Goal Structuring Notation in a Radiation Hardening Assurance Case for COTS-Based Spacecraft

A. Witulski\textsuperscript{1}, R. Austin\textsuperscript{1}, J. Evans\textsuperscript{2}, N. Mahadevan\textsuperscript{1}, G. Karsai\textsuperscript{1}, B. Sierawski\textsuperscript{1}, K. LaBel\textsuperscript{3}, R. Reed\textsuperscript{1}

\textsuperscript{1}Vanderbilt University \hspace{1em} \textsuperscript{2}NASA HQ \hspace{1em} \textsuperscript{3}NASA GSFC

This work supported under NASA Grant and Cooperative Agreement Number NNX15AV48G
Background: Mission Assurance

- NASA classifies spacecraft missions by criteria: Cost, national significance, priority, lifetime, launch constraints
  - Class A: High-budget, highly significant, e.g. space telescope
    - Low risk tolerance: Conventional radiation testing, hardened parts, etc.
  - (Sub) Class D: Low-budget, limited scope, short lifetime: Cube Sat
    - Relatively high risk tolerance
    - Conventional radiation hardness assurance too expensive
    - Majority use of commercial off the shelf (COTS) parts
    - Still need as much mission assurance as possible.
- Model-Based representations of spacecraft systems can define sub-system functionality and interfacing, reliability parameters
  - Quantitative evaluation of sub-system interactions
  - Entire team works from one virtual model set
  - Fault or failures can be propagated from one sub-system to another
- New paradigm for assurance: model-centric, not document-centric
Graphical Argument

**Argument:** “A connected series of claims intended to support an overall claim.” [1]

**Assurance Case:** “A reasoned and compelling argument, supported by a body of evidence, that a system, service or organisation will operate as intended for a defined application in a defined environment.” [1]

Goal Structuring Notation (GSN)

GSN is a visual representation of a hierarchy of claims [1]

University of York U.K.

Goal=Claim
Strategy=Inference
Solution=Evidence
Context=Background
Justification=Rationale
Assumption=Unsubstantiated Claim

Colors/Shapes Denote Function

Benefits of GSN

- Graphical argument form clarifies relationships between claims and makes assumptions explicit
- Facilitates connecting mission assurance claims to model-based representations of the system
  - Document-centric/model-centric mission assurance (MA)
  - Eventual goal: connect MA and quantitative models
- Graphical assurance case can be constructed concurrently with design-MA influences design
- Radiation Context:
  - References rad test data, hardened part specs
  - Relates mitigation strategy to total Assurance Case
Vanderbilt Custom GSN Modeling Language

• Vanderbilt Institute for Software Integrated Systems
• WebGME: Web-based Generic Modeling Environment
• *WebGME used to develop Modeling Framework for Goal Structured Notation (GSN)*
• Support for customizable Domain Specific Modeling Languages (DSML)
  • Specify modeling rules (meta-models)
• Allow for customizable visualization
• Support for model interpretation
  • Software that traverses models to generate artifacts – documents/texts, code, inputs for integrating with other software/utilities/analysis engines
  • Provides framework for linking to model-based descriptions of sub-systems
WebGME GSN Screenshot

Model Editor Canvas
Model Parts Panel
Model Tree Browser
Attributes Panel
Link to next GSN path fragment

© 2016 Vanderbilt University version 1.5.0 SHA1 or branch -- webgme@vanderbilt

GSN

Goal:1
System remains functional for intended radiation environment (NASA RAM mod) in order to complete science mission objective: Record the number of upset in 28nm bulk $\text{RAM}$ in LEO for a period of 1 year.

Strategy:1
Understand radiation failure mechanisms, eliminate and/or control radiation failure cause and degradation, and limit radiation failure propagation to reduce likelihood of failure to an acceptable level (NASA RAM mod).

Context:1
Radiation environment for Phoenix mission.

Context:2
Functional model of REM.

Context:3
Behavioral model of REM.

Context:4
Mission constraints.

Ref - Goal:2
System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA RAM).

Ref - Goal:3
System is tolerant to radiation faults and failures (NASA RAM mod).

Radiation Parts Char...
GSN

Radiation Fail Trace...
GSN
NASA Reliability & Maintainability Template

Objectives-based approach to Reliability and Maintainability

General Structure for top-level goals in GSN Assurance Case

VU Cube Sat SRAM Experiment Test Bed

- VU Cube Sat Architecture
- Space environment radiation test bed for TID, SEE
- Successful 8 x 4Mb SRAM experiment, launched 2015, reports SEUs, resets, power
GSN Demo Case: 28nm Commercial SRAM SEU Test in LEO

• Launch December 2016
• Radiation Effects Modeling (REM) Board
• Detect SEUs in the SRAM
  • Protect data from other SEE s on the board
  • Count upsets from SEUs in SRAM, not SELs
• Current monitoring for latch up detection
  • Monitor separate for SRAM and rest of the board
  • High-current on SRAM causes the experiment to reset and not count the upsets seen
  • High-current on the rest of the board causes the microcontroller to reset while the SRAM continues to be on and record upsets
Mitigation techniques for latch-up in board components
GSN Assurance REM SEU Experiment Board

- Top Goal states overall objective
- Context statements give easy access to relevant mission docs
- Artefacts
- Top level goals and strategies track NASA R & M template
Not all branches of GSN graph shown
- Assumptions are clearly identified
- Argument path terminates in Solution
- Validity of Assurance case determined by reading from Solutions to top level goals.
Summary