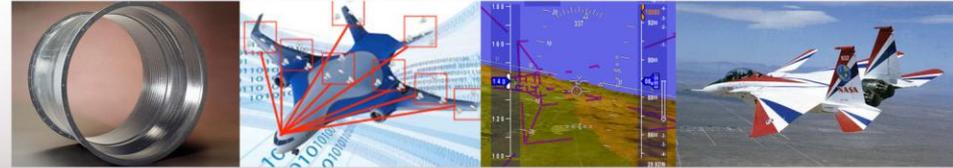




# NASA Research Planning in V&V for Flight Critical Systems

**Douglas A. Rohn**  
Director, Aviation Safety Program  
Presentation to NAC Aeronautics Committee, April 23, 2010



# Outline

---



- Challenge
- Research Areas
- Next Steps



# CHALLENGE

# Goals & Objectives

---



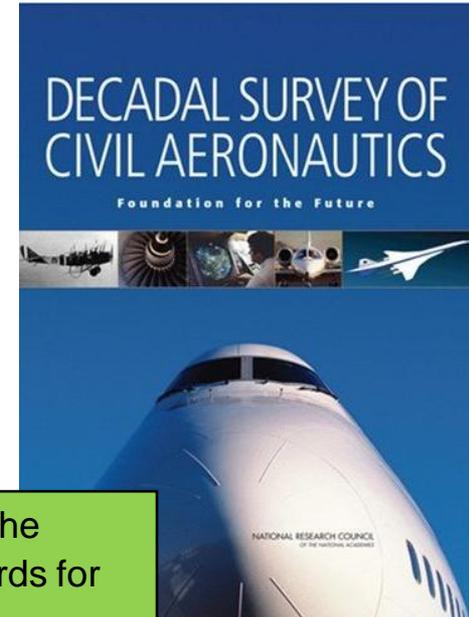
- PROGRAM GOAL
  - By 2016, identify and develop tools, methods, and technologies for improving overall aircraft safety of new and legacy vehicles operating in the Next Generation Air Transportation System.
- V&V OBJECTIVE (working)
  - Research and development of transformative safety V&V methods needed to rigorously assure the safety of Next Generation Air Transportation System (NextGen) developments in a time- and cost-effective manner.

# V&V: Broad Challenge



"Developers do not have effective ways to model and visualize software complexity, including the possible range of interactions, especially unexpected and anomalous behaviors that can occur among software and hardware components.

Developers also do not have time- or cost-effective ways to test, validate, and certify that software-based systems will perform reliability, securely, and safely as intended, particularly under attack or in partial failure."



Fundamental research is needed to create the foundations for practical certification standards for new technologies

- methods and models are needed for assessing the safety and reliability of complex, large-scale, human-interactive, nondeterministic software intensive systems



**JPDO Identified Critical Gap in V&V Methods**

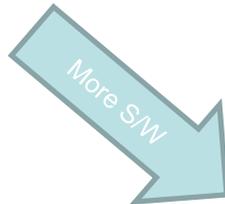
# Cost (and time) Barrier

- With current methods, V&V can cost more than all other design and implementation costs combined, in some cases, effectively prohibiting novel operations and technologies.

System	Lines of Code
Mars Reconnaissance Orbiter	545K
Orion Primary Flight Sys.	1.2M
F-22 Raptor	1.7M
Seawolf Submarine Combat System AN/BSY-2	3.6M
Boeing 777	4M
Boeing 787	6.5M
F-35 Joint Strike Fighter	5.7M
Typical GM car in 2010	100M

