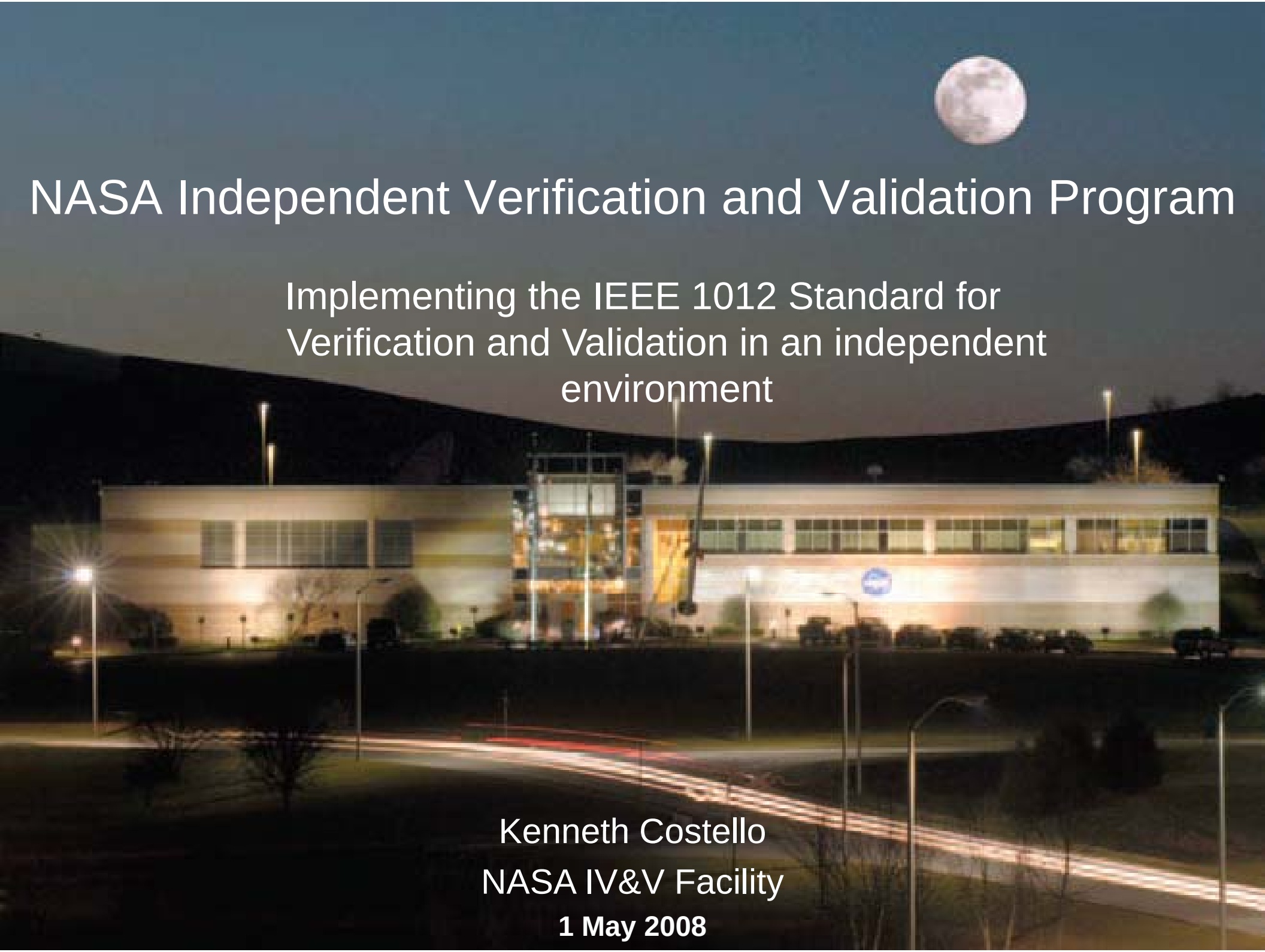


NASA Independent Verification and Validation Program

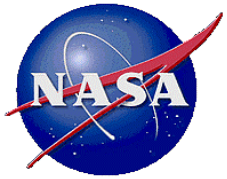
Implementing the IEEE 1012 Standard for Verification and Validation in an independent environment

