Model Based Assurance At JPL

Office of Safety and Mission Success

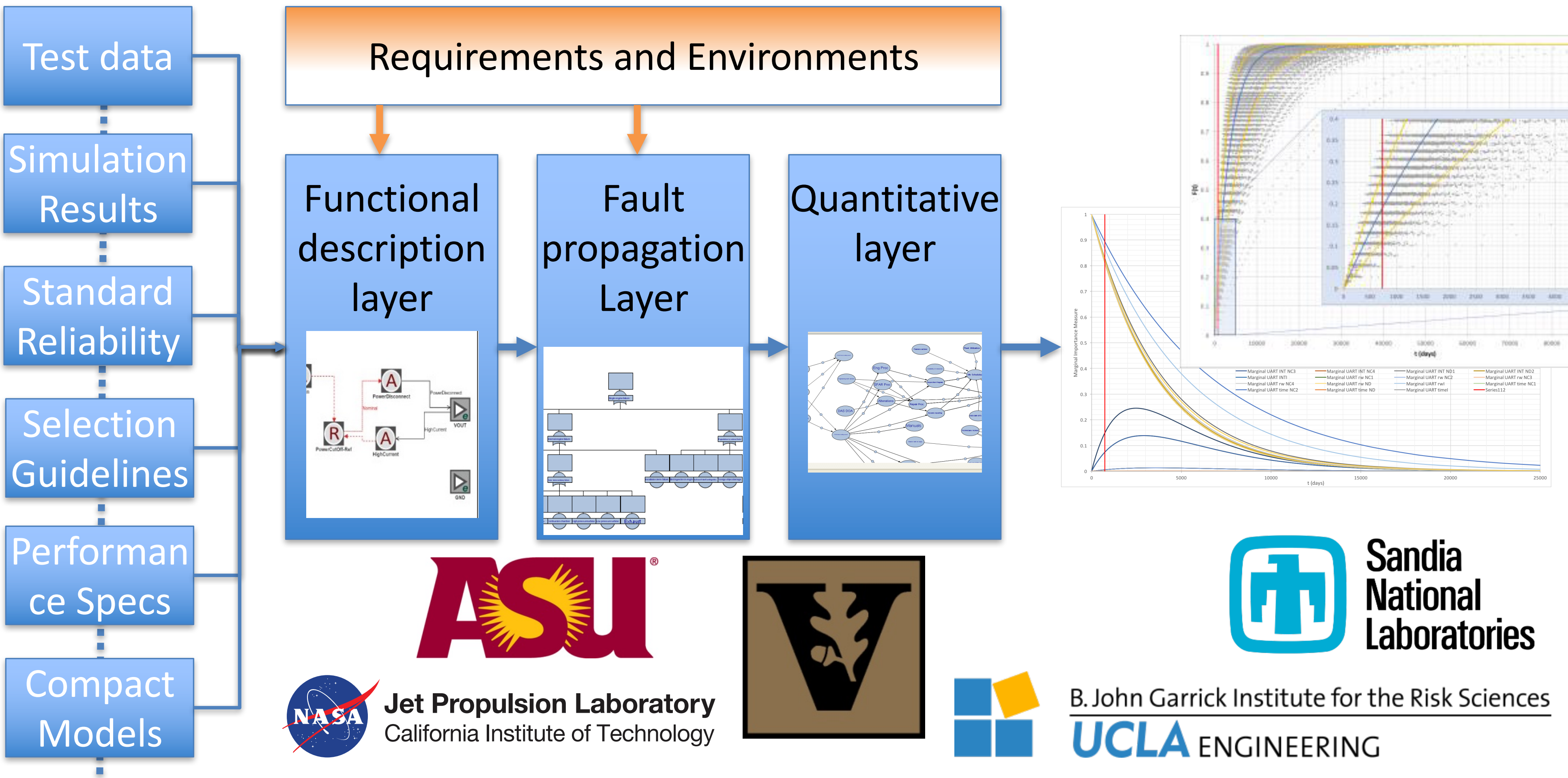
October 2017

Jet Propulsion Laboratory
California Institute of Technology

High Level Goals

- Aid design decision throughout the project life cycle
- Tailor model fidelity to project risk posture and design maturity
- Low fidelity models are
  - not quantitative and use generic and/or best guess reliability information
  - comparative to support system architecture studies and fault protection
  - informing the user of key risk drivers
  - very fast! Spacecraft models created in weeks. Scenarios executed in minutes.
- High fidelity models
  - are multi scale and have the ability to model piece parts and entire spacecraft
  - use test data, physics based simulation results, lookup tables, heuristics, etc.
  - are quantitative and estimate level of confidence (UQ, Monte Carlo, …)

