Safety Related Considerations in Autonomy

Dr. Guillaume Brat
Intelligent Systems Division
NASA Ames Research Center

NASA ARMD
Airspace Operations and Safety Program

Presented at the OPTICS Workshop: **ROM HAZARD MANAGEMENT TO OPERATIONAL RESILIENCE**
April 28-29, 2015

Support for NASA ARMD Strategic Goals

Safe, Efficient Growth in Global Operations

- Enable full NextGen and develop technologies to substantially reduce aircraft safety risks

Innovation in Commercial Supersonic Aircraft

- Achieve a low-boom standard

Ultra-Efficient Commercial Vehicles

- Pioneer technologies for big leaps in efficiency and environmental performance

Transition to Low-Carbon Propulsion

- Characterize drop-in alternative fuels and pioneer low-carbon propulsion technology

Real-Time System-Wide Safety Assurance

- Develop an integrated prototype of a real-time safety monitoring and assurance system

Assured Autonomy for Aviation Transformation

- Develop high impact aviation autonomy applications

NASA ARMD Program re-structuration

Aviation Safety Program

Conduct cutting-edge research to produce innovative concepts, tools, and technologies to improve the intrinsic safety attributes of current and future aircraft and air traffic management systems

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

Airspace Operations and Safety Program

The goal of AOSP-developed NextGen methods and means is to provide advanced levels of automated support to air navigation service providers and aircraft operators for reduced air travel times and air travel-related delays, and to insure greater safety in all weather conditions.

AOSP Mapping to NASA ARMD Strategic Goals

Safe, Efficient Growth in Global Operations
- **Enable full NextGen and develop technologies to substantially reduce aircraft safety risks**

Innovation in Commercial Supersonic Aircraft
- Achieve a low-boom standard

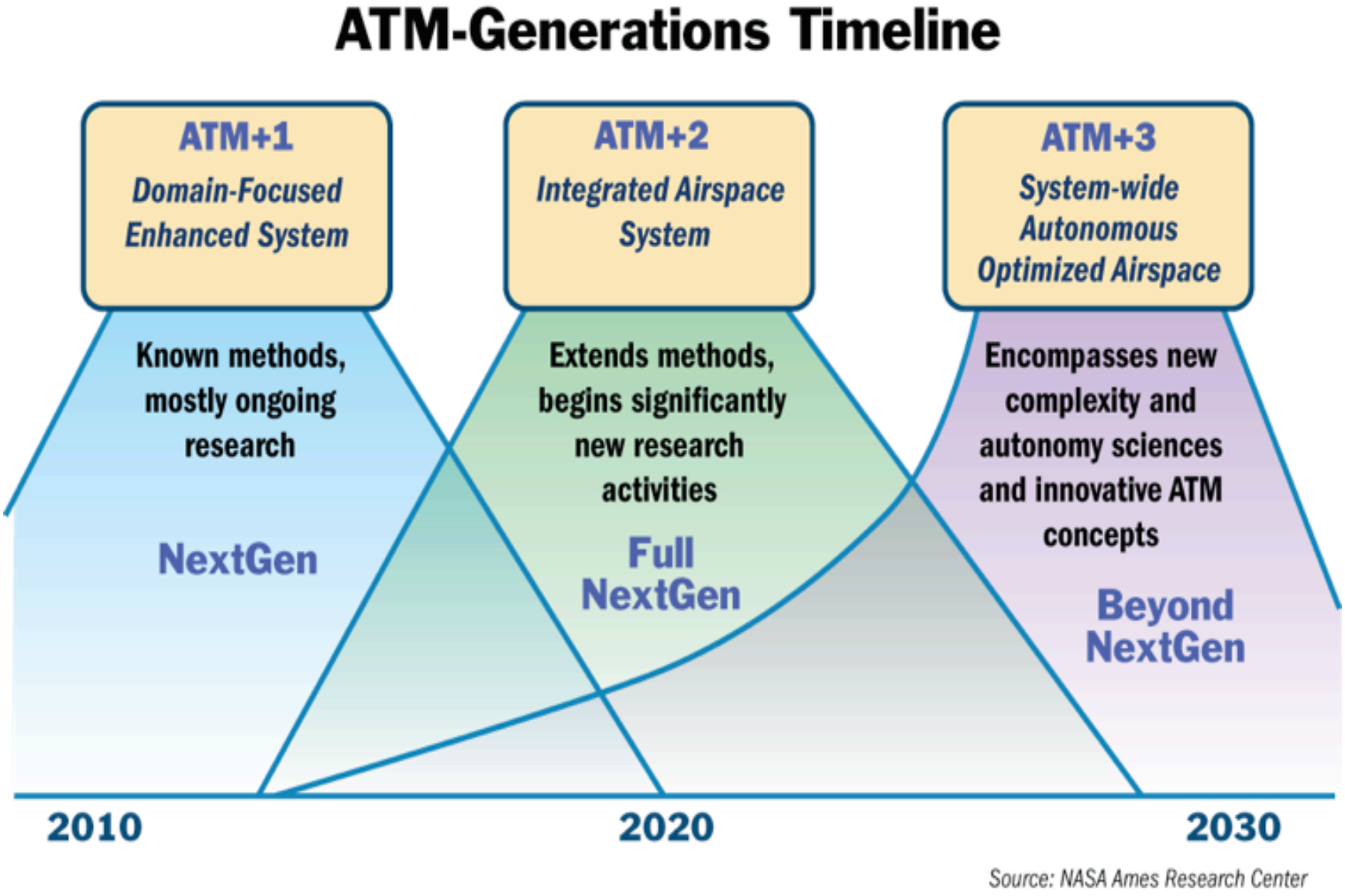
Ultra-Efficient Commercial Vehicles
- Pioneer technologies for big leaps in efficiency and environmental performance

