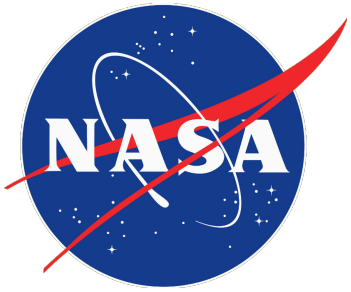
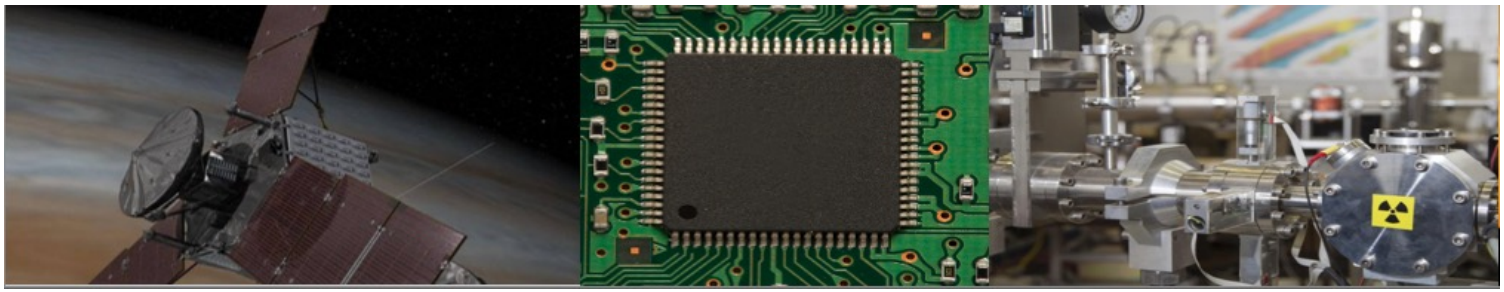


Systematic Propagation of Component-Level Failure Effects for Spacecraft Reliability Evaluation

M. Reaz, R. Alles, A. Witulski, G. Karsai, N. Mahadevan,
B. Sierawski, R. Reed & R. Schrimpf
Vanderbilt University

This work supported by NASA grant and contract 80NSSC20K0424

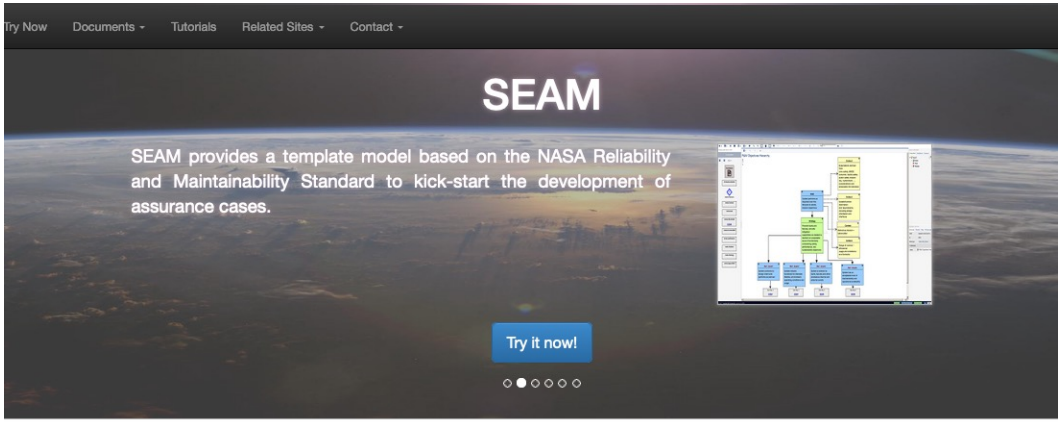


To be presented by Arthur Witulski at TRISMAC 2021 Trilateral Safety & Mission Assurance Conference (TRISMAC), virtual, May 17-20, 2021.

SEAM: Systems Engineering Assurance Modeling

Vanderbilt Engineering

- Dedicated browser-based platform
- Based on WebGME
- Access as guest or create account
- Maintained by VU/NASA GSFC
- Contains examples and tutorial information
- Diagrams in following presentations
- Customer server installations available



GSN Assurance Models

SEAM supports the Goal Structuring Notations (GSN) standard to build assurance case models. SEAM uses hierarchical models, as well as cross-referencing to manage complexity in GSN models. Additionally, SEAM allows linking assurance cases to system models to provide context to the assurance case argument.

System Models

SEAM supports a subset of block diagram models in the SysML modeling standard. These include functional (hierarchical requirement) models and architecture design with block diagram models.

Fault Models

SEAM extends the internal block diagram models to allow specification of discrete fault propagation to capture the faults and their anomalous effects within a block (subsystem) and their propagation across the system through subsystem interfaces.

Integrated Models

SEAMS allows context specification through cross-referencing of modeling entities across the models. Functional models are cross-referenced in the system fault propagation models to capture the impact (function loss or degradation) of and response (mitigation function) to failure effects. Sub-system models that implement specific functions are cross-referenced in functional models.

NASA R&M Hierarchy

NASA's Reliability and Maintainability Standard serves as a template to build radiation hardness assurance cases for using COTS systems in space missions. SEAMs provides template models of the R&M hierarchy to kick-start the assurance case development.