Kenneth Costello

NASA IV&V Facility

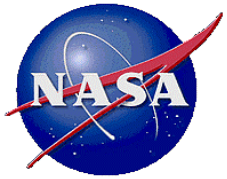
1 May 2008

Agenda



- IV&V at NASA
- The IEEE 1012 Standard
- Developing an IV&V WBS
- Developing a method for determining tasking
- Future of the standard and NASA IV&V
- Summary

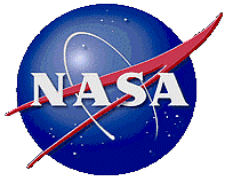
Agenda



IV&V Program

- IV&V at NASA
- The IEEE 1012 Standard
- Developing an IV&V WBS
- Developing a method for determining tasking
- Future of the standard and NASA IV&V
- Summary

IV&V at NASA

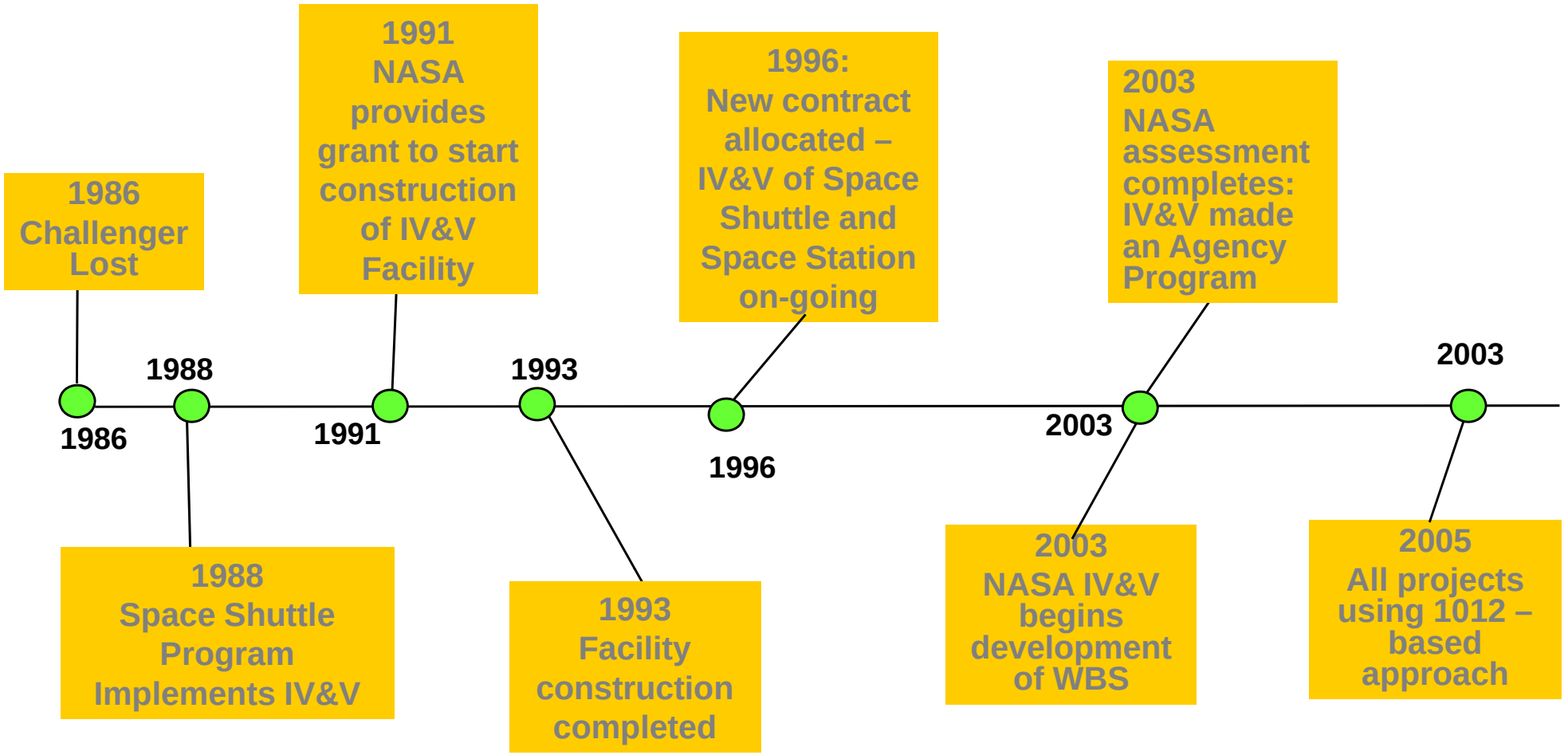


IV&V Program

- IV&V grew out of the Challenger accident in 1986
- IV&V implemented on the Space Shuttle Program initially
- NASA wanted to further expand IV&V
  - Technical Independence: Achieved by IV&V personnel who use their expertise to assess development processes and products independent of the developer
  - Managerial Independence: Requires responsibility for the IV&V effort to be vested in an organization separate from the organization responsible for performing the system implementation
  - Financial Independence: Requires that control of the IV&V budget be vested in an organization independent of the development organization

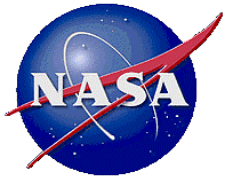
Brief History of IV&V at NASA

IV&V Program



- The goal of IV&V is to provide a higher level of confidence that the software will be fit for operation and satisfy its requirements for safety, availability, quality and function
  - The goal is achieved by performing engineering analysis focused on identifying defects in development artifacts
  - The IV&V team identifies risks that may be present due to poor development processes or incomplete development efforts

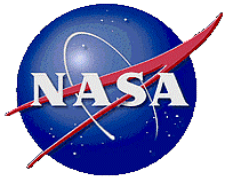
Agenda



IV&V Program

- IV&V at NASA
- The IEEE 1012 Standard
- Developing an IV&V WBS
- Developing a method for determining tasking
- Future of the standard and NASA IV&V
- Summary

