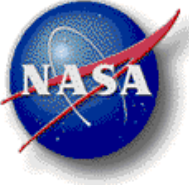




# Assurance Challenges for UAM Platforms and Concepts: A Way Forward

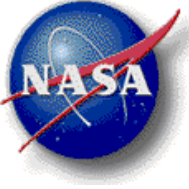
Natasha Neogi  
AIAA SciTech  
Kissimmee, FL  
January 8, 2018



# Outline

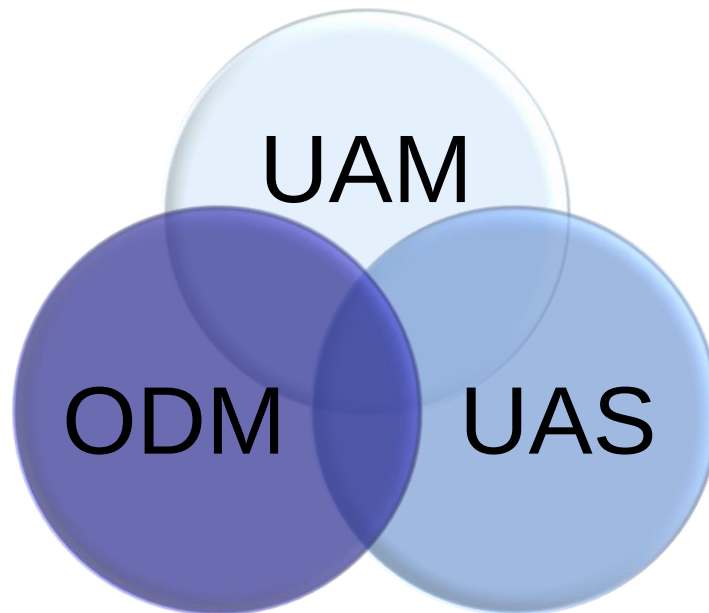
---

- Introduction and Motivation
- Challenges and Barriers
- A Way Forward: Potential Techniques for Establishing Assurance
- Summary Thoughts

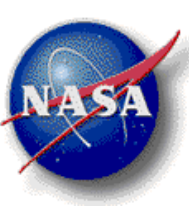


# UAM Operations

---



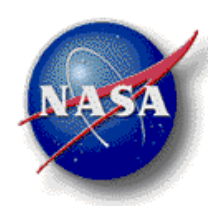
**Operation + Platform → Risk**



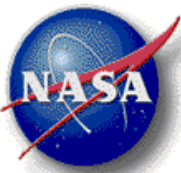
# Assurance Conundrums for UAM

---

- Safety vs. Affordability
  - Competing transportation modes
- Safety vs. Security
  - Communications Links, Physical Vehicles, Landing Platforms etc.
  - Availability
- Infrastructure Access vs. Infrastructure Development
  - Regulation, Standards and Acceptable Means of Compliance
- Public Risk Acceptance
  - Safety of 3<sup>rd</sup> parties not connected to the operation
  - Privacy
  - Liability



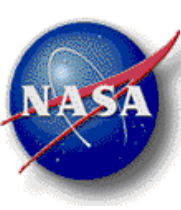
# CHALLENGES AND BARRIERS



# Assurance Challenges to Fielding UAM 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
- Public Acceptance/Trust

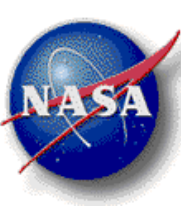




# Assurance Barriers to Fielding IA UAM Systems

---

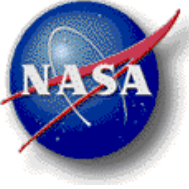
- Lack of approaches, tools and techniques for evaluating safety properties in Increasingly Autonomous (IA) functions
  - Current approaches geared towards obtaining quantitatively predictable outcomes
  - Statistical approaches may not be sufficient
  - Require a confluence of analytic, simulation, test and evaluation techniques
- Lack of scalability of current approaches
  - DO-178C and software complexity
  - Frequency of flights, overflowed population density, fleet size
- Lack of cost effectiveness
  - Barrier to entry for new applicants
  - Change management



# Assurance Barriers to Fielding IA UAM Systems

- 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 qualified infrastructure and enabling technologies to ensure the desired confidence in IA functions for UAM
  - Communications, security, positioning systems, collision avoidance etc.
- Lack of certification standards to ensure desired emergent behavior of the National Airspace System (NAS)
  - Current level of safety
  - 3<sup>rd</sup> parties not concerned with operation

