



Reliability Assurance of CubeSat Payloads using GSN, Bayesian Nets and Radiation-Induced Fault Propagation Models

Arthur Witulski, P.I., Gabor Karsai, Co-P.I., Nag Mahadevan, Rebekah Austin, Brian Sierawski, Ron Schrimpf, Robert Reed

Sponsored by NASA OSMA, NEPP Grant #NNX16AR25G, and JPL OSMS, Subcontract 1568812

Small Satellite TIM 10/11/17

Integrated System Design for Radiation Environments*



Vanderbilt Engineering

Requirements

*This slide and many of the following from: R. Austin, "Reliability Assurance of CubeSat Payloads using Bayesian Nets and Radiation-Induced Fault Propagation Models," Single Event Symposium 2017

Design



Integrated System Design for Radiation Environments





Motivation for Alternate Reliability Approach



- Shift from document-centric to model-centric repository of design information (SysML)
- Shift from prescriptive reliability paradigm to objectivesbased paradigm for reliability
 - NASA-STD-8729.1A Reliability and Maintainability Std.
 - Goal Structuring Notation (GSN)
- Increased use of COTS parts on spacecraft
 - Relatively little info on physics of parts available from manufacturers
 - High variability in radiation response of COTS parts
 - Well-suited to probabilistic modeling (Bayesian nets)
- Rapid acceptance and deployment of small spacecraft
 - Short schedule, limited budget and resources
 - Extensive radiation testing and rad-hard parts not feasible

Chronological Overview of Research Effort



- Year 1 (FY 2016): Use of GSN to create a safety case for the impact of single events on a Cube Sat experiment board
 - Sponsored by John Evans (OSMA/HQ) and Ken LaBel (NEPP)
- Year 2 (FY 2017): Development of SysML/GSN/BN model on Cube Sat Experiment board
 - Sponsored by John Evans (OSMA/HQ) and Ken LaBel (NEPP)
 - Development and launch of public website deployed on AWS
- Year 2 (FY2017): TID and Reliability Modeling of Sphinx C&DH board
 - Sponsored by Harald Schone and Phillipe Adell (OSMS) at JPL
 - First task: deterministic modeling of TID impact on system parameters
 - Second task: application of SEAM modeling to Sphinx board

Chronological Overview – Proposed Work



- Vanderbilt Engineering
- Year 3 (FY 2018): Reliability of Cube Sat Board
 - Improve SysML import compatibility (e.g. MagicDraw),
 - move into automatic creation of Bayesian nets
 - Integrate with other reliability approaches
 - Sponsored by Ken LaBel (NEPP) and John Evans (OSMA/HQ)
- Year 3 (FY2018): TID and Reliability Modeling of Sphinx C&DH board
 - TID modeling task: Work towards higher fidelity modeling, incorporation of software in simulation
 - SEAM tasks: create model library for Sphinx board components, interface SEAM modeling to IRIS system modeling (UCLA)
 - Sponsored by Harald Schone and Phillipe Adell (OSMS) at JPL

Foundation: NASA Reliability & Maintainability (R&M) Hierarchv

۲



Basis of NASA-STD-8729.1 (R&M Standard) Context: Expectations derived from crew safety, MMOD concerns, facility safety, public Incorporates R&M into MBSE safety, mission obj., sustainment..... considerations and associated risk tolerance Top Objective: System performs as required over the lifecycle to satisfy mission objectives Moves to objectives-based Context: System/function description and requirements. including design information reliability requirements and interfaces Context: Reference mission + Strategy: Prevent faults and failures, provide before/after mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and Context: Range of nominal/ sustainability objectives off-nominal usage and conditions/environments **Objective: System** Objective: System is Objective: System is **Objective:** System remains functional for designed to have an tolerant to faults. conforms to design intended lifetime, acceptable level of failures and other intent and performs availability and environment, anomalous internal as planned operating conditions maintenance and external events (1) and usage demands (3)(4)

(2)

Graphical Assurance Cases





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): Visual Representation of an Argument



