VANDERBILT
School of Engineering

Capturing and Modeling Radiation Hardness Assurance throughout the Project Lifecycle

R. A. Austin

Co-authors: R. D. Schrimpf, A. F. Witulski, N. Mahadevan, G. Karsai, B. D. Sierawski, and R. A. Reed

Vanderbilt University

Nashville, TN

Supported by NASA Grant and Cooperative Agreement Number 80NSSC18K0493

Acronyms and Abbreviations

- **CRÈME: Cosmic Ray Effects on Micro-Electronics Code**
- **DOD: Department of Defense**
- **GSN: Goal Structuring Notation**
- **JWST: James Webb Space Telescope**
- **MBMA: Model-Based Mission Assurance**
- **MBSE: Model-Based Systems Engineering**
- **MRQW: Microelectronics Reliability & Qualification Workshop**
- **NASA: National Aeronautics and Space Administration**
- **RAM: Reliabilty, Availability, and Maintainabilty**
- **R&M: Reliability & Maintainabiltiy**
- **R-GENTIC: Radiation GuidelinEsfor Notional Threat Identification and Classification**
- **RHA: Radiation Hardness Assurance**
- **SEAM: System Engineering and Assurance Modeling**
- **STD: Standard**
- **SysML: System Modeling Language**

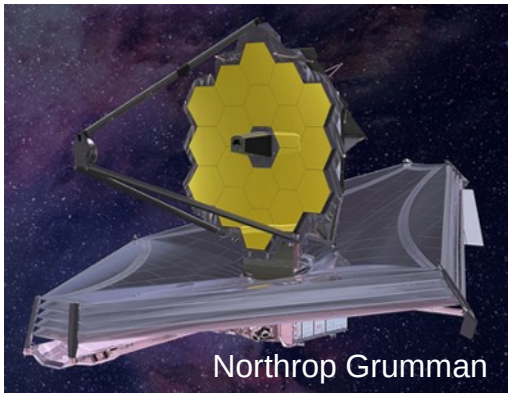
The Parts Engineer

- **End work product: The approved part list**
- **Information needed: Mission orbit and lifetime (can change), parts currently in the system (can change), how the parts are used in the system (can change)**
  - How can I keep up to date with system changes so that I am not working on a part that is no longer in the system?
  - How can I capture my analysis so that another engineer could take over my work?
  - How can I capture my analysis so that it can be reviewed and the risks understood?

Part	Status	Comment
Microcontroller	Passed	
Regulator	Passed with comments	Only passed to X krad (Si)

Model-Based Mission Assurance

- **Goal Structuring Notation (GSN): Modeling language for modeling assurance cases (MRQW 2017)**
  - Language that models safety cases, usually at the end of the design
- **Systems Engineering and Assurance Modeling (SEAM): Web-based platform for MBMA (MRQW 2018)**
  - Supports GSN language and integrates with Model-Based Systems Engineering (MBSE)



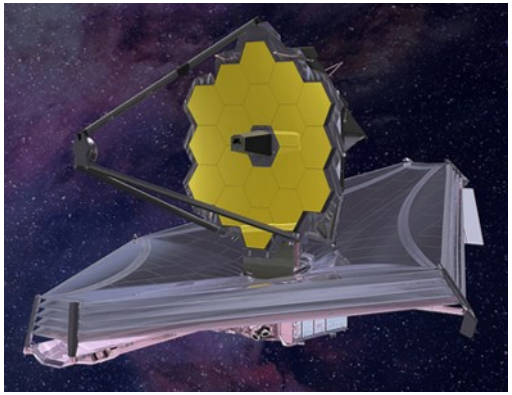
JWST

Orion

CubeSat Deployment

Model-Based Mission Assurance

- **Model-Based Mission Assurance (MBMA): Modeling of mission assurance activities and integration with MBSE**
  - Move from safety cases at the end of the design to mission assurance throughout the design
  - Make mission assurance activities explicit
  - Include MBMA under the MBSE umbrella
  - Capture the logic of the arguments for the assurance of the system, connect to the actual models of the system design