Examples

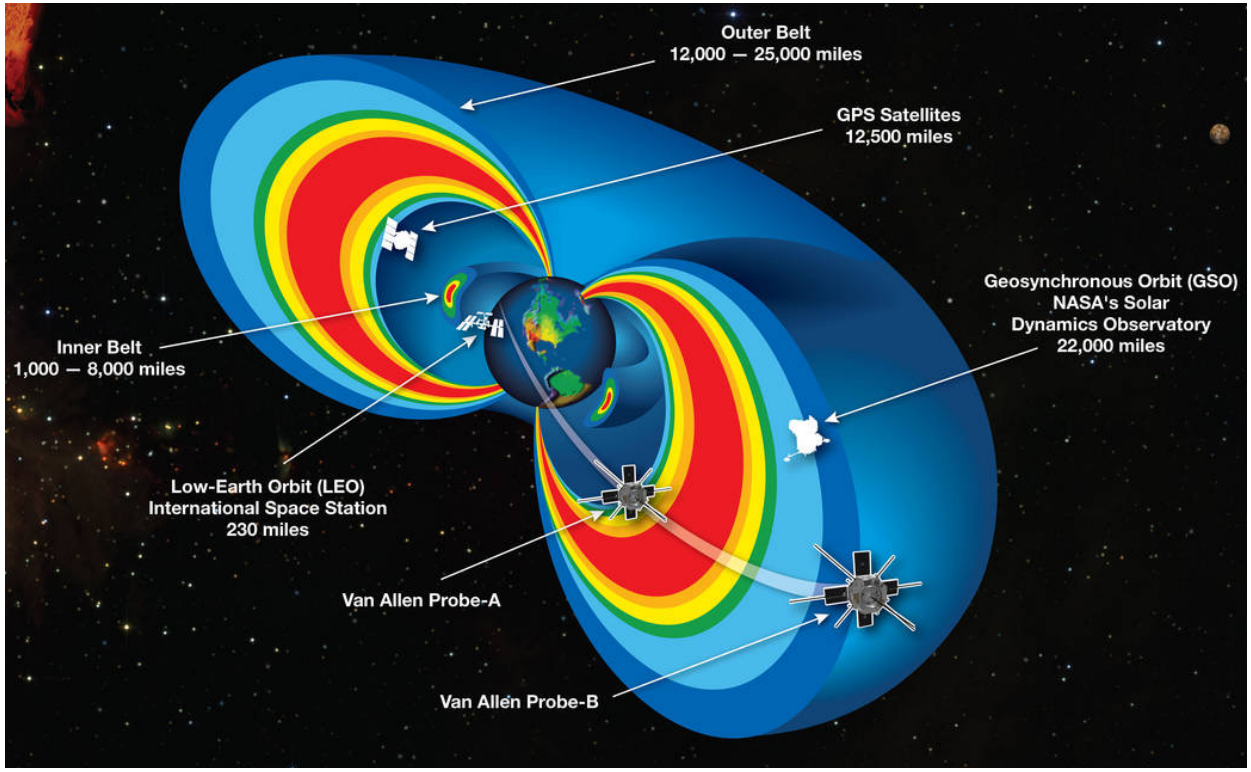
Collaborate

Collaborate with your colleagues by simultaneously working on the same project. SEAM uses the WebGME modeling framework that works just like Google Docs; it updates and shows all changes to each user concurrently. And you never lose work because the models are stored in a database in the cloud.

https://modelbasedassurance.org

Radiation in Space

Vanderbilt Engineering



https://www.nasa.gov/sites/default/files/styles/full_width_feature/public/images/730056main_20130228-radiationbelts-orig_full.jpg

Inner Belt:

- Low energy electrons
- Protons

Outer Belt

- High energy Electrons

Outside the Belts

- Solar particles
- Galactic cosmic rays (GCR)
- Planetary/lunar environments

Modelling Approach - SEAM

Vanderbilt Engineering

- Identify failure modes in components and subsystems
- Define fault origin, anomaly, and effects in each block
- Connect blocks accordingly to architectural hierarchy
- Assign fault propagation paths through model ports
- Reference fault effects to blocks/subsystems
- Allocate functions to specific component instances
- Derive fault tree and Bayesian relashipship
- Classify mission critical failures and associated components

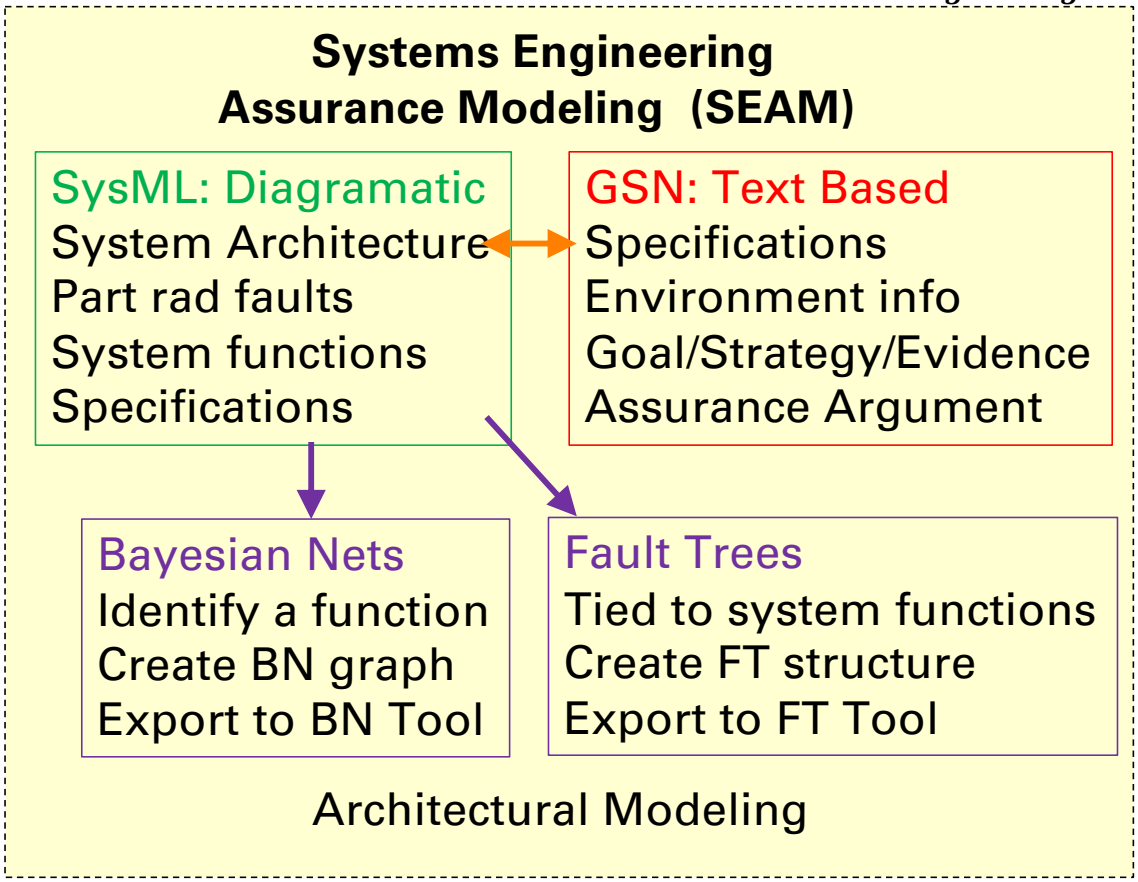
Overview: SEAM Modeling

Vanderbilt Engineering

Meta-model: extended definitions beyond SysML

Architectural Models:

- Meta-Model relates functions to components
- Useful in early stages of a design
- Limited component knowledge
- Connects physical models and reliability models



"Meta-Model:" Augmenting the SysML Diagram Set

Vanderbilt Engineering

Architectural Model : Define the rules of engagement for fault propagation through physical components and ports in a complex system

Goal : Calculate the sensitivity of system functions to faults in a heterogeneous architecture

