

Safety Assurance JPDO Perspective

Maureen Keegan
11 October, 2012

JPDO Safety Activities

- **Trajectory Based Operations (TBO) safety activities**
- **NextGen V&V (Safety Assurance)**
- **Where are we? JPDO assessment**

- JPDO UAS Initiative – potential risks
- Targeted 2025 (NGOps-4) safety analysis
- JPDO Risk Register

TBO Safety Activities

Background

- **“Trajectory-Based Operations (TBO) Operational Scenarios for 2025” (9/2010)**
 - *Prepared by the JPDO TBO Study Team*
- A basic element of TBO was *to* separate aircraft by automation
- The study team found that, if the safety case cannot be made, the fundamental concept for TBO would need to change

Safety Working Group Follow Up

- Established a TBO Safety Study Team in response to this recommendation
- Two sub groups established to:
 - Perform a TBO Capability Safety Assessment (CapSA)
 - Develop a TBO Safety Case Plan
- Delivered Final Reports last December

Safety Study Team Results

- Findings
 - There are no insurmountable safety barriers for TBO
 - There are safety gaps in the concept, in the technologies, and in policies needed to implement TBO
 - A public safety policy setting process that involves all stakeholders is needed
 - Simulation, including large scale, high fidelity simulation, must be used throughout the life cycle to refine and validate TBO
- Safety Study Team charged with addressing three follow on areas identified in the recommendations (March 2012)

Three New Sub-Groups Established To:

- Develop RE&D requirements to address TBO safety concerns identified in previous study
- Develop a recommendation for a multi-domain interagency Safety Council to serve as a forum for discussion of System of System safety concerns
- Identify TBO simulation needs and determine what, if any, new simulation capabilities are required

RE,& D Requirements Group

- Define the Research, Engineering and Development requirements to support the implementation of Trajectory Based Operations
 - *Describe specific experiments and deliverables*
 - *Create format/template that is meaningful to the responsible organization*
 - *Provide the time-line required to make impact (schedule)*
- The sub-team's mission was to describe the area requiring research in great enough detail for the responsible organization to decide how to approach the task and confirm the time-line (or define a time-line that is achievable)
- Completed September, 2012

Safety Council Group

- Develop a recommended governance construct and implementation pathway for a TBO safety council, including
 - sources and boundaries of its authority
 - scope and nature of its activities
 - composition of its membership and
 - legal and regulatory processes and procedures for its establishment and management.
- The study team's mission was not to make engineering decisions, but rather to develop recommendations for the characteristics of a council that would make specific recommendations about allocating risk mitigation responsibilities among projects/components, including components of integrated air/ground capabilities, so that the total system wide risk is acceptable.
- Completed a narrative report and roster of attributes and best practices to be emulated by the proposed TBO safety council (September, 2012)

Simulation Group

- Define the specific simulation needs for TBO concept development, validation, and implementation (completed 9/2012)
- Assess and document the capabilities of existing ATM simulations applicable to TBO (completed 9/212)
- Determine their adequacy for TBO and, if not, what extensions to existing simulations and/or creation of new simulations are necessary (due 12/2012)

NextGen V&V (Safety Assurance)

- NextGen Gap Analysis Identified V&V as a Gap (2008)
- NASA Stepped Up to Address this Gap and Started the V&V R&D Program (2008/2009)
- JPDO Initiated NASA-FAA-JPDO V&V Coordination (2010)
- Initially, Coordination Focused on Information Exchange Because NASA V&V Was Not Fully Funded.
- Focus has shifted to finding:
 - opportunities for prototype use of more mature NASA V&V tools
 - FAA representative software for use in NASA R&D

Safe and Rapid Deployment of NextGen - 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

Argument-Based Safety Assurance

know in advance that a system will be safe to use in its intended environment



Authority and Autonomy

unambiguous, comprehensive, and conflict-free assignment of roles between air/ground, human/machine



Distributed Systems

sound assurance of safety-critical distributed systems properties to help eliminate unintended consequences in NextGen



Software-Intensive Systems

new V&V techniques to increase software assurance and dependability



NextGen V&V Needs

NextGen Characteristics (1/2)

- It is system of systems - more complex than current NAS
 - Cuts across systems, organizations, and cultures
 - Functions are more distributed across components, agents, systems, and locations
 - More interaction of different system components
 - Net-centric system gives everyone access to common information for decision making

NextGen Characteristics (2/2)

- New roles and responsibilities
 - Different roles for humans and computers
 - Change in air/ground functional allocation
- Experience has shown new functions are rarely used as envisioned
- World in which 2025 functions will be used is still uncertain
- System architecture not inherently as resilient as today's NAS
 - Can't count on controllers to provide resilience (today they are able to deal with most failures)
 - Comm - Nav – Surv no longer “independent”

Safety Assurance Implications (1 of 3)

- Needs in the Near Term
 - Current methods are, for most part, adequate
- Needs in the Mid Term
 - Assure resilience of future system architecture
 - Assure System of System Safety
 - Look at air/ground – humans/automation together
 - Large scale simulations in a net-centric environment
 - Tools to understand System of System risks

Safety Assurance Implications (2 of 3)

- Long Term Needs
 - Start validating TBO concepts
 - Validation must take uncertainty of future environment into account
 - V&V tools for higher levels of automation
 - Safety assurance of agent-based (non-deterministic) software

Safety Assurance Implications (3 of 3)

- General Needs
 - More safety focus in early and late part of life cycle
 - Safety validation must include people and multiple stakeholders
 - Adopt existing tools that don't require independence assumptions
 - Adopt "Safety Case" methodology
 - Validate that a function continues to behave correctly as NextGen evolves
 - Deal with emergent behavior of new functions

So Where Are We?

JPDO assessment of possible improvements to FAA safety assurance (based on interaction with participants in JPDO safety activities and FAA/NASA V&V coordination)

- Need more safety assurance in early part of lifecycle (like the CapSAs for TBO and merging and spacing)
 - There is agreement about this across lines of business
 - Need to formalize process
- The integrated risk picture work is a great start, but FAA needs more system level safety assessments

So Where Are We? (cont'd)

- V&V progress
 - V&V is now embedded in AMS
 - Agreement on V&V need in early part of lifecycle
 - Need better V&V tools, especially for mid and long term NextGen
- Need better continuity in tracking safety risk through complete lifecycle assessment
- Need more rigor and better requirements for what is included in safety documents like the SRMD
- Informal integration across lines of business has started, but need better formal integration
- Need to integrate the ATO and AVS safety data systems such as ASIAs and ATSAP

Thank You!