

# Assurance of Software-Intensive Flight Critical Systems:

A plan for enabling validation & verification in NextGen



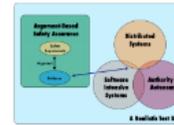
Dr. Misty Davies

Research Computer Engineer  
NASA Ames Research Center

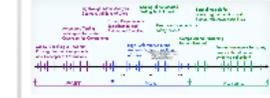
For the Complex Aerospace Systems Exchange  
September 12, 2012

## The Plan:

A Framework for Getting . . . .



. . . From NearGen to FarGen.



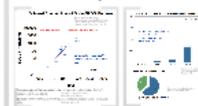
## The Goal is to Maintain Safety While . . . .

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

For FAA-compliant airborne systems software in which a failure would be catastrophic (DO178B Level A) industry spends 7 times as much on verification (review, 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)

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

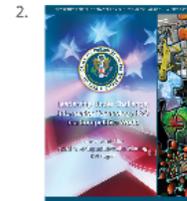


. . . and Using Advanced Techniques.



## Why do we need to do V&V differently?

1. NextGen is complex



3. JPDO Integrated Work Plan



<http://jipo.jpdo.gov/ee/request/home>

# Assurance of Software-Intensive Flight Critical Systems:

A plan for enabling validation & verification in NextGen



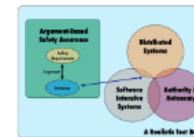
**Dr. Misty Davies**

Research Computer Engineer  
NASA Ames Research Center

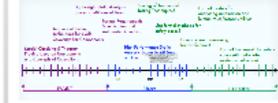
**For the Complex Aerospace Systems Exchange  
September 12, 2012**

## The Plan:

A Framework for Getting . . .



. . . From NearGen to FarGen.



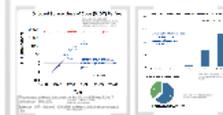
## The Goal is to Maintain Safety While . . .

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

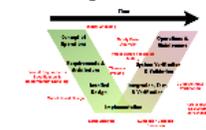
For FAA-compliant airborne systems software in which a failure would be catastrophic (DO178B Level A) industry spends 7 times as much on verification (reviews, analysis, test) as it does for development. (12% development, 88% for verification)

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)

. . . 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.