Challenge : Identifying the minimum cut set of failure at the component level

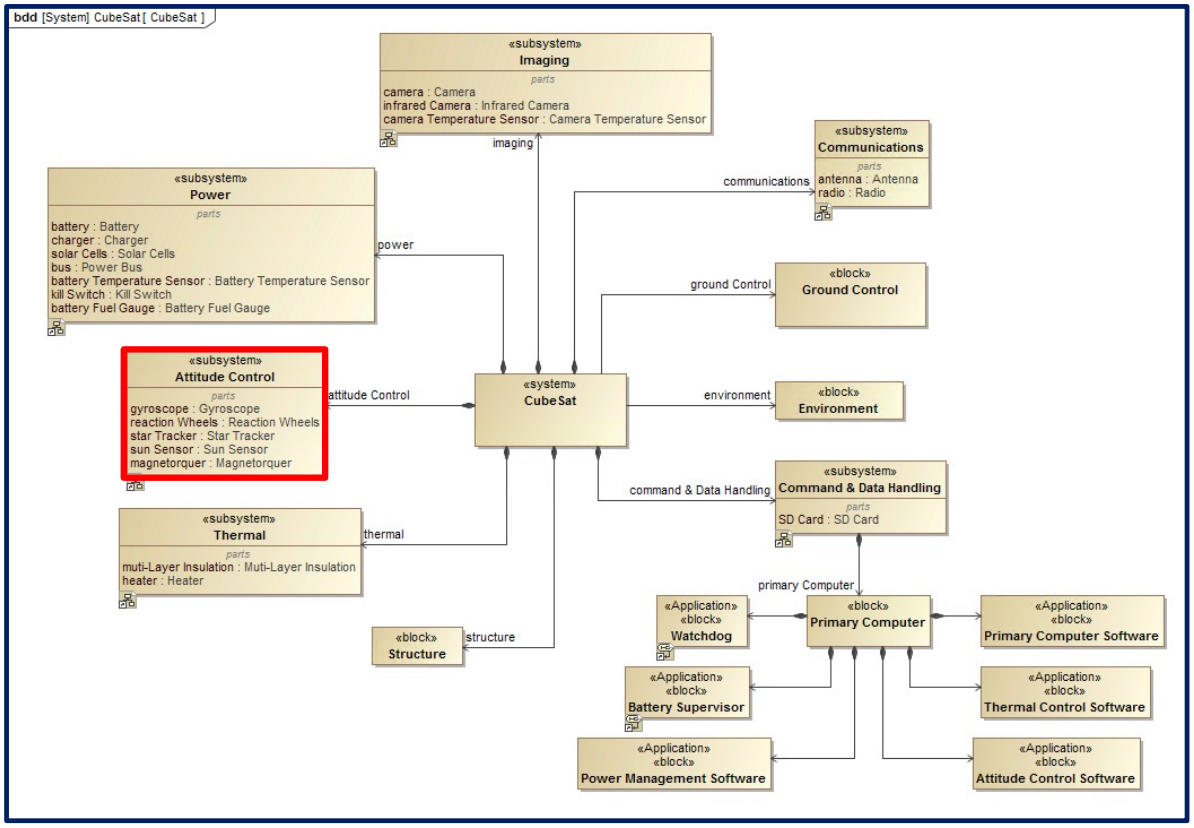
Proposed Solution : Validation of models by quantifiable methods such as FT or BN

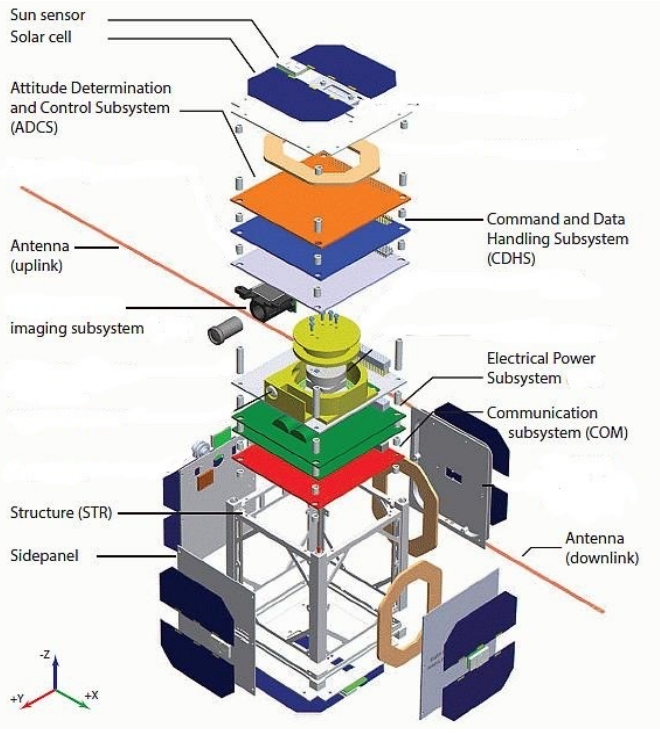
- Functional decomposition diagrams assign "responsibility" to sub-functions and component instances
- Component instances are linked to fault models
- Framework for Probabilistic Analysis: Fault Tree / Bayesian Net

- Fault origination and effect propagation diagrams model the resulting anomalies, and effects, and how they propagate to other components.
- Multiple fault causes and multiple anomalies can be modeled for each component
- Fault effects can be propagated upstream and downstream in block diagram

Trilateral Assurance CubeSat (TACS)