JWST

Orion

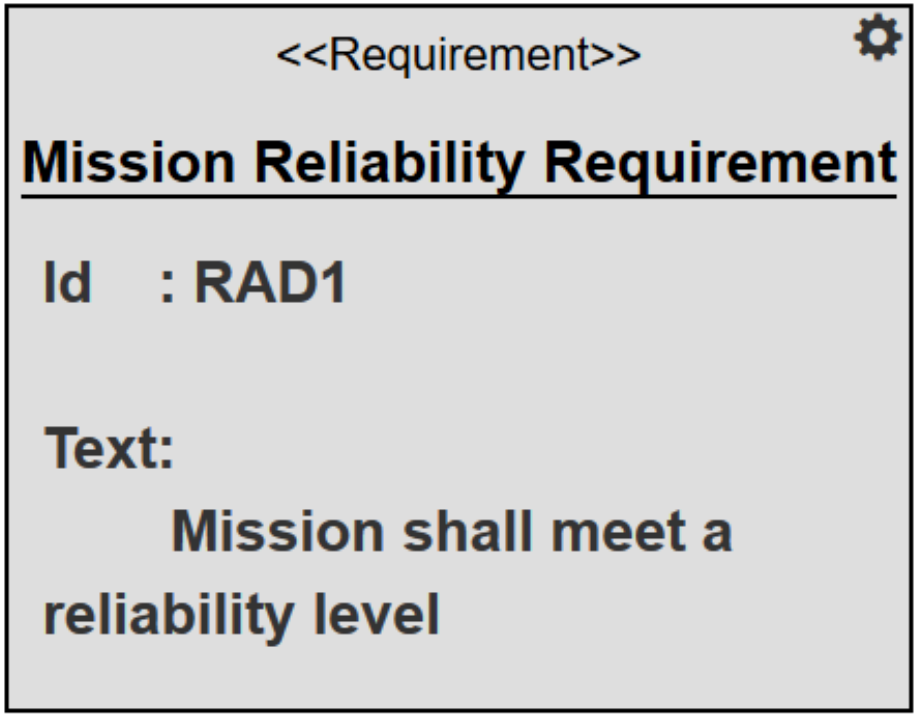
CubeSat Deployment

Today's Example: Total Ionizing Dose Requirement

- **End Requirement: Mission shall meet a reliability level**

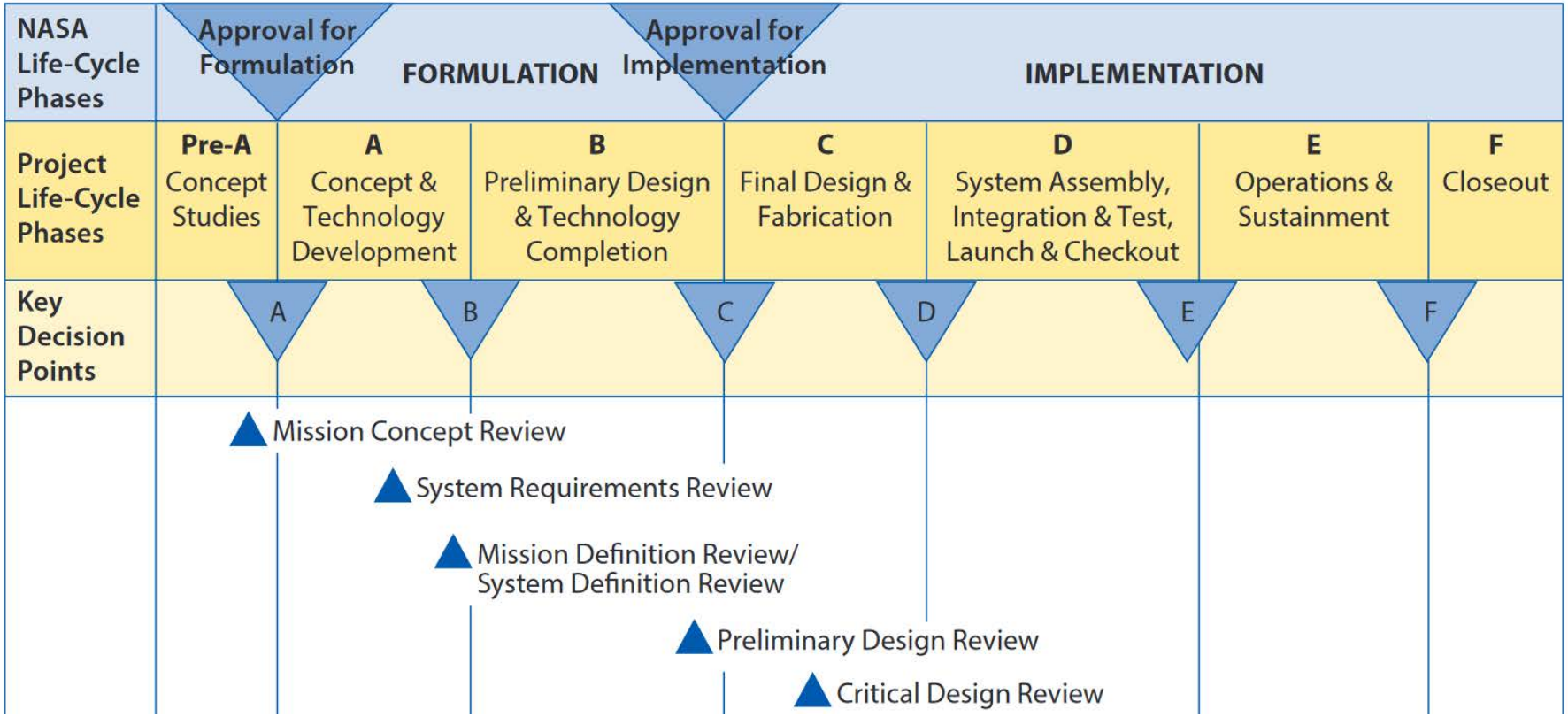
- **How did we derive this requirement?**