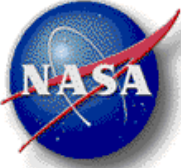




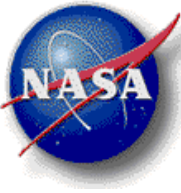
# Areas for Fundamental Research

---

- 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
  - UAM ConOps

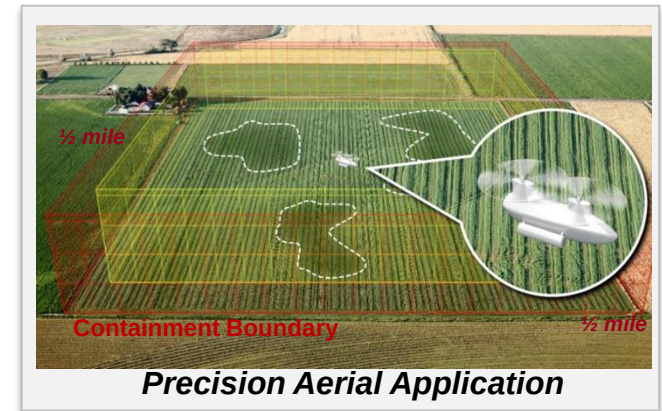


# **A WAY FORWARD: POTENTIAL TECHNIQUES FOR ESTABLISHING ASSURANCE**

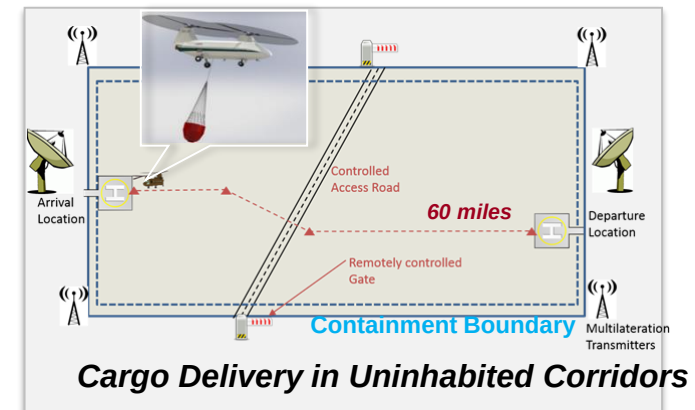


# Risk-Based Certification

- Developed 2 detailed concepts of operation for midrange unmanned rotorcraft
  - precision aerial application
    - 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

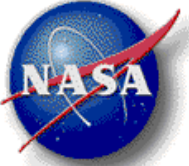


Supported by Dragonfly Pictures, Inc.



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

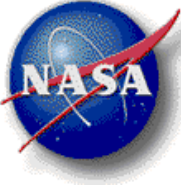
**Supports development of airworthiness standards for midsize unmanned rotorcraft**



# Risk Based Certification: Lessons Learned

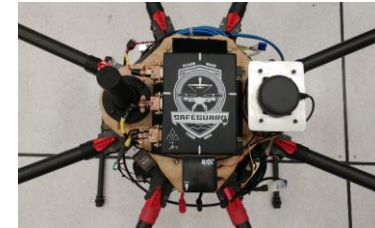
---

- Details about the concept of operations are really 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

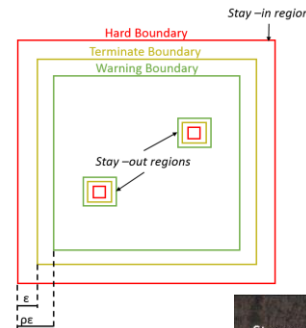


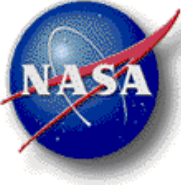
# Safeguard

- 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 databases of geospatial constraints (e.g., Unmanned Traffic Management (UTM))



\* patent-pending



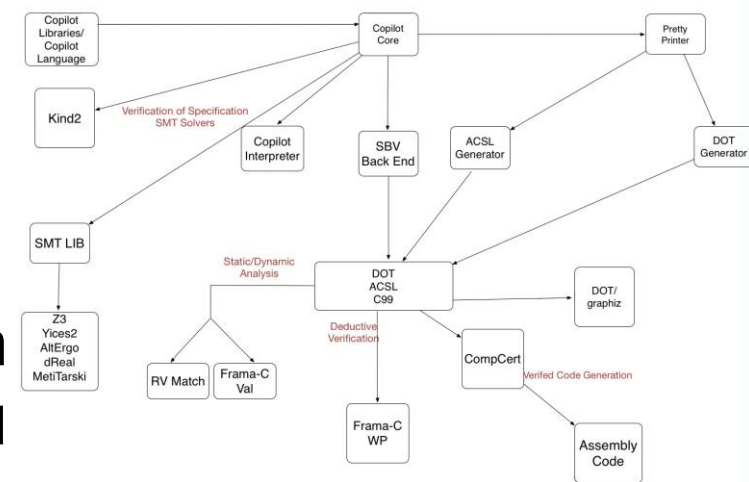


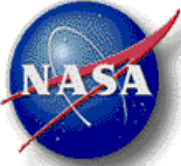
# Runtime Verification

- Runtime verification (RV) is where monitors observe the behavior of a system and detect if it is inconsistent with a given specification
  - Monitored system - system under observation (SUO)
- Specification is written in a decidable logic or appropriate abstract notation
  - Regular languages
  - Linear temporal logic (LTL)
  - Metric temporal logic (MTL)
- When a monitor detects that a property is violated, it may raise an alarm or steer the system into a safe mode of operation
- RV frameworks synthesize monitors from specs

# Copilot: A Run-Time Monitoring DSL

- The work described here is done in the context of our Copilot effort
- 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 system under observation
  - Can miss state changes if not sampled



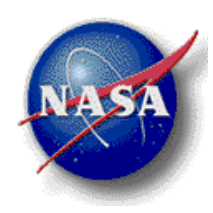


# Formal Methods for V&V of CDR/DAA Algorithms

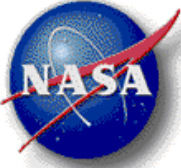
---

- [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.