Transition to Low-Carbon Propulsion
- Characterize drop-in alternative fuels and pioneer low-carbon propulsion technology

Real-Time System-Wide Safety Assurance
- Develop an integrated prototype of a real-time safety monitoring and assurance system

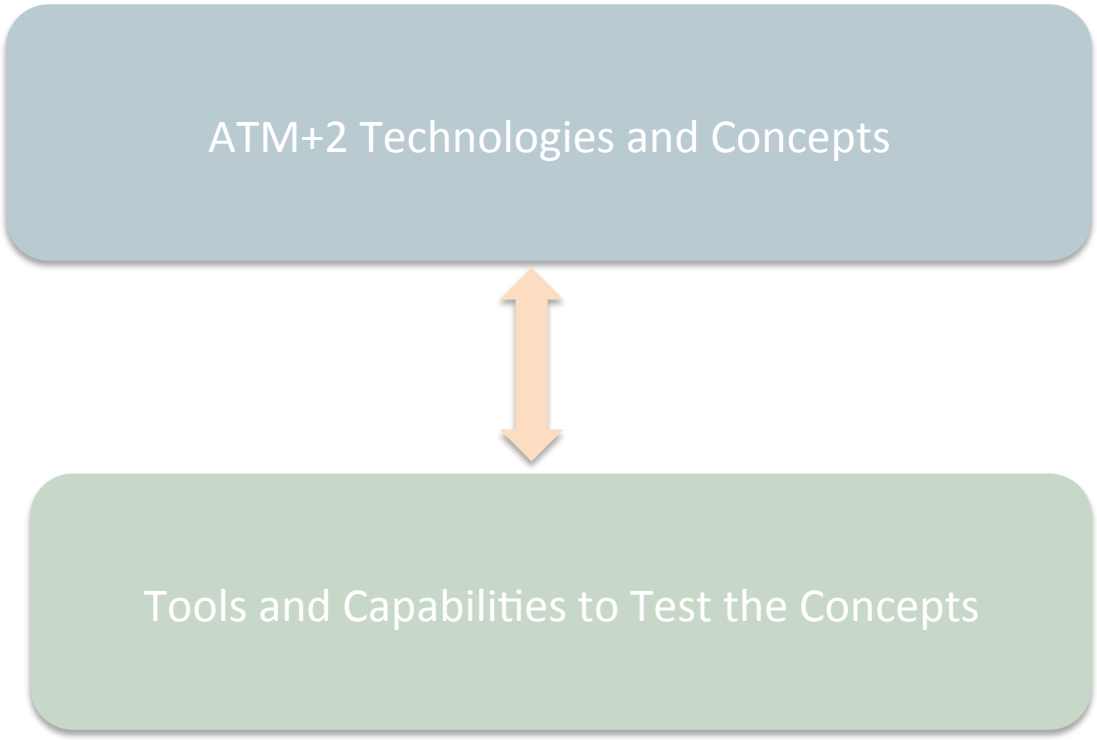
Assured Autonomy for Aviation Transformation
- **Develop high impact aviation autonomy applications**

