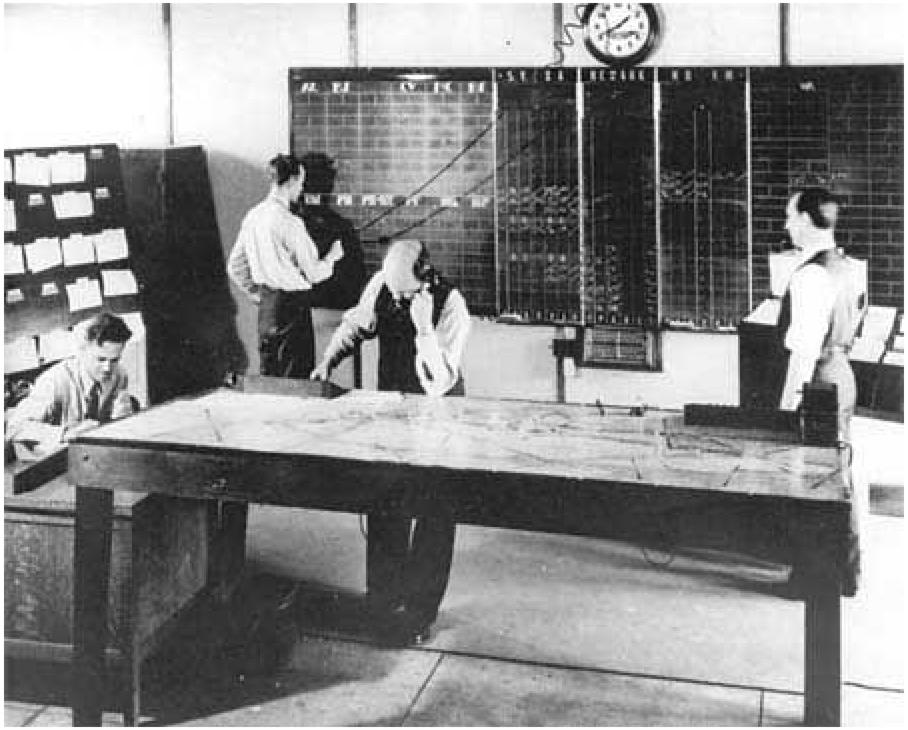
NextGen Aviation Safety

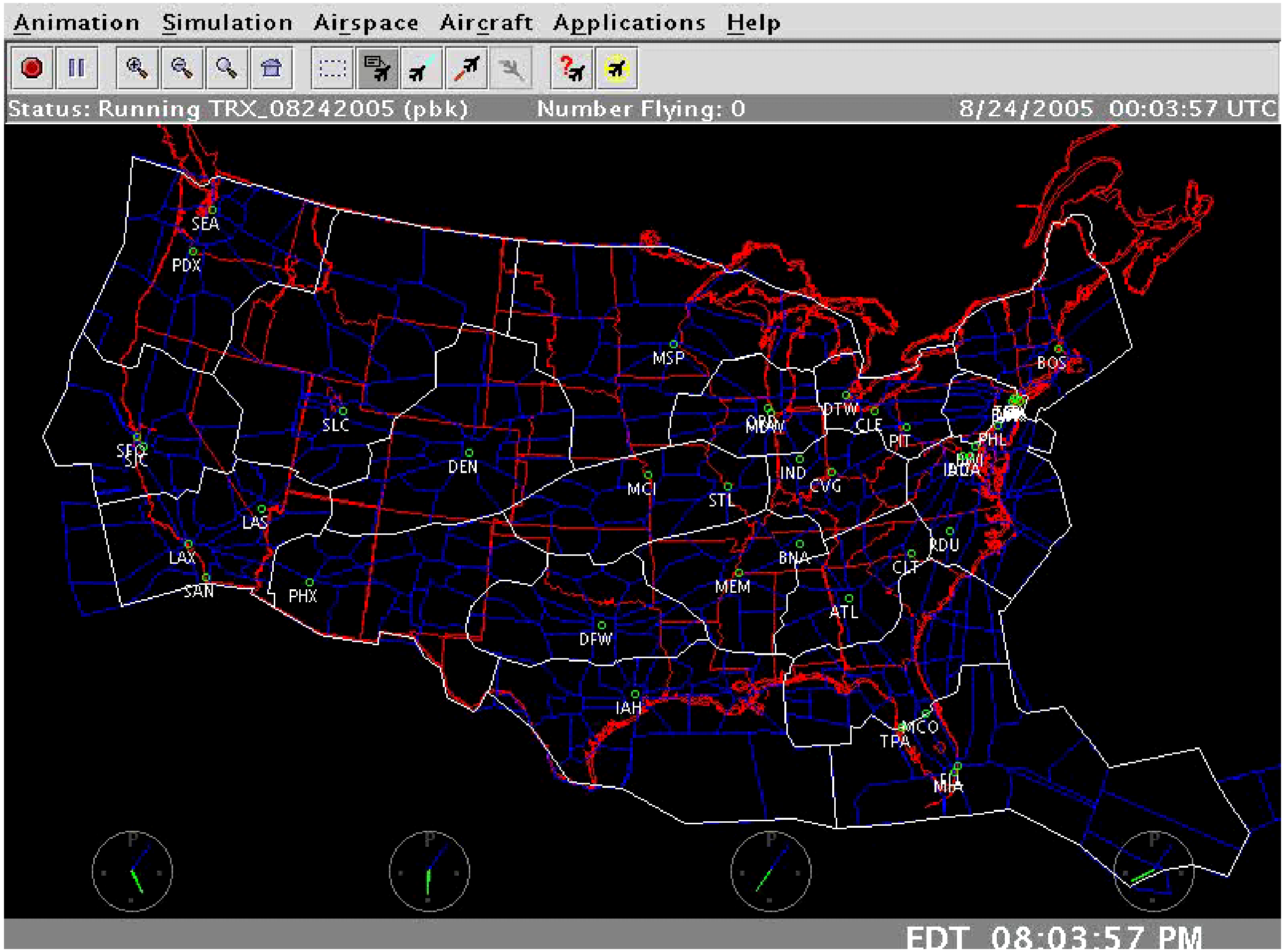
Amy Pritchett

Director, NASA Aviation Safety Program

‘NowGen’ Started for Safety!



