Risk–Driven Spacecraft Flight Software Independent Verification and Validation

Pavan Rajagopal, GeoControl Systems
James B. Dabney, UHCL
Gary Barber, GeoControl Systems
Overview

- Objectives of Work
- IV&V Background
- Importance of early defect identification
- Conventional Strategies for Targeting IV&V
- Using Critical Events for Targeting IV&V
- Critical Event Identification
- Assurance case overview
- Risk Tree
- Adjectival and Probabilistic Scoring of Risk
- Detailed Analysis & Scoring
- Benefits of Approach
- Conclusions and Future work
Objectives

Spacecraft FSW is prone to defects
IV&V identifies and resolves defects

Objectives of methodologies:
- Accurately scope & target IV&V
- Effectively perform IV&V to identify and resolve defects
- Measure the risk reduction achieved
IV&V Background

- Evaluates system and software for Correctness & Completeness
- Technically, Organizationally and Financially Independent
- Most effective when applied throughout lifecycle
- Key information sources
  - Developer artifacts
  - IV&V Technical Reference
Typical IV&V Activities

- Analyze technical artifacts
- Assess adequacy of verification activities and environments
- Perform Independent testing
  - Algorithms
  - Complex or High-risk code fragments
  - Off-nominal scenarios
Value of Early Defect Identification

Relative Cost to Fix Defects per Phase Found

Defect Type
- Requirements
- Design
- Code
- Test
- Integration

Phase Found
- Requirements
- Design
- Code
- Test
- Integration
- Operations

Source: Ref [1]
Strategies for Targeting IV&V

- Criticality Analysis and Risk Assessment (CARA)
  - Identify critical function
  - Prioritize using risk (likelihood of problem) and criticality (consequences)
- Portfolio-based risk assessment [2]
  - Based on hardware and software entities
  - Also uses risk–criticality matrix
- Both methods result in broad IV&V targets
Targeting using Critical Events

- Based on flow of mission events
  - Mission timelines
  - Concept of operations

- Benefits
  - Permits early lifecycle IV&V participation
  - Narrows analysis targets and enables prioritization
  - Enables cross cutting analysis
Critical Event Identification

Based on risk categories
- Human safety
- Loss of mission
- Damage to asset
- Loss of key mission objectives

Scoring
- Events scored for each category of risk
- Composite score used to rank events
- Highest ranked events get priority in analysis
Assurance Case Overview

- Structured argument [3]
  - Based on safety cases
  - Uses logical flow (decomp) from
    - Claims
    - Supporting claims
    - Evidence

- High-level claim is successful performance of system function or objective

- Supporting claims deal with
  - System Configuration
  - Environment
  - Procedures
  - HW/SW functionality

- Evidence examples
  - Documentation
  - Testing
  - Analyses
Risk Tree

- Uses assurance case structure
- Overall risk for top-level claim depends on
  - Risk of lower level supporting claims
  - Strength of influence of lower level supporting claims
- Completeness and correctness of evidence determines risk for lowest level supporting claim
- Score rollup options
  - Adjectival (stoplight chart)
  - Numerical weighting
  - Probabilistic (requires extensive calibration)
- Rollup can feed into project risk management tool
Risk Tree

- Uses assurance case structure
- Overall risk for top-level claim depends on
  - Risk of lower level supporting claims
  - Strength of influence of lower level supporting claims
- Completeness and correctness of evidence determines risk for lowest level supporting claim
- Score rollup options
  - Adjectival (stoplight chart)
  - Numerical weighting
  - Probabilistic (requires extensive calibration)
- Rollup can feed into project risk management tool
Examples of risks related to Mission–critical events

- Staging failure
- Docking failure
- Failure of Trajectory and orbit maneuvers
Examples of Risk Sub-claims

- System is not configured for event
- Precursor events do not successfully complete
- Failed Event Triggers
- Missed or failed Execution steps
- Failure to confirm correct completion
Examples of evidence used to mitigate risks

- Requirements
- Design
- Testing
- Analysis
- Prior use of subsystem
- Formal methods analysis
Partial Critical Event Risk Tree Example

Deorbit Burn Fails
- Incorrect Computation of Burn Parameters
  - Miscompute Delta V
    - Requirements Evidence
    - Design Evidence
  - Miscompute Ignition Time
    - Requirements Evidence
    - Design Evidence
- Incorrect Execution of Burn
  - Flight Control Failure
    - Requirements Evidence
    - Design Evidence
  - Uncompensated HW Failure
    - Requirements Evidence
    - Design Evidence
Adjectival Score Rollup