AOSP Structure

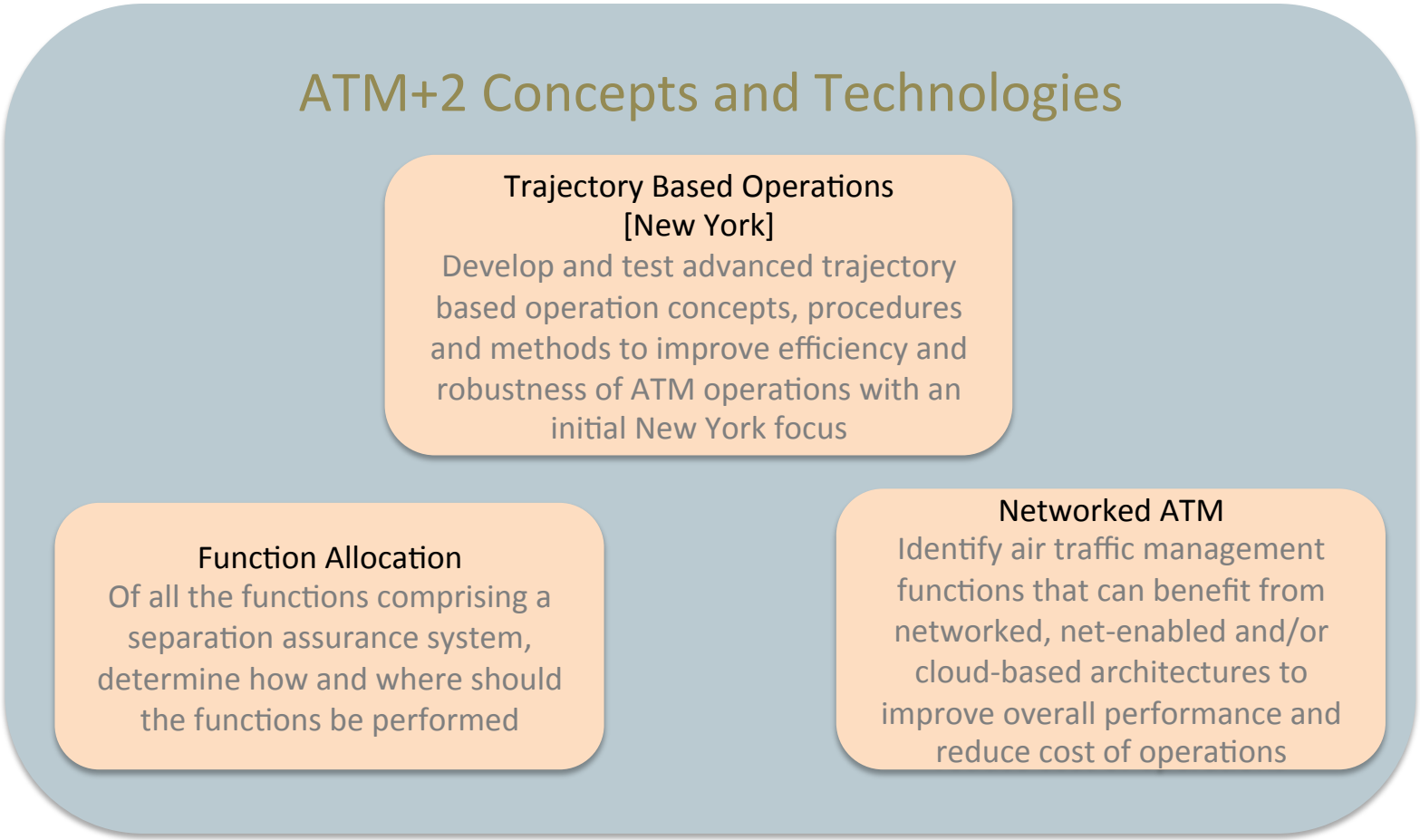


SMART NAS Scope and Objectives

Explore and Develop Concepts, Technologies and a Test Bed for Safe, Global, Gate-to-Gate Trajectory Based Operations in the ATM+2 time horizon (2025-2035)



SMART NAS Concepts and Technologies



SMART NAS Tools and Capabilities

Tools and Capabilities to Test the Concepts

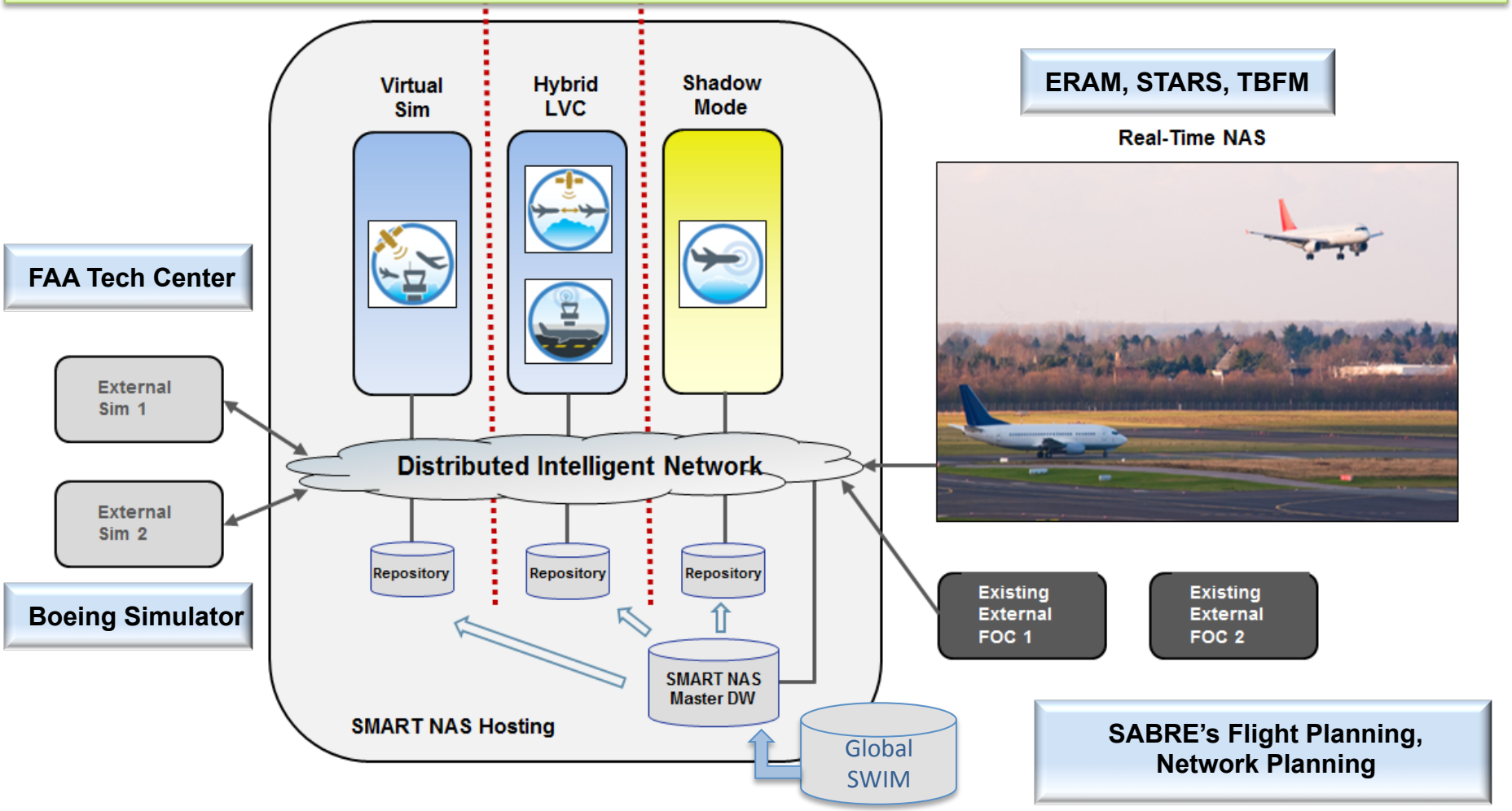
SMART NAS Test-bed
Develop an open, distributed evaluation capability critical to the ATM community, allowing full NextGen and beyond NextGen concepts and technologies to be assessed and developed

