

NEPP ETW 2017



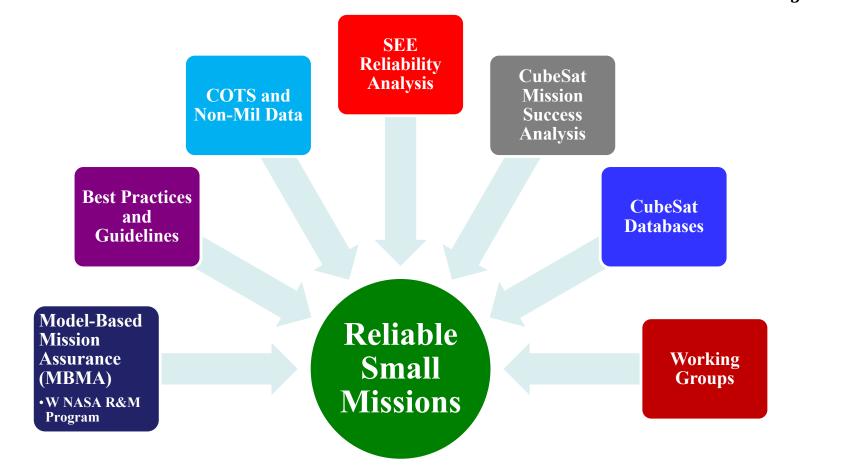
Reliability Assurance of CubeSats using Bayesian Nets and Radiation-Induced Fault Propagation Models

A. Witulski, R. Austin, G. Karsai, N. Mahadevan, B. Sierawski,R. Schrimpf, R. Reed

This work supported by NEPP and the NASA Reliability and Maintainability Program under Grant and Cooperative Agreement Number NNX16AR25G

NEPP - Small Mission Efforts





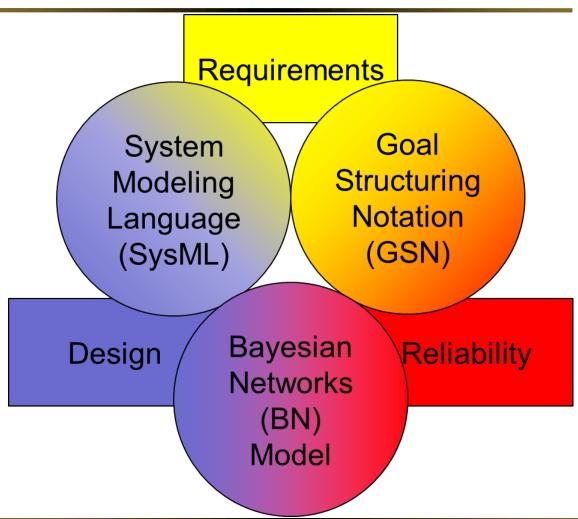


Requirements

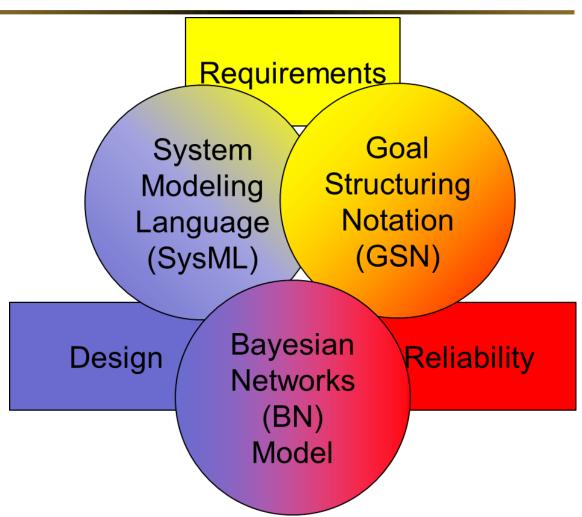
Design

Reliability





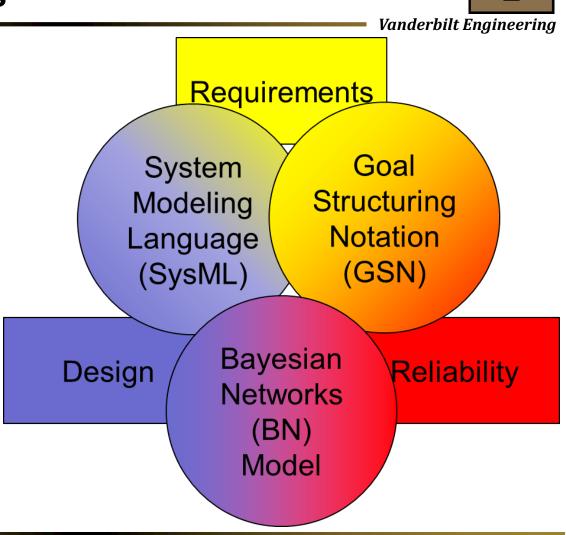






Reasons for Activity interaction

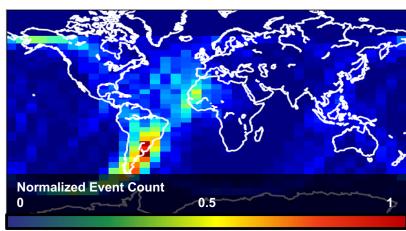
- Commercial parts (COTS)
- Document-centric work flow to model-based system engineering
- Smaller teams
- System mitigation (for COTS)
- Shorter schedules for small spacecraft



