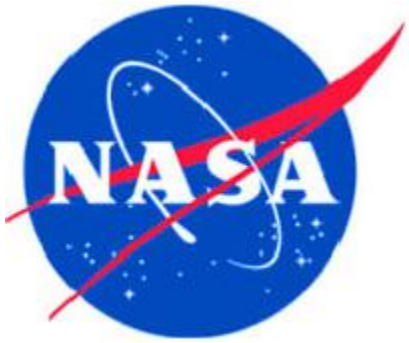


Goal Structuring Notation in a Radiation Hardening Assurance Case for COTS-Based Spacecraft

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

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

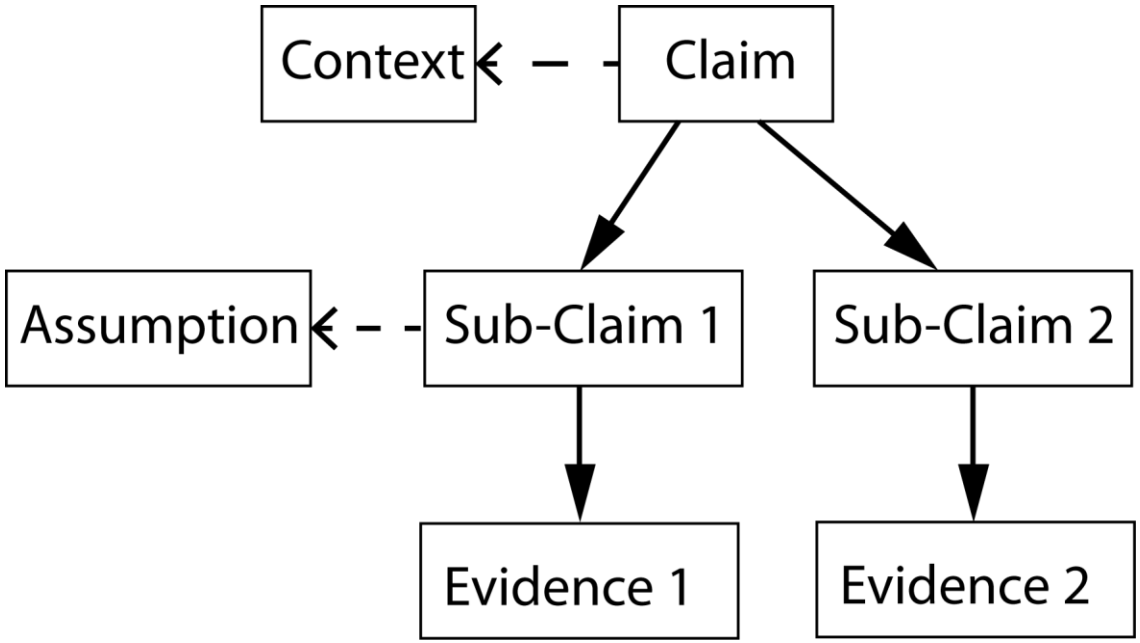
This work supported under NASA Grant and Cooperative Agreement Number NNX15AV48G

