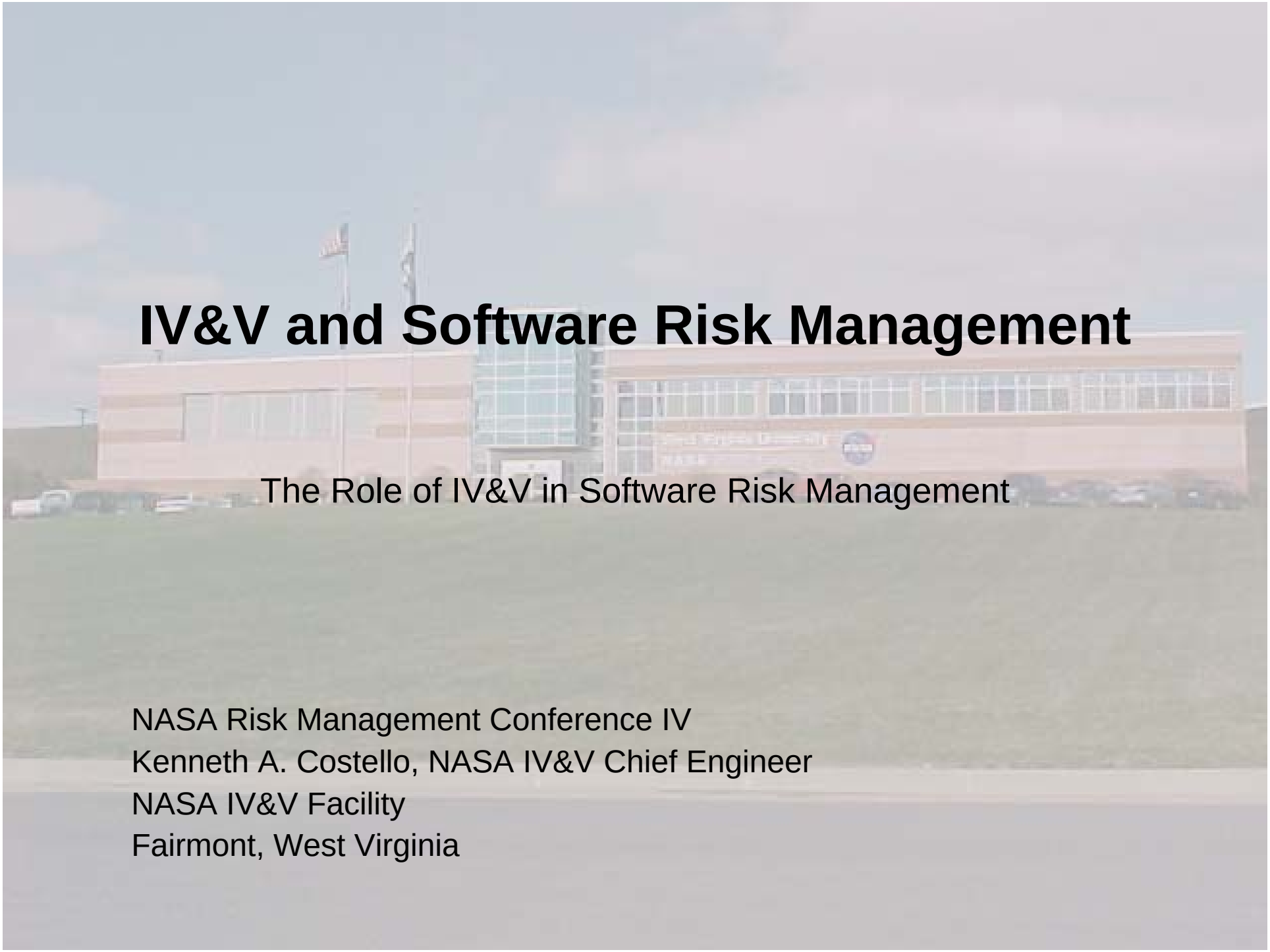
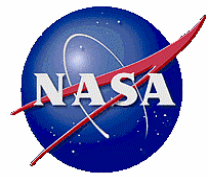


IV&V and Software Risk Management

The Role of IV&V in Software Risk Management

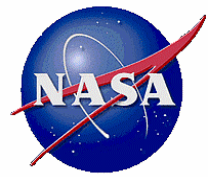
NASA Risk Management Conference IV
Kenneth A. Costello, NASA IV&V Chief Engineer
NASA IV&V Facility
Fairmont, West Virginia



IV&V Facility

Discussion Outline

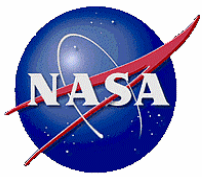
- Software Risk
- What is IV&V at NASA?
- IV&V and Software Risk Management



IV&V Facility

Software Risk

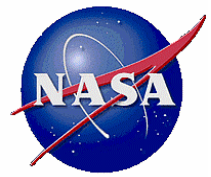
- Risk
  - The possibility of suffering damage or harm
  - The likelihood of an event along with the consequences of it occurring
- Software risk
  - The risk inherent in the development of software
    - Poor estimating
    - Personnel shortfalls
    - Requirements creep/Inadequate requirements
  - The risk associated with software failure
    - Hazardous event not controlled
    - Incorrect command execution
    - Erroneous navigation calculations
- Software Risk Management
  - Active process
  - Identify and address risks as early as possible
  - Relate them to the software and the system/mission as a whole