## Size Comparisons of Embedded Software

NASA Study  
Flight Software Complexity, 4/23/2009



**Software example. Also need to consider human performance, concepts of operation, and new technologies!**

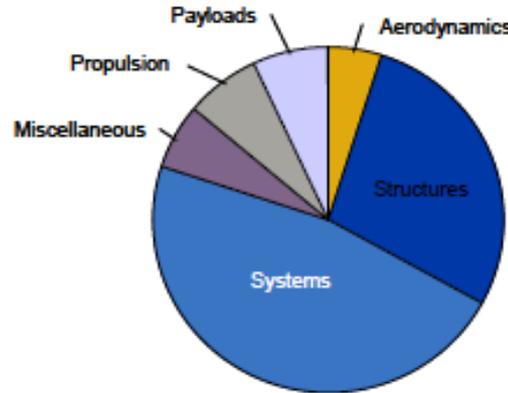
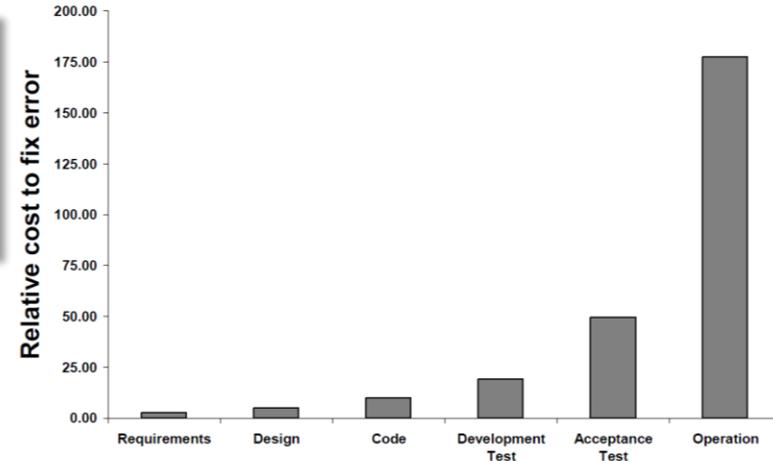