Background: Mission Assurance

Vanderbilt Engineering

- **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

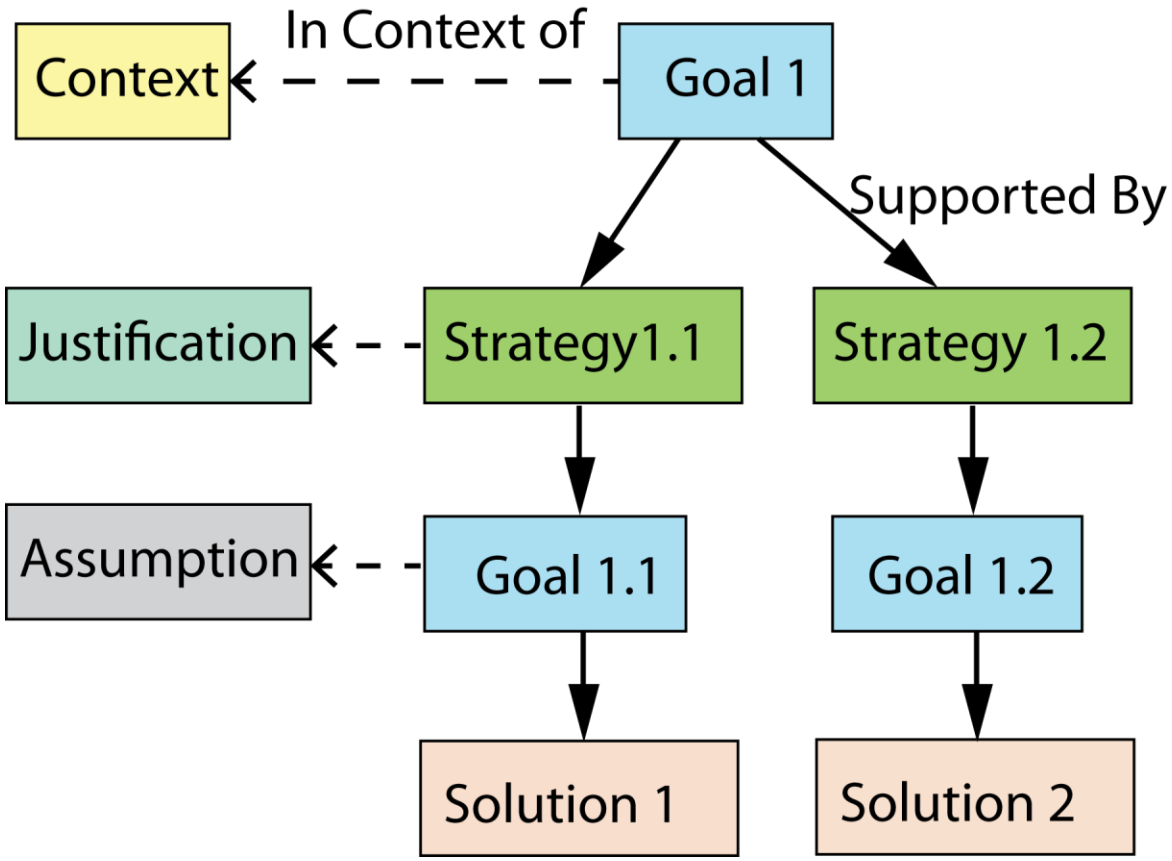


Argument: "A connected series of claims intended to support an overall claim." [1]

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]

