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

A. Witulski[1], R. Austin[1], J. Evans[2], N. Mahadevan[1], G. Karsai[1], B. Sierawski[1], K. LaBel[3], R. Reed[1], R.Schrimpf[1]

[1]Vanderbilt University   [2]NASA HQ   [3]NASA GSFC

This work supported under NASA Grant and Cooperative Agreement Number NNX15AV48G

To be presented by Arthur F. Witulski at the GOMAC Tech 2016 Government Microcircuits Applications & Critical Technologies Conference, Orlando, FL, March 16, 2016.

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

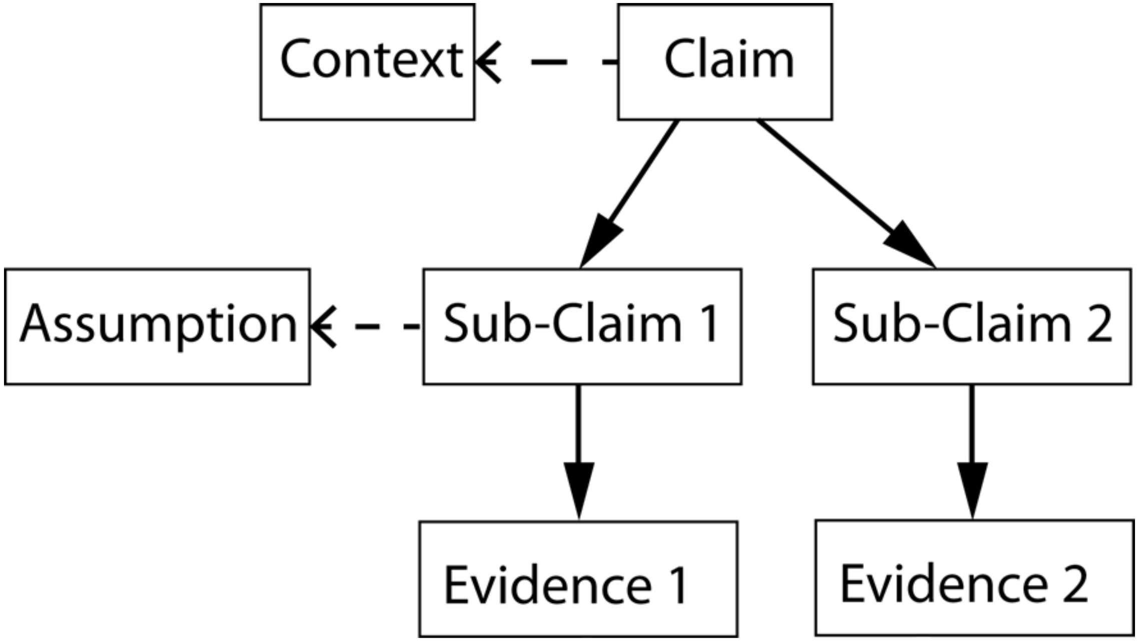
WDT = Watchdog Timer

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

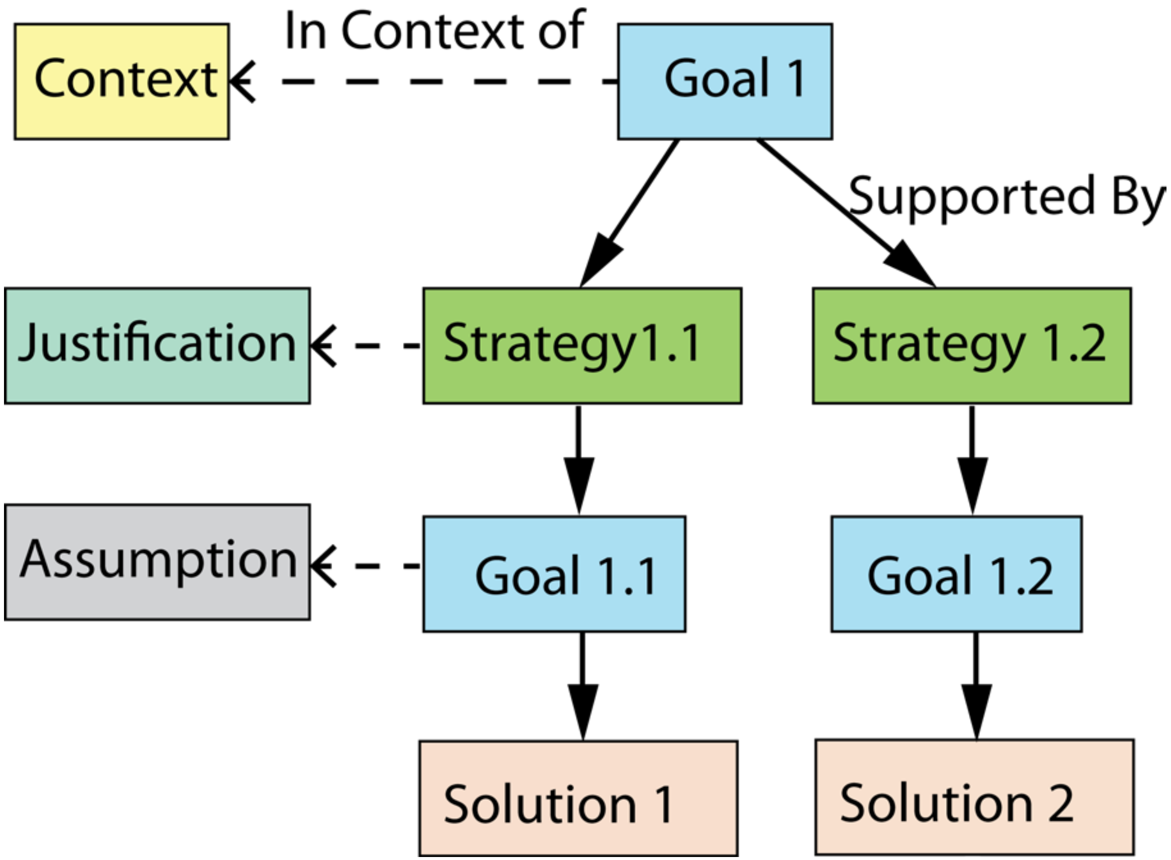


Argument: "A connected series of claims intended to support an overall claim." [1]

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]