- **How do we verify this requirement?**



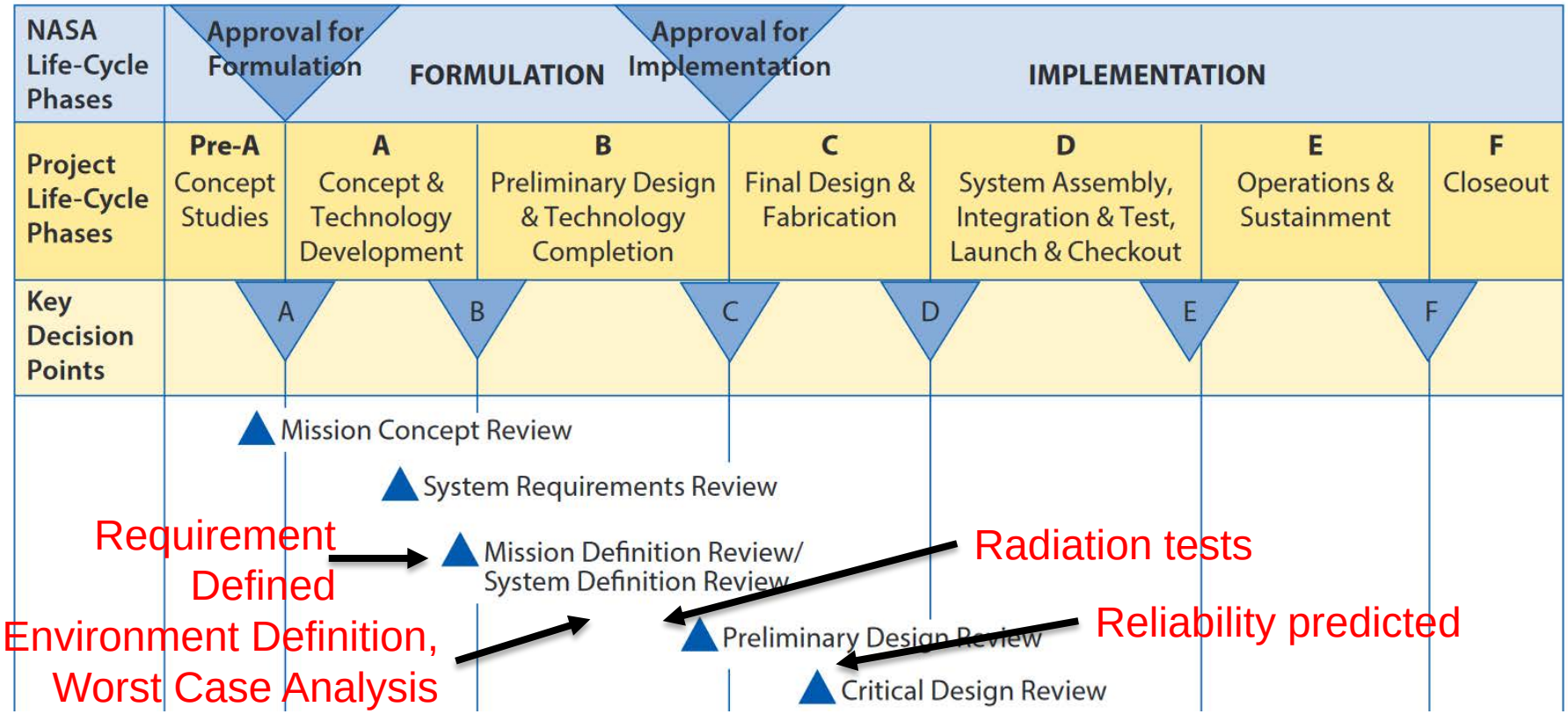
NASA Project Lifecycle Phases

- **The reliability tests and analysis required to verify the requirement take place during several life-cycle phases**
  - In addition, the analysis requires the system to mature and will have to be re-evaluated if the system or mission changes



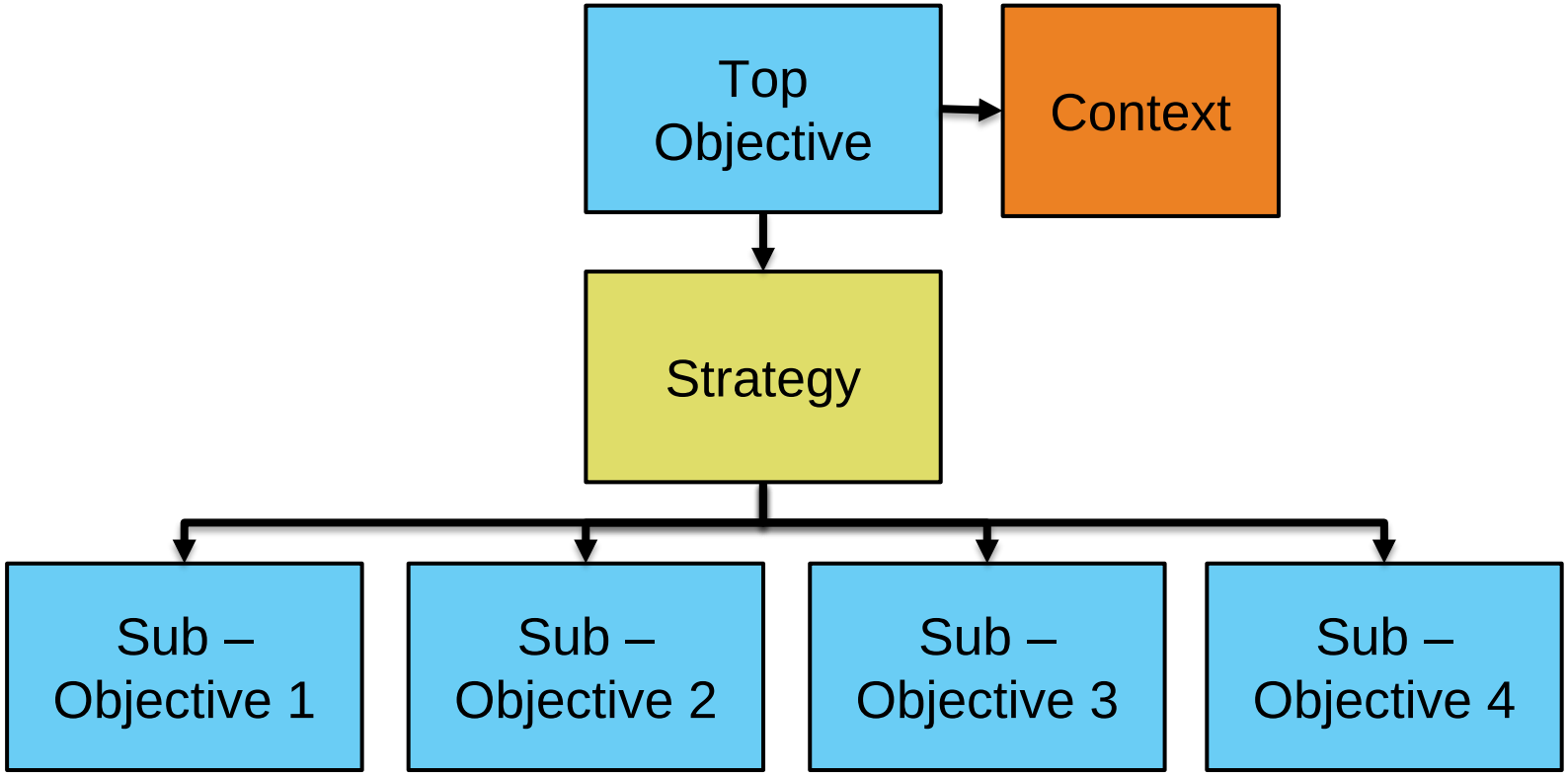
NASA Project Lifecycle Phases

- **The reliability tests and analysis required to verify the requirement take place during several life-cycle phases**
  - In addition, the analysis requires the system to mature and will have to be re-evaluated if the system or mission changes