Goal:3 Justification:1 Assumption:1 System and its elements Heavy-ion SEL tests were Radiation tests are not performed because the are designed to withstand performed on parts with nominal and extreme heavy-ion environment the same part number and loads and stresses does not significantly manufacurer but nothing (radiation) for the life of contribute to the radiation is known about the lot. the mission (NASA R&M). environment. ChoiceJr Strategy: Strategy:6 Strategy:3 Strategy:4 Strategy:5 Reasoning Process does not have Perform proton SEL Perform TID Effects of SEL are mitigated on system parts. parasitic thyristors. characterization tests on characterization tests on step, nature of system parts. system parts. argument Context:5 Goal:5 Goal:6 COTS parts pass mission COTS parts pass TID Parts that did not pass proton SEL requirement: requirement at 30 proton SEL requirement or No latch-up seen up to 5e9 krads(SiO2). did not have proton SEL (p/cm2) protons. testing performed: Microcontroller, WDT, regulators, logic Supported by: translator, and Goal:10 Goal:19 mux/demux. Inferential or Microcontroller **Current Monitor** evidential (PIC24FJ256GB210-I/PT (INA193AIDBVR) passes SEL mission requirement. passes TID mission relationships requirement: Supply current <18mA, runs flight program, and can be reset. Solution: Items of Solution:3 Goal: Results from IUCF: No evidence. Test latch-up seen on Current Claims of the reports linked. Monitor up to 5e10 (p/cm2) protons. argument

Model Integration of SysML, GSN, and BN*





Overview of Modeling Languages Used



| SysML | GSN | BN Network |
|---|---|---|
| Specification of systems through standard notation Added fault propagation paths | Visual representation of argument Goals, Strategies, and Solutions | Nodes describe probabilities of states Calculate conditional probabilities from observations |
| VI VI VI VI VI VI VI VI VI VI VI VI VI V | Goal:1 Isolate and contain Latch up fault effects close to the fault source. Strategy:1 Containment by load switches. Goal:2 The load switch on v3p3_uC detects high current conditions (>1A) and shuts down the power bus. | Single Event Environment ✓ Vdd SEU Absent 50% Fresent 50\% Fresent 50\% Frese |

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







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
 - Adapted from NASA R & M
 <u>Standard</u>





SysML Block Diagram of REM Experiment Board



V

SysML Block Diagram of REM Experiment Board



SysML Internal Block Diagram with Fault **Propagation Paths** Vanderbilt Engineering Load Switch Requirements Goal System - Faults (F) - Nominal response Modeling Structuring Language Notation (SysML) (GSN) – Anomalies (A) - Degraded response Bayesian Design Reliability Networks - Responses (R) - Ports (BN) Model LowVoltage Degraded LowVOut



SysML Internal Block Diagram with Fault **Propagation Paths**

ullet

System

Modeling

Language

(SysML)

(BN)

Model

Design





Pruned Bayesian Network Model of the REM Experiment Board

- SEE environment set to LEO or SAA
- Input is data from microcontroller
 - Assumed correct
- Show sensitivity of SRAM data to SEE environment







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



Modeling JPL Sphinx C&DH Board: Issues of Scale



- Sphinx much more complex than Cube Sat board
- Hierarchy for managing complexity
- Schemes for categorizing subsystems
- Subsystems based on functionality
- Components belong to more than one subsystem



Advantages of Functional Strategy:

- Specifies purpose of components
- Simplifies functional models
- Parallels thinking of GSN arguments
- Abstraction level same as deterministic simulation
- Disadvantages:
- Uses same components in multiple subsystems





GSN Radiation Parts Characterizations







Deriving the Bayesian Net from SysML Models for the Temperature Loop Subsystem



- Block Diagram view includes all components directly involved in system functionality
- Links connection paths directly involved in system functionality
- Visualizes fault and failure propagation paths



Temperature Control Bayesian Net



 BN only considers TID (no SELs or external faults)

- MissionTime branch sets TID
- System output is board temperature
- PowerAvailability node represents stress on satellite power bus due to increased heater usage
- Annotations add details and assumptions







Jet Propulsion Laboratory California Institute of Technology

Overview of TID and Reliability Modeling of the JPL Sphinx C&DH Board

- Arthur Witulski, P.I., Gabor Karsai, Co-P.I., Nag Mahadevan, Jeff Kauppila,
- Ronald Schrimpf, Robert Reed

