Vanderbilt Engineering

Model-Based Mission Assurance

Rebekah Austin, Brian Sierawski, Arthur Witulski, Nag Mahadevan, Gabor Karsai, Ronald Schrimpf, Robert Reed

This work is supported by NASA Electronic Parts and Packaging and the NASA Office of Safety and Mission Assurance, Reliability and Maintainability Program under Grant and Cooperative Agreement Number 80NSSC18K0493

Vanderbilt Engineering

Acronym and Abbreviations

AMSAT: Radio Amateur Satellite Corporation
AO-85: AMSAT OSCAR Satellite #85
AO-91: AMSAT OSCAR Satellite #91
BN: Bayesian Network
COTS: Commercial Off-the-Shelf
DoD: Department of Defense
ELaNa: Educational Launch of Nanosatellites
FinFET: Fin Field Effect Transistor
FRAM: Ferroelectric Random-Access Memory
GSN: Goal Structuring Notation
I2C: Two wire communication Protocol
LEO: Low-earth orbit
LEP: Low-energy proton
LEPF: Low-energy proton FinFET
MBE: Model-Based Engineering
MBMA: Model-Based Mission Assurance
MBSE: Model-Based System Engineering
MOSFET: Metal-oxide-semiconductor field-effect transistor
NASA: National Aeronautics and Space Administration
NXP: Parts Manufacturer
OSCAR: Orbiting Satellite Carrying Amateur Radio
RadFxSat: Radiation Effects Satellite
R&M: Reliability and Maintainability
REM: Radiation Effects Modeling
RHA: Radiation Hardness Assurance
SEE: Single-event effects
SEFI: Single-event functional interrupt
SEL: Single-event latch-up
SEU: Single-event upset
SRAM: Static random-access memory
SSO-A: Sun Synchronous Express
STMicro: STMicroelectronics, parts manufacturer
SysML: System Modeling Language
TI: Texas Instruments, parts manufacturer
TID: Total-ionizing dose
VUC: Vanderbilt University Controller
WDI: Watchdog Timer Input
WDO: Watchdog Timer Output
WDT: Watchdog Timer

Visit nasa.gov

OSMA
OFFICE OF SAFETY & MISSION ASSURANCE

Print Version

Is Model-Based Mission Assurance the Future of NASA SMA?

NOVEMBER 09, 2015 // RELIABILITY AND MAINTAINABILITY, RELIABILITY AND MAINTAINABILITY

Share Like 1

Model Based Mission Assurance (MBMA): NASA's Assurance Future

John Evans, PhD, NASA OSMA
Steven Cornford, PhD, JPL
Martin S. Feather, PhD, JPL

Key Words: Assurance, Model Based Systems Engineering

SUMMARY & CONCLUSIONS

Model Based Systems Engineering (MBSE) is seeing increased application in planning and design of NASA's missions. This suggests the question: what will be the corresponding practice of Model Based Mission Assurance (MBMA)?

Contemporaneously, NASA's Office of Safety and Mission Assurance (OSMA) is evaluating a new objectives-based approach to standards to ensure that the Safety and

environments. For these reasons and more, it is anticipated MBSE will enable more capable missions without sacrificing cost-effectiveness despite increase in complexity. Because of its growing adoption in the aerospace industry and because it is imperative that there is also no sacrifice of safety and mission success, NASA's OSMA has initiated a roadmapping effort to pave the way for full integration of mission assurance into this model-based world – "Model Based Mission Assurance."

Visit nasa.gov

SUMMARY & CONCLUSIONS

Model Based Systems Engineering (MBSE) is seeing increased application in planning and design of NASA's missions. This suggests the question: what will be the corresponding practice of Model Based Mission Assurance (MBMA)?

Key Words: Assurance, Model Based Systems Engineering

SUMMARY & CONCLUSIONS

Model Based Systems Engineering (MBSE) is seeing increased application in planning and design of NASA's missions. This suggests the question: what will be the corresponding practice of Model Based Mission Assurance (MBMA)?

Contemporaneously, NASA's Office of Safety and Mission Assurance (OSMA) is evaluating a new objectives-based approach to standards to ensure that the Safety and

environments. For these reasons and more, it is anticipated MBSE will enable more capable missions without sacrificing cost-effectiveness despite increase in complexity. Because of its growing adoption in the aerospace industry and because it is imperative that there is also no sacrifice of safety and mission success, NASA's OSMA has initiated a roadmapping effort to pave the way for full integration of mission assurance into this model-based world – "Model Based Mission Assurance."

Model-Based Engineering

Vanderbilt Engineering

- **Model-Based Engineering: An approach to engineering that uses models as an integral part of the technical baseline that includes the requirements, analysis, design, implementation, and the verification of a capability, system, and/or product throughout the acquisition life cycle**

- **Model: A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. (DoD 5000.59-M 1998)**

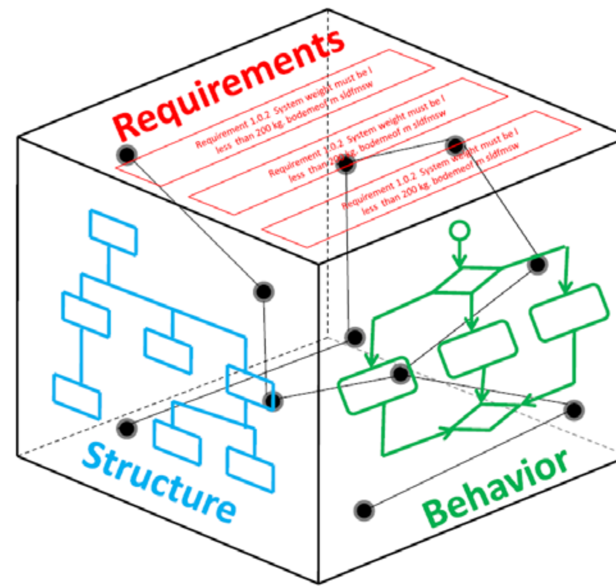


Image Credit: MBSE Connects the Dots (U.S. Army)
http://armytechnology.armylive.dodlive.mil/index.php/2015/07/01/15-3/

NDIA Final Report of the Model Based Engineering (MBE) Subcommittee, 2011.

Characteristics of Models

- **Models apply to a wide range of domains (eg. systems, software, electrical, mechanical, human behavioral, logistics, manufacturing, business, socio-economic, regulatory)**
- **Computer-interpretable computational model**
  - Time varying (e.g., performance simulations) or static (e.g., reliability models)
  - Deterministic or stochastic (e.g., Monte Carlo)
  - May interact with hardware, software, human, and physical environment
  - Includes input/output data sets
- **Human-interpretable descriptive models (e.g., architecture/design SysML or electrical schematic)**
  - Symbolic representation with defined syntax and semantics
  - Repository based (i.e., the model is stored in structured computer format)
  - Supporting metadata about the models including assumptions, versions, regions of validity, etc.
- **MBE can also include the use of physical models**

NDIA Final Report of the Model Based Engineering (MBE) Subcommittee, 2011.

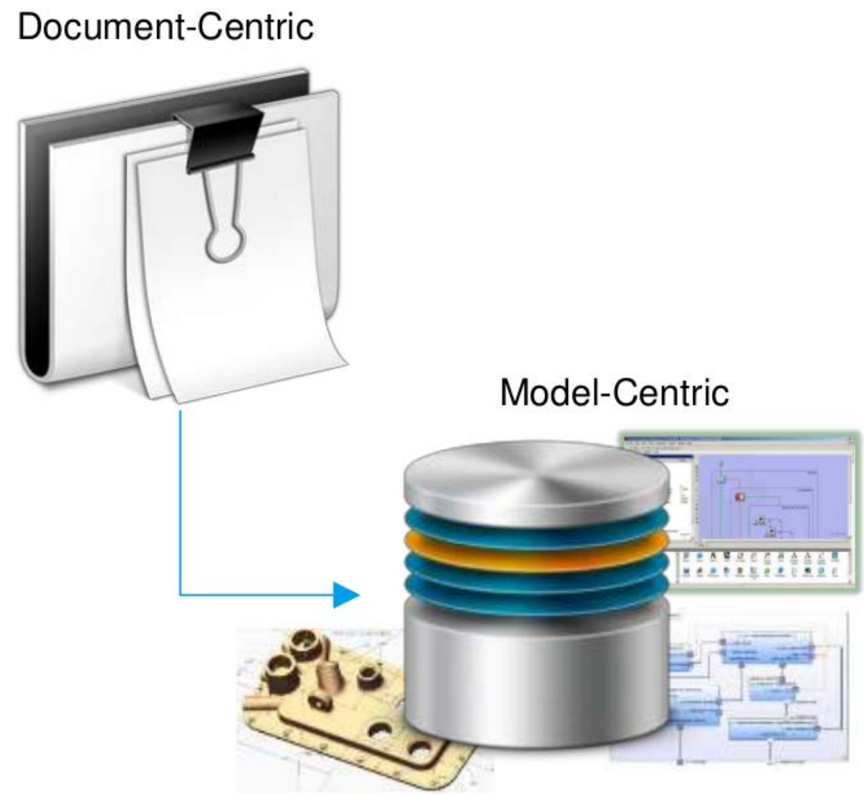
High-Level Benefits of MBE

- **Reduce time to acquisition of first article for systems and solutions**
  - More complete evaluation of the trade space
  - Earlier risk identification and mitigation
  - Concurrent and collaborative engineering
  - Accelerated development
- **Reduce the time to implement planned and foreseen changes in systems**
  - Design reuse
  - Rapidly evaluate changing threats and explore trade space
- **Enhance Reliability**
  - Earlier and continuous requirements and system verification
  - Identify and resolve errors / issues earlier → fewer post-fielding issues
- **Enhance Interoperability**
  - Inclusion of the operating environment and external interfaces in system models
  - Early and continuous interface and interoperability verification

NDIA Final Report of the Model Based Engineering (MBE) Subcommittee, 2011.