Real-time Safety Modeling
Develop data mining and prognostic techniques to perform real-time safety assessments of Air Traffic operations to identify precursors to safety incidents, detect emerging safety threats, and discover previously unknown safety threats and precursors to safety incidents, and to evaluate mitigation strategies

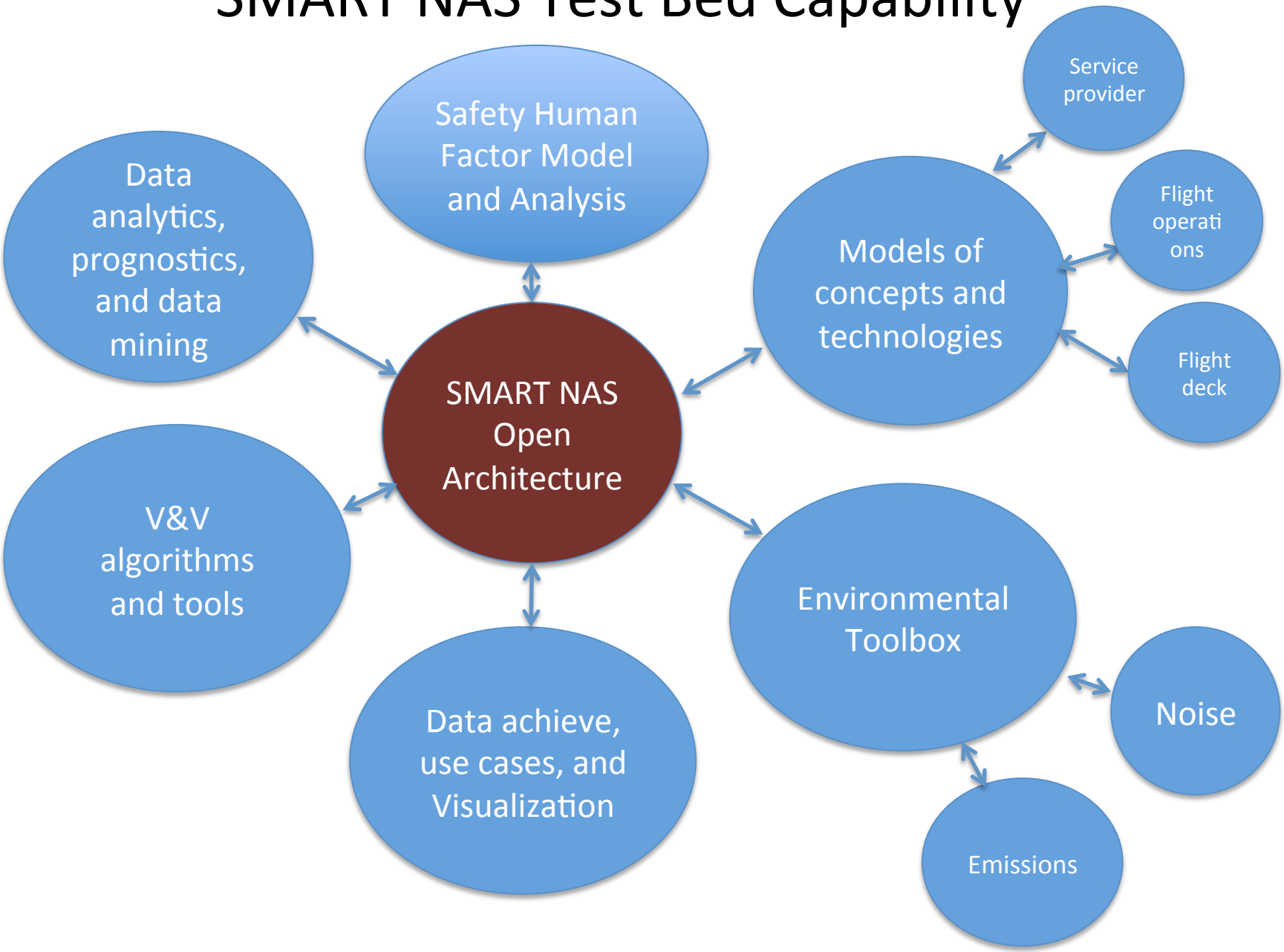
Systems Assurance Technologies
Design, develop, integrate and deploy real-time safety monitoring and assurance systems that are critical to the safety of flight operations

SMART NAS Test Bed

Develop a cloud-based, live, virtual and constructive simulation of the National Airspace System to perform integrated, multi-fidelity evaluations of future concepts and technologies



SMART NAS Test Bed Capability



SMART NAS V&V Focus

Complex ATM system evolution

Develop FAA-focused methods and tools for assessing the impact of design decisions throughout a software-intensive ATM system's evolution with respect to both safety and future costs.