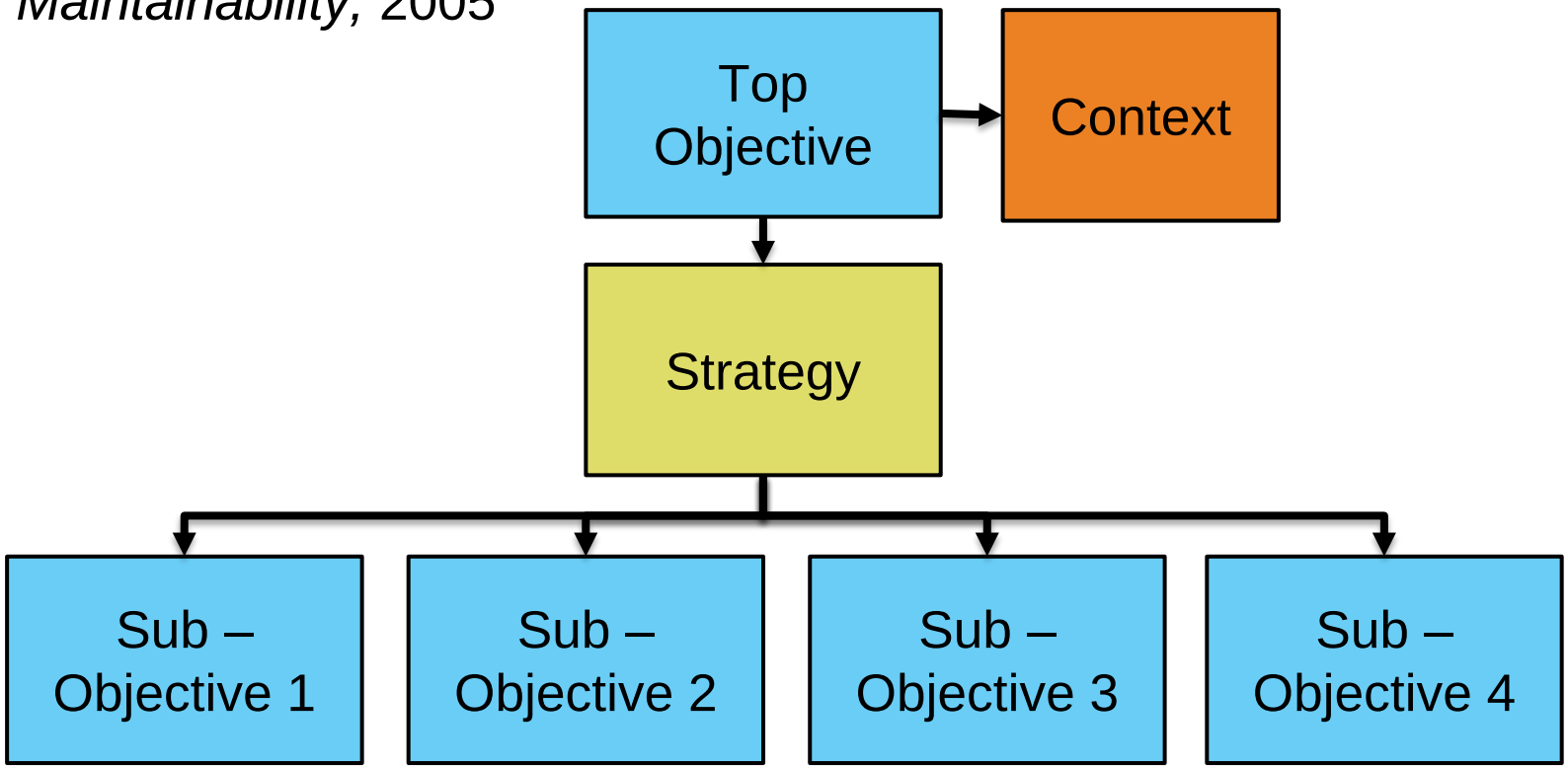
Foundation: NASA Reliability & Maintainability (R&M) Hierarchy

- **Basis of NASA-STD-8729.1 (R&M Standard) released January 2018**
- **Moves to objectives-based reliability requirements**



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

1. **"Understand and document user needs an constraints,**
2. **Design and redesign for RAM,**
3. **Produce reliable and maintainable systems,"**
   - *DOD Guide for Achieving Reliability, Availability, and Maintainability,* 2005