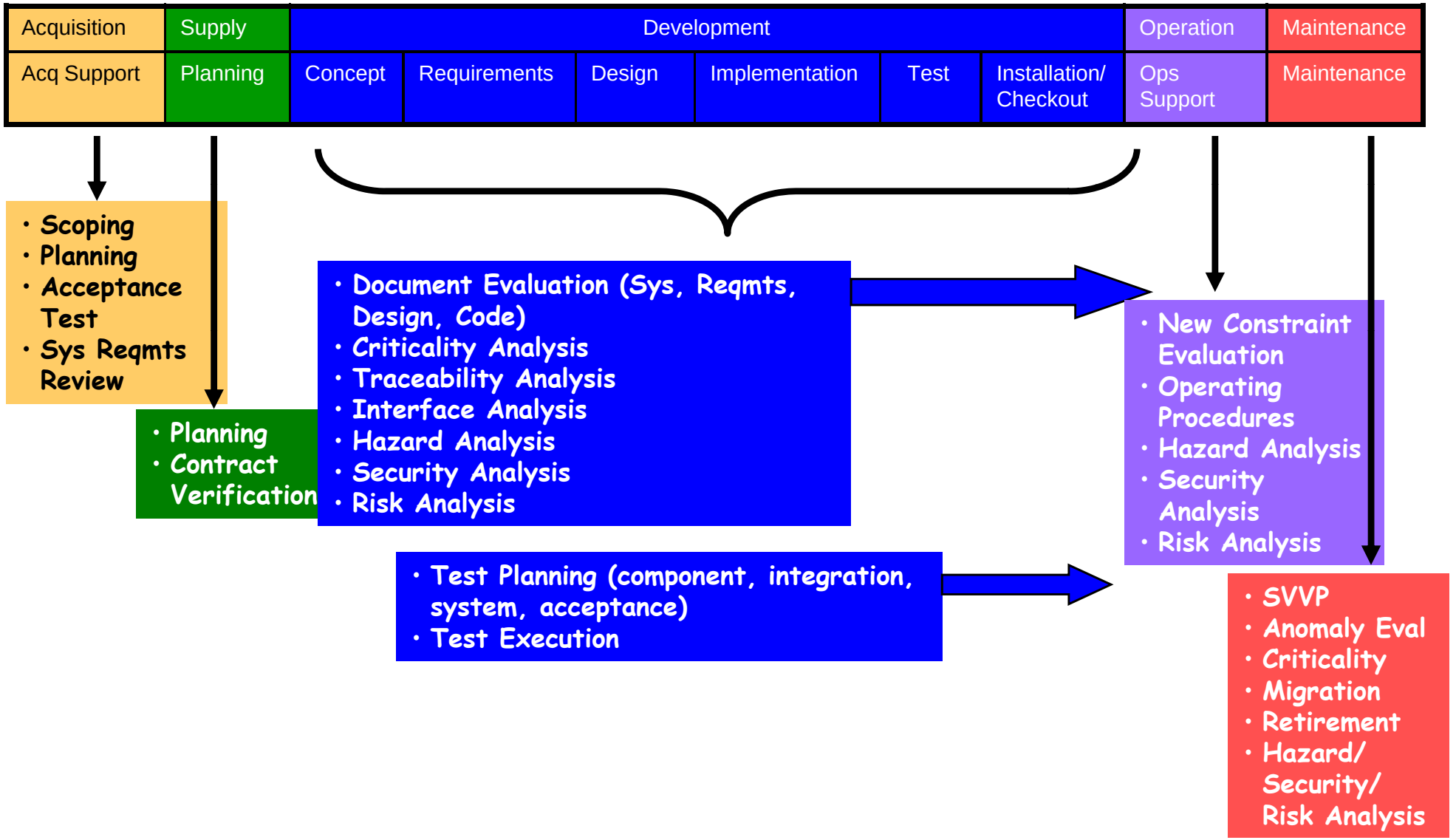
What does IEEE 1012 cover?



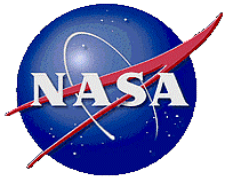
- The focus of IEEE 1012 is on the verification and validation of software within the context of the system being developed
- It views V&V as a systems engineering discipline
  - What role does the software play in the system?
  - Is it critical to mission success or have safety implications?
  - Does it provide only information? Does it control other components?
- It is performed in parallel with the developer's efforts – It is not something that is only applied at the end of the project
- Since software directly affects system behavior and performance, the scope of V&V processes is the software system, including the operational environment, operators and users, hardware, and interfacing software

Overview of IEEE 1012

IV&V Program



Agenda



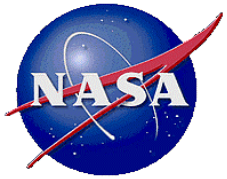
IV&V Program

- IV&V at NASA
- The IEEE 1012 Standard
- Developing an IV&V WBS
- Developing a method for determining tasking
- Future of the standard and NASA IV&V
- Summary

The Starting Point

- Prior to instantiation as a program IV&V tasking was abstract
  - Terminology not always consistent
  - Specific tasking not determined prior to beginning work
- Led to issues communicating with projects
  - Once work started definition clarified
  - Effort to get start larger than expected
  - Finding of the assessment team
- Needed to develop a WBS that communicated tasking prior to work being performed
  - Important for communication with project
  - Important for estimating effort needed

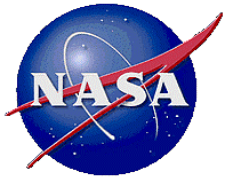
Using IEEE 1012: Similarities and Differences