Fig. 1 - Typical Transport Aircraft Development Cost Distribution - Current Generation

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



Phase in which error was detected and corrected

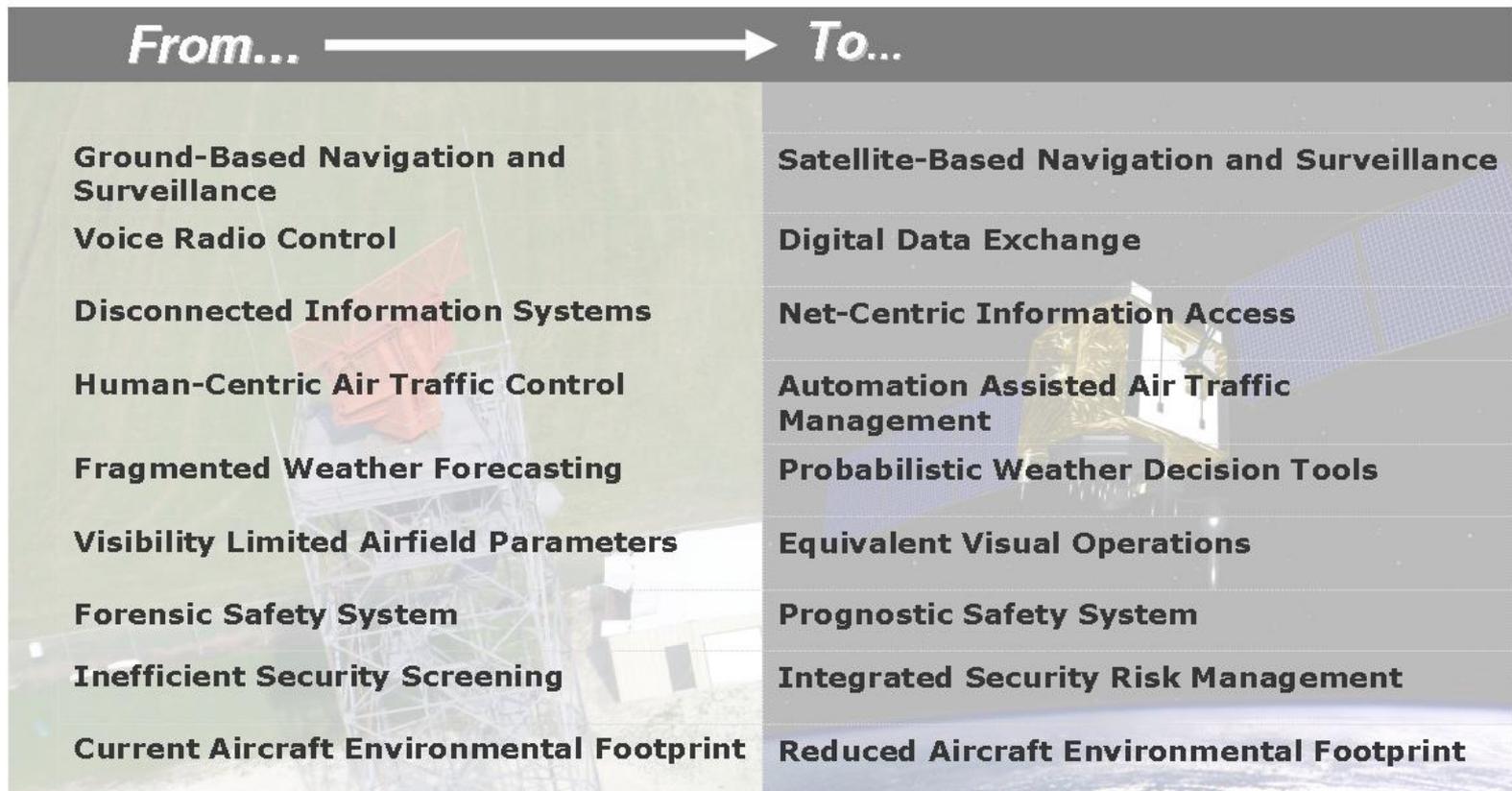
Boehm, B. 1981 *Software Engineering Economics*, as cited in DAA, 2008