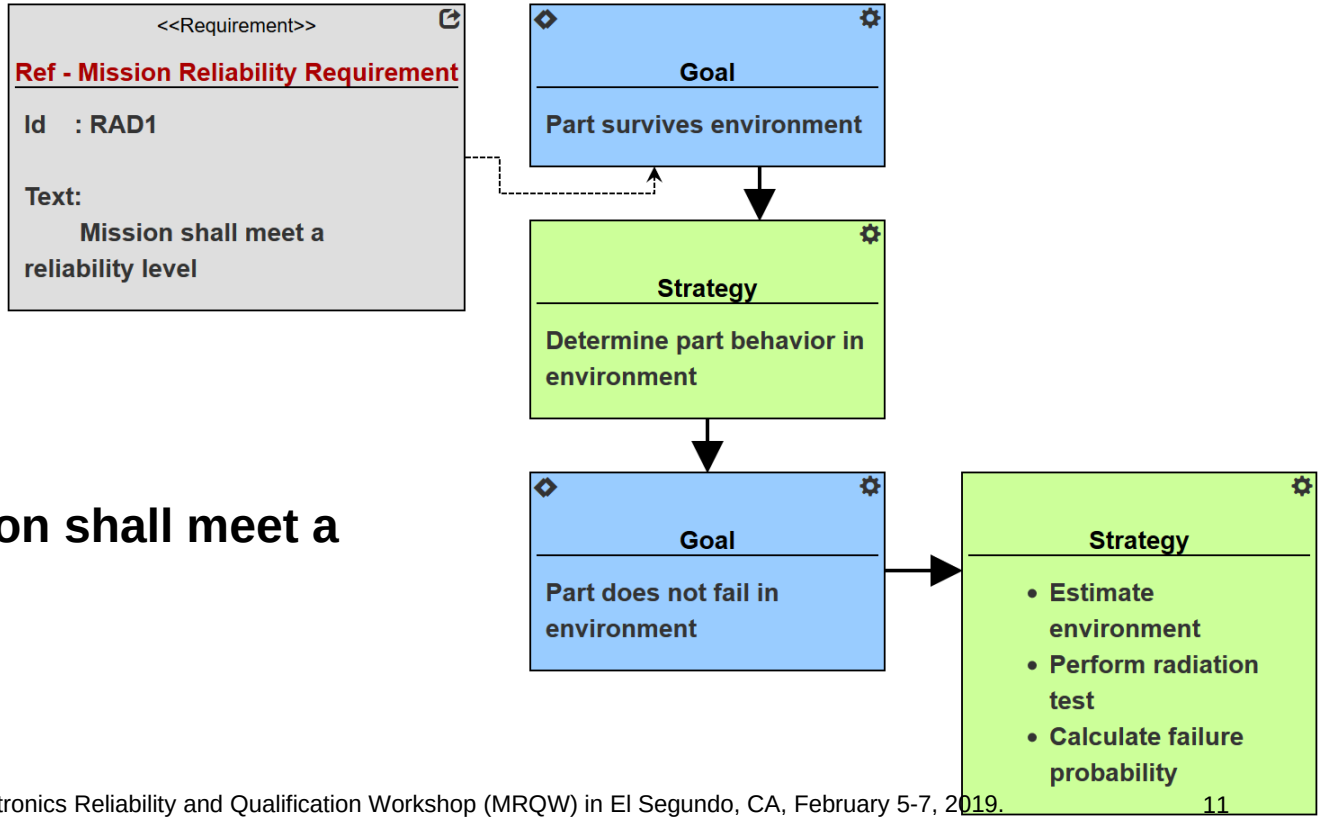
Today's Example: Total Ionizing Dose Requirement

Vanderbilt University School of Engineering

Project Life-Cycle Phases	Pre-A Concept Studies	A Concept & Technology Development	B Preliminary Design & Technology Completion	C Final Design & Fabrication	D System Assembly, Integration & Test, Launch & Checkout	E Operations & Sustainment	F Closeout

Requirement Defined

- **Beginning of Phase B: GSN template for part assurance**
  - Generic goals generated from part assurance templates
  - Framework for planning RHA activities



- **Requirement: Mission shall meet a reliability level**

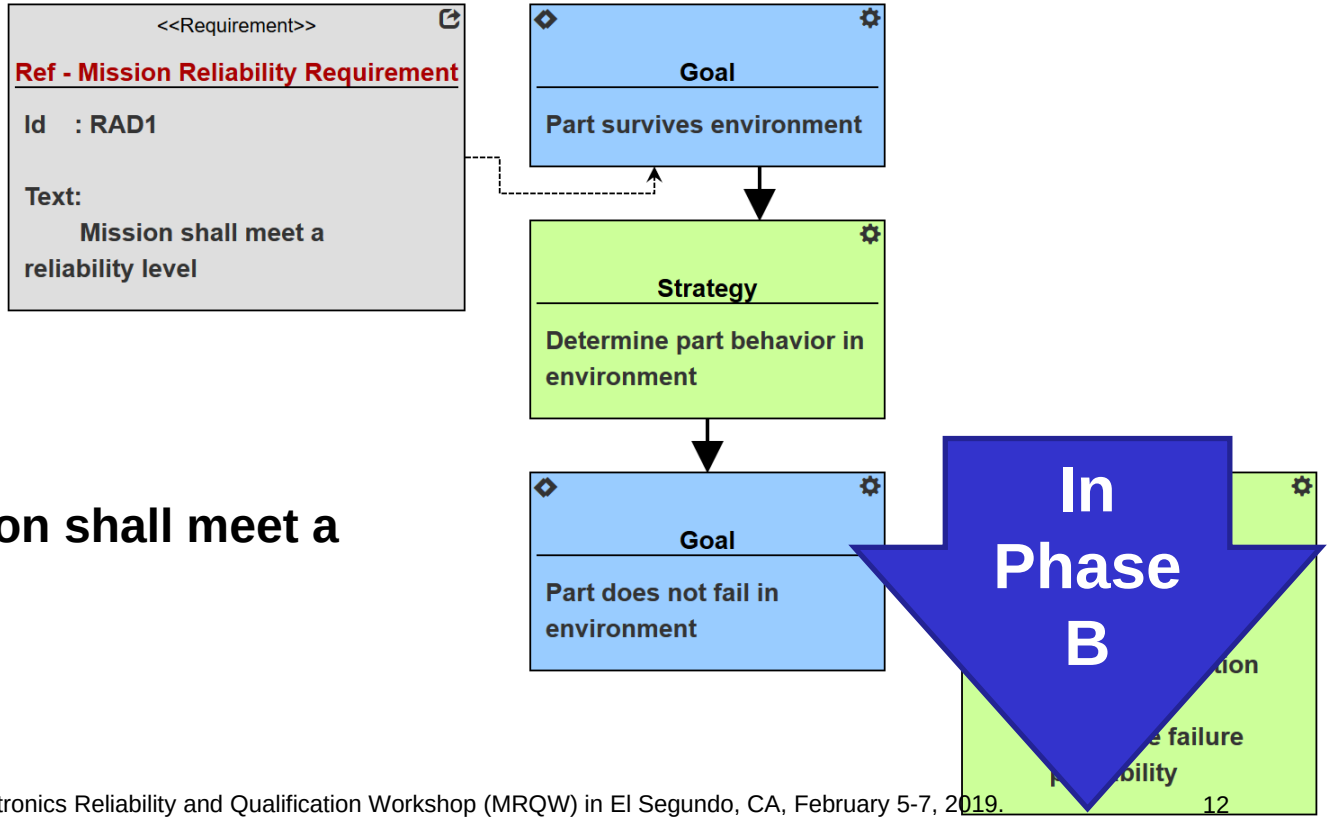
Today's Example: Total Ionizing Dose Requirement