Vanderbilt Engineering

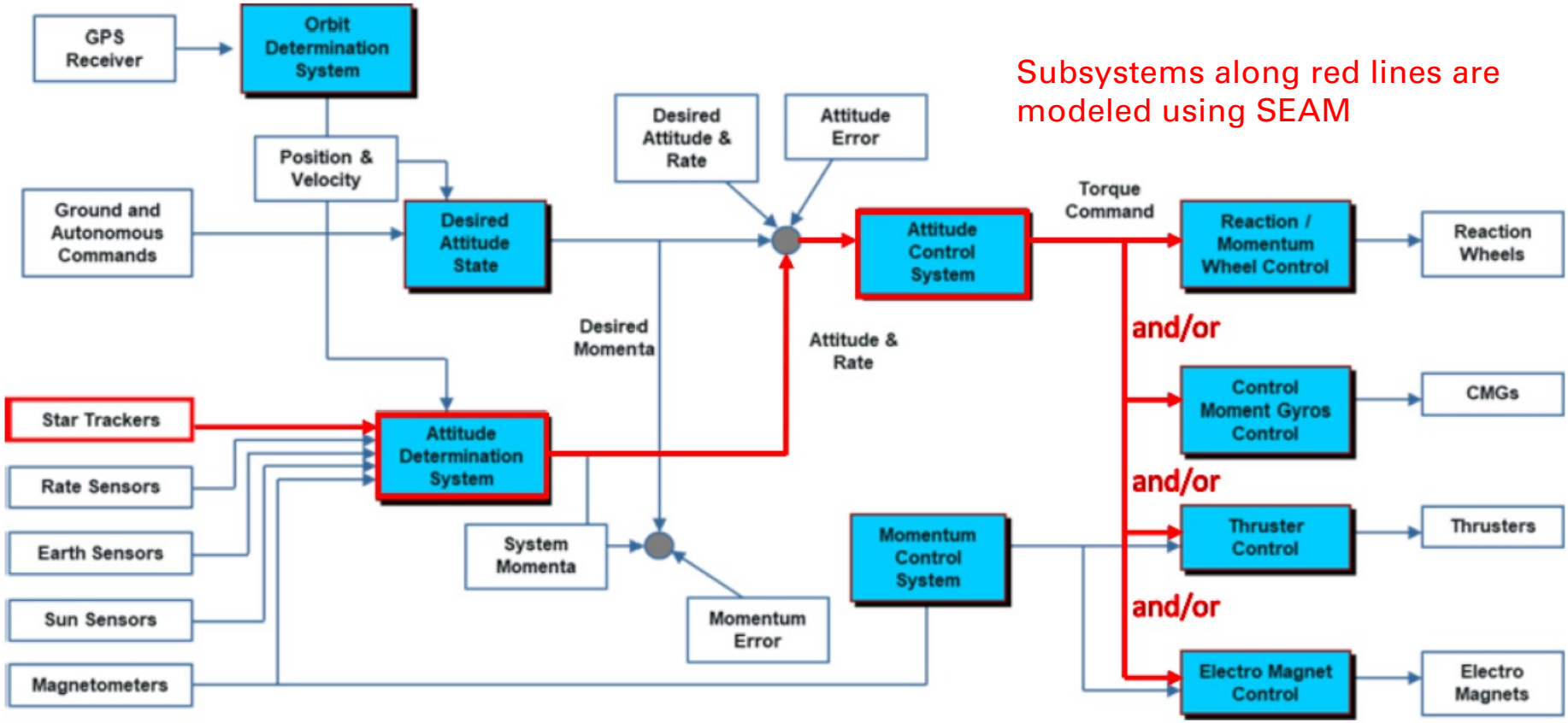




Adapted and Modified from ESTCube-1

Typical Satellite Control System

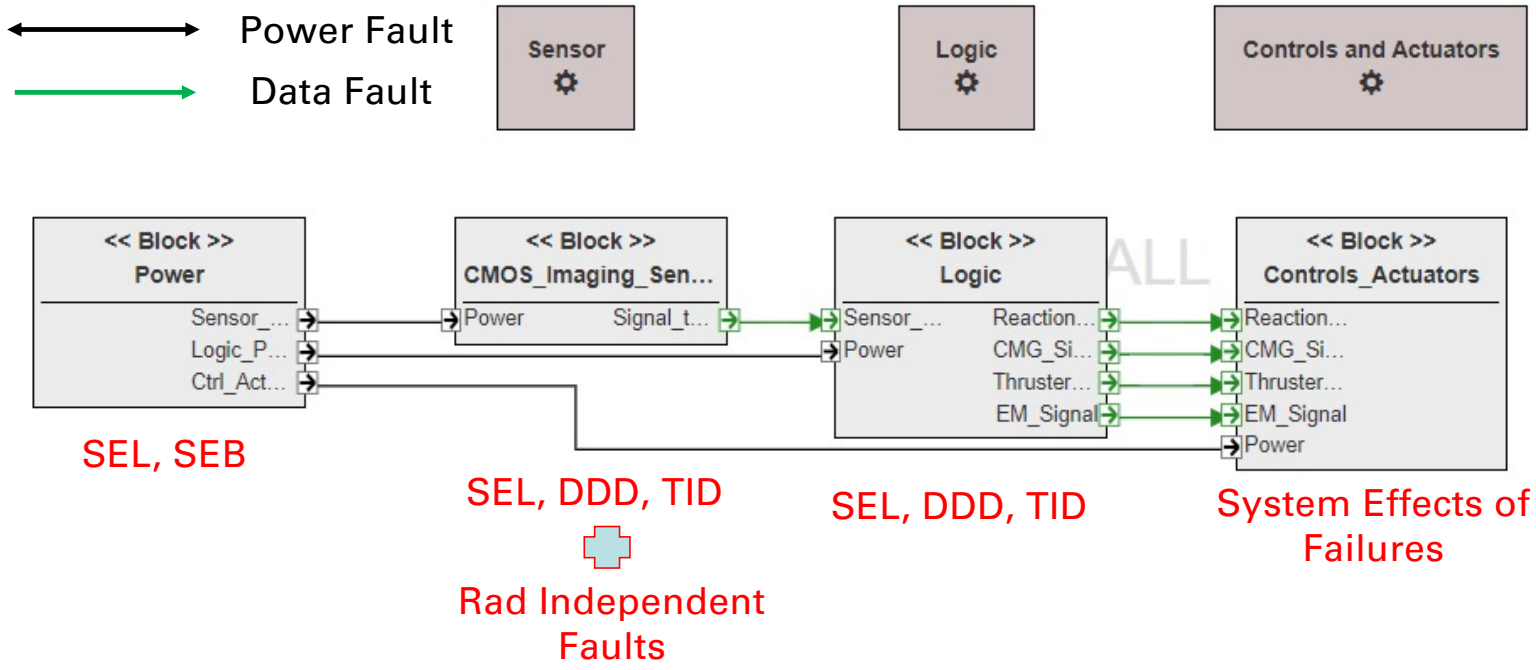
Vanderbilt Engineering



Subsystems along red lines are modeled using SEAM

Architectural Model and Fault Dependencies of Star Tracker

Vanderbilt Engineering



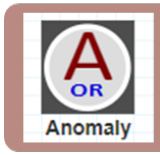
SEL: Single Event Latchup
SEB: Single Event Burnout
DDD: Displacement Damage
TID: Total Ionizing Dose

Definitions : Logical Modeling of Failure Propagation

Vanderbilt Engineering

Fault Propagation Models show how fault originate in components and their effects propagate through the structure of the system.