Document-Based vs. Model-Based

- Digital models have been common in engineering since the late 1960s but today's focus on Model-based Engineering goes beyond the use of disparate models
- Model-based Engineering moves the record of authority from documents to digital models including SysML managed in a data rich environment
- Shifting to model-based enables engineering teams to more readily understand design change impacts, communicate design intent and analyze a system design before it is built

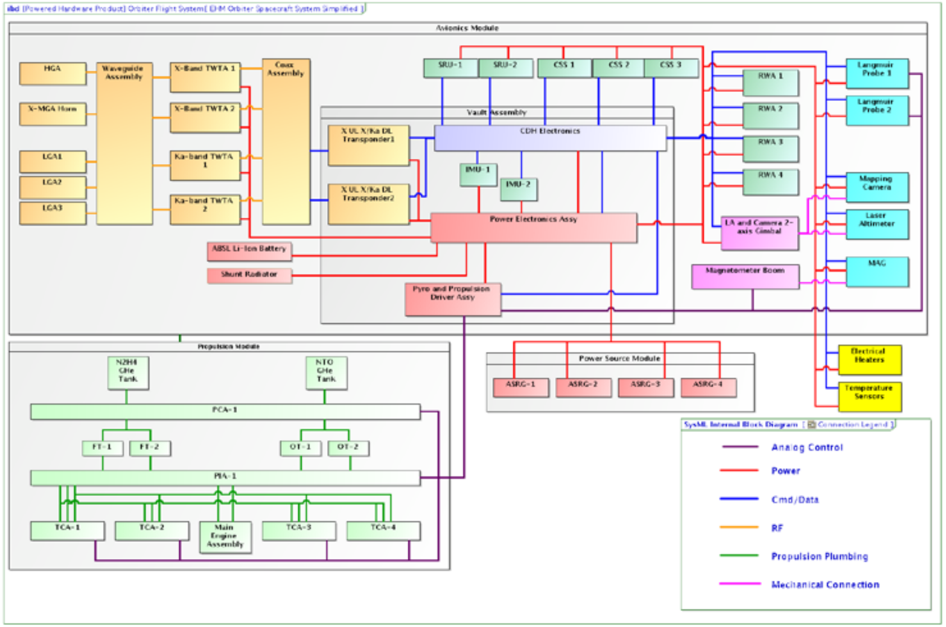


L. Hart, *Introduction To Model-Based System Engineering (MBSE) and SysML*, 2015.

Application of MBSE

Vanderbilt Engineering

- **Models of spacecraft systems can represent sub-system functions, interfacing, and reliability properties**
  - Facilitates quantitative evaluation of sub-system interactions
  - Engineer team works from one virtual model set
  - Models can include fault propagation across sub-systems



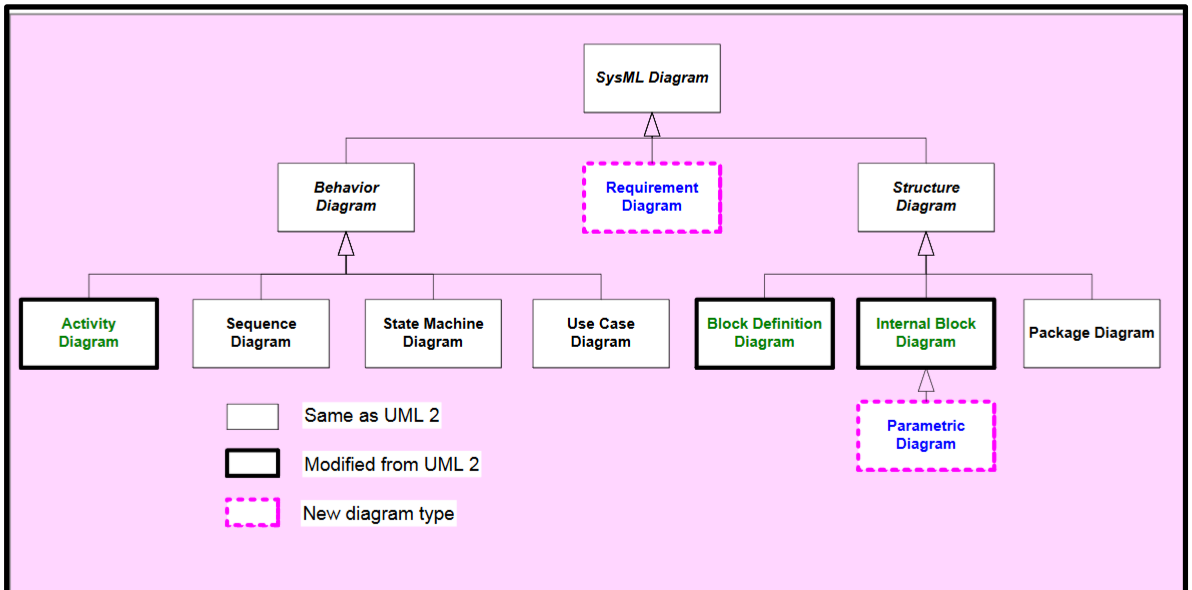
Flight System Block Diagram

T. Bayer, *Europa Mission Concept Studies*, 2012.

System Modeling Language (SysML)

Vanderbilt Engineering

- **Graphical modeling language that supports specification, analysis, design, verification, and validation of systems**
  - Systems include hardware, software, data, personnel, procedures, and facilities



“OMG SysML™ Tutorial,” http://www.omgsysml.org/INCOSE-OMGSysML-Tutorial-Final-090901.pdf

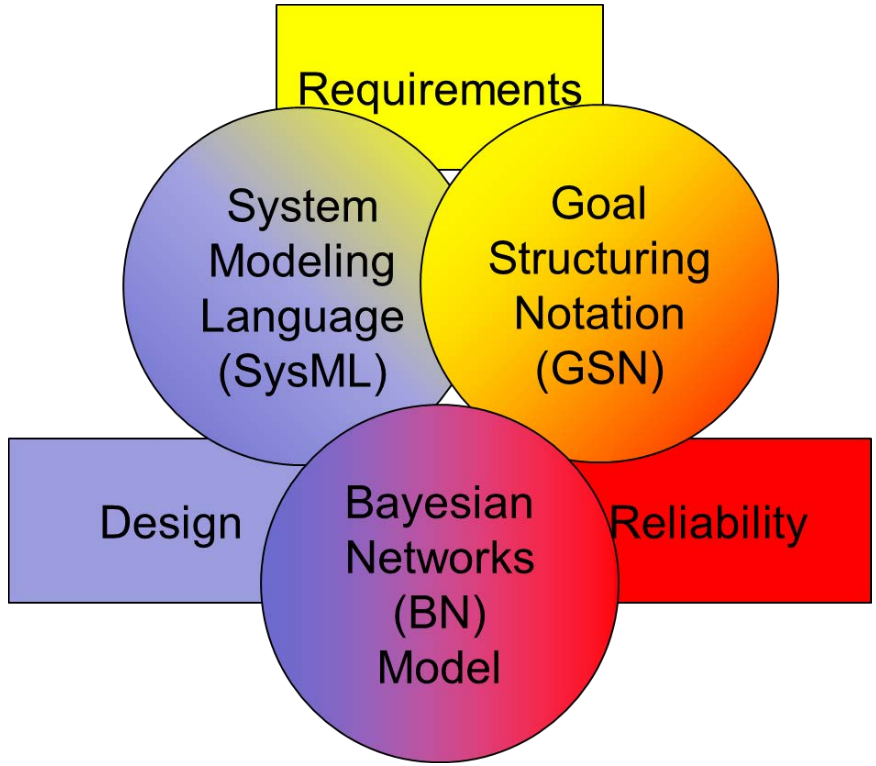
Model-Based Mission Assurance

- **Shift from document-centric to model-centric repository of design information**
- **Shift from prescriptive reliability paradigm to objectives-based paradigm for reliability**
  - NASA-STD-8729.1A Reliability and Maintainability Standard
- **Driver: Increased use of COTS parts on spacecraft**
  - Little information on design of parts available from manufacturers
  - High variability in performance of COTS parts
- **Payoff: Rapid acceptance and deployment of small spacecraft**
  - Short schedule, limited budget and resources
  - Extensive testing and space-qualified parts not a universal requirement

Integrated System Design for Radiation Environments

Vanderbilt Engineering

- **Goal Structuring Notation:**
  - R&M Template
  - Visual representation of argument
- **System Modeling Language (SysML):**
  - Specification of systems through standard notation
- **Bayesian Network (BN)**
  - Nodes describe probabilities of states
  - Calculate conditional probabilities from observations