[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=Unsub-stantiated Claim

Colors/Shapes Denote Function

[1] GSN Community Standard Version 1 2011

Benefits of GSN

Vanderbilt Engineering

- 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

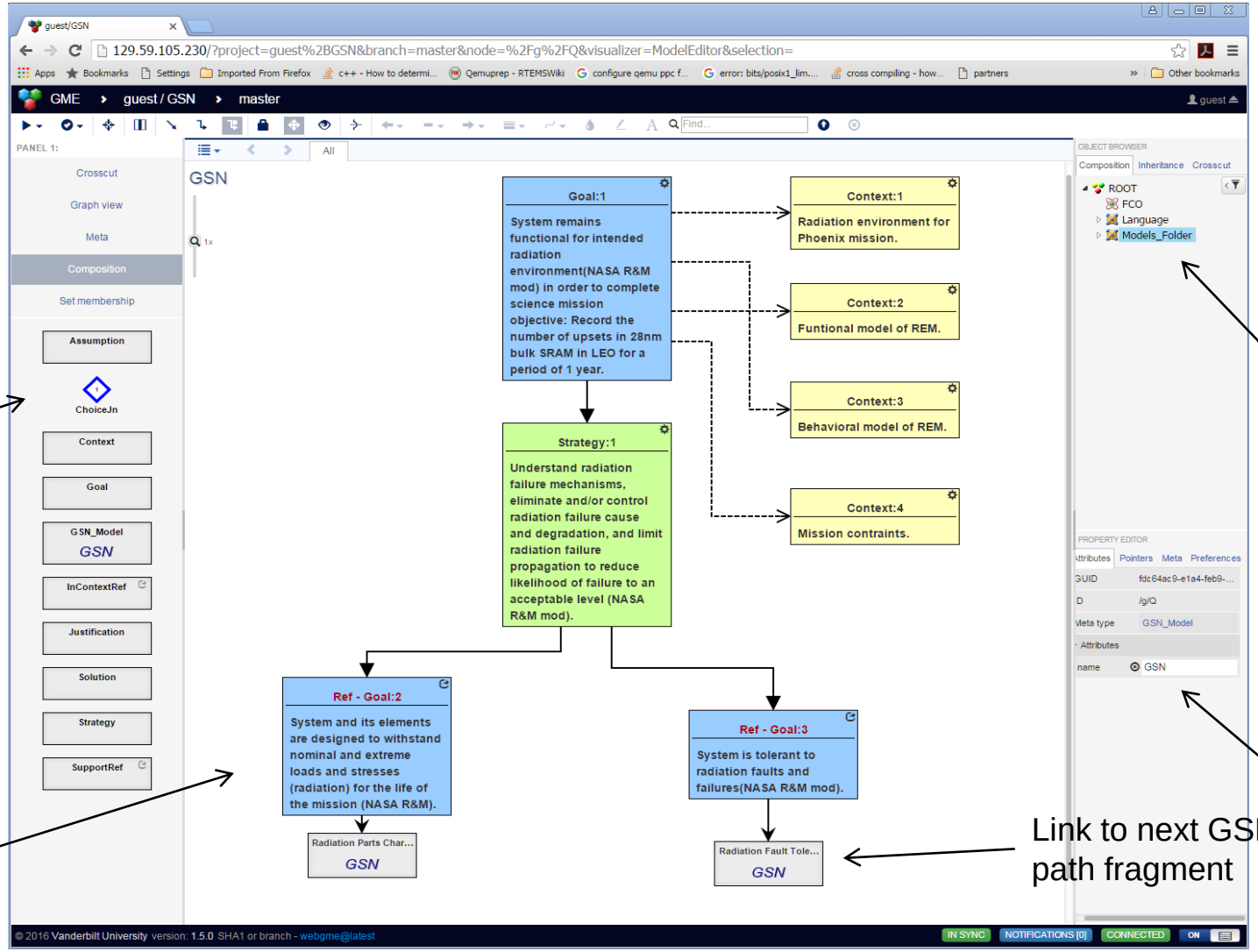
Vanderbilt Custom GSN Modeling Language

Vanderbilt Engineering

- **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

Vanderbilt Engineering



Model Parts Panel

Model Tree Browser

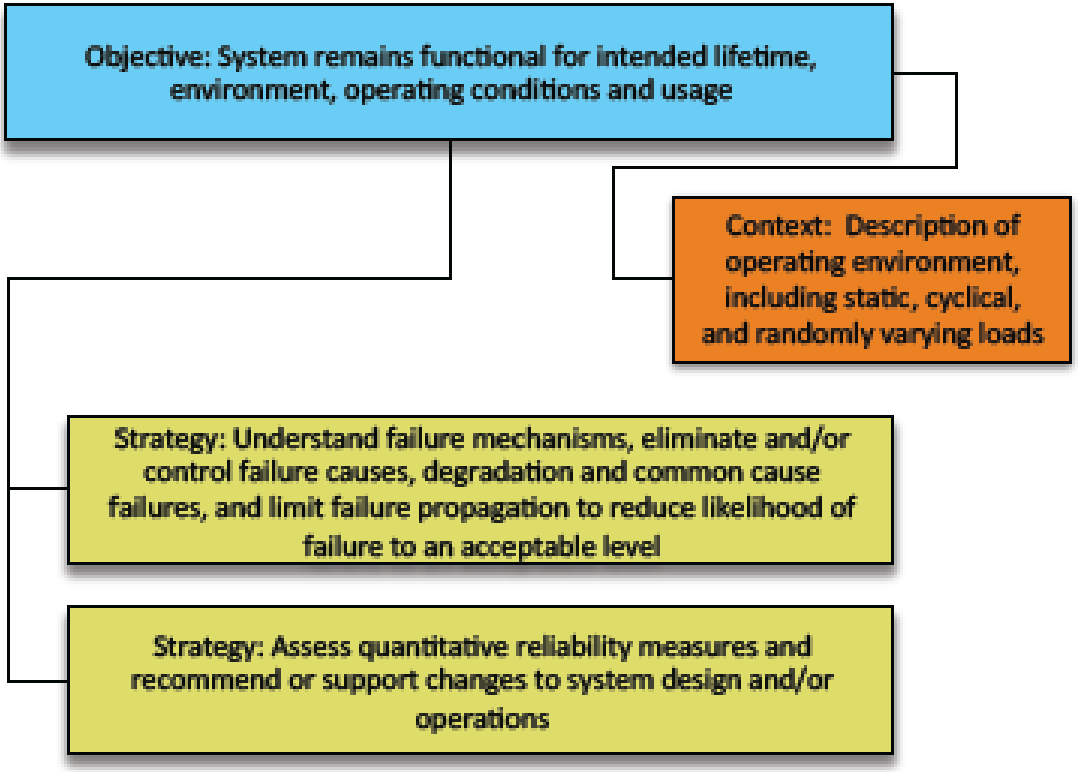
Attributes Panel

Model Editor Canvas

Link to next GSN path fragment