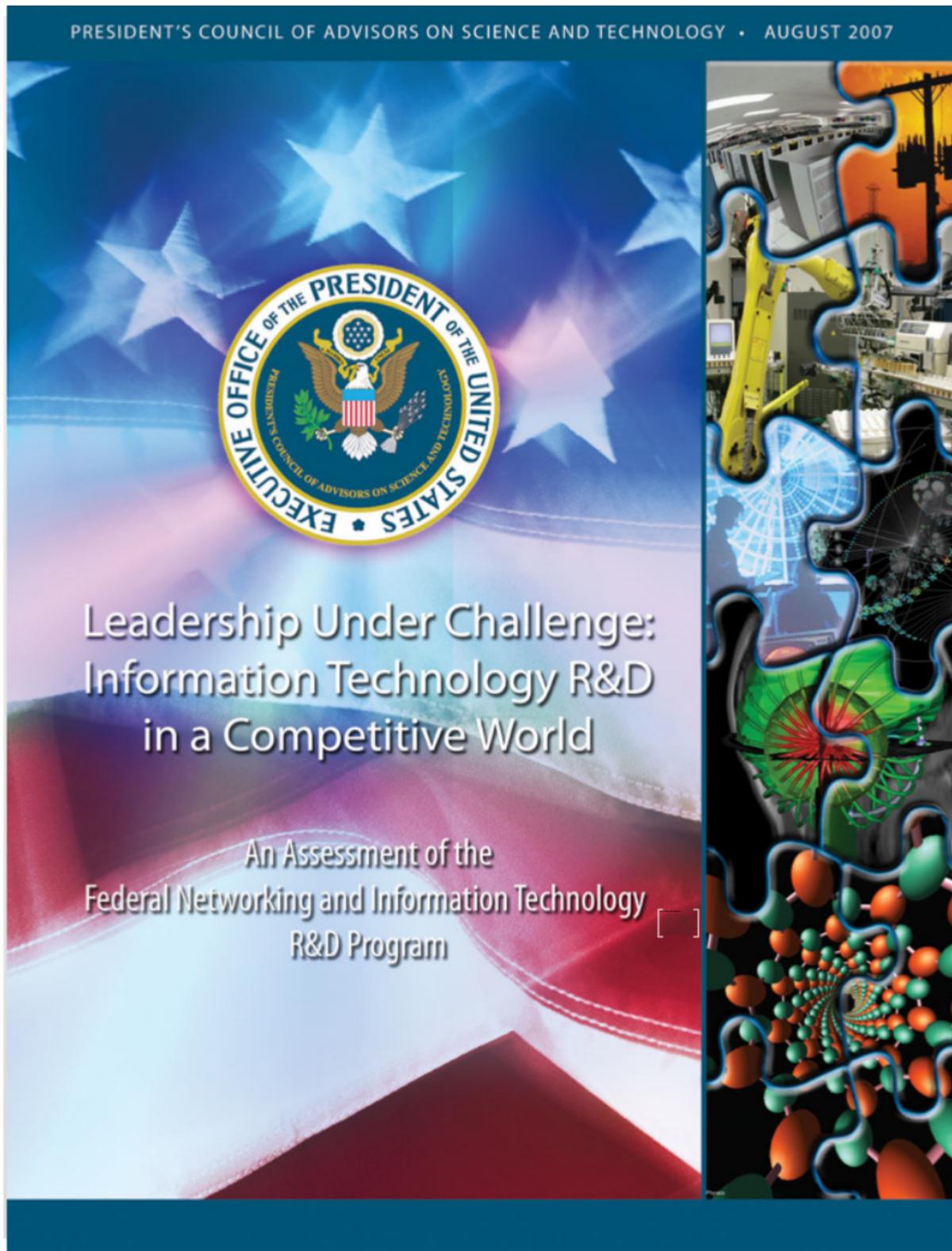
3. JPDO Integrated Work Plan



<http://jpe.jpdo.gov/ee/request/home>



2.



3. JP

## 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."

# JPDO Integrated Work Plan

The screenshot shows the JPDO NextGen Joint Planning Environment (JPE) website. At the top left is the JPE logo with the text "JOINT PLANNING ENVIRONMENT POWERED BY JPDO". To the right of the logo is a login section with fields for "Username:" and "Password:", and buttons for "Register", "Login", and "Search". Below the logo is a navigation menu with items: Overview, ConOps, Glossary, IWP, and Reports. A breadcrumb trail shows the path: Home > IWP > Er > Er > Se > Sa > Safer Practices Enablers > NextGen JPDO Joint Planning Environment (JPE).

**Headlines**

- [IWP FY14 R1 Released](#)
- [Enterprise Architecture Now in Secured Area \(May 25, 2011\)](#)
- [Access the JPE Help Video](#)  
*Quick Video Tutorial For Using the JPE Effectively!*

**Welcome to the JPDO NextGen Joint Planning Environment (JPE)**

The JPDO NextGen Joint Planning Environment (JPE) is a web-accessible application which serves as a foundation for collaboration, alignment, analysis and integration of NextGen related activities among the JPDO's partners and NextGen stakeholders. This application allows the JPDO to communicate NextGen planning information in a clear and concise way to partner agencies and stakeholders more quickly, with additional features not possible via paper based publication.

Using the JPE, NextGen partner agencies and stakeholders may search across NextGen work products, view data by agency, data element type, or agency specific framework. Users also have the ability to view detailed reports, charts, and graphs.

By integrating this information and presenting it via a Web based interface, users will be able to gain further insight and make meaningful decisions that may not be possible via a paper based, non-integrated approach to consuming these work products.

**Integrated Work Plan**

**Concept of Operations**

**Joint Planning Framework**

**Reports**

*Hover over any menu item to see more information. Click on the menu item to access the information.*

The JPDO's Joint Planning Environment has been updated to provide enhancements that enable...

<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

  
Enabler [IWP FY14 R1] - 1020335

### Related Reports

 EN Timetable

EN Timetable

### Attributes

Attribute	Value
  <b>Name</b>	Advanced Complex System Validation and Verification Methods
  <b>Text Id</b>	EN-3050
  <b>Description</b>	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).
  <b>Grouping</b>	<a href="#">Safer Practices Enablers</a>
  <b>Planning Initial Availability</b>	2017
  <b>OPR/Reference No.</b>	FAA (Suggested)
  <b>OCR/Reference No.</b>	NASA

# an Enabler for NextGen . . . .

## EN Timetable

### Value

#### 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

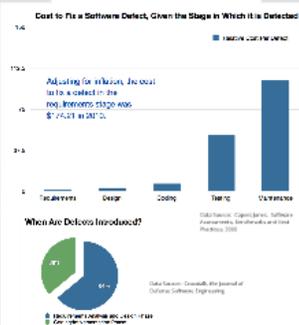
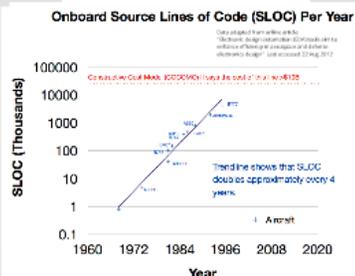
# The Goal is to Maintain Safety While . . . .