- Suitable structure and format for stoplight risk management process

<table>
<thead>
<tr>
<th>Root Claim</th>
<th>Supporting Claim</th>
<th>Evidence</th>
<th>Risk</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>1.1.1</td>
<td>1.1.1.1</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>1.1.2</td>
<td>1.1.1.2</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>1.1.2.1</td>
<td>1.1.1.3</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>1.2</td>
<td>1.2.1</td>
<td>1.1.2.2</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>1.2.2</td>
<td>1.1.2.1</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>1.2.2.2</td>
<td>1.2.1.1</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>1.2.3</td>
<td>1.2.2.1</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>1.2.3.1</td>
<td>1.2.2.2</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>1.2.3.2</td>
<td>1.2.3.1</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

- Adapted from Ref [4]
Probabilistic Scoring and Rollup

- Uses Dempster–Shafer belief functions
  - Based on historical data from similar projects
  - Correlated to project characteristics and activities
- Computes belief that claims will be realized based on:
  - Confidence in Evidence
  - Relative importance of supporting claims
<table>
<thead>
<tr>
<th>Level</th>
<th>Claim</th>
<th>Risk</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Root Claim</td>
<td>0.370%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.1 Supporting Claim</td>
<td>0.416%</td>
<td>70.00%</td>
</tr>
<tr>
<td></td>
<td>1.1.1 Supporting Claim</td>
<td>0.551%</td>
<td>70.00%</td>
</tr>
<tr>
<td></td>
<td>1.1.1.1 Evidence</td>
<td>0.500%</td>
<td>100.00%</td>
</tr>
<tr>
<td></td>
<td>1.1.1.2 Evidence</td>
<td>0.500%</td>
<td>10.00%</td>
</tr>
<tr>
<td></td>
<td>1.1.1.3 Evidence</td>
<td>0.001%</td>
<td>100.00%</td>
</tr>
<tr>
<td></td>
<td>1.1.2 Supporting Claim</td>
<td>0.051%</td>
<td>60.00%</td>
</tr>
<tr>
<td></td>
<td>1.1.2.1 Evidence</td>
<td>0.500%</td>
<td>10.00%</td>
</tr>
<tr>
<td></td>
<td>1.1.2.2 Evidence</td>
<td>0.001%</td>
<td>90.00%</td>
</tr>
<tr>
<td></td>
<td>1.2 Supporting Claim</td>
<td>0.098%</td>
<td>80.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.1 Supporting Claim</td>
<td>0.050%</td>
<td>60.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.1.1 Evidence</td>
<td>0.100%</td>
<td>50.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.2 Supporting Claim</td>
<td>0.020%</td>
<td>90.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.2.1 Evidence</td>
<td>0.001%</td>
<td>50.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.2.2 Evidence</td>
<td>0.100%</td>
<td>20.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.3 Supporting Claim</td>
<td>0.100%</td>
<td>50.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.3.1 Evidence</td>
<td>0.001%</td>
<td>20.00%</td>
</tr>
<tr>
<td></td>
<td>1.2.3.2 Evidence</td>
<td>0.500%</td>
<td>20.00%</td>
</tr>
</tbody>
</table>

*Yellow risk cells are computed*
Detailed Analysis & Scoring

- **Analysis**
  - Performed on lowest level supporting claims
  - Involves
    - Traditional IV&V inspection and analysis
    - Simulation
    - Independent testing

- **Scoring**
  - Performed at the lowest level supporting claim
  - Based on subjective assessment of evidence by qualified IV&V analyst
  - This assessment is fit into a range of defect densities from historical like projects
  - Tree structure used to establish score at mid level and top nodes
Benefits of approach

- Drives cross cutting analysis across multiple participating subsystems (HW and SW)

- Analysis provides insight
  - Points out omissions or errors in evidence
  - Identifies issues and defects

- Enhances objectivity in evaluating risk
Conclusions

- Critical event, risk-driven approach is effective
- Allows relatively fine grained analysis targeting
- Provides solid support for scope and analysis decisions
- Construction of risk tree aids and documents system understanding
  - Records Analysis decisions
  - Facilitates change impact analysis
Future Work

- Increase insight into scoring by tracking defects vs risk assessment
- Integrate methods into workflow toolset
- Automate tracking and reporting of risk score
References


