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

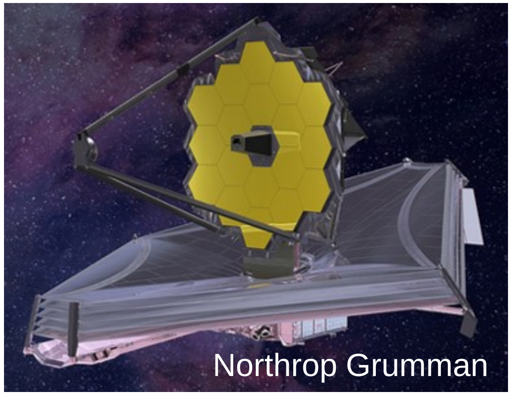
# The Parts Engineer

- **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)


Northrop Grumman

JWST

NASA

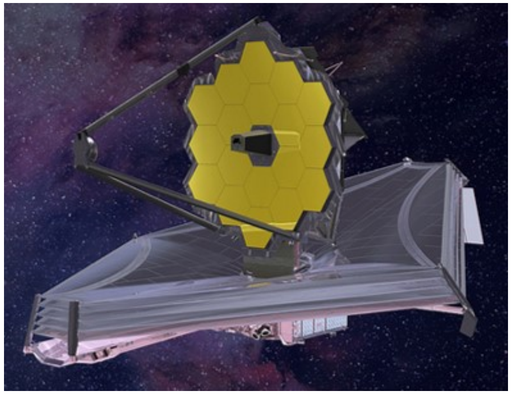
Orion

NASA