<https://shemesh.larc.nasa.gov/people/cam/>



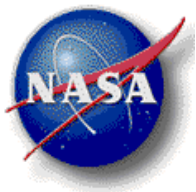
# SUMMARY THOUGHTS



# Thoughts and Opinions

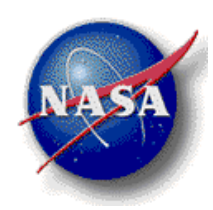
---

- Assurance of IA systems for UAM is a socio-technical problem with legal implications
- UAM will require a sea change in operational models, frequency and scale of aircraft operation
  - Heterogeneous system interactions
- Current V&V methodologies and practices may not be able to assure IA systems to the level required for UAM
  - Non-determinism and adaptive behavior
  - Cost and scalability
- Need new methodologies for assuring systems and operational concepts not traditionally used in civil aviation

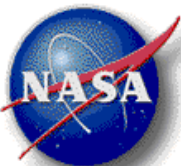


# Questions?

Natasha.a.neogi@nasa.gov



**BACKUP**



# UAS Integration into the NAS: UAM

## UAS Technologies:

T01 - Airport Operations Technologies

T02 - Airworthiness Standards

T03 - Command, Control, Communications (C3)

T04 - Detect & Avoid (DAA)

T05 - Flight & Health Mngmt Systems

T06 - GCS Technologies

T07 - Hazard Avoidance

T08 - Highly Automated Architectures

T09 - Navigation

T10 - Power & Propulsion

T11 - Weather

## ATM Services & Infrastructure:

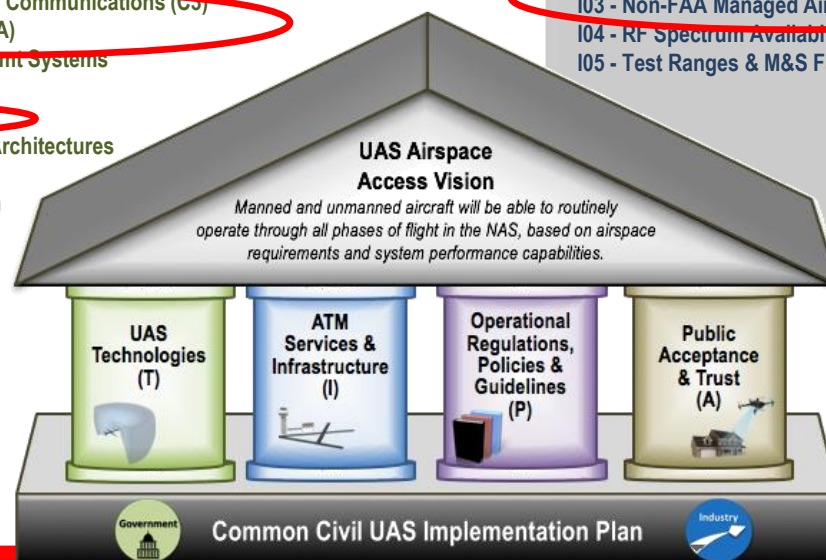
I01 - Airport Infrastructure

I02 - ATM Infrastructure

I03 - Non-FAA Managed Airspace Infrastructure

I04 - RF Spectrum Availability

I05 - Test Ranges & M&S Facilities



## Operational Regulations, Policies & Guidelines:

P01 - ATM Regulations / Policies / Procedures

P02 - Airworthiness Regulations / Policies / Guidelines

P03 - Operating Rules / Regulations / Procedures

P04 - Safety Risk Mngmt & Methods of Compliance

## Public Acceptance & Trust:

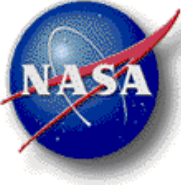
A01 - Cybersecurity Criteria & Methods of Compliance

A02 - Legal & Privacy Rules / Guidelines

A03 - Noise Reductions

A04 - Physical Security Criteria & Methods of Compliance

A05 - Public Safety Confidence



# Challenges

---

- **Research challenges include, but are not limited to development in:**
  - Compositional architectures for learning-enabled systems that guarantee and preserve specified properties
  - Formalisms, abstractions, and domain specific modeling languages for representation of learning-enabled components, systems and their dynamics
  - Scalable methods addressing formal verification of safety and liveness properties of LE-CPS
  - Simulation approaches that drive the learning enabled system to elicit unanticipated behaviors
  - Approaches for maximizing test coverage of LE-CPS
  - Transformations for automated synthesis of assurance monitors.



# Human Machine Teaming

- 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

