GEOCONTROL SYSTEMS, INC.

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

GEOCONTROL SYSTEMS, INC.

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

GEOCONTROL SYSTEMS, INC.

- 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

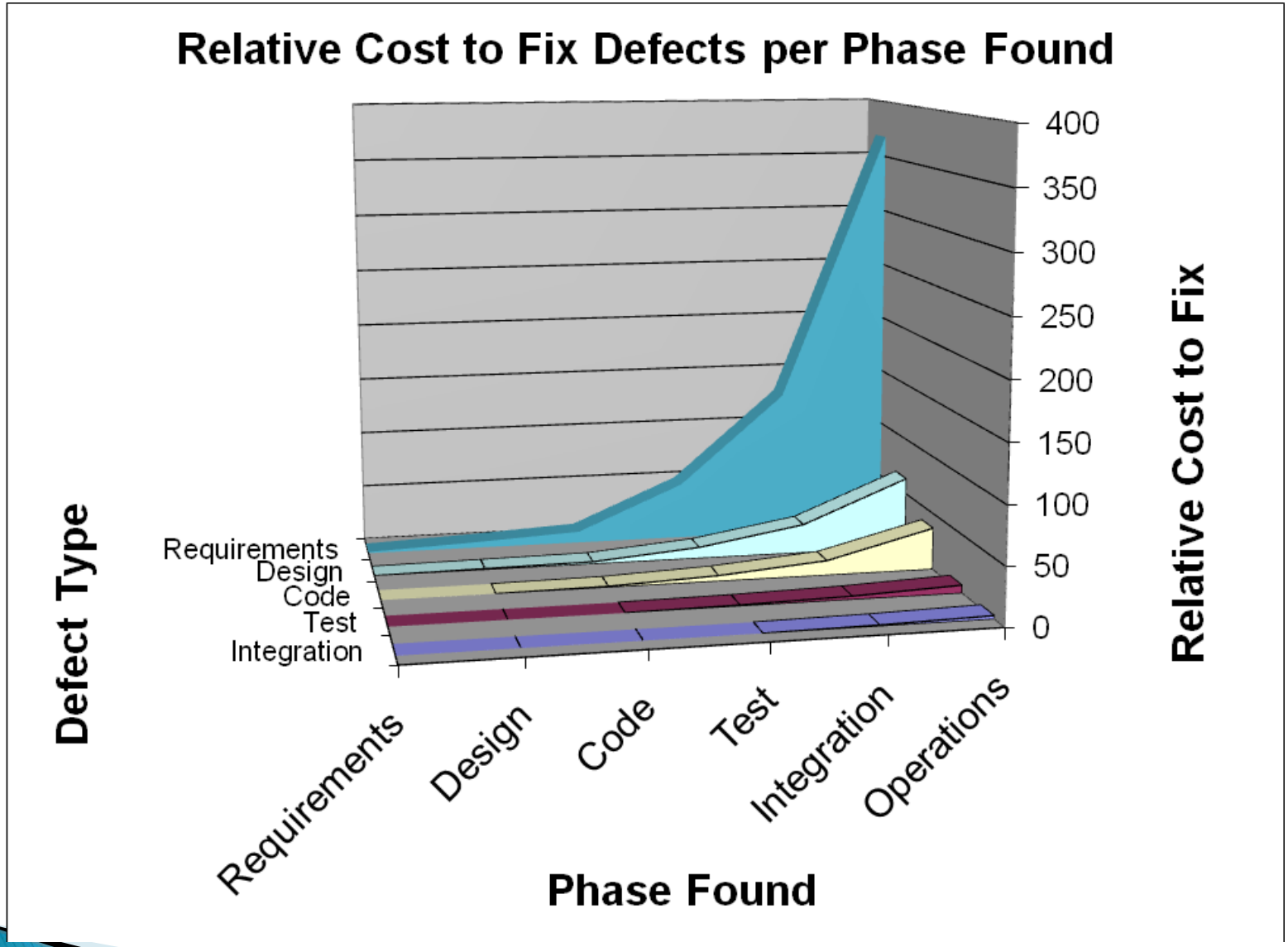
Typical IV&V Activities

GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.



Source: Ref [1]

Strategies for Targeting IV&V

GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.