IV&V Facility

IV&V Overview

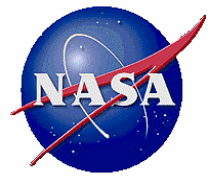
- What is the goal of IV&V analysis?
  - Provide a higher level of confidence that the software will be fit for operation and satisfy its requirements for safety, availability, quality and function
  - Reduce the risk associated with development and operation
- What is Independent Verification and Validation?
  - A set of engineering tasks executed throughout the development process
  - Performed at the unit, module, integration and system levels (as required)
  - Consists of system domain and software experts
  - Focused approach to assessing software for high-criticality risks/issues
- What is the output from IV&V?
  - Generally analysis summary reports and issues
  - The issues can either be errors in a development artifact or errors (risks) in the development process



IV&V Facility

IV&V Execution

- NASA's definition of Independent Verification and Validation
  - Independent – managerial, technical, financial
  - Verification – Is the product built right?
  - Validation – Are we building the right product?
- IV&V at NASA is treated as a *system* level activity that starts by assessing the role of software within a system
- We want to answer the following questions within a system context
  - 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?
  - How does the development approach fit within the overall system development?
- A set of engineering analysis tasks are then performed against the software/system based upon the assessment (the answers to the questions)



IV&V Facility

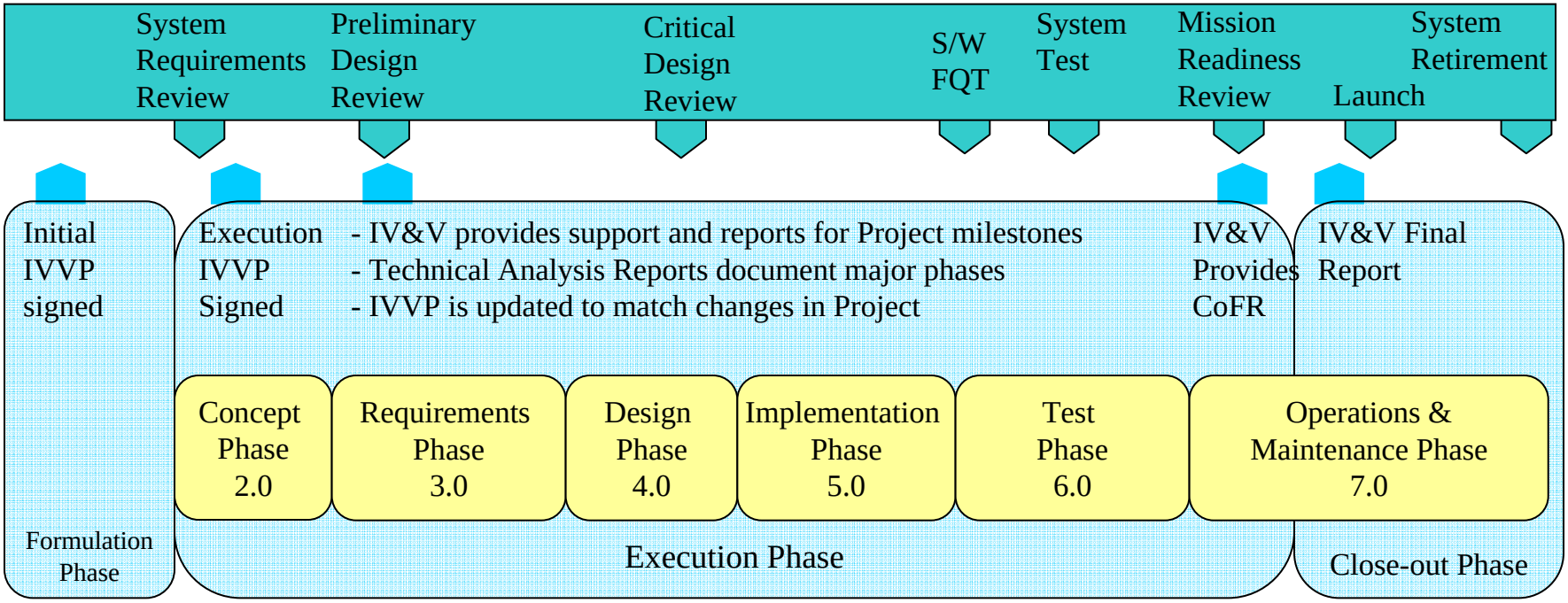
IV&V Execution (2)

- Once the IV&V Team understands the role of the software, the team then employs techniques, processes and methods of varying levels of rigor to evaluate the correctness and quality of the software throughout the project life cycle
- It is important to note that the approach taken is *throughout* the life cycle
- IV&V is not viewed nor applied as a test only approach to software risk identification/mitigation at NASA
- Proper application of IV&V provides
  - Analysis of the software within the context of the system being developed
  - Greater insight into the software development status
  - Early insight into potential problem areas allows problems to be fixed sooner

IV&V Facility

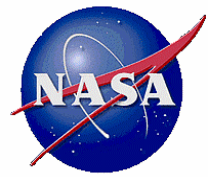
IV&V Life Cycle

Nominal Software Development Life Cycle



Nominal IV&V Life Cycle

Note: numbers correspond to IV&V WBS



IV&V Facility

IV&V and Software Risk Management

- The IV&V Team provides early identification of issues/risks
  - Software and system level
  - Issues may affect the development process
  - Issues may affect the operation of the system
- While independent, the IV&V Team results should be integrated into the risk management process
  - Development project needs to work with IV&V Team to address issues found
  - Communication is important to ensure critical issues are addressed as early as possible
  - Need to understand definition of risk on both sides