Assurance of Software-Intensive Flight Critical Systems:

A plan for enabling validation & verification in NextGen

Dr. Misty Davies
Research Computer Engineer
NASA Ames Research Center
For the Complex Aerospace Systems Exchange
September 12, 2012

The Plan:
A Framework for Getting...

...From NearGen to FarGen.

The Goal is to Maintain Safety While...

...Reducing the Cost of Verification and Validation...

...By Pushing V&V Earlier in the Lifecycle...

...and Using Advanced Techniques.

Why do we need to do V&V differently?

1. NextGen is complex
2. JPDO Integrated Work Plan
Assurance of Software-Intensive Flight Critical Systems:
A plan for enabling validation & verification in NextGen

Dr. Misty Davies
Research Computer Engineer
NASA Ames Research Center
For the Complex Aerospace Systems Exchange
September 12, 2012
Why do we need to do V&V differently?

1. NextGen is complex

2. JPDO Integrated Work Plan

http://jpe.jpdo.gov/ee/request/home
Leadership Under Challenge: Information Technology R&D in a Competitive World

An Assessment of the Federal Networking and Information Technology R&D Program
Critical Gap in V&V Methods:

"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."
PDO Integrated Work Plan

http://jpe.jpdo.gov/ee/request/home
Advanced Validation and Verification Methods as an Enabler for NextGen

EN-3050 Advanced Complex System Validation and Verification Methods

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>EN-3050 Advanced Complex System Validation and Verification Methods</td>
</tr>
<tr>
<td>Text Id</td>
<td>EN-3050</td>
</tr>
<tr>
<td>Description</td>
<td>Advanced tools and processes are developed to improve the verification and validation of complex systems and software. Improvements will focus on reducing the time and resources needed to conduct validation and verification as well as improving the quality of the results. The advanced tools and processes will be created using the combined results of analysis, research and development. Advanced tools and processes such as fast time, real time, and human in the loop simulations will be used to test and evaluate complex systems and software. They will replace and substitute for exhaustive testing. The tools and processes will provide estimates of system risks associated with complex system and software deployment. They will use standards protocols for system simulation and support the creation of a standard protocol for implementation. The tools and processes will establish the minimum acceptability criteria and risk standards applied for Validation and Verification (V&amp;V).</td>
</tr>
<tr>
<td>Grouping</td>
<td>Safer Practices Enablers</td>
</tr>
<tr>
<td>Planning Initial Availability</td>
<td>2017</td>
</tr>
<tr>
<td>OPR/Reference No.</td>
<td>FAA (Suggested)</td>
</tr>
<tr>
<td>OCR/Reference No.</td>
<td>NASA</td>
</tr>
</tbody>
</table>
### Advanced Complex System Validation and Verification Methods

**EN-3050**

Advanced tools and processes are developed to improve the verification and validation of complex systems and software. Improvements will focus on reducing the time and resources needed to conduct validation and verification as well as improving the quality of the results. The advanced tools and processes will be created using the combined results of analysis, research and development. Advanced tools and processes such as fast time, real time, and human in the loop simulations will be used to test and evaluate complex systems and software. They will replace and substitute for exhaustive testing. The tools and processes will provide estimates of system risks associated with complex system and software deployment. They will use standards protocols for system simulation and support the creation of a standard protocol for implementation. The tools and processes will establish the minimum acceptability criteria and risk standards applied for Validation and Verification (V&V).

### Safer Practices Enablers

2017

FAA (Suggested)

NASA
The Goal is to Maintain Safety While . . . .

. . . By Pushing V&V Earlier in the Lifecycle . . . .

. . . Reducing the Cost of Verification and Validation . . . .

For FAA-compliant airborne systems software in which a failure would be catastrophic (DO178B Level A) industry spends 7 times as much on verification (reviews, analysis, test) as it does for development. (12% development, 88% for verification)

For similar software in which a failure would only be hazardous (DO178B Level B) verification cost is reduced by approximately 15%. (25% development, 75% verification)

. . . and Using Advanced Techniques.

Why do we need to do V&V differently?
Reducing the Cost of Verification and Validation

For FAA-compliant airborne systems software in which a failure would be catastrophic (DO178B Level A) industry spends 7 times as much on verification (reviews, analysis, test) as it does for development. (12% development, 88% for verification)

For similar software in which a failure would only be hazardous (DO178B Level B) verification cost is reduced by approximately 15%. (25% development, 75% verification)

and Using Advanced Techniques.
The average software defect rate in the U.S. in 2000 was 5.9 to 7 defects per 1000 SLOC.

Between 1997-1998 and 1999-2000, software defect rates increased 15%.

Capers Jones. Software Assessments, Benchmarks and Best Practices.


Data adapted from online article:
"Electronic design automation (EDA) tools aim to enhance efficiency in aerospace and defense electronics design" Last accessed 22 Aug 2012
By Pushing V&V Earlier in the Lifecycle

Onboard Source Lines of Code (SLOC) Per Year

Constructive Cost Model (COCOMO II) says the cost of this line >$10B

Trendline shows that SLOC doubles approximately every 4 years.

SLOC (Thousands)

Year


The average software defect rate in the U.S. in 2000 was 5.9 to 7 defects per 1000 SLOC.

Between 1997-1998 and 1999-2000, software defect rates increased 15%.

Cost to Fix a Software Defect, Given the Stage in Which it is Detected

Adjusting for inflation, the cost to fix a defect in the requirements stage was $174.21 in 2010.

When Are Defects Introduced?

Data Source: CrossTalk, the journal of defense Software Engineering

Data Source: Capers Jones, Software Assessments, Benchmarks and Best Practices, 2000
Cost to Fix a Software Defect, Given the Stage in Which it is Detected

Adjusting for inflation, the cost to fix a defect in the requirements stage was $174.21 in 2010.

When Are Defects Introduced?

Data Source: Capers Jones. Software Assessments, Benchmarks and Best Practices. 2000

Data Source: Crosstalk, the Journal of Defense Software Engineering
... and Using Advanced Techniques.

Verification cost is reduced by approximately 15%. (25% development, 75% operation)
The Plan:

A Framework for Getting . . .

. . . From NearGen to FarGen.
A Framework for Getting . . . .

- Argument-Based Safety Assurance
  - Safety Requirements
  - Evidence
- Distributed Systems
- Software Intensive Systems
- Authority & Autonomy

A Realistic Test Bed
... From NearGen to FarGen.
IKOS due to be released as Open Source software under NOSA

IKOS (Inference Kernel for Open Static analyzers),
- a high-performance static analysis platform based on Abstract Interpretation and developed at NASA,
- demonstrated to yield low false positive rates (<5%)
- on embedded avionic code up to 270 KLOC,
- with analysis times ranging in minutes on a laptop.
... From NearGen to FarGen.
Assurance of Software-Intensive Flight Critical Systems:
A plan for enabling validation & verification in NextGen

Dr. Misty Davies  
Research Computer Engineer  
NASA Ames Research Center  
For the Complex Aerospace Systems Exchange  
September 12, 2012

The Plan:
A Framework for Getting . . . .  
. . . From NearGen to FarGen.

The Goal is to Maintain Safety While . . . .
. . . By Pushing V&V Earlier in the Lifecycle . . . .
. . . Reducing the Cost of Verification and Validation . . . .
. . . and Using Advanced Techniques.

Why do we need to do V&V differently?
1. NextGen is complex
2.  
3. JPDO Integrated Work Plan

http://casa.arc.nasa.gov/research/home