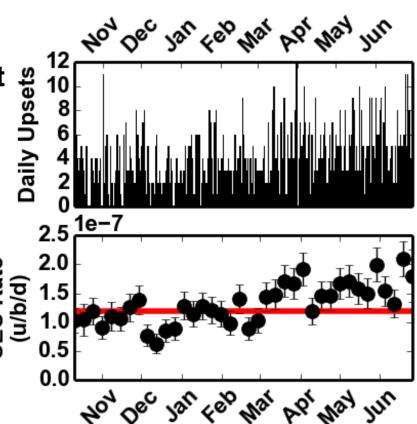
Demo Vehicle: CubeSats, VU/Amsat AO-85 Results



- Launched October 8th, 2015 as part of ELaNa-XII
- 800-500 km, 65° inclination orbit
- Carries 65nm SRAM SEU experiment



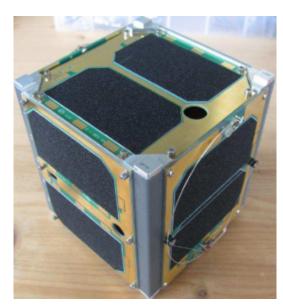
Geolocation of SEUs



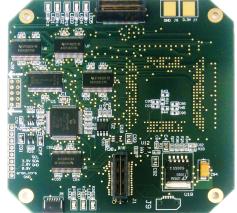
Radiation Reliability Assessment of CubeSat SRAM Experiment Board

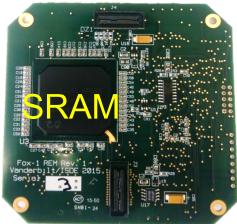


- Assessment completed on REM
 - 28nm SRAM SEU experiment
- Reasons for integrated modeling
 - 1. Use commercial off-the-shelf (COTS) parts
 - 2. System mitigation of SEL
 - 3. System mitigation of SEFI on microcontroller



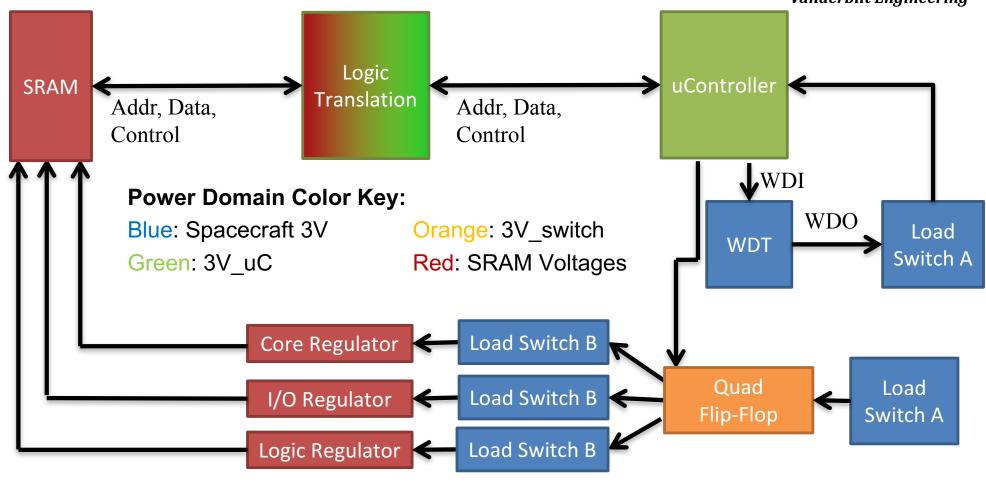
Courtesy of AMSAT





System-level RHA: Block Diagram of 28nm SRAM SEU Experiment





Overview of Model Integration of SysML, GSN, BN



Vanderbilt Engineering

SysML-Description

Functional Requirements

Related to radiation effects

Cross Reference

Design/ Architecture

- Hierarchical Block Diagram models
- Component / Subsystem interface and interconnection.
- Fault Model Radiation induced fault effects and their propagation

Components/ Functionalities

GSN-Safety Case

- Model-based documentation of arguments for radiation reliability assurance
- Construct argument template from R&M hierarchy and System Models

Feedback,

Design iteration

BN Inference

Bayes Nets-Cause/Effect

Causal Relationship

Construct BN structure by traversing the fault propagation paths

Overview of Modeling Approaches Used



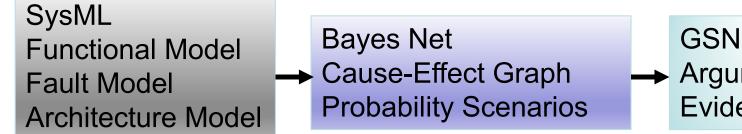
Vanderbilt Engineering

BN Network SysML GSN Specification of systems Nodes describe probabilities of Visual representation through standard notation of argument states Added fault propagation Goals, Strategies, Calculate conditional and Solutions paths probabilities from observations Single Event Environmen Goal:1 Isolate and contain Latch up fault effects close to the fault source. Input Vdd Absent 50% Correct 100% Present 50% Strategy:1 ncorrect 0% Containment by load switches. Word Correct 100% Goal:2 Solution:1 Wrong 0% Corrupted 20% The load switch on Results from IUCF: When v3p3_uC detects high the beam was pointed at current conditions (>1A) the microcontroller, high-SRAMData and shuts down the power current conditions resulted in the v3p3 uC to be shut down. Bad 16%