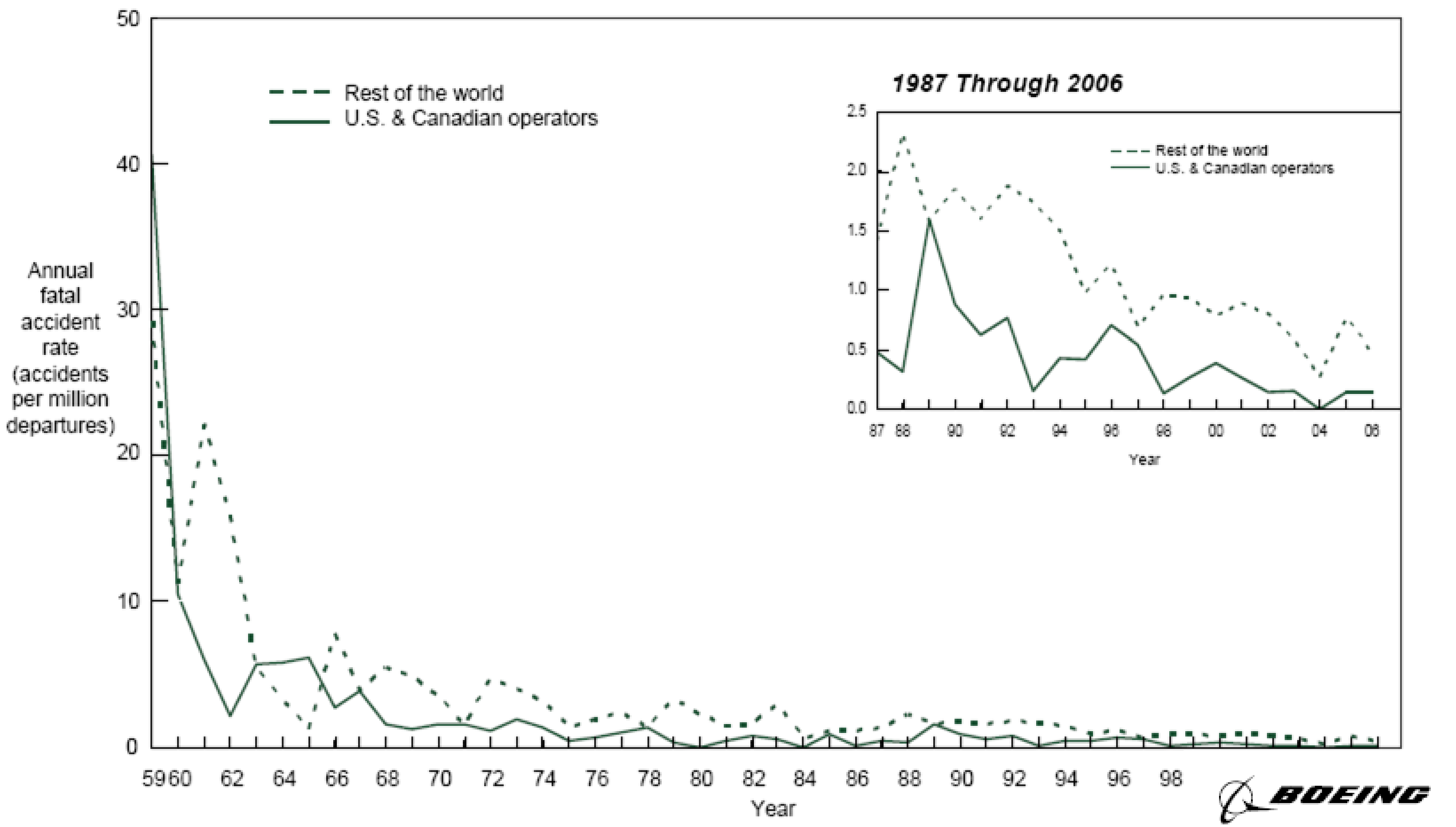
System ‘Complexity’ Has Increased…



... As Safety Has Also Increased!

U.S. and Canadian Operators Accident Rates by Year

Fatal Accidents – Worldwide Commercial Jet Fleet – 1959 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?

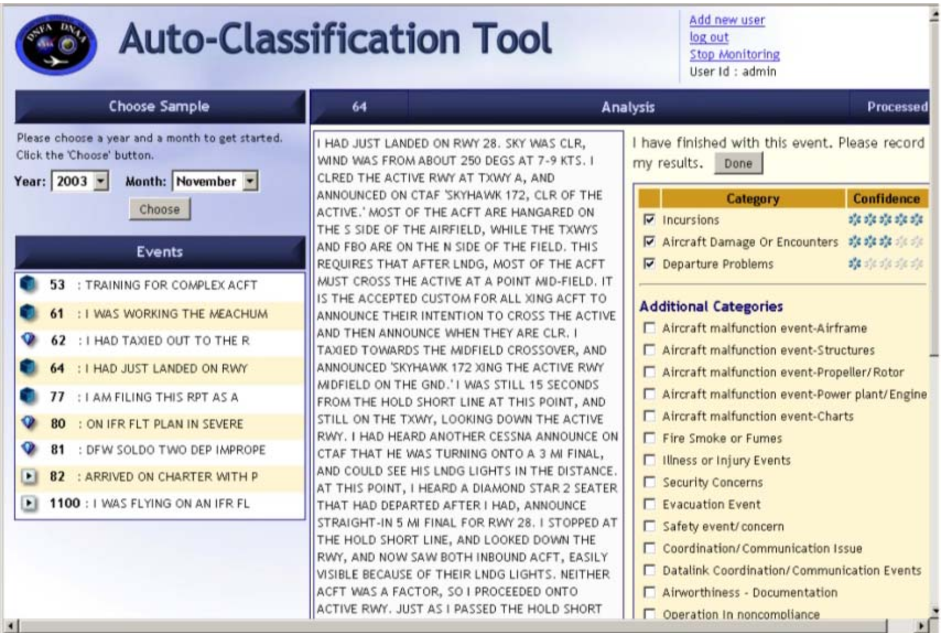
So, When We Talk About NextGen Safety…

- 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?

