NASA Aviation Safety Program
Overview

Richard Barhydt
Deputy Program Director

Safe & Secure Systems & Software Symposium
June 14, 2011
Beavercreek, OH
NASA Aeronautics R&D Strategy

- Foster revolutionary ideas with “Seedling” fund
- More robust technology transfer to industry and other government agencies through innovative fundamental research and further maturation of technologies and concepts in system level research
- Conduct integrated systems research in relevant environments (e.g., flights, full simulations) to realize next set of technological breakthroughs and inspire next generation
NASA Aeronautics Portfolio

**Fundamental Aeronautics Program**
Conduct cutting-edge research that will produce innovative concepts, tools, and technologies to enable revolutionary changes for vehicles that fly in all speed regimes.

**Integrated Systems Research Program**
Conduct research at an integrated system-level on promising concepts and technologies and explore/assess/demonstrate the benefits in a relevant environment.

**Airspace Systems Program**
Directly address the fundamental ATM research needs for NextGen by developing revolutionary concepts, capabilities, and technologies that will enable significant increases in the capacity, efficiency and flexibility of the NAS.

**Aviation Safety Program**
Conduct cutting-edge research that will produce innovative concepts, tools, and technologies to improve the intrinsic safety attributes of current and future aircraft.

**Aeronautics Test Program**
Preserve and promote the testing capabilities of one of the United States' largest, most versatile and comprehensive set of flight and ground-based research facilities.
History of NASA’s Aviation Safety Program

• Original Program began FY98/00
  – Responding to a White House Commission, NASA created a program, complementing FAA and industry activities, to develop and demonstrate technologies that would contribute to the national goal to reduce accident and fatality rates by a factor of five by 2007
  – Intensive NASA-Gov't-Industry team effort to define investment strategy

• FY06/07 Restructure of NASA Aeronautics
  – Focus on “core competencies of aeronautics research”
    • Mostly a bottoms-up portfolio
  – Integration of best out-of-house research ideas (via NRA process)
    • Strong partnerships with Universities
    • Intellectual partnerships (via Space Act Agreements) with industry
  – Program goal: “By 2016, identify and develop tools, methods, and technologies for improving overall aircraft safety of new and legacy vehicles operating in the Next Generation Air Transportation System.”
  – Some Projects have revised their plans since FY07

• FY10 Re-plan of AvSP
  – Top-down refocus; not a total restart
Outstanding Contribution to Aviation Safety

2000 – 2005
Aviation Safety Program I
• System wide safety
• Wx in the cockpit
• Synthetic vision
• Aircraft safety

2006
Reformulation of NASA Aeronautics programs emphasizing fundamental research

2008
CAST – winner of the 2008 Collier Trophy

2010
Streamline/reorganize Aviation Safety Program to strengthen relevance and impact

2011
Start V&V of Flight Critical Systems
Program Goal & Objectives

Goal: Proactively identify, develop, and mature tools, methods and technologies for improving overall aircraft safety of new and legacy vehicles operating in NextGen

Three Objectives

• “Assure system-wide safety”
  – Provide knowledge, concepts and methods to proactively manage increasing complexity in the design and operation of vehicles and the air transportation systems

• “Maintain and improve vehicle safety in key areas”
  – Identify risks and provide knowledge needed to avoid, detect, mitigate, and recover from hazardous flight conditions, and to maintain vehicle airworthiness and health

• “Deal with the presence of atmospheric risks”
  – Investigate sources of risk and provide technology needed to help ensure safe flight in and around atmospheric hazards
Organization

**Aviation Safety Program (AvSP)**
- Program Director: Douglas Rohn
- Deputy Director: Richard Barhydt
- Technical Integration Manager: John Orme
- Program Integration Manager: Brenda Bentley

**System-Wide Safety and Assurance Technologies (SSAT) Project** (ARC hosted)
- Project Manager: Dr. Ashok Srivastava
- Deputy Project Manager: Dr. Jessica Nowinski
- Project Scientist: Dr. Robert Mah

**Vehicle Systems Safety Technologies (VSST) Project** (LaRC hosted)
- Project Manager: Paul Krasa
- Deputy Project Manager: Sharon Graves
- Project Scientist: Richard Ross
- Project Scientist: Dr. Steve Young
- Project Scientist: Dr. Christine Belcastro

**Atmospheric Environment Safety Technologies (AEST) Project** (GRC hosted)
- Project Manager: Dr. Renato Colantonio

“Assure system-wide safety”
“Maintain and improve vehicle safety in key areas”
“Deal with the presence of atmospheric risks”
Technical Challenges