Integrated Model-Based Assurance Path



Vanderbilt Engineering



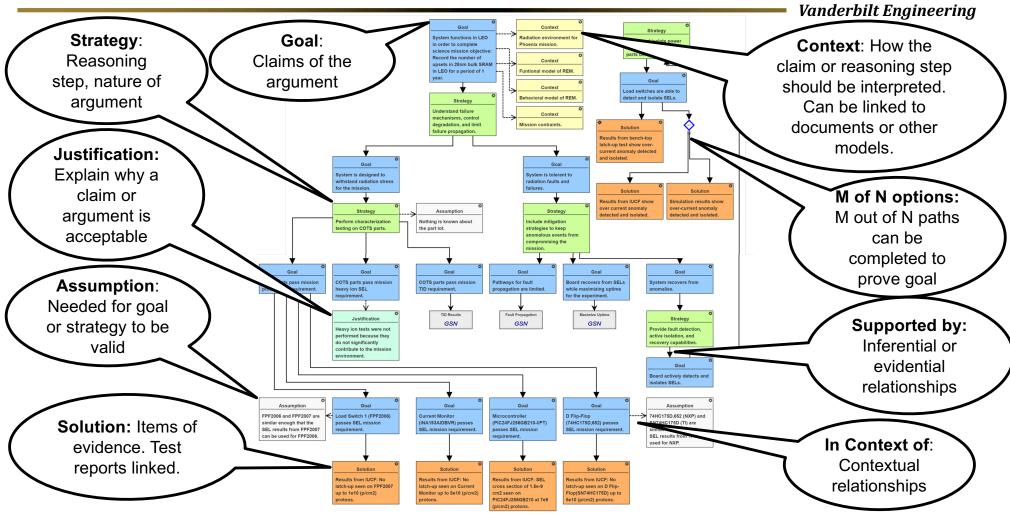
Argument Structure Evidence from BN

Objectives

- -Obtain systematic coverage of possible faults
- -Move towards quantitative assessment of risk/reliability

Goal Structuring Notation (GSN): Visual Representation of an Argument





Austin - A CubeSat-Payload Radiation-Reliability Assurance Case

NASA Reliability & Maintainability (R&M) Template



Vanderbilt Engineering

 Old Paradigm: Reliability proven through list of tests passed

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

Proposed New Paradigm: NASA Reliability & Maintainability (R&M) Template created to change reliability requirements to be objective-based (Groen, RAMS 2015)

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

- Based on Goal Structuring
 Notation
- Created with Class A Missions in mind
- Graphical structure to reliability requirements allows for integration with MBSE

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

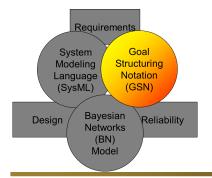
R&M Template (Groen, RAMS 2015)

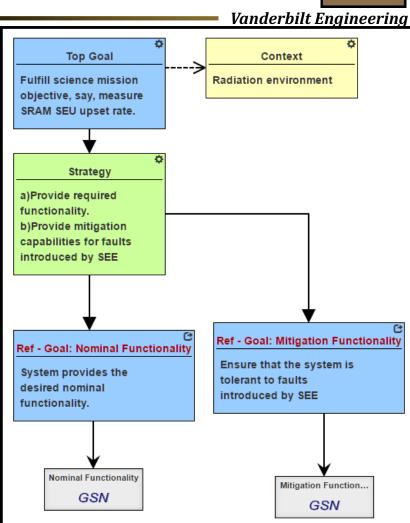
 Can an assurance case for the radiation-reliability of a sub-Class D mission be made? Is it useful?

Top Level GSN Model of REM Experiment Board



- Top level goal: Complete science mission objective
- Strategies: Provided functionality and mitigate radiation environment
- Goals: Validation of "Nominal" and "Mitigation" functionalities
 - Focused on radiation-induced faults





GSN Models for Single Event SRAM Experiment



Vanderbilt Engineering <u>Identify</u> **Validate Mitigation Functions Validate Nominal Functions** Component Goal: Nominal Functionality Mitigation functionality at **Susceptibility** each level of the system System provides the desired nominal has been verified and validated functionality. Goal: Understand susceptibility Strategy to SEE for components Test mitigation (and maybe subsystems Test functionality of each functionality of each component and component and subsystem to meet subsystem to meet desired mitigation desired functionality functionality ₩ Strategy Goal Test SEE susceptibility of Test "Processing" each component (and Test "Handle SEE" maybe subsystem?) through all fault "Functions" "Functions" propagation paths in system model. to validate to validate Ref -Goal **Functionality Test Results Blocks** Goal Test "Exec Instructions" Test "Power Regulation" Test "Store Data" a) Test "Trim Current at **Test SEE Susceptibility** Max" Test "Handle SEI" Test "Handle SEFI" b) Test "Regulate power" a) Power Bus Solution: b) Voltage Regulator Solution Goal **Functionality Test Results** c) Load Switch Goal **Functionality Test Results** Test "Power Regulation" d) SRAM Test "Detect High Test "Detect Missing a) Test "Trim Current at Test "Reset" e) Microprocessor Current" Heartbeat" f) WDT b) Test "Regulate power" g) Microprocessor+ Voltate Regulator + Load Switch **Functionality Test Results** Goal h) SRAM + Voltate Goal Regulator + Load Switch Test "Power Cycle" Test "Power Supply" Solution Solution SEE susceptibility test **Functionality Test Results** SEE Mitigation functionality results