IV&V Program

- Similarities
  - Goals are the same
    - Find defects throughout the life cycle
    - Provide information back to the development project
  - Approach is the same
    - System engineering discipline
    - Understand role of software within the system
- Differences
  - Provided needed task definitions
  - Provided insight into how to determine and plan tasking
- The standard fit within our approached and goals and provided the information we were seeking

An Adaptation



IV&V Program

- NASA IV&V was not looking to be standard compliant
- Standard used as a source of foundation on which to build an approach that met our needs
- Focus was on development tasks
  - NASA currently had a management system
  - Provided process for planning, etc.
- Approach was to compare tasks in standard with current abstract approach and determine where to drill down
- In the end, our adaptation is rather straight forward

Adapting the Standard to NASA IV&V

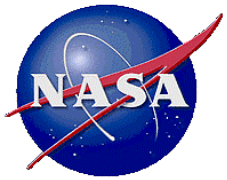
IV&V Program

Acquisition	Supply	Development						Operation	Maintenance
Acq Support	Planning	Concept	Requirements	Design	Implementation	Test	Installation/ Checkout	Ops Support	Maintenance

- **Phase Independent Tasking**
- **Phase Dependent Tasking**

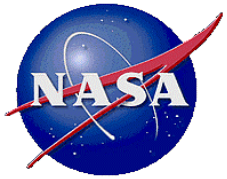
- 1012 Standard has 6 distinct types of tasks – Life cycle phases shown above, plus management (not shown above)
- Processes already existed to cover most management, acquisition and supply
- Divided 6 phases into two – Phase Independent and Phase Dependent

NASA Phases



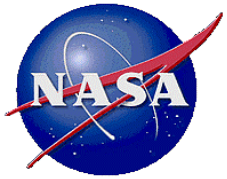
- Phase Independent Tasking
  - Tasks not directly associated with artifact analysis
  - Management and planning, issue tracking, process improvement, analysis tool support etc
- Phase Dependent Tasking
  - Tasks directly associated with artifact analysis
  - Further decomposed into artifact types or phases based on the life cycle phases in the standard
    - Concept, Requirements, Design, Implementation, Test, Installation/Checkout, Operations and Maintenance
  - IV&V scope usually ended with the launch of a vehicle
    - Installation/Checkout dropped
    - In the initial iterations Operations and Maintenance were included – eventually dropped also due to IV&V scope

Other Changes



- In addition to generating a task grouping, specific task changes were also made
- Related to differences in the concept of V&V versus IV&V, at least from the NASA perspective
- The standard focuses first on V&V
  - Includes the development of what might be seen as development artifact
  - Specific examples are in the testing area
- NASA IV&V focuses on analyzing development artifacts not generating
- Example
  - Standard has a task for Software Integration Test Plan Generation
  - NASA adapted the task to Software Integration Test Plan Analysis
  - Resulted in changes to wording in the task in addition to title

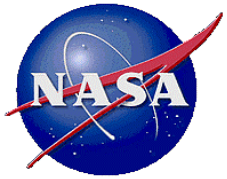
Adapting the Standard was not Difficult



IV&V Program

- Straight-forward Process with changes as noted
- A traceability matrix was created to show how the standard was adapted
  - What was used directly
  - What was changed
  - What may not have been used
- As noted, goal was not to be standard compliant, but to use the standard
  - Starting point to build an internal standard that had a foundation in industry best practices, but recognized the differences in the NASA environment

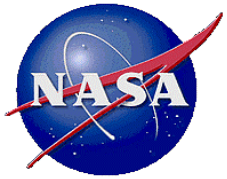
IV&V Tasking Matrix



IV&V Program

1.0	Phase Independent Support
1.1	Management and Planning of Independent Verification and Validation
1.2	Issue and Risk Tracking
1.3	Final Report Generation
1.4	IV&V Tool Support
1.5	Management and Technical Review Support
1.6	Criticality Analysis
1.7	Identify Process Improvement Opportunities in the Conduct of IV&V

IV&V Tasking Matrix (2)