[1] GSN Community Standard Version 1 2011

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

[1] GSN Community Standard Version 1 2011

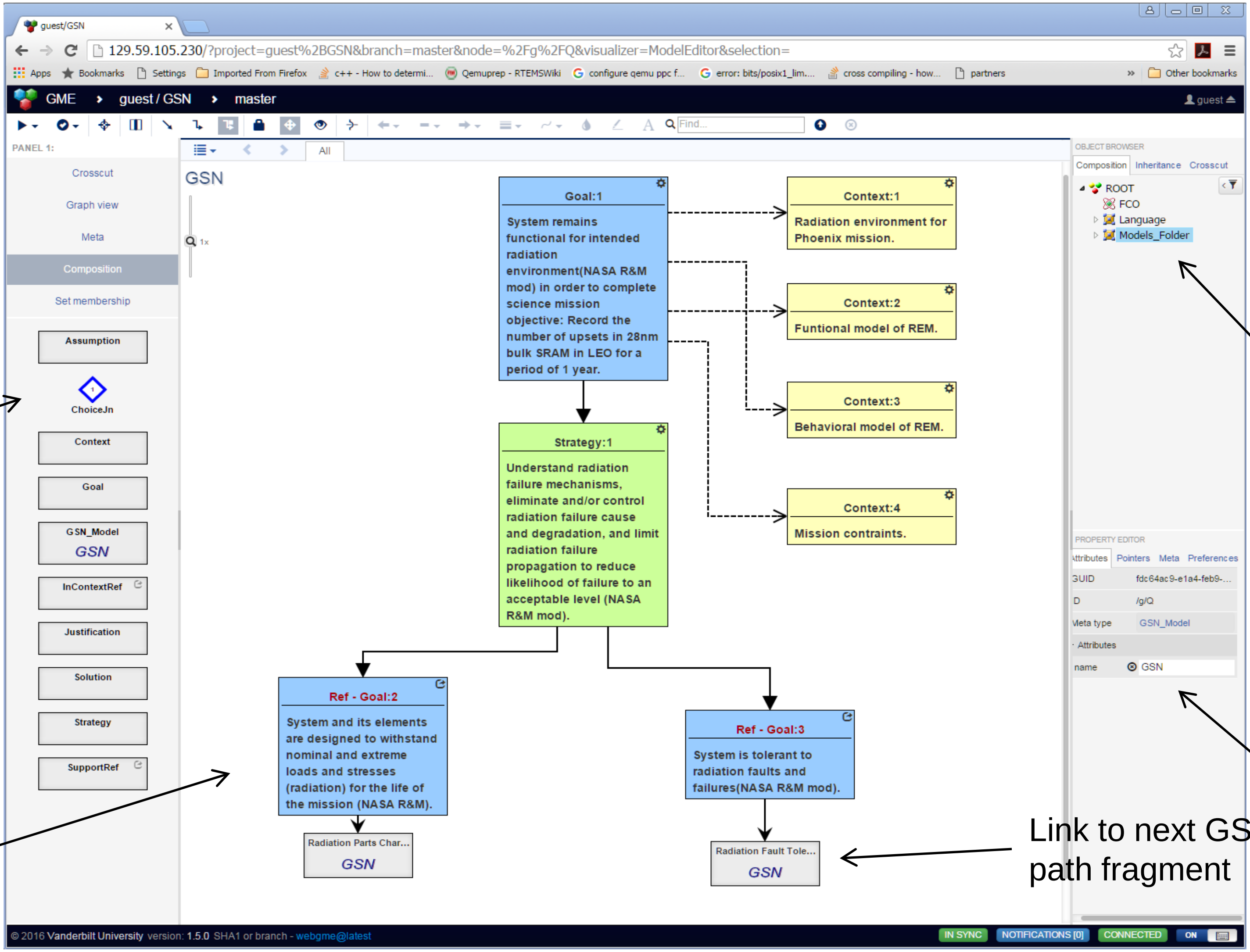
Benefits of GSN

- 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 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 sub-systems

WebGME GSN Screenshot



Goal:1
System remains functional for intended radiation environment(NASA R&M mod) in order to complete science mission objective: Record the number of upsets in 28nm bulk SRAM in LEO for a period of 1 year.

Context:1
Radiation environment for Phoenix mission.

Context:2
Funtional model of REM.

Context:3
Behavioral model of REM.

Context:4
Mission contraints.

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 R&M mod).

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 R&M).