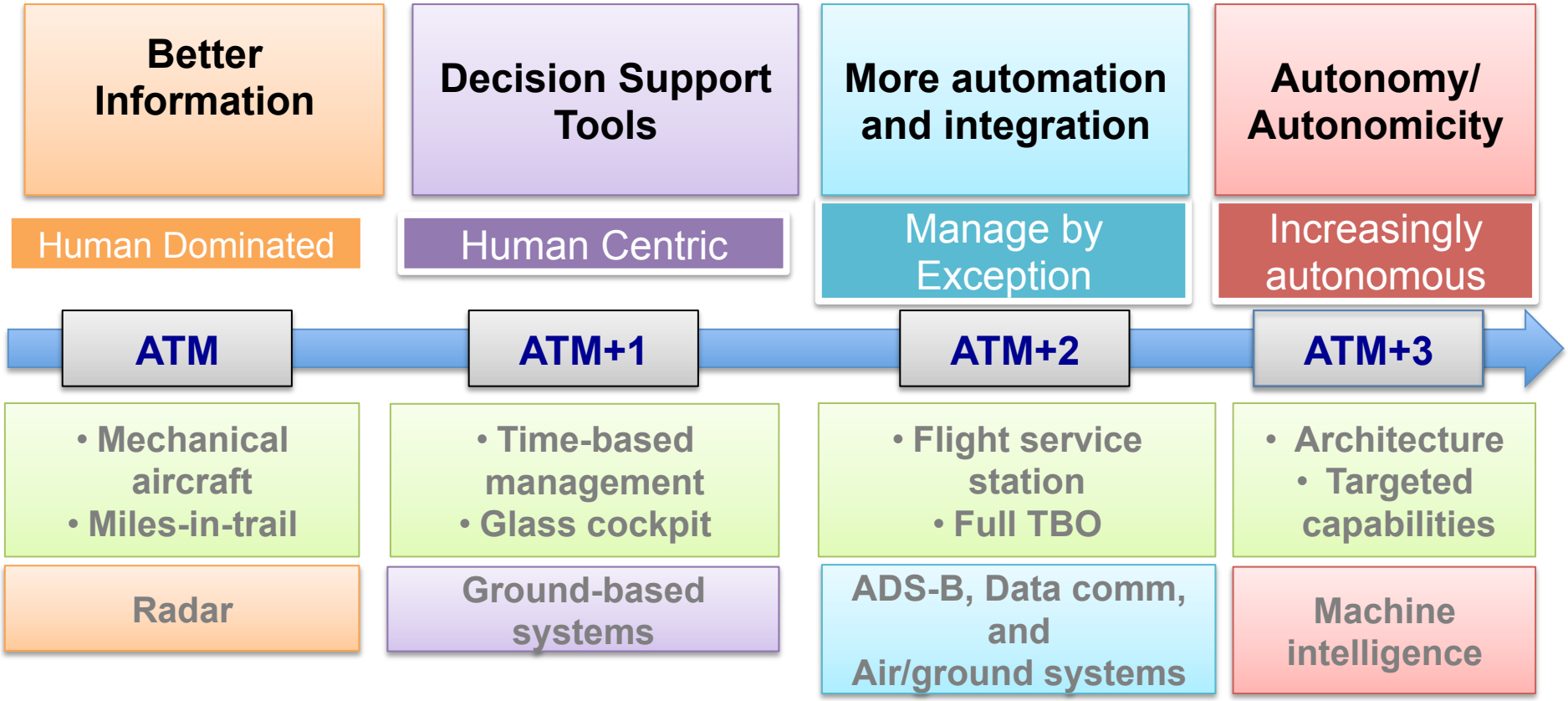
FAA Airworthiness Certification

Develop methods and tools for enabling safety assurance throughout all phases of aviation systems lifecycles for automated technologies introduced in both ground and airborne aviation systems.

Assurance of Flight Critical Systems

Develop tools, techniques, and architectural patterns to enable efficient verification and validation of complex safety-critical systems at all phases of system development and deployment

