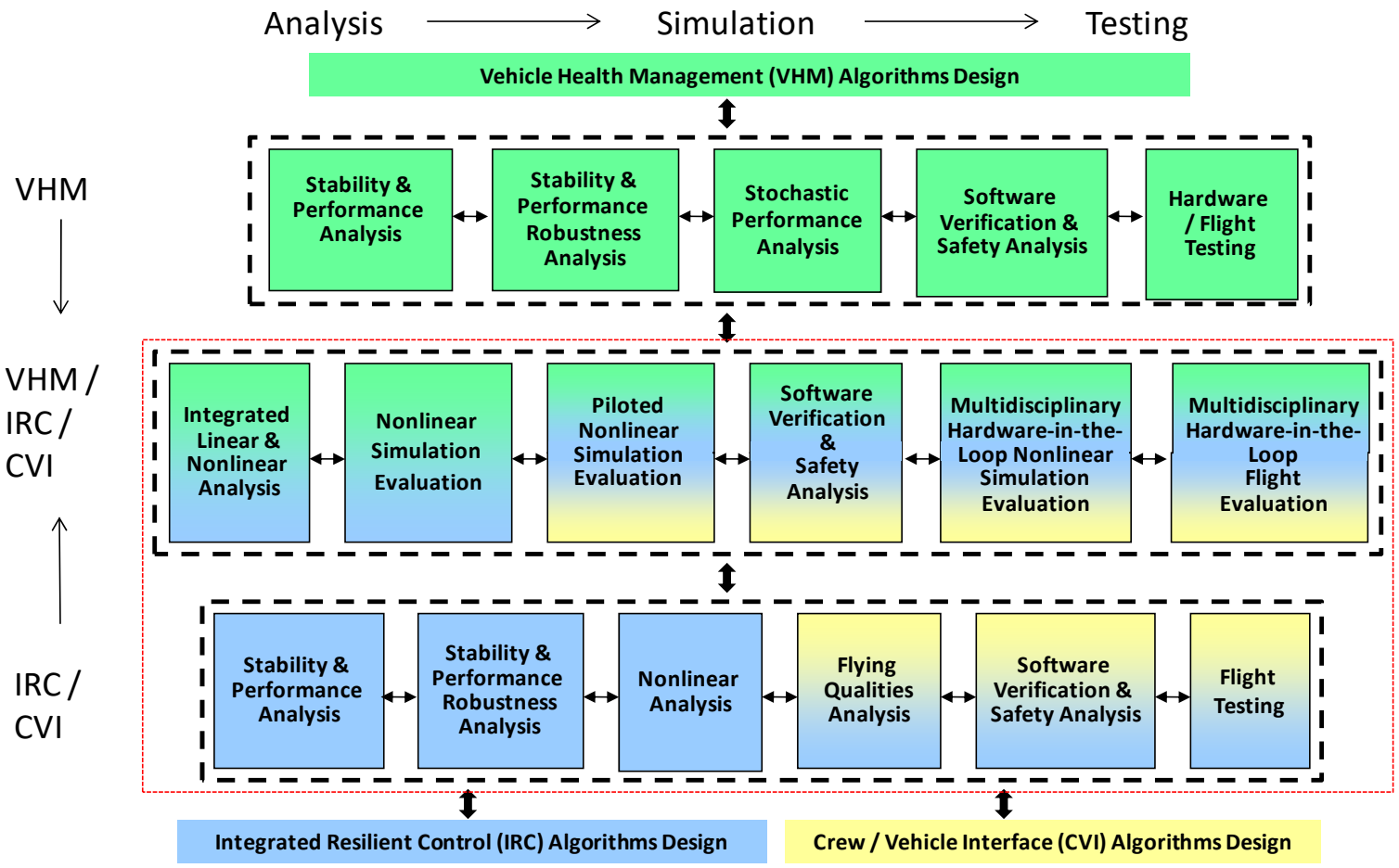
Technical POC: Dr. Ersin Ancel, NASA Langley

Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



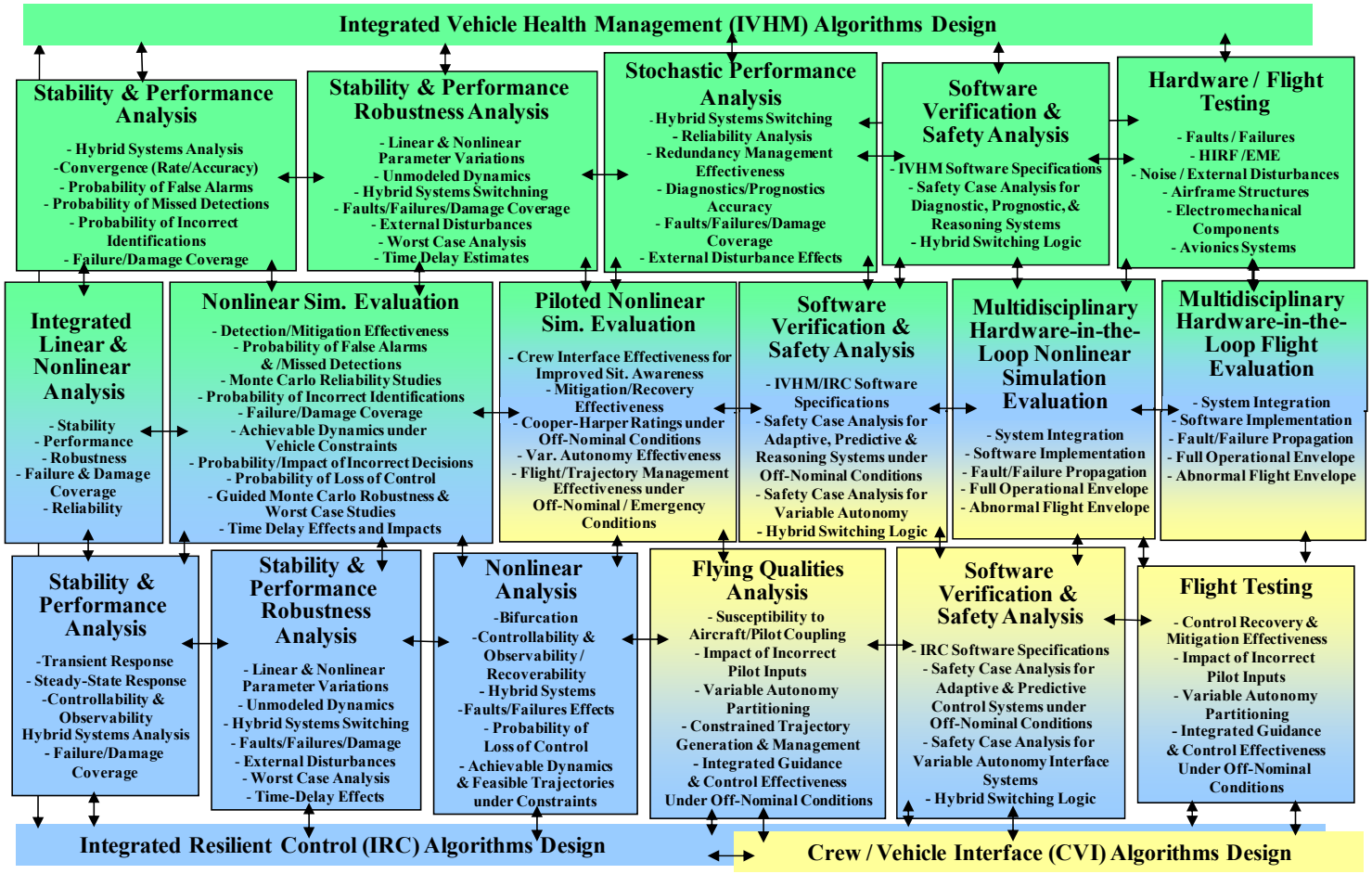
Integrated Validation Process: A Concept (1)



Advanced Integrated Technologies:

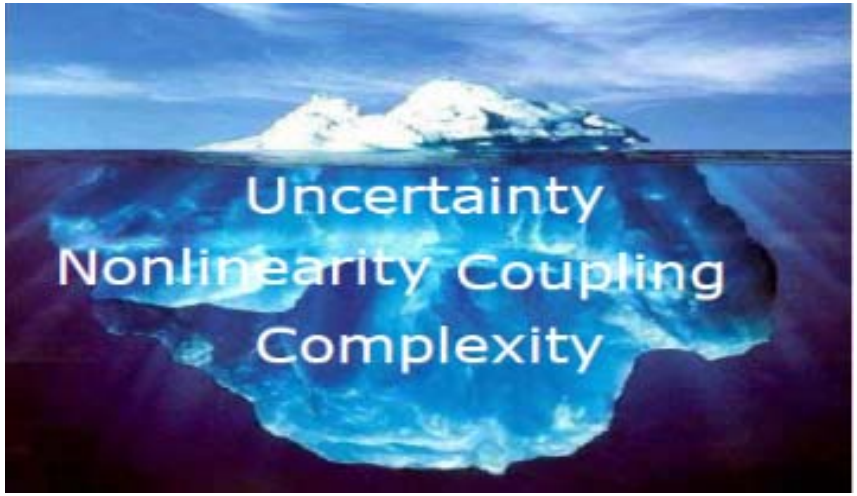
- Vehicle Health Management Systems
- Resilient Guidance & Control Systems
- Crew / System Interface Systems

Integrated Validation Process: A Concept (2)

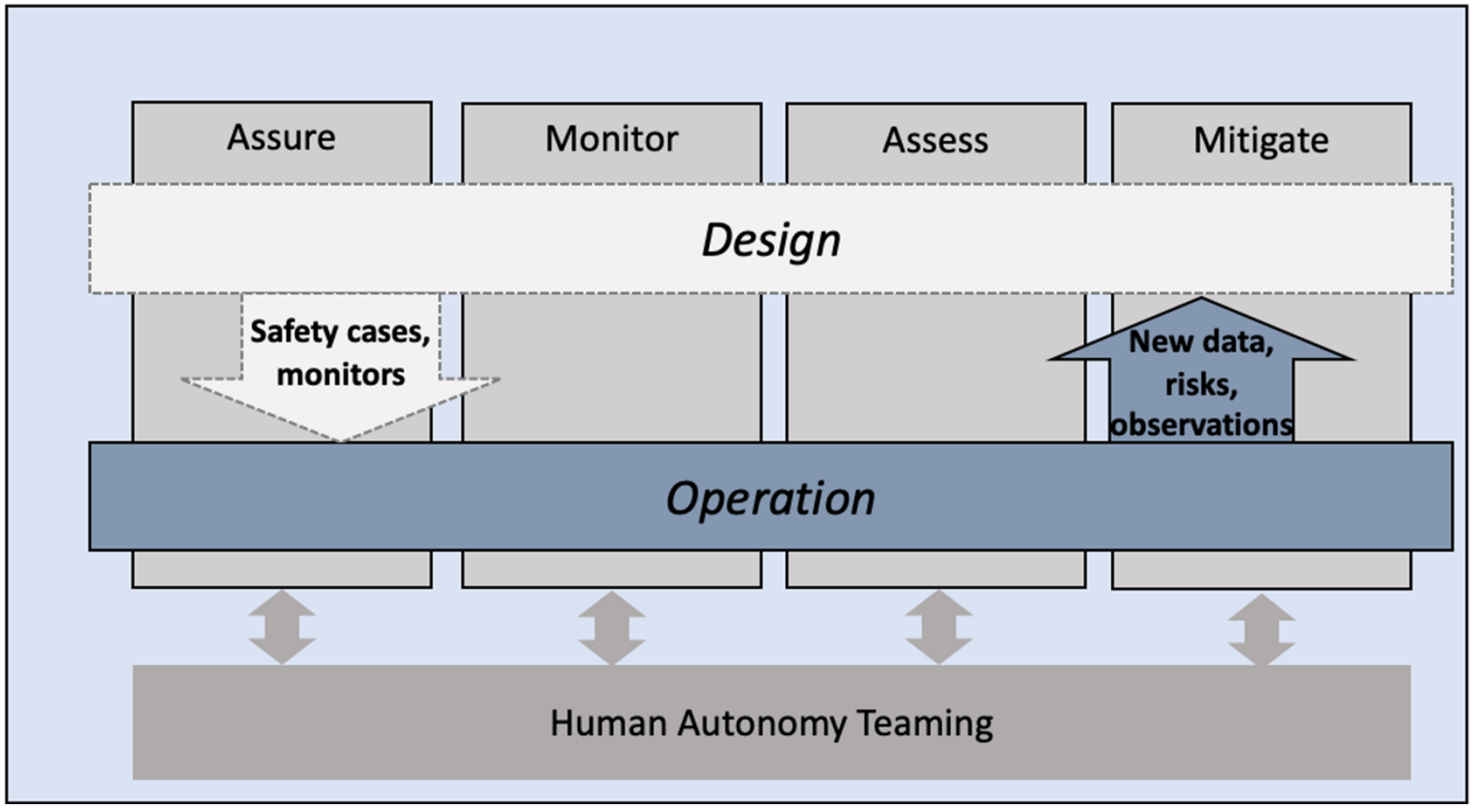


Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



Notional Verification & Certification Approach



Assurance Challenges to Fielding IA Systems

- Verification and Validation of Increasingly Autonomous (IA) Systems
  - Properties of Concern: Safety, Liveness, Security, Fairness…
- Human Machine Teaming Interactions
  - Role Allocation: Authority and Responsibility
- Bounding Behavior of IA Functions in Uncertain Environments
  - Contingency Management
  - Fault Containment
  - Heterogeneous Vehicles
  - Mixed ConOps
- Trusted Decision Making
  - Adaptive/Non-Deterministic
  - Shifting control paradigm
- Certification & Operational Approval
- Public Acceptance/Trust

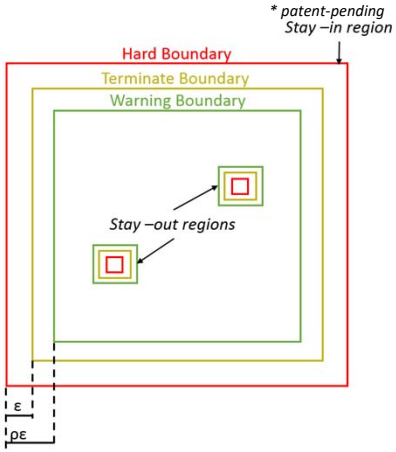
Barriers

- Lack of scalability of current approaches
  - DO-178C and software complexity
  - Frequency of flights, overflown population density, fleet size
- Lack of approaches, tools and techniques for evaluating safety properties in Increasingly Autonomous (IA) functions
  - Current approaches geared towards obtaining quantitatively predictable outcomes
  - Need models, methods and tools to develop high confidence in systems with
    - » Shifting locus of control between humans and automation
    - » Non-deterministic and/or adaptive decision making
- Lack of models and methods to develop high confidence in systems with a shifting locus of control between humans and automation
  - Significant variation in degree of human involvement, capability, and management
  - Dynamic role allocation
- Lack of rigorously defined processes and procedures to establish system-level performance requirements and functionality that are applicable to and derived from specified levels of safety, reliability, and operational performance.
- Lack of Certification Standards
  - Need rigorously defined processes and procedures to establish system-level performance requirements and functionality derived from specified levels of safety
  - Cost Effectiveness, Barrier to Entry, Change Management

Safeguard

- Flying beyond authorized safe regions is an operational hazard for unmanned aircraft

- **Safeguard reliably enforces geospatial constraints**
  - Uses formally verified algorithms to monitor and predict non-conformance
  - Isolated and independent of non-aviation grade components (e.g., autopilot)
  - Operates without sole reliance on Global Navigation Satellite Systems (e.g., GPS)
  - Streamlined design to facilitate compliance with safety standards and anticipated regulatory requirements
  - Designed to work with established geospatial database processes and service-oriented architectures (e.g., Unmanned Traffic Management (UTM))

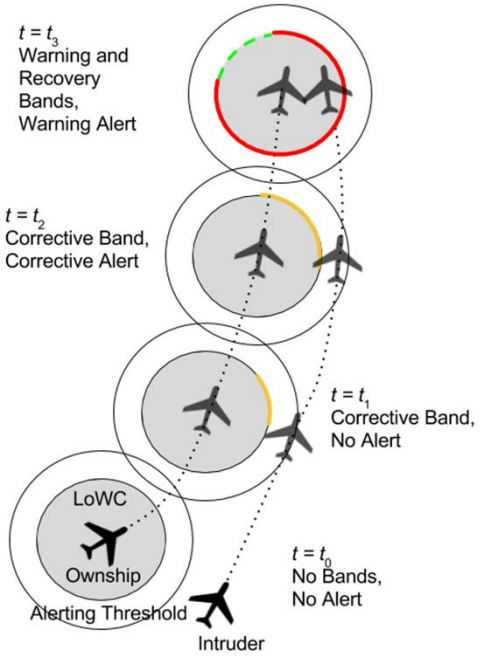


https://www.youtube.com/watch?v=0Kc01cV7vCU&list=PL7470F7E7702EB301&index=10&t=0s

Technical POC: E. Dill, NASA Langley

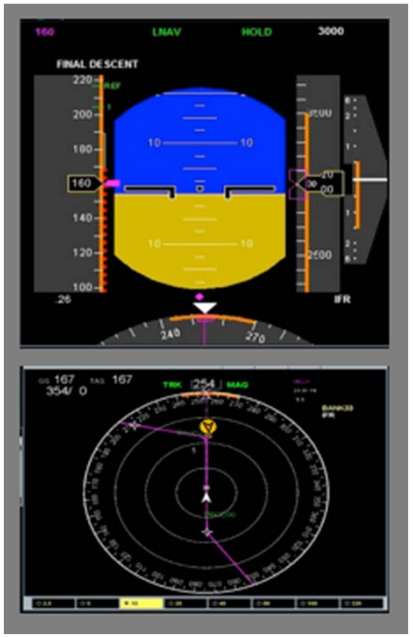
Detect & Avoid Alerting Logic for Unmanned Systems