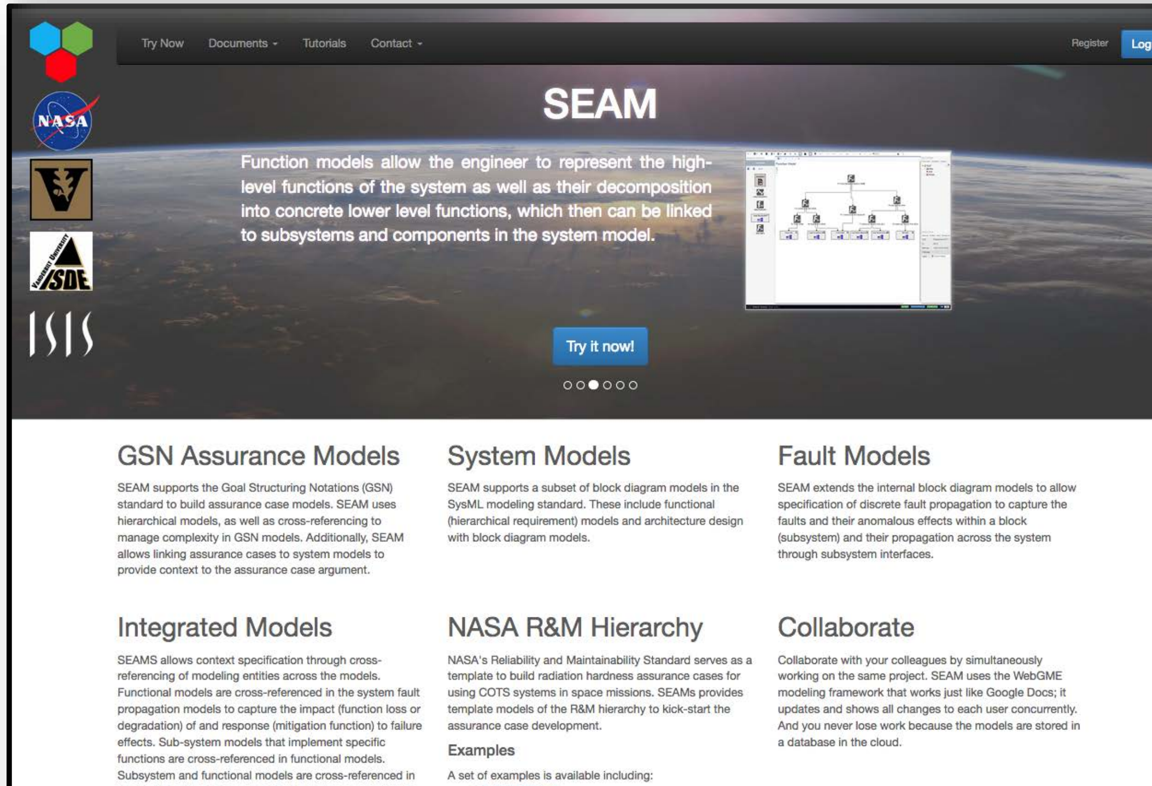


System Engineering and Assurance Modeling (SEAM) Platform

Vanderbilt Engineering

- **Web-browser based**
- **GSN implementation**
- **SysML+fault propagation models**
- **Functional Models**
- **Integration of GSN+SysML**
- **Export to Bayes Net software tools**
- **Examples based on CubeSat expmt.**