Radiation Parts Char... GSN

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

Radiation Fault Tole... GSN

GUID	fdc64ac9-e1a4-feb9-...
ID	/g/Q
Meta type	GSN_Model
Attributes	
name	GSN

Model Tree Browser

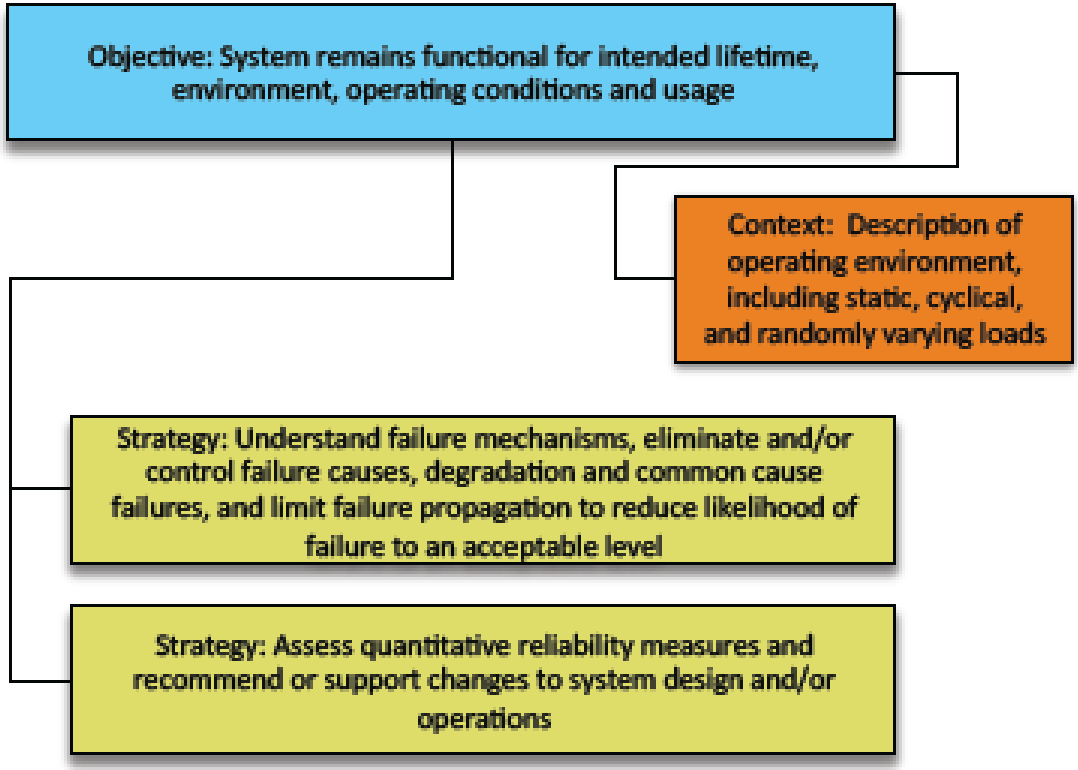
Model Parts Panel

Attributes Panel

Link to next GSN path fragment

Model Editor Canvas

NASA Reliability & Maintainability Template


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

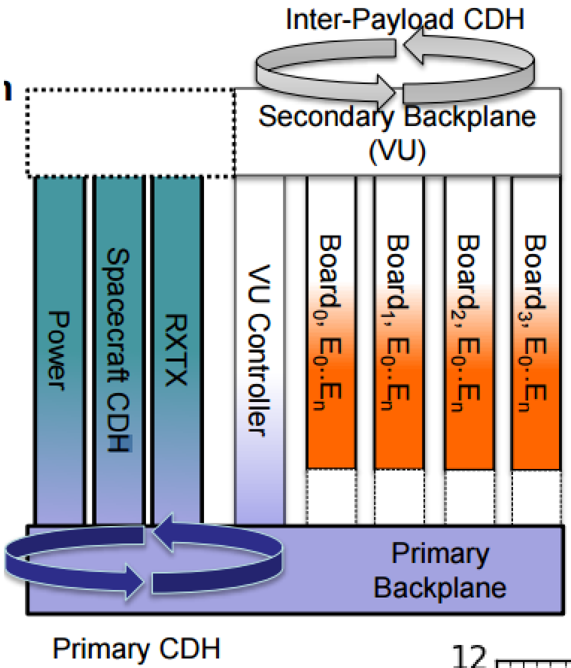
Objectives-based approach to Reliability and Maintainability

General structure for top-level goals for GSN assurance case

[2] Groen, F.J.; Evans, J.W.; Hall, A.J., "A Vision for Spaceflight Reliability: NASA's Objectives Based Strategy," RAMS, 2015, 26-29 Jan. 2015