DAIDALUS



- Developed as reference system for UAS Detect and Avoid, supporting RTCA SC-228 (UAS MOPS)
- Based on ”Well Clear” definition for UAS
- Provides Alerting (1x1) for situational awareness
- Provides Maneuver Guidance (1xN) for PIC maneuver recommendation
- Formally verified core algorithms for both alerting and guidance
- Version 2:
  - Support for dynamic alerting logic (Phase I and Phase II)
  - Integrated sensor uncertainty mitigation logic

https://shemesh.larc.nasa.gov/fm/DAIDALUS/



Daidalus in use in the MACS simulation environment

Brendon K. Colbert, J. Tanner Slagel, Luis G. Crespo, Swee Balachandran, and César Muñoz, *PolySafe: A Formally Verified Algorithm for Conflict Detection on a Polynomial Airspace*, Proceedings of 1st Virtual IFAC World Congress (IFAC-V 2020), 2020
Technical POC: C. Munoz, NASA Langley

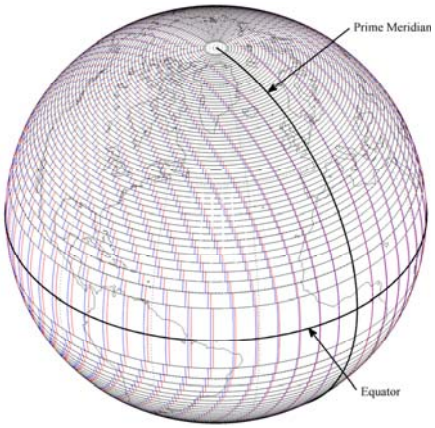
Independent Configurable Architecture for Reliable Operations for Unmanned Systems

- On-board software architecture of formally verified, configurable core algorithms for building safe, autonomous unmanned applications
- Includes path planning (RRT, A*, ..), traffic avoidance (DAIDALUS), geofence handling (PolyCARP), autonomous decision making (PLEXIL), merging and spacing, stand-off distance, object tracking
- Uses a communication publisher-subscriber middleware: NASA's cFS with DDS support.
- Won 2nd place at the XCELLENCE Awards by the AUVSI in the category of Detect and Avoid solutions
- Highly configurable:
  - Sensor agnostic: ADS-B, RADAR, V2V
  - Flight tested on different type of aircraft: small rotorcraft, large fixed wing, manned aircraft.
- Publicly available under NASA's Open Source Agreement: https://github.com/nasa/ICAROUS

https://shemesh.larc.nasa.gov/fm/ICAROUS/

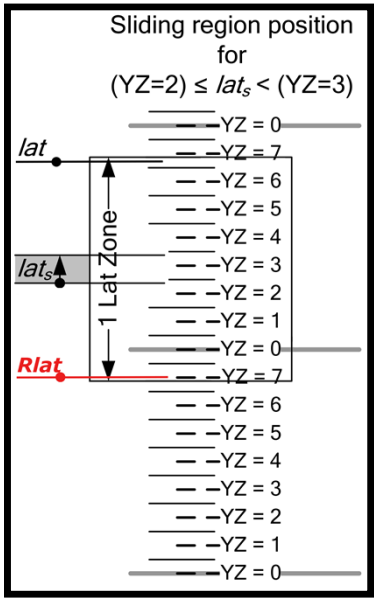
Technical POC: C. Munoz, NASA Langley

Compact Position Reporting – ADS-B Positioning



CPR divides the globe into "zones," and transmits only the target's position within the zone. The receiver has to determine the correct zone for proper decoding.

- CPR is used to save message space in ADS-B position messages
- Formal analysis led to tightening of decoding requirements, and simplified calculations.
- Spurred development of a PRECiSA, a tool for formal analysis of floating point (IEEE-754 spec) programs
- Formally verified implementations in floating point (double) and fixed point (single).
- Changes from formal analysis and verified implementation to be in revision C of DO-260 (ABS-B MOPS)



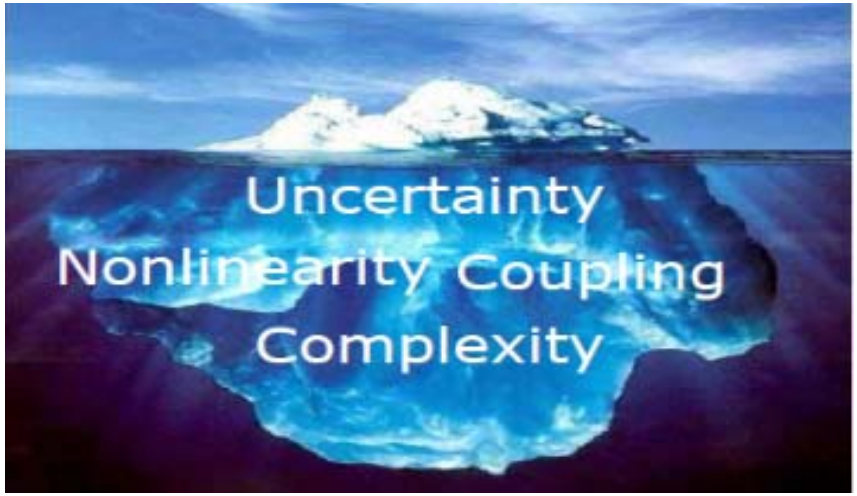
Visualization of loose requirement for decoding. Target is within stated distance threshold, but decodes incorrectly

https://shemesh.larc.nasa.gov/fm/CPR/ , https://shemesh.larc.nasa.gov/fm/PRECiSA/

Technical POC: A. Dutle, NASA Langley

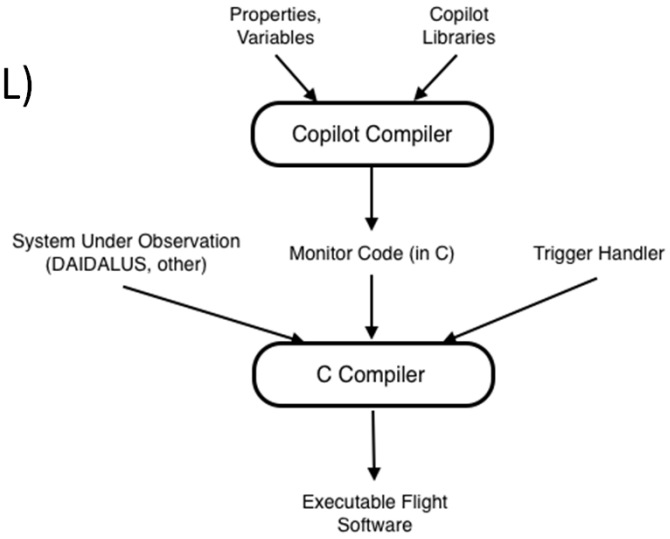
Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



Operational Assurance: Runtime Verification and Copilot

- **Can Runtime Verification (RV) safeguard a system that cannot be otherwise assured?**
  - Can we recover the safety and predictability through RV even if using Machine Learning?
    - » High-assurance RV can be assured like any conventional safety-critical system though the system under observation cannot
    - » Far simpler than the System Under Observation (SOU)
- Copilot
  - Haskell based Embedded Domain Specific Language (DSL)
  - Synthesize monitors for real-time embedded systems
  - Generates Misra-like C monitors
    - » Constant time, constant memory
  - Minimum instrumentation of SUO source code
  - Samples the system under observation
    - » Can miss state changes if not sampled



Technical POC: A. Goodloe, NASA Langley

RV Challenges

Challenges

- If RV is to ensure safety, the specifications being enforced must be derived from safety analysis
- RV frameworks should generate documentation to support traceability from specification to code
- Assure the correctness of the monitor specifications
- Code generated by RV frameworks are subject to the same sort of common bugs as any software
- Assure that the monitors correctly implement the specification
- Assured RV must safely compose with the SUO

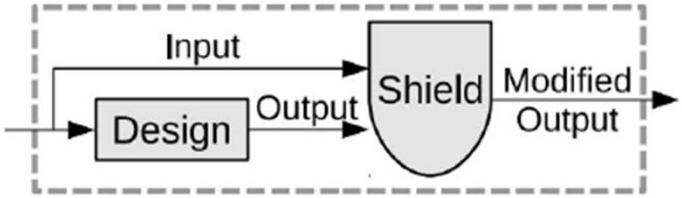
Conclusions

- High-Assurance RV will only become a reality if there is ample tool support for verification and validation
  - Will require tool builders to focus on reals and floats and engineering math
- RV frameworks require collaboration with both static analysis and deductive verification research

Technical POC: A. Goodloe, NASA Langley

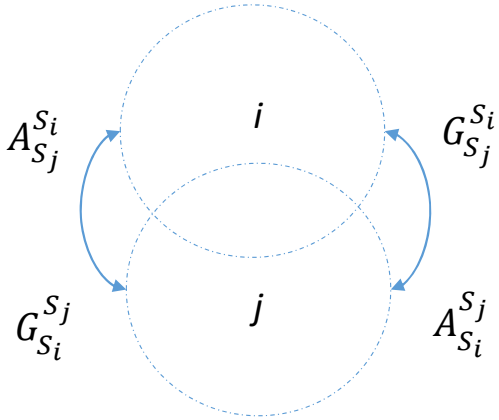
Shielded Execution

- Safety Shields for Multi-Agent Systems Enforce Global Safety Properties
  - Quantitative interference costs (c_{INT}), Fair Shielding
- What a shield is not…a planner!
- What do we want from a shield?
  - Agnostic of underlying goals/algorithms
  - A runtime enforcer of safety
  - Guaranteed progress



- Decentralized Shield Synthesis

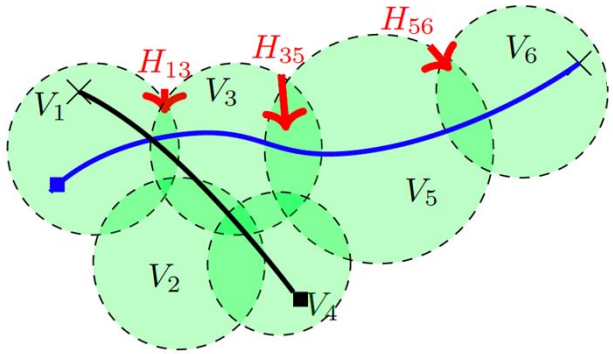
1. For each shield construct a game from the given safety specification and augment with contracts.
2. Solve for a permissive strategy.
3. Compute locally optimal deterministic strategy.

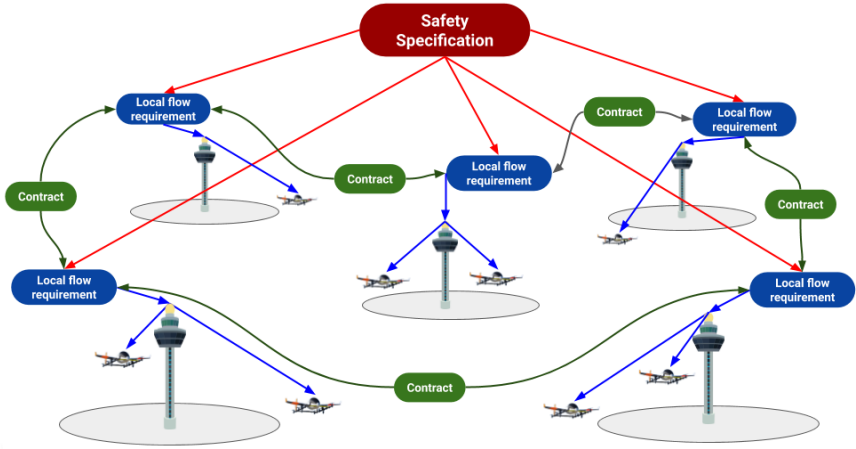


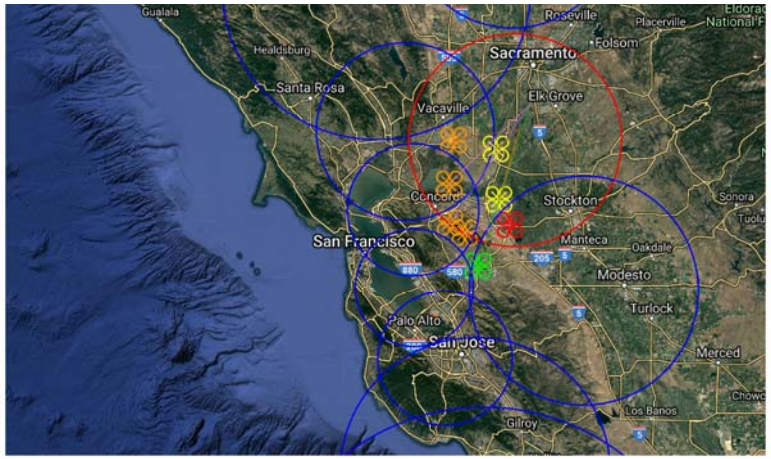
Note: Assume-Guarantee Contract between Shield S_i and S_j is specified as $C_{S_j}^{S_i} = (A_{S_j}^{S_i}, G_{S_j}^{S_i})$

Game Construction and Simulation

- Game with acceptance condition defined by original safety requirement (e.g., congestion)
- Augment with contract requirements—still a safety game!
- Solve game using SmalL bUt Complete GROne Synthesizer (Slugs)
  - UAM example over SFO
  - Hierarchical approach
  - Controllers synthesized independently
    - Assume-Guarantee contracts



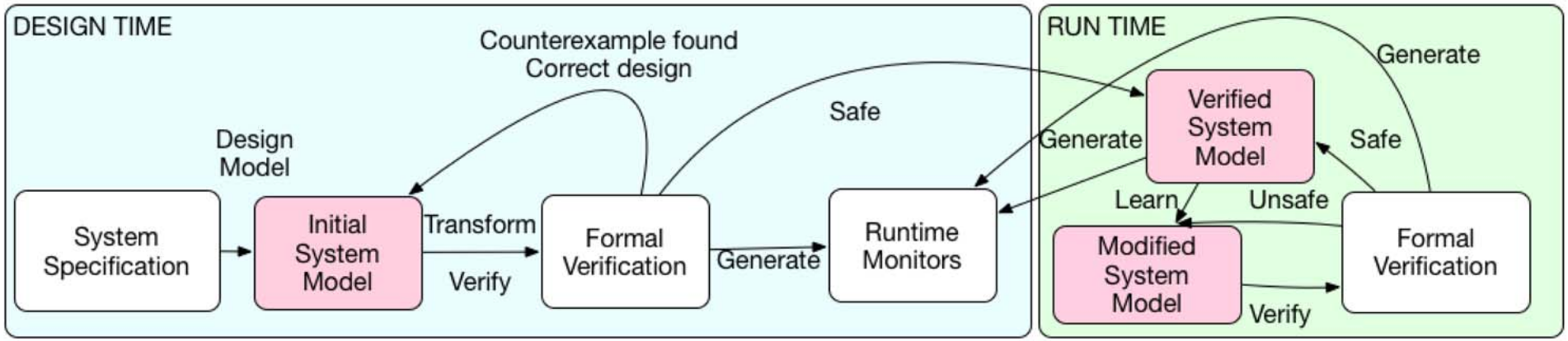




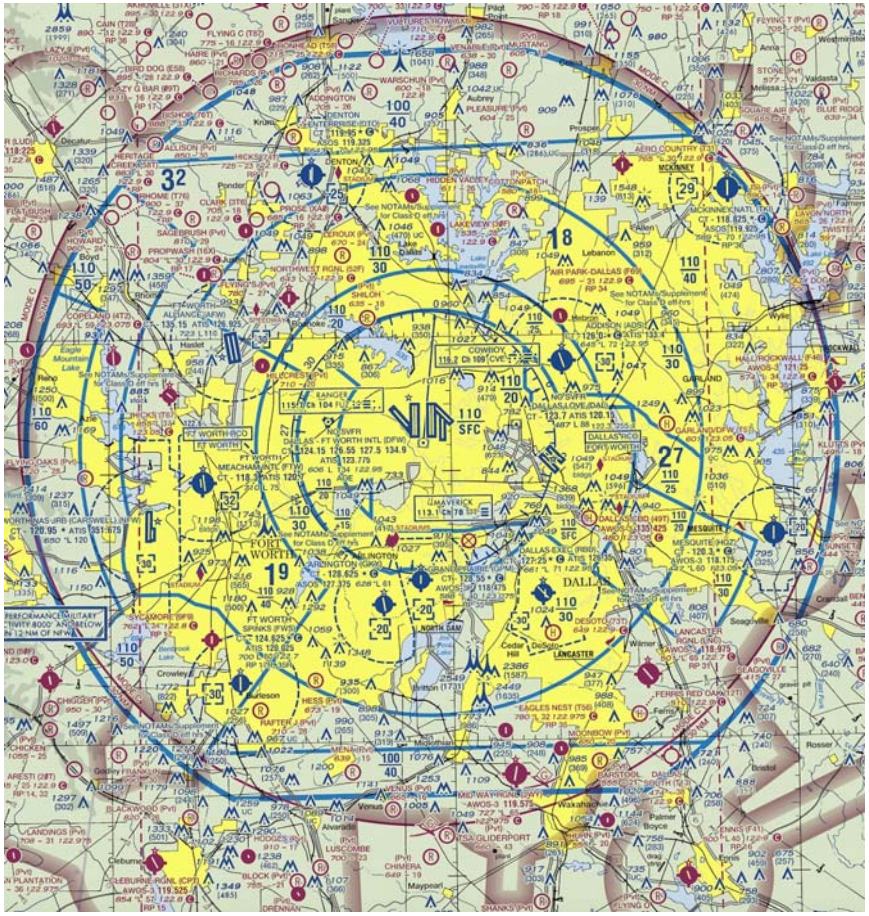
Suda Bharadwaj, Steven Carr, Natasha Neogi, Hasan Poonawala, Alejandro Barberia Chueca, Ufuk Topcu: **Traffic Management for Urban Air Mobility.** NFM 2019: 71-87

