Independent Verification and Validation of Large System Architectures

Don Ohi, L-3 Communications
Chris Walter, WW Technology Group
Jim Dabney, L-3 Communications
Overview

- Architecture IV&V
- Architecture Analysis Research Elements
  - Architecture Perspectives
    - Topics for analytical investigation
    - Views for improving architecture specifications
  - Architecture Analysis Framework
    - Tailorable set of architecture analysis objectives
    - Methods for accomplishing objectives
NASA IV&V

- Independent
  - Technical
  - Managerial
  - Financial
- Analytical approach to evaluate software
  - Correctness
  - Completeness
- Key information sources
  - IV&V Technical Reference
  - Developer artifacts
Architecture Specification Emphasis

- Increasing emphasis on architecture throughout NASA
  - Constellation program
    - System architecture requirements document
    - Software architecture description document
    - Flight operations scenarios annex
    - Technical performance measures plan
    - Interface control documents
- JUNO (Jupiter Uranus Neptune Outreach)
- SMAP (Soil Moisture Active-Passive ADD)
Impact of Architecture Phase IV&V

- Architectural issues are a leading source for integration problems.
- Without systematic upfront analysis these problems are costly to repair.
- Application of complexity, safety and dependability analysis enables addressing the issues early on.
- Architectural decisions impact what is required of the software.
- Improved architecture specifications reduce software risk and increase IV&V’s ability to validate and verify the software.

Architecture Analysis Research Elements

Analysis Perspectives

Completeness  Verifiability  Levels of Specification

Tasks

Techniques

Tools

December 10, 2010

FOCUS  PROGRESS
Frameworks

DoDAF 2.0

4 + 1

ATAM

Evaluation

Representation

December 10, 2010
## Constellation Software Architecture IV&V

### CSADD
- Tailored from DoDAF 1.0

<table>
<thead>
<tr>
<th>View</th>
<th>Comments</th>
</tr>
</thead>
</table>
| OV-2 | - Operational resource flow description  
        - Map to operational scenarios  
        - Hierarchical or mission phase views |
| OV-3 | - Operational resource flow matrix  
        - Decomposed by mission phase and needline type |
| OV-5 | - Operational activity model  
        - Presented via activity diagrams and flowcharts |
| SV-1 | - System interface description  
        - Systems and interfaces to realize OV-2 |
| SV-2 | - Systems communication description |
| SV-6 | - Systems data exchange matrix  
        - Tabular characterization of data form SV-1 and SV-2  
        - CSADD contains abridged SV-6 |

### Tailored-out viewpoints

<table>
<thead>
<tr>
<th>View</th>
<th>Comments</th>
</tr>
</thead>
</table>
| AV-1 | - AV-1 Executive Summary  
        - Hierarchical or mission phase views |
| AV-2 | - Integrated dictionary |
| OV-6 | - Operational activity sequence & timing |
| SV-4 | - Systems functionality description  
        - Systems and interfaces to realize OV-2 |
Verifiability

- Features of the architecture are mapped to requirements, which are then mapped to the verification tests that verify them
  - All components have requirements that are tested
  - All component interfaces have specified requirements that are mapped to verification tests
  - All critical scenarios coverable/covered by test cases
- Technical budgets, budget allocations, and compliance to budgets expressed in observable/measurable terms
- Risks noted for untestable capabilities, services, interactions, and scenarios and a risk mitigation approach using simulation and analysis planned
Managing Levels of Specification

- This perspective is concerned with managing
  - Properties of a system as a whole
  - Properties that are allocated to the parts from which it is composed

- Document descriptions are information subsets (i.e. abstractions) that need to fit in an organized hierarchy

- Assessing levels of specification can:
  - Detect misalignment of levels of specifications (e.g. semantics)
  - Gaps in interfacing stakeholder/developer abstractions (e.g. omissions)
  - Potential system integration issues (e.g. pattern errors)
Levels of Specification and Multiple Objectives

- The primary objectives of a system should leave many degrees of freedom for design open
  - Detect stakeholder biases that introduce artificial constraints on downstream tradeoffs
    - Requirements that bias the problem space
    - Implementations that bias the solution space
- Downstream options are then eliminated on the basis of the secondary objectives of the work system
- In many systems, the primary objectives, secondary objectives, and external constraints are often conflicting
- Objectives, like safety or fault tolerance, can have conflicting implementations (e.g. “do nothing” may be safest!)
Levels of Specification and Safety Example

- When objectives, like safety or fault tolerance, have conflicting implications it was unclear in the CSADD how conflicts were resolved.
- There is a risk that system level requirements like safety may merely be specified as measures of goodness at a component level.
- Need to determine if interpretation of safety is consistent at different levels of specification and among system stakeholders.
- Need to determine if an implementation can compromise a critical objective when mixed with other factors (either critical/non-critical).
  - E.g. scheduling of critical communications over a shared network or writing to a shared database.
IV&V Techniques

- Specification Completeness
  - DoDADF content checklists

- Levels of Specification Identification
  - Keyword and phrase pattern search vertically through document tree

- Scenario analysis
  - Scenario modeling, and simulation and test

- Fault Management and Redundancy Analysis
  - Error propagation analysis and containment
  - Coupling analysis

- Technical budgets Analysis
  - Budget identification from ADD and document tree
  - Analyze budget allocation, feasibility

- Mapping Tasks (Functional Capability Mapping, Dependency Mapping Analysis, I/F Requirements Traceability Analysis, Top-level Requirements Mapping)
  - Quality function deployment (QFD) matrix
Tool Support Opportunities

- Smart keyword search
- Budget mapping tool
- Scenario visualization and testing
- Tracing tools (implement QFD House of Quality)
Architecture Analysis Tailoring

- Involves selecting project-applicable tasks
- Guided by project manager’s tailoring goals
  - Breadth vs. depth
  - Comprehensive vs. limited
- Driven by many factors
  - Overall system criticality and risk
  - Architecture style (DoDAF, 4+1, etc)
  - Mission type/System type
  - Development approach
  - Development phase
  - Artifact availability and maturity
  - Task dependencies
Summary

- Architecture IV&V essential
- CSADD-inspired ADD improvements
  - Completeness
  - Verifiability
  - Levels of abstraction
- IV&V architecture methodologies
  - Ideal task set covers all aspects of architecture
  - Techniques achieve tasks
  - Tools facilitate and automate techniques