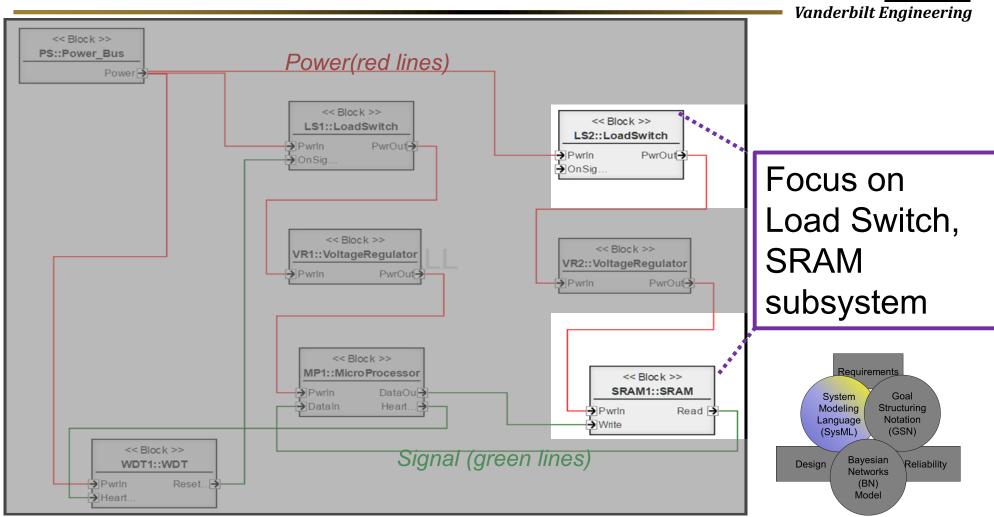
SysML Block Diagram of REM Experiment Board



Vanderbilt Engineering << Block >> PS::Power Bus Power(red lines) Power -<< Block >> << Block >> LS1::LoadSwitch LS2::LoadSwitch → Pwrln PwrOut-OnSig. OnSig. << Block >> << Block >> VR1::VoltageRegulator VR2::VoltageRegulator PwrOut-PwrOut-<< Block >> Requirements MP1::MicroProcessor << Block >> SRAM1::SRAM Pwrln DataOu-Goal System **→** DataIn Heart.. Modeling Pwrln Structuring Read -Notation Language (SysML) << Block >> Signal (green lines) Bayesian WDT1::WDT Reliability Networks → Pwrln Reset... (BN) Model Heart.

SysML Block Diagram of REM Experiment Board

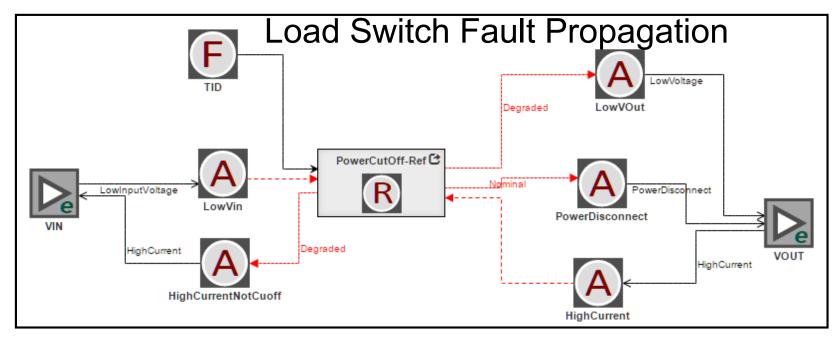




SysML Internal Block Diagram with Fault Propagation Paths

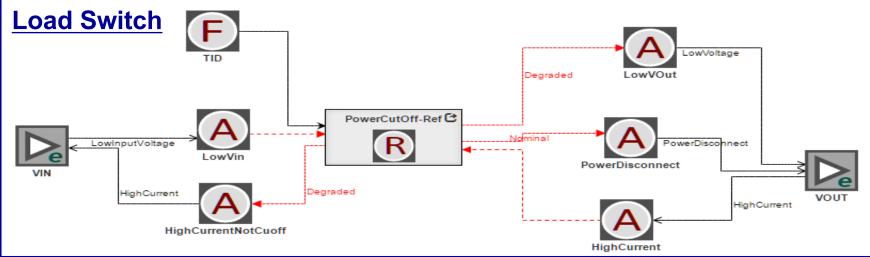


- Fault (F) Change in physical operation, depart from nominal
- Anomaly (A) Observable effect or anomalous behavior from fault
- Response (R) Intended response of component to A and F (mitigation)