JPL Sphinx C&DH Block Diagram



V



- **Problem**: How to estimate impact of transistor-level degradation on system-level performance?
 - Need fast modelling turn-around time so process can be iterative
 - Must be able to accommodate many signal and part types
 - Analog-SPICE-like continuous waveforms
 - Pure digital (one-zero level)
 - Digital in the electrical domain
 - Behavioral: VHDL and Verilog AMS
 - Software: Control algorithms, etc.
 - Must be tolerant of incomplete knowledge of part performance and radiation behavior
 - Need fast run time so Monte Carlo Bayesian approach is possible

Demonstration: Temperature regulation loop model with TID Degradation



Radiation modeling embedded in parameter variation



- The Questa ADMS simulation package from Mentor Graphics is the simulation engine within the Expedition PCB design flow
 - Capable of co-simulating SPICE, Behavioral (Verilog, Verilog-AMS, VHDL, VHDL-AMS), and SystemC
 - Synchronization of time steps and convergence routines
- Questa's ability to simulate models from multiple hierarchy levels provides the capability to model a complex system
 - Accurate and detailed transistor level models (Temp Sensor)
 - IBIS models at digital interfaces for signal integrity
 - Behavioral level models for complex circuits (ADC, FPGA, etc.)
- We have successfully simulated behavioral models, IBIS models, Spice models and SystemC within one netlist and transient simulation

Temperature Regulation Loop – Questa ADMS





Questa ADMS Simulation Results - Temperature





Continuous Bayesian Network (BN) Model



Vanderbilt Engineering

TID k_1, k_2, k_3 V_TS a_1, a_2, a_3 Code = a₁+ Code_ADC i_σ,s_σ Error_Ctrl_Inp

Legend

- X
- -- Stochastic node X= Gaussian(μ , σ)
- Deterministic node (V_TS, Code, μ_e,σ_e)
 Root Nodes with Uniform priors (Temp, TID)
- <mark>n.</mark> -- Likelihood Function for deterministic nodes

BN Model (PyMC code)

- BN Nodes \rightarrow Domain Variables and function parameters.
- Relationship between Nodes \rightarrow Likelihood functions.

BN Setup/ Observations (Test bench data)

- Initialize parameter nodes with (prior) probability distributions.
- Associate evidence (data) with appropriate BN nodes.

BN Execution

- Markov Chain Monte Carlo sampling algorithms sample prior distributions and evaluate outputs (likelihood functions).
- Iterate until predictions converge to observed data.

BN Results

- Posterior (updated) distribution for each node.
- Use posterior distributions of parameters to get an estimation of the spread (distribution) in domain variables such as
 - Output voltage of temperature sensor (V_TS)
 - Output code from ADC (Code_ADC)
 - Error in input to controller (Error_Ctrl_Input)

Continuous Bayesian Network Results





Questa ADMS Sim Distributions Electrical and Radiation Parameters



Regulated Temperature - Set Point = 290 K 310 Temperature (K - Volts in Simulation) 305 300 Dotted Lines = Monte Carlo Sims (10 runs) 295 290 285 280 Pre-Rad - Nominal 275 TID = 30 kRad - Nominal —Desired 270 20 10 15 0 5 Time (s)

Set point = 290 K

Monte Carlo analysis of the circuit with Pre-Rad and 30 kRad component models Black shows component variations pre-rad

Conclusions



- Vanderbilt Engineering
- Board-level modeling requires simulation of analog, mixed-signal, and fully digital components, as well as software
- Created modeling and simulation paradigm for a fully capable, multidomain board simulator using Mentor Questa with SystemC
 - Shows the impact of component-level variations on board-level system parameters
 - Fast run times for long simulation clock times
 - Fully customizable abstraction levels from software to all-digital to behavioral models to Spice-like circuit simulation
 - Compatible with other Mentor products like circuit board layout and parasitic tools
 - Parameter variation and Monte Carlo simulation capability
- Simulation demonstrates significant impact on the system-level variable (Temperature) owing to TID degradation of ADC and sensor
- Clear road map for next steps in C&DH radiation modeling