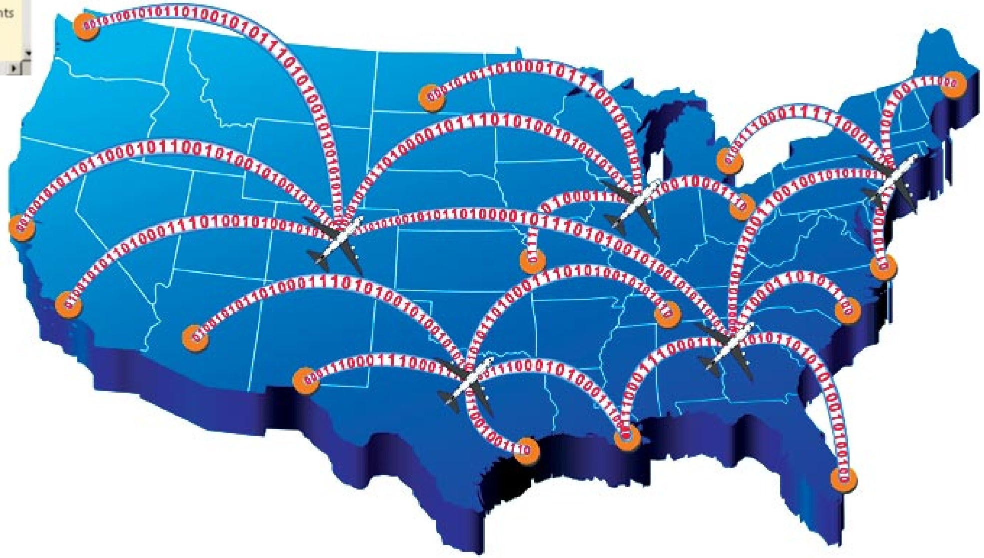
Monitoring Current Operations

- 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



Challenges:
Data Sharing
Data Analysis
'Just Culture'

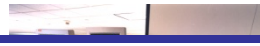


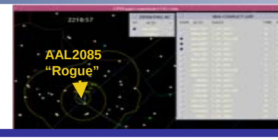
Initiatives:
ASIAS
ASAP/ATSAP/etc

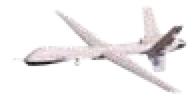
Recent History in ATM Design

Research

Prod



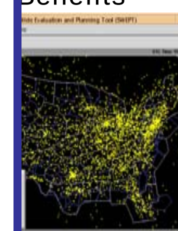




Gen

Flight Management Systems

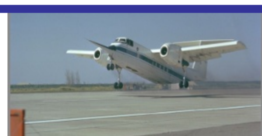
Benefits

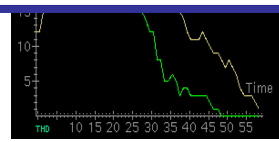


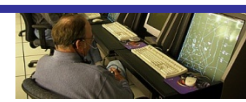
198

1970

"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."

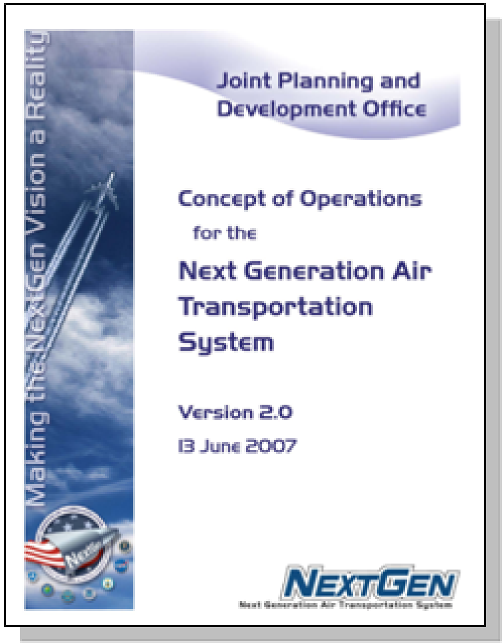






Research Spectrum

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

Timeline by Design Space

ConOps?
Organizational structure?
Inherent structural safety?