Fault Model – Load Switch





- A LowInputVoltage anomaly (from another component) leads to appropriate *Nominal* response from PowerCutOff function, leading to PowerDisconnect
- A HighCurrent anomaly (from another component) leads to appropriate *Nominal* response from PowerCutOff function, leading to PowerDisconnect
- TID fault could affect load switch response, leading to *Degraded* PowerCutOff functionality
 - LowInputVoltage anomaly could be passed on to the component downstream
 - HighCurrent anomaly may not be detected or cutoff

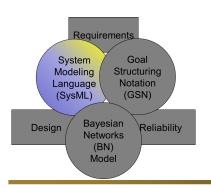
SysML Internal Block Diagram with Fault Propagation Paths

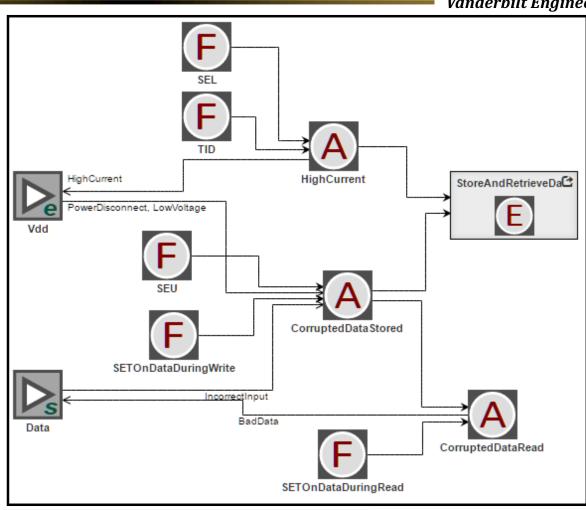


Vanderbilt Engineering

SRAM

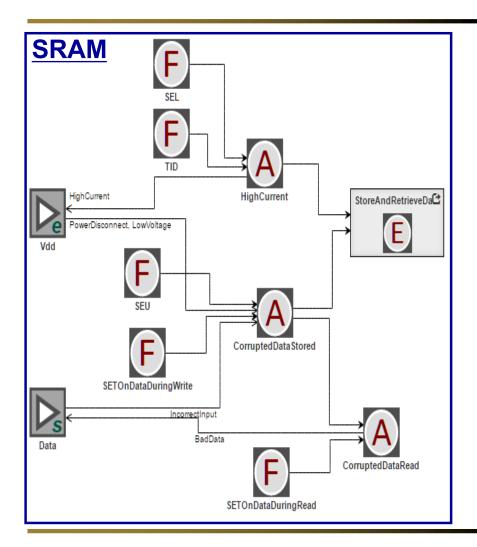
- Effects (E) impact on functionality
- Faults/Anomalies
 flow through ports
 to affect other
 components





Fault Model - SRAM

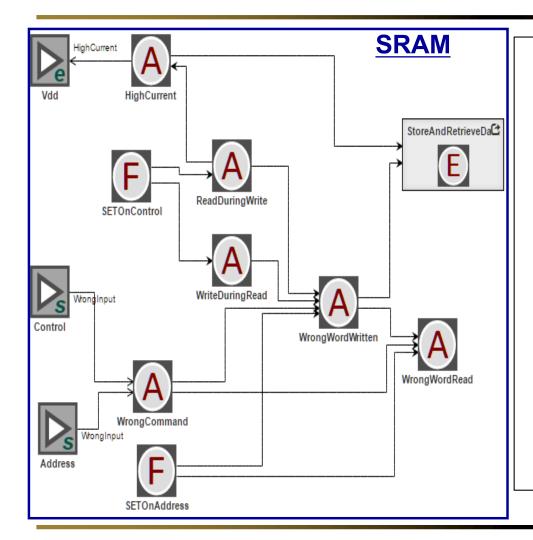




- SEL, TID faults could lead to HighCurrent anomaly
- HighCurrent failure-effect is output to other components through the Vdd power-port
- SEU, SETonDataDuringWrite faults could lead to CorruptedDataStored anomaly
- PowerDisconnect, LowVoltage, IncorrectInput failure-effects from other components could also lead to CorruptedDataStored anomaly
- CorruptedDataRead anomaly results from CorruptedDataStored anomaly as well as SETonDataDuringRead fault. Further, it leads to output of BadData failure-effect
- StoreAndRetrieveData functionality can be degraded (Effect node) due to HighCurrent as well as CorruptedDataStored anomalies

Fault Model – SRAM cntd.





- SETOnControl fault could lead to ReadDuringWrite and WriteDuringRead anomalies, which could lead to WrongWordWritten anomaly.
- ReadDuringWrite could lead to HighCurrent anomaly.
- WrongInput failure-effect from other components to Control or Address ports could lead to WrongWordWritten or WrongWordRead anomalies.
- SETonAddress fault could lead to WrongWordWritten or WrongWordRead anomalies.
- StoreAndRetrieveData functionality can be degraded (Effect node) due to HighCurrent as well as WrongWordWritten anomalies.