The **radiation-effects** such as '**TID**' and '**SEL**' are captured as **fault: 'F'** nodes

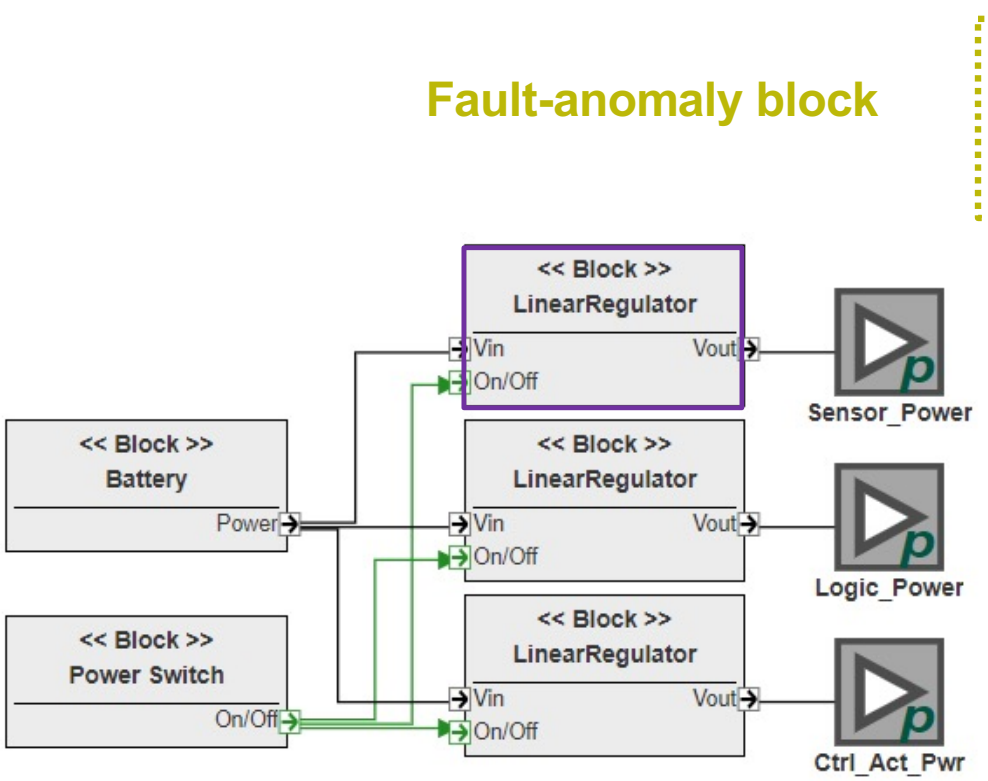


Fault ('**F**' nodes) leads to **anomalies** ('**A**' nodes) such as 'Bad_Data' or 'Low_Vout'

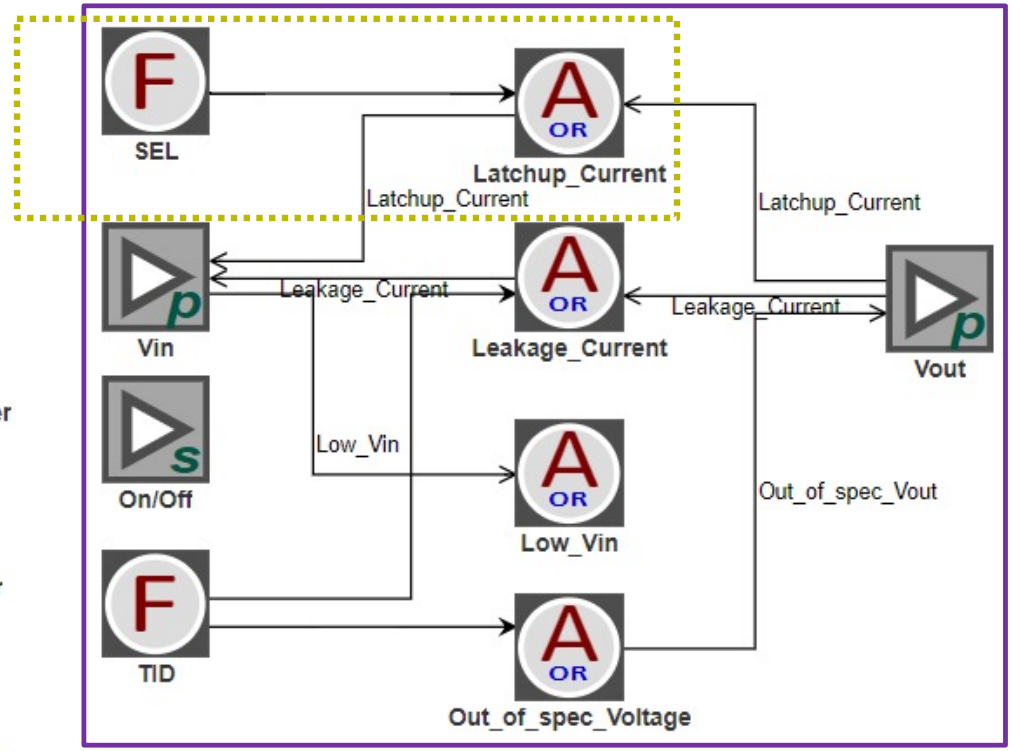
Anomalies lead to the functional **response effects** representing 'Degraded Operations' or 'Mitigation Mechanisms'