Functions and operations?

Selection of technologies?

Technologies, ConOps Given
Make Them Work

Demands advances on our part:
Envisioning the ConOps
Defining roles

NearGen
Variants on current con ops

FarGen
Transformative, 2-3X

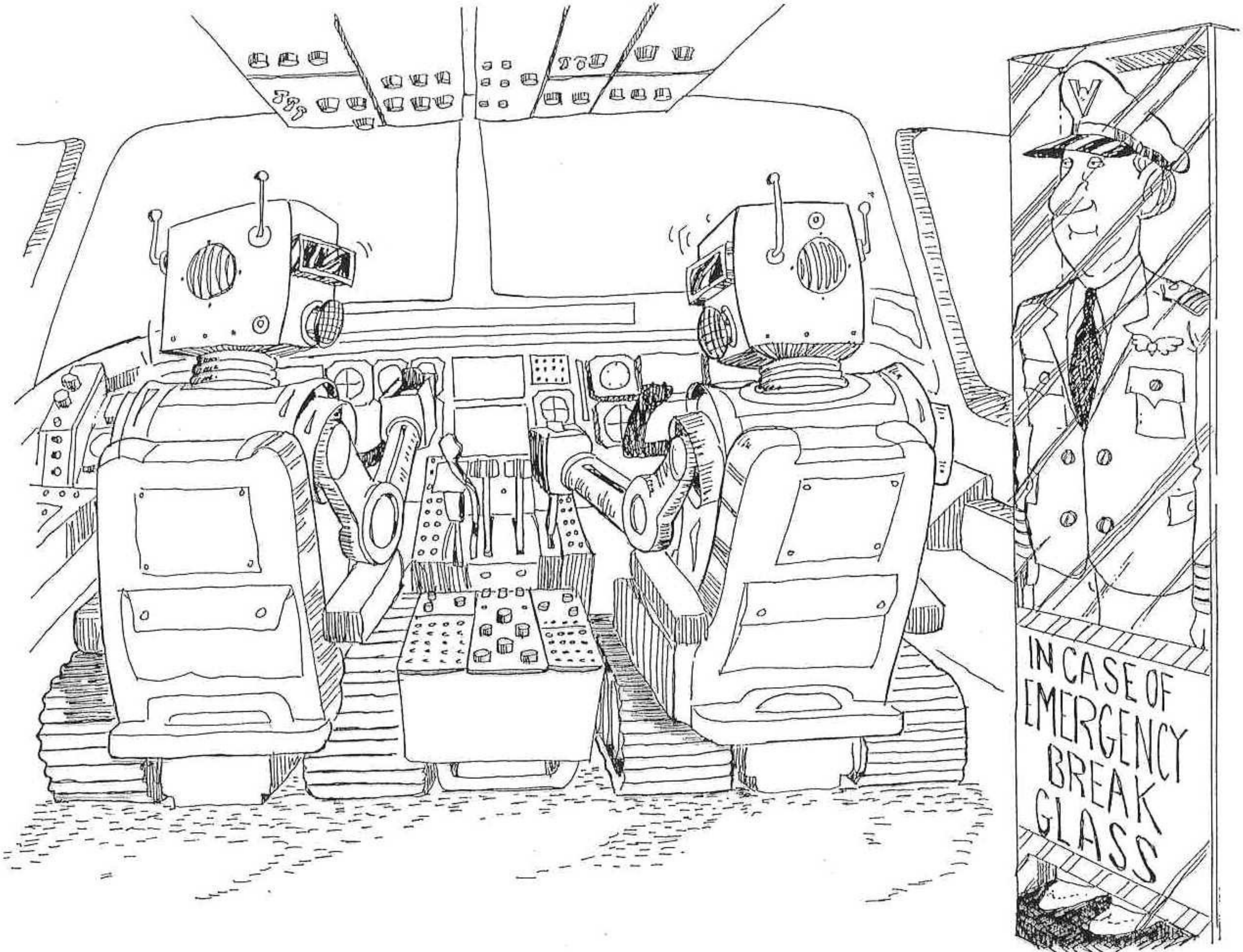
Are Humans the Problem or the Solution?

- 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

???


