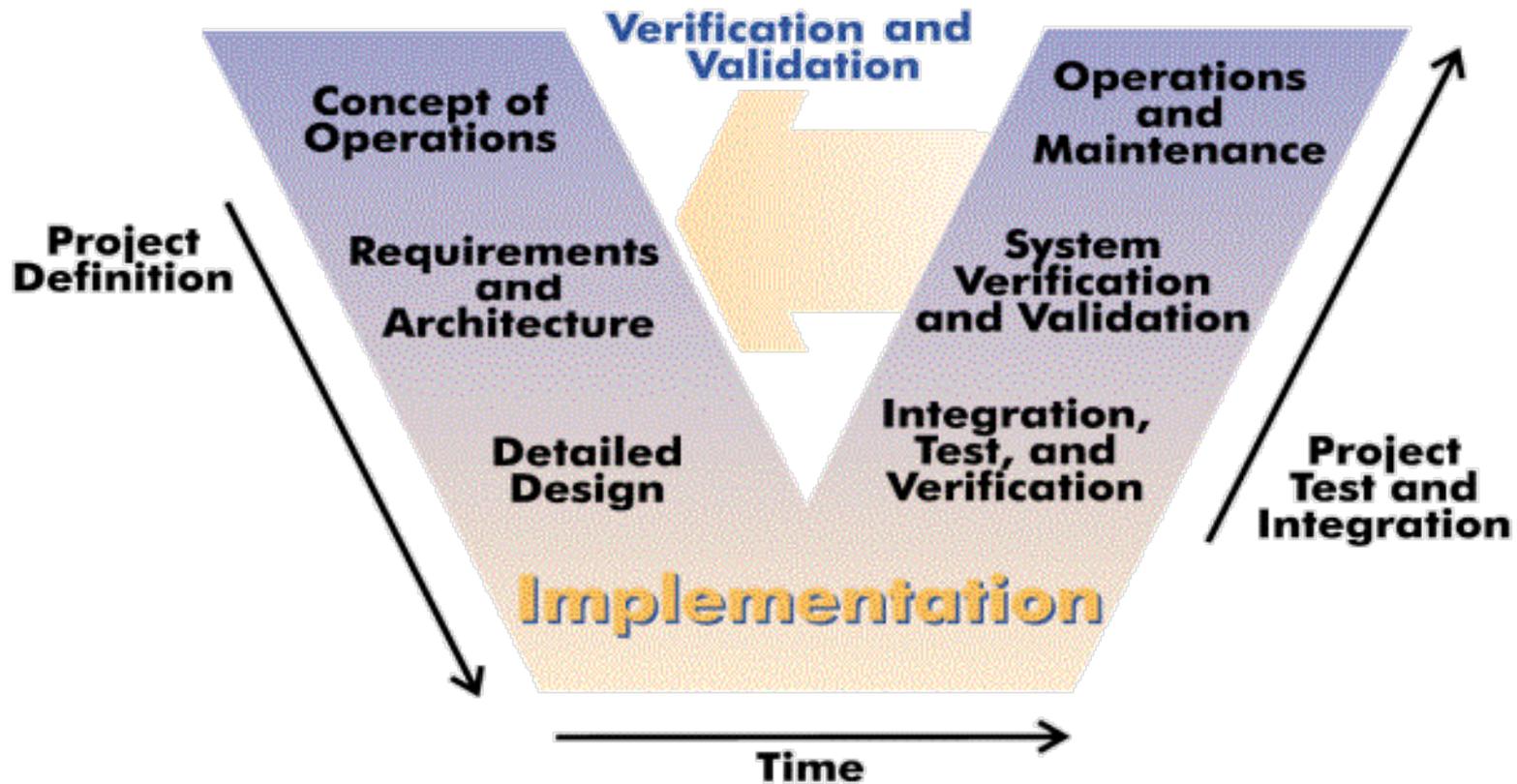




Verification & Validation of Flight Critical Systems Assessment of Critical Research Areas

Amy R. Pritchett
Director
NASA Aviation Safety Program

A Common View of the Development Timeline...