Custom Modeling Environment - WebGME

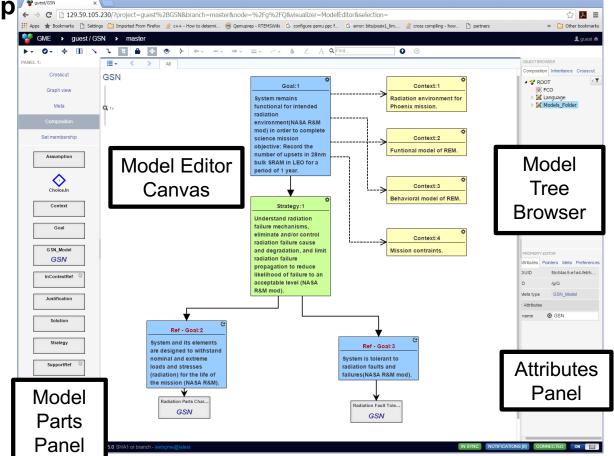


Vanderbilt Engineering

 WebGME is used to develop the modeling framework

- Models include:
 - Goal Structuring Notation (GSN)
 - System model (SysML)
 - Fault Propagation
 - Function/Behavior Models
- Allows for links across models
- Links to external documents

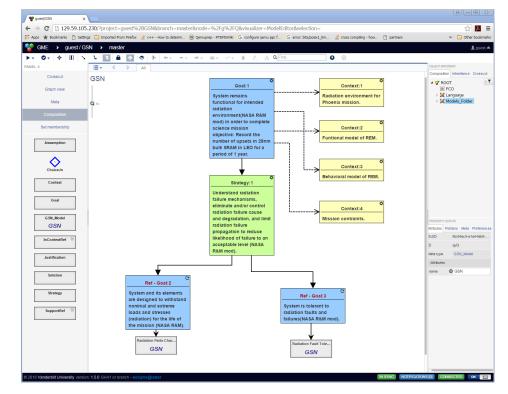
https://webgme.org/



Model-Based Assurance Case (MBAC+ (=WebGME)) for Radiation Hardness Assurance Activities



- Tutorial at **NSREC 2017 Tuesday, July 18th**, during lunch
- Learn how to use NASA's Reliability and Maintainability Template to construct a radiation reliability assurance case
- Modeling environment also supports SysML Block Diagram modeling with fault propagation (no Bayesian nets yet)
- Browser based
- Free non-proprietary site hosted on Amazon (AWS) (like Crème)
- Free images of site for proprietary or export controlled modelling for hosting on Amazon GovCloud or internal servers



Bayesian Network Models



Vanderbilt Engineering

BN Structure

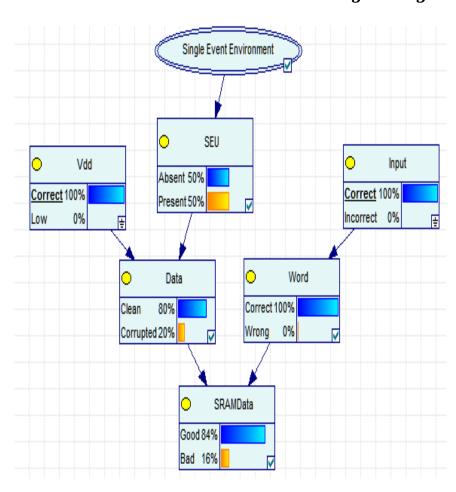
- Node are probabistic or determinstic variables in a domain
- Nodes can also be discrete or continuous.
- Directed edges capture the dependency relationship between the nodes

BN Parameters

- State of a probabilistic nodes are expressed as probability (or probabistic distribution)
- Dependency relationship of a child node on its parents is expressed in terms of conditional probability tables (or likelihood functions)

BN Inference

 The BN inference process estimates the probabilistic distribution (posterior) of each node, when the states of certain nodes are fixed (observation/ evidence)



Development of Bayesian Network Models from SysML



Vanderbilt Engineering

SysML models
- Architecture, Fault Models

- Functional requirement models

Traverse design model from each fault to generate flat causal relationship graph.

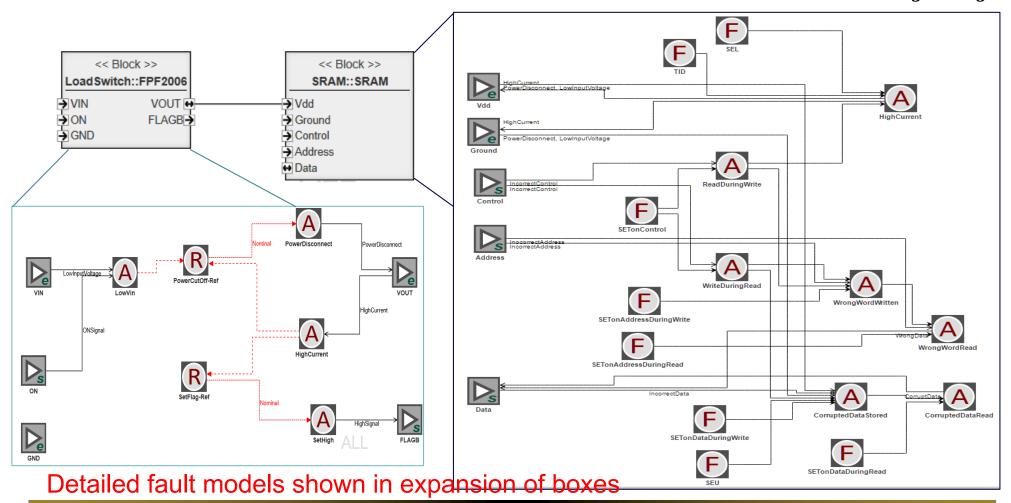
For each component/ subsystem sub-graph, add functionality (leaf node) based on functional model (if not present).