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

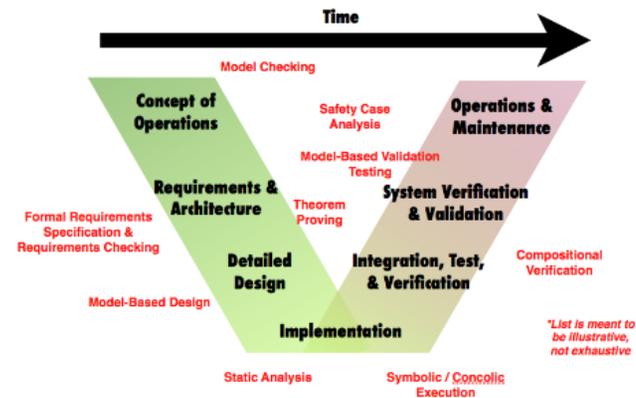
For FAA-compliant airborne systems software in which a failure would be catastrophic (DO178B Level A) industry spends 7 times as much on verification (reviews, analysis, test) as it does for development. (12% development, 88% for verification)

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)

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



## . . . and Using Advanced Techniques.



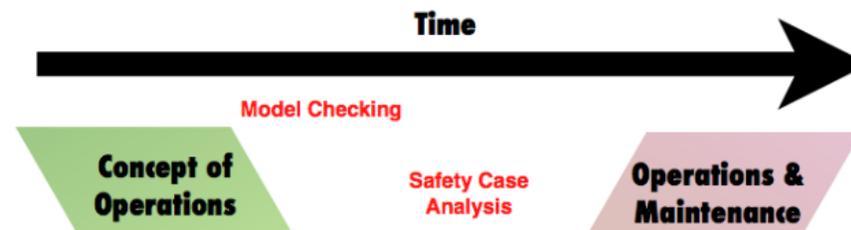
# Why do we need to do V&V differently?

## ... 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)

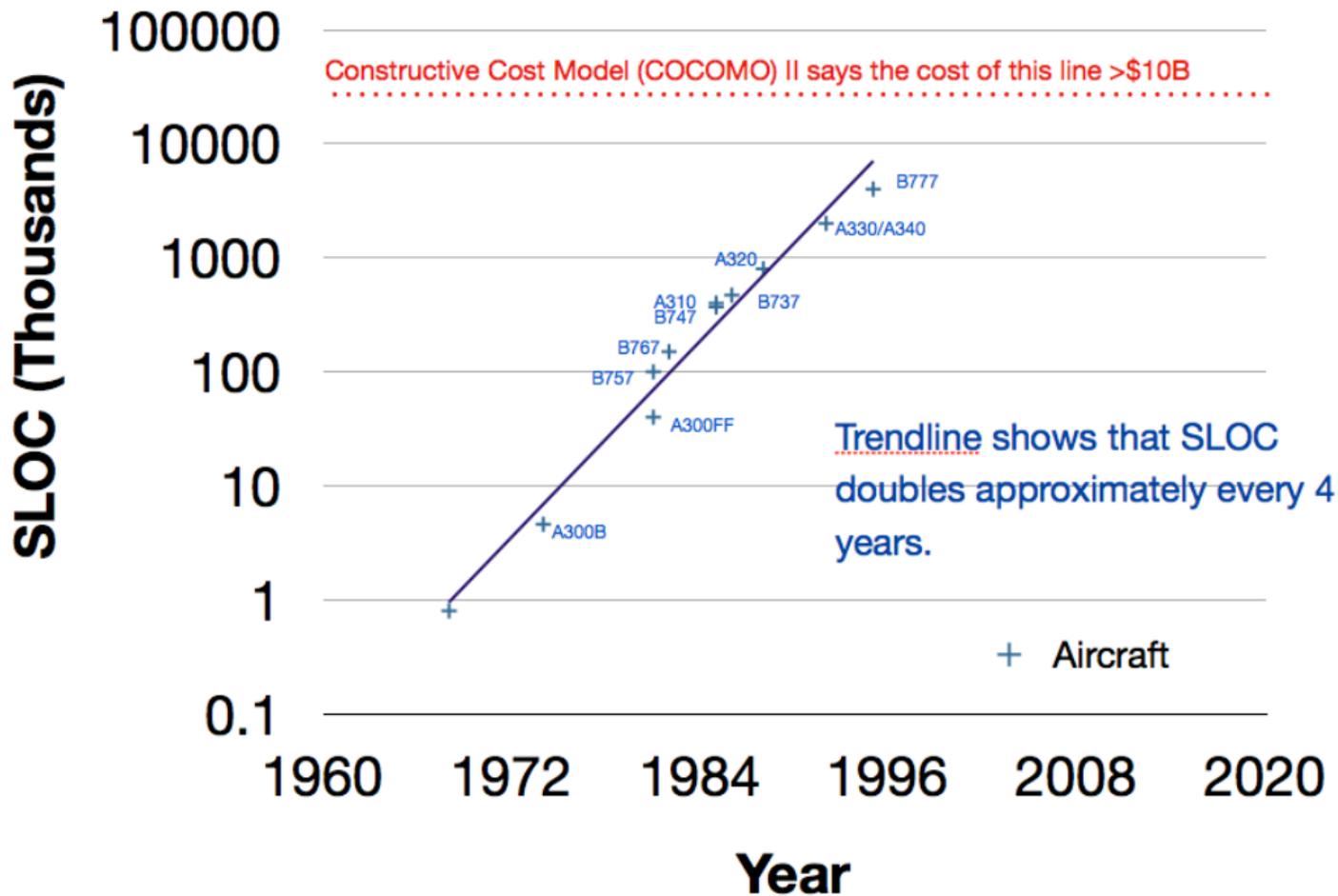
For similar software in which a failure would only be hazardous (DO178B Level B) verification cost is reduced by approximately 15%. (25% development, 75% verification)

## ... and Using Advanced Techniques.



# Onboard Source Lines of Code (SLOC) Per Year

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



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

Capers Jones. Software Assessments, Benchmarks and Best Practices.