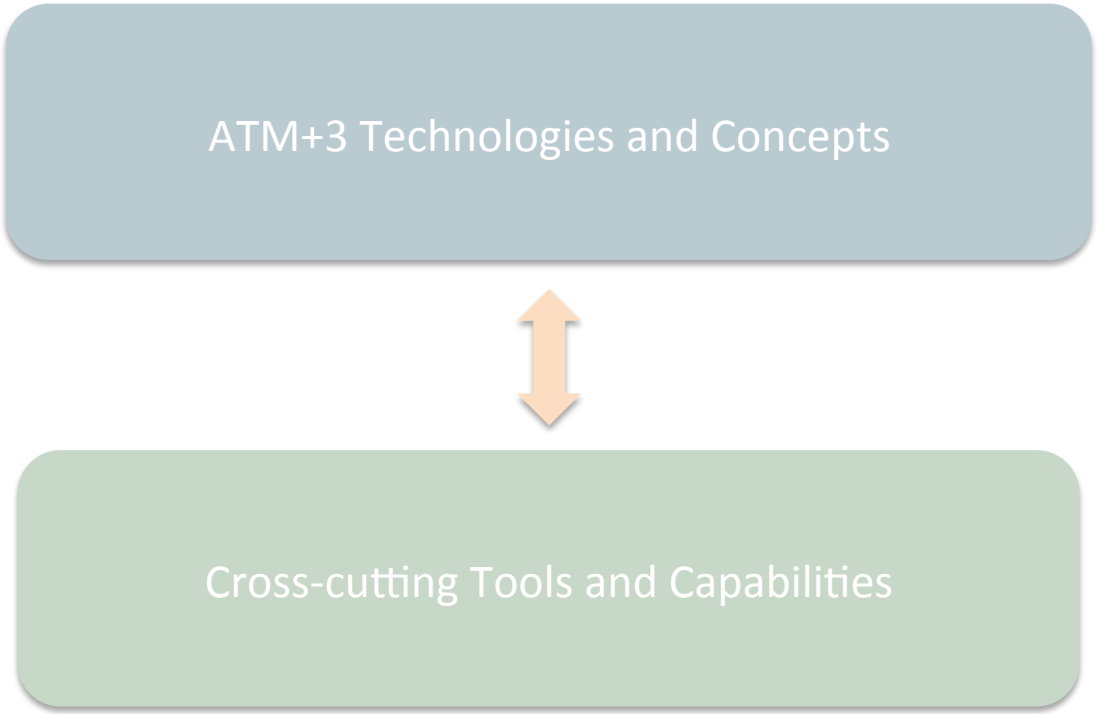
Towards Autonomy



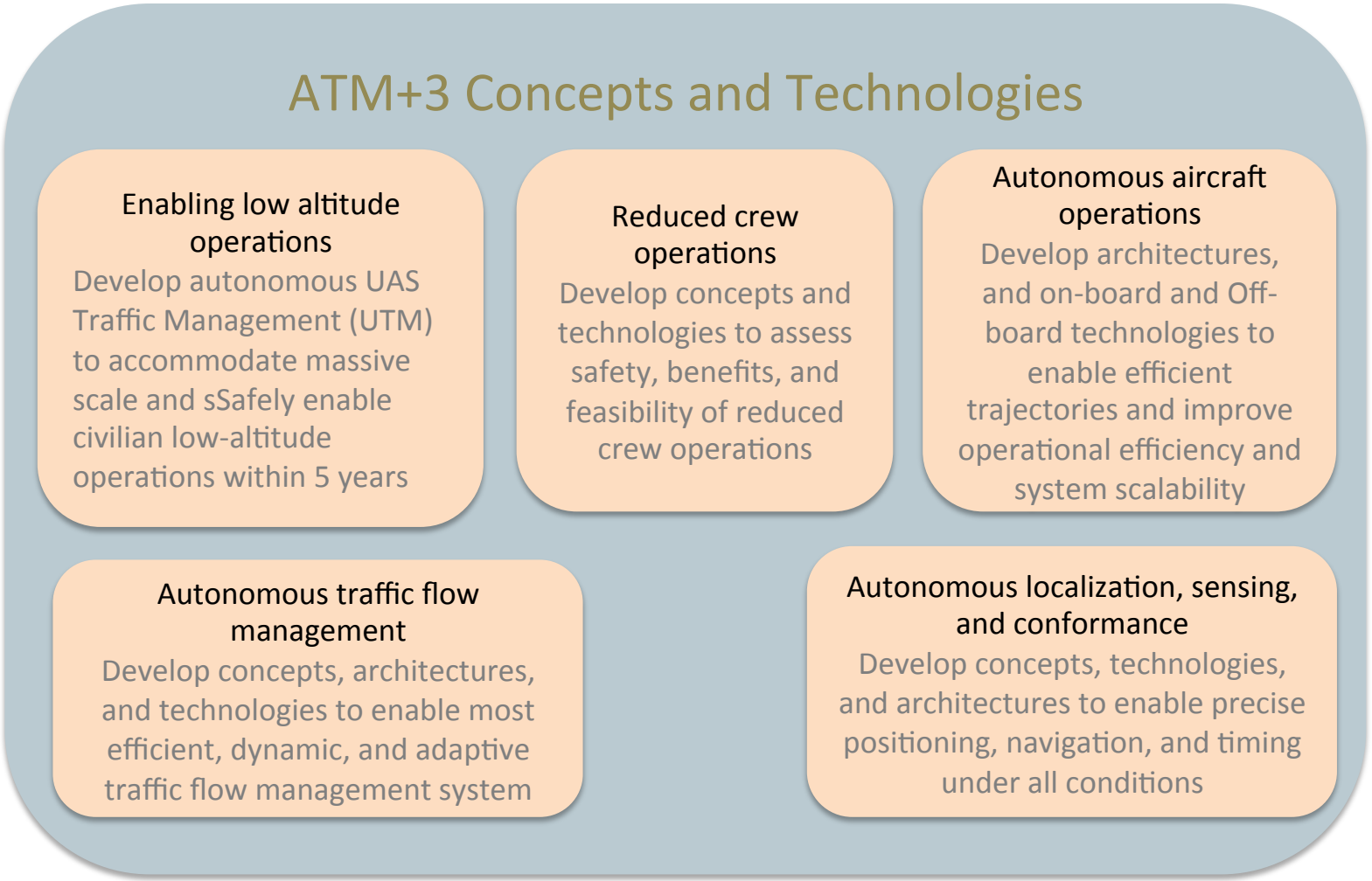
- Develop concepts, algorithms, technologies, and architecture(s) towards ATM+3
- Validate key “phase transition” technologies are feasible, safe and can be assured
- Analyze benefits and ensure overall autonomy architecture compatibility
- Fully develop, validate and migrate towards architecture that support safe autonomous operations
- Transition safe and beneficial technologies to stakeholders for operational use