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

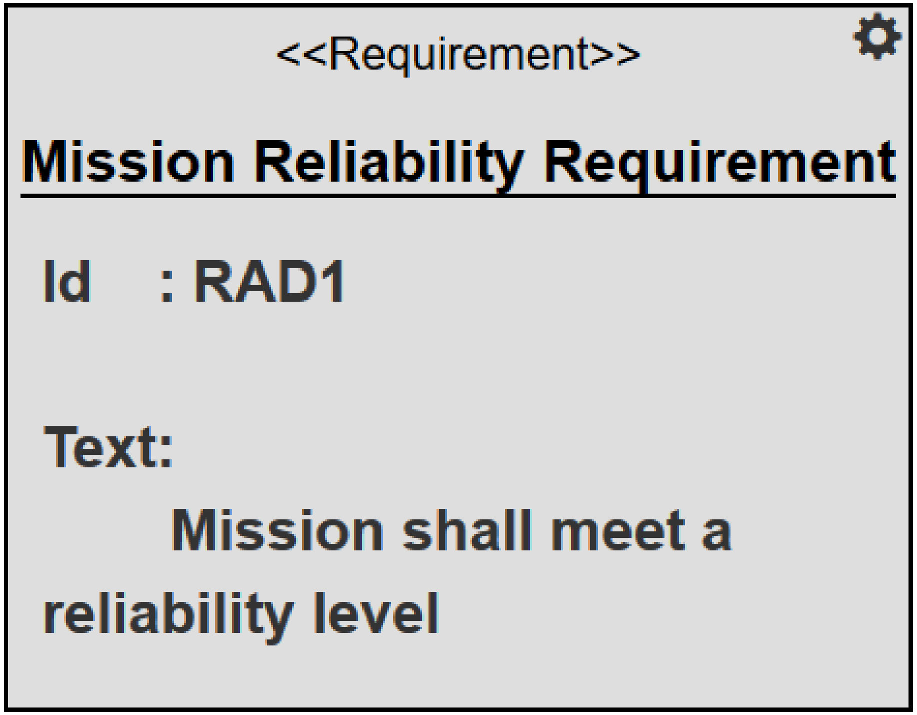
CubeSat Deployment

# 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?**



<<Requirement>>

**Mission Reliability Requirement**

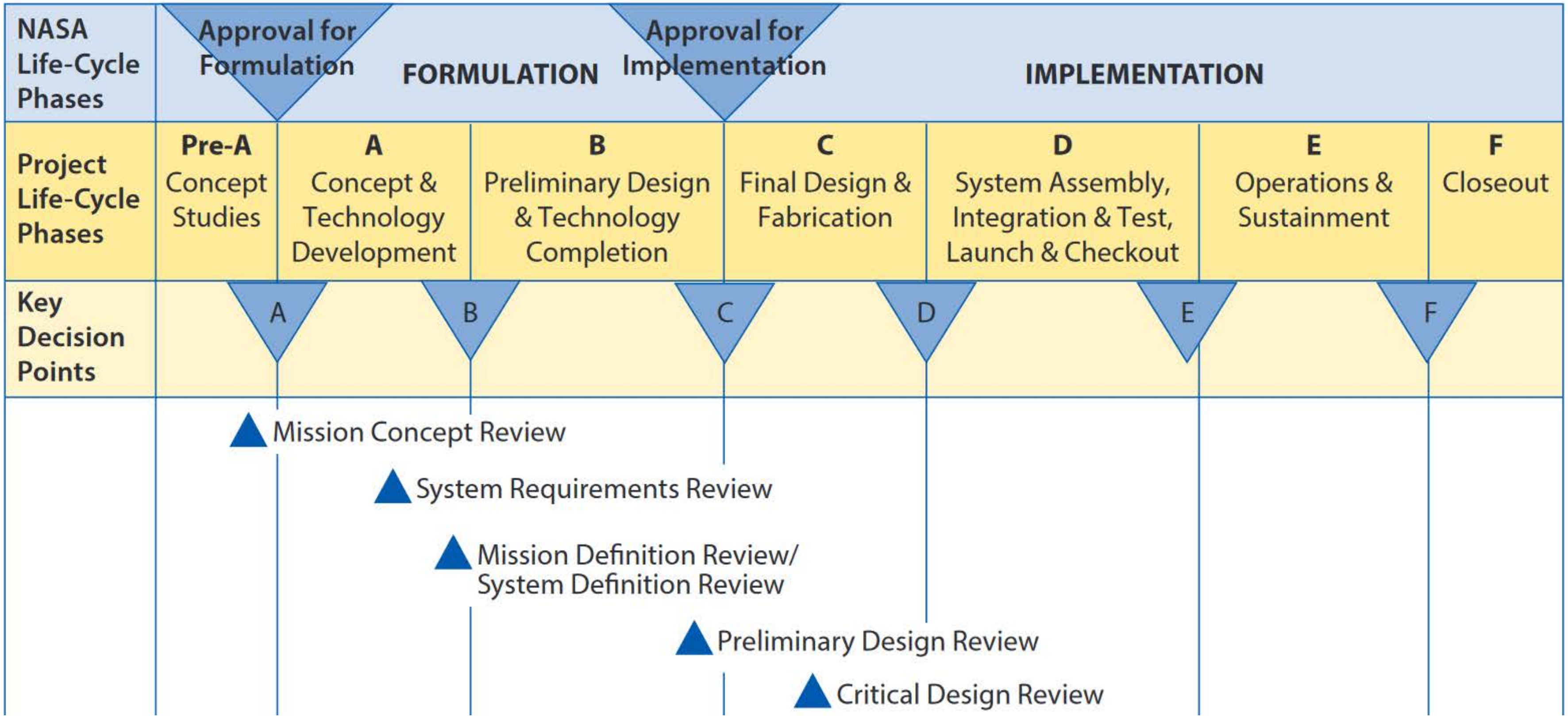
Id : RAD1

Text:

Mission shall meet a reliability level

# 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 Life-Cycle Phases

Approval for Formulation

FORMULATION

Approval for Implementation

IMPLEMENTATION

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

Key Decision Points

A B C D E F

Mission Concept Review

System Requirements Review

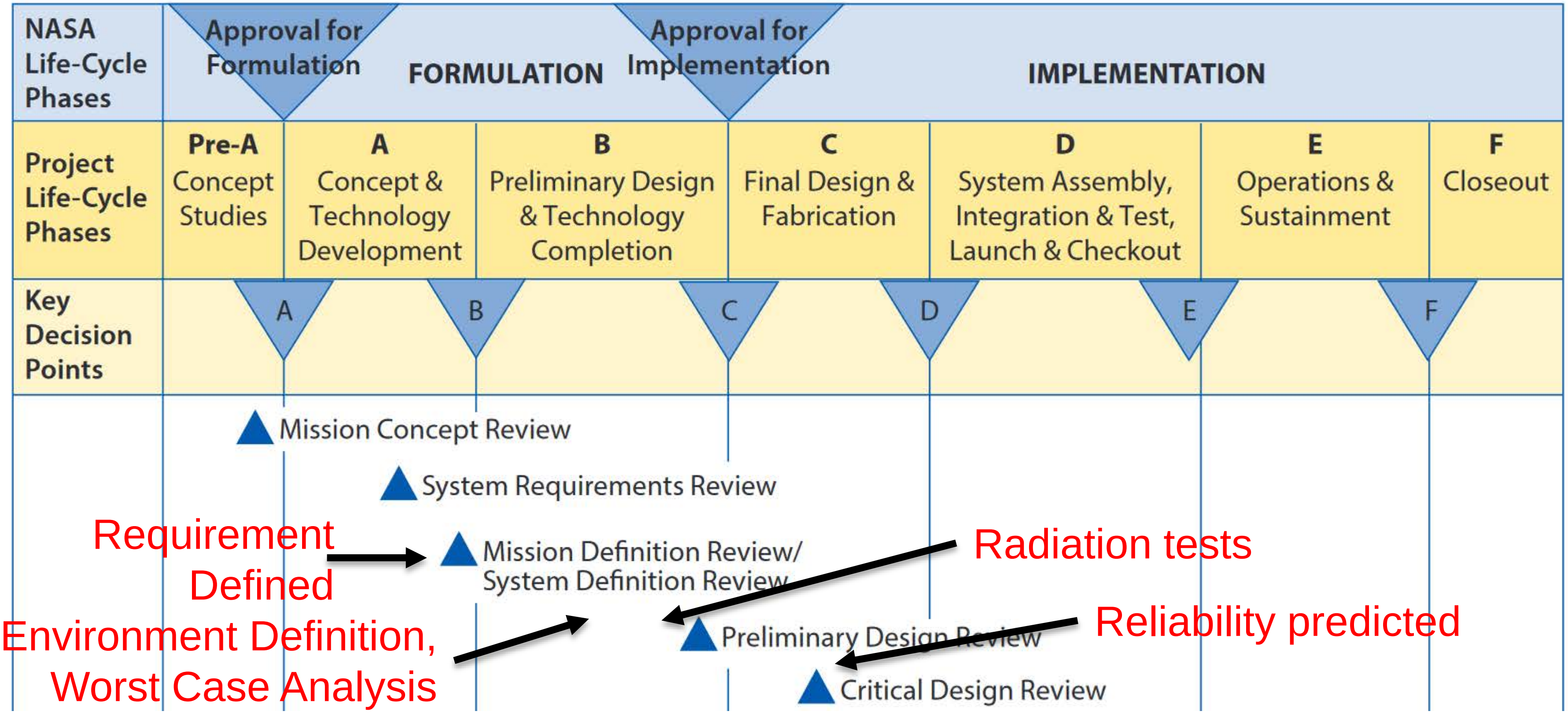
Mission Definition Review/ System Definition Review

Preliminary Design Review

Critical Design Review

# 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 Life-Cycle Phases

Approval for Formulation — FORMULATION — Approval for Implementation — IMPLEMENTATION