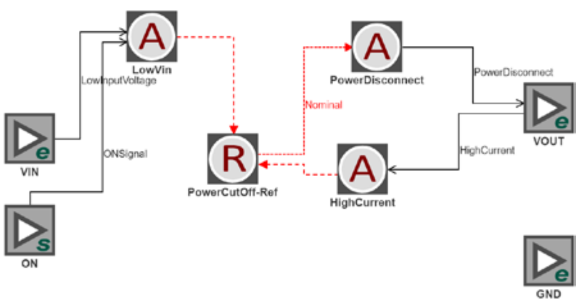
https://modelbasedassurance.org/

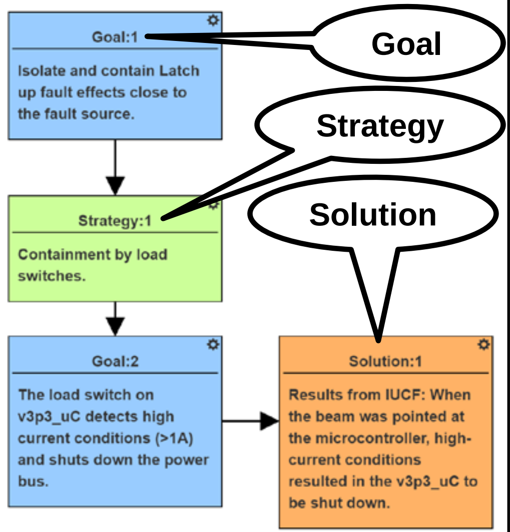


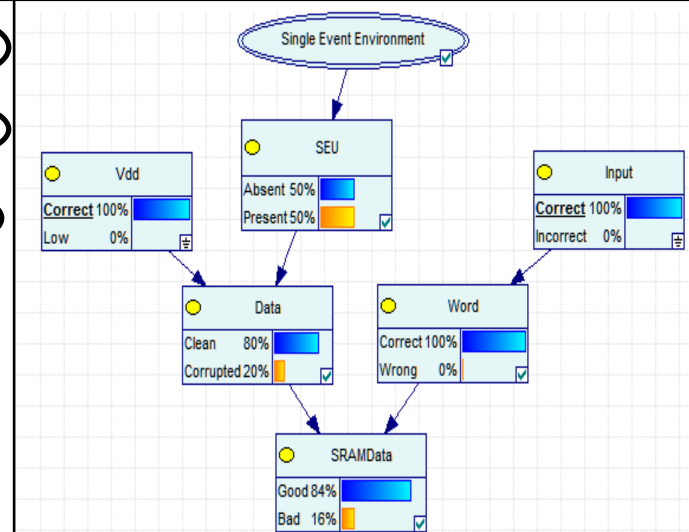
Vanderbilt Engineering

SEAM: Overview of Modeling Languages Used

SysML	GSN	Bayes Net
• 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





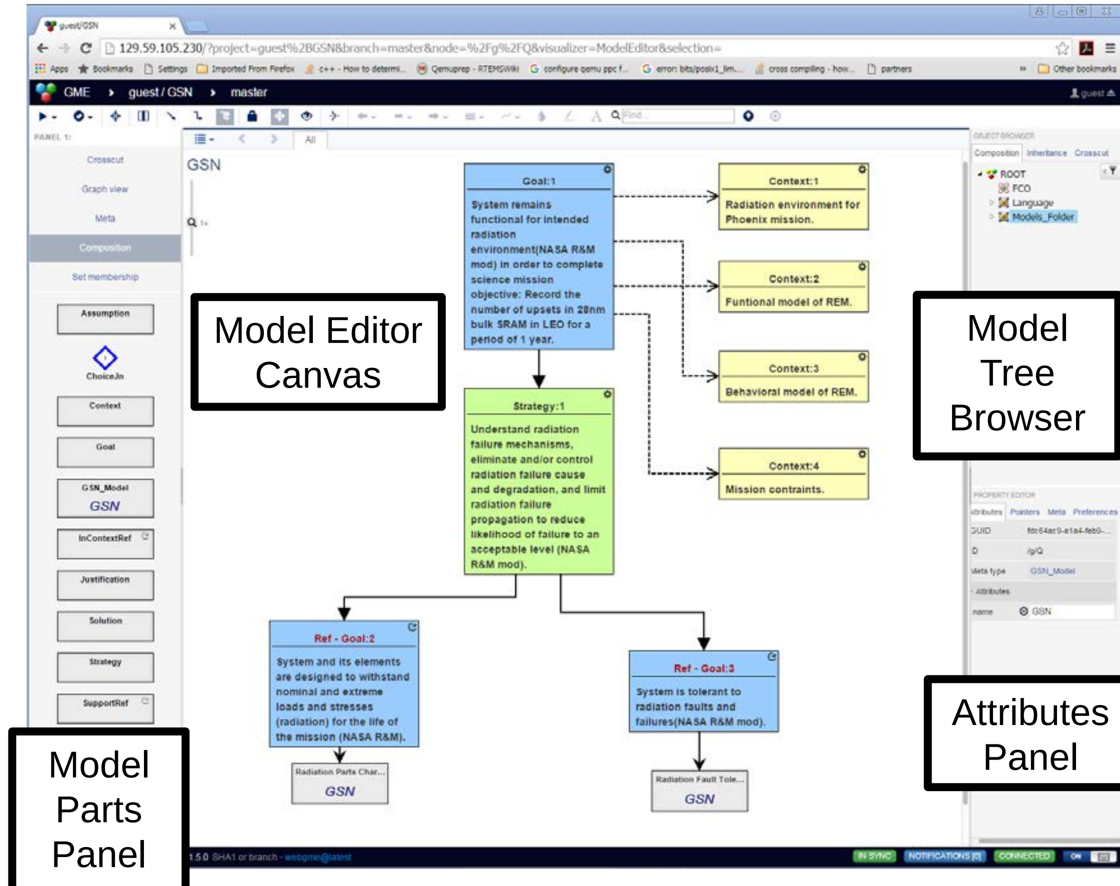


SEAM Components

Vanderbilt Engineering

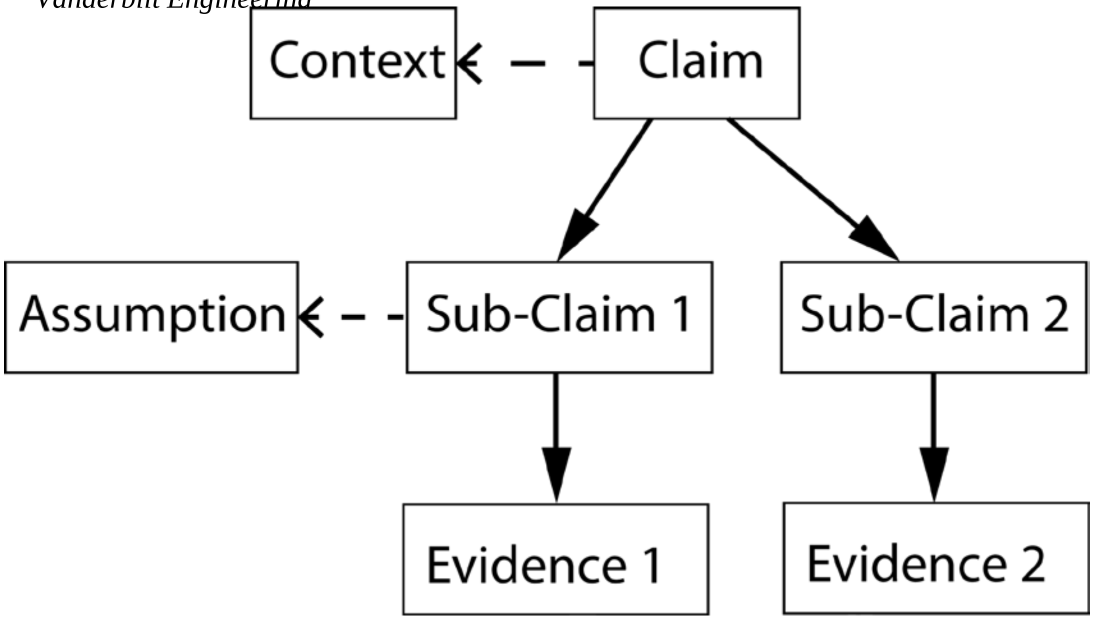
- **A set of linked modeling languages to implement MBMA for radiation effects developed at Vanderbilt**

- **Integrates Radiation Hardness Assurance activities into overall system design process**



Graphical Assurance Cases

Vanderbilt Engineering



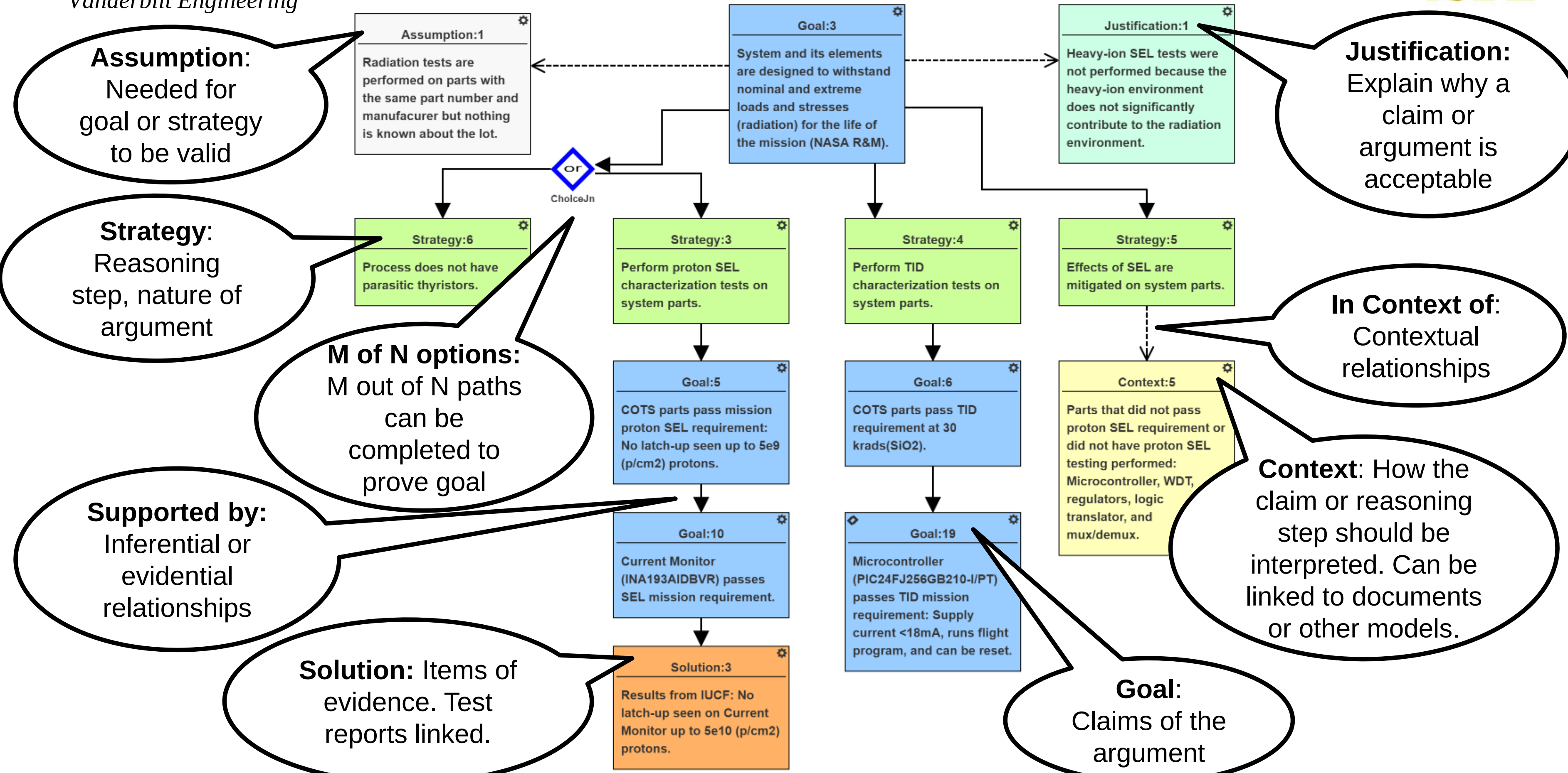
Argument: "A connected series of claims intended to support an overall claim."

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."

GSN Community Standard Version 1 2011

Goal Structuring Notation (GSN): Visual Representation of Argument

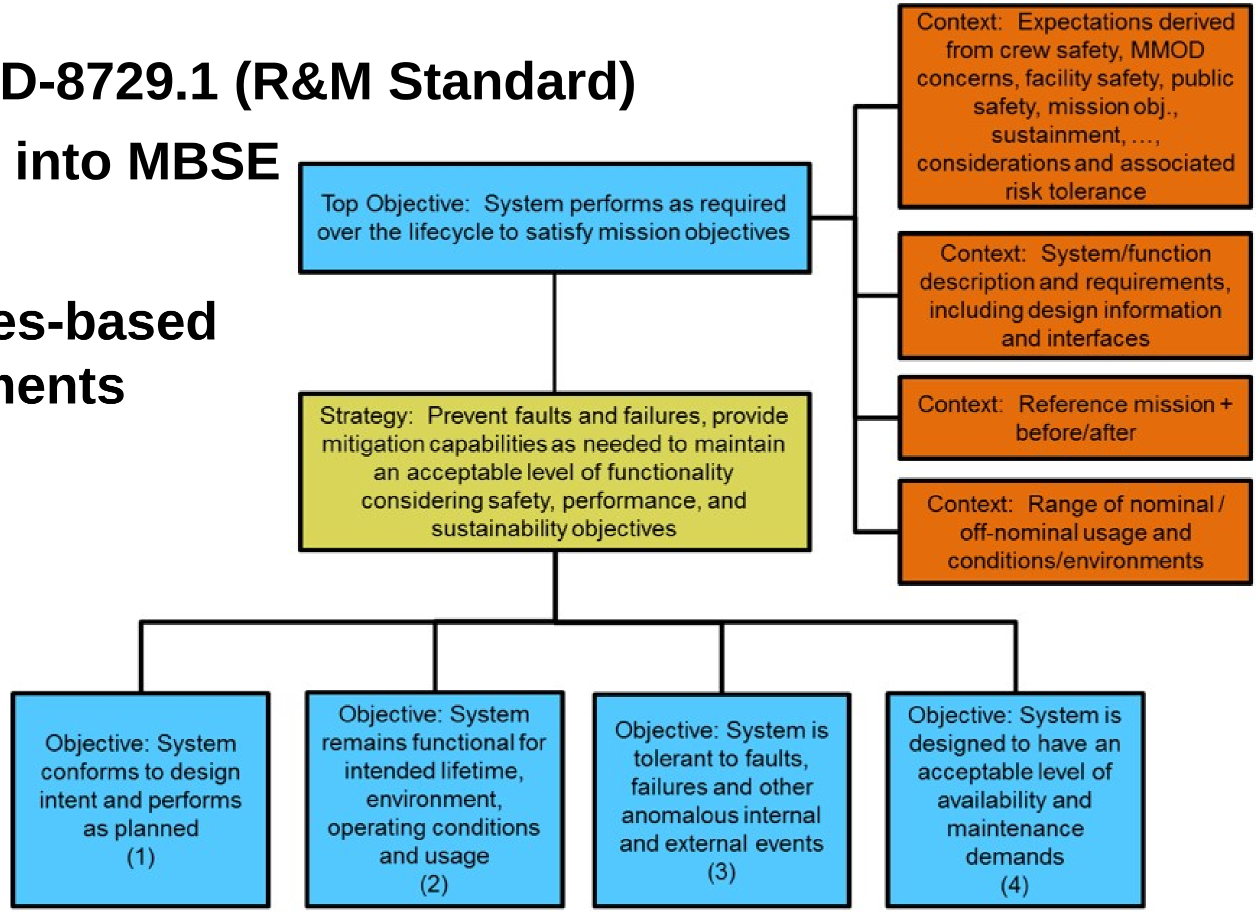
Vanderbilt Engineering



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

Vanderbilt Engineering

- Basis of NASA-STD-8729.1 (R&M Standard)
- Incorporates R&M into MBSE
- Moves to objectives-based reliability requirements