# NextGen Challenge



- NextGen will require the implementation of complex software systems coupled with advanced hardware and communications capabilities
  - The validation and verification (V&V) of these complex technological developments is an integral part of the system safety assurance process.





# A NextGen Example

---

- 4-D Trajectory Negotiation
  - Distributed air-ground system
  - With lots of automation
  - Elements of Authority and Autonomy not fully defined

Requires new safety standards, operational procedures and regulation...

and new V&V methods and algorithms to support its development, risk assessment and eventually certification/operational procedure decisions



---

# RESEARCH AREAS

# NASA AvSP Steps to Date

---



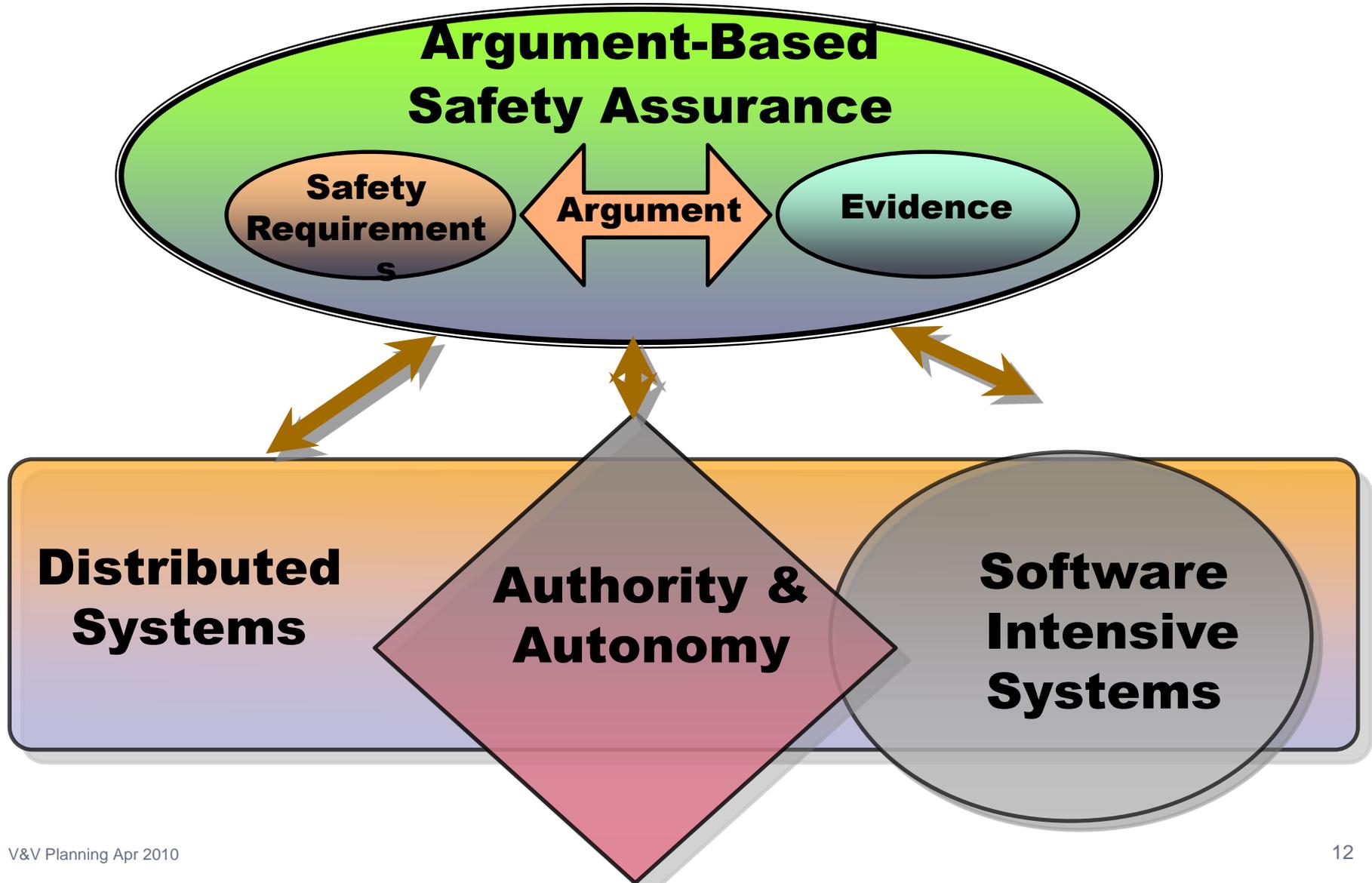
- Engaged community to formulate and validate initial research requirements for reducing the cost, time and difficulty of doing V&V for system safety
  - Gathered together existing activities within Program
  - RFI (July 2009)
  - Inter-Agency Working Group, JPDO interactions
- Presented material to NRC aviation safety Review Panel
- Coordinated planning with other government agencies
  - Interagency Coordination Meeting (Sept 2009)
- Presented assessment of critical research areas at Aviation Safety Technical Conference (Nov 2009)
  - Proposed near-term research activities
  - Proposed long-term research
- NRA Solicitation NNH09ZEA001N-VVFCSS1 released
  - Proposals received Dec 2009
  - Selections made and in negotiation
- Initiating Assessment Environment with test bench build-up

# Study of V&VFCS Research Needs



- Scope
  - Explicit study of cross-cutting issues in V&V
  - Focus on the ‘safety’ aspects
  - Aware of broader “systems” issues
    - e.g., interaction of new flight control systems with the entire aircraft data bus and sensor suite
- Objectives
  - Demonstrate advanced methods to answer relevant questions from aviation community
  - Reduce barriers to innovation associated with safety V&V
  - Develop V&V methods for safety throughout the entire life cycle
- Key themes in research noted
  - Make V & V Cost- and Time-Effective
  - Support the Entire Product Lifecycle
  - Consider Disturbances & Degradations
  - Humans and Software Are Central
- Four Challenge Areas identified with critical research needs