• Each project has a succinct, lofty, and worthy objective
  – Defined at a fairly high level because safety is a broad domain

• Research plans have been built around Technical Challenges
  – Essentially the “tall poles” within that objective
  – Enduring challenges to aviation, but will be updated as new info is available

• They define NASA Aviation Safety Program success
  – Each is captured in a:
    • Description with goal, metric, date, domain, and benefit; and a
    • Roadmap/timeline with milestones
  – Define our research’s impact on the aviation community
Technical Challenges

- **System-Wide Safety and Assurance Technologies Project**
  - Assurance of Flight Critical Systems
  - Discovery of Safety Issues
  - Automation Design Tools
  - Prognostic Algorithm Design

- **Vehicle Systems Safety Technologies Project**
  - Vehicle Health Assurance
  - Crew-System Interactions and Decisions
  - Loss of Control Prevention, Mitigation, and Recovery

- **Atmospheric Environment Safety Technologies Project**
  - Engine Icing
  - Airframe Icing
  - Atmospheric Hazard Sensing & Mitigation
Partnerships and Technology Transfer

• We put high value on partnerships – *to help get research tasks done*…
  – Expand the program’s scope
  – Strengthen existing capabilities
  – Accelerate the development of new capabilities
• …and to *accomplish technology transfer*

• Various organizations
  – >100 NASA Research Announcement (NRA) awards (cooperative agreements & contracts) to date, ~80 currently active
  – 26 Space Act Agreements; 12 Inter Agency Agreements; 5 International Agreements
    • Several more SAAs and IAs in the works

• Involvement with committees
  – Aviation committee membership
  – AvSP-led Working Groups
  – Community-led Teams

• Rapid dissemination of results
  – Collaboration
  – DASH link, open source & open platform

• Publications and formal research output – journals, conferences, patents
   - Development of **safe, rapid, and cost effective NextGen Systems** using a unified safety assurance process for ground based and airborne systems.

2. Automated Discovery of Precursors to Safety Incidents (FY19):
   - **Automated discovery** of previously unknown **precursors** to aviation safety incidents in **massive** (>10 TB) heterogeneous data sets.
3. Automation Design Tools (FY20):
• Increase safety of human – automation interaction by incorporating human performance considerations throughout the design lifecycle in NextGen technologies.

• Development of verifiable prognostic algorithms to help remove obstacles to certification.

Flight Tests of Prognostic Algorithms
VVFCS Sub-Project Research Area Leads

**SSAT**
PM – Ashok Srivastava (Ames)
DPM – Jessica Nowinski (Ames)
PS – Robert Mah (Ames)

**VVFCS**
Verification & Validation of Flight Critical Systems
Co-leads: E. Cooper, P. Miner (LaRC)
Technical Integration Mgr: G. Brat (ARC)

**VVFCS Sub-Project Research Area Leads**

**ABSA**
Argument-Based Safety Assurance
C. M. Holloway (LaRC)

**SIS**
Software Intensive Systems
G. Brat (ARC)

**DS**
Distributed Systems
P. Miner (LaRC)

**AA**
Authority and Autonomy
M. Shafto (ARC)
Verification and Validation for Flight Critical Systems Objectives:

- Develop methods to **reduce cost and increase safety** through improved safety assurance and dependability.

- Provide **advanced analytical, architectural, and testing capabilities** to enable sound assurance of safety-critical properties for distributed systems-of-systems.

- Improve the ability to **design for safety**, and constrain the burdens of dealing with safety in new and more complex systems, i.e., the cost of flight critical software.

- Develop methods that ensure flight-critical systems’ **assignment of authority and autonomy are comprehensive, lack conflict and ambiguity**, and correspond to agents’ capabilities and accountability.
Argument-Based Safety Assurance

**Description:**
Consistent and comprehensive argument-based safety assessment and assurance methods
- that cover the system life cycle
- and work for all types of aviation systems and services (ATM and airborne)

Improved methods, tools, and processes for requirements
- throughout the system life cycle
- such that safety requirements can be easily "seen"
- improving change impact assessment

Improved methods, tools, and processes for safety-related evidence
- sources and types of evidence needed to support safety
- criteria and methods for analyzable arguments about safety

**Major Activities:**
- Determine feasibility of argument-based assurance
- Understand safety requirements
- Determine needed evidence
- Investigate arguments
- Apply argument-based safety assurance
## Argument-Based Safety Assurance NRAs