SASO Scope and Objectives

Develop concepts, algorithms, technologies, and architectures to safely meet future National Airspace System (NAS) needs in the ATM+3 time horizon (> 2035) to enable airspace operations of greater complexity, density, scalability, mobility, efficiency, and affordability by justifiable combination of automation and autonomy



SMART NAS Concepts and Technologies



SMART NAS Tools and Capabilities

Tools and Capabilities to Test the Concepts

Foundational verification and validation

Develop concepts, methods, tools, and body of knowledge to assure autonomous operations and technologies

Ab-Initio Architecture

Design, develop, integrate and deploy real-time safety monitoring and assurance systems that are critical to the safety of flight operations

Needs, Barriers, Research, and Technical Challenges (initial FY15)

Operational Need	Barriers/Missing Link	Technical Challenge
Mobility: Safe and efficient operations at all altitudes all the way to door step/ground	• Infrastructure to support all altitude air operations • Assured precise positioning without GPS	TC1: Enabling low altitude operations TC5: Assured and Autonomous Localization, Sensing, Conformance
Affordability: Labor cost differences affect competitiveness	Technologies and certification approaches to allowing reduced crew operations	TC2: Reduced Crew Operations
Efficiency and Safety of flight: Aircraft will have to be efficient and safe under future congested airspace	Human workload, aircraft technologies, and access to information to make real-time decisions in cockpit	TC3: Autonomous Aircraft Operations

Needs, Barriers, Research, and Technical Challenges (Initial FY15)

Operational Need	Barriers/Missing Link	Technical Challenge
Airspace System Efficiency: Entire National Airspace System has to accommodate diverse mix and be as efficient as possible **Airport System Efficiency (under planning)**	Weather's contributions to delays is 75% and future diverse mix of airspace operations will need dynamic flow and airspace management strategies. Technologies to manage airspace (and airports) and flows dynamically to accommodate future mix are missing	TC4: Autonomous Traffic Flow Management

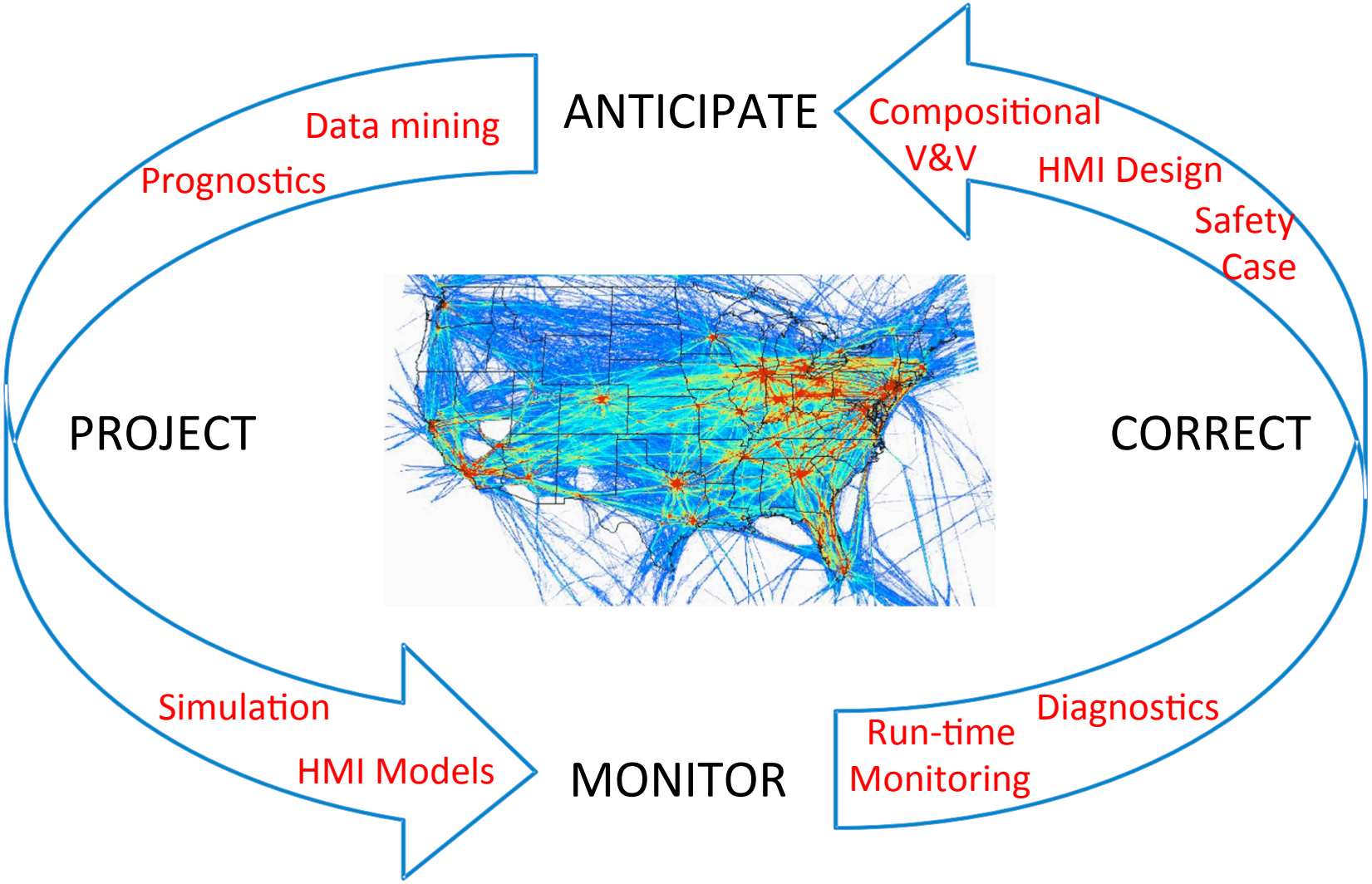
Needs, Barriers, Research, and Technical Challenges (Initial FY15)