# Challenge Areas



# Argument-based Safety Assurance



- **PROBLEM:** NextGen changes the conventional boundaries and layers -- and, consequently, safety assurance
  - Significant differences exist in how the “case for safety” is made for a new/modified system
    - Different organizations responsible for different types of systems
    - Different standards, vocabulary, guidance on acceptability, and degrees of design freedom for automated systems
    - Different certification and approval processes that are not formally linked
  - Forms a barrier to the accuracy & efficiency of safety assurance for new, complex concepts.
- **NEED:** A more uniform safety approach will capture safety information from new and existing tools to satisfy end-to-end safety requirements in complex systems.
- **RESEARCH:** A framework that explicitly captures:
  - safety goals/claims/objectives, especially for new functions
  - evidence that goals have been met
  - arguments linking evidence to goals (assumptions, justifications, and other context)
  - This framework should support design and integration
    - Used to trace conflicts or gaps in assumptions and evidence of combined functioning during component integration
  - This framework should support the entire lifecycle
    - Endures beyond first design/implementation, to support modification and integration

# Authority and Autonomy

---



- **PROBLEM:** Future aircraft systems and operational concepts will be designed with a larger number of interacting human and automated systems.
- **NEED:** Improved V&V tools are needed to ensure that new roles and interactions don't introduce conflicts, gaps, or ambiguity in the assignment of safety responsibility.
  - Authority requires both accountability and capability
    - Need authority aligned with autonomous capabilities
    - Need to avoid competing authorities
    - Need to avoid gaps in authority, maintain clearly who/what is in charge
- **RESEARCH:** Methods for early-on assessment of 'big issues':
  - Is authority assigned properly?
  - Is authority assigned with correct assumptions regarding capabilities?
  - Are there conflicts or gaps?

# Flight-critical Distributed Systems



- **PROBLEM:** Aviation system is a distributed network of distributed systems
  - NextGen will have functions distributed as well as integrated across a system of systems. This can result in unintended consequences under normal or degraded operations.
  - Multiple levels of distribution exist
    - Multi-core processors (system on a chip)
    - Fault-tolerant mechanisms
    - Airspace concepts of operation: Airborne/Space-based/Ground-based
    - Human/Automation
- **NEED:** Advanced analytical, architectural, and testing capabilities are needed to enable the assurance of reliable and safe functionality in distributed systems.
- **RESEARCH:** 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

# Software-Intensive Systems

---



- **PROBLEM:** The trend for future capabilities relies on increasingly complex, software-intensive systems.
  - NextGen plans increase reliance on software-intensive systems in both ATC and aircraft systems
  - Software will interact with other software, systems, devices, sensors, and with people
- **NEED:** Research is needed on efficient and effective methods to significantly reduce software V&V cost while increasing safety
- **RESEARCH:** Methods for examining software-intensive systems
  - Appropriate extension of formal methods
  - Increasing capabilities for numerical calculation
  - Generalized capabilities for software testing throughout coding

# Initial Test Cases

---



DEFINITION: Realistic platform or environment to develop & test V&V tools; the platform or application itself benefits from V&V assessment

- Integrated Alerting and Notification concepts implemented in Integrated, Modular Avionics (IMA) Architecture
  - Dryden Flight Research Center will provide h/w & s/w in the loop test bench at the highest level of fidelity
- Investigating the use of Airspace applications
  - Automated conflict detection & resolution
  - Separation Assurance
  - Efficient Flows into Congested Airspace (EFICA)
- Others