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

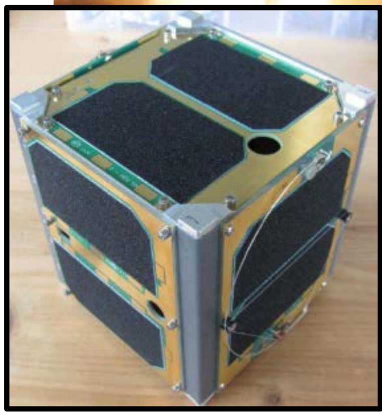
- **System performs as required over the lifecycle to satisfy mission objectives**
  - System conforms to design intent and performs as planned.
  - System remains functional for intended lifetime, environment, operating conditions and usage.
  - System is tolerant to faults, failures and other anomalous internal and external events.
  - System has an acceptable level of maintainability and operational availability.

Evans, "Model Based Mission Assurance (MBMA): NASA's Assurance Future"

Application Example

- **Objective: Design a reliable, low-cost, on-orbit testbed to improve modeling of the impact of space radiation effects on target satellite components and systems**
- **Launch and monitor CubeSats hosting testbed payloads**
    - AO-85 and AO-91
- **Apply model-based, graphical arguments to radiation hardness assurance activities for documentation and design reviews**

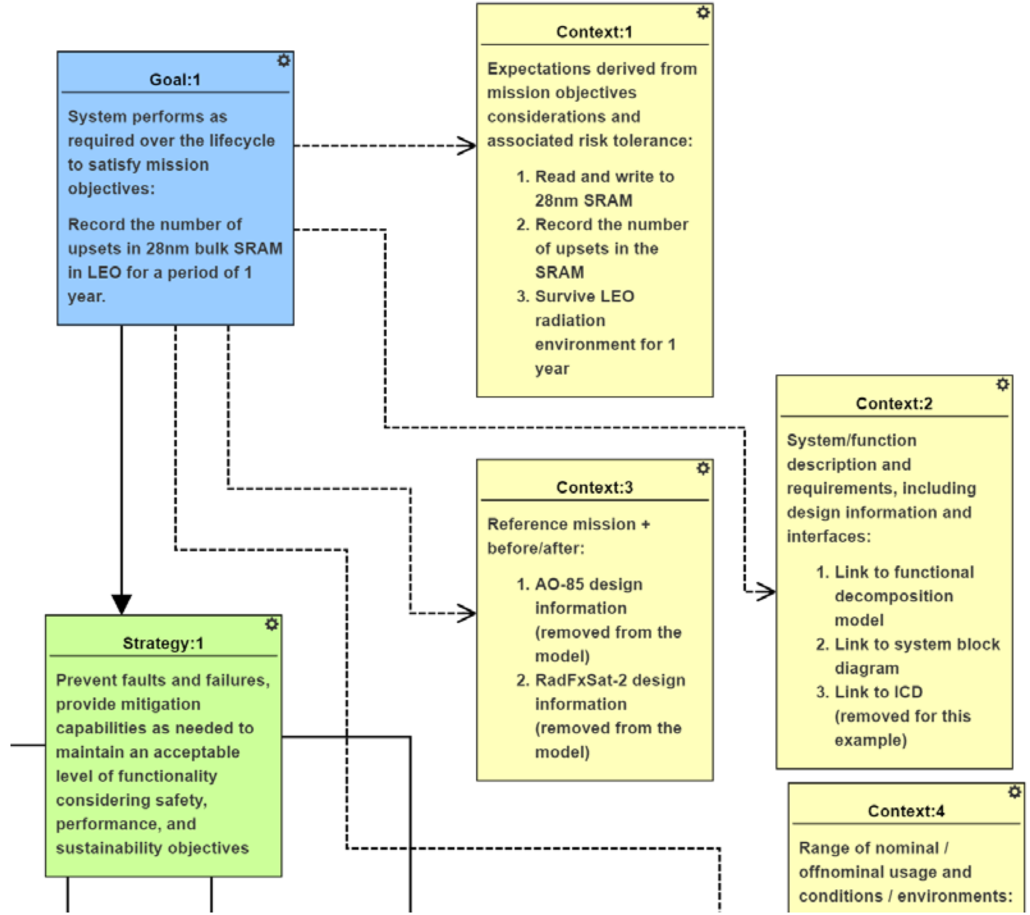
Courtesy NOAA



Courtesy of AMSAT

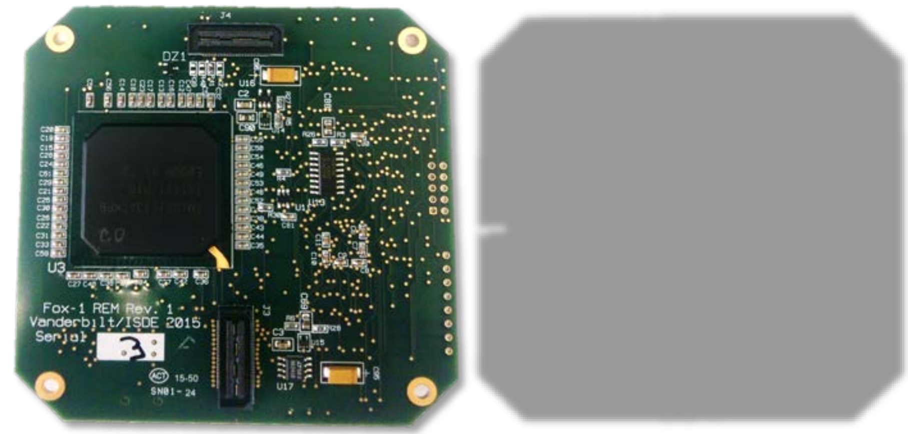
Top-Level GSN Argument

- **Based on R&M Standard**
- **Mission specific information added related to radiation effects and mitigation**



Mission Assurance Activities

1. Parts management
2. Screening (TID)
3. Mitigating single event effects
4. Ensuring temperature operability
5. Designing robust software
6. Performing post-assembly inspections
7. Performing burn-in



Radiation Effects Modeling (REM) – 28 nm bulk SRAM experiment

Parts Management

Vanderbilt Engineering

- **Commercial-grade electronics (industrial-grade when available)**
- **Majority of parts supplied by Digi-Key**
- **Bulk purchases considered a “lot”**
  - Traceability only extends to handling and storage after purchase
  - No guarantee parts were manufactured on the same line or plant
- **Acceptance tests should be performed on the same “lot”**
  - Additionally, limited resources means this may be only a few samples

Assumption:1

Radiation tests are applicable to parts with the same part number and manufacturer (not lot testing).

Goal:5

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

Screening COTS Parts for TID

Vanderbilt Engineering

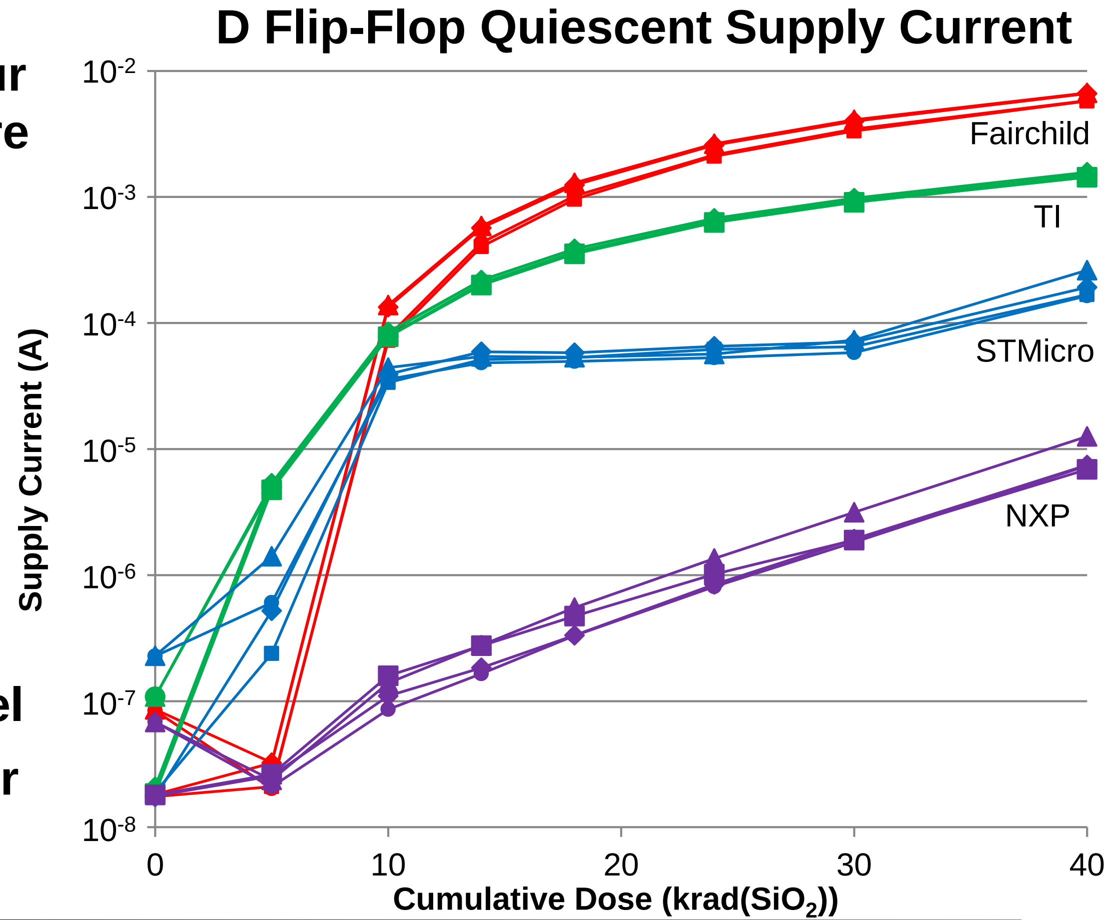
- **D Flip-flop designs from four different manufacturers were considered**