NASA Reliability & Maintainability Template

Vanderbilt Engineering



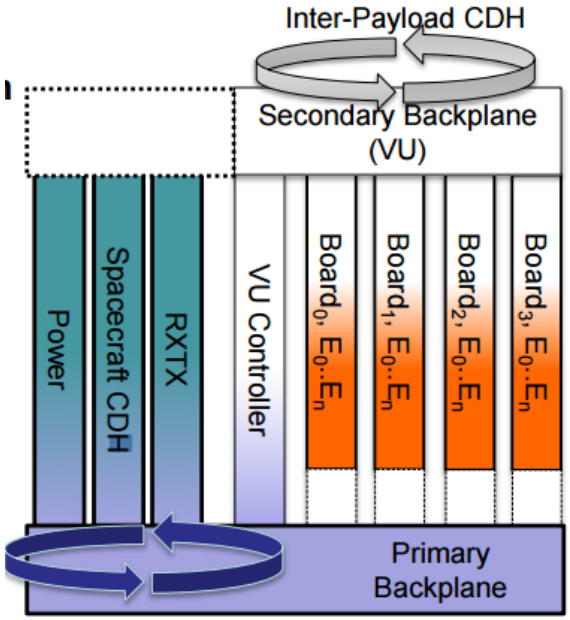
Objectives-based approach to Reliability and Maintainability

General Structure for top-level goals in 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 Cube Sat SRAM Experiment Test Bed

Vanderbilt Engineering



- VU Cube Sat Architecture
- Space environment radiation test bed for TID, SEE
- Successful 8 x 4Mb SRAM experiment, launched 2015, reports SEUs, resets, power

Primary CDH

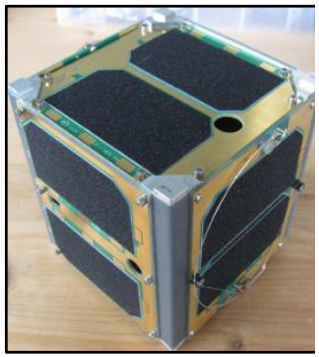
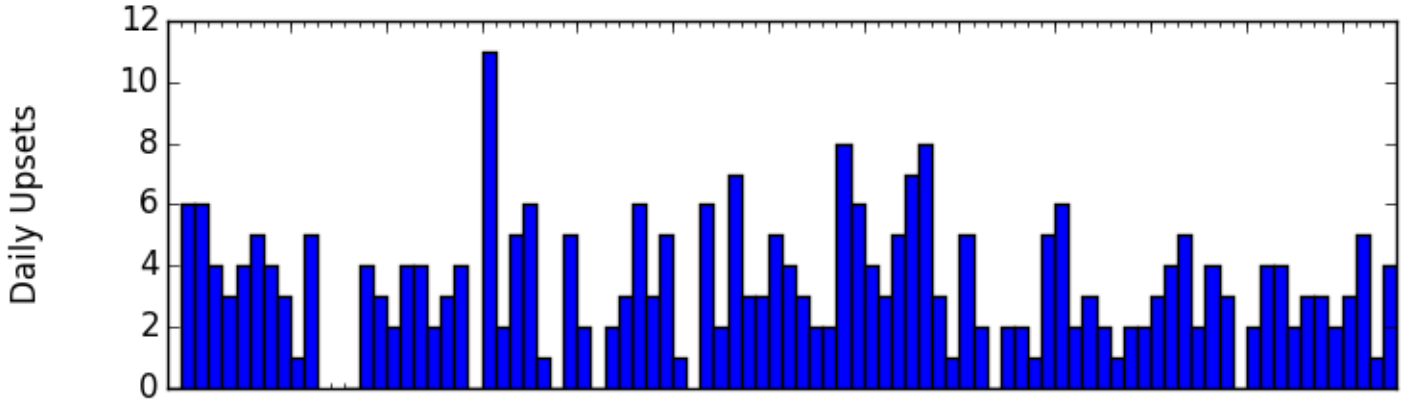