IN CASE OF EMERGENCY BREAK GLASS

Addressing Human Performance

1951 Fitts Report

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

- Research Objective I. Determination of the Relative Abilities of Men and Machines to Perform Critical Functions in Air-Navigation and Traffic-Control Systems.
- Research Objective II. Determination of the Capacities of Human Operators for Handling Information.
- Research Objective Ill. Determination of the Essential Information Required at Every Stage in the Operation of an Air-Navigation and Traffic-Control System.
- Research Objective IV. Establishment of Criteria and "Indices-of.Merit" for Human-Operator and Man-Machine Performance.
- 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 VIII. Optimum Man-Machine Systems Engineering.
- 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

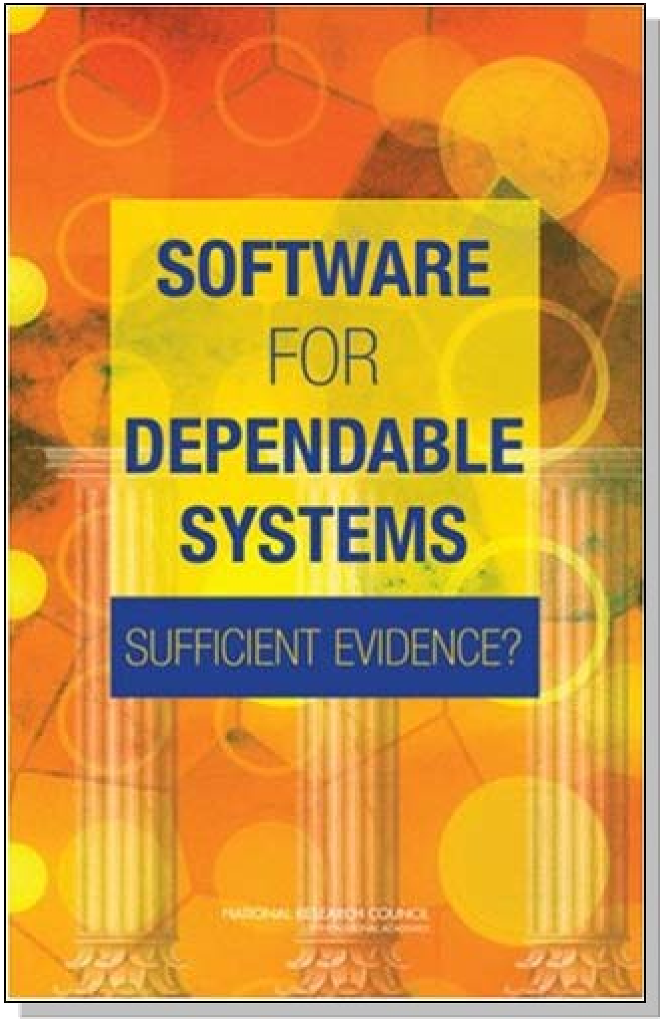
- Robustness: The range of operating conditions with satisfactory performance
- Autonomy:
  - (Engineering): The sophistication of the automation’s behaviors when objective and subjective reality overlap – regardless of problems with robustness
  - (Management): The ability to go do any task, no matter 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

Characteristic Software Development Productivity	Source Line of Code/Work Month (SLOC/WM)
Classic rates	130-195
Evolutionary approaches	244-325
New embedded flight software	17-105

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

* Lum, Karen Et, *Handbook for Software Cost Estimation.* May 30, 2003, JPL D-26303, Rev 0, Jet Propulsion Laboratory .

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

V & V This! (And This is Just One Vehicle)

Integrated Vehicle Health Management (IVHM) Algorithms Design

Stability & Performance Analysis
- Hybrid Systems Analysis
-Convergence (Rate/Accuracy)
- Probability of False Alarms
- Probability of Missed Detections
- Probability of Incorrect Identifications
- Failure/Damage Coverage

Stability & Performance Robustness Analysis
- Linear & Nonlinear Parameter Variations
- Unmodeled Dynamics
- Hybrid Systems Switching
- Faults/Failures/Damage Coverage
- External Disturbances
- Worst Case Analysis
- Time Delay Estimates