Vanderbilt University School of Engineering

Project Life-Cycle Phases	Pre-A Concept Studies	A Concept & Technology Development	B Preliminary Design & Technology Completion	C Final Design & Fabrication	D System Assembly, Integration & Test, Launch & Checkout	E Operations & Sustainment	F Closeout

Requirement Defined

- **Beginning of Phase B: GSN template for part assurance**
  - Generic goals generated from part assurance templates
  - Framework for planning RHA activities



- **Requirement: Mission shall meet a reliability level**

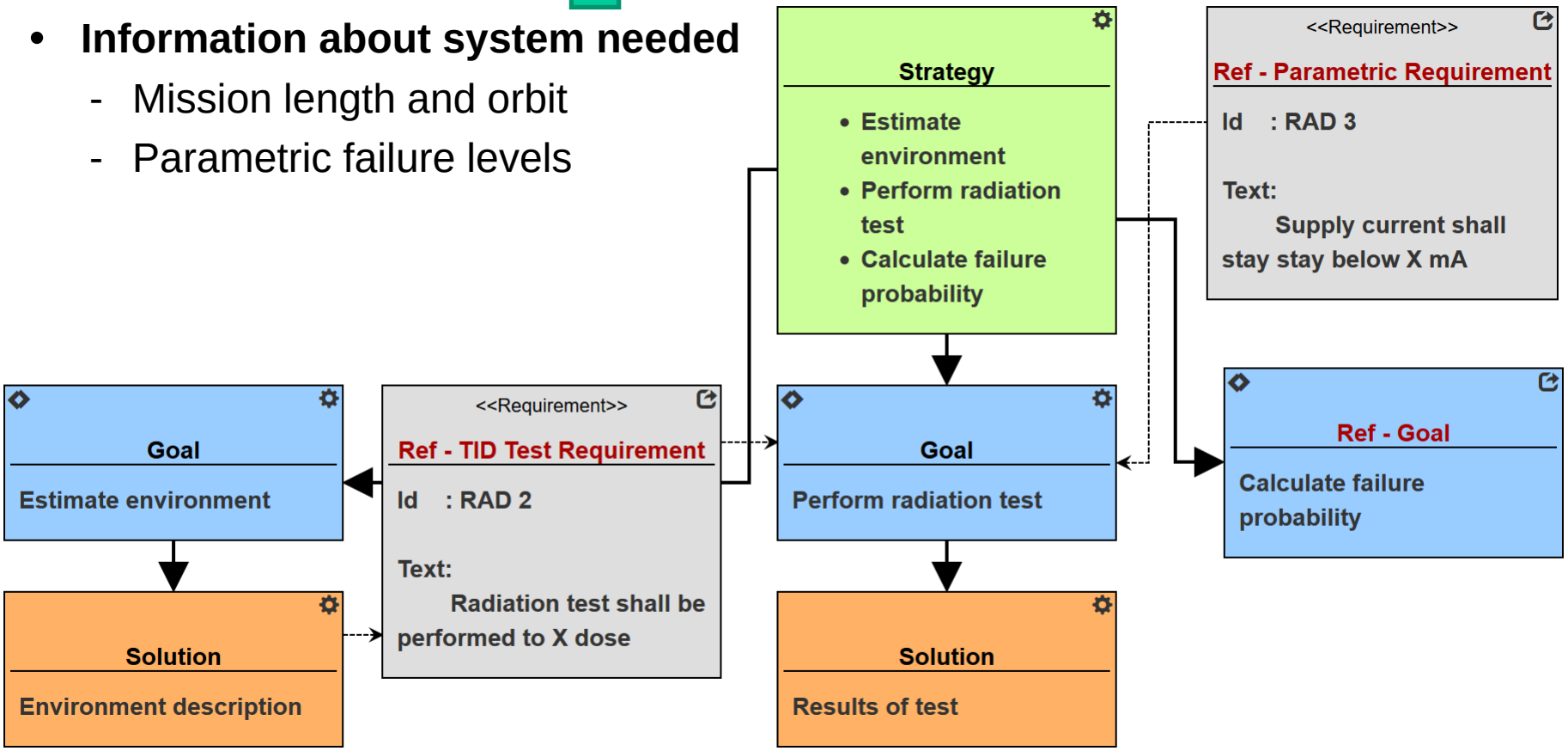
Today's Example: Total Ionizing Dose Requirement

Vanderbilt University School of Engineering

Project Life-Cycle Phases	Pre-A Concept Studies	A Concept & Technology Development	B Preliminary Design & Technology Completion	C Final Design & Fabrication	D System Assembly, Integration & Test, Launch & Checkout	E Operations & Sustainment	F Closeout

Radiation Test Performed

- **Information about system needed**
  - Mission length and orbit
  - Parametric failure levels