Notional Flow



ASU

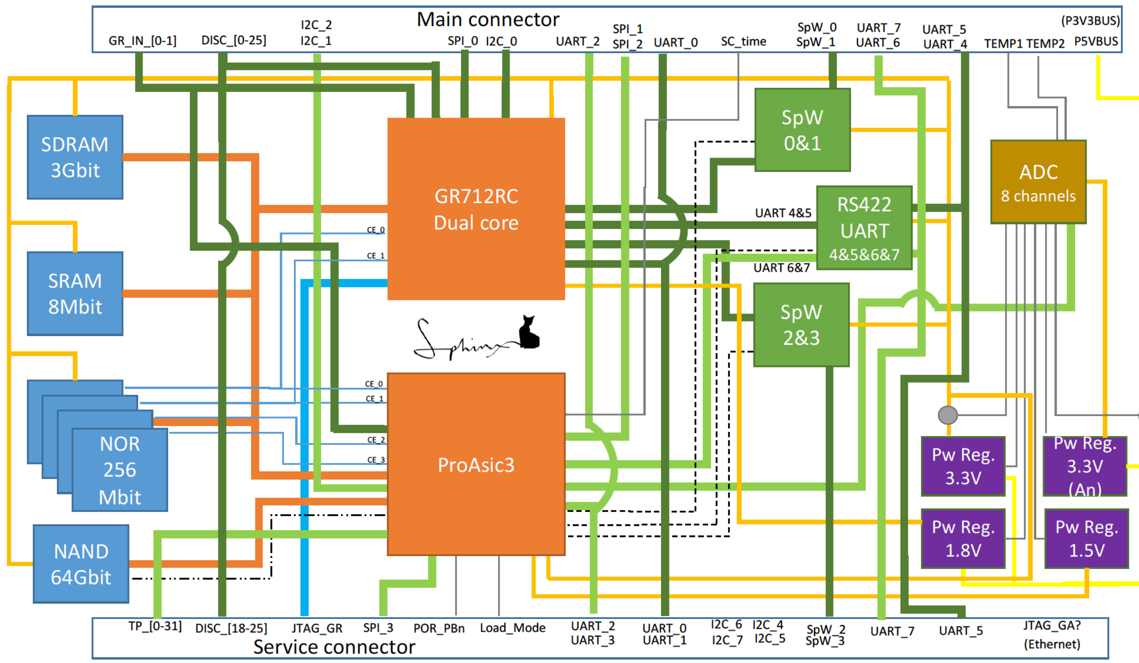
Jet Propulsion Laboratory
California Institute of Technology