<table>
<thead>
<tr>
<th>Title</th>
<th>Org</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assuring Safety using System Theoretic Concepts (NNL10AA13C)</td>
<td>MIT</td>
<td>Application of System Theoretic Process Analysis (STPA) to hazard analysis and safety assurance. Early case study using the NextGen application In-Trail Procedures in Oceanic Airspace (ATSA-ITP), which is defined in the document RTCA DO-312 Safety, Performance and Interoperability Requirements Document for the In-Trail Procedure in Oceanic Airspace (ATSA-ITP) Application, and the Honeywell implementation of this application, called Traffic Computer – Electronic Flight Bag (TC-EFB)</td>
</tr>
<tr>
<td>A Safety Case Workbench (NNL10AA08C)</td>
<td>KESTREL</td>
<td>Develop a flexible and adaptable prototype tool for planning, capturing, analyzing and maintaining safety cases via an Eclipse-based user interface that will support safety case definition in Goal Structure Notation or text-based input.</td>
</tr>
<tr>
<td>Automating the Generation of Heterogeneous Aviation Safety Cases (NNL10DE83C)</td>
<td>SGT</td>
<td>Extend and adapt the AutoCert tool to support the automated creation of evidence-based arguments (AutoCert is a code verification tool that automatically analyzes software source code for compliance to mathematically specified correctness and safety requirements).</td>
</tr>
</tbody>
</table>
Authority and Autonomy

Description:
Develop tools to assess whether advanced operational constructs properly assign authority and autonomy in a safe and coordinated manner, and that the authority and autonomy of flight-critical systems are
- clear,
- deadlock- and conflict-free,
- comprehensive, and,
- consistent with agreed-upon roles and responsibilities

Major Activities:
• Safety analysis of existing organizational models for ATS
  - advance methods to analyze organization-oriented models of ATS elements
  - explore the potential for formal methods and simulation techniques to safety analysis
• Define formal representation of complex organizations
• Develop methods for V&V of authority and autonomy constructs involving human-automation interaction to identify predictable problems in A&A assignment
• Augment / enhance tools to assess the resilience of authority and autonomy properties within complex organizations involving human and automated systems such as NextGen
• Develop comprehensive toolkits for the formal analysis of organizations
<table>
<thead>
<tr>
<th>Title</th>
<th>Org</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextGenAA: Integrated model checking and simulation of NextGen</td>
<td>UNIVERSITY OF VIRGINIA</td>
<td>Integrated suite of simulation, formal verification, and trace analysis tools that use an agent modeling language description for examining Authority and Autonomy safety issues. Create openly available and re usable models and verification approaches applicable to assessing A&amp;A safety issues beyond scenarios tested.</td>
</tr>
<tr>
<td>authority and autonomy (NNA10DE79C)</td>
<td>PI: Ellen Bass</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UIUC, GA Tech, SRI</td>
<td></td>
</tr>
</tbody>
</table>
Distributed Systems

Description:
Provide advanced analytical, architectural, and testing capabilities to enable sound assurance of safety-critical properties for distributed systems of systems

• Guidelines for multiple levels of distribution
  – Fault-tolerant mechanisms
  – Airspace concepts of operation: Airborne/Space-based/Ground-based
  – Human/Automation

• Develop methods for ensuring robust system performance at all levels of distribution:
  – Distributed across multiple architecture
  – Distributed across multiple air and ground elements
  – Interactions between components as intended
  – Robust to faults, failures and degradations

Major Activities:
• Develop validated models of failures, disturbances, & degradations

• Verify properties of distributed algorithms (e.g. for diagnosis, resource management, aircraft separation, etc.) using various communication topologies and technologies, in presence of disruptions identified in (1)
  – Validate using research test bench

• Develop modeling approaches for new system decompositions and functional integration enabled by technological advances
  – Models of coupling and dependencies
  – Non-interference between functions of different criticalities

• Transition models into practical engineering realizations
## Distributed Systems NRAs

<table>
<thead>
<tr>
<th>Title</th>
<th>Org</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation and Verification of Safety-Critical Integrated Distributed Systems (NNL10AB32T)</td>
<td>HONEYWELL PI: Kevin Driscoll SRI, WW Technology</td>
<td>Analysis tools for distributed systems and reusable, validated models of fault-tolerant frameworks such as TTEthernet. Approaches and models will be openly available and reusable and include publicly available artifacts illustrating difficult aviation V&amp;V problems suitable for demonstrating and validating novel V&amp;V techniques.</td>
</tr>
<tr>
<td>Hierarchical Component-Based Framework for the Formal Verification and Validation of Complex Aerospace Software Systems (NNX07AD37A)</td>
<td>Northeastern University PI: P. Manolios Georgia Tech, NIA</td>
<td>Develop a framework that ensures the individual components that comprise avionic systems are connected integrated, and assembled in a manner that satisfies global requirements. Provides an approach to verify systems that are too complex to verify monolithically.</td>
</tr>
</tbody>
</table>
Software-Intensive Systems