Star Tracker Module: Fault Propagation models

Vanderbilt Engineering



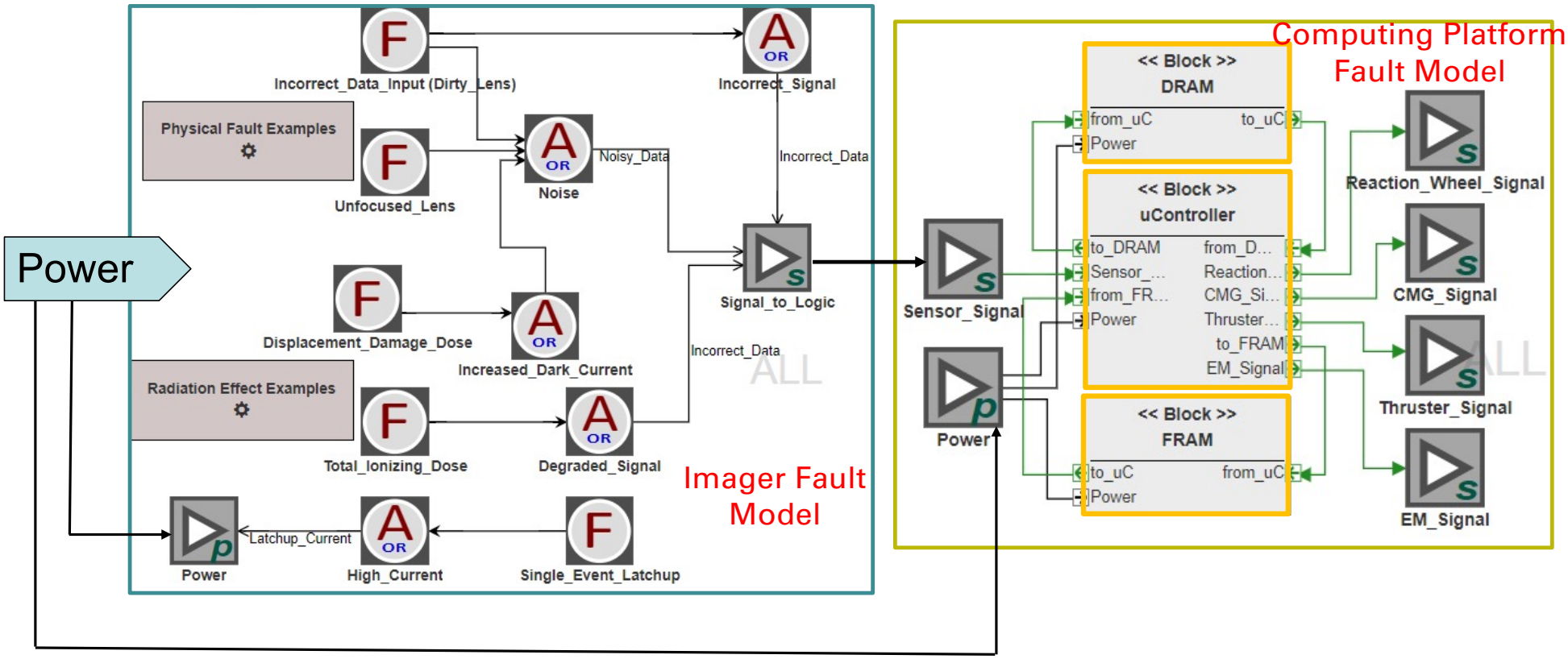
Power System



Linear Regulator

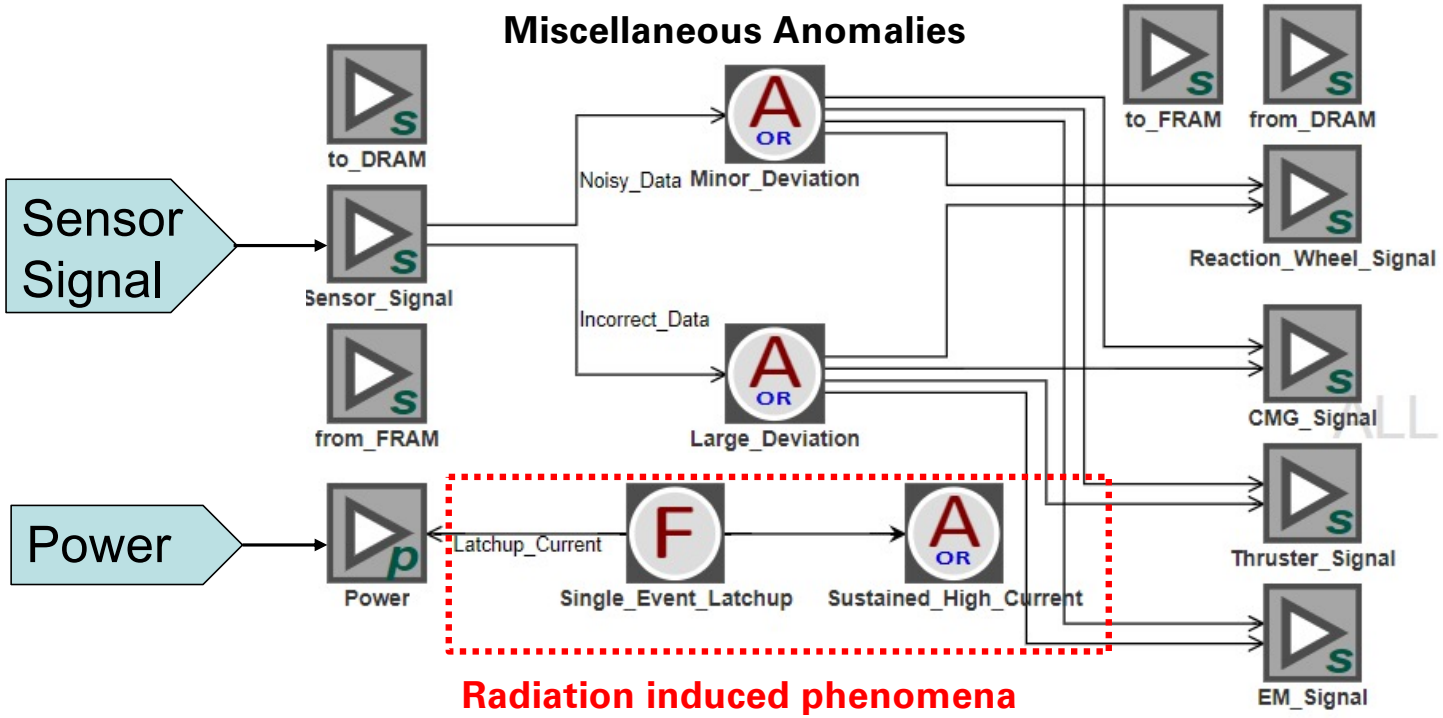
Fault Propagation Diagram- CMOS Sensor & Logic Block

Vanderbilt Engineering



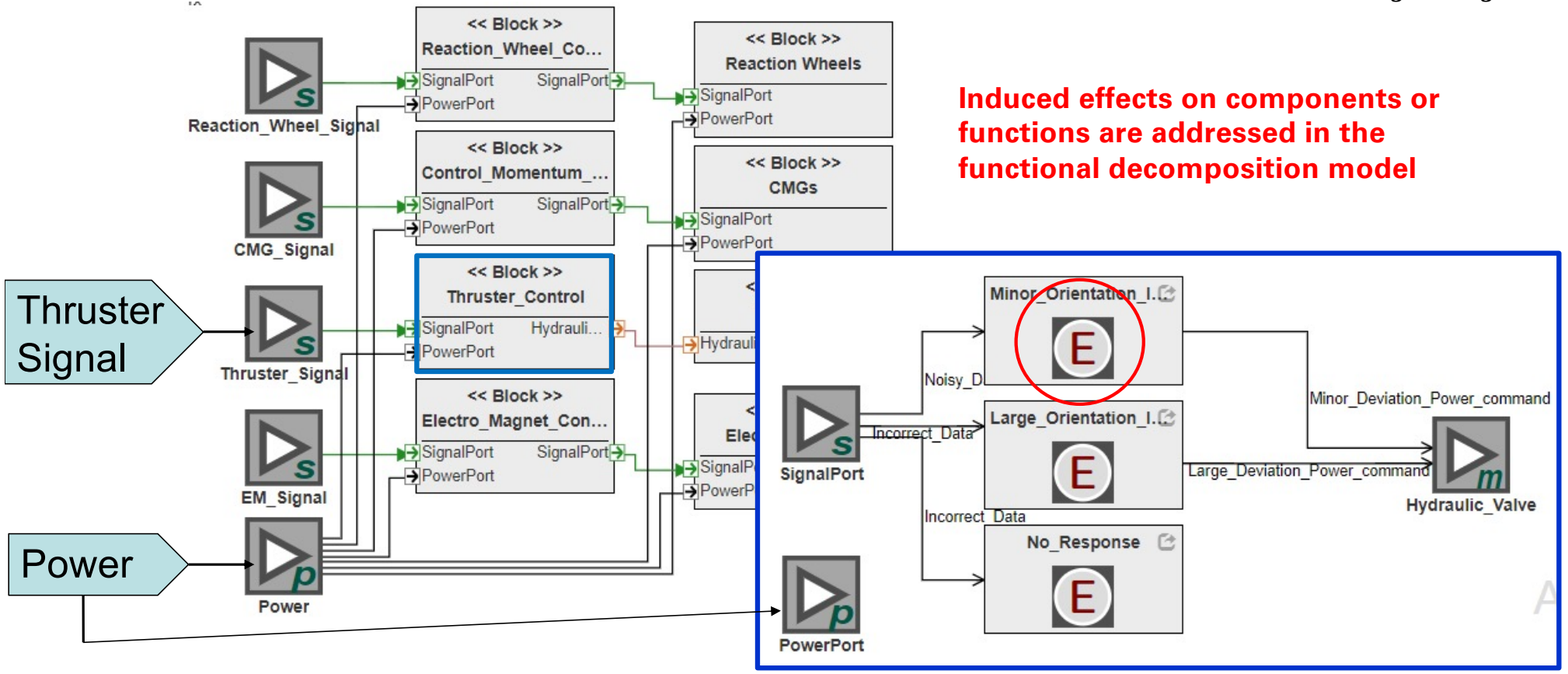
Fault Propagation Diagram- Microprocessor