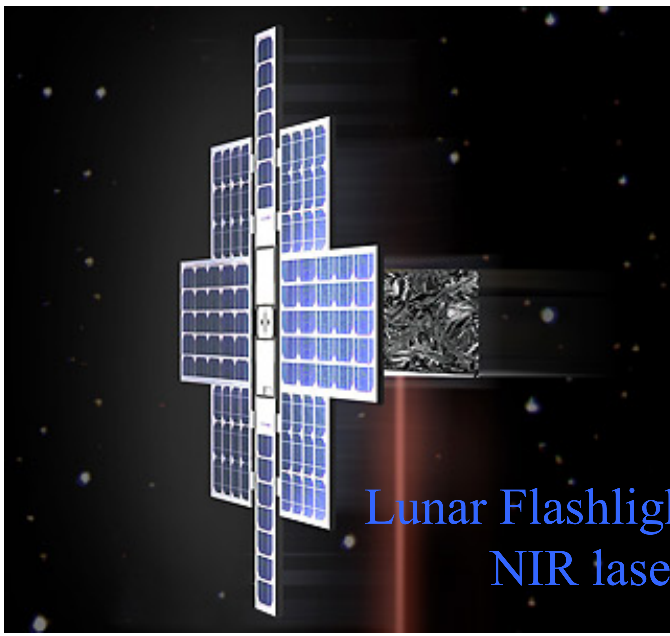
Sandia National Laboratories

B. John Garrick Institute for the Risk Sciences
UCLA ENGINEERING

Our Test Case: Lunar Flashlight C&DH

- **We provided a complete part list**
- **CAD Drawings**
- **FMECA**





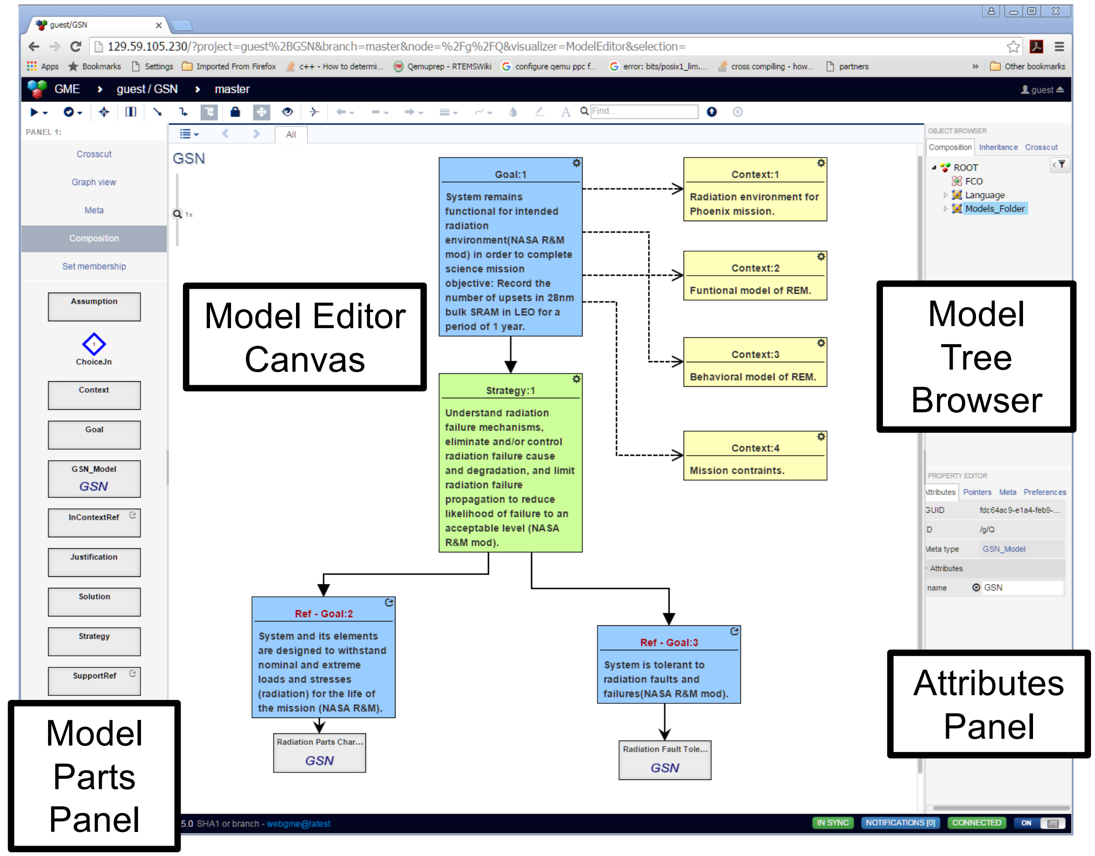
Lunar Flashlight (6U)
NIR laser

TID Modeling within SEAM Tool

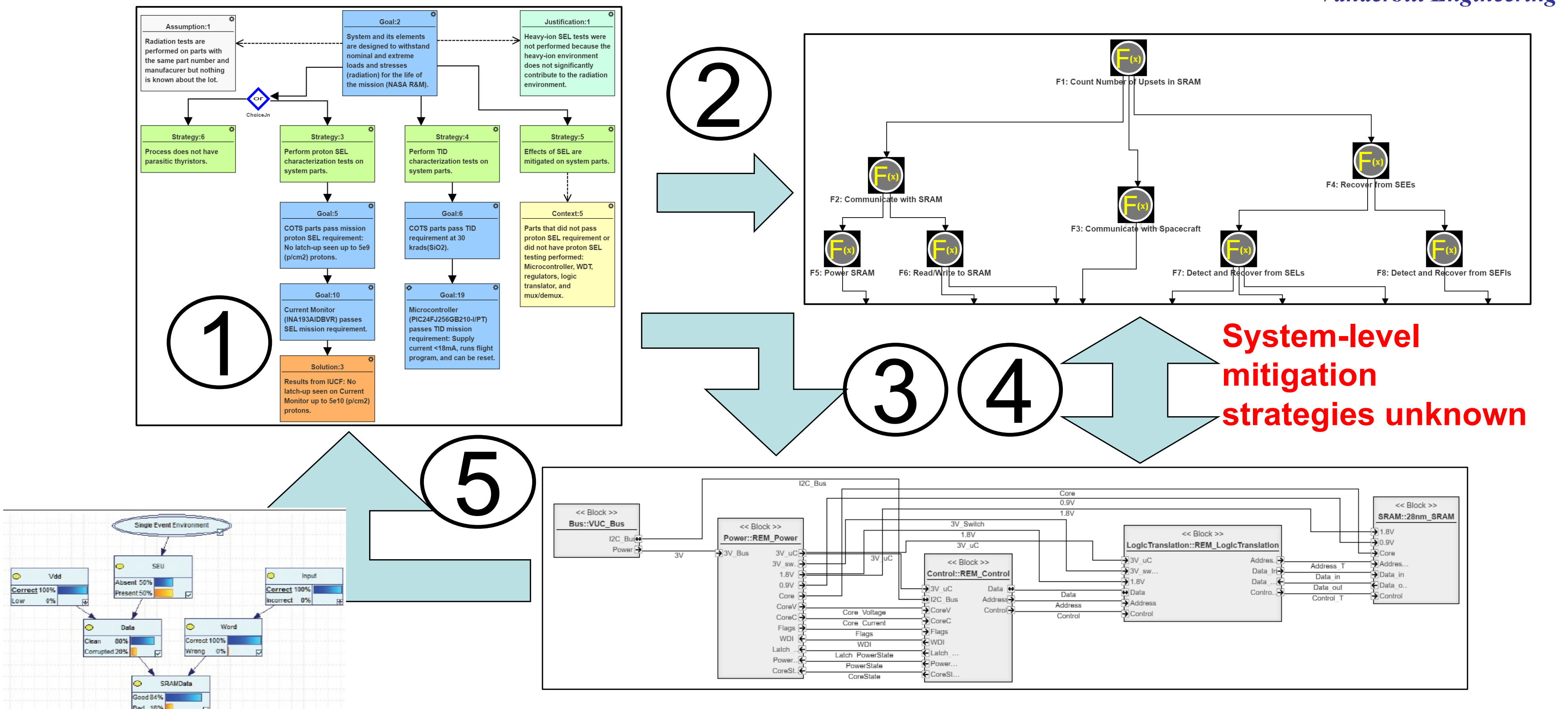
(System Engineering Analysis and Modeling)

Vanderbilt Engineering

- **SEAM is built using WebGME tool**
- **Users can**
  - construct functionality and fault propagation diagrams in SysML
  - create GSN arguments for safety cases,
  - link between the SysML and the GSN descriptions.