What's Changed?

- An increasing reliance on software, without 'blueprints' and 'load analysis' equivalents during design
 - Instead, just test-test-test of the 'finished' design
- 'Strong coupling' between components
 - Requires combined analysis of their interaction
- Tighter margins and higher safety requirements
 - Wider range of effects must be considering, including human performance and definition of operations
- Long-lifetime of aviation systems, with many subsequent modifications

Impact: Cost, and Constraints on Innovation



Size Comparisons of Embedded Software

System	Lines of Code
Mars Reconnaissance Orbiter	545K
Orion Primary Flight Sys.	1.2M
F-22 Raptor	1.7M
Seawolf Submarine Combat System AN/BSY-2	3.6M
Boeing 777	4M
Boeing 787	6.5M
F-35 Joint Strike Fighter	5.7M
Typical GM car in 2010	100M

NASA Study
Flight Software Complexity, 4/23/2009

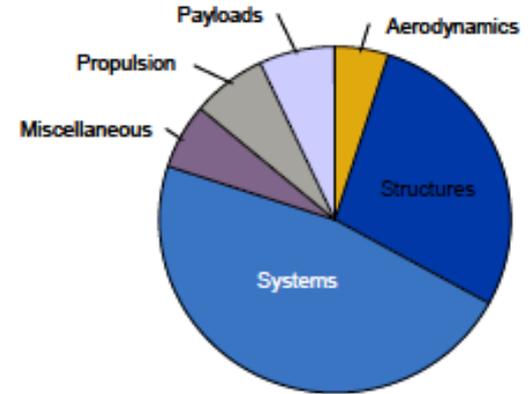
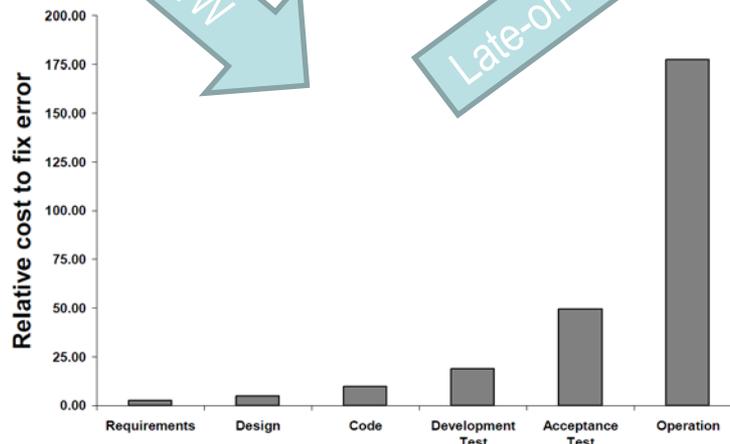


Fig. 1 - Typical Transport Aircraft Development Cost Distribution - Current Generation

Winter, D. (VP, Engineering & IT, Boeing PW)
Testimony to House Committee on Science and Technology, July 31, 2008



Boehm, B. 1981 *Software Engineering Economics*, as cited in DAA, 2008

More S/W

Late-on Testing

And this is just s/w!
Also need to consider human performance, airspace concepts of operation, and new technologies!