Cognitive Model with Formal Verification Flow

- Agent requirements and constraints are specified in (cognitive) architecture that enables multiple learning mechanisms
- Agent is transformed into formal environment for verification
  - Generates runtime monitors
  - Corrects the present design
- Agent can learn efficient ways
  - Creates or modifies rules which are evaluated and/or verified



UAS Lost Link Case Study



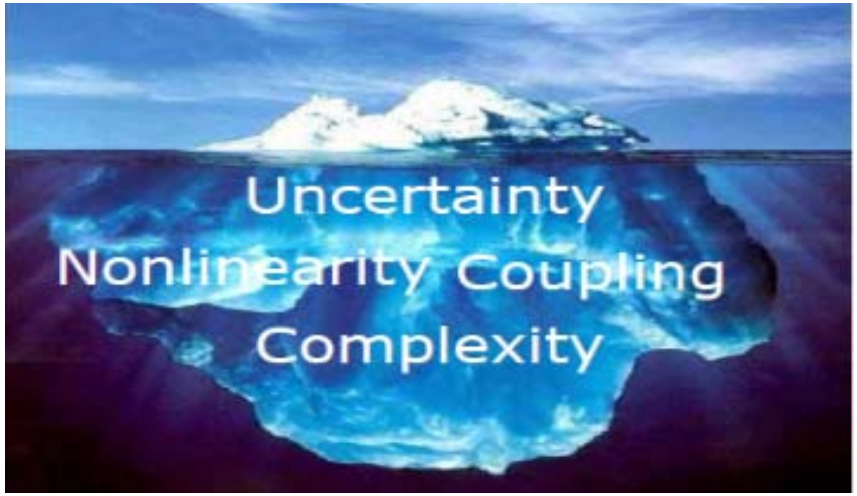
- Lost link simulated while overflying Dallas region
- 4 contingencies based on population of overflown area
- 5 safety properties verified, along with 1 liveness property
- Verification is agnostic to learning mechanism
  - Rules learned through chunking
- Working on extension to generation of proof carrying code (Frama-C)

Timothy Wang, Romain Jobredeaux, Heber Herencia-Zapana, Pierre-Loïc Garoche, Arnaud Dieumegard, Eric Feron, Marc Pantel: **From Design to Implementation: an Automated, Credible Autocoding Chain for Control Systems.** CoRR abs/1307.2641 (2013)

Romain Jobredeaux, Heber Herencia-Zapana, Natasha A. Neogi, Eric Feron: **Developing proof carrying code to formally assure termination in fault tolerant distributed controls systems.** CDC 2012: 1816-182

Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



Current Certification Practices

- Conventional aircraft airworthiness regulations serve to protect persons onboard the aircraft
  - Protection of persons and property on the ground is a resultant benefit.
- Current regulations are based on decades of experience and extensive historical data on aircraft and system designs, performance, and limitations
  - Hazards that require regulation are well understood
- One key aspect of regulation is certification:
  - Airworthiness Certification
  - Crew Certification
  - Instructions for Continuing Airworthiness
  - Air Operator Certification

- *Air Traffic Management (ATM), Air Navigation Service Provider(ANSP), Ground Infrastructure, and Aerodromes are regulated internally by the CAA.*

Regulatory Framework

- Regulation of aircraft in civilian airspace occurs through the application of (legally codified) rules
  - e.g.,1998 CASR, 14CFR, EC No 216/2008, ICAO…
- Guidance for compliance is detailed in supplementary documentation (Soft Law)
  - Advisory Circulars (AC), Acceptable Means of Compliance and Guidance Materials (AMC-GM), etc.
- Standards Documents referenced in AC/AMC-GM provide detailed processes for showing acceptable means of compliance
  - e.g., DO-178C/ED-12C, DO-254/ED-80 etc.

DO-178 C Rewrite and DO-333

- Actively participated in RTCA/EUROCAE SC 190/WG 52, formed to perform a rewrite of DO-178B/ED-12B, "Software Considerations in Airborne Systems and Equipment Certification”
  - FAA approved AC 20-115C on 19 Jul 2013, making DO-178C a recognized "acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the software aspects of airborne systems and equipment certification."
- Lead development of RTCA DO-333 Formal Methods Supplement to DO-178C and DO-278A
  - provides guidance for software developers wishing to use formal methods in the certification of airborne systems and air traffic management systems
  - supplement identifies the modifications and additions to DO-178C and DO-278A objectives, activities, and software life cycle data that should be addressed when formal methods are used as part of the software development process

Based on Work by K. Hayhurst, NASA Langley (Retired)

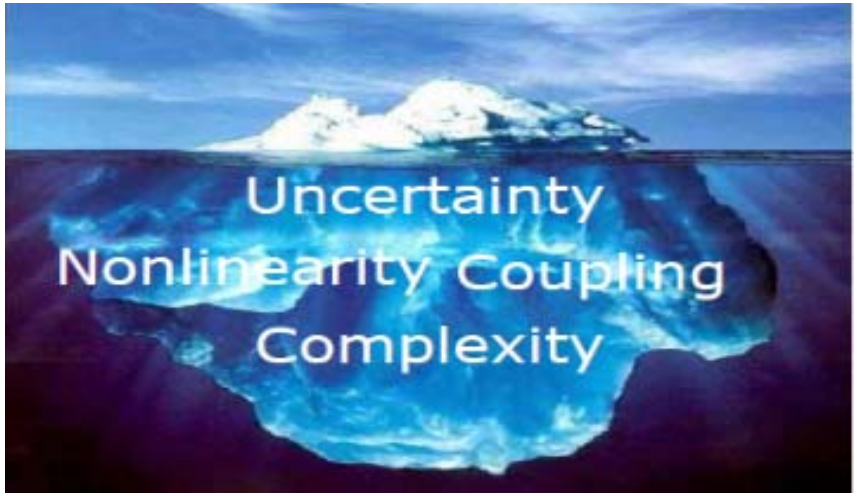
Streamlining Assurance: Overarching Properties

- Overarching Properties encapsulate the essential properties that should be satisfied by any entity (software, hardware, or system) for which approval is sought
  - Intent, Correctness and Necessity
- Overarching Properties Working Group is currently working to "identify and justify evaluation Criteria that will facilitate producing sufficient evidence that the Overarching Properties are satisfied"
  - Creating format and requirements of OP descriptions
  - Providing current uses of argument-based approaches to assurance (safety cases)
  - Use of the Goal-Structuring Notation (GSN) for expressing arguments
  - Lexicography, lexicology, grammar, and style of written materials
  - Assisting in modifying the scope document to facilitate agreement between EASA and the FAA
- Work to be done after completion of Criteria draft includes
  - Writing supplementary materials to help industry and authorities understand the Overarching Properties
  - Conducting evaluation of the sufficiency of the OPs relative to currently recognized standards

Technical POCs: M. Graydon and C. M. Holloway, NASA Langley

Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



Certification of IAS

- Extreme cost of existing safety assessment and substantiation processes is a substantial barrier
- No airworthiness standards have been approved for certification of different types of UAS for civil/commercial operations without operational restrictions
- Existing classification taxonomy may not be appropriate because
  - Airworthiness standards may not be appropriate
    - » DO-178C, MIL-HBK-516C etc.
  - UAS don't fit under current classes or categories

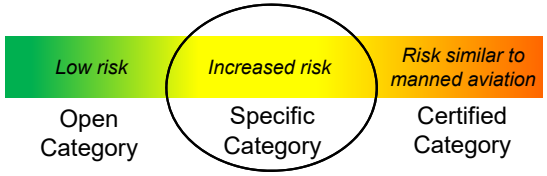
Risk-based Certification

- Primary aim of aircraft certification (Part 21 etc.) is to provide assurance of safety by: (1) assuring that items perform their *intended (safe) functions* under any foreseeable operating condition, and (2) assuring that *unintended functions* are improbable.
- A certification approach in which in which the imposed requirements are proportional to the operational risk
  - Only considering safety risks

General Characteristics of Airworthiness Standards for Conventional Aircraft	Expected Characteristics of Risk-based Airworthiness Standards for UAS
Originate from experience with system designs, performance, and limitations	Will originate from *a priori* functional and operational hazard analysis for an aircraft and operation
Operation agnostic	Will be operationally driven
Based on aircraft designs from 1950's and 1960's	Will not presuppose a reference aircraft
Focus on protection of people onboard	Will focus on protection of people on the ground and in other aircraft
Both performance-based safety objectives and prescriptive (technology-centric) requirements	Will primarily be performance-based safety objectives

UAS Airworthiness

- **Mission: investigate airworthiness requirements for *midrange* UAS**
  - To what extent should existing airworthiness requirements apply to UAS?



- **Approach: examine how design and operational differences between UAS and manned aircraft affect hazards and ways to mitigate them**
  - For classification
    - Are factors used to classify manned aircraft necessary and sufficient for UAS?
  - For airworthiness requirements/regulation
    - Are design and performance requirements for manned aircraft necessary and sufficient for UAS?

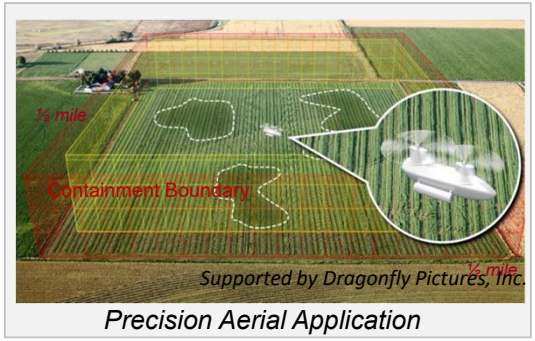
- **Factors Affecting Airworthiness Considerations**
  - Operational risk might provide a better basis than weight or kinetic energy for defining UAS classes and categories and additional steps in the UAS integration process

- **Accomplishments**
  - Identified design and operational factors affecting airworthiness considerations for UAS
  - Conducted 2 research studies identifying specific airworthiness requirements for an unmanned, 1000-lb rotorcraft

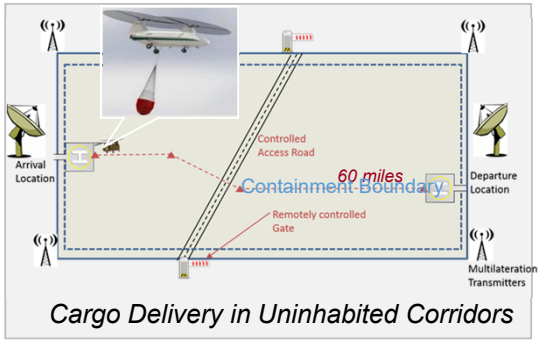
Technical POC: Dr. Natasha Neogi

Research Studies

- Developed 2 detailed concepts of operation for midrange unmanned rotorcraft
  - precision aerial application
  - cargo delivery in uninhabited corridors
    - operations *contained* over uninhabited areas
- Derived 85 design and performance requirements from hazard analysis and current regulations
  - 80 based on Part 27 (260 requirements)
  - 5 new for novel UAS systems and equipment
    - Containment*
    - Detect/avoid other aircraft
    - Detect/avoid ground-based obstacles
    - Safety-critical command and control links
    - Systems/equipment to support pilot's safety role
- Supports development of airworthiness standards for midsize unmanned rotorcraft



Precision Aerial Application



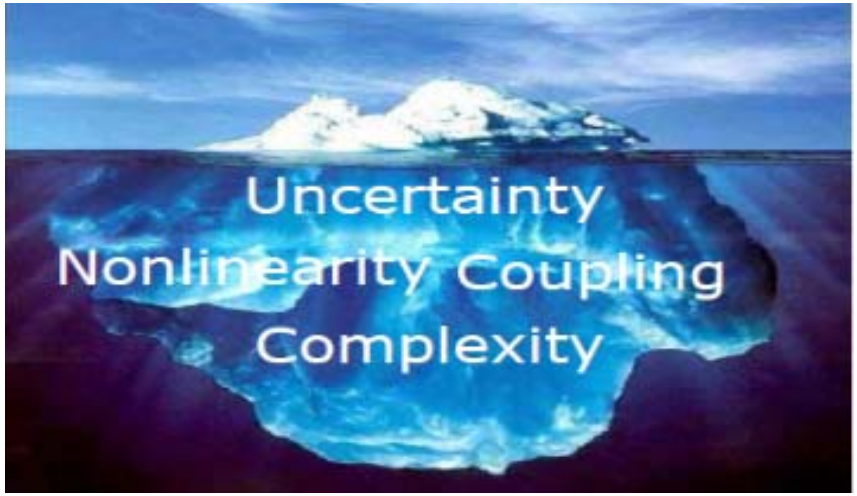
Cargo Delivery in Uninhabited Corridors

*The containment concept has been developed into a patent-pending prototype system called Safeguard

Technical POC: Dr. Natasha Neogi

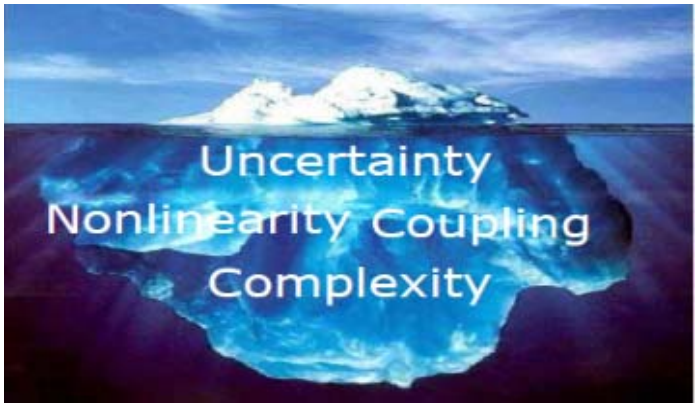
Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



Summary & Concluding Remarks (1)

- Significant Progress in Validation Methods, Tools, & Testbeds
  - Analysis of Nonlinear Uncertain Systems
    - » Uncertainty Modeling
    - » Stability & Robustness Properties
    - » Nonlinear Dynamics & Control Effects
    - » Probabilistic Uncertainty Effects
    - » Diagnostic & Stochastic Systems, Complex Integrated Systems, Human-in-the-Loop Systems
  - Simulation of Transport Aircraft under LOC Conditions
    - » Sub-Scale Vehicle Engineering Simulation in Matlab / Simulink (Generic Transport Simulation - GTM)
    - » Full-Scale Vehicle Simulation for Piloted Evaluations (Transport Class Model Simulation – TCM)
    - » High-Fidelity Fixed- and Motion-Based Simulations
  - Experimental Testing
    - » Subscale Vehicle Testing under LOC Conditions (AirSTAR)
    - » Full-Scale Testing under Off-Nominal Conditions
  - Real-Time Monitoring
    - » Envelope Estimation & LOC Prediction
    - » Algorithm Monitoring (Control, Failure Detection)
    - » Safety Risk Assessment
  - Integrated Coordinated Validation Process
    - » Initial Framework Developed
    - » Integrated Systems
      - Resilient Control Systems
      - Vehicle Health Management Systems
      - Crew Interface Systems
  - LOC Hazards-Based Test Scenarios
    - » LOC Problem Analysis Performed Based on LOC Accidents
    - » Initial Set of Hazards-Based Test Scenarios Developed
    - » Follow-On Work for UAVs Incorporated Future Risks and Mission Task Elements (See Backup)

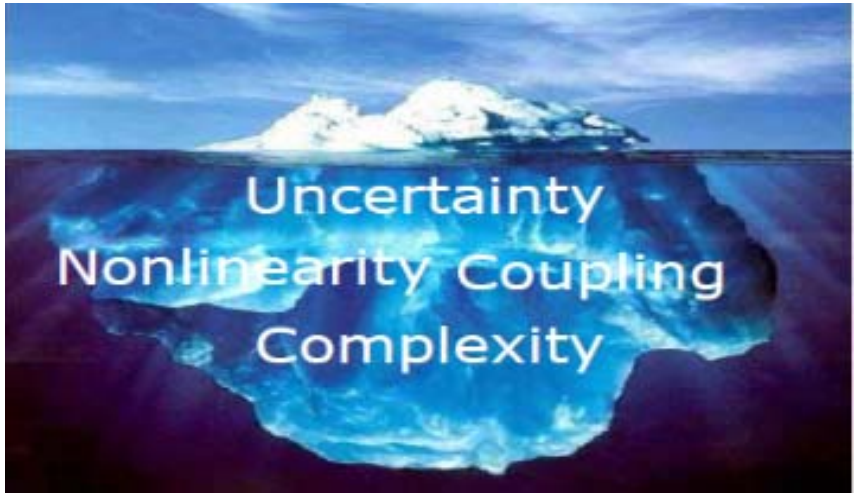


Summary & Concluding Remarks (2)

- Formal Verification (Design Time)
  - PolyCARP: A collection of formally verified algorithms and software for computations with polygons.
  - DAIDALUS (Detect and Avoid Alerting Logic for Unmanned Systems): A collection of formally verified detect and avoid algorithms for Unmanned Aircraft Systems.
  - ICAROUS (Integrated Configurable Algorithms for Reliable Operations of Unmanned Systems): A software architecture that enables the robust integration of mission specific software modules and highly assured core software modules for building safety-centric autonomous unmanned aircraft applications.
  - PRECiSA (Program Round-off Error Certifier via Static Analysis): A static analysis tool that generates provably correct round-off error bounds of floating-point functional expressions.
- Formal Verification (Operational/Runtime)
  - Automatic generation of minimally invasive monitors (e.g., executable C code) from formal specifications
  - Generation of provably correct shields for distributed controller synthesis
  - Provably correct translation of rule-based learning mechanisms specified in cognitive architectures into formal verification framework
- Certification
  - DO-333 Formal Methods Supplement, DO-178C, Overarching Properties
  - Development of mock certification basis for midsize UAS with operational restrictions

Outline

- Overview of V&V in Aviation Safety
  - Definitions
  - Current and Emerging Aviation Safety Issues
    - » Aircraft Loss of Control
    - » Increasing Levels of Autonomy
  - Onboard System Certification Requirements for Transport Aircraft
- Validation of Safety-Critical Aircraft Systems
  - Analysis
  - Simulation
  - Experimental Testing
  - Real-Time Monitoring
  - Integrated Validation Process
- Verification
  - Design Time Verification (Assurance Cases)
    - » Conventional verification practices
    - » Novel modelling, analysis and simulation techniques
  - Run Time Verification (Operational Safety)
    - » Requirements Elicitation and Precursor Identification
    - » Architectures (Monitor, Assess, Mitigate)
- Certification
  - Current Practices and Standards
  - Enabling new operations and increasingly autonomous systems
- Summary & Concluding Remarks
- Future Directions