- 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

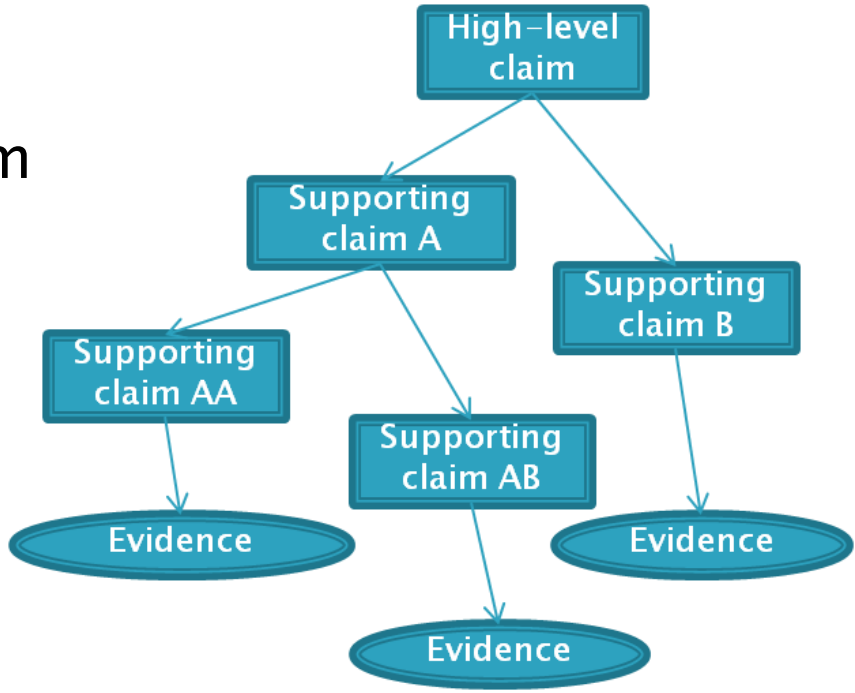
GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.

- 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

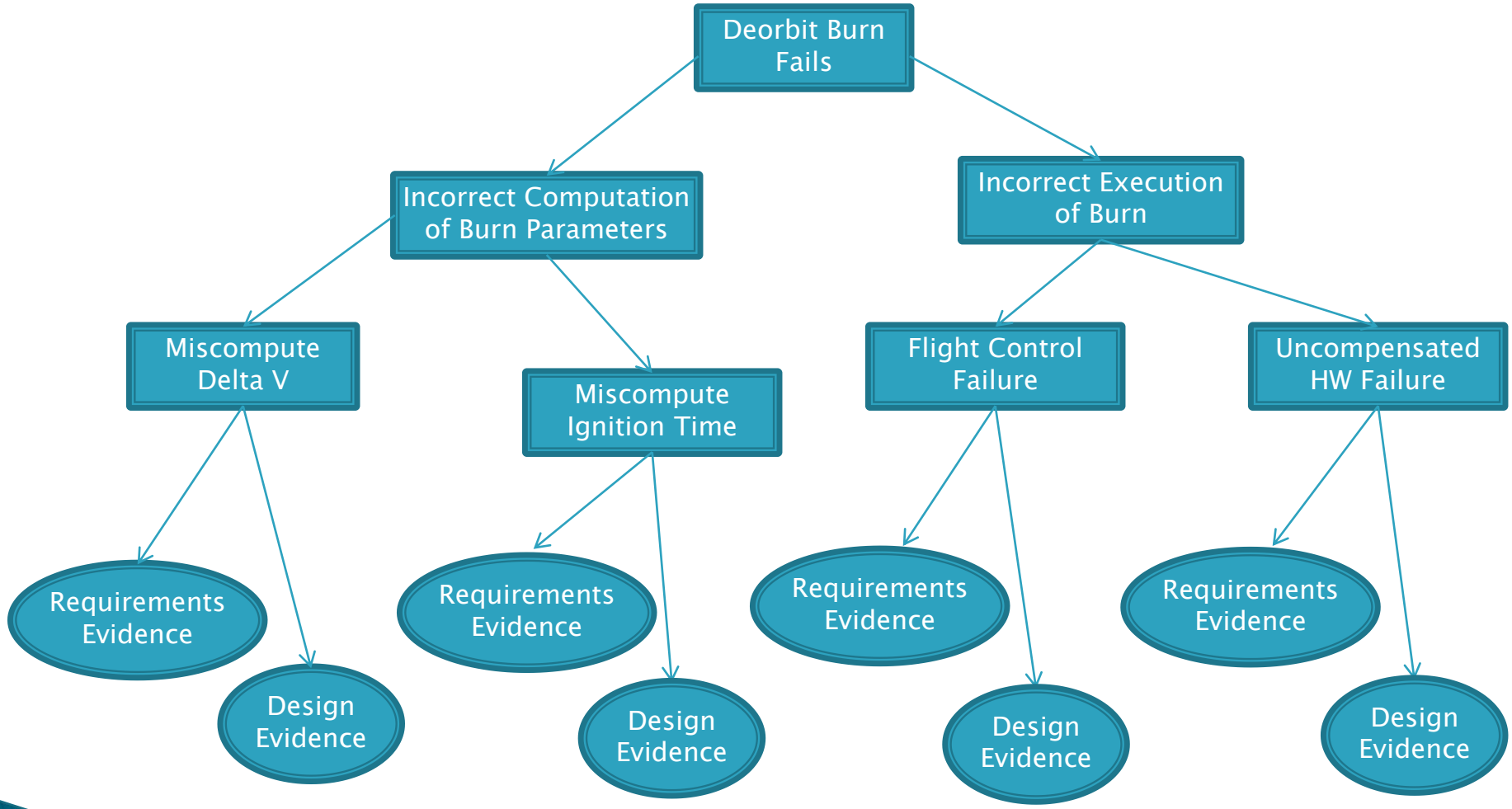
- System is not configured for event
- Precursor events do not successfully complete
- Failed Event Triggers
- Missed or failed Execution steps
- Failure to confirm correct completion

