Spaceflight Software Architecture Analysis Techniques

October 19, 2011

Don Ohi, L-3 Communications
Heath Haga, L-3 Communications
Jim Dabney, L-3 Communications

This presentation consists of general capabilities information that does not contain controlled technical data as defined within the International Traffic in Arms (ITAR) Part 120.10 or Export Administration Regulations (EAR) Part 734.7-11
Overview

- Architecture IV&V
- Specification completeness
- Stakeholder analysis
- Key driving requirements
- Technical budgets analysis
- Scenario analysis
- Next steps
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

Objectives

- Adequately specified
- Complies with requirements
- Feasible
Architecture Analysis Research Elements

Analysis Perspectives

- Completeness
- Verifiability
- Levels of Specification

Analysis Framework

- Tasks
- Techniques
- Tools

FOCUS
PROGRESS
Architecture Analysis Context

- IV&V Architecture Analysis Tasks
  - Observations
  - Issues
  - Risks
  - Evidence

- Informal developer–IV&V communications
- Developer – IV&V issue resolution Process
- Developer Risk Management Process

- Architecture Specifications (OpsCon, ADD …)
- IV&V Analysis Planning
- IV&V Requirements, Design, Implementation, and Test Analysis
IV&V Architecture Analysis Tasks

**Completeness**
- Specification completeness
- Functional Capability Mapping
- Dependency mapping analysis
- Technical budgets analysis
- Top-level requirements mapping
- Scenario development
- Fault management and redundancy analysis

**Verifiability**
- Reuse Analysis
- Interface requirements traceability analysis
- Key driving requirements validation

**Levels of Specification**
- Levels of specification identification
- Stakeholder analysis
- Evolvability analysis
- Comparison to lower level architecture specifications
Task Phasing

Concept Review

- Stakeholder analysis
- Levels of Specification Identification
- Key Driving Requirements Validation
- Top-level Requirements Mapping

SRR

- Specification Completeness SDR

SDR

- Scenario Analysis

PDR

- Specification Completeness PDR
- Fault Management and Redundancy Analysis
- Technical Budgets Analysis
- Reuse Analysis
- Functional Capability Mapping
- Dependency Mapping Analysis
- Evolvability Analysis
- Interface Requirements Traceability Analysis

CDR

- Specification Completeness CDR
- Comparison to Lower Level Architecture Specifications
Specification Completeness

- Assess tailoring
  - Identify architecture specification
  - Analyze tailoring
  - Tailoring guidelines per lifecycle phase
- Assess viewpoint representation
  - Breadth
  - Depth
Frameworks

DoDAF 2.0

- Suitable for large integrated systems
- Consists of sets of viewpoints

4 + 1

- Smaller systems
- Less guidance on viewpoint content
Specification Completeness Trial

- Large ground based system
- No formal framework followed
- Size appropriate for DoDAF 2.0
- Mapped artifacts to DoDAF viewpoints
- Tailoring expectations tables
  - Identified early lifecycle need for OV-4
    (Organizational Relationships Chart)
Stakeholder Analysis

- Basis for any systems engineering activity
- Drives other IV&V (and systems engineering) tasks

Key elements

- Identify stakeholders
- Assess power, influence, interest
- For key stakeholders
  - Concerns
  - Priorities
  - Risks
Influence Diagram

Information giving
- e.g. media, opinion formers

Dialogue
- e.g. government departments, other NGOs

Information gathering
- e.g. general public

Consultation
- More passive
- More interactive

- e.g. Local communities
Onion Diagram

The Wider Environment

The Containing System

The System

The Product

Developer

Ops Support

Payload Cust.

Operator

Interfacing Systems

IV&V

Maintainer

NASA

Public

Regulator

DOD

Political Beneficiary

Funding Champion

Project Opponents

Academic Researchers
## Participation Matrix

<table>
<thead>
<tr>
<th>Participation Type</th>
<th>Inform</th>
<th>Consult</th>
<th>Partner</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Needs Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring &amp; Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Stakeholder Analysis Trial

- Identified from system documentation and domain knowledge
- Several stakeholders not documented
- Found revised participation matrix better fit
- Influence diagram particularly helpful
## Revised Participation Matrix (abridged)

<table>
<thead>
<tr>
<th></th>
<th>Needs Assessment</th>
<th>Planning</th>
<th>Implement</th>
<th>Monitor &amp; Eval</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fund</strong></td>
<td>Level II &amp; III</td>
<td>Level II &amp; III</td>
<td>Level II &amp; III</td>
<td>Level II &amp; III</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Level II - IV</td>
<td>Level II - IV</td>
<td>Level II - IV</td>
<td>Level II - IV</td>
</tr>
<tr>
<td><strong>Specify</strong></td>
<td>Level III &amp; IV Test Team Systems Eng</td>
<td>Level III &amp; IV Test Team App Dev</td>
<td>Level III &amp; IV Test Team App Dev</td>
<td>Level III &amp; IV Test Team</td>
</tr>
<tr>
<td><strong>Accept</strong></td>
<td></td>
<td></td>
<td>Test Team Facility Mgt Sys Eng</td>
<td></td>
</tr>
<tr>
<td><strong>Develop</strong></td>
<td>Level IV</td>
<td>Level IV</td>
<td>Level IV Contractors Gov Agencies</td>
<td></td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td>Sust Eng Log &amp; Maint</td>
<td>Sust Eng Log &amp; Maint Other Centers</td>
<td>Sust Eng Log &amp; Maint Other Centers</td>
<td>Facility Mgt Safety Secutiry</td>
</tr>
<tr>
<td><strong>Advise</strong></td>
<td>Operators</td>
<td>Operators</td>
<td>Operators Public Affairs</td>
<td>Operators Other Centers</td>
</tr>
</tbody>
</table>
Key Driving Requirements

- High-level (user) requirements which define mission success
- Flow from stakeholder analysis

Sources
- Generic based on mission type
- Ops concepts/capabilities (CV-1, CV-4, CV-6)
- Business case, vision
Attributes

- Requirement – succinct statement
- Stakeholder
- Success criteria
- Relevant scenarios
- Quality measures
- Priorities
- Risks
- Dependencies
- Verification
- Relevant artifacts
- How satisfied
- Issues
Key Driving Requirement Trial

- Developed list of concerns/needs/expectations for key stakeholders
- Mapped expectations to documented requirements
- Some potential mismatches identified
Technical Budgets

- Flows such as data streams, fluids, energy
- Physical characteristics such as weight, volume, moment of inertia
- Operational factors such as workload, risk
- Budget management mechanisms
  - Authority – who’s responsible
  - Tracking
    - Identification procedures
- Technical budget levels of specification
  - Operational (logical) level
  - Systems (services, physical)
Technical Budget Assessment

- Identify budgets managed / should be managed
- Evaluate consistency
- Evaluate feasibility
- Evaluate testability
Scenario Analysis

- Scenario completeness
  - Flows from stakeholder and key driving requirements analysis
  - Nominal scenarios
  - Maintenance and update scenarios
  - Abort and degraded system scenarios

- Scenario correctness
  - Analytical (decision tree, event tree, activity network diagram)
  - Simulation
Next Steps

- Continue testing & refining methods on ongoing IV&V project
- Define additional analysis techniques
  - Levels of specification
  - Fault management & redundancy analysis
  - Mapping tasks
  - Safety analysis
- Develop tools