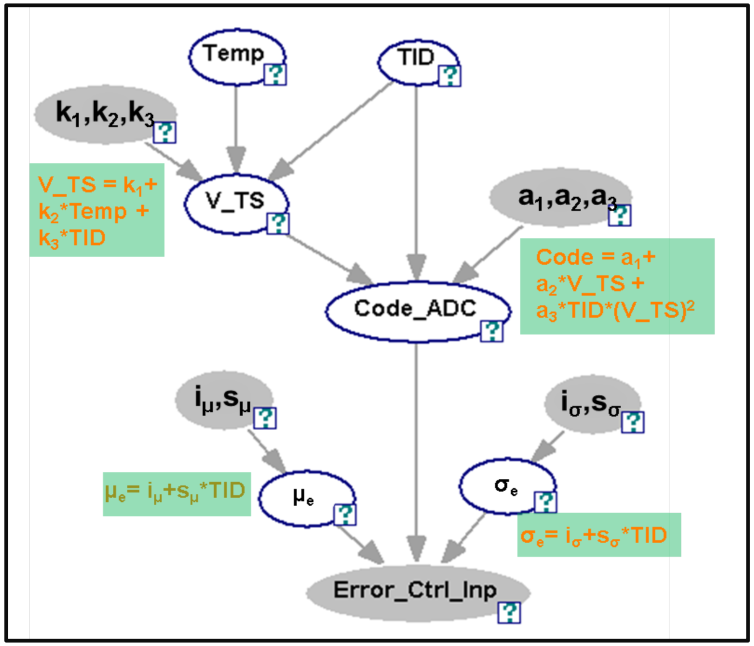
Notional Modeling Flow



Continuous Bayesian Network Results

(Temp control loop)

Vanderbilt Engineering



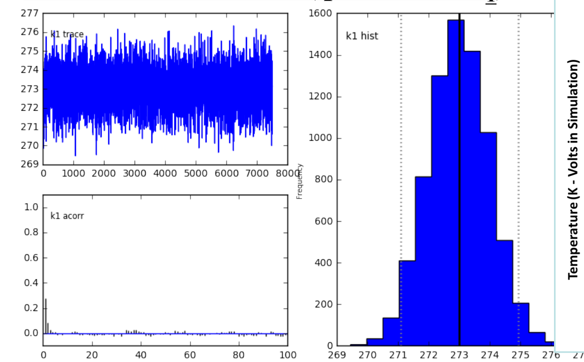
Legend

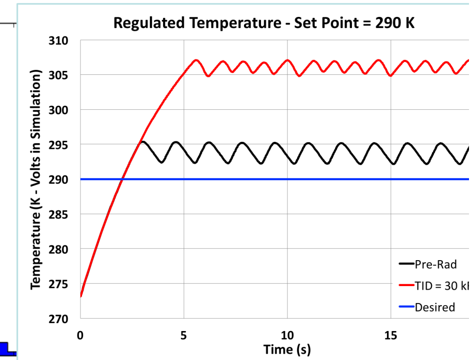
x -- Stochastic node – X= Gaussian(μ,σ)

y -- Deterministic node (V_TS, Code, μ_e , σ_e)
Root Nodes with Uniform priors (Temp, TID)

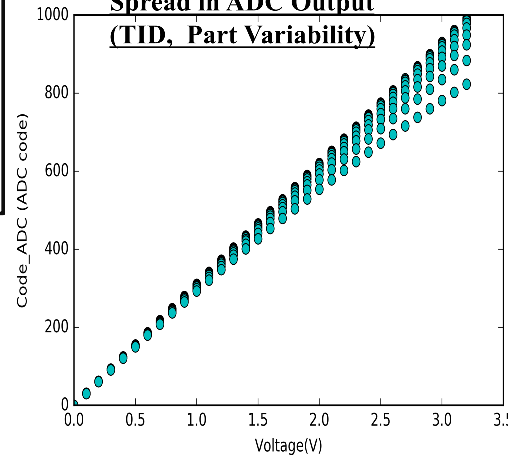
Eqn. -- Likelihood Function for deterministic nodes

Posterior Distribution (parameter k_1)

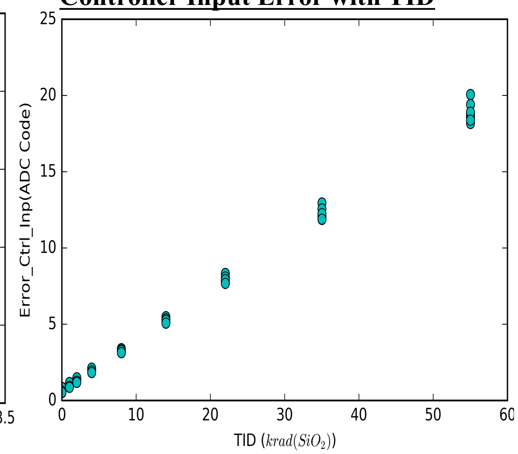




Spread in ADC Output (TID, Part Variability)