Goal:1

System performs as required over the lifecycle to satisfy mission objectives:

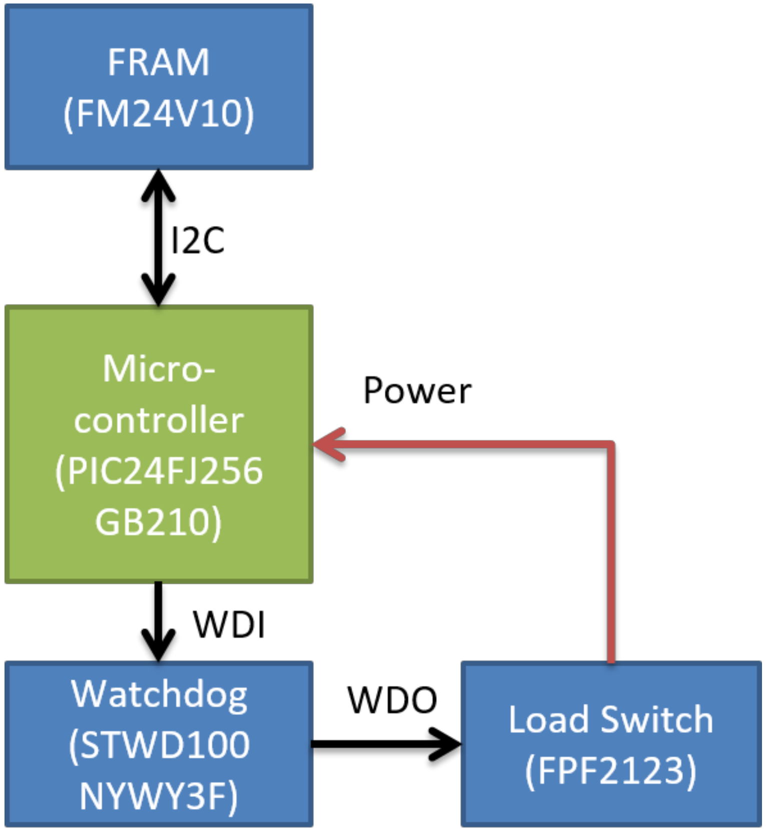
Record the number of upsets in 28nm bulk SRAM in LEO for a period of 1 year.

- **Context: Environment model**
- **Evidence: Performance after 40 krad(SiO_2) with Cs-137 source**



Mitigating Single Event Effects

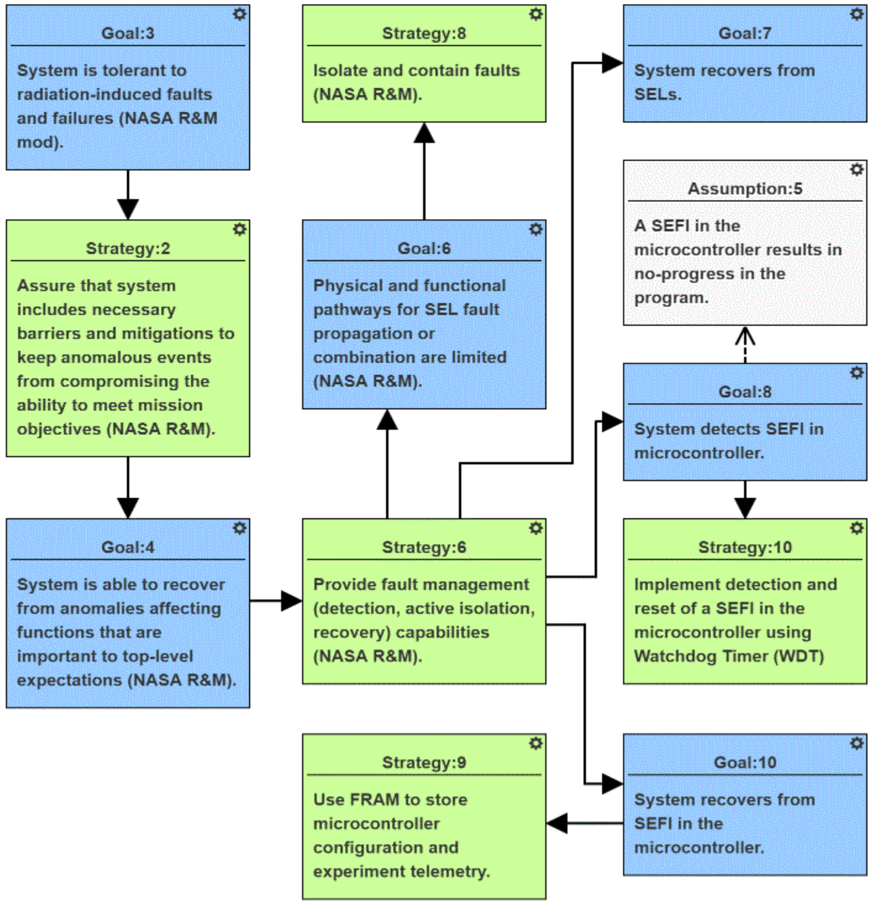
Vanderbilt Engineering



- **Example: Microcontroller SEEs**
  - Non-volatile memory for storing configuration to recover from SEFIs
  - Load Switches to detect and recover from SELs
  - Watchdog timer for SEFI detection
- **System-level 200 MeV protons testing for validation of SEL and SEFI mitigation schemes**

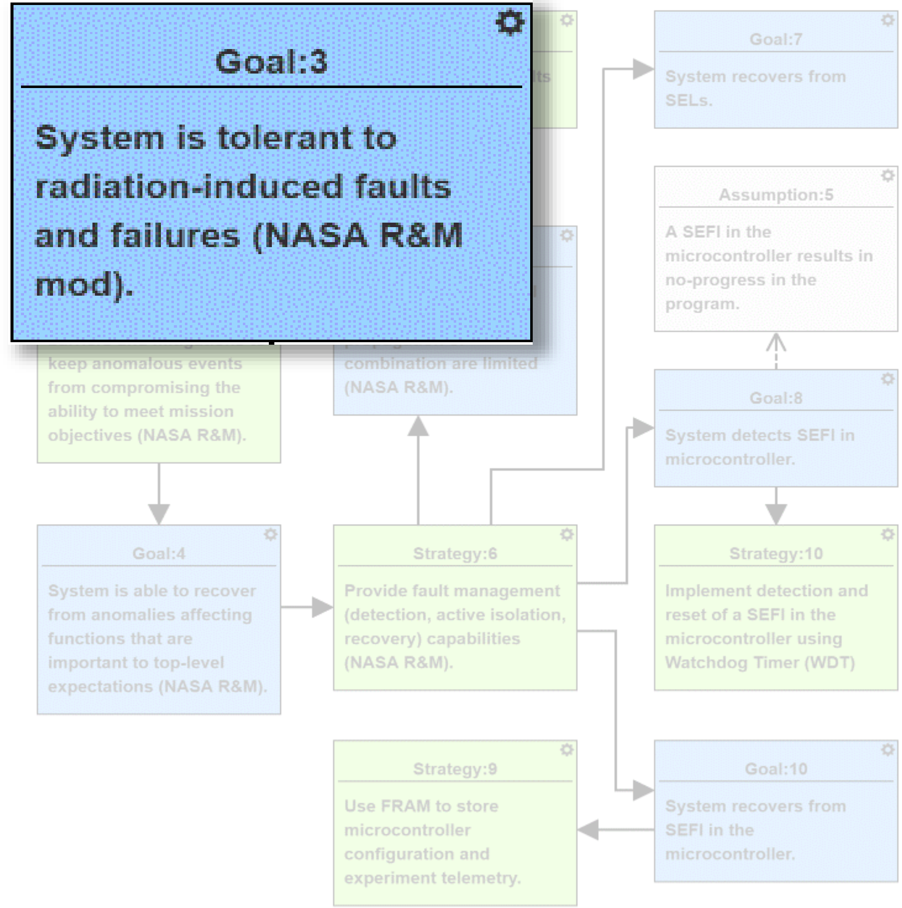
Mitigating Single Event Effects

- **Model-based graphical argument for RHA**
  - Documents RHA activities, results, and decisions
  - Enables improved discussion of RHA plan