Description:
New V&V techniques that can significantly reduce cost and increase software assurance and dependability
• Improve analytical capabilities for building dependable software that makes significant use of numerical calculation.
• New capabilities that support reusable artifacts and publicly available libraries of definitions and theorems for invocation during formal analysis.
• Methods to increase the precision and the coverage of testing while decreasing its cost.
• Methods to enable use of formal methods in argument-based safety assurance and in the context of model-based development methodologies widely adopted in industry.

Major Activities:
• Static analysis methods for detecting anomalous behavior
• Composable verification for re-use and scalability
• Automating test artifact (test cases and oracles) generation using symbolic code execution
• Formal methods and model-based development
  – Certifiable code-generation
## Software-Intensive Systems NRAs

<table>
<thead>
<tr>
<th>Title</th>
<th>Org</th>
<th>Description / Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compositional Verification for Flight Critical Systems (NNA10DE60C)</td>
<td>CARNEGIE MELLON UNIVERSITY</td>
<td>Develop scalable algorithms for exhaustive verification of safety properties for NextGen flight critical systems</td>
</tr>
<tr>
<td></td>
<td>PI: Vishwanath Raman SGT</td>
<td></td>
</tr>
<tr>
<td>An Evidential Tool Bus for Flight Critical Software Systems (NNA10DE73C)</td>
<td>SRI</td>
<td>Integrated tool suite of individual modeling and analysis component tools that automate the design, implementation, validation, verification, and certification of software-intensive, flight-critical systems; that is, to build an automated tool suite that combines many different formal verification and validation tools under the Evidential Tool Bus in order to develop assurance cases. Validated using representative case studies and will automatically generate human-readable assurance cases that can be used to certify the safety of software.</td>
</tr>
<tr>
<td></td>
<td>PI: Natarajan Shankar Honeywell</td>
<td></td>
</tr>
</tbody>
</table>
Thank you.
Summary

• VVFCS is largest sub-project of the System-wide Safety Assessment Technologies Project
  – In-house research and NRA awards

• Four Research Areas:
  – Argument-based Safety Assurance
  – Authority & Autonomy
  – Distributed Systems
  – Software-Intensive Systems

• Coordination with other NASA projects / programs

• Coordination with other Agencies
  – JPDO
  – FAA
  – AFRL
Back-Up
Technical Challenge Summaries
Summary of SSAT Project Technical Challenges (1 of 2)

   Safe, Rapid Deployment of NextGen Systems
   - **Goal**: Unified safety assurance processes for ground based and airborne systems that significantly reduces time and cost of testing NextGen systems.
   - **Benefits**:
     - Rapid but safe incorporation of technological advances in avionics, software, automation, and aircraft and airspace concepts of operation and operating procedures.
     - Availability of safety assurance methods for confident and reliable certification, enabling manufacturers and users to exploit latest technological advances and operational concepts.

2. Discovery of Safety Issues (FY19):
   Automated discovery of previously unknown precursors to aviation safety incidents
   - **Goal**: A first-of-a-kind demonstration of the automated discovery of precursors to aviation safety incidents through automated analysis of massive (>10 TB) heterogeneous data sets.
   - **Benefits**:
     - Understanding of the impact of degradations in flight crew operational state or performance on aircraft operations
     - Identifying fleet-wide anomalies due to mechanical and other related issues that can impact safety, maintenance schedules, and operating cost
• **3. Automation Design Tools (FY20):**
  Increasing Safety of Human – Automation Interaction by Incorporating Human Performance
  
  • **Goal:** Develop revolutionary and first-of-a-kind methods and tools that incorporate the limitations of human performance throughout the design lifecycle of human-automation systems to increase safety and reduce validation costs in NextGen.
  
  • **Benefits:**
    • Methods and tools to help designers, trainers and operators predict human performance, and identify, evaluate and resolve Human – Automation interaction issues.
    • Tools for identification of novel system failures.
    • Computational Human Model-Based safety design tools.

• **4. Prognostic Algorithm Design for Safety Assurance (FY25):**
  Development of verifiable prognostic algorithms
  
  • **Goal:** Remove obstacles to the certification of prognostic algorithms. Currently, the aerospace community has no known transition path for non-deterministic algorithms and massive amounts of simulation and testing for deterministic algorithms.
  