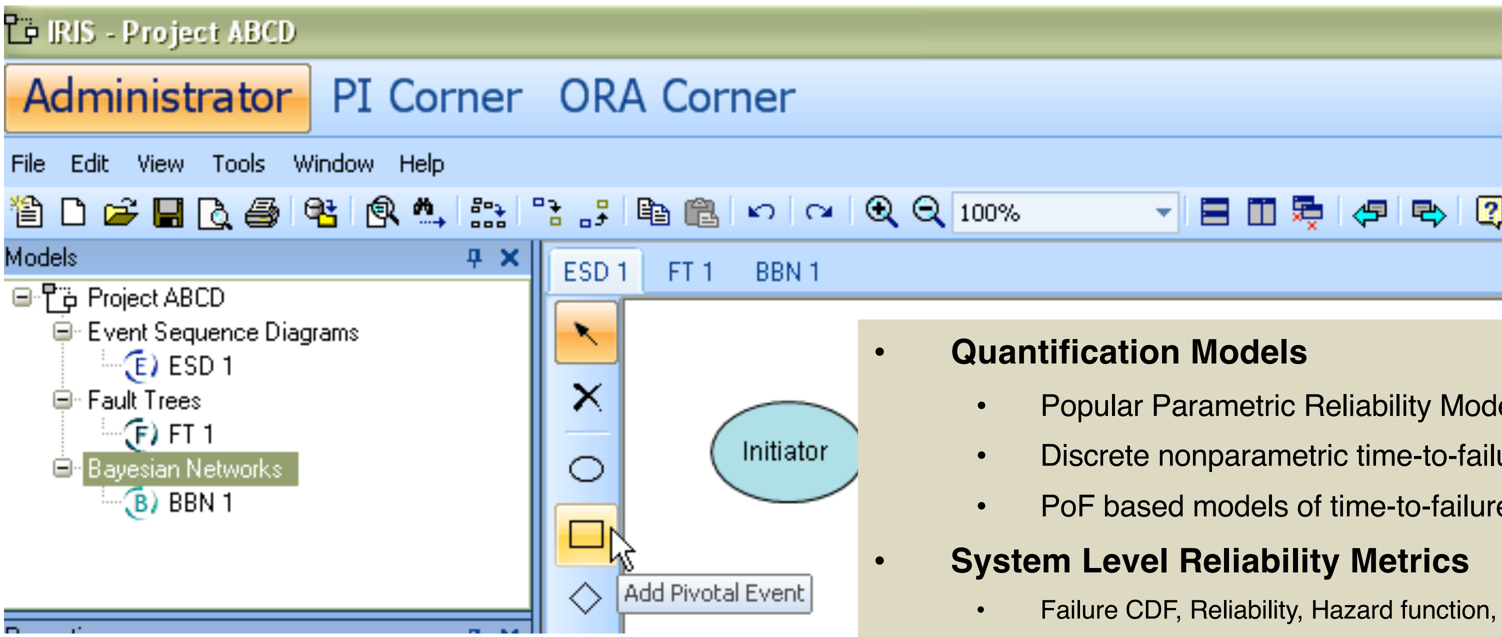


Controller Input Error with TID



System Reliability Modeling within IRIS

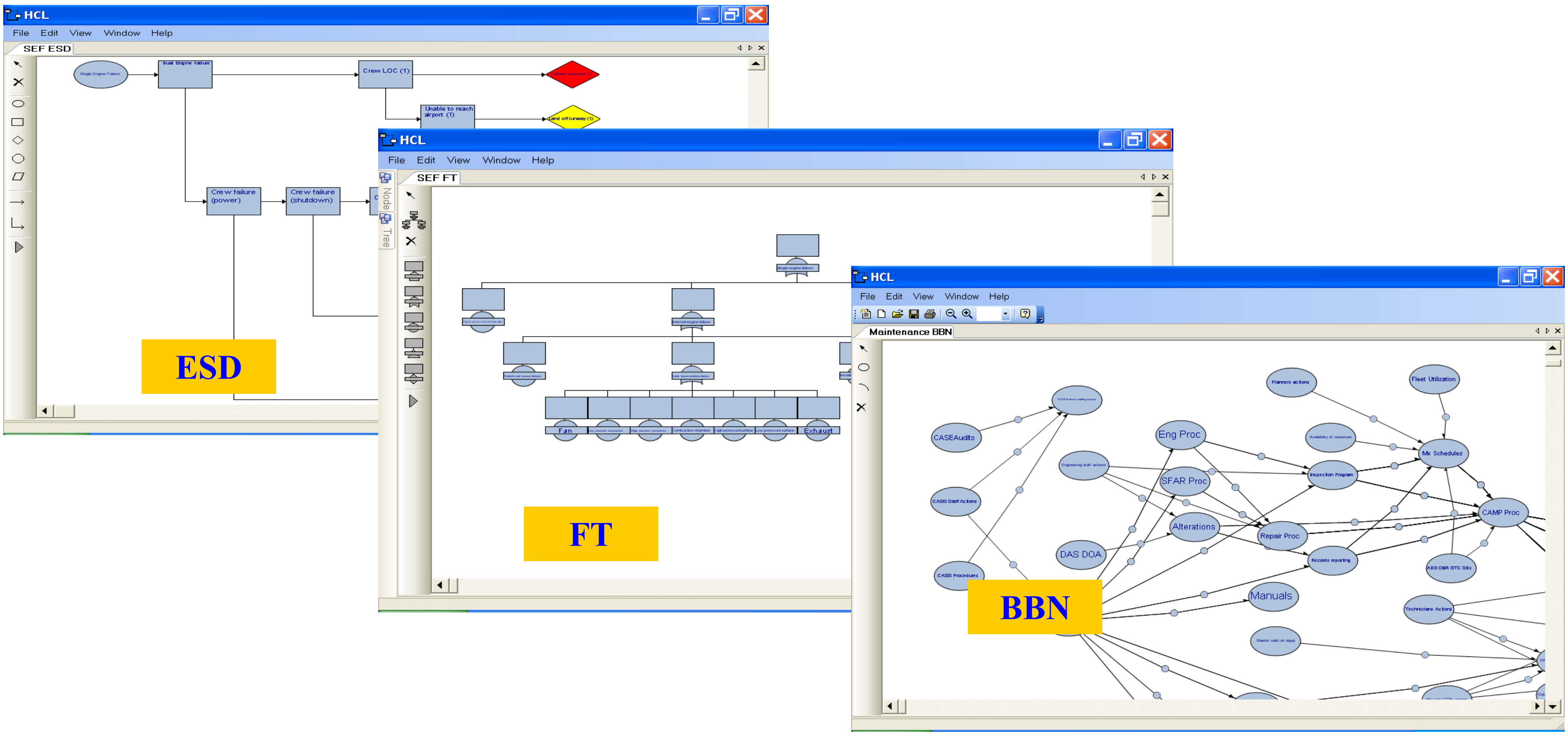
(Integrated Risk Information System)