Vanderbilt Engineering



Fault Propagation Diagram- Control Actuators

Vanderbilt Engineering

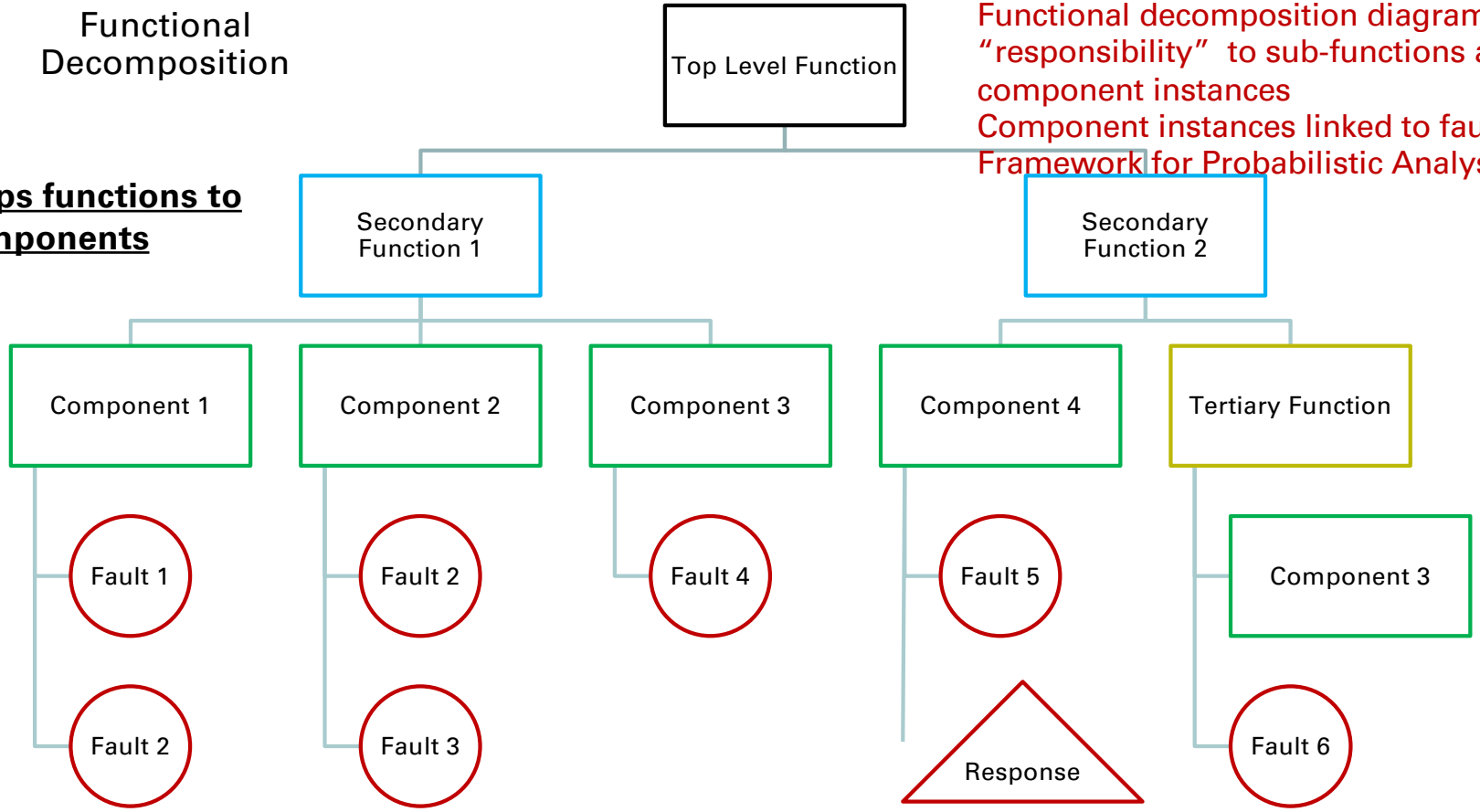


Additional Diagram to SysML Canonical Set: Functional Decomposition Model

Vanderbilt Engineering

Functional Decomposition

Maps functions to components



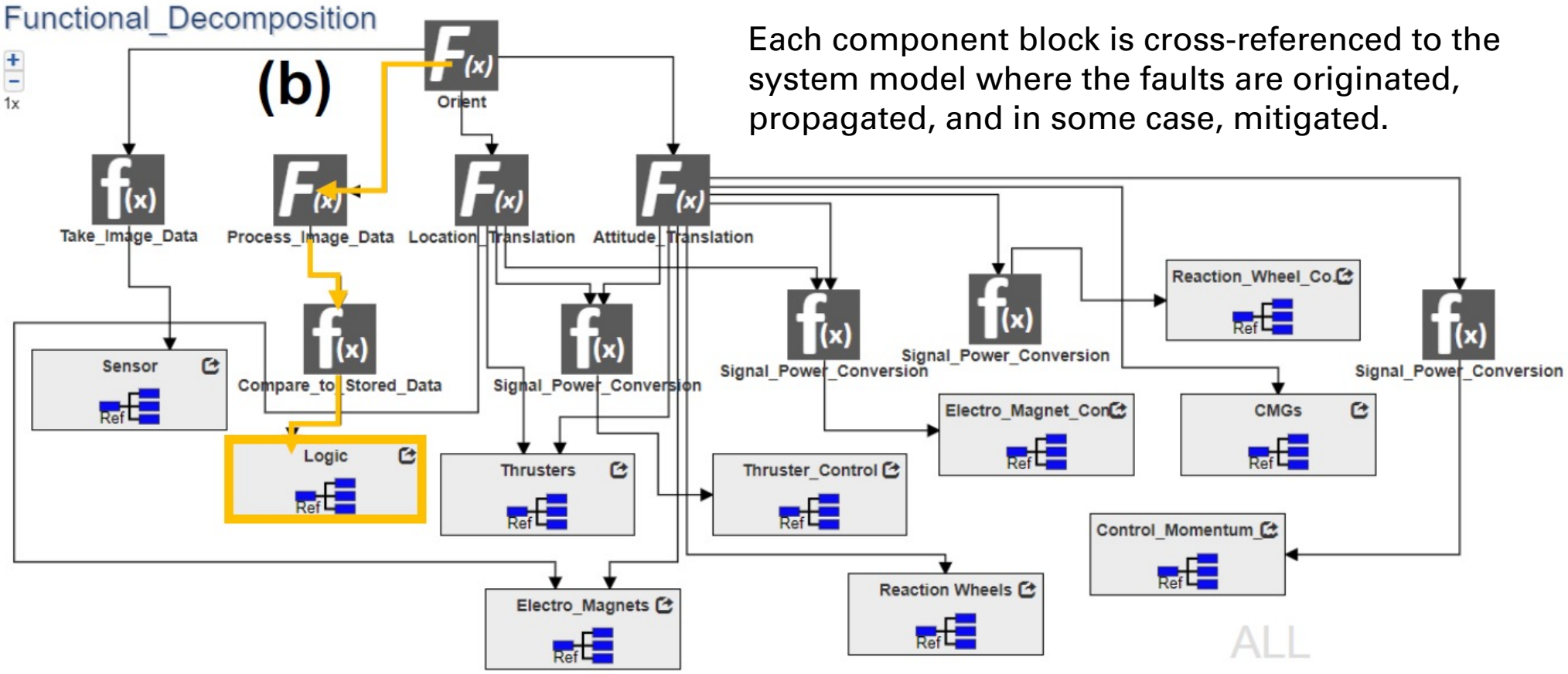
Functional decomposition diagrams assign "responsibility" to sub-functions and component instances

Component instances linked to fault models

Framework for Probabilistic Analysis: FT, BN

Functional Decomposition Model: Star Tracker Subsystem

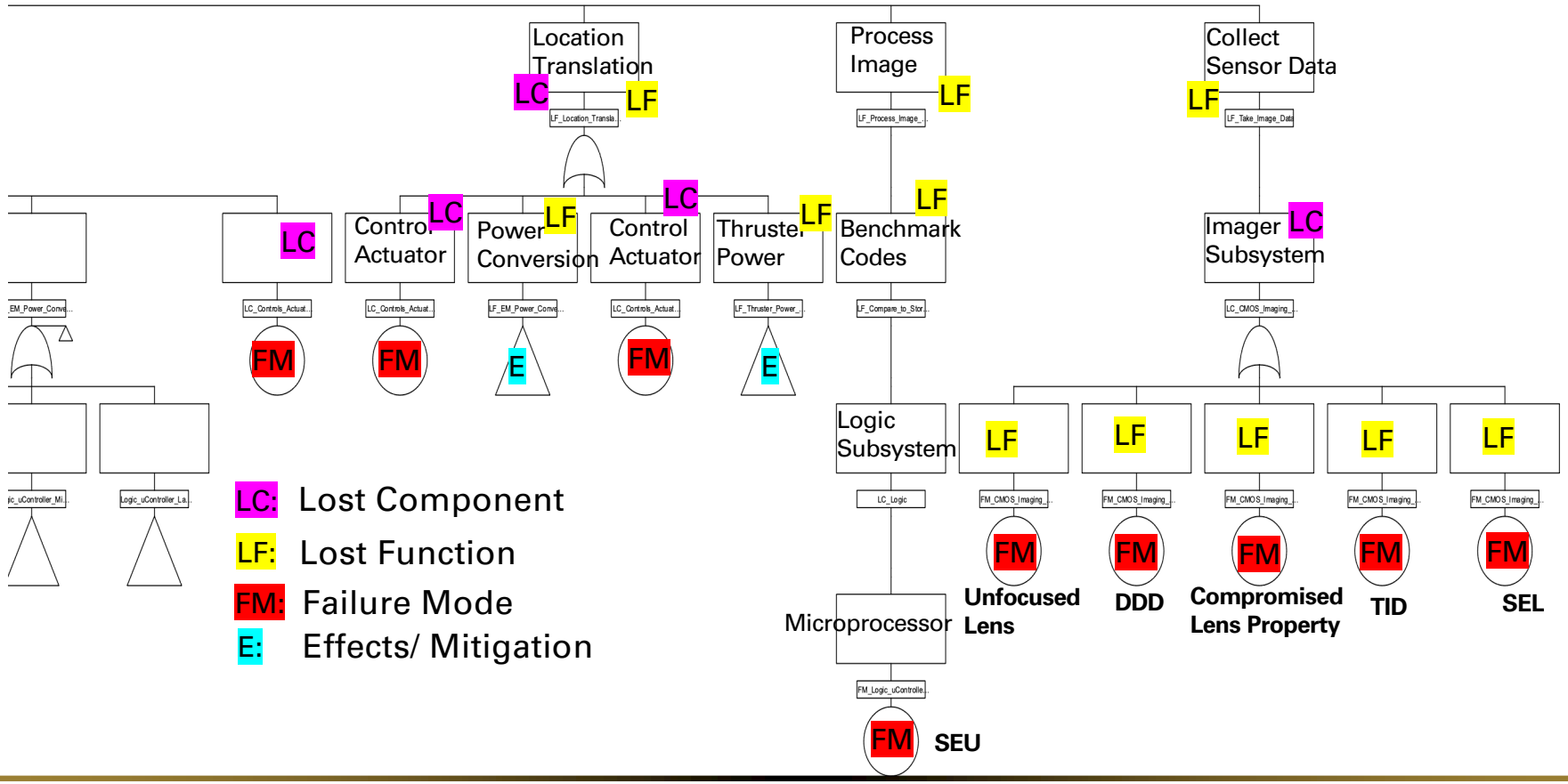
Vanderbilt Engineering



Each component block is cross-referenced to the system model where the faults are originated, propagated, and in some case, mitigated.

Fault Tree Analysis Based on Functional Decomposition

Vanderbilt Engineering



Summary

Vanderbilt Engineering

- SEAM platform based on SysML Diagram set, plus two diagrams
  - Fault origination and propagation diagram
  - Functional decomposition diagram
- Model combination allows low-level fault modeling of individual components, e.g., radiation effects on semiconductors
- Fault-effects can be propagated from components to impact on top-level system functions
- Sufficient information to generate fault trees and Bayesian nets
- Demo version: modelbasedassurance.org

Future work: Create radiation assurance case for radiation performance of star tracker and use automatic cross checker to ensure each fault effect in the SysML model is addressed in an argument in the assurance case