Need	Barriers	Cross-cutting and Emerging
Acceptance/Trust/ Certification: Autonomous systems have to be acceptable to stakeholders	Assurance and V&V of technologies that rely on high levels of autonomy/ autonomicity are missing	CC1: Foundational V&V methods to assure autonomous operations and technologies
Architecture: Most efficient and effective architecture to support ATM+3 and beyond operations	Current architecture is not scalable and human-centric	Emerging: *Ab initio* architecture to enable future operations

Cross-Cutting Area 1: V&V of Increasingly Autonomous Systems

Goals: Develop concepts, methods, tools, and body of knowledge to assure autonomous systems

V&V In-the-loop for Increasingly Autonomous NAS



Autonomy-specific V&V Elements

Requirements for autonomous systems

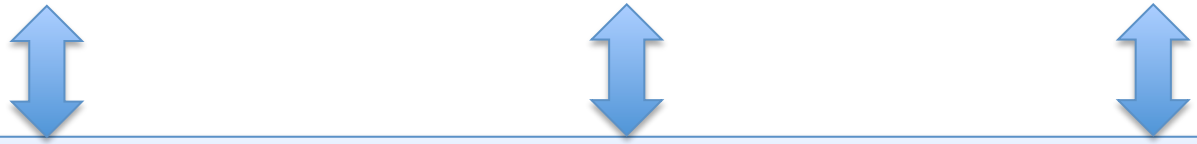
- Unambiguous requirements to support automated V&V
- Specific autonomy requirements, especially safety ones

V&V of autonomy algorithms

- Non-linear, probabilistic, adaptive/learning, model-based algorithms
- Probabilistic analysis, floating-point computation analysis

Incremental V&V in-the-loop

- Compositional V&V
- Runtime monitoring and analysis
- Incremental V&V

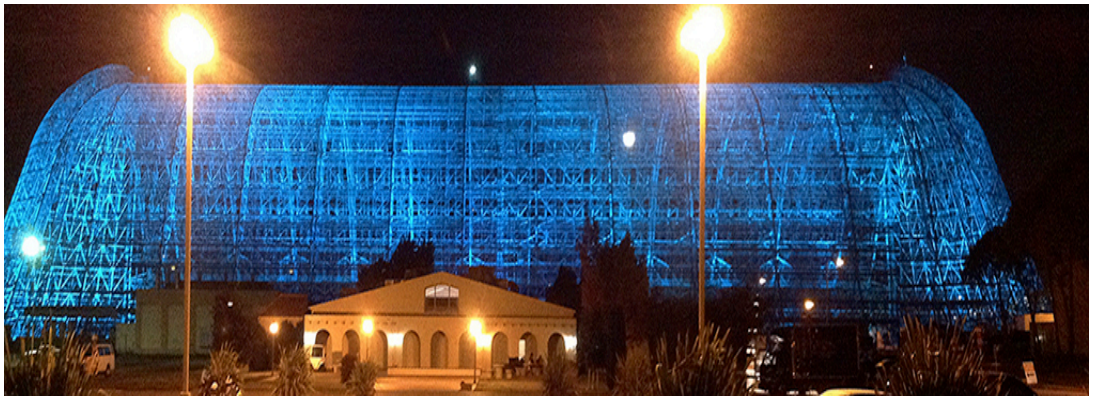


Lifecycle-long Safety Assurance Cases

- How can a safety case evolve? Incremental safety case?
- How can evolution be checked automatically and efficiently?
- Relationship with current, traditional certification (DO-'78)
  - Close relationship might create faster acceptance

Assurance of Autonomous Systems for Aviation Workshop, May 27-28, 2015

NASA Ames, Building B152
https://ti.arc.nasa.gov/events/aasa-2015/



- Can current assurance methods address autonomy? Where are the limits and can we go beyond them? Should we limit the degree of autonomy when considering safety?
- Do we really need to sacrifice performance for assurance? Can we drive towards a notion of performance-based assurance?
- How can we reason about human interaction with autonomous systems, especially when the autonomous systems hands over control to the human?
- How do we provide assurances for existing systems, especially when they were not originally developed to the required design assurance levels?
- Can we address assurance challenges in less time than it takes today? Can it be done without requiring a high-level of analytical skill on the part of the practitioner?

Conclusions

Airspace Operations and Safety Program

The goal of AOSP-developed NextGen methods and means is to provide advanced levels of automated support to air navigation service providers and aircraft operators for reduced air travel times and air travel-related delays, and to insure greater safety in all weather conditions.

SMART NAS Test Bed: Develop a cloud-based, live, virtual and constructive simulation of the National Airspace System to perform integrated, multi-fidelity evaluations of future concepts and technologies

Increased Autonomy Focus: Enable airspace operations of greater complexity, density, scalability, mobility, efficiency, and affordability by justifiable combination of automation and autonomy

V&V Strategy: Develop concepts, methods, tools, and body of knowledge to assure autonomous systems, including autonomy algorithm V&V, V&V in-the-loop, and easier access to V&V for third-party autonomy solutions