# Proposed Research Deliverables

---

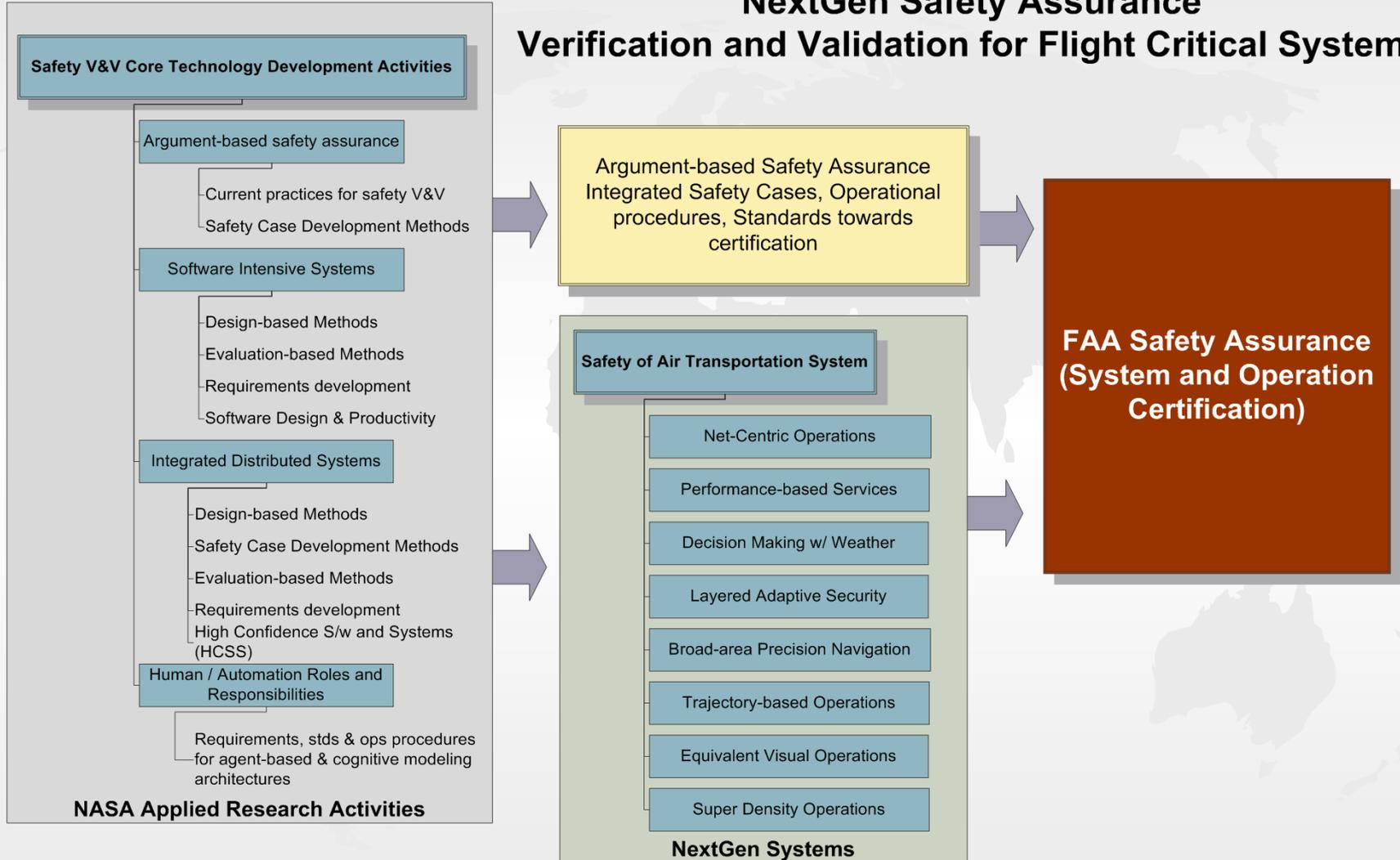


- Safety Assurance Framework for NextGen systems
  - Involvement in aviation safety standards & procedures
    - RTCA, etc.
    - FAA internal
    - Industry best practices
  - Standardized certification methods/operating procedures
- Aviation safety design guidelines
  - Re-usable tools & models
  - “Cookbook of recipes” for designing software and distributable systems
    - Open source, generic platforms
  - Tools for analyzing safety issues in human-system organizations
- Methods/models for insertion early and throughout lifecycle
  - Formal methods (Theorem proving methods, model checking, certifiable code synthesis)
  - Static and dynamic analysis

# Research Products & Application



## NextGen Safety Assurance Verification and Validation for Flight Critical Systems





---

# NEXT STEPS

# Next Steps

---



- Detailed planning of milestones, deliverables, resources (ongoing)
- Interagency review of research plans with government partners
  - Informal feedback
  - NASA/FAA/JPDO VVFCs Transition 1-day workshop
- Solicit wider aviation safety community feedback through a focused workshop
  - VVFCs Meeting of Experts Workshop (NRC-led)
- Conduct applicable NASA procedures and reviews for project formulation



**THANK YOU**