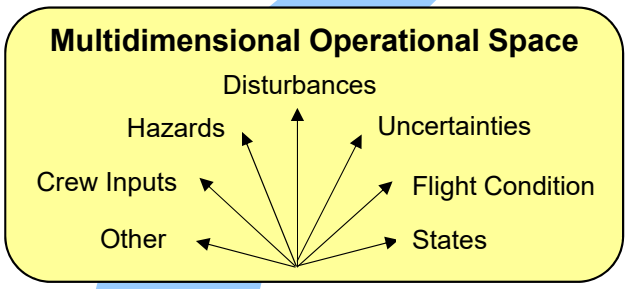
Future Directions (1)

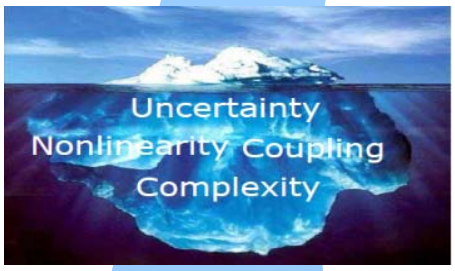
V&V of Autonomous Systems
- Dynamic Function Allocation & Variable Autonomy
- Off-Nominal, Abnormal, & Worst Case Conditions
- Expected & Unexpected Hazards

V&V of Complex Integrated Systems
- Vehicle Health Management
- Resilient Guidance, Navigation, & Control
- Crew Interface

V&V of Resilient Systems
- Comprehensive Hazards-Based Test Scenarios (e.g., LOC)
- Identification of Worst-Case Conditions
- Integrated Analysis, Simulation, & Experimental Test Methods, Tools, & Testbeds for Assessing System Effectiveness under Off-Nominal / Hazardous Conditions

V&V of Uncertain Nonlinear Systems
- Identification of Safe / Unsafe Regions of Operation
- Analysis Methods & Tools for Uncertainty, Nonlinear Effects, & Robustness Assessments





Current Systems / V&V Methods

Evidence-Based Certification / Assurance of Safety-Critical Resilient Autonomous Systems

Quantifiable Level of Confidence in the V&V Results

Individual & Integrated Technology Limitations, Weaknesses & Constraints

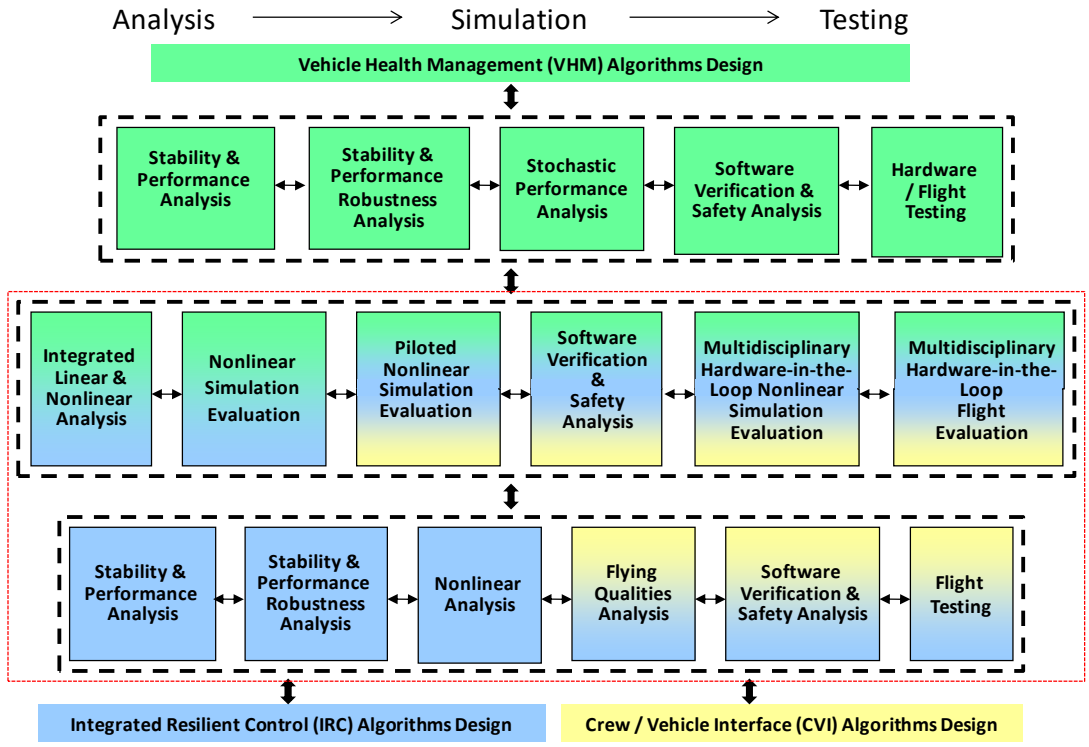
Level of Hazards Coverage

Degree of Technology Effectiveness

Future Directions (2)

Advanced Integrated System Technologies:

- Vehicle Health Management Systems
- Resilient Guidance & Control Systems
- Crew / System Interface Systems



Advanced Integrated V&V Technologies:

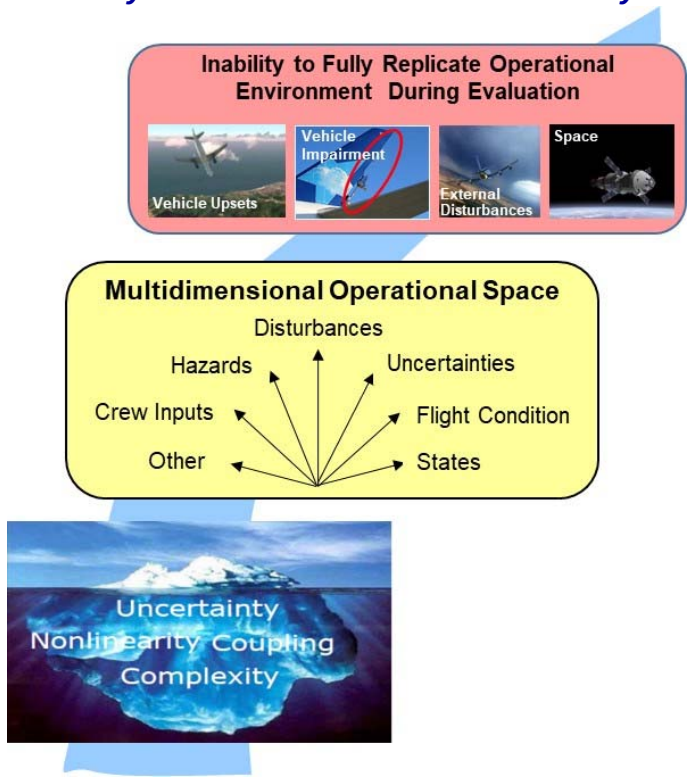
- ***Evidence-Based VV&C***
- ***Complex Integrated Systems***
- ***Relevant Focus Problems***

Develop & Demonstrate Integrated V&V and Certification Process for Safety-Critical Resilient & Autonomous Systems

Future Directions (3)

- Validation
  - Analysis of Nonlinear Uncertain Systems
    - » Expansion of Underlying Computational Methods for Large-Scale System Analysis
    - » Automated Methods & User Interfaces that Facilitate the Use of Multiple Analysis Tools
  - Simulation of Transport Aircraft under LOC Conditions
    - » Development of Guided Monte Carlo Tools that Utilize Analysis Results and
    - » Assess Potentially Problematic Regions in a Multidimensional Problem Space
  - Experimental Testing
    - » Subscale Vehicle Platforms that Enable the Assessment of Multidisciplinary Hazard Effects
    - » Multidisciplinary Ground-Based Assessment Capability that Provides Linked Lab Assessments (SAFETI Lab)
  - Real-Time Monitoring
    - » Improvement, Demonstration, & Evaluation of Individual Methods Developed to Date
    - » Development of Integrated Monitoring Methods for Ensuring Flight Safety
  - Integrated Coordinated Validation Process
    - » Refinement of Coordinated Framework & Demonstration of Methodical Process to Apply It
    - » Development of User Interfaces to Assist in Coordinated Validation Process
  - LOC Hazards-Based Test Scenarios
    - » Comprehensive Set of Test Scenarios Needed for Current & Future Hazards
    - » Use of Mission Task Elements (MTEs) to Ensure Effective Hazards Coverage Across the Mission
    - » Mechanisms for Assessing Realistic “Unexpected / Unanticipated” Hazards

Evidence-Based Certification / Assurance of Safety-Critical Resilient Autonomous Systems



Current Systems / V&V Methods

Future Directions (4)

Verification: Areas for Fundamental Research

- Scalable methods addressing formal verification of safety and liveness properties of Increasingly Autonomous (IA) systems
  - Domain specific formalisms that are readable and reviewable
  - Formal verification techniques that are fully scalable
  - Composition and Reuse
- Methods for assuring safety over diverse role allocation and decision-making paradigms
  - Mathematical models for describing adaptive/nondeterministic processes as applied to humans and machines.
- Provably Correct Synthesis of Assurance Monitors
  - Formally Verified Runtime Monitors, Steering Functions
- Simulation and Testing approaches to increase confidence in safety critical decision making for IA systems
- Certification Standards
  - IA systems, Novel (aviation) ConOps

Key References (1)

Validation

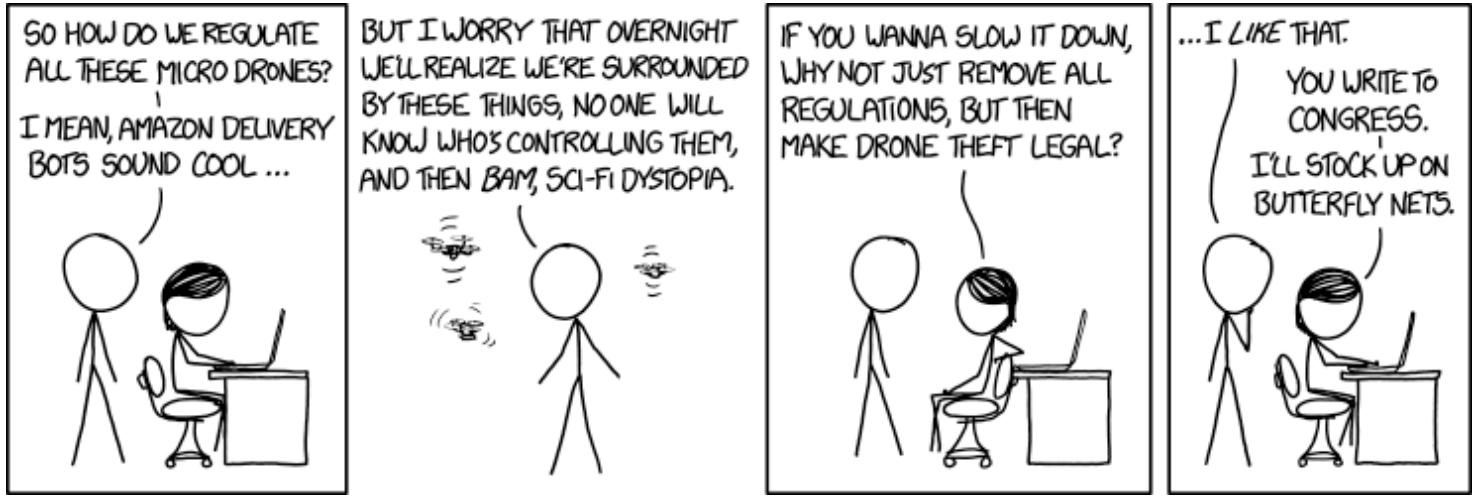
- ***Journal of Guidance, Control, and Dynamics*: Special Issue on Aircraft Loss of Control, Vol. 40, No. 4, April 2017**
  - **Belcastro, et al: "Aircraft Loss of Control Problem Analysis and Research Toward a Holistic Solution"**
- Belcastro, et al; "Hazards Identification and Analysis for Unmanned Aircraft System Operations;" 2017 Aviation Forum ATIO-ATM Conference.
- Belcastro, et al; "Aircraft Loss of Control: Problem Analysis for the Development and Validation of Technology Solutions;" AIAA Conference on Guidance, Navigation, and Control, SciTech Forum, 2016.
- Belcastro, et al; "Preliminary Analysis of Aircraft Loss of Control Accidents: Worst Case Precursor Combinations and Temporal Sequencing", *AIAA Conference on Guidance, Navigation, and Control*, *SciTech Forum*, 2014.
- Newman, Richard; "Pitot-Static Blockages;" Aviation Safety Magazine, Aircraft Systems, November 2020. (To Appear)
- Belcastro, Christine M.; "Validation of Safety-Critical Systems for Aircraft Loss-of-Control Prevention and Recovery;" *AIAA Conference on Guidance, Navigation, and Control*, 2012.
- Belcastro, Christine M.; Validation and Verification of Future Integrated Safety-Critical Systems Operating under Off-Nominal Conditions;" *AIAA Conference on Guidance, Navigation, and Control*, 2010.
- Belcastro, Christine M., "Validation and Verification Techniques and Tools," Encyclopedia of Systems & Control, Edited by John Baillieul and Tariq Samad, Springer, February 2015.
- Belcastro, Christine M.: *Validation & Verification of Safety-Critical Systems Operating under Off-Nominal Conditions.* Chapter 20 of the Book Entitled: Optimization-Based Clearance of Flight Control Laws, Springer, 2011.

Key References (2)

Verification

- Neogi, N., Bhattacharyya, S, Greissler, D., Kiran, H., and M. Carvalho, "Assuring Intelligent Systems: A UAS Case Study", IEEE Transactions on Intelligent Transportation Systems, Special Issue on Unmanned Aerial Systems Traffic Management, Accepted for Publication October 2020.
- Bharadwaj, S., Carr, S., Neogi, N., Poonawala, H., Barberia Chueca, A., and U. Topcu, "Traffic Management for Urban Air Mobility". IEEE Transactions on Control of Network Systems, Special Issue on Control of Very Lare Scale Robotic (VLSR) Networks, Accepted for publication April 2020.
- Bharadwaj, S., Carr, S., Neogi, N., Poonawala, H., Barberia Chueca, A., and U. Topcu, "Traffic Management for Urban Air Mobility". NFM 2019: 71-87.
- Washington, A., Clothier, R., Neogi, N., Silva, J., Hayhurst, K., and B. Williams, "Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems," Safe. Sci. Vol 118, October 2019, pp. 654-673.
- Bhattacharyya, S., Eskridge, T., Neogi, N., Carvalho, M., and M. Stafford. "Formal Assurance for Cooperative Intelligent Autonomous Agents." NFM 2018: 20-36.
- Neogi, N., and A. Sen, "Integrating UAS into the National Airspace System", in *Unmanned Aerial Vehicles and Networks*, Kamesh Namuduri (ed.), Cambridge University Press, November 2017.
- Hayhurst, K. J.; Maddalon, J. M.; Neogi, N. A.; Verstynen: Design Requirements for Unmanned Rotorcraft used in Low-Risk Concepts of Operation, NASA/TM–2016-219345, November 2016, 107 p. Subject Category 03.

Questions?



Oh, weird, Amazon is out of butterfly nets…

https://xkcd.com/1523/

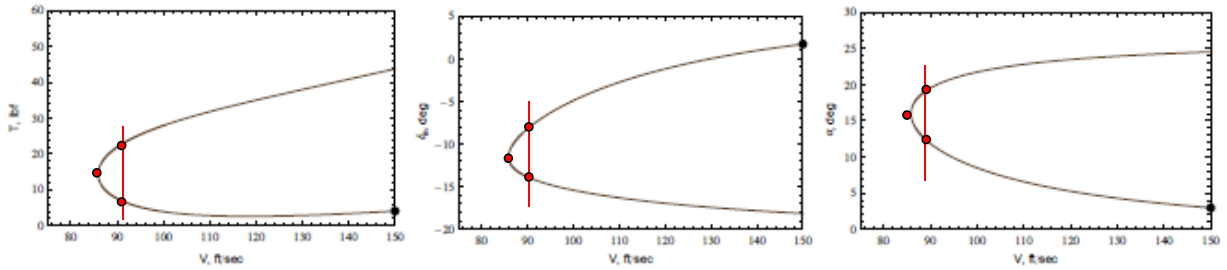
Contact Information

- Validation
  - Dr. Christine M. Belcastro (Retired, Distinguished Research Associate, NASA Langley)
    - » christine.m.belcastro@nasa.gov; christine.m.belcastro@gmail.com
  - Mr. John V. Foster (john.v.foster@nasa.gov)
  - Dr. Irene M. Gregory (irene.m.gregory@nasa.gov)
  - Dr. David E. Cox (david.e.cox@nasa.gov)
  - Dr. Sean P. Kenny (sean.p.kenny@nasa.gov)
  - Dr. Luis G. Crespo (luis.g.crespo@nasa.gov)
  - Dr. Eugene Morelli (e.a.morelli@nasa.gov)
  - Dr. Ersin Ancel (ersin.ancel@nasa.gov)
  - Mr. Gautam H. Shah (gautam.h.shah@nasa.gov)
  - Mr. Kevin Cunningham (kevin.cunningham@nasa.gov)
- Verification
  - Dr. Natasha A. Neogi (NASA Langley)
    - » natasha.a.neogi@nasa.gov
  - Dr. Evan T. Dill (evan.t.dill@nasa.gov)
  - Dr. Cesar A. Munoz (cesar.a.munoz@nasa.gov)
  - Dr. Aaron M. Dutle (aaron.m.dutle@nasa.gov)
  - Dr. Alwyn E. Goodloe (a.goodloe@nasa.gov)
  - Dr. Mallory Graydon (m.s.graydon@nasa.gov)
  - Mr. Michael Holloway (c.michael.holloway@nasa.gov)

Backup Slides

Analysis Method: Nonlinear Dynamics & Control

Stall Bifurcation Analysis Example: Trim Motion of the Phugoid Dynamics



(a) Thrust (b) Elevator Position (c) Angle of Attack

Fig. .1 The figure shows the trim values for thrust, elevator and angle of attack for various values of airspeed, V, and $\gamma = 0$. Note that the starting point for the continuation is identified by the black dot.