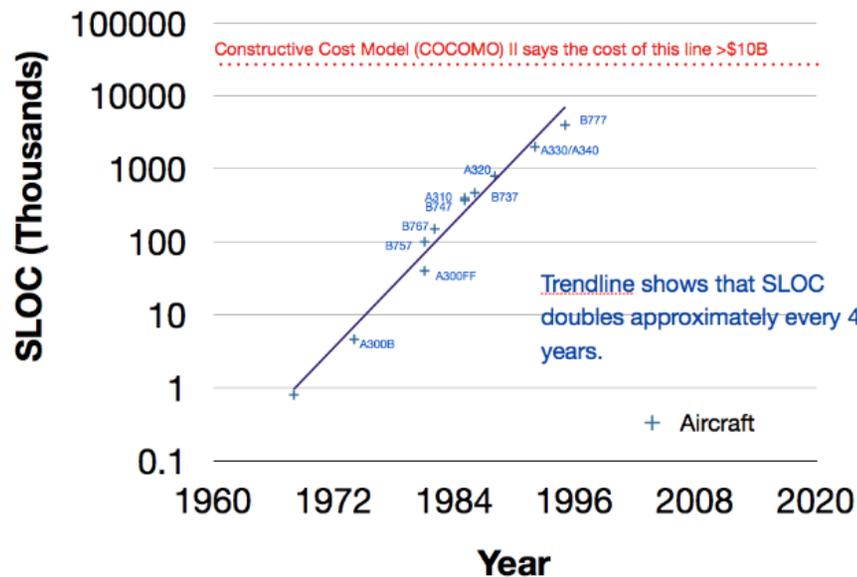
Between 1997-1998 and 1999-2000, software defect rates increased 15%.

Meta Group. January 2002

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

## Onboard Source Lines of Code (SLOC) Per Year

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



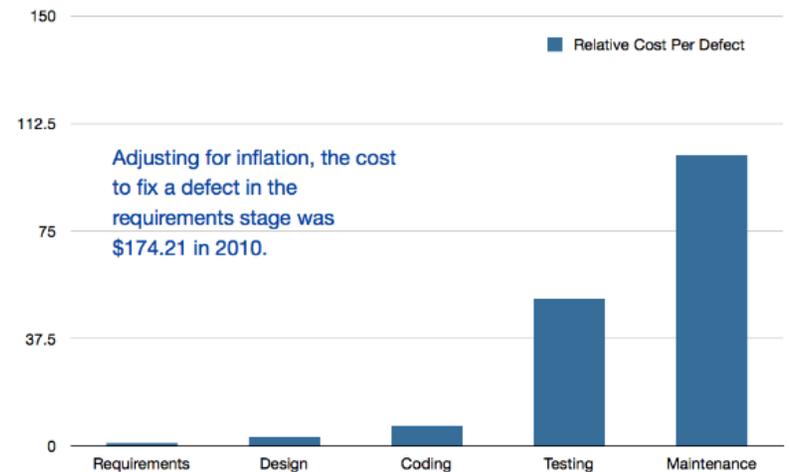
The average software defect rate in the U.S. in 2000 was 5.9 to 7 defects per 1000 SLOC.

Capers Jones. Software Assessments, Benchmarks and Best Practices.