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

Key Decision Points: A, B, C, D, E, F

Mission Concept Review

System Requirements Review

Mission Definition Review/ System Definition Review

Preliminary Design Review

Critical Design Review

Requirement Defined

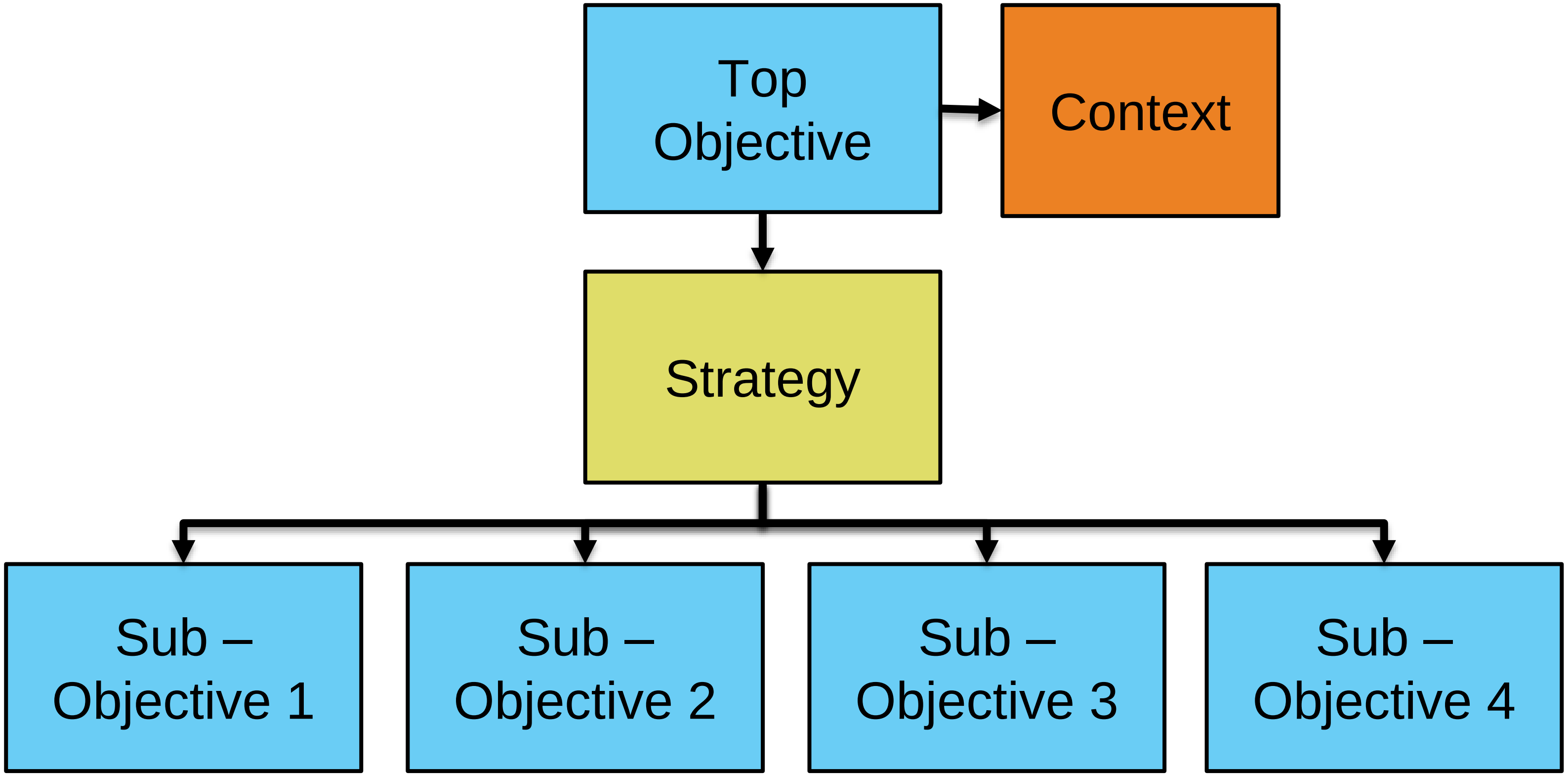
Environment Definition, Worst Case Analysis

Radiation tests

Reliability predicted