Bifurcation: Points in the state space (or flight envelope) which result in abnormal dynamic response and at which normal vehicle trim cannot be achieved

Analysis Results

- **At the Bifurcation Point: Thrust and Elevator are Redundant → Both V and γ Cannot be Controlled**
- **Control Behaviors Around the Bifurcation Point:**
  - **Elevator Control Reversal between Upper and Lower Branch**
  - **Thrust Reversal Near Stall (i.e., Increasing Thrust Corresponds to Decreasing Airspeed)**

These Characteristics Make Vehicle Flight Control Difficult and Non-intuitive

Research Partners: Drexel University, Techno-Sciences, Inc.

Analysis Method: Uncertainty Quantification (1)

Uncertainty Quantification

Determine probability of a given outcome when properties of the system are not exactly known.

Standard Practice: Monte-Carlo Simulation

Model the physics, bound the parameters, and test requirements for every combination (that you have time for).

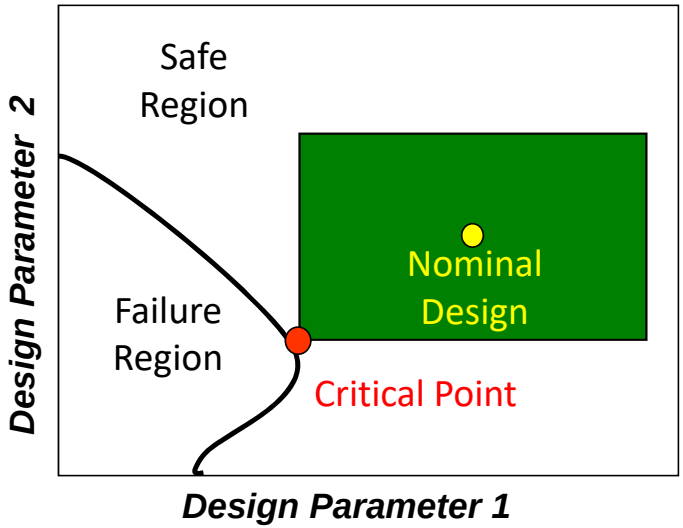
Monte-Carlo is prohibitively expensive when the probability of failure is low or the dimension of the parameter space is large.

Analytic Techniques

Homothetic Deformation. Starting from a nominal design point expand contiguous region until a critical point where requirements fail.

UQTools

Software Toolbox, developed under Aviation Safety in 2010 and available via Software Release, that implements Analytic Techniques.



Safe/Failure outcome is defined by performance requirements.

Technical POCs: Dr. Sean Kenny and Dr. Luis Crespo, NASA Langley

Analysis Method: Uncertainty Quantification (2)

Example: How accurate do identified aero coefficients need to be to retain adequate closed-loop performance

Physics:

GTM Simulation, Baseline Flight Controller

Requirements: 9 conditions including

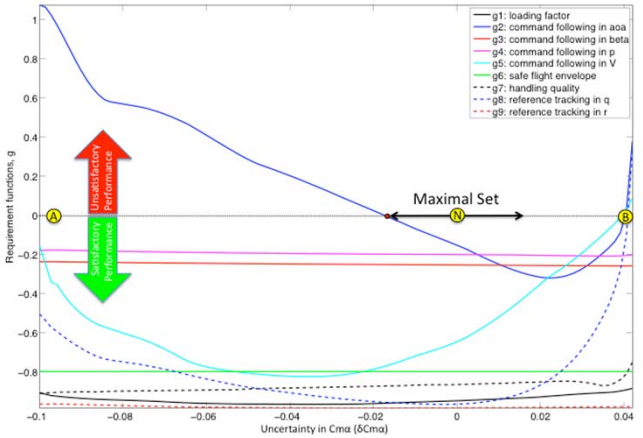
- Max load factor
- Command tracking (Wind Angles & Rates)
- Handling Quality (Stick response)

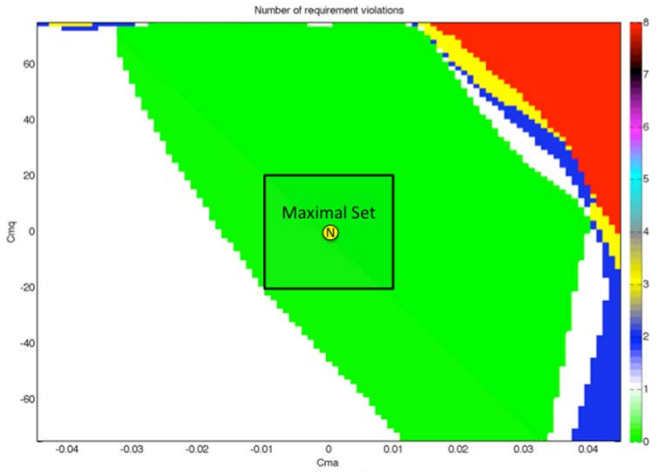
Parameters:

- Aero Coefficients
- Control Authority

Results:

Bounding box on acceptable variation in aero coefficients. Validated with exhaustive search on 2-D case.





POCs: Dr. Sean Kenny and Dr. Luis Crespo, NASA Langley

Analysis Method: Uncertainty Quantification (3)

Challenge Problem is a microcosm of a full project cycle: Model, Evaluate, Test, and Validate.

Physics:

GTM Simulation, parameterized controller.

Requirements:

8 Performance requirements, including command tracking, stability, control power limits, etc.

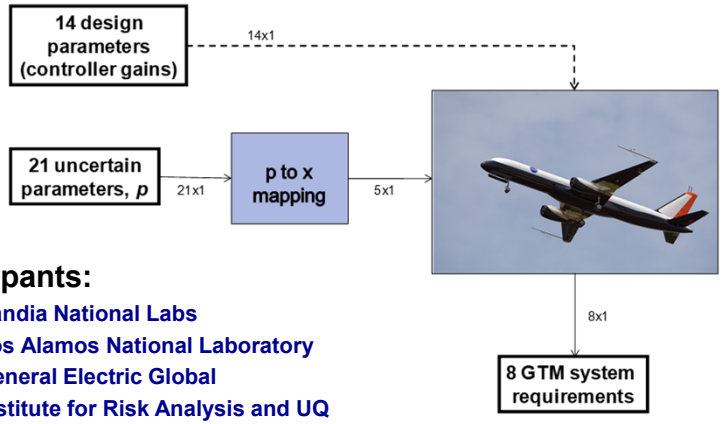
Parameters:

21 poorly known parameters.

Challenge Problem:

Given model, parameter range estimates and limited observations of the true system:

1) Refine uncertain ranges required to explain available data
2) Determine sensitivity to parameters
3) Request 2nd set of "truth" data selected parameters exercised



Participants:

- Sandia National Labs
- Los Alamos National Laboratory
- General Electric Global
- Institute for Risk Analysis and UQ
- Vanderbilt University
- University of Florida
- Supelec, France
- Swiss Institute of Technology
- University of South California
- Southwest Research Institute (SwRI)
- NASA Ames

Output:

10 papers at SciTech 2014

Special UQ edition of the AIAA Journal of Aerospace Information Systems

POCs: Dr. Sean Kenny and Dr. Luis Crespo, NASA Langley
To be Presented on December 15

Analysis Method: Probabilistic Uncertainty Effects (1)

Algorithms for Uncertainty Representation and Analysis (AURA)

- Potential Sources of Uncertainty in Complex Safety-Critical Systems
  - Uncertain structural and rigid body dynamics due to factors including
    - » variability in manufacturing processes
    - » wear and other aging effects
    - » limited modeling, particularly in low-cost systems
  - Operational environments with unpredictable composition
  - Communication interference, delays, or drop-outs
  - Random external forces due to wind gusts or other effects
  - Sensor data that is noisy, mis-calibrated, or otherwise corrupted
  - Actuators with uncertainties, such as free-play
  - Adaptation or learning-based components
- **Understanding** the range of possible system behaviors in response to these **uncertainties is critical for verification, validation and certification** of safety critical systems

- AURA Probabilistic Analysis Toolset
  - Enables designers to directly model uncertainties associated with design, implementation, and operation of complex systems
  - Propagates these uncertainties through system components and around feedback loops
  - Computes the resulting variability in system behavior
- AURA Capabilities
  - Highly efficient C++ library, with seamless integration to both Matlab and Simulink, that:
    - » Adds new datatypes and functions for manipulating random quantities
    - » Can interact with previously constructed models and code bases
  - Works with complete characterizations of random quantities, and can compute:
    - » Mean, variance, higher-order moments, and sensitivity indices
    - » Marginal and joint PDFs and CDFs of arbitrary variable combinations
    - » Probabilities of arbitrary events
  - Based on generalized polynomial chaos theory
    - » Has a rigorous and well-developed theoretical foundation
    - » Can represent arbitrary probability distributions
    - » Handles arbitrary dependencies between random quantities in a system

Research Partner: Barron Associates

Analysis Method: Probabilistic Uncertainty Effects (2)

AURA Application Examples

Validation of Autonomous Path Planning Algorithms for UAS

- Produce efficient global models of path planning algorithm performance
- Enable analysis and visualization of algorithm performance
  - What is the worst-case value of a metric?
  - What is the likelihood of a metric exceeding a specified limit?
  - What is the likelihood of a metric falling in a specified range?
  - What values/combinations of operating space parameters lead to worst case behavior?

- Develop tools to integrate into existing infrastructure and workflow
- Minimize human analyst interaction during gPC model generation
- Proof-of-concept demonstrations with representative path planners have shown these features

Other AURA Applications

- Determining the expected performance of onboard vehicle diagnostic systems to support certification of those components
- Mitigating risks of aeroelastic instability in flight tests conducted near the flutter boundary
- Deriving safe operating boundaries of automated aircraft control algorithms that are protected by run-time assurance architectures
- Computing the likely trajectory of orbital debris from noisy and infrequent sensor measurements
- Constructing personalized models of drug pharmacokinetics, expressing how a compound migrates between organ systems to support personalized medicine
- Predicting power consumption of electric cars over alternative routes with different driving styles

Research Partner: Barron Associates

Simulation: Enhanced Fixed-Base

Example: Enhanced Transport Aircraft Simulation Model for Stall

Baseline Simulation followed by Enhanced Simulation

POCs: Gautam Shah, John Foster, and Kevin Cunningham, NASA Langley
Research Partner: Boeing

Simulation: Enhanced Motion-Based

NASA LaRC Motion-Based Simulator Facility

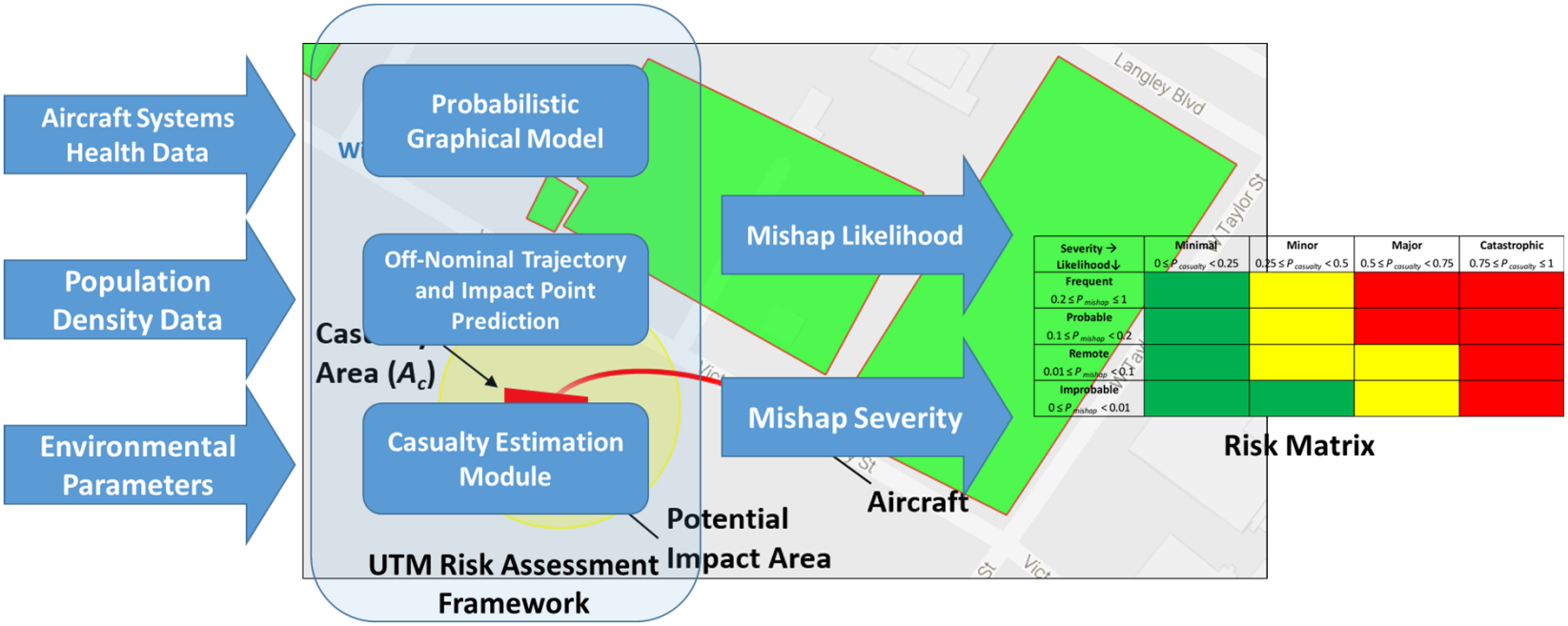
POCs: Gautam Shah, John Foster, and Kevin Cunningham, NASA Langley

Research Partner: Boeing

Onboard Monitoring: Real-Time Risk Assessment

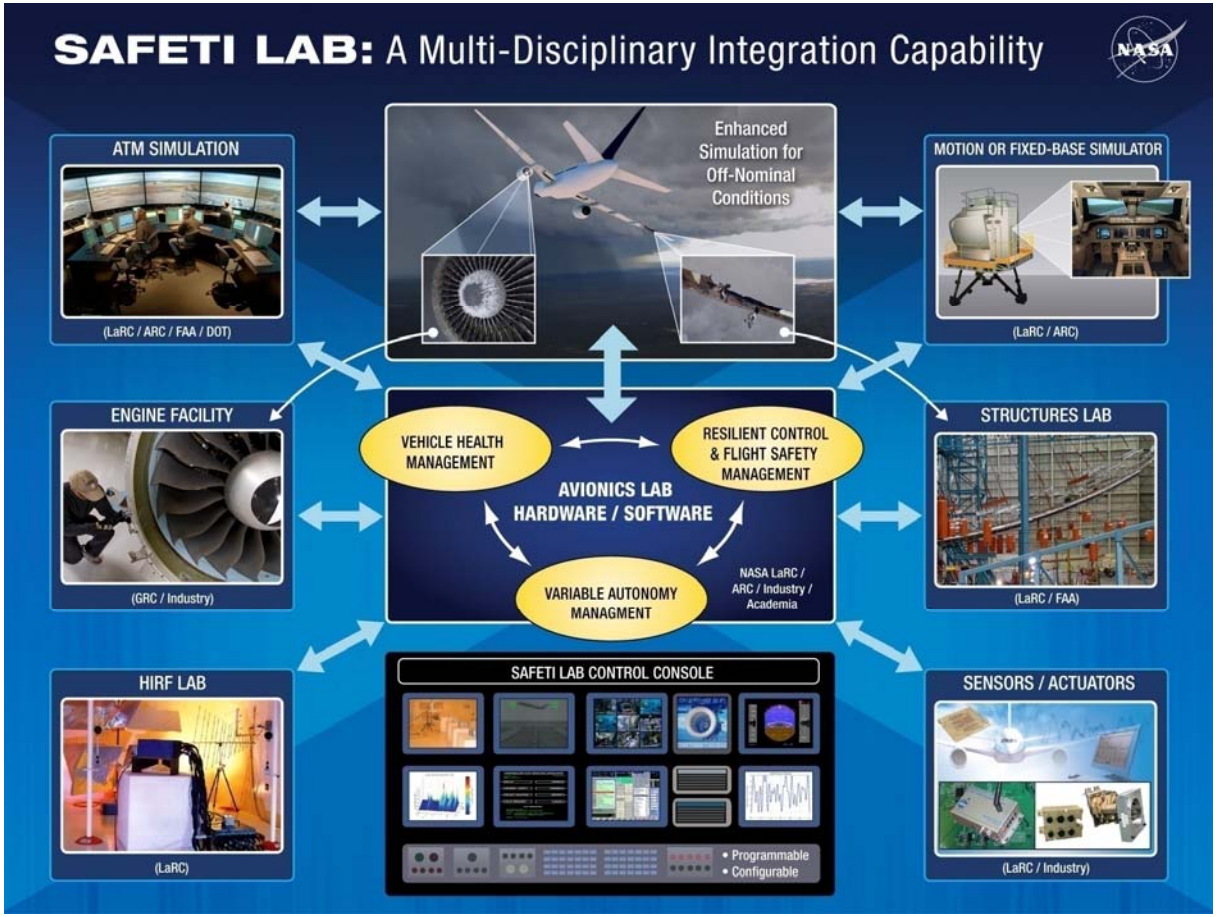
UAS Risk Assessment Framework (URAF)

- Developed under UTM project, URAF modular architecture helps develop non-participant casualty risk estimation implementations
- Configured for pre-flight and in-flight applications
- Employs available aircraft health, population, and environmental data to estimate the ground risk to support various decision making activities