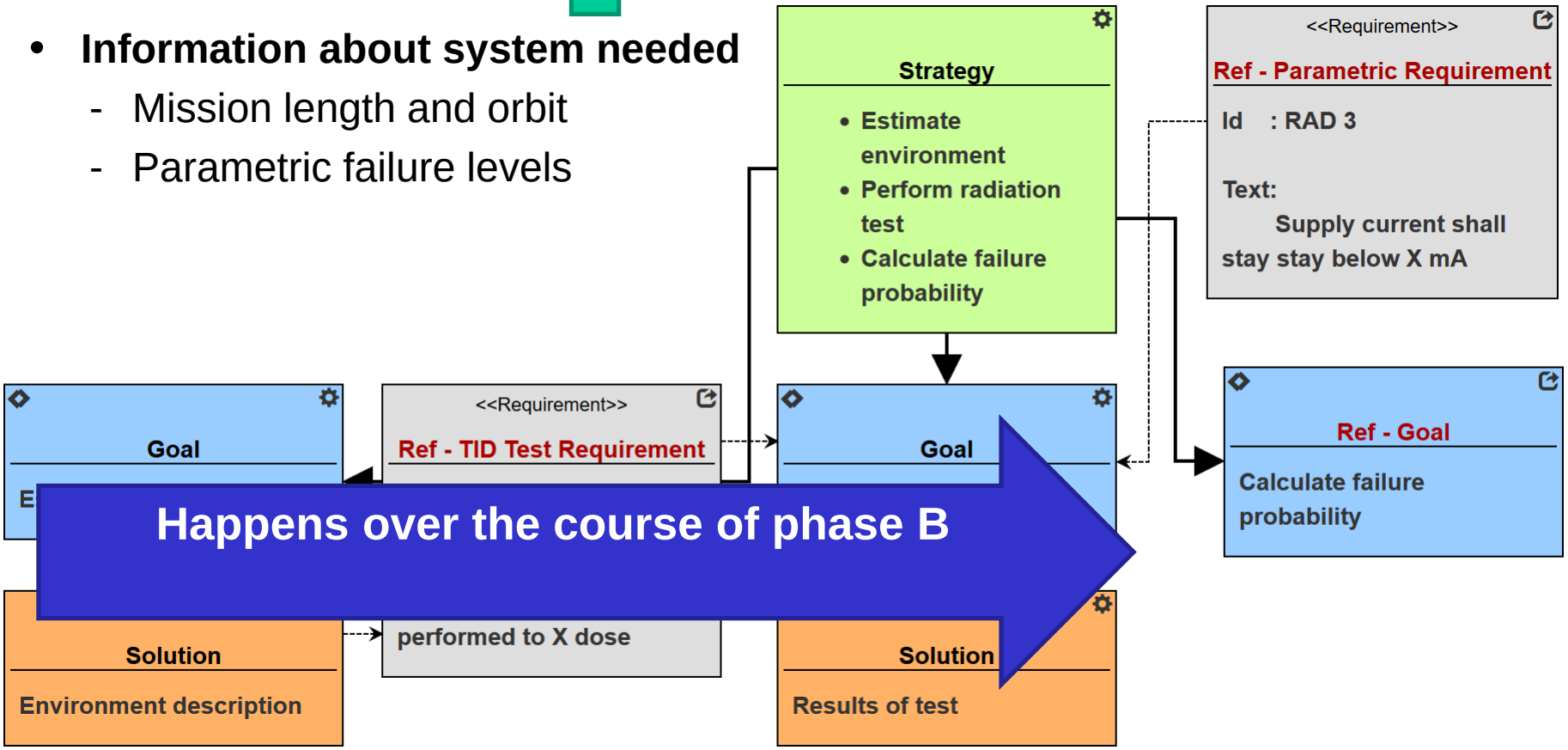


Today's Example: Total Ionizing Dose Requirement

Vanderbilt University School of Engineering

Project Life-Cycle Phases	Pre-A Concept Studies	A Concept & Technology Development	B Preliminary Design & Technology Completion	C Final Design & Fabrication	D System Assembly, Integration & Test, Launch & Checkout	E Operations & Sustainment	F Closeout

- **Information about system needed**
  - Mission length and orbit
  - Parametric failure levels