Impact: New Types of Safety Issues Fall Through the Cracks



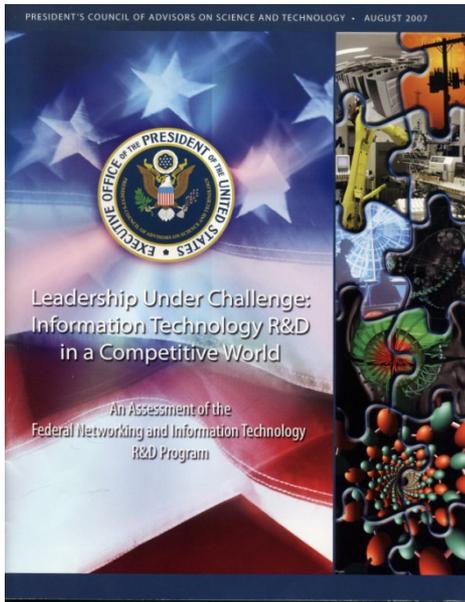
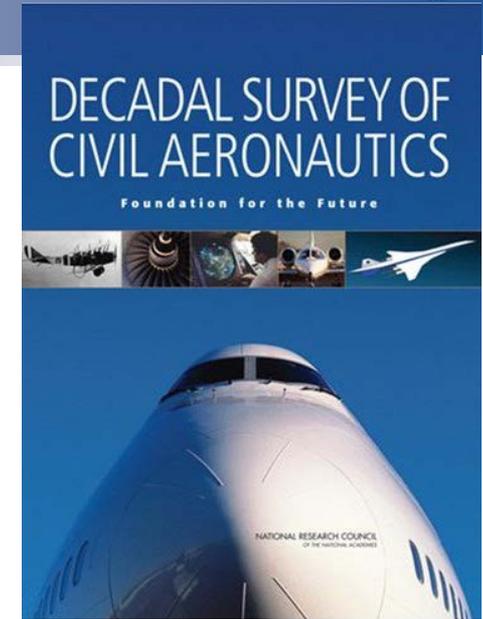
Quantas A330, 7 October 2008 – Bad flight computer response to bad sensor data

Widely Recognized Need for Research



Recommendation 4: Fundamental research is needed to create the foundations for practical certification standards for new technologies

- methods and models are needed for assessing the safety and reliability of complex, large-scale, human-interactive, nondeterministic software intensive systems



"Developers do not have effective ways to model and visualize software complexity, including the possible range of interactions, especially unexpected and anomalous behaviors that can occur among software and hardware components. Developers also do not have time- or cost-effective ways to test, validate, and certify that software-based systems will perform reliability, securely, and safely as intended, particularly under attack or in partial failure."

JPDO Identified Critical Gap in V & V Methods



Summary of NASA Effort To Date

- Goal

Develop verification and validation tools, methods and techniques that advance safety assurance and certification of complex, networked, distributed flight critical systems operating in the Next Generation Air Transportation System

- Objectives

- Meet the JPDO's critical interagency needs associated with V&V research in support of NextGen transformation
- Demonstrate advanced methods to answer relevant questions from aviation community
- Reduce barriers to innovation associated with safety V&V
- Develop V&V methods for safety throughout the entire life cycle