Identify states, likelihood relations, prior and conditional probabilities. Prune graph based on expert knowledge, convenience etc. Add additional edges based on functional dependency. Add additional nodes (edges) for higher level functions (functional model).

Merge common nodes across fault paths - faults, anomalies, functional effects and responses.

SysML Fault Models SRAM/Load Switch Sub-System



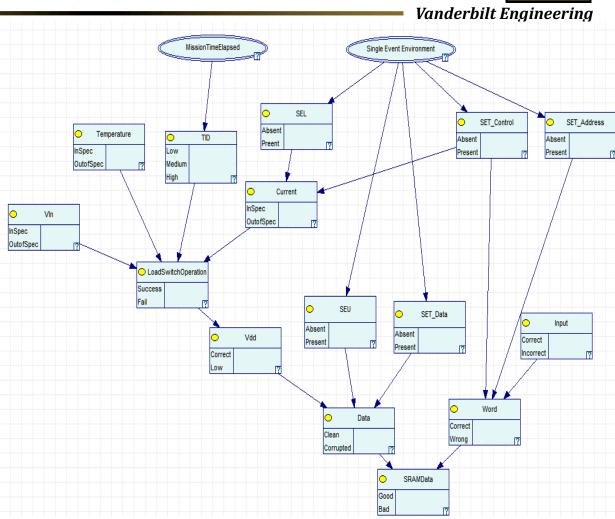


Bayesian Network SRAM/Load Switch (1/3)



Determinstic Node Description:

- MissionTimeElapsed: Time elapsed in the mission can be set to any of the following states
 - < 1 year for Low TID
 - 1-2 year for moderate TID
 - > 2 year for High TID
- SingleEventEnvironment: The current environment can be set to any of the following states
 - Low Rate Region: Low probability of SEE occurrence.
 - South Atlantic Anomaly (SAA): Greater probability of SEE occurence



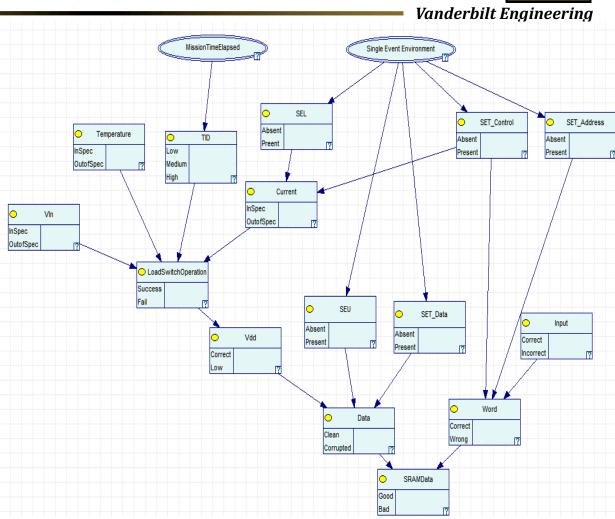
Bayesian Network SRAM/Load Switch (2/3)



Probabilistic Nodes Description (1/2):

Probability of ...

- TID: Presence/level of TID
- SEL: Occurrence of Latch up
- Current: Supply current being in spec
- Temperature: Load Switch temperature being in spec.
- Vin: Load Switch input voltage being in spec
- LoadSwitchOperation: Quality ("success") of load switch operation to cut off power



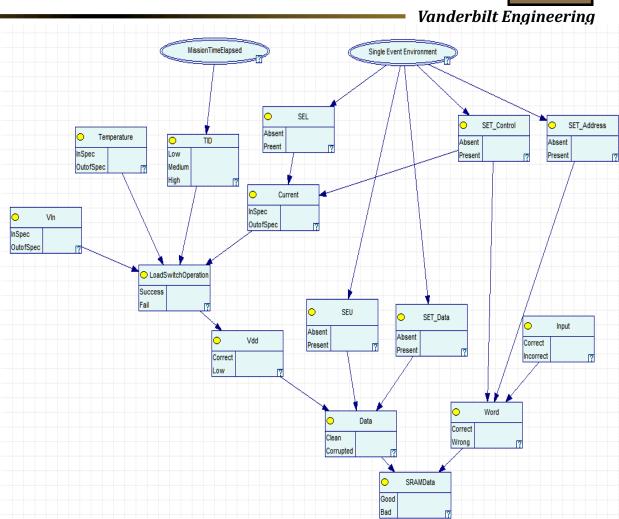
Bayesian Network SRAM/Load Switch (3/3)



Probabilistic Nodes Description (2/2):