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

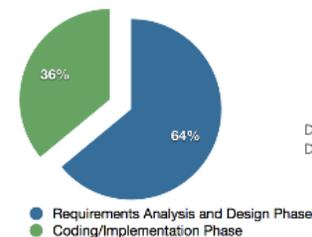
Meta Group, January 2002

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



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

## When Are Defects Introduced?



Data Source: Crosstalk, the Journal of Defense Software Engineering

# Year

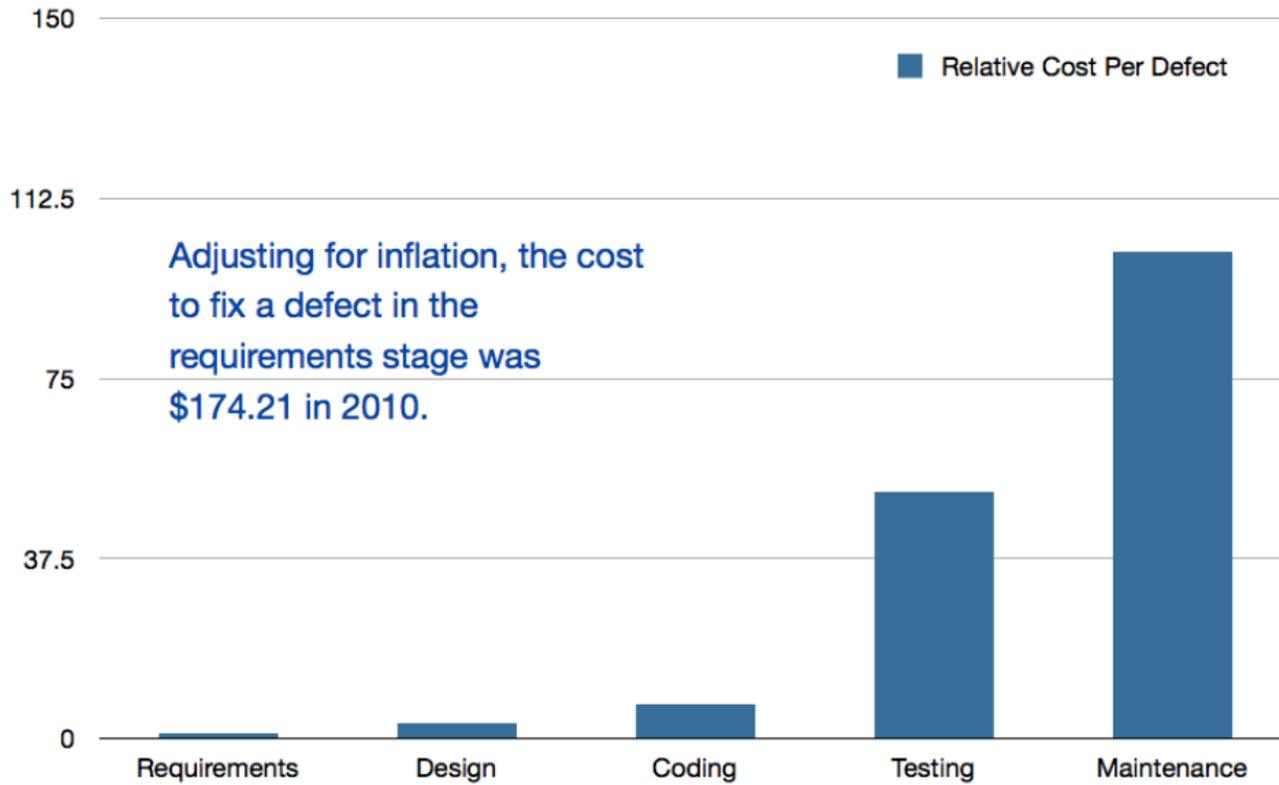
s aim to  
ense  
g 2012

C  
ery 4

20

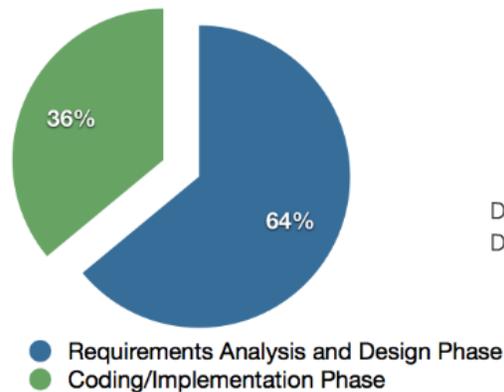
ased

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



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

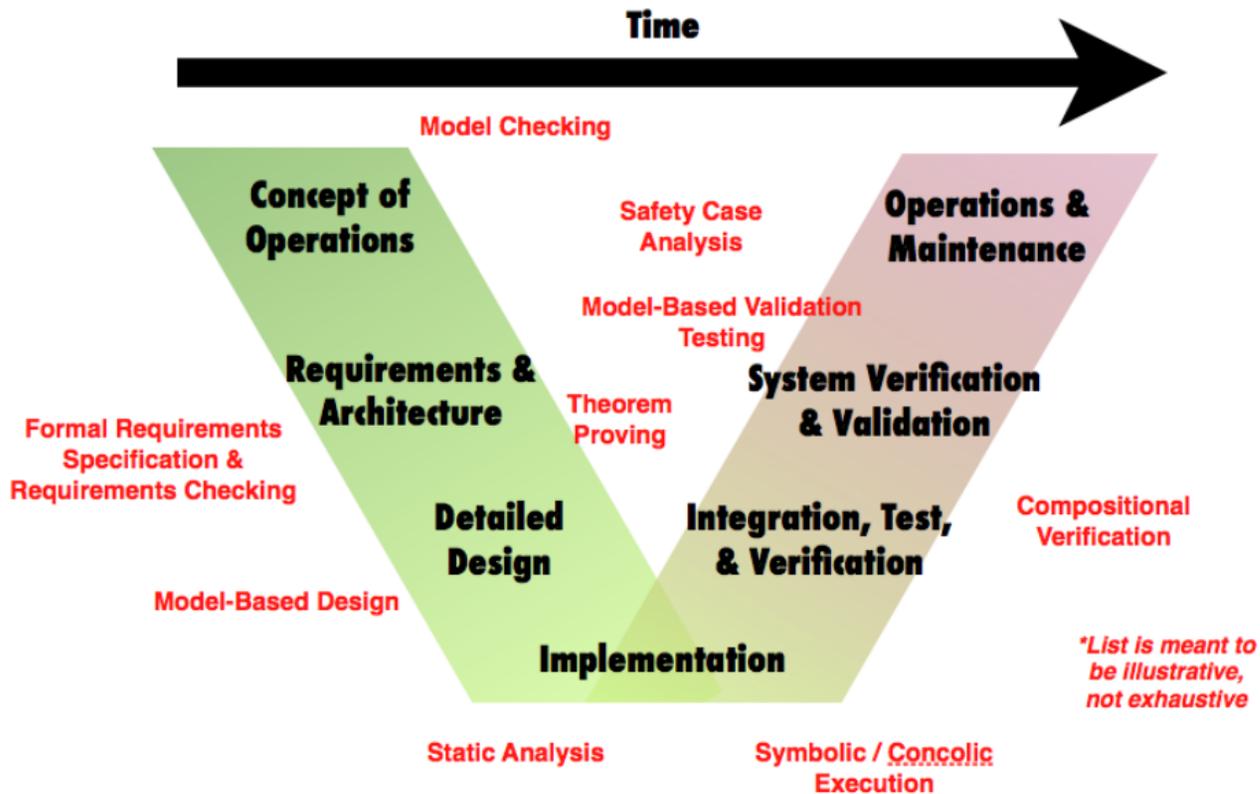
## When Are Defects Introduced?