Image Credit: AMSAT



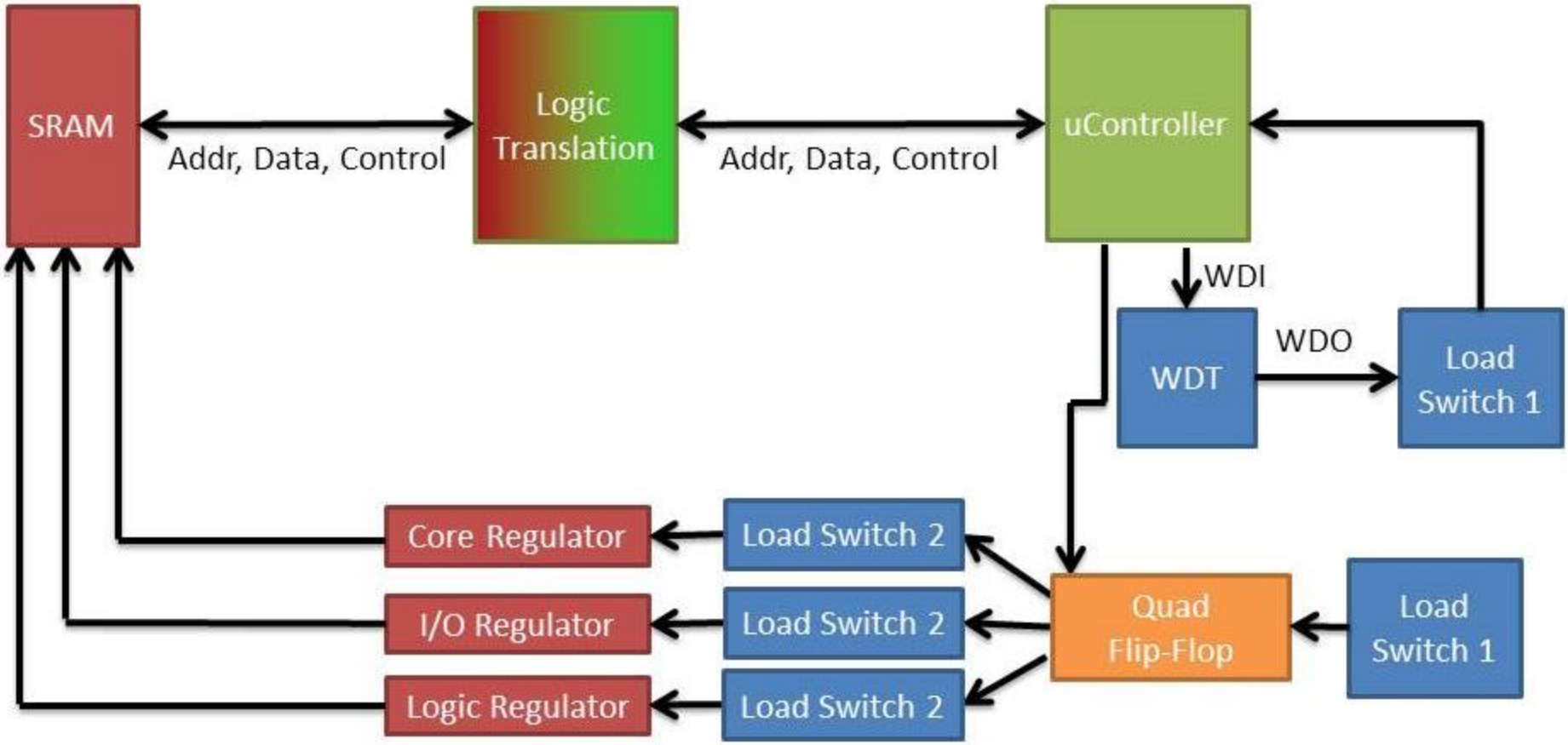
GSN Demo Case: 28nm Commercial SRAM SEU Test in LEO