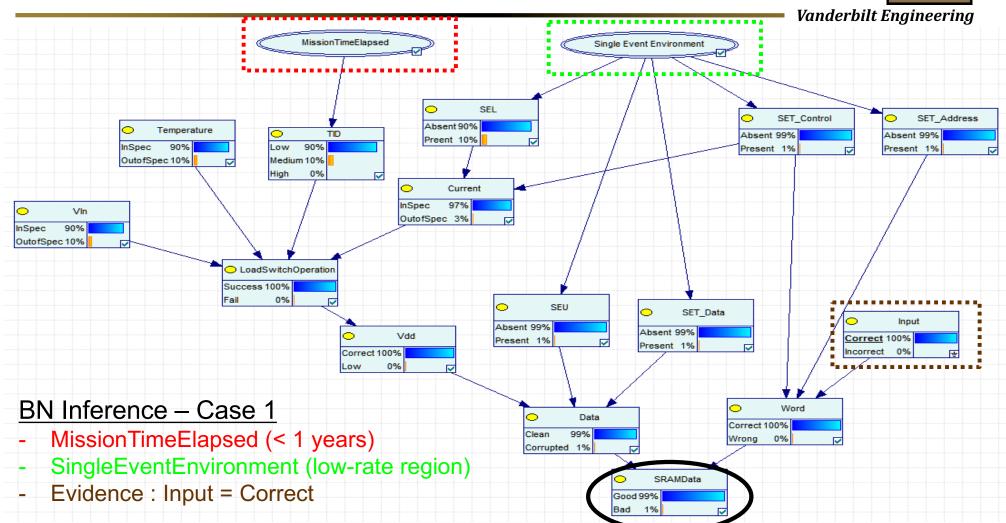
Probability of ...

- SEL: Occurrence of Latch up
- SEU: SRAM- occurrence of upsets
- SET_x (x=control, address, data):
 SRAM occurrence of transients on control, address, data ports
- Input: Incorrect input to SRAM
- Vdd: Input Power to SRAM being correct or low
- Data: SRAM data being correct or corrupted
- Word: SRAM words being correct or wrong
- SRAMData: SRAM Data being correct



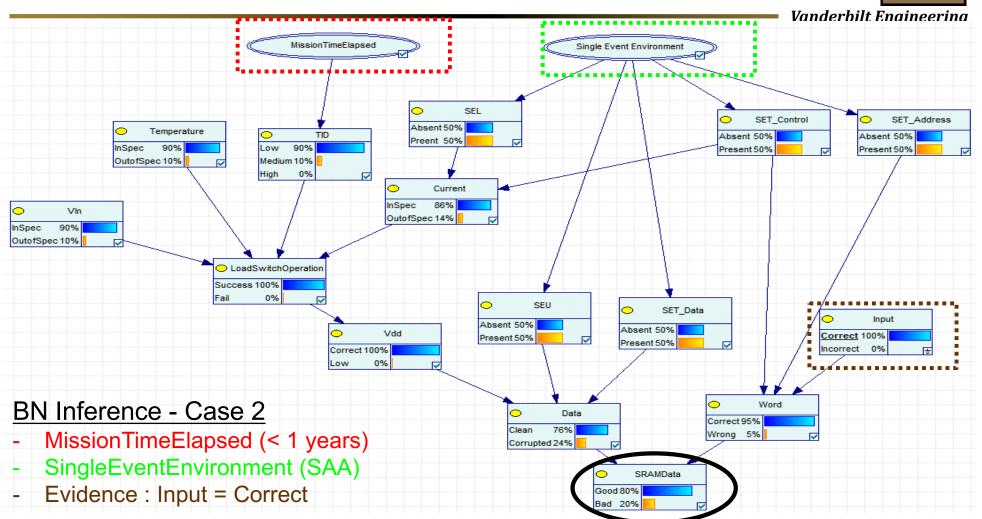
Bayesian Network Inference – Case 1





Bayesian Network Inference – Case 2





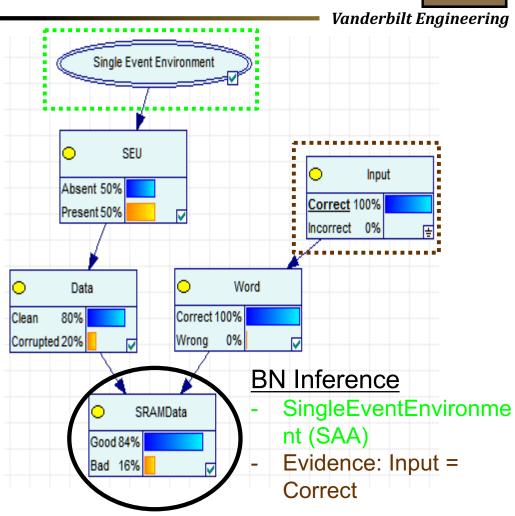
Inference with Pruned Bayesian Network



BN Pruned based on

 Load Switch operates correctly for mission time of 2 years

- Remove Load switch portions
- 2. SET probability of affecting SRAM is very little
- Remove SET_* nodes
- 3. Input to SRAM is correct
- Input (data)= Correct
- SEE environment set to LEO or SAA
- Shows sensitivity of SRAM data to SEE environment



Transition and Related Work with JPL



Vanderbilt Engineering

Related Project with JPL

- Command and Data Handling (C&DH) Board
- Build reliability models and Safety case for subset of C&DH functions



Lunar Flashlight 6U Form Factor

Sphinx C&DH Board



"CubeSat flight system development for enabling deep space science,"T. Imken et al, IEEE Aerospace Conference 2017

Summary



 Developed integrated process for model-based assurance case for radiation reliability

Constructed example
 SysML models augmented
 with radiation-induced faults
 and propagation

 BN inference "observations" used to assess impact of various faults on SRAM performance