- Currently a *planning* effort conducted on ARRA funds

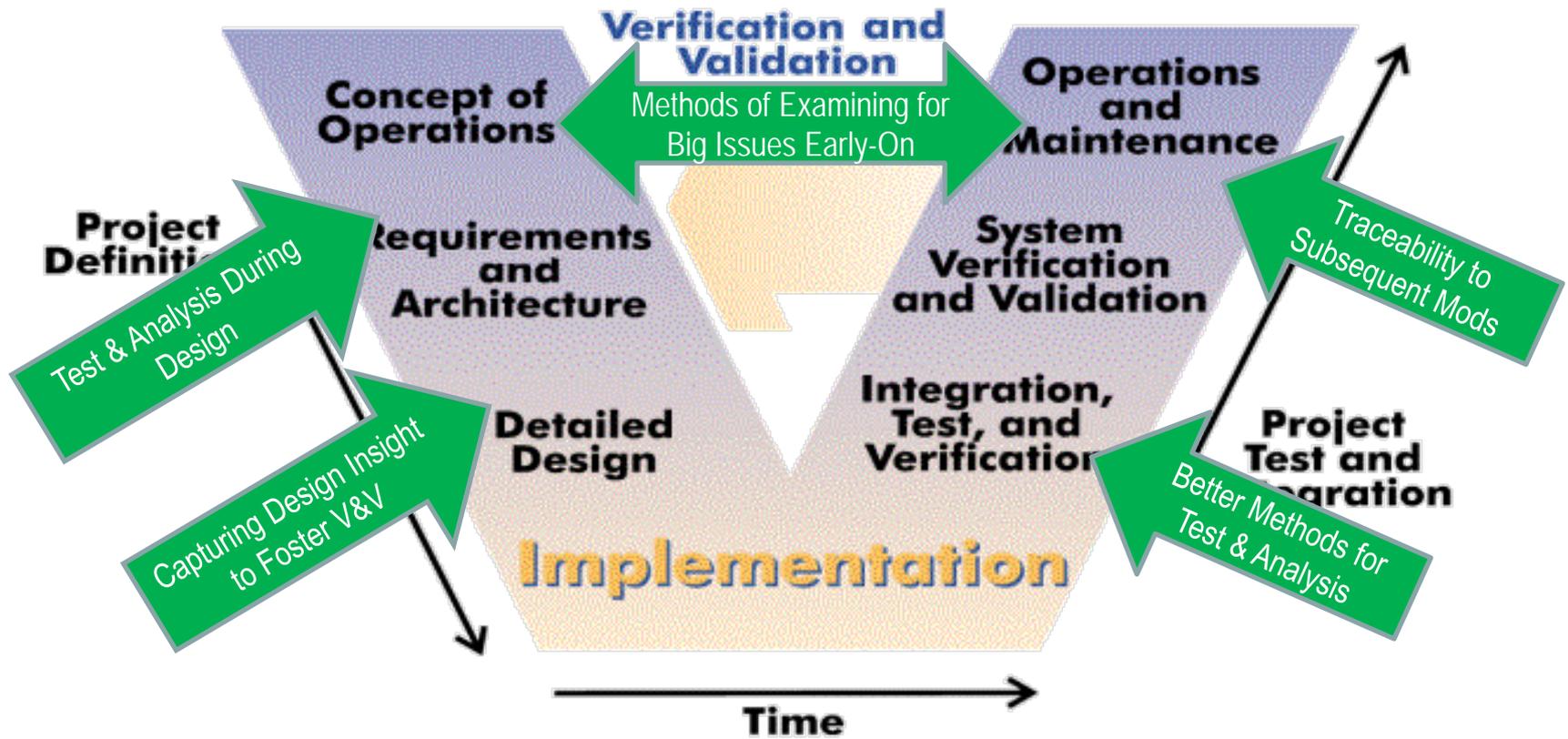
- Assessing research needed to meet these objectives



Scope

- Explicit study of cross-cutting issues in V&V
 - Applicable to a broad range of vehicle and airspace systems
- Focus on the 'safety' aspects
 - Let other research projects focus on their systems' "performance"
- Aware of broader "systems" issues
 - E.g., how will that new flight control systems interact with the entire aircraft data bus and sensor suite?
 - E.g., how to factor in life-cycle and operational concerns?

What We're Seeking





Approach

Common Themes

- Make V & V Cost- and Time-Effective
- Support the Entire Lifecycle
- Consider Disturbances & Degradations
- Humans and Software Are Central

Challenge Areas

- Argument-based Safety Assurance
- Distributed Systems
- Autonomy and Authority
- Software-Intensive Systems

Common Test Cases Applied Throughout

- Vehicle System: Integrated Alerting and Notification
- Airspace

Research Area 1: Argument-based Safety Assurance



- NextGen changes the conventional boundaries and layers -- and, consequently, safety assurance
- We envision a framework that explicitly captures:
 - safety goals/claims/objectives, especially for new functions
 - evidence that goals have been met
 - arguments linking evidence to goals
 - ❖ assumptions, justifications, and other context
- This framework should support design and integration
 - Used to trace conflicts or gaps in assumptions and evidence of combined functioning during component integration
- This framework should support the entire lifecycle
 - Qualitative early in design
 - Endures beyond first design/implementation, to support modification and integration

Research Area 2: Authority and Autonomy



- Authority requires both accountability and capability
 - Need authority aligned with autonomous capabilities
 - Need to avoid competing authorities
 - Need to avoid gaps in authority, maintain clearly who/what is in charge
- We envision methods for early-on assessment of 'big issues':
 - Is authority assigned properly?
 - Is authority assigned with correct assumptions regarding capabilities?
 - Are there conflicts or gaps?