Stochastic Performance Analysis
-Hybrid Systems Switching
- Reliability Analysis
- Redundancy Management Effectiveness
- Diagnostics/Prognostics Accuracy
- Faults/Failures/Damage Coverage
- External Disturbance Effects

Software Verification & Safety Analysis
- IVHM Software Specifications
- Safety Case Analysis for Diagnostic, Prognostic, & Reasoning Systems
- Hybrid Switching Logic

Hardware / Flight Testing
- Faults / Failures
- HIRF /EME
- Noise / External Disturbances
- Airframe Structures
- Electromechanical Components
- Avionics Systems

Integrated Linear & Nonlinear Analysis
- Stability
- Performance
- Robustness
- Failure & Damage Coverage
- Reliability

Nonlinear Sim. Evaluation
- Detection/Mitigation Effectiveness
- Probability of False Alarms & /Missed Detections
- Monte Carlo Reliability Studies
- Probability of Incorrect Identifications
- Failure/Damage Coverage
- Achievable Dynamics under Vehicle Constraints
- Probability/Impact of Incorrect Decisions
- Probability of Loss of Control
- Guided Monte Carlo Robustness & Worst Case Studies
- Time Delay Effects and Impacts

Piloted Nonlinear Sim. Evaluation
- Crew Interface Effectiveness for Improved Sit. Awareness
- Mitigation/Recovery Effectiveness
- Cooper-Harper Ratings under Off-Nominal Conditions
- Var. Autonomy Effectiveness
- Flight/Trajectory Management Effectiveness under Off-Nominal / Emergency Conditions

Software Verification & Safety Analysis
- IVHM/IRC Software Specifications
- Safety Case Analysis for Adaptive, Predictive & Reasoning Systems under Off-Nominal Conditions
- Safety Case Analysis for Variable Autonomy
- Hybrid Switching Logic

Multidisciplinary Hardware-in-the-Loop Nonlinear Simulation Evaluation
- System Integration
- Software Implementation
- Fault/Failure Propagation
- Full Operational Envelope
- Abnormal Flight Envelope

Multidisciplinary Hardware-in-the-Loop Flight Evaluation
- System Integration
- Software Implementation
- Fault/Failure Propagation
- Full Operational Envelope
- Abnormal Flight Envelope

Stability & Performance Analysis
-Transient Response
- Steady-State Response
-Controllability & Observability
Hybrid Systems Analysis
- Failure/Damage Coverage

Stability & Performance Robustness Analysis
- Linear & Nonlinear Parameter Variations
- Unmodeled Dynamics
- Hybrid Systems Switching
- Faults/Failures/Damage
- External Disturbances
- Worst Case Analysis
- Time-Delay Effects

Nonlinear Analysis
-Bifurcation
-Controllability & Observability / Recoverability
- Hybrid Systems
-Faults/Failures Effects
- Probability of Loss of Control
- Achievable Dynamics & Feasible Trajectories under Constraints

Flying Qualities Analysis
- Susceptibility to Aircraft/Pilot Coupling
- Impact of Incorrect Pilot Inputs
- Variable Autonomy Partitioning
- Constrained Trajectory Generation & Management
- Integrated Guidance & Control Effectiveness Under Off-Nominal Conditions

Software Verification & Safety Analysis
- IRC Software Specifications
- Safety Case Analysis for Adaptive & Predictive Control Systems under Off-Nominal Conditions
- Safety Case Analysis for Variable Autonomy Interface Systems
- Hybrid Switching Logic

Flight Testing
- Control Recovery & Mitigation Effectiveness
- Impact of Incorrect Pilot Inputs
- Variable Autonomy Partitioning
- Integrated Guidance & Control Effectiveness Under Off-Nominal Conditions

Integrated Resilient Control (IRC) Algorithms Design

Vehicle / Crew Interface (VCI) Algorithms Design

Developing a Plan for V & V

Entities Needing V & V	Objectives of V & V
Concepts Underlying V & V	Methods for V & V

What’s Involved?

<u>Objectives of V & V</u>

- 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	Interactions Between Components	System Dynamics
e.g. reliability failure modes	*e.g. fault tree architecture analysis*	*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

Thank You! Questions?