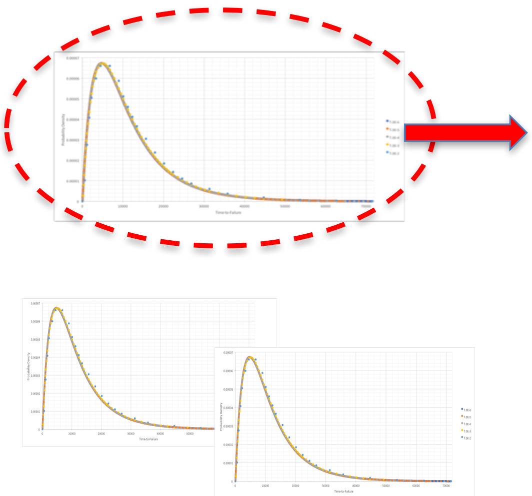
- **Quantification Models**
  - Popular Parametric Reliability Models
  - Discrete nonparametric time-to-failure: e.g. output from MATLAB
  - PoF based models of time-to-failure (with global parameters)
- **System Level Reliability Metrics**
  - Failure CDF, Reliability, Hazard function, Mean time-to-failure, etc
- **Post-processing of results**
  - Cut-sets
  - Ranking of basic events by the following importance measures:
    - Conditional probability, Marginal Improvement Potential, Criticality, Diagnostic, Risk Achievement / Reduction Worth

IRIS Logic Modeling Capability

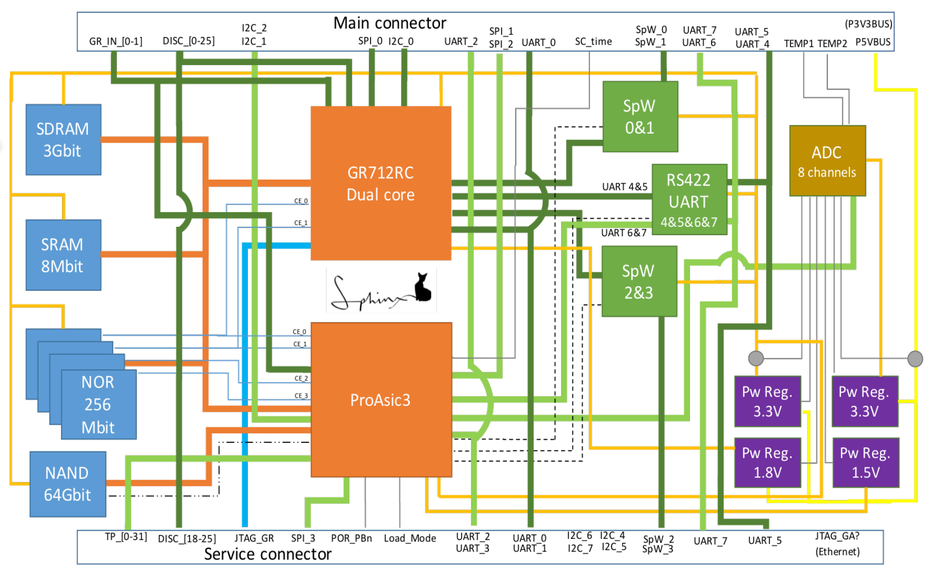
UCLA

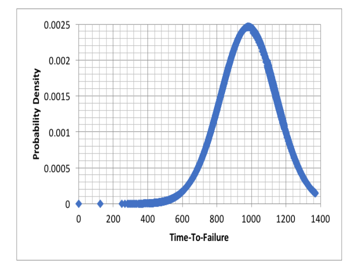


The Entire C&DH Board
(Using Standard reliability functions)



