Next Generation Air Transportation System Enterprise Architecture, Software, Safety, and Human Factors Review

An Interim Report

David Liddle, Chair, Committee to Review the Enterprise Architecture, Software Development Approach, and Safety and Human Factor Design of the Next Generation Air Transportation System

Computer Science and Telecommunications Board
National Research Council

NATIONAL ACADEMY OF SCIENCES

1863–2013 • Celebrating 150 Years of Service to the Nation

Task Statement

- From Sec. 212 of the FAA Modernization and Reform Act of 2012, PL 112-95; study funded by the Federal Aviation Administration.
- An ad hoc committee will conduct a study and prepare a report that will
  - (1) highlight the technical activities, including human-system design and testing, organizational design, and other safety and human factor aspects of the system, that will be necessary to successfully transition current and planned modernization programs to the future system envisioned by the Joint Planning and Development Office of the Administration and obtain necessary certifications and operational approval;
  - (2) assess technical, cost, and schedule risk for the software development that will be necessary to achieve the expected benefits from a highly automated air traffic management system and the implications for ongoing modernization projects; and
  - (3) determine how risks with automation efforts for the NextGen can be mitigated based on the experiences of other public or private entities in developing complex, software-intensive systems, particularly for life-critical, real-time operational systems, and including past aviation system development programs.
- Issue a *brief interim report* providing an initial assessment focusing on software development challenges.
- *Final report with recommendations anticipated in 2014.*

Committee Membership

- David E. Liddle, U.S. Venture Partners, *Chair*
- Steven M. Bellovin, Columbia University
- John-Paul B. Clarke, Georgia Institute of Technology
- George L. Donohue, George Mason University
- R. John Hansman, Jr., Massachusetts Institute of Technology
- Mats P.E. Heimdahl, University of Minnesota, Twin Cities
- John C. Knight, University of Virginia
- Leon J. Osterweil, University of Massachusetts, Amherst
- Walker E. Royce, International Business Machines Corporation
- Gavriel Salvendy, Purdue University
- Thomas B. Sheridan, Massachusetts Institute of Technology
- Robert F. Sproull, Oracle (retired)
- James W. Sturges, Lockheed Martin (retired)
- Elaine Weyuker, Independent Consultant

Interim Report – Project Status

- Still data-gathering; broad topic; diverse committee
- No conclusions, findings, or recommendations yet

Context & Background

- FAA is currently working on near- and mid-term capabilities
- NextGen efforts have significant implications for complexity, and safety-criticality of NAS systems
- … and corresponding enterprise and system architectures.
- Large-scale software-intensive systems are almost always challenging and risky
  - in terms of cost, schedule, and system performance

Constraints

- Operational & Capacity Constraints
  - Uncertainty re future capacity needs.
  - Localized congestion (metroplexes)
- Political, Economic, Cultural
  - Variety of stakeholders and significant scrutiny
  - Some benefits cannot be fully realized without participation and costly adoption by stakeholders.
  - Workforce expectations and skillset considerations
  - Competing internal goals
    - E.g., conservative safety culture may inhibit adoption of new technologies or increased automation.

Technical Realities

- Need for integrity, fault tolerance, flexibility, integration in dynamic environment
- Operational procedures, certification of avionics, international adoption
- Design for human-intensive systems
- Importance of a system integrator
  - Natural tension between client (FAA) and supplier (various contractors) re *architecture leadership*

Emerging Topics of Focus and Concern For This Committee

- Understanding and managing benefit and cost expectations
- System integration and software development approaches
- System safety
- Human factors, automation, and decision support
- System security
- Unmanned aircraft system integration
- Spectrum management

Understanding and Managing Benefit and Cost Expectations

- Alignment among
  - the overarching NextGen vision
  - the expected benefits and the risks to achieving them
  - the estimated costs (and who bears those costs).

- How are expected benefits and uncertainties understood and managed?
- How are lessons learned folded into subsequent increments?
- How to characterize programmatic, engineering, and operational risk?

Architecture

- Committee is focused on both the enterprise architecture and the technical and systems architecture
- Who are the users of these architectures?
- What decisions do the architectures influence?
- Does the architecture afford extensibility, room for innovation
- Who is responsible for architectural leadership?

System Integration and Software Development Approaches

- What is the incremental build plan and processes for integrating new capabilities?
- How are quantified measures and expert engineering judgments of software change costs and trends used?
- How are technical and system requirements, expectations, and changes communicated to and from the FAA?
  - What are the underlying technical and architectural assumptions?
  - How is testing and integration managed?
- What have been the biggest challenges (technical, process, operational, or organizational)?
- What are current uncertainties and risks and anticipated mitigation plans?
- Would like to see details of these in exemplar programs (e.g., DataComm?)

System Safety

- NextGen offers opportunity to introduce new safety capabilities while current capabilities should be maintained or improved
- Safety is an emergent property that derives from careful design at all levels.
- What techniques are included in the NextGen architecture, design, and implementation to mitigate residual risk?
- What specific techniques are being used to undertake hazard identification and estimate residual risk at each phase of deployment?
- What is the role of quantification in deployment decisions?

Human Factors, Automation, & Decision Support Tools

- What are the current and anticipated automation and decision-support capabilities and plans for training & managing the transitions from existing tools and processes to NextGen?
- At what stage in the process does the human factors team become involved and how?
- Reasons for integrating (or not) past human-factors recommendations
- Differences between current ATC & anticipated NextGen ATC technologies and processes re needed skill sets and knowledge requirements for controllers and pilots.
- How and when to use HITLS
- Impact of computer-based decision aids and the dependency on these by controllers.

System Security

- What are the plans, processes, and mechanisms for managing system security in the national airspace?
  - How is the threat model validated, and how will threats be monitored over time as context and adversaries change?
  - What is the scope and focus of security concerns for NextGen and how they are accounted for in the system architecture.
  - What are the most significant security risks and challenges and what plans are in place to address them?
  - Where does overall responsibility for security reside?
  - How are security considerations managed and addressed in the various programs of NextGen (such as ADS-B and DataComm)?
  - How do NextGen and the NAS cope with the insider threat—that is, authorized users of the systems with malicious intent

UAS Integration

- UAS procedural and technical challenges will have significant implications for NAS and NextGen
- UAS pose numerous procedural and technical challenges and introduce new requirements; they introduce safety and security challenges.
  - What are the key factors that will guide FAA work in this space, and what is the projected time line for policy decisions and any associated implementation?
  - What design and architectural decisions (if any) have been or will need to be taken in NextGen to accommodate UAS of varying flight profiles, capabilities, and weights and types?

Spectrum Management

- The management and use of spectrum in the future will need to be a critical element of the systems architecture.
- The committee is focused on current and anticipated plans with regard to spectrum management for the NAS and NextGen.

Importance of Modernization

- NextGen aimed at transforming U.S. airspace
  - There are significant modernization opportunities along the way
  - A key is balancing evolutionary changes with revolutionary changes and
  - …. aligning these changes with the most significant challenges in the NAS
- An ambitious long-term vision would include short- and medium-term initiatives that will
  - provide a foundation for a longer-term vision
  - enable critically needed modernization of aging elements of the NAS
- In the committee's view, both of these elements are critically important

For More Information

- Project information at www.cstb.org
- Staff contacts:
  - Jon Eisenberg (jeisenbe@nas.edu)
  - Lynette Millett (lmillett@nas.edu)
  - Gin Bacon Talati (vbtalati@nas.edu)