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



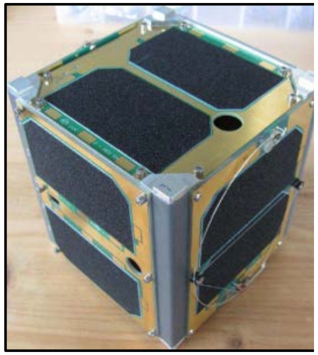
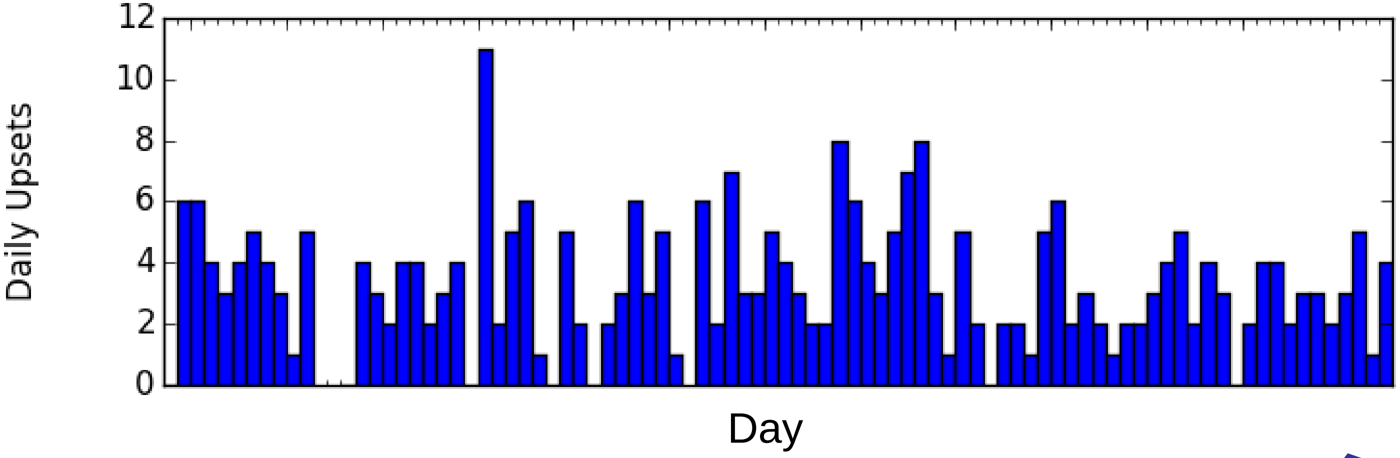