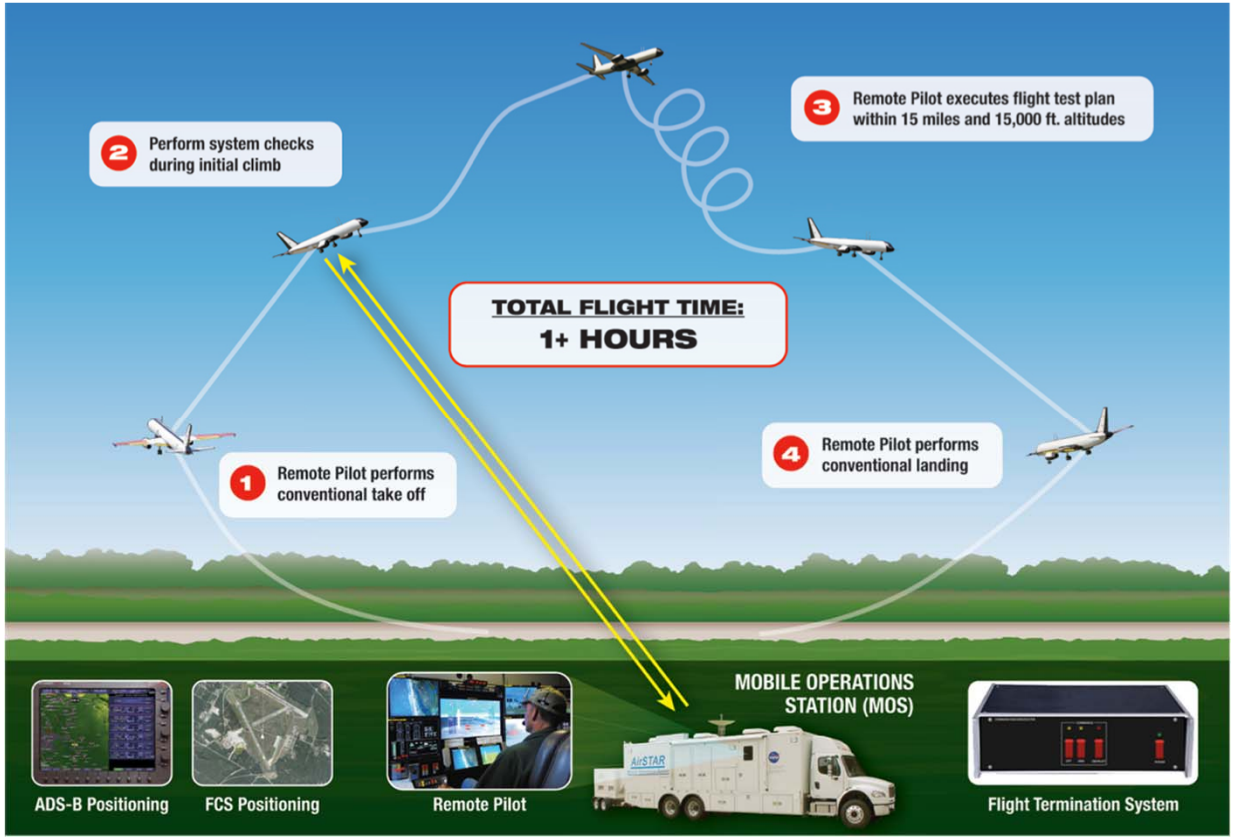
POC: Dr. Ersin Ancel, NASA Langley

Experimental Methods: Multidisciplinary Ground Testing



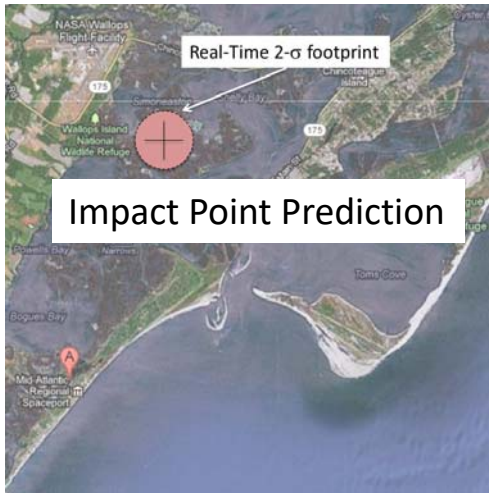
Experimental Methods: Subscale Flight Testing (1)

AirSTAR Flight Beyond Visual Range (BVR)



Low-Risk Test Vehicle

Real-Time Impact Point Prediction in the Presence of Uncertainty



POCs: Dr. David Cox and Mr. Kevin Cunningham, NASA Langley

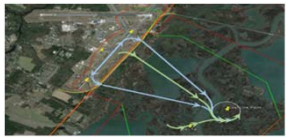
Experimental Methods: Subscale Flight Testing (2)

AirSTAR Flight Beyond Visual Range (BVR)

- BVR Deployment Conducted in May 2015 at NASA Wallops Flight Facility
- Airspace
  - Terminal operations area
    - » Standardized departure, arrival, approach procedures
    - » Carefully planned & simulated (workload, range safety)
  - Flight operations area
    - » Maneuvering airspace
    - » To 10 nm and 10,000 feet
- Airborne Systems Included 2 Contingency Systems (CS-A and CS-B)
- Ground Systems in the AirSTAR Mobile Operations Station (MOS)
  - Included System Health Monitor

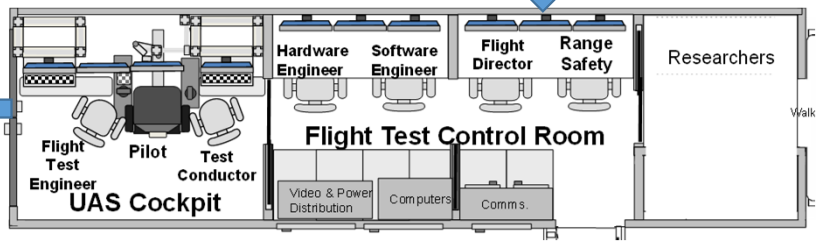
AirSTAR BVR Contingency Systems

Contingency System "A" (CS-A)
- Autopilot (independent of FCU)
- COTS equipment
- Auto or manual engagement
- Loss of: C&C link, FCU, cockpit



Contingency System "B" (CS-B)
- Flight termination capability
- COTS equipment
- Aero. controls for spin/spiral
- Impact point predictor
  - C_D, Wind profile, Spin entry params.
  - Uncertainties

AirSTAR Mobile Operations Station (MOS)

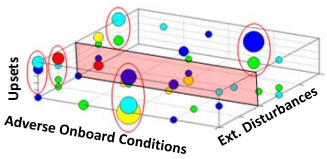


Approach for Developing LOC Test Scenarios

Hazards Analysis ⟷ **Realistic Test Scenarios with Traceability to the Hazards Sets**

Accident Data / Future Risks

Worst-Case Hazards Combinations

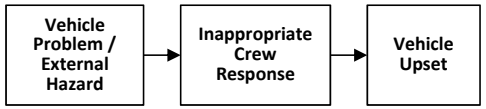


Crew Hazards
- Loss of Aircraft State Awareness
- Spatial Disorientation

Vehicle and Environmental Hazards
- Control Component Failures
- Icing Effects
- Wake Vortices

Abnormal Flight / Upset Hazards
- Extreme Attitudes
- Abnormal Energy States
- Abnormal Control Response
- Stall / Departure

Hazards Sequences



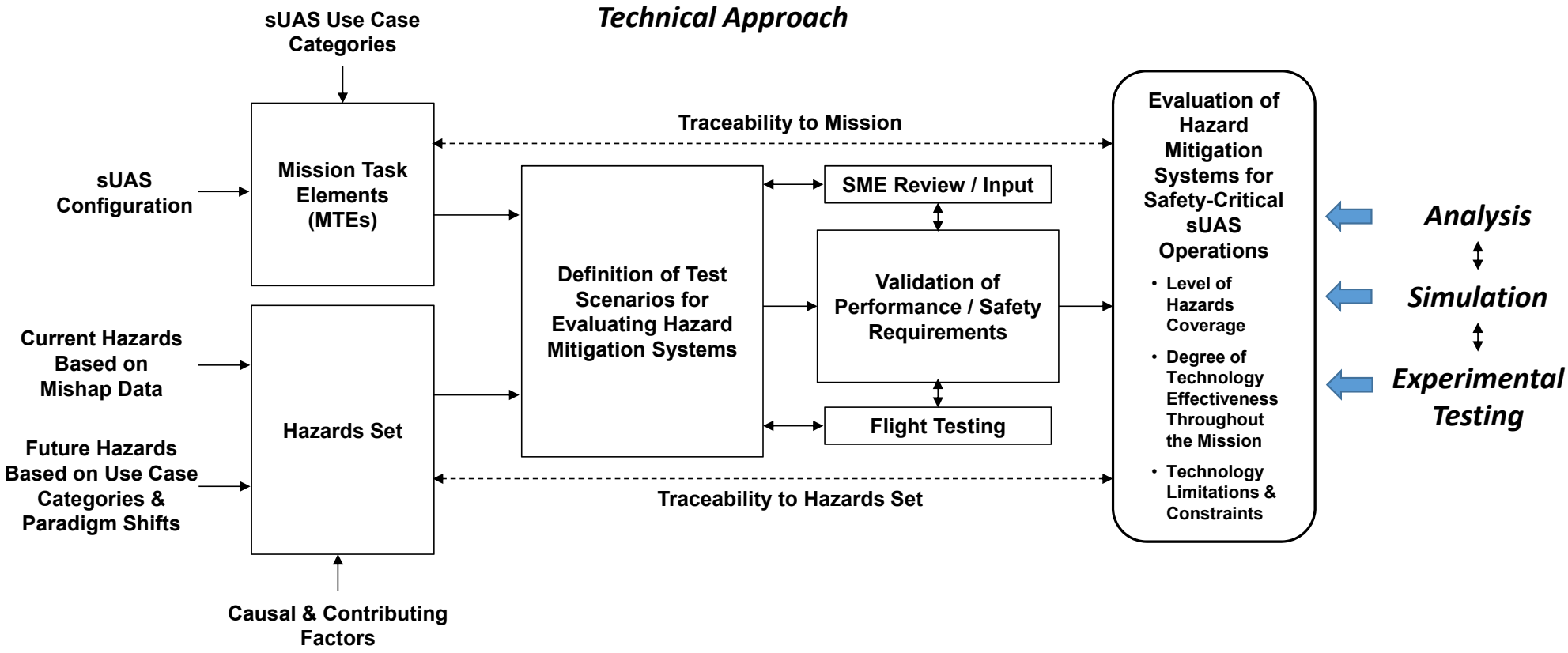
Unique & Generalized Sequences

Partners: NTSB & NIA (CAST / ATLAS)

Scenario Set Number	Recommended Evaluation Methods	Scenario Description	Flight Condition	Adverse Onboard Conditions	Inappropriate Crew Response	External Hazards & Disturbances	Vehicle Upset Conditions
Four Precursor LOC Scenarios: Vehicle Failure –> Inappropriate Crew Response –> Upset –> Vehicle Damage							
55	Analysis, Batch Simulation, Piloted Simulation	Engine Failure Followed by Crew Distraction Leading to Upset and Vehicle Damage	Cruise	1. Single Engine Failure (100% Thrust Loss); 4. Various Levels of Structural Damage with and without Loss of Control Effector	2. Crew Distraction Resulting in Delayed Response Followed by Excessive Response		3. Decreased Airspeed, Asymmetric Forces / Moments, Stall / Departure

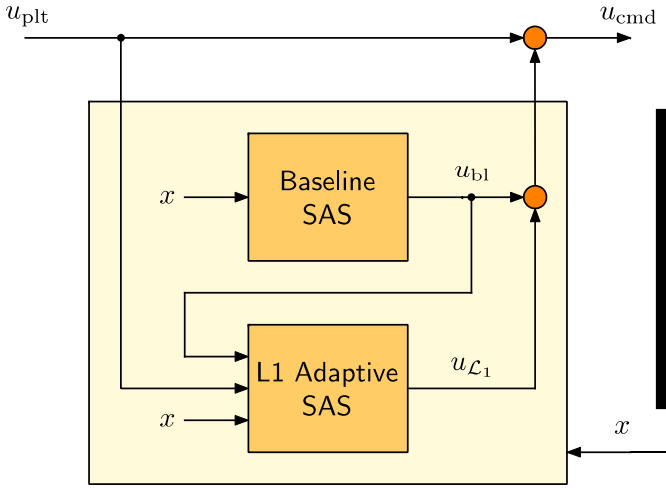
Scenario Set Number	Generalized Sequence	Coverage of Hazards Based on Historical Data & Future Potential Risk Sets								
		Accidents from Data Set Covered by Scenario	Number of Accidents from Data Set Covered by Scenario	Future Risks Covered by Scenario	Number of Future Risks Covered by Scenario	% Coverage of Data Set		% Cumulative Coverage		
						Accidents	Future Risks	Accidents	Additional Future Risks Covered	Future Risks
1	D	56	1	3	1	0.79%	10%	0.79%	1	10%
2	D	62, 63	2	3	1	1.59%	10%	2.38%	0	10%
3	D	1, 15, 18, 41, 79	5	3	1	3.97%	10%	6.35%	0	10%
4	D, E	17, 20, 8, 113	4	3	1	3.17%	10%	9.52%	0	10%
5	D	13	1	3	1	0.79%	10%	10.32%	0	10%
6	D	7	1	3	1	0.79%	10%	11.11%	0	10%
7	D	3	1	10	1	0.79%	10%	11.90%	1	20%
8	D	2	1	3, 10	2	0.79%	20%	12.70%	0	20%
9	D	2, 110	2	3, 10	2	1.59%	20%	14.29%	0	20%
10	D	N/A	0	7	1	0.00%	10%	14.29%	1	30%
11	D	16	1	8	1	0.79%	10%	15.08%	1	40%
12	D	N/A	0	4	1	0.00%	10%	15.08%	1	50%

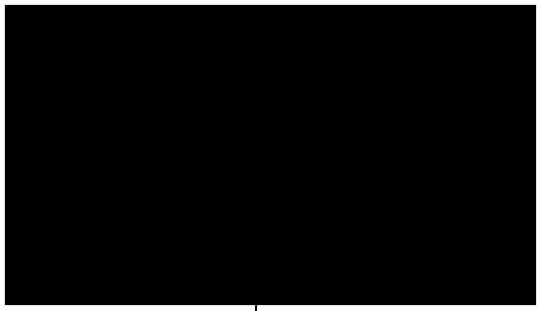
Test Scenarios for Assessing UAS Hazard Mitigation System Effectiveness



2017 AIAA Aviation Forum Paper: Belcastro, et.al, "Experimental Flight Testing for Assessing the Safety of Unmanned Aircraft System Safety-Critical Operations"

Full-Scale Flight Testing: Adaptive Control





Designed to maintain MIL-HDBK-1797 Level 1 flying qualities, and to prevent adverse aircraft-pilot interactions in the presence of aircraft failures

*Puig-Navarro, Ackerman, Hovakimyan, et. al., "An L1 Adaptive Stability Augmentation System Design for MIL-HDBK-1797 Level 1 Flying Qualities." AIAA Guidance, Navigation and Control Conference, San Diego, CA 2019.

* Ackerman, Puig-Navarro, Hovakimyan, et. al., "Recovery of desired Flying Characteristics with an L1 Adaptive Control: Flight Test Results on Calspan's VSS Learjet." AIAA Guidance, Navigation and Control Conference, San Diego, CA 2019.

POC: Dr. Irene Gregory, NASA Langley

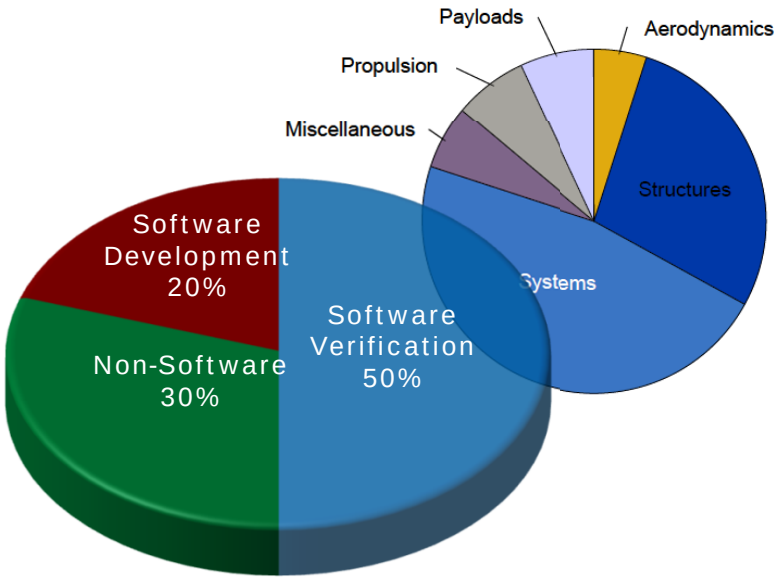
Research Partner: UIUC

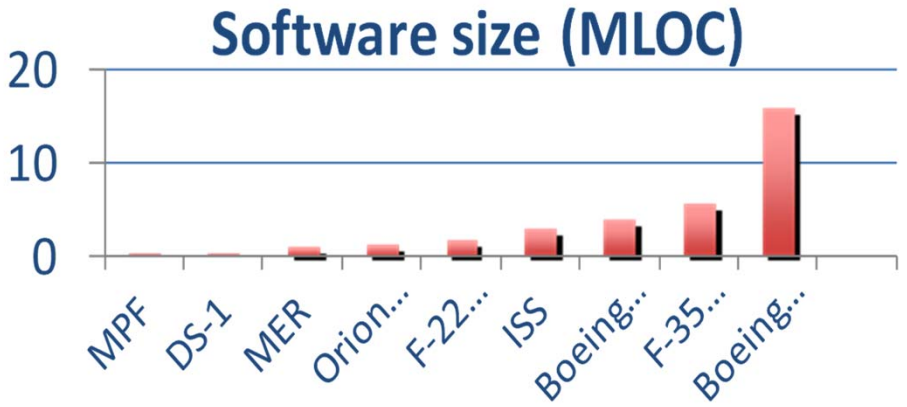
Introduction

- Increasing autonomy prevalent in critical-infrastructure systems
- Need to address challenges in:
  - Verification and Validation
  - Changing roles in human-machine teams
  - Managing system complexity and uncertainty in non-nominal conditions
  - Learning systems
- Must assess for mismatches in authority/responsibility
- Feasibility of task/capability of agent may be dynamic
  - Environment, faults, input blocking etc.
- Dynamic allocation likely requires creation of communications/coordination/monitoring tasks
- Task termination/correctness

Grand Challenge

Development of verification and validation techniques to establish confidence that new technologies are safe and provide a cost-effective basis for assurance and certification of complex civil aviation systems





Sources: Boeing 787: The Boeing Company. Others: *NASA Study on Flight Software Complexity*: *Final Report*. Ed. Daniel L. Dvorak. NASA Jet Propulsion Laboratory, California: NASA, March 5, 2009.