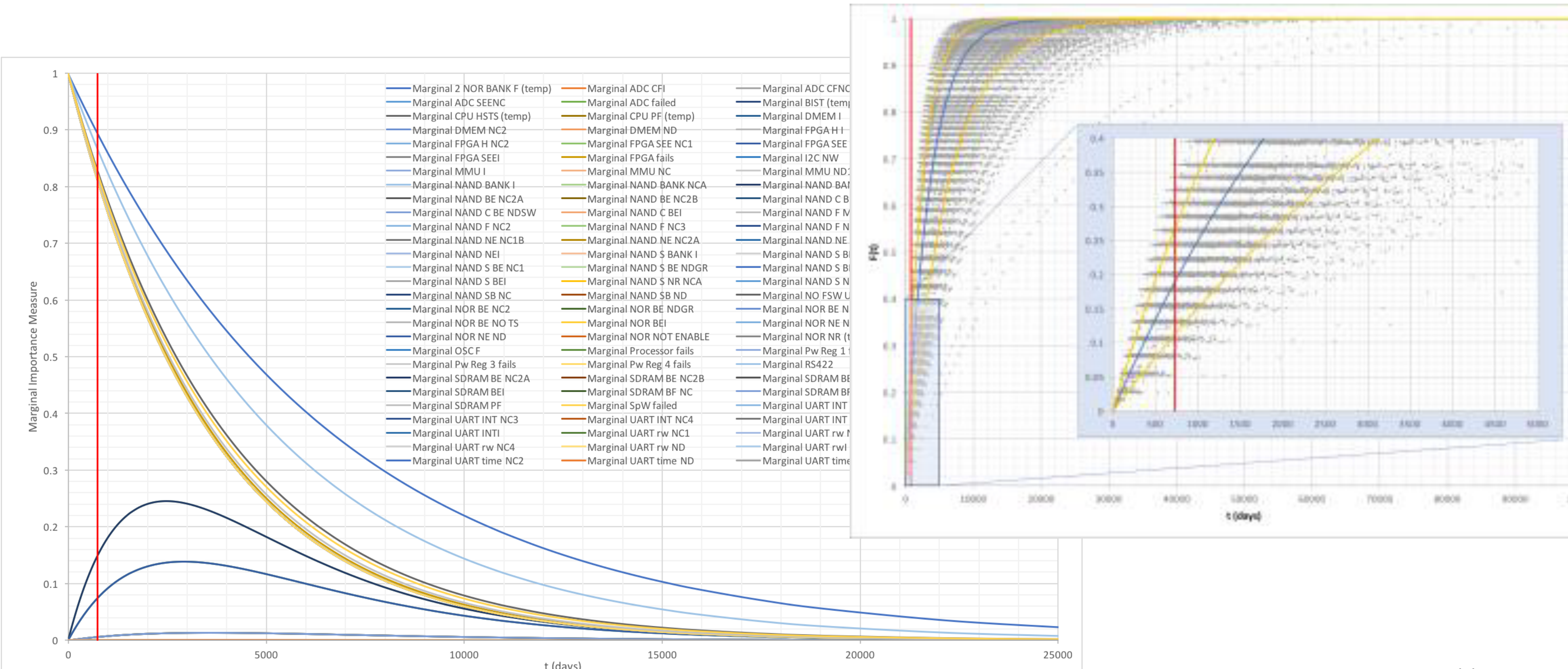
Component Reliability Metrics





System Reliability Metrics

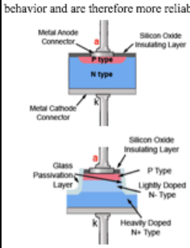
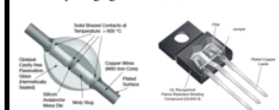
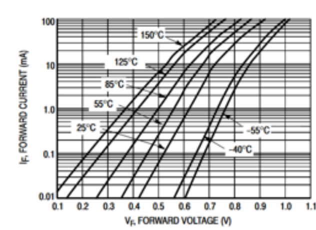
Example Output



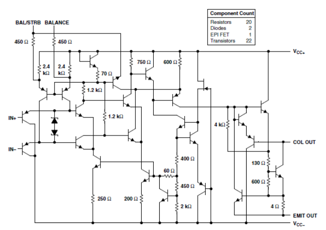
User Guidelines

- Caps, Diodes, Optoelectronics, Microcircuits, Resistors, Thermistors, Transistors
- For each Part Type:
  - Overview/General Construction
  - Circuit Applications
  - Common Failure Modes
  - Failure Mechanisms
  - Technology Trends & General Reliability
  - Recommendations for operation