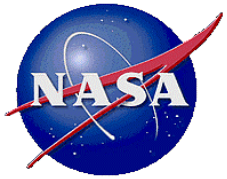


IV&V Program

2.0	Concept Phase
2.1	Reuse Analysis
2.2	Software Architecture Assessment
2.3	System Requirements Review
2.4	Concept Document Evaluation
2.5	Software/User Requirements Allocation Analysis
2.6	Traceability Analysis
3.0	**Requirements Phase**
3.1	Traceability Analysis – Requirements
3.2	Software Requirements Evaluation
3.3	Interface Analysis – Requirements
3.4	System Test Plan Analysis
3.5	Acceptance Test Plan Analysis
3.6	Timing and Sizing Analysis

4.0	Design Phase
4.1	Traceability Analysis – Design
4.2	Software Design Evaluation
4.3	Interface Analysis – Design
4.4	Software FQT Plan Analysis
4.5	Software Integration Test Plan Analysis
4.6	Database Analysis
4.7	Component Test Plan Analysis

IV&V Tasking Matrix (3)

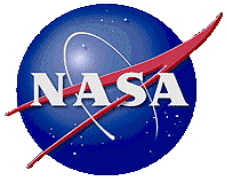


IV&V Program

5.0	Implementation Phase
5.1	Traceability Analysis - Code
5.2	Source Code and Documentation Evaluation
5.3	Interface Analysis - Code
5.4	System Test Case Analysis
5.5	Software FQT Case Analysis
5.6	Software Integration Test Case Analysis
5.7	Acceptance Test Case Analysis
5.8	Software Integration Test Procedure Analysis
5.9	Software Integration Test Results Analysis
5.10	Component Test Case Analysis
5.11	System Test Procedure Analysis
5.12	Software FQT Procedure Analysis

6.0	Test Phase
6.1	Traceability Analysis - Test
6.2	Regression Test Analysis
6.3	Simulation Analysis
6.4	System Test Results Analysis
6.5	Software FQT Results Analysis
7.0	**Operations and Maintenance Phase**
7.1	Operating Procedure Evaluation
7.2	Anomaly Evaluation
7.3	Migration Assessment
7.4	Retirement Assessment

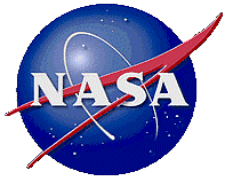
Agenda



IV&V Program

- IV&V at NASA
- The IEEE 1012 Standard
- Developing an IV&V WBS
- Developing a method for determining tasking
- Future of the standard and NASA IV&V
- Summary

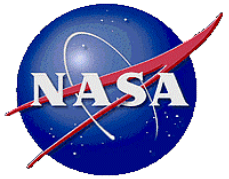
The next step: What tasks do I perform?



IV&V Program

- Two requirements from the Assessment Team
  - WBS
  - Method for determining tasks to perform
- WBS was built by adapting the standard
- Task determination also made use of the standard in the form of Annex B
- Task called Criticality Analysis
  - Used to determine where to focus (I)V&V attention within the system
  - Items of higher criticality should receive more rigor and intensity in the performance of the task

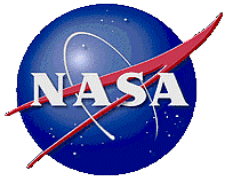
Software Integrity



IV&V Program

- Annex B describes the concept of a software integrity level
  - Software components are assigned integrity levels based on their importance within the system
  - Integrity levels are then used to determine tasks to be performed and the rigor and intensity of those tasks
- The standard provides an approach
- NASA adapted that idea and the approach to fit within our environment