"Systems cost shifting away from structures, aero and propulsion to software and systems"

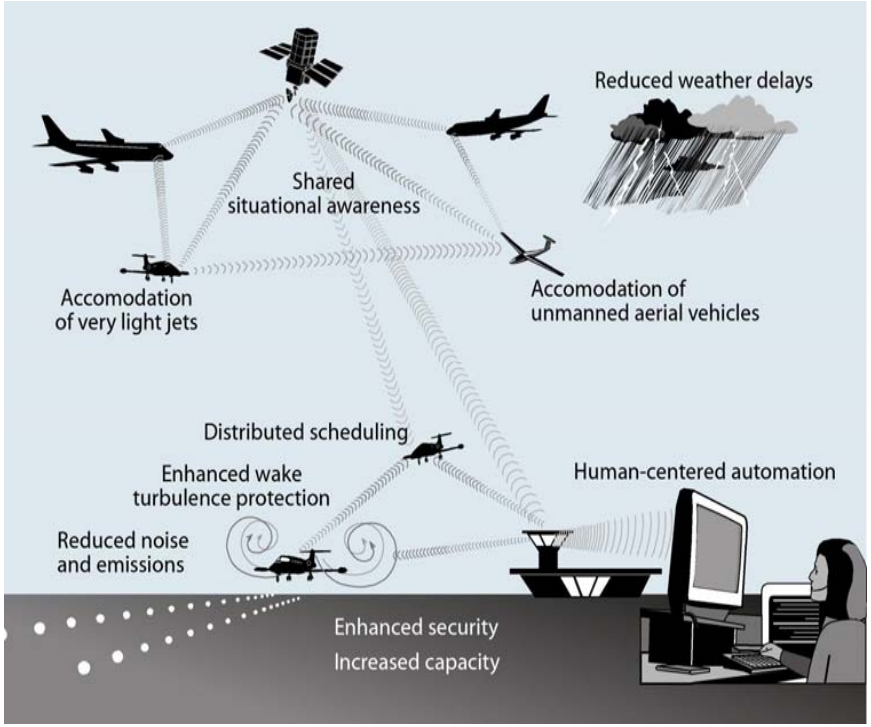
"Software verification is becoming one of the leading components of system cost – supporting certification"

"Verification will become even larger challenge as systems become more highly integrated"

Source: Winter, D. (VP, Engineering & IT, Boeing PW) Testimony to House Committee on Science and Technology, July 31, 2008.

Key Challenge Elements

- **Certification & Cost**
  - Composition
  - Reuse
- Bounding behavior of IA systems
- Trusted Decision Making
- Human Machine Integration
  - Extent of Human Supervision
- Formal Methods
- Run-Time V&V
- Safety Cases
- Security and Data Integrity



Autonomy's Impact on Aviation

Direct Effect

- Safety becomes increasingly dependent on software/automation
- Role of the pilot/controller becomes enmeshed more than ever with the automation
- Determining requirements becomes more difficult
  - especially for contingency management
- Data integrity and availability become more important
- Functionality moves further from federated systems to complex, integrated, network-centric system-of-systems
  - potentially more obscure error sources

Consequence

- Increased reliance on adaptive systems
  - systems that use real-time machine learning and statistical methods to mimic intelligence
- Needing improved system safety methods to identify & mitigate hazards
  - especially related to human roles/ responsibilities
- Needing improved methods for verification and validation that enable us to trust autonomy in all circumstances
  - Distinguishing correct and incorrect behavior is more difficult

Formal Methods for V&V of CDR/DAA Algorithms

- ACCoRD (Airborne Coordinated Conflict Resolution and Detection): A formal framework for the development of state-based separation assurance systems.
- DAIDALUS (Detect and Avoid Alerting Logic for Unmanned Systems): A collection of formally verified detect and avoid algorithms for Unmanned Aircraft Systems.
- ICAROUS (Integrated Configurable Algorithms for Reliable Operations of Unmanned Systems): A software architecture that enables the robust integration of mission specific software modules and highly assured core software modules for building safety-centric autonomous unmanned aircraft applications.
- PolyCARP: A collection of formally verified algorithms and software for computations with polygons.
- PRECiSA (Program Round-off Error Certifier via Static Analysis): A static analysis tool that generates provably correct round-off error bounds of floating-point functional expressions.

return

Air-on-Ground Determination

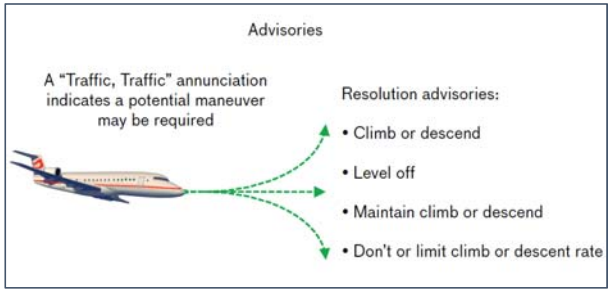
- FAA reports thousands of ADS-B equipped GA aircraft are **incorrectly reporting Air/Ground status** in ADS-B messages
- Aircraft lack mechanical means for determining this status
- Reporting Air while on ground makes aircraft appear with en-route service volumes to ATC (nuisance, cluttering)
- Reporting Ground while in air makes aircraft invisible to ATC (**dangerous**)
- CSC chose to develop an algorithm for performing this calculation, to be included in DO-260 (ADS-B MOPS)

- SWS supporting the Air-on-Ground subgroup. Conducting research toward specification, development, and testing of candidate Air/Ground determination algorithm
- Leveraging expertise in formal methods for capturing requirements, and in the future for algorithm verification.
- Assisting Air-on-Ground subgroup in data analysis

Technical POC: A. Dutle, NASA Langley

Model-based V&V Methodologies for Autonomous Systems Operation

Autonomy-based goal: Develop a V&V methodology for software following model-based execution, demonstrate it on the next generation onboard collision avoidance standard (ACAS X), and study its applicability to other autonomous algorithms.



Approach:

- 4/30/17 Demonstrate model-based V&V methodology on the next generation onboard collision avoidance standard (ACAS X).
- 8/31/17 Release toolset for model-based V&V of autonomous software. Produce report describing the developed V&V methodology and lessons learned from its application to ACAS X, including its applicability to other autonomous algorithms in support of UTM or SECAT.

Significance:

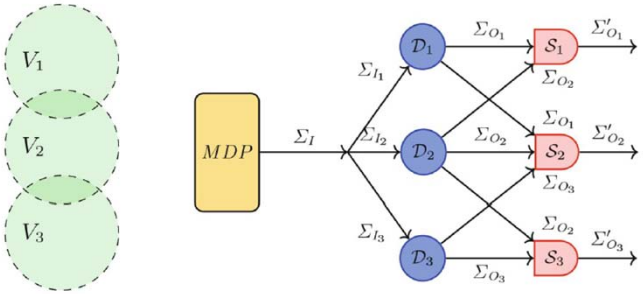
- Achieved ongoing collaboration with the FAA ACAS X team and infusion of the AdaStress (Adaptive Stress Testing) tool developed under the project within their V&V efforts. AdaStress identified bugs in the past and is currently used for regression testing and in support of the certification process.
- The optimization algorithms used in ACAS X are relevant to several autonomy problems so the approaches developed by our project are expected to play an important role for the V&V of autonomous systems.

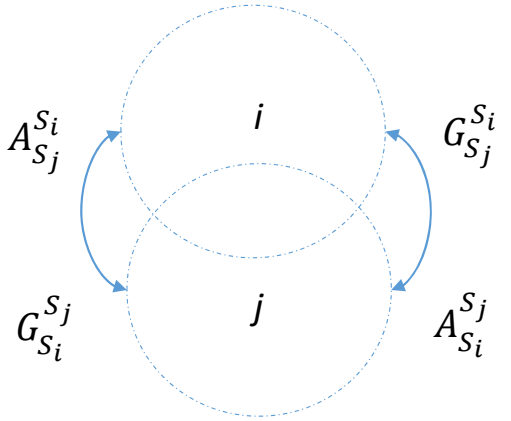
Decentralized Shield Synthesis

1. For each shield construct a game from the given safety specification and augment with contracts.
2. Solve for a permissive strategy.
3. Compute locally optimal deterministic strategy.

Note: Assume-Guarantee Contract between Shield S_i and S_j is specified as

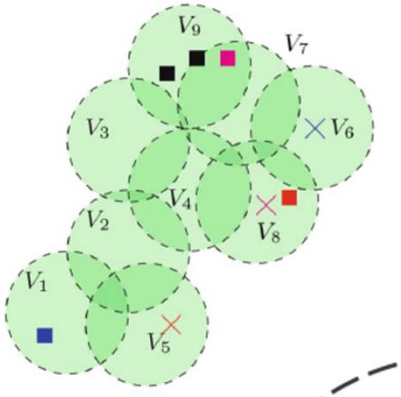
$$C_{S_j}^{S_i} = (A_{S_j}^{S_i}, G_{S_j}^{S_i})$$

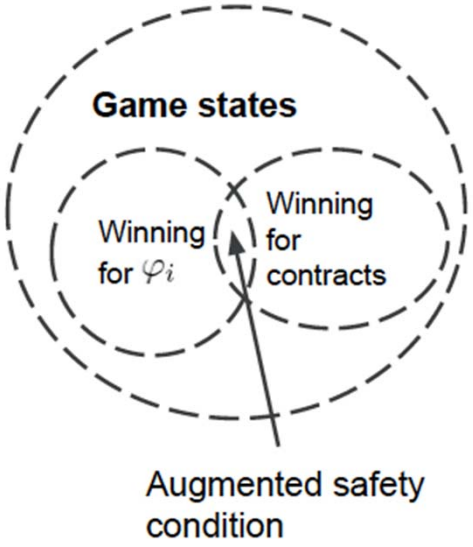




Game Construction and Simulation

- Game with acceptance condition defined by original safety requirement (e.g., congestion)
- Augment with contract requirements—still a safety game!
- Solve game using SmalL bUt Complete GROne Synthesizer (Slugs)



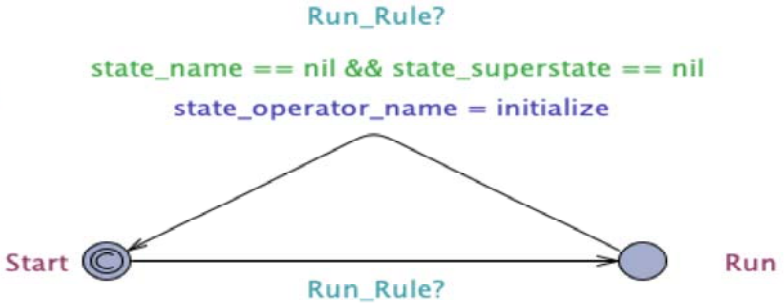


Suda Bharadwaj, Steven Carr, Natasha Neogi, Hasan Poonawala, Alejandro Barberia Chueca, Ufuk Topcu: **Traffic Management for Urban Air Mobility.** NFM 2019: 71-87

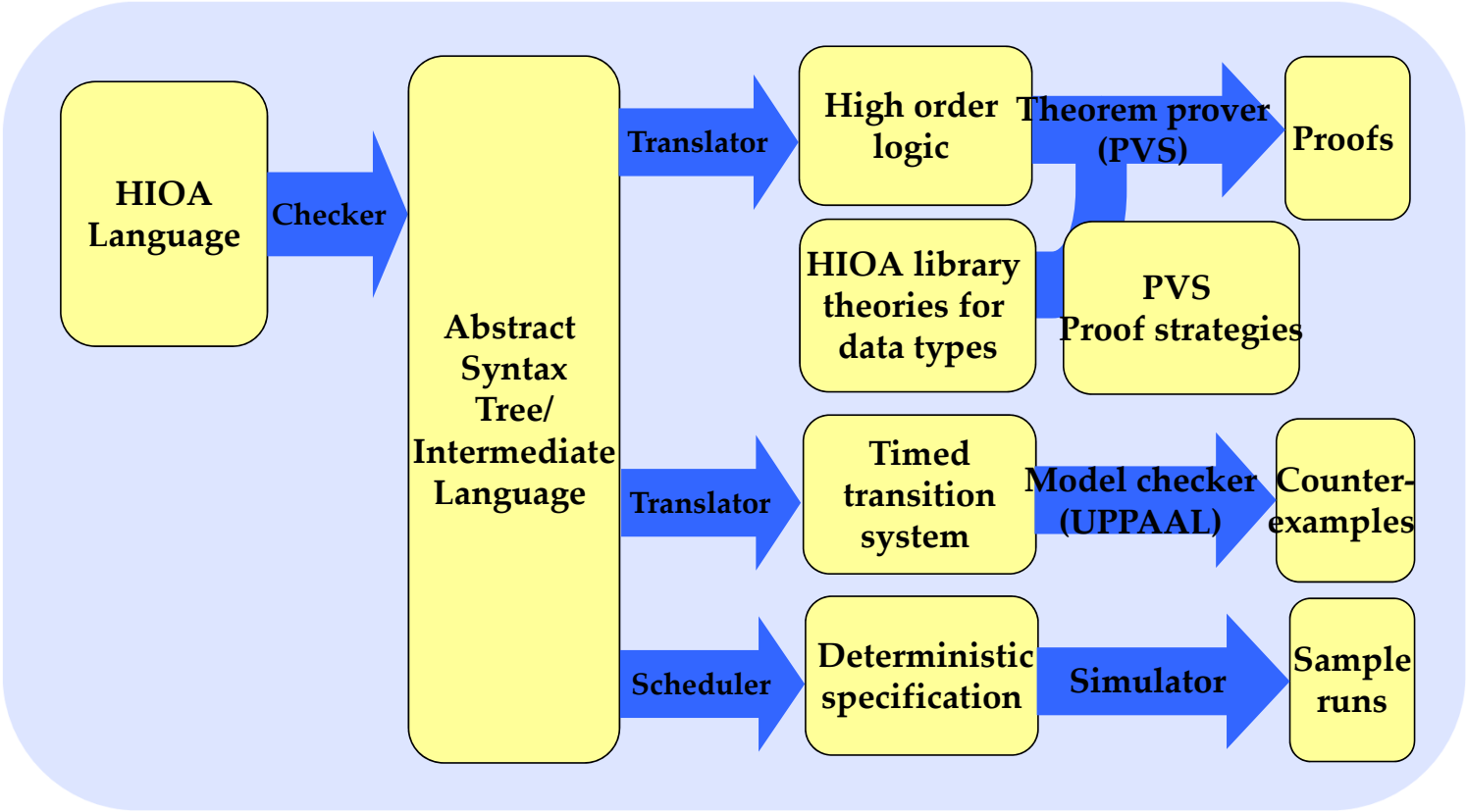
Perspectives

- Need to develop the what the right properties/standards are to Verify/Certify
  - **Correspondence between certification standards and software verification and validation artifacts is needed**
- Novel V&V technologies will require the development of new practices, techniques and qualification methods to meet certification standards and assure system wide safety

```
sp {proposeInitialize
(state <s> ^type state -^name ^superstate nil)
-->
(<s> ^operator <o> +)(<o> ^name initialize)}
```