  • **Benefits:**
    • New class of verifiable prognostic algorithms and methods
    • Lowered barrier to deployment of prognostics
Summary of VSST Technical Challenges

- **Vehicle Health Assurance (VHA) (FY25):**
  Assure vehicle health in all conditions and throughout its lifetime
  - **Goal:** Demonstrate a 60% reduction in aircraft-related risks for subsystems on current and future aircraft under Part 91, 121, and 135 operations
  - **Benefits:** Increased health state awareness, reduced inappropriate crew response, aids for improved designs; Awareness, integration, and decision-making benefits for automated and human decision-making
  - **Domain of Applicability:** Current and next generation aircraft (N, N+1) that will be piloted in existing and NextGen environments under FAR Parts 91, 121, and 135 operations

- **Effective Crew-System Interactions and Decisions in All Conditions (CSI) (FY21):**
  Simultaneously increase the crew’s ability to avoid, detect, and recover from unexpected events, while also providing countermeasures to pilot error
  - **Goal:** Demonstrate 75% improvement in crew decision-making and system interactions in off-nominal conditions (against a baseline set of off-nominal conditions and scenarios established in FY11)
  - **Benefits:** Eliminate causal factors by improving crew awareness of vehicle health, automation mode, energy state, weather, traffic, path, and airspace system state; Remove dependency on visibility conditions for safe terminal area operations; Assure appropriate crew engagement in future highly automated flight decks; Proactive mitigation of risks associated with new operating concepts – such as NextGen’s 4D TBO
  - **Domain of Applicability:** Piloted aircraft (N, N+1) operating in current and NextGen NAS. Initial validation domain: terminal area ops and subsonic fixed-wing aircraft. Domain and consideration of additional causal factors expanded over time to achieve the ten-year goal.

- **Aircraft Loss of Control Prevention, Mitigation, and Recovery (LOC) (FY25):**
  Simultaneously improve vehicle avoidance, detection, mitigation, and recovery capabilities relative to adverse onboard conditions, external hazards and disturbances, and vehicle upsets
  - **Goal:** Develop, integrate, & validate technologies to eliminate 85% of loss-of-control risk in current and NextGen operations for current/future aircraft
  - **Benefits:** Flight safety assurance under LOC precursor conditions through onboard vehicle health management, flight safety risk assessment and management, mitigation of hazardous conditions, upset prevention and recovery, and improved situational awareness and synergistic response by automated systems and crew
  - **Domain of Applicability:** Piloted and autonomous aircraft (N, N+1, N+2) operating in current and NextGen NAS under Part 91, 121, and 135 or comparable operations
Summary of AEST Project Technical Challenge

**Engine Icing: Characterization and Simulation Capability (FY25):** Develop knowledge bases, analysis methods, and simulation tools needed to address the problem of engine icing; in particular, ice-crystal icing

**Goal:** Eliminate turbofan engine interruptions, failures, and damage due to flight in high ice-crystal content clouds

**Benefit:** Verified basis for engine icing certification requirements; enable new engine icing protection systems and methods

**Benefit Domain:** All turbofan/turbojet powered aircraft; engine manufacturers, aviation system regulators, and pilots and operators

**Airframe Icing Simulation and Engineering Tool Capability (FY25):** Develop and demonstrate 3-D capability to simulate and model airframe ice accretion and related aerodynamic performance degradation for current and future aircraft configurations in an expanded icing environment that includes freezing drizzle/rain

**Goal:** Achieve acceptance of simulation tools for design and certification of swept wing configurations over an expanded range of icing conditions

**Benefit:** Enable aircraft manufacturers to perform reliable icing assessments and build in effective icing mitigation approaches for current and future aircraft; development of technology that enables safe flight operations in an super-cooled large droplet environment

**Benefit Domain:** Aircraft and aircraft sub-system manufacturers and aviation system regulators

**Atmospheric Hazard Sensing & Mitigation Technology Development (FY25):** Improve and expand remote sensing and mitigation of hazardous atmospheric environments and phenomena

**Goal:** Mature technologies for sensing and measurement of icing, turbulence, and wake vortex hazards for real-time information to the pilot and operators in the NAS and to address low visibility conditions for safer runway operations; develop technologies for a lightning immune composite aircraft

**Benefit:** Greater ability for aircraft to avoid hazards; hazard information available for sharing with other aircraft and ground-based systems; reduced vulnerability to lightning and other hazards

**Benefit Domain:** All aircraft flying in the NAS; pilots, operators, and controllers