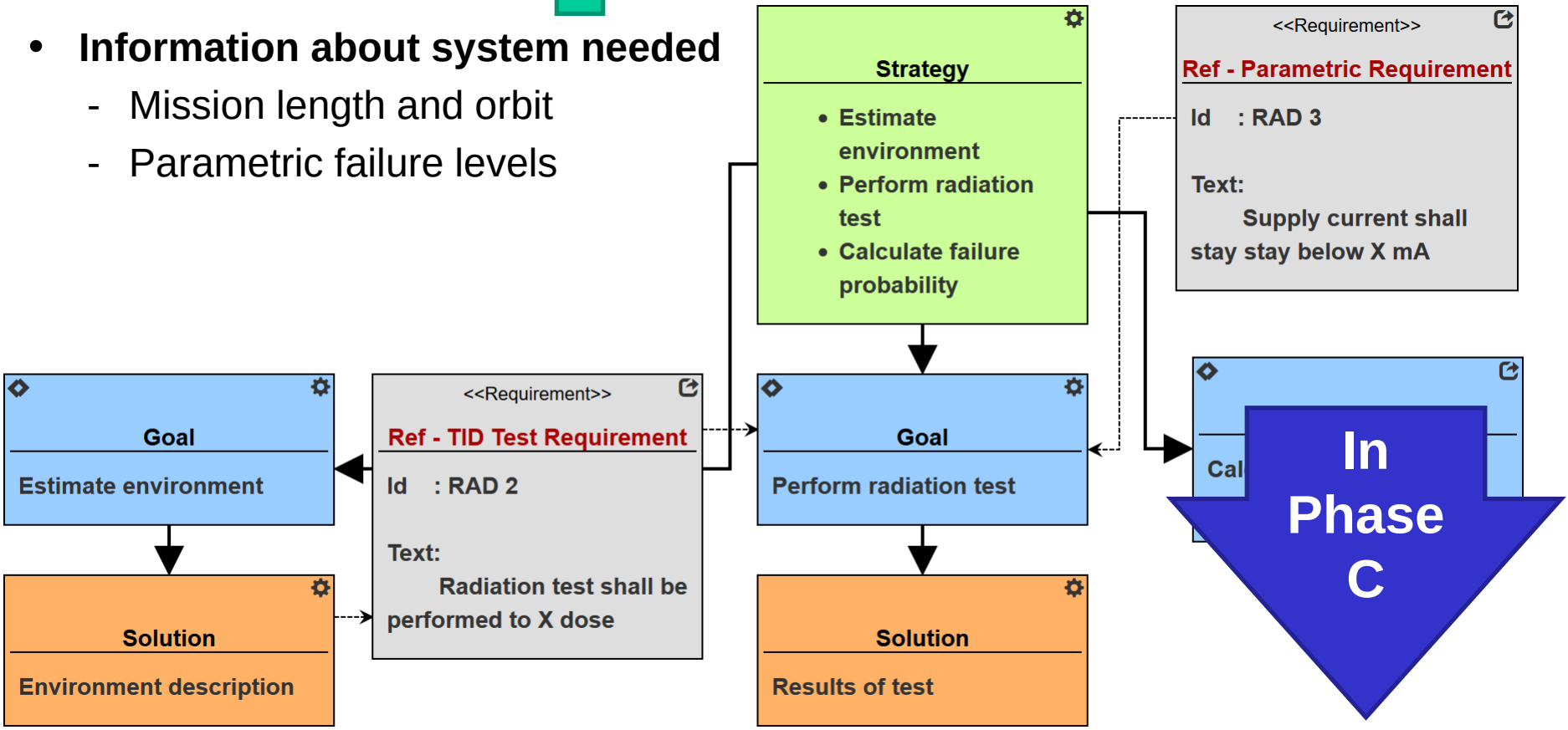


Today's Example: Total Ionizing Dose Requirement

Vanderbilt University School of Engineering

Project Life-Cycle Phases	Pre-A Concept Studies	A Concept & Technology Development	B Preliminary Design & Technology Completion	C Final Design & Fabrication	D System Assembly, Integration & Test, Launch & Checkout	E Operations & Sustainment	F Closeout

- **Information about system needed**
  - Mission length and orbit
  - Parametric failure levels



Today's Example: Total Ionizing Dose Requirement

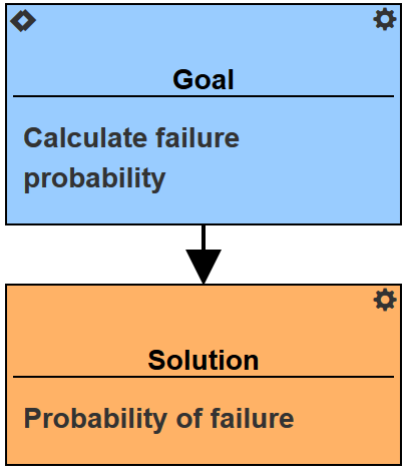
Vanderbilt University School of Engineering

Project Life-Cycle Phases	Pre-A Concept Studies	A Concept & Technology Development	B Preliminary Design & Technology Completion	C Final Design & Fabrication	D System Assembly, Integration & Test, Launch & Checkout	E Operations & Sustainment	F Closeout

Reliability Predicted

- **Requirement: Mission shall meet a reliability level**

- **End of Phase C**
  - Probability calculation
  - Assuming nothing changed about the system from Phase B

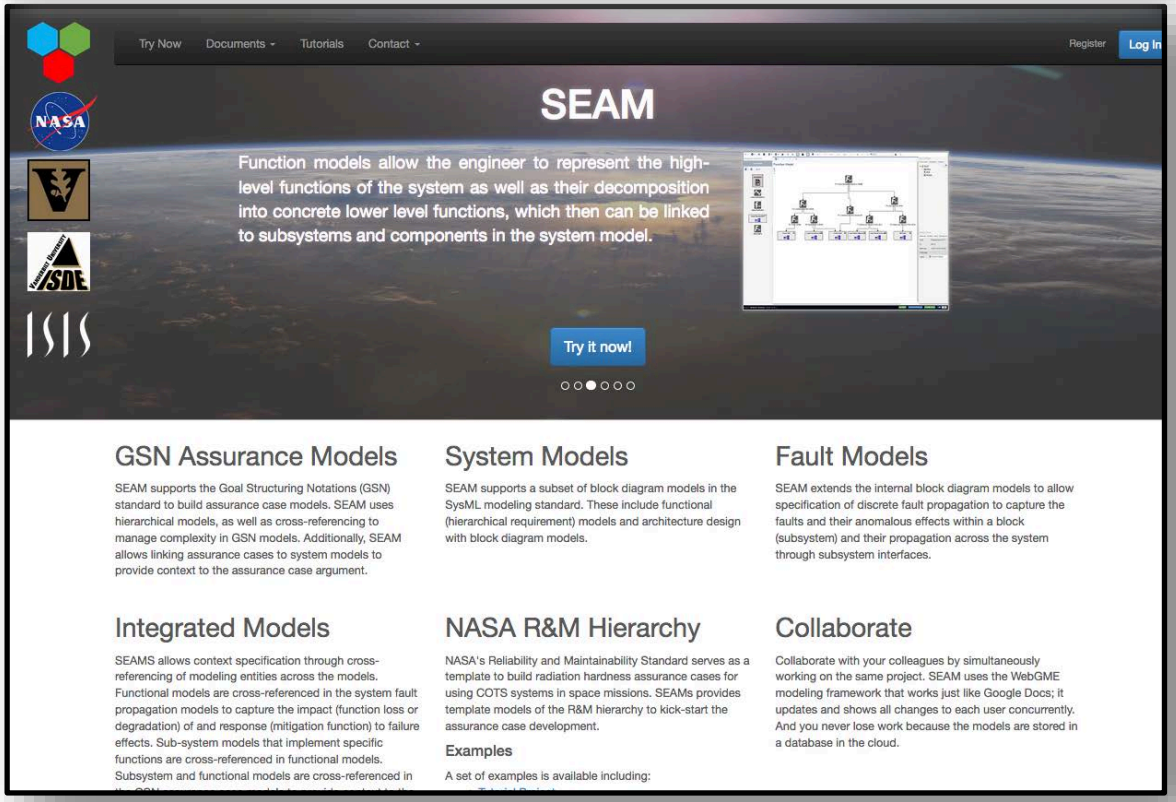


System Engineering and Assurance Modeling (SEAM) Platform

Vanderbilt University School of Engineering

- **Models included**
  - Goal Structuring Notation
  - SysML Block Diagrams with fault propagation models
  - SysML Requirements Diagrams
  - Functional models
- **Import/Export to**
  - Bayes net software tools
  - Fault Tree tools
- **View**
  - CRÈME
  - R-GENTIC

https://modelbasedassurance.org/



Conclusions

- **MBMA is a function of time**
  - Captures the evolution of mission assurance as the system is developed
- **MBMA enables intelligent mission-specific requirements**
  - Illustrates the creation of reliability requirements as more about the mission is known
- **MBMA enables self-documentation of mission assurance**
  - Argument structure show how a requirement is verified and how it is derived
- **MBMA enables concurrent engineering of reliability and design engineering**