NextGen Aviation Safety

Amy Pritchett
Director, NASA Aviation Safety Program
‘NowGen’ Started for Safety!
System ‘Complexity’ Has Increased…
…As Safety Has Also Increased!

U.S. and Canadian Operators Accident Rates by Year

Annual fatal accident rate (accidents per million departures)

1987 Through 2006
So, When We Talk About NextGen Safety...

- How can we make the system even safer?
- How can we ease constraints imposed by safety?
- How can we prove the system is safe?
So, When We Talk About NextGen Safety...

• How can we make the system even safer?
  – Monitor for safety
  – Design for safety

• How can we ease constraints imposed by safety?

• How can we prove the system is safe?
Monitoring Current Operations

• While we strive for predictive methods for identifying and resolving safety concerns, we must still monitor for the unexpected

• Early implementation:
  Aviation Safety Reporting System (ASRS)
  – In 30 years of service, over 700,000 reports provided by pilots, controllers and others
  – Examined to flag research issues and operational issues

• Potential for much more!
  – Examine for ‘vehicle’ issues and ‘system’ issues
  – Definition of ‘normal’ or ‘allowable’ operations to compare against?
  – Traceability and comparison to assumptions throughout life-cycle?
  – Presents a vast data-mining challenge to live up to full potential!
Monitoring of (in) NextGen

Initiatives:
ASIAS
ASAP/ATSAP/etc

Challenges:
Data Sharing
Data Analysis
‘Just Culture’
“From our research experience, we realized that developing ATM tools could not proceed in a traditional linear design fashion going from concept to simulation to field tests to implementation. Rather we needed to get prototypes to realistic operational settings early and often.”
NextGen Attributes Relevant to Safety

- Emergent concerns in decentralized, tightly-coupled operations
- New roles for humans
- Greater demands for reliability
- Operation closer to hazardous conditions

Addressed early, many improvements to safety can also help efficiency measures (and vice versa)

Left too late, well...
Emergence

• Emergence: Behaviors observed at one level of abstraction which can not be predicted (maybe not explained!) at a different level of abstraction

• Example:
  – An unstable compression wave in a traffic stream in which each aircraft is individually stable

• My hypothesis: Many aspects of complex system safety are emergent phenomenon
  – How does analysis at one level extrapolate to another?
Timeline by Design Space

NearGen
Variants on current con ops

FarGen
Transformative, 2-3X

This is an opportunity to make the system good from the start!
Timeline by Design Space

Demands advances on our part:
- Envisioning the ConOps
- Defining roles

ConOps? Organizational structure? Inherent structural safety?
Functions and operations?
Selection of technologies?
Technologies, ConOps Given Make Them Work

NearGen
Variants on current con ops

FarGen
Transformative, 2-3X
• Sometimes we make the humans sound like the problem. . .
  “the problem with the current system is that it is human-centric” . . .

• Can anyone name an accident not caused by ‘human error’?

• We don’t even systematically record all the cases where humans ‘saved the day’ – that’s their job
Human Contribution in Next Gen?

• Is it wise to plan for:
  – Automated activity beyond the capability of the human
  – Human supervising the automation for automation failures
  – Human intervening in degraded operations beyond the design limits of the automation

???
Automated Cockpit?
1951 Fitts Report

*Human Engineering for an Effective Air-Navigation and Traffic-Control System*

- Research Objective II. Determination of the Capacities of Human Operators for Handling Information.
- Research Objective V. Determination of Principles Governing the Efficient Visual Display of Information.
- Research Objective VI. Determination of Optimum Conditions for the Use of Direct Vision.
- Research Objective VII. Determination of the Psychological Requirements for Communication Systems.
- Research Objective IX. Maximum Application of Existing Human-Engineering Information.
Our NextGeneration Fitts Report

Our human factors methods need to change!

- From metaphor and guideline to concrete, unambiguous, design guidance
  - Collaborative with tech designers – they need to hear human performance considerations, and we the physical constraints
- ConOps and operating procedures as the subject of rigorous design
- System engineering approach to identifying in and focusing resources on the biggest issues
  - Applying coarse methods at first to capture the ‘low-hanging fruit’
- Predictive methods to guide R & D
Describing Automation

• Robustness: The range of operating conditions with satisfactory performance

• Autonomy:
  - (Engineering): The sophistication of the automation’s behaviors when objective and subjective reality overlap – regardless of problems with robustness
  - (Management): The ability to go do any task, no matter how simple, and report back when the manager should know anything

Robustness & Autonomy (management definition) will be our bigger challenges!
So, When We Talk About NextGen Safety…

• How can we make the system even safer?
  – Monitor for safety
  – Design for safety

• How can we ease constraints imposed by safety?
  – Notable example – Software!

• How can we prove the system is safe?
Dependable software identified as critical to many safety-critical systems, especially aviation.
Software Cost as a Constraint on Innovation

• Software Development Productivity for Industry Average Projects*
  – Cost from requirements analysis through software integration and test

<table>
<thead>
<tr>
<th>Characteristic Software Development Productivity</th>
<th>Source Line of Code/Work Month (SLOC/MM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic rates</td>
<td>130-195</td>
</tr>
<tr>
<td>Evolutionary approaches</td>
<td>244-325</td>
</tr>
<tr>
<td>New embedded flight software</td>
<td>17-105</td>
</tr>
</tbody>
</table>

• Assuming a full cost rate of $150k/year/person the cost for one line of new embedded flight software is between $735 and $119

So, When We Talk About NextGen Safety...

• How can we make the system even safer?
  – Monitor for safety
  – Design for safety

• How can we ease constraints imposed by safety?
  – Notable example – Software!

• How can we prove the system is safe?
  – V & V of complex systems
What’s Involved?

Objectives of V & V

- Demonstrate/confirm safety of new designs
- Demonstrate/confirm performance of new designs
- Demonstrate/confirm design models’ and methods’ predictions
- Remove V & V barriers to new functions
  - e.g., cost- and time-effective *a priori* V & V
  - e.g., viable *in situ* V & V to support dynamic configuration / composition
What’s Involved?

Methods for V & V

- Safety Cases
  Are the assumptions correct and traceable?
- Design-based Methods
  Can we build in safety/performance through process?
- Evaluation-based Methods
  Can we evaluate safety/performance experimentally?
- Longitudinal Methods
  Can we track potential issues during and following implementation?
What’s Involved?

Entities Needing V & V

Sub-systems
- Hardware
- Software
- Liveware

Vehicle/Facility

Broader Operation
- Airspace
- Airline operations
- Maintenance

← May Use Common Theories and Methods →
What’s Involved?

Concepts Underlying V & V

Component Analysis
- e.g. reliability
- failure modes

Interactions Between Components
- e.g. fault tree
- architecture analysis

System Dynamics
- e.g. emergence

May require communication between different methods!
So, When We Talk About NextGen Safety…

- How can we make the system even safer?
  - Monitor for safety
  - Design for safety

- How can we ease constraints imposed by safety?
  - Notable example – Software!

- How can we prove the system is safe?
  - V & V of complex systems