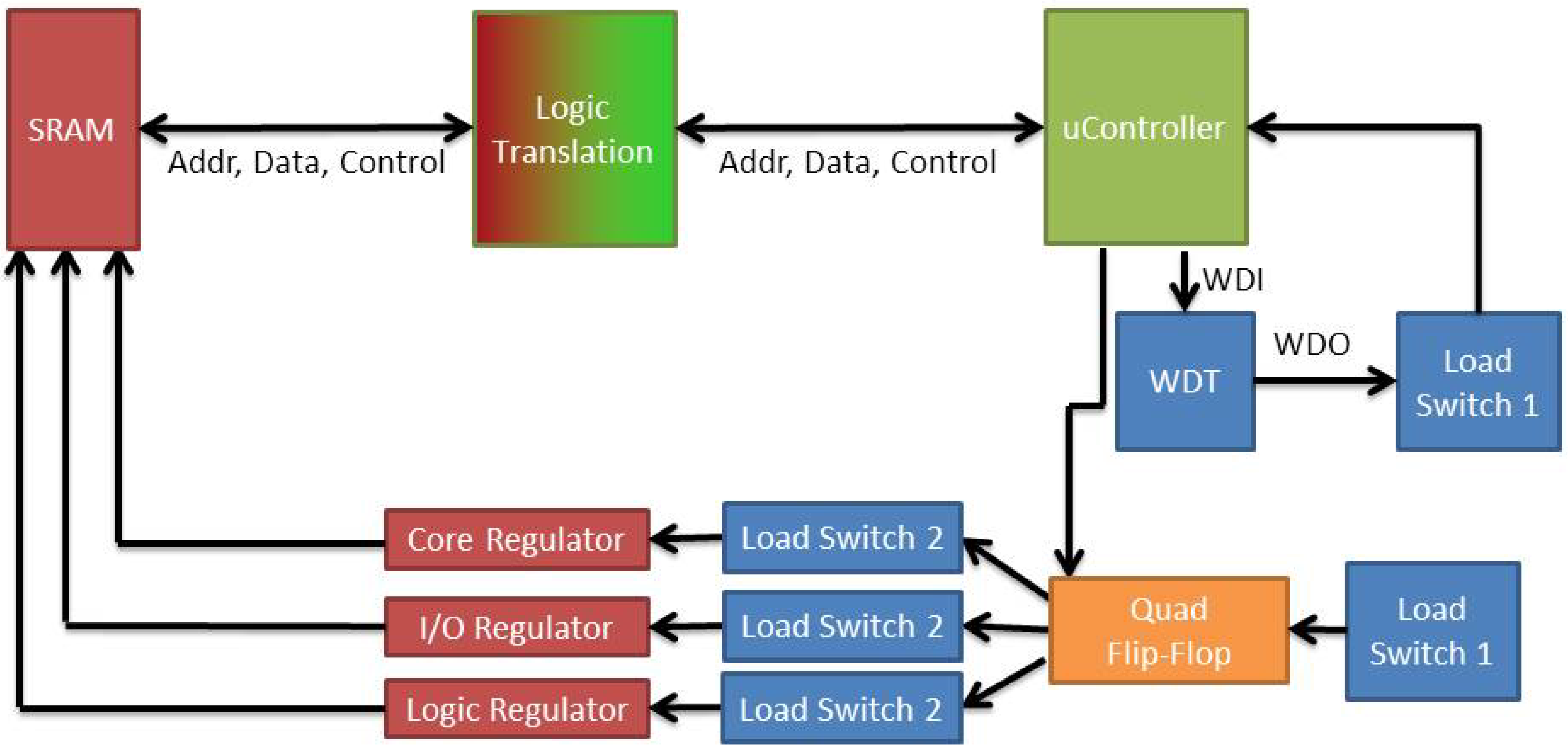
Image Credit: AMSAT



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

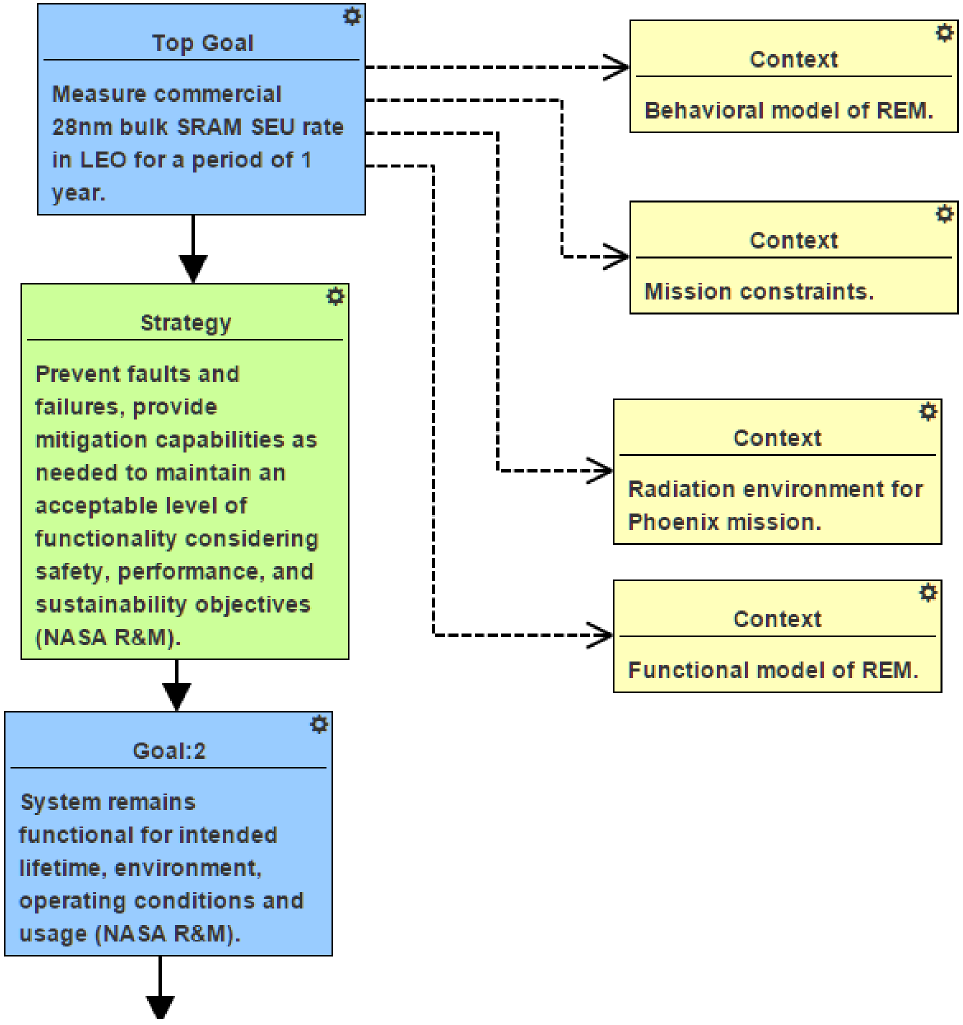
- Launch January 2017
- Radiation Effects Modeling (REM) Board
- SEU detection in the SRAM
  - Protect data from other SEEs on the board
  - Count upsets from SEUs in SRAM, not SELs
- Current monitors for latch up detection
  - Monitor separate for SRAM and other components
  - High-current on SRAM causes 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

Block Diagram SRAM SEU Experiment Board



Sub-Class D: Allow latch-up, employ mitigation
Current monitors, watch-dog timer sense SEL