Vanderbilt Engineering

- Launch December 2016
- Radiation Effects Modeling (REM) Board
- Detect SEUs in the SRAM
  - Protect data from other SEEs 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

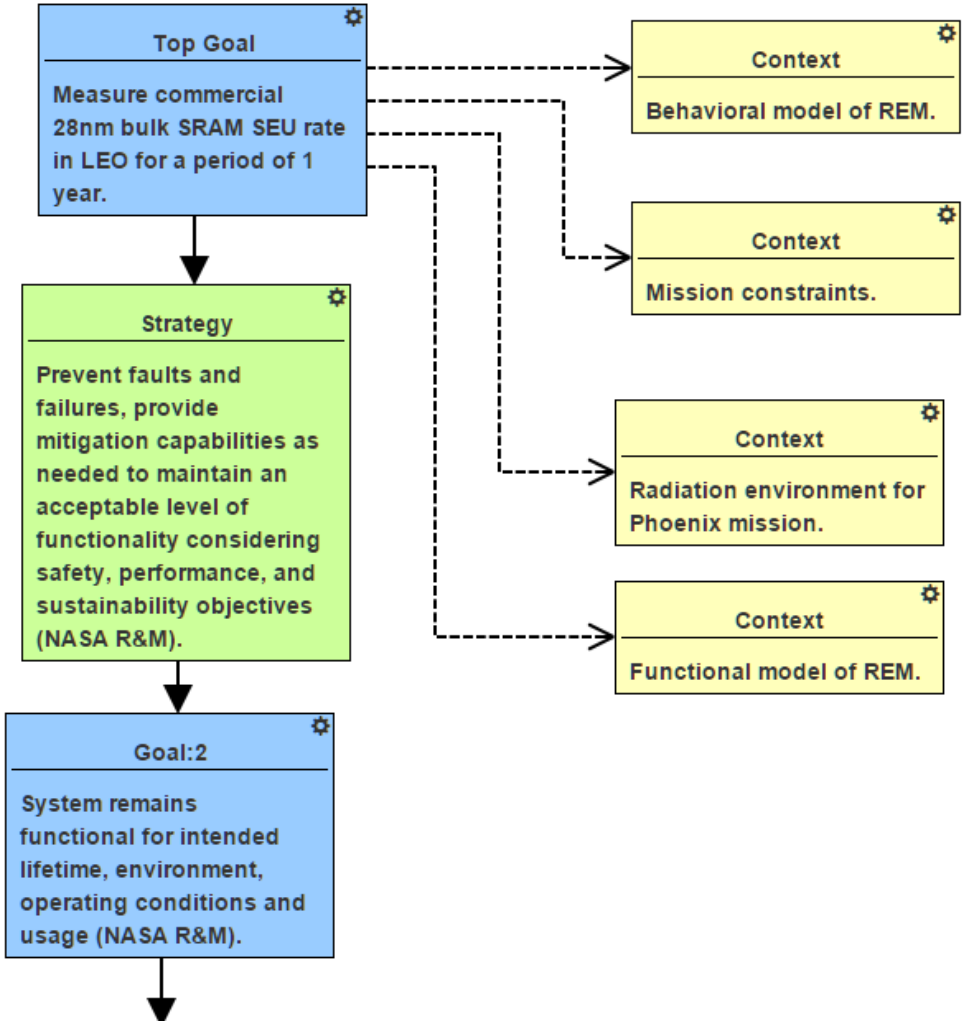
Block Diagram SRAM SEU Experiment Board

Vanderbilt Engineering



Mitigation techniques for latch-up in board components

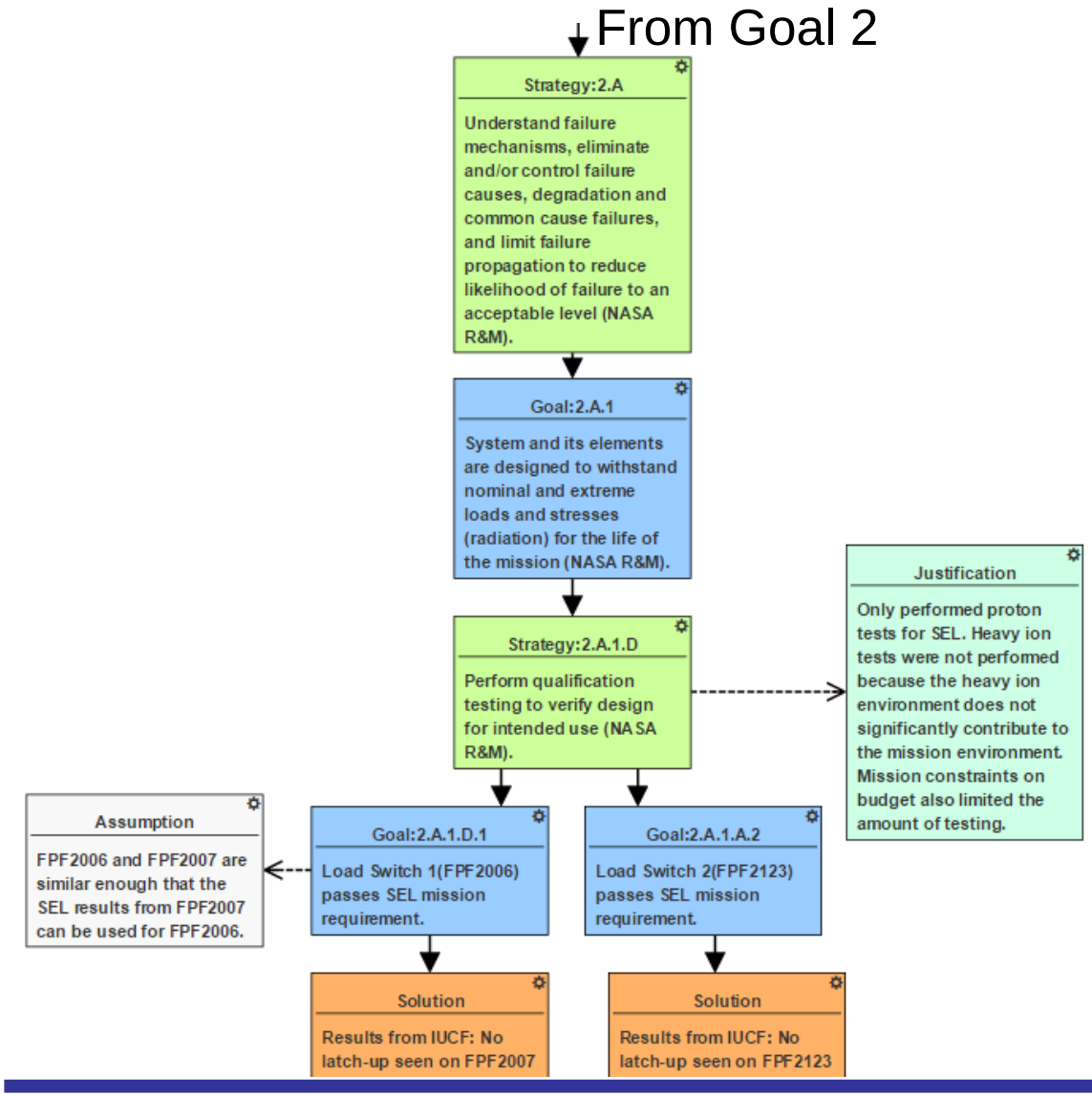
GSN Assurance REM SEU Experiment Board



- 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

GSN Assurance REM SEU Experiment Board

Vanderbilt Engineering



- Not all branches of GSN graph shown
- Assumptions are clearly identified
- Argument path terminates in Solution
- Validity of Assuance case determined by reading from Solutions to top level goals.

Summary