Data Source: Crosstalk, the Journal of Defense Software Engineering

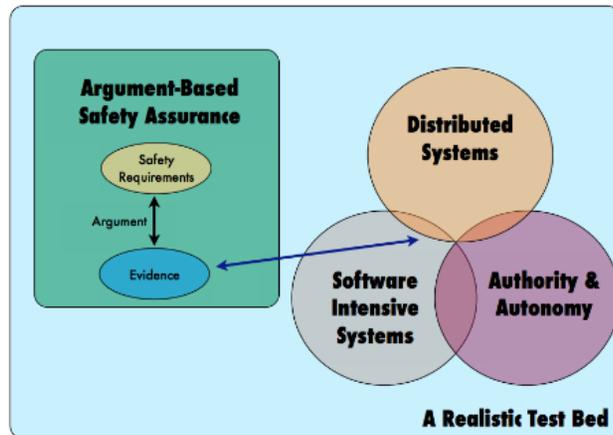
ification cost is reduced by approximately 15%. (25% development, 75%  
ation)

## ... and Using Advanced Techniques.

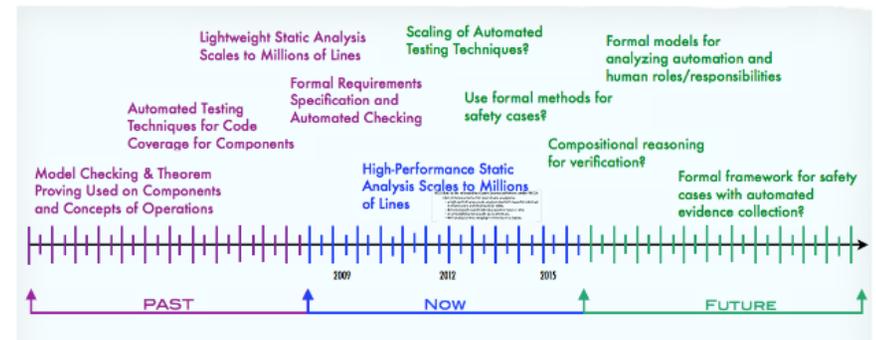


# The Plan:

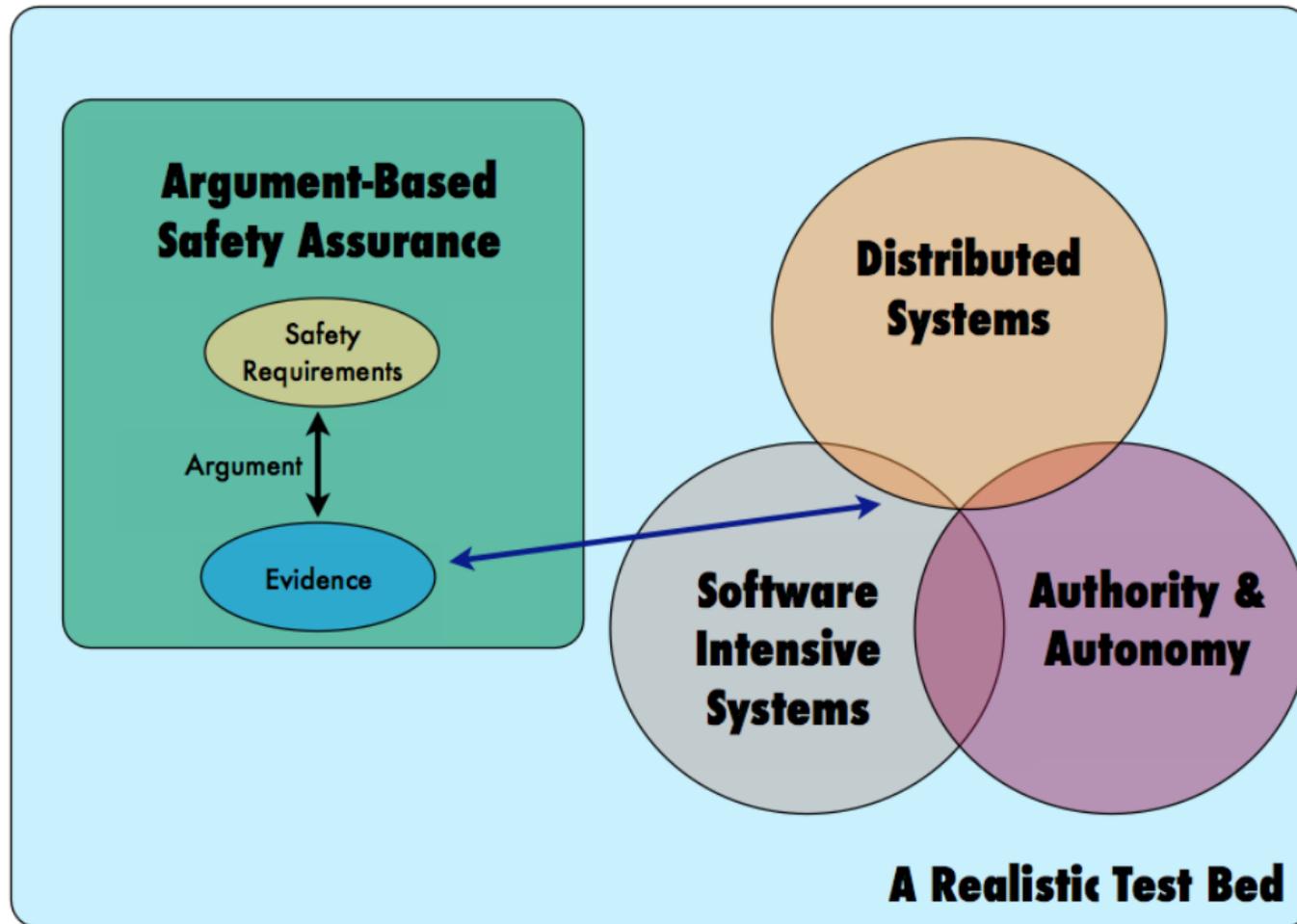
## A Framework for Getting . . . .



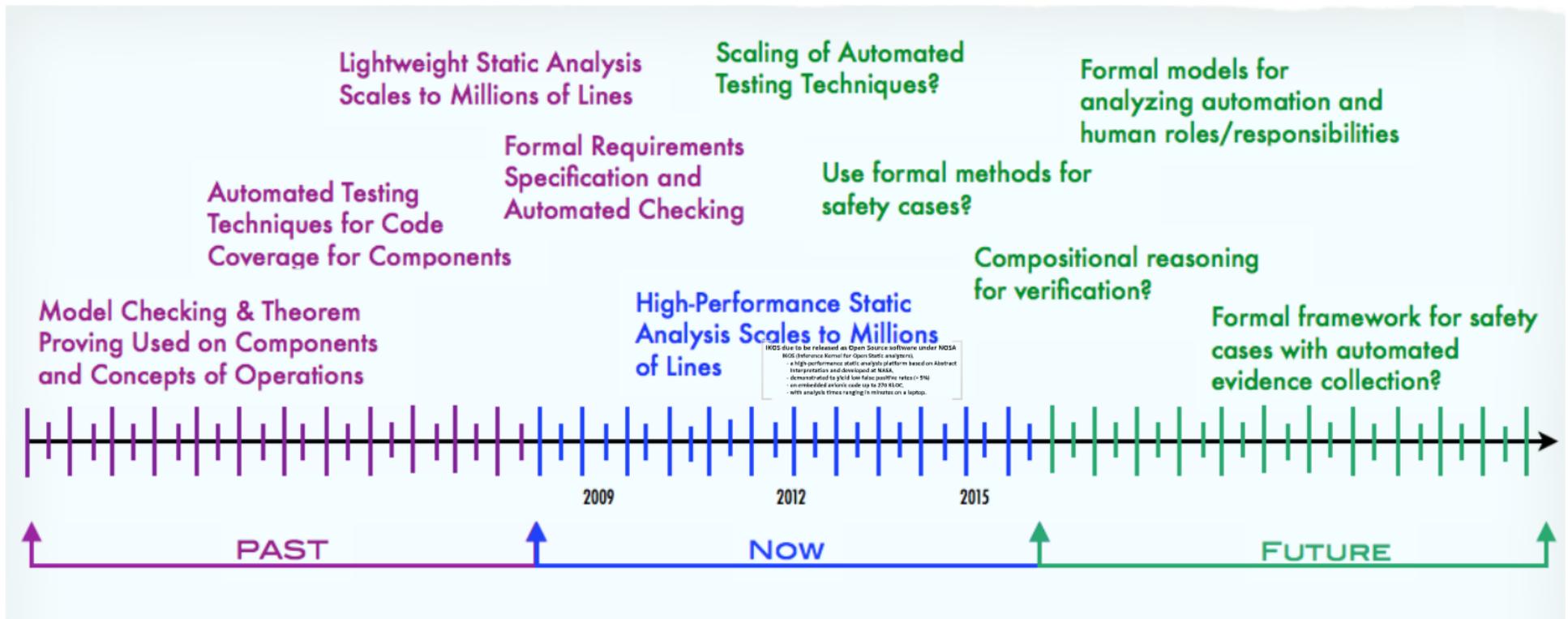
## . . . From NearGen to FarGen.