Examples of evidence used to mitigate risks

GEOCONTROL SYSTEMS, INC.

- Requirements
- Design
- Testing
- Analysis
- Prior use of subsystem
- Formal methods analysis

Partial Critical Event Risk Tree Example



Adjectival Score Rollup

GEOCONTROL SYSTEMS, INC.

- Suitable structure and format for stoplight risk management process

				Risk	Weight
1 Root Claim	1.1 Supporting Claim	1.1.1 Supporting Claim	1.1.1.1 Evidence	High	High
			1.1.1.2 Evidence	High	Low
			1.1.1.3 Evidence	Low	High
		1.1.2 Supporting Claim	1.1.2.1 Evidence	High	Low
			1.1.2.2 Evidence	Low	High
	1.2 Supporting Claim	1.2.1 Supporting Claim	1.2.1.1 Evidence	Medium	Medium
		1.2.2 Supporting Claim	1.2.2.1 Evidence	Low	Medium
			1.2.2.2 Evidence	Medium	Low
		1.2.3 Supporting Claim	1.2.3.1 Evidence	Low	Low
			1.2.3.2 Evidence	High	Low

Adapted from Ref [4]

Probabilistic Scoring and Rollup

GEOCONTROL SYSTEMS, INC.

- 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

Probabilistic Rollup Scoring

GEOCONTROL SYSTEMS, INC.

				Risk	Importance
1 Root Claim				0.370%	
	1.1 Supporting Claim			0.416%	70.00%
		1.1.1 Supporting Claim		0.551%	70.00%
Yellow risk cells are computed			1.1.1.1 Evidence	0.500%	100.00%
			1.1.1.2 Evidence	0.500%	10.00%
			1.1.1.3 Evidence	0.001%	100.00%
		1.1.2 Supporting Claim		0.051%	60.00%
			1.1.2.1 Evidence	0.500%	10.00%
			1.1.2.2 Evidence	0.001%	90.00%
	1.2 Supporting Claim			0.098%	80.00%
		1.2.1 Supporting Claim		0.050%	60.00%
			1.2.1.1 Evidence	0.100%	50.00%
		1.2.2 Supporting Claim		0.020%	90.00%
			1.2.2.1 Evidence	0.001%	50.00%
			1.2.2.2 Evidence	0.100%	20.00%
		1.2.3 Supporting Claim		0.100%	50.00%
			1.2.3.1 Evidence	0.001%	20.00%
			1.2.3.2 Evidence	0.500%	20.00%

Detailed Analysis & Scoring

GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.

- 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

GEOCONTROL SYSTEMS, INC.

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

References

[1] J. B. Dabney and G. Barber, " Direct return on investment of software independent verification and validation: Methodology and initial case studies," Assurance Technology Symposium, 5 June 2003

[2] N. Alvaro and S. Raque, "Portfolio based risk assessment and risk-based assessment process," Technical Report, NASA IV&V Center, Fairmont, WV, 2012

[3] S. Blanchette, Jr., "Assurance cases for analysis of complex system of systems software," Software Engineering Institute, June, 2010

[4] G. Barber, "Risk reduction demonstration pilot," NASA IV&V Workship, Morgantown, WV, September 13 – 15, 2011