NASA Software Integrity Levels



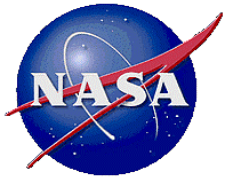
IV&V Program

- Software Integrity Levels
  - Ultimately want to define, for a software component, the required level of integrity in terms of its role in the system
    - Understand how the component fits within the system
    - Understand what is required of that component to be able to maintain the functionality of the system
- Definition of Software Integrity Level
  - The software integrity level corresponds to the tolerable level of risk that is associated with the system.
    - A software component can be associated with risk because
      - a failure (or defect) can lead to a threat, or
      - its functionality includes mitigation of consequences of initiating events in the system's environment that can lead to a threat
  - This definition was developed using not only software but also system level integrity as a basis for the definition (ISO/IEC 15026, 6 and IEEE 1012)

A Risk-based approach

- In order to develop a risk-like view, needed to determine criticality and some probability
- Criticality taken as the consequence of a credible failure of the software under consideration within the context of the system
  - Consequence is a measure of the impact of an error in a software component
    - Generally, take the worse case error (at the software component level) that has a reasonable or credible fault/failure scenario
    - Then consider the system architecture and try to understand how that software fault/failure scenario may affect the system
- The probability looked at the probability of an error being inserted into the system – across the life cycle
  - Error Potential is a measure of the probability that the developer may insert an error into the software component

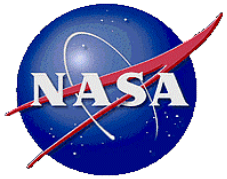
Developing Criteria



IV&V Program

- To assess the two factors criteria needed to be developed
- Foundational information in the standard; expanded and adapted to the NASA environment
- Ultimately, scoring determined the tasking to be performed using the concept that higher scores required more analysis
- Tasks allocated based on the consequence
- Tasks allocated based on the error potential
- Tuned to find defects associated with product defects and process defects

Agenda



IV&V Program

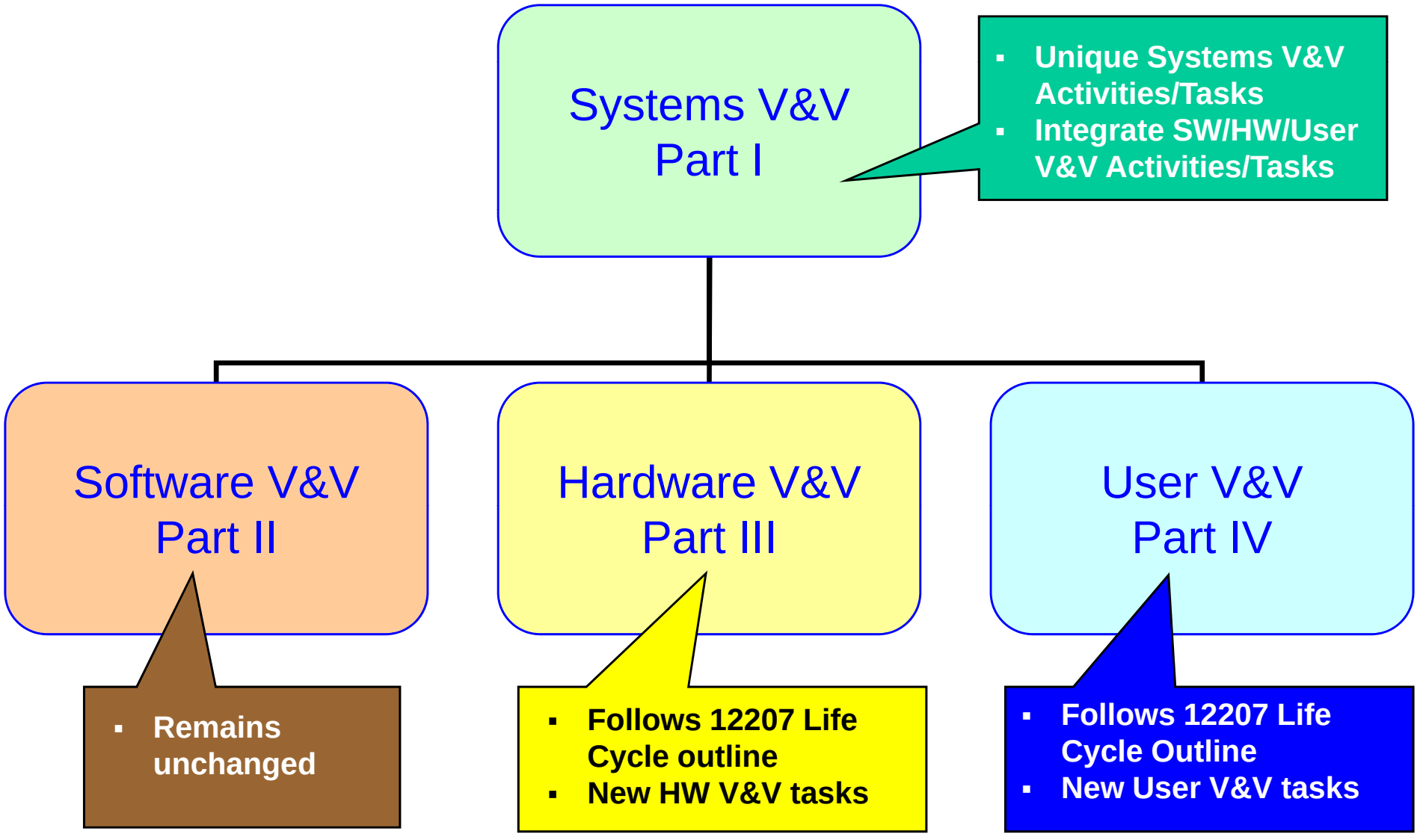
- IV&V at NASA
- The IEEE 1012 Standard
- Developing an IV&V WBS
- Developing a method for determining tasking
- Future of the standard and NASA IV&V
- Summary