Research Area 3: Flight-Critical Distributed Systems



- Aviation system is a distributed network of distributed systems
- Multiple levels of distribution exist
 - Multi-core processors (system on a chip)
 - Fault-tolerant mechanisms
 - Airspace concepts of operation: Airborne/Space-based/Ground-based
 - Human/Automation
- We envision methods for ensuring robust system performance at all levels of distribution:
 - Distributed across multiple architecture
 - Distributed across multiple air and ground elements
 - Interactions between components as intended
 - Robust to faults, failures and degradations

Research Area 4: Software-Intensive Systems



- NextGen plans increase reliance on software-intensive systems in both ATC and aircraft systems
 - Software will interact with other software, systems, devices, sensors, and with people
- We envision methods for examining software-intensive systems
 - Appropriate extension of formal methods
 - Composition verification
 - Increasing capabilities for numerical calculation
 - Generalized capabilities for software testing throughout coding



Approach

Common Themes

- Make V & V Cost- and Time-Effective
- Support the Entire Lifecycle
- Consider Disturbances & Degradations
- Humans and Software Are Central

Challenge Areas

- Argument-based Safety Assurance
- Distributed Systems
- Autonomy and Authority
- Software-Intensive Systems

Common Test Cases Applied Throughout

- Vehicle System: Integrated Alerting and Notification
- Airspace



Two Application Domains

- Integrated Alerting and Notification concepts, implemented in Integrated, Modular Avionics (IMA) Architecture
 - Dryden Flight Research Center will provide h/w & s/w in the loop test bench at the highest level of fidelity
- High-density merging and spacing operations
 - New procedures and tools for merging and spacing developed by Airspace Super Density Operations effort
 - Also can be tested / demonstrated in high fidelity simulations



In Conclusion: Approach

Common Themes

- Make V & V Cost- and Time-Effective
- Support the Entire Lifecycle
- Consider Disturbances & Degradations
- Humans and Software Are Central

Challenge Areas

- Argument-based Safety Assurance
- Distributed Systems
- Autonomy and Authority
- Software-Intensive Systems

Common Test Cases Applied Throughout

- Vehicle System: Integrated Alerting and Notification
- Airspace



Progress and Next steps

- Continue project formulation activities (Jul-Nov 2009)
- Initiate research activities using FY09 (Jul-Sep2009) and FY10 (Q2FY10) augmentation and recovery act funds
- Coordinate planning with other government agencies
 - Held Interagency Coordination Meeting on Sept 7th, 2009
- Present assessment of critical research areas at NASA Aviation Safety Technical Conference (Nov 17-19, 2009)
 - Near-term research activities (FY09 & FY10)
 - Present assessment of critical long-term research activities

Points of Contact for V&V Assessment of Critical Research Areas



- Amy Pritchett, Director, Aviation Safety Program, amy.r.pritchett@nasa.gov
- John Orme, Technical Integration Manager, Aviation Safety Program, john.s.orme@nasa.gov
- Sharon Graves, Acting Project Manager, sharon.s.graves@nasa.gov
- Guillaume Brat, Acting Project Scientist, guillaume.p.brat@nasa.gov
- Paul Miner, Technical POC for Distributed Systems, p.s.miner@nasa.gov
- Kelly Hayhurst, Technical POC for Safety Assurance, kelly.j.hayhurst@nasa.gov
- Joe Coughlin, Technical POC for Software V&V, joseph.c.coughlan@nasa.gov
- Steve Darr, Planning Team Coordinator, stephen.t.darr@nasa.gov

Thank You!



Thoughts, questions?