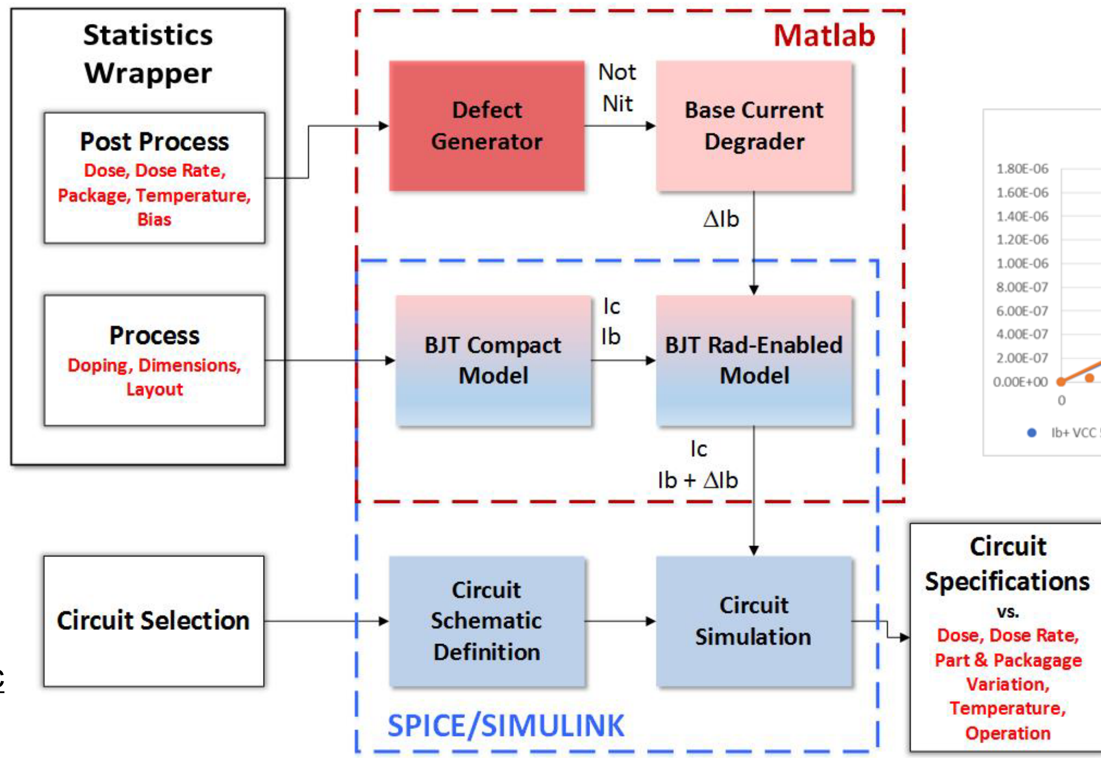
D-1 Diodes

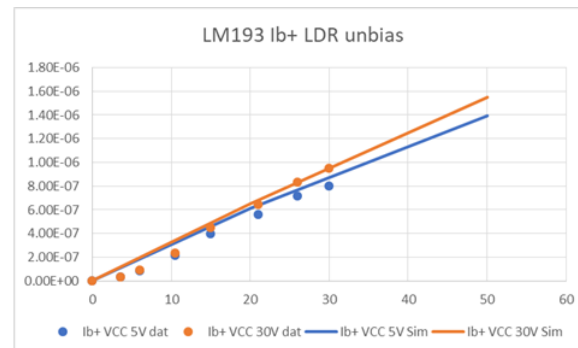
Type	*Overview/General Construction*	*Circuit Applications*	*Common Failure Modes*	*Failure Mechanisms*	*Technology Trends*	*Reliability*	*Recommendations*	*Relevant Graphs & Figures*
Rectifier Diode	Rectifier diodes can handle higher current flow than regular silicon diodes and are generally used in order to change alternating current into direct current. They are designed as discrete components or as integrated circuits and are usually fabricated from silicon and characterized by a fairly large P-N-junction surface. This results in high capacitance under reverse-bias conditions. In high-voltage supplies, two rectifier diodes or more may be connected in series in order to increase the peak-inverse-voltage (PIV) rating of the combination. ***Planar diode structures*** Substrate diode Well diode Epi diode 	Mainly used to convert AC to DC. Used to regulate power in computers and the electrical power in motor vehicles. Also, used in battery chargers for rechargeable batteries, computer power supplies and vehicle batteries.	• Thermal runway • Increase in leakage current • Reduction in reverse breakdown voltage • Open circuit • Short circuit	• Excessive power dissipation due to EOS (electrical over stress) • ESD • Degradation of passivation oxide	Mesa diode construction has better electrical behavior and are therefore more reliable. 	Diodes will experience displacement damage and ionizing damage in severe radiation environments, which can cause significant increases in reverse current. However, diodes show very little functional detriment up to about 10 kRads 50 to 100. Advanced packaging for rectifiers: 	Industry standard derating for 10-yr reliability: • Maximum Tj = 0.75 (Tjmax - 25°C) + 20°C -•Forward Current ≤ 80% Reverse Voltage ≤ 70% Power ≤ 75%	

Creating Compact Model Library for Analog Devices



Bipolar Linear Part Schematic





LT1175, AD590, LP2953, LM193, and TL431

Backup

Current IRIS Features

- **HCL based system logic solver**
- **Scenario cut-set identification, allowing for the identification of the top contributing cut-sets**
- **Scenario point estimate and uncertainty quantification**
- **ESD supports binary pivotal events, and pinch points (multi-phase sequences)**
- **Fault tree supports AND, OR, NOT, K/N gate types**
- **Discrete Bayesian Belief Networks**
- **Modularized design allows different configurations of BBN solvers, BDD solvers**

A More Suitable Platform: Questa ADMS

– mixed-signal modeling and simulation environment
– adaptive/ dynamic stepping solver for differential algebraic equations,
– access to analog models developed in SPICE, VERILOG-AMS and VHDL-AMS,
– easy integration with existing digital components designed in SystemC
– features to use manufacturer supplied IBIS files for modeling communication between the components.