# A Framework for Getting . . . .



# ... From NearGen to FarGen.



# Performance Static sales to Millions

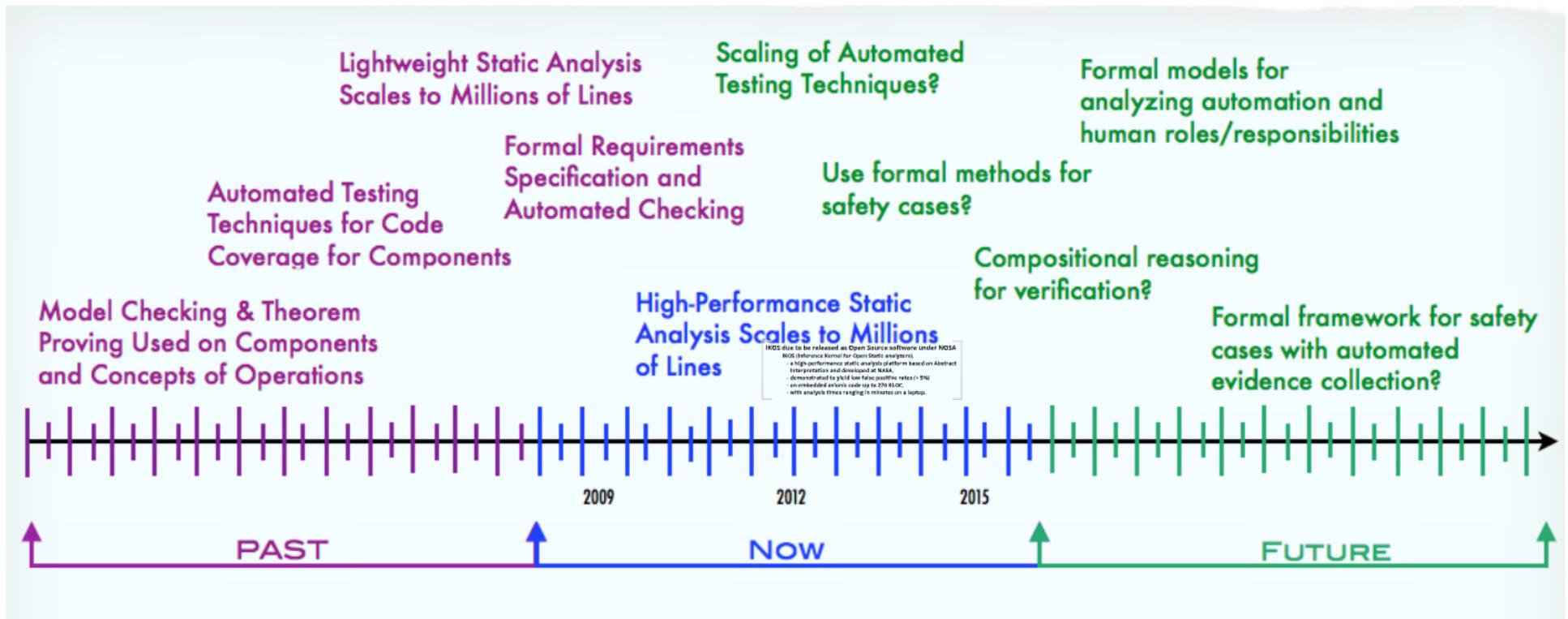
**IKOS due to be released as Open Source software under NOSA**

**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



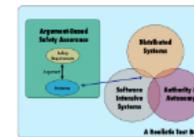
**Dr. Misty Davies**

Research Computer Engineer  
NASA Ames Research Center

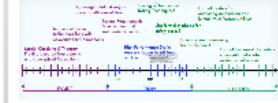
**For the Complex Aerospace Systems Exchange  
September 12, 2012**

## The Plan:

A Framework for Getting . . .



. . . From NearGen to FarGen.



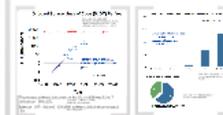
## The Goal is to Maintain Safety While . . .

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

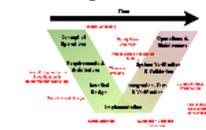
For FAA-compliant airborne systems software in which a failure would be catastrophic (DO178B Level A) industry spends 7 times as much on verification (reviews, analysis, test) as it does for development. (12% development, 88% for verification)

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)

. . . 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.



3. JPDO Integrated Work Plan



<http://jpe.jpdo.gov/ee/request/home>