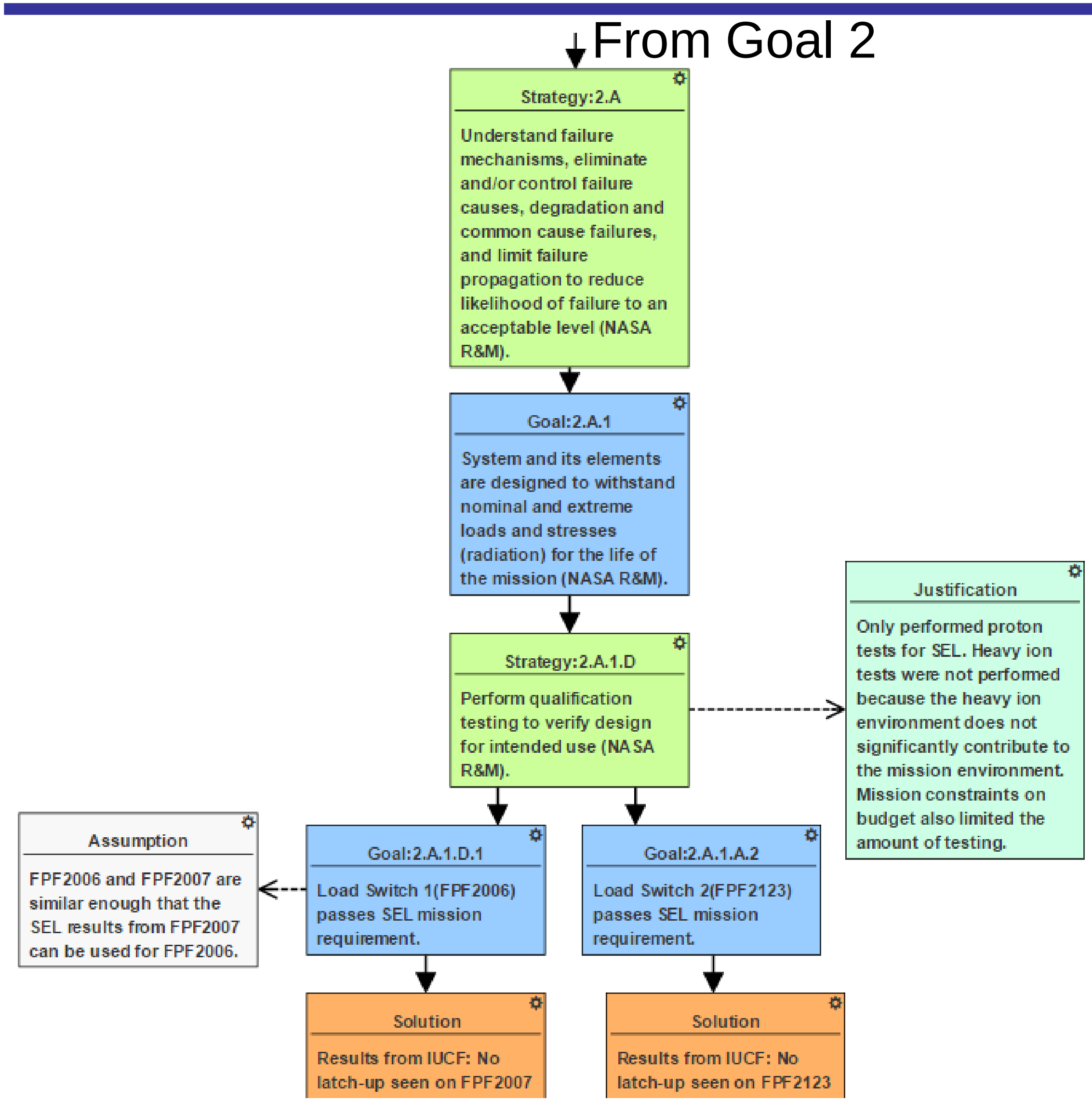
GSN Assurance REM SEU Experiment Board


Top Goal
Measure commercial 28nm bulk SRAM SEU rate in LEO for a period of 1 year.
Strategy
Prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives (NASA R&M).
Goal:2
System remains functional for intended lifetime, environment, operating conditions and usage (NASA R&M).
Context
Behavioral model of REM.
Context
Mission constraints.
Context
Radiation environment for Phoenix mission.
Context
Functional model of REM.

To Strategy 2

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

GSN Assurance REM SEU Experiment Board



From Goal 2

Strategy:2.A

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 (NASA R&M).

Goal:2.A.1

System and its elements are designed to withstand nominal and extreme loads and stresses (radiation) for the life of the mission (NASA R&M).

Strategy:2.A.1.D

Perform qualification testing to verify design for intended use (NASA R&M).

Justification

Only performed proton tests for SEL. Heavy ion tests were not performed because the heavy ion environment does not significantly contribute to the mission environment. Mission constraints on budget also limited the amount of testing.

Assumption

FPF2006 and FPF2007 are similar enough that the SEL results from FPF2007 can be used for FPF2006.

Goal:2.A.1.D.1

Load Switch 1(FPF2006) passes SEL mission requirement.

Goal:2.A.1.A.2

Load Switch 2(FPF2123) passes SEL mission requirement.

Solution

Results from IUCF: No latch-up seen on FPF2007

Solution

Results from IUCF: No latch-up seen on FPF2123

- 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