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

A. Witulski¹, R. Austin¹, J. Evans², N. Mahadevan¹, G. Karsai¹, B. Sierawski¹, K. LaBel³, R. Reed¹, R. Schrimpf¹

¹Vanderbilt University  ²NASA HQ  ³NASA GSFC

This work supported under NASA Grant and Cooperative Agreement Number NNX15AV48G
List of Acronyms

Addr = Address
AMSAT = Radio Amateur Satellite Corporation
CDH = Command and Data Handling (bus and processor)
COTS = commercial off the shelf
FPF2006/2007/2123 = Fairchild Semiconductor family of load switches
GSN = Goal Structured Notation
I/O = input/output
IUCF = Indiana University Cyclotron Facility
LEO = Low-Earth Orbit
MA = mission assurance
R & M = reliability and maintainability
REM = Radiation Effects Modeling (SRAM circuit board & experiment)
RXTX = Receiver and Transmitter
SEE = Single Event Effect
SELs = Single Event Latchups
SEUs = Single Event Upsets
SRAM = Synchronous Random Access Memory
TID = Total Ionizing Dose
VU Cube Sat = Vanderbilt University CubeSat
WDT = Watchdog Timer
WebGME = Web-based Generic Modeling Environment (software)
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: CubeSat
    - 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 organization 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

• 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
• Construct graphical assurance case concurrently with design allows designers to address MA early
• Radiation Context:
  • References radiation test data, hardened part specs
  • Relates mitigation strategy to overall Assurance Case

Vanderbilt Custom GSN Modeling Language

- **WebGME: Web-based Generic Modeling Environment**
  - Developed by Vanderbilt Institute for Software Integrated Systems
  - Used to develop modeling framework for Goal Structured Notation
  - Support for customizable Domain Specific Modeling Languages (DSML)
  - Customizable modeling rules (meta-models) specify the syntax and semantics of the model
  - Model elements may contain hyperlinks to engineering documents and relevant artifacts

- **Support for model interpretation**
  - Model interpreter algorithms traverse models to generate artifacts – documents, code, inputs for integrating with other software/ utilities/ analysis engines
  - Provides framework for linking to model-based descriptions of subsystems
WebGME GSN Screenshot

Objectives-based approach to Reliability and Maintainability

General structure for top-level goals for GSN assurance case

Objective: System remains functional for intended lifetime, environment, operating conditions and usage

Context: Description of operating environment, including static, cyclical, and randomly varying loads

Strategy: Understand failure mechanisms, eliminate and/or control failure causes, degradation and common cause failures, and limit failure propagation to reduce likelihood of failure to an acceptable level

Strategy: Assess quantitative reliability measures and recommend or support changes to system design and/or operations

VU CubeSat SRAM Experiment Test Bed

- VU CubeSat payload architecture
- Space environment radiation testbed for TID, SEE
- Successful 8 x 4Mb SRAM experiment, launched 2015, reports SEUs, resets, power

Image Credit: AMSAT
GSN Demo Case: 28nm Commercial SRAM SEU Test in LEO

- Launch January 2017
- Radiation Effects Modeling (REM) Board
- SEU detection in the SRAM
  - Protect data from other SEEs on the board
  - Count upsets from SEUs in SRAM, not SELs
- Current monitors for latch up detection
  - Monitor separate for SRAM and other components
  - High-current on SRAM causes the experiment to reset and not count recent upsets
  - High-current on the rest of the board causes the microcontroller to reset while the SRAM continues to hold data

Sub-Class D: Allow latch-up, employ mitigation
Current monitors, watch-dog timer sense SEL
GSN Assurance REM SEU Experiment Board

- Top Goal states overall objective
- Context statements give easy access to relevant mission docs
- Top-level goals and strategies track NASA R&M template

To Strategy 2
From Goal 2

- 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: Graphical Assurance Case Argument in Goal Structuring Notation

- Dependence of argument claims made explicit
- Structure imposes rigor on assurance case
- Surfaces assumptions implicit in text arguments
- Graphical form naturally compatible with model-based descriptions of systems: SysML, CyPhyML
- Custom GSN modeling language in development
- GSN example demonstrated in design of CubeSat SRAM SEU experiment circuit board
- Graphical assurance case helps designers address mission assurance concerns during design