Looking Forward

- 1012 working group looking to expand standard beyond just software
- Adapting the standard in accordance with the harmonization of ISO/IEC 12207-1995 Standard for Information Technology – Software Life Cycle Processes and ISO/IEC 15288-2002 Systems engineering – System life cycle processes
- Changes in processes – Verification and Validation now separate processes from a system perspective
- NASA IV&V Facility currently changing WBS to call out specific Validation and Verification processes
  - Enhances focus on each process – develops a flow of not verifying artifacts until they have been validated
  - Expands analysis to include some system level analysis

Draft Outline

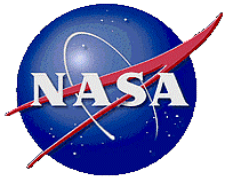
IV&V Program



Challenges for the update

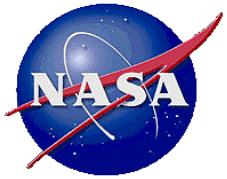
- Selection of a baseline system life cycle model that maps easily to any other life cycle model
- Enhanced criteria for V&V of COTS and reusable software
- Identification of a process or task to address new implementation of hardware/software development
  - System architectural model validation and compliance
  - Formal requirements definition language (proof of correctness)
  - Automated code generation from formal requirements definition language
  - Field Programmable Gate Array (FPGA), Application Specific Integrated Circuit (ASIC), Programmable Array Logic (PAL), Complex Programmable Logic Device (CPLD), Programmable Logic Device (PLD)
  - Concurrent engineering and its impact on the V&V process
- V&V of adaptive software or non-deterministic software (e.g., neural networks)

Agenda



- IV&V at NASA
- The IEEE 1012 Standard
- Developing an IV&V WBS
- Developing a method for determining tasking
- Future of the standard and NASA IV&V
- Summary

Summary



- The IEEE 1012 Standard for Software Verification and Validation was easily adaptable to the NASA environment
- Provided a clear industry best practice foundation on which to build a NASA specific approach to performing IV&V
- Provided a foundation to develop a task determination approach focusing IV&V effort on the most risky portions of the system
- IEEE 1012 working group actively updating the standard to incorporate systems level V&V
- Goal is to use the harmonization of international and IEEE Std 1012 in the new IEEE Std 1012-200x to gain broader use and acceptance of V&V as one of the methods to ensure better and safer systems and software