Mitigating Single Event Effects

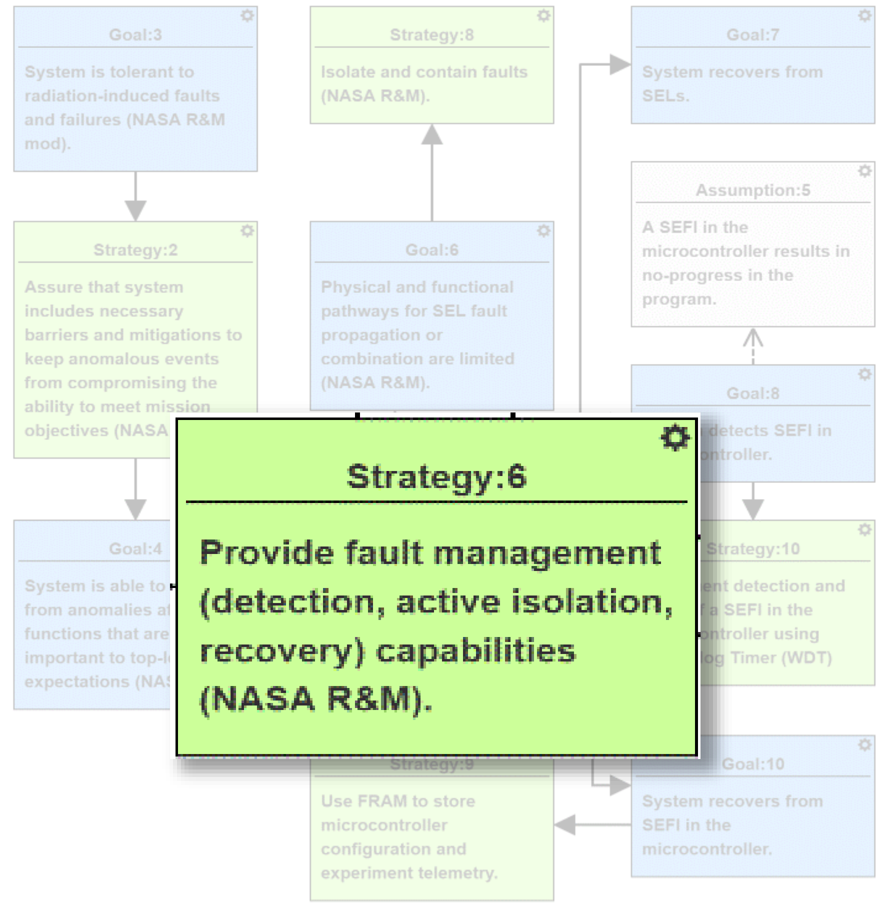
- **Model-based graphical argument for RHA**
  - Documents RHA activities, results, and decisions
  - Enables improved discussion of RHA plan



Mitigating Single Event Effects

Vanderbilt Engineering

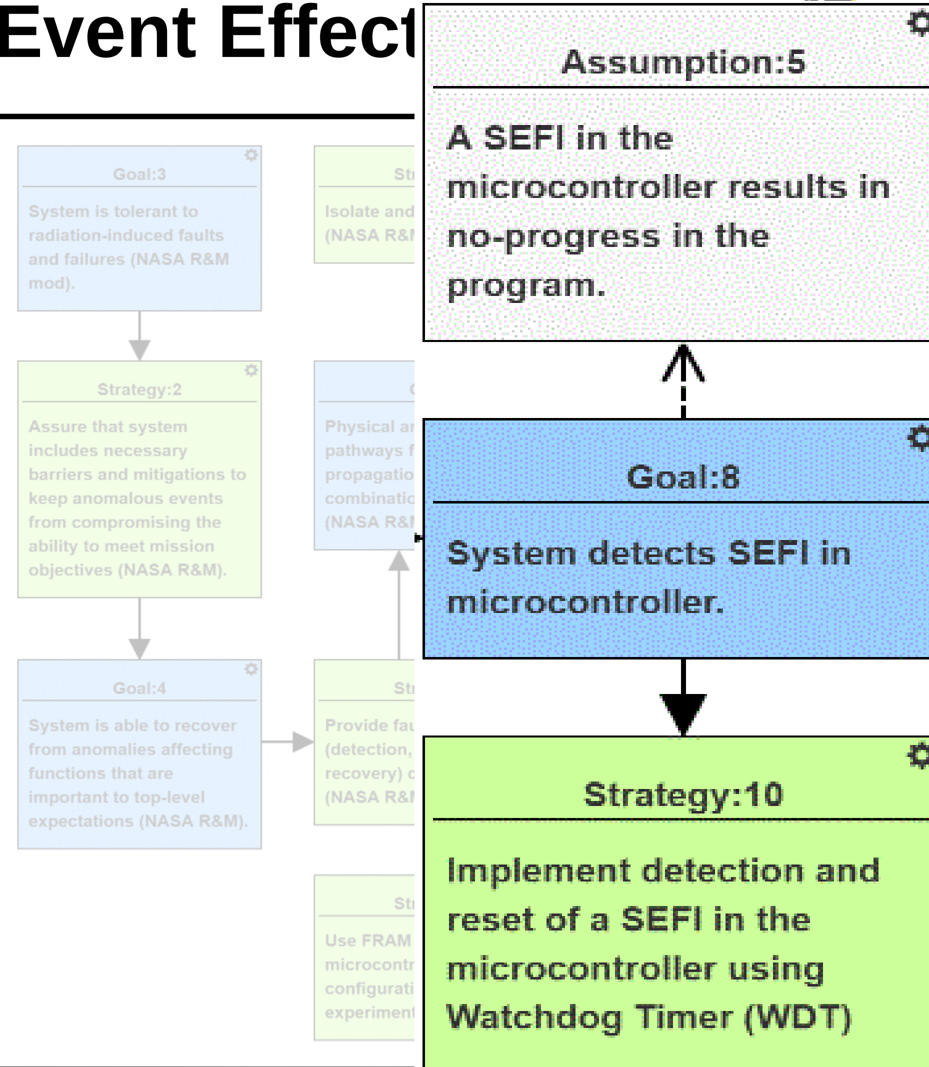
- **Model-based graphical argument for RHA**
  - Documents RHA activities, results, and decisions
  - Enables improved discussion of RHA plan



Mitigating Single Event Effect

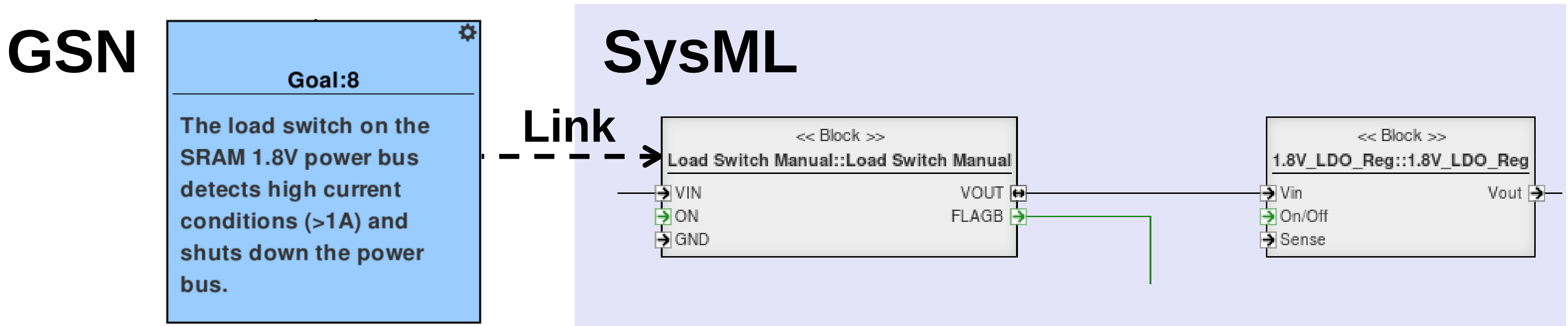
Vanderbilt Engineering

- **Model-based graphical argument for RHA**
  - Documents RHA activities, results, and decisions
  - Enables improved discussion of RHA plan



Ensuring Temperature Operability

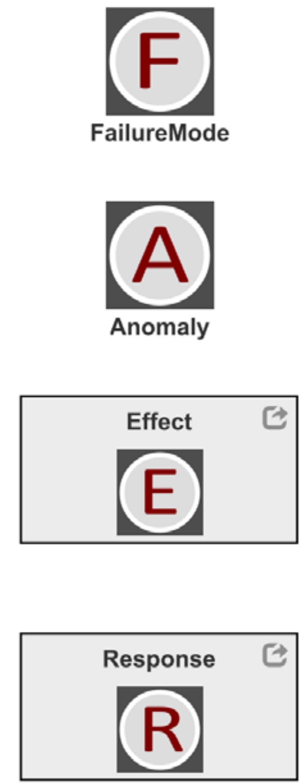
- **Electronics should be able to operate in both reduced and elevated temperatures (minimal thermal control)**
- **Environmental test demonstrated**
  - Increased static power at elevated temperatures
  - Unexpected failures of SRAM at reduced temperatures
- **Increased in-rush current exceeded overcurrent threshold in place to mitigate SEL**