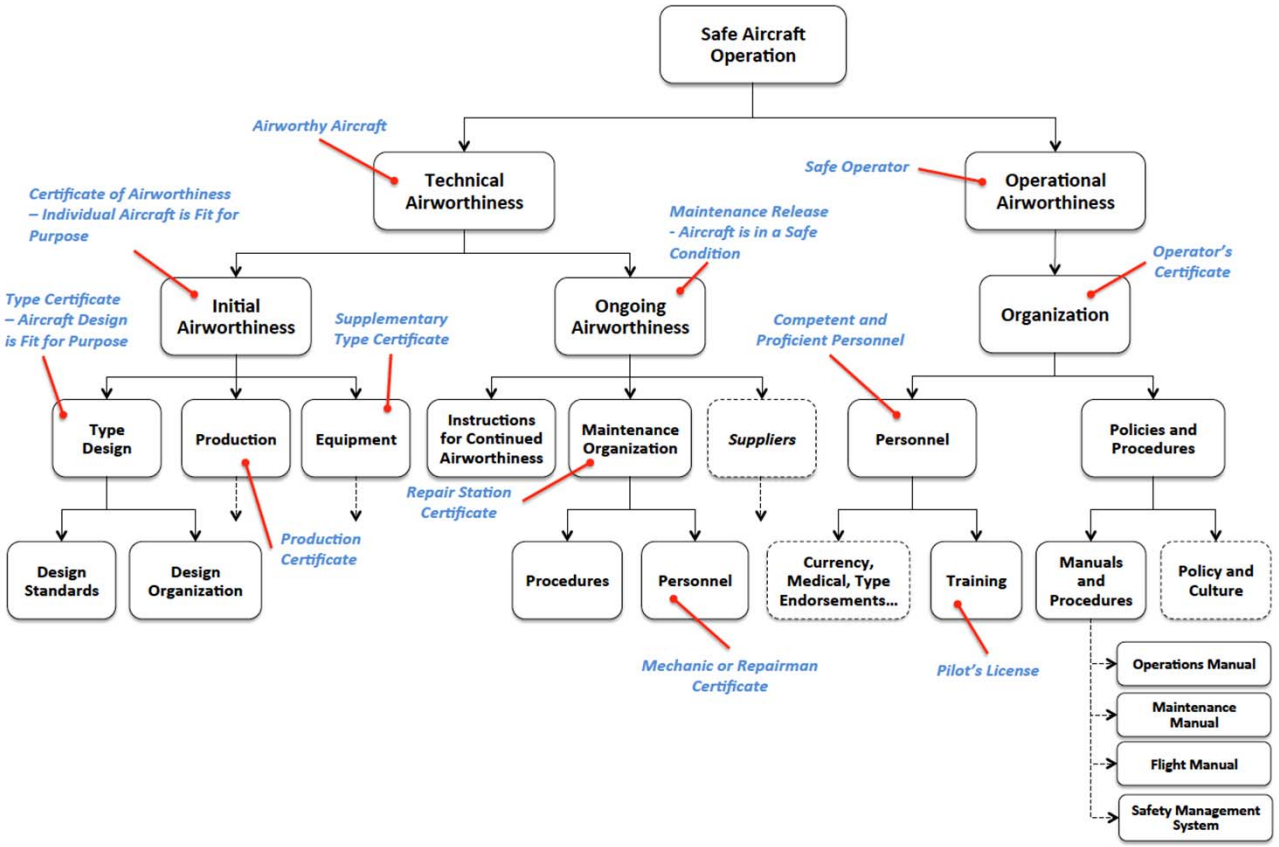
UAS Lost Link Case Study

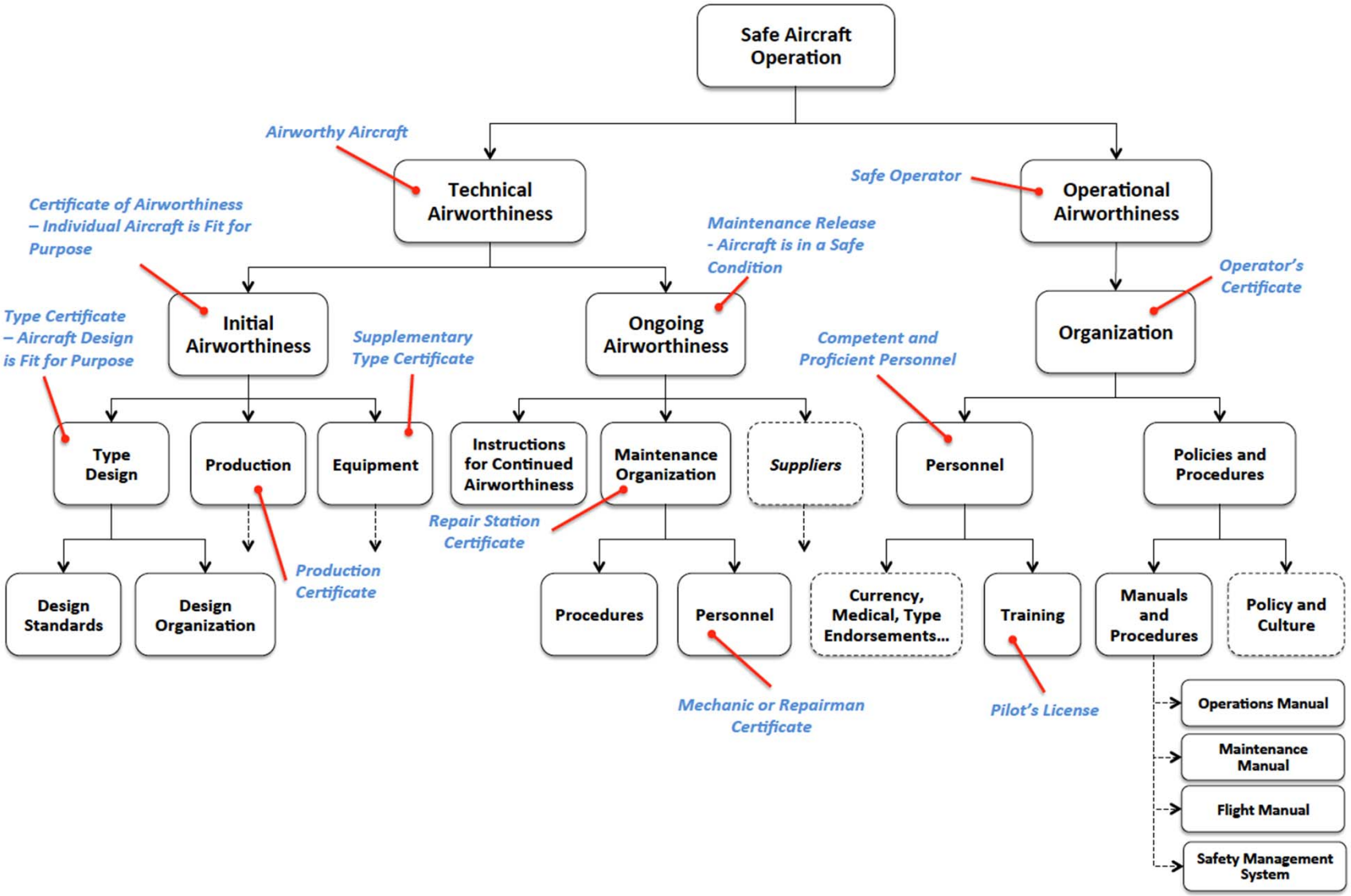


Timothy Wang, Romain Jobredeaux, Heber Herencia-Zapana, Pierre-Loïc Garoche, Arnaud Dieumegard, Eric Feron, Marc Pantel: **From Design to Implementation: an Automated, Credible Autocoding Chain for Control Systems.** CoRR abs/1307.2641 (2013)

Romain Jobredeaux, Heber Herencia-Zapana, Natasha A. Neogi, Eric Feron: **Developing proof carrying code to formally assure termination in fault tolerant distributed controls systems.** CDC 2012: 1816-182

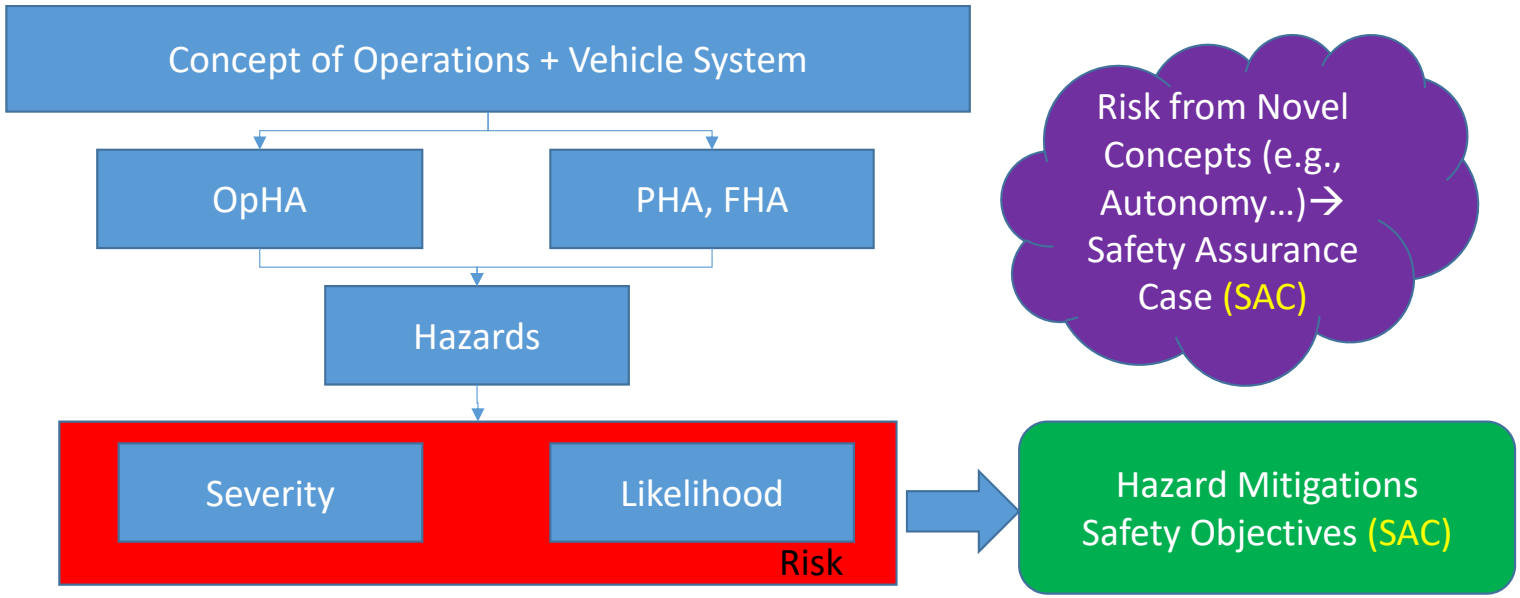
Simplified Representation




Safe Aircraft Operation
Airworthy Aircraft
Technical Airworthiness
Safe Operator
Operational Airworthiness
Certificate of Airworthiness – Individual Aircraft is Fit for Purpose
Maintenance Release - Aircraft is in a Safe Condition
Operator's Certificate
Initial Airworthiness
Ongoing Airworthiness
Organization
Type Certificate – Aircraft Design is Fit for Purpose
Supplementary Type Certificate
Competent and Proficient Personnel
Type Design
Production
Equipment
Instructions for Continued Airworthiness
Maintenance Organization
Suppliers
Personnel
Policies and Procedures
Repair Station Certificate
Production Certificate
Design Standards
Design Organization
Procedures
Personnel
Currency, Medical, Type Endorsements...
Training
Manuals and Procedures
Policy and Culture
Mechanic or Repairman Certificate
Pilot's License
Operations Manual
Maintenance Manual
Flight Manual
Safety Management System

Certification, Hazard Analysis and Risk

Primary aim of aircraft certification (Part 21 etc.) is to provide assurance of safety by: (1) assuring that items perform their *intended (safe) functions* under any foreseeable operating condition, and (2) assuring that *unintended functions* are improbable.



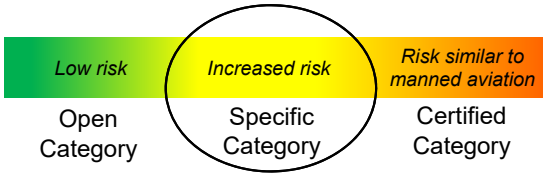
Risk-based Certification

- A certification approach in which in which the imposed requirements are proportional to the operational risk
  - Only considering safety risks

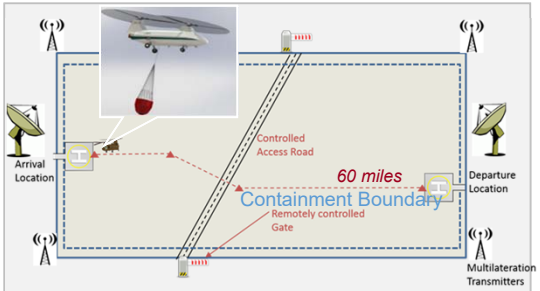
General Characteristics of Airworthiness Standards for Conventional Aircraft	Expected Characteristics of Risk-based Airworthiness Standards for UAS
Originate from experience with system designs, performance, and limitations	Will originate from *a priori* functional and operational hazard analysis for an aircraft and operation
Operation agnostic	Will be operationally driven
Based on aircraft designs from 1950's and 1960's	Will not presuppose a reference aircraft
Focus on protection of people onboard	Will focus on protection of people on the ground and in other aircraft
Both performance-based safety objectives and prescriptive (technology-centric) requirements	Will primarily be performance-based safety objectives

Airworthiness Certification for Midrange UAS

- Examined how differences between UAS and manned aircraft affect hazards and mitigations
- Developed 2 detailed concepts of operation for midrange unmanned rotorcraft
  - precision aerial application
  - cargo delivery in uninhabited corridors
    - ➢ operations *contained* over uninhabited areas
- Derived 85 design and performance requirements from hazard analysis and current regulations
  - 80 based on Part 27 (260 requirements)
  - 5 completely new for novel UAS systems and equipment
- Supports development of airworthiness standards for midsize unmanned rotorcraft



Precision Aerial Application



Cargo Delivery in Uninhabited Corridors

Hayhurst, K. J., Maddalon, J. M., Neogi, N. A., and Verstynen, H. A., Design Requirements for Unmanned Rotorcraft Used in Low-Risk Concepts of Operations, NASA/TM-2016-219345, November 2016

Factors Affecting Airworthiness Considerations

Design Factors	Representative Range	Reason this Factor Matters
Mass	Micro (<4.4 lb), Small (<55 lb), Medium (<7000 lb), Large (>7000 lb)	Harm to people
Operational Speed	Low Speed, Medium Speed, Subsonic, Supersonic	Harm to people
Remote Control Authority	Inner Loop, Outer Loop, Autonomous	Interference with crew safety role
GCS to UA Ratio	0:1, 1:1, 1:n, m:1, m:n	Interference with crew safety role
Operational Factors		
Population Density	None, Sparse, Medium, Dense	Harm to people
Operational Altitude	<500 ft, <18000 ft, <60000 ft, >60000 ft	Degradation of safety margin
Air Traffic Density	None, Light, Moderate, Heavy	Degradation of safety margin
Mission Duration/ Range	Minutes, Hours, Days, Weeks	Degradation of safety margin
Visual Conditions	Day VMC, Night VMC, IMC	Interference with crew safety role
Operational Volume	Contained, Uncontained	Degradation of safety margin
Access to Overflown Area	Controlled, Uncontrolled	Harm to people
Pilot locality	VLOS-RLOS, BVLOS-RLOS, VLOS-BRLOS, BVLOS-BRLOS	Interference with crew safety role

- Operational characteristics should play a significant role in UAS classification
- Operational risk might provide a better basis than weight or kinetic energy for defining UAS classes and categories and additional steps in the UAS integration process

Human Machine Integration

- Task Analysis (Human Factors)
  - Action Oriented Approach: describes observable aspects of operator behavior & structure of the task : focus on the mental processes that underlie observable behavior
- Models of Computation (Computer Science)
  - descriptions of allowable primitive operations & associated unit costs
- Specify tasks to be allocated among agents (roles), then translate to formally verify (derived) safety properties
  - Learning will allow for Dynamic Allocation
- Verification of the system occurs through formal means (semi-automated)
  - Translation of cognitive models to formally verifiable mathematical models
  - Potential for auto-coding to preserve guarantees

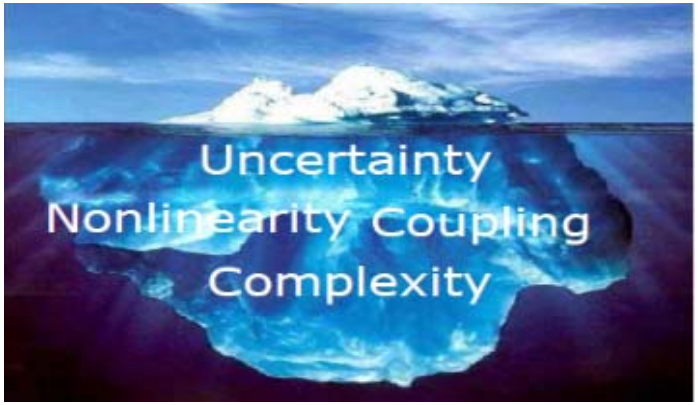
Lessons Learned

- Details about the concept of operations are very important
  - characteristics of the operation and operational environment have a significant impact on hazards and options for mitigation
    - ➢ thorough hazard identification is critical because potential for harm to others is not always obvious
- Airworthiness requirements are needed for new safety-related automation that provides functionality previously provided by the pilot
  - maintain geospatial operating limitations (containment)
  - detect/avoid intruder aircraft, ground-based obstacles, changes in the operational environment
  - systems/equipment supporting the pilot's safety role (e.g., safety-critical command/control links, sensors/displays providing safety-relevant information)
    - ➢ clearly defined safety roles for pilot and crew are essential to determining systems and equipment needed for safety of flight

Technical POC: Dr. Natasha Neogi

Summary & Concluding Remarks

- Validation of Safety-Critical Resilient & Autonomous Systems
  - LOC is an Excellent Focus Problem for V&V Development
    - » Large Hazards Set with Numerous Combinations
    - » Solving it Requires Integrated Systems Technologies
    - » Difficult / Impossible to Fully Replicate the Operational (Hazards) Environment
  - Technical Approach Involved Significant Technology Development
    - » Analysis
      - Nonlinear Uncertain Systems
      - Robustness
    - » Simulation
      - Highly Nonlinear Flight Dynamics & Numerous Hazards Effects
      - Analysis-Guided Monte Carlo Simulation Evaluation
    - » Experimental Testing under Highly Off-Nominal / Hazardous Conditions
      - Ground-Based Testing
      - Flight Testing
    - » Real-Time Monitoring
      - Safety
      - Risk
    - » Coordinated Validation Process with Comprehensive Set of Hazards-Based Test Scenarios
      - Technology Effectiveness & Level of Hazards Coverage
      - Technology Limitations & Unsafe Operational Regions



Summary & Concluding Remarks (3)

V&V is a Socio-Technical Problem

Software verification and validation process outputs must clearly align with certification standards order to enable industrial development of increasingly autonomous aviation systems.

- Process Outputs of V&V tools, methods and techniques need to be unambiguous in their interpretation by non-experts
- How are V&V tools, techniques and methods qualified in order to guarantee correctness?
- What are the appropriate certification standards for IAS (e.g., safety vs. acceptable risk)?
- Are they easily understandable and demonstrable?
- V&V process outputs must be readable and reviewable to a layperson (e.g., regulator)
- Outputs should contribute to the satisfaction of a certification goal
- Commercial aviation systems require some form of airworthiness certification to participate in the NAS
- Are V&V techniques cost effective and useable without expert training?

Regulatory Aspects impact viability of V&V Solutions