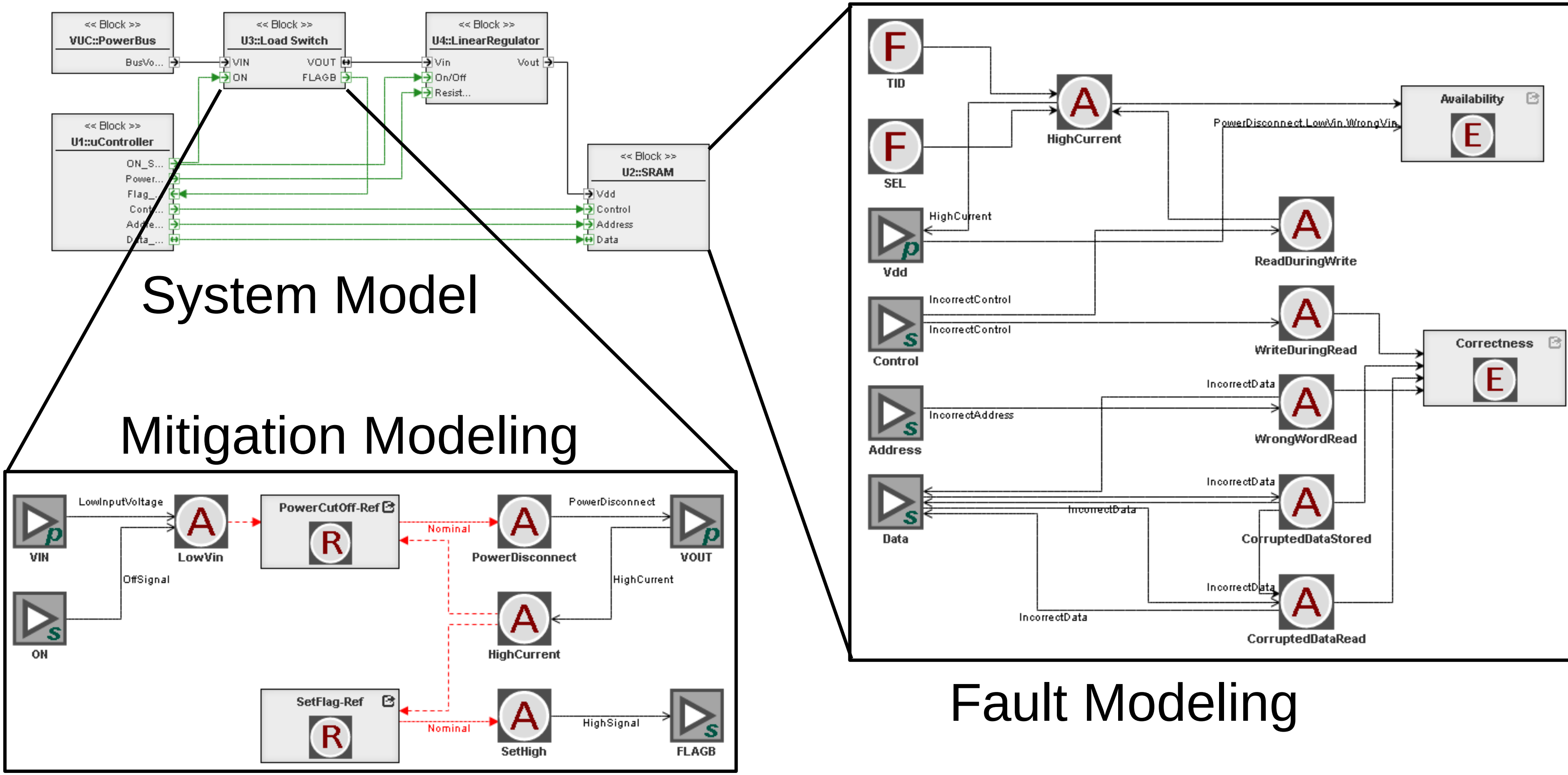
Radiation Fault Propagation Modeling

- **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)**
- **Effects (E): Impact on functionality**

- **Faults/Anomalies flow through ports to affect other components**



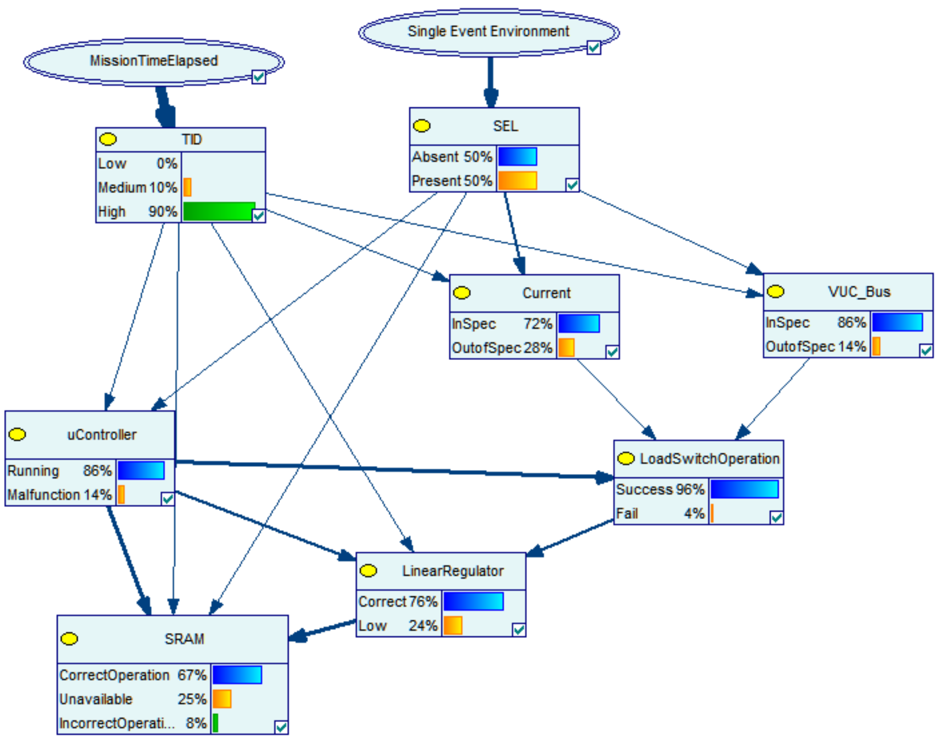
SysML Model with Fault Propagation



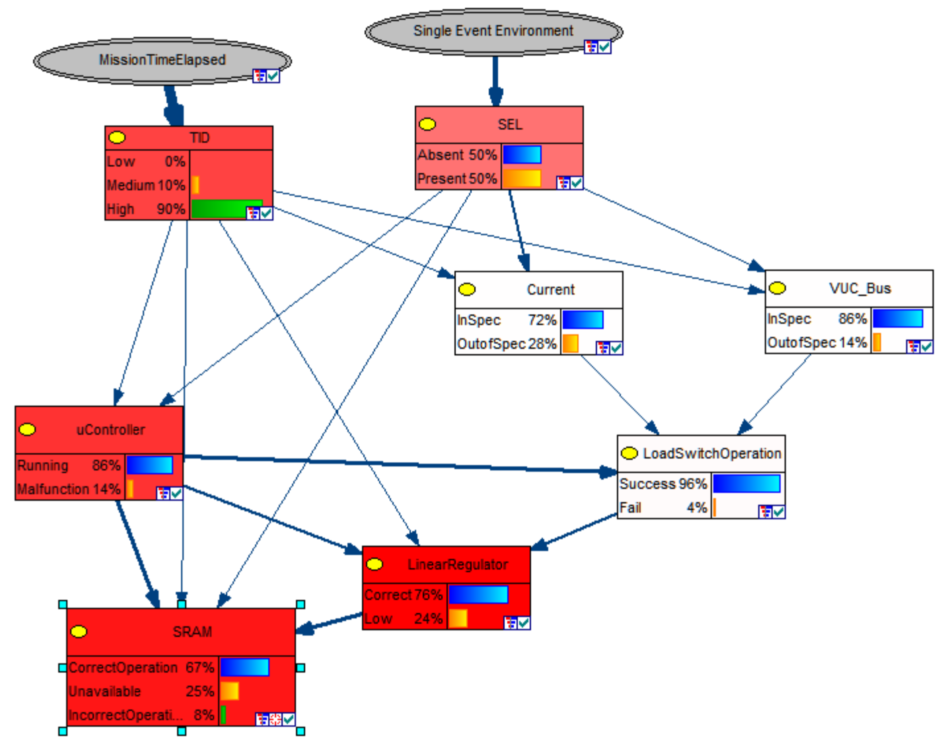
Bayesian Net for Evaluating Probability of Functional Effects

Vanderbilt Engineering

Net for radiation environment



Sensitivity Analysis for SRAM



Vanderbilt Engineering

Summary

- **New model-based paradigm for mission assurance**
  - Driven by increased use of COTS and risk management instead of risk avoidance
- **Investigating how to interface SEAM tool to existing RHA tools for mission planning, environment modeling, radiation parts databases, and error-rate calculations**
- **Website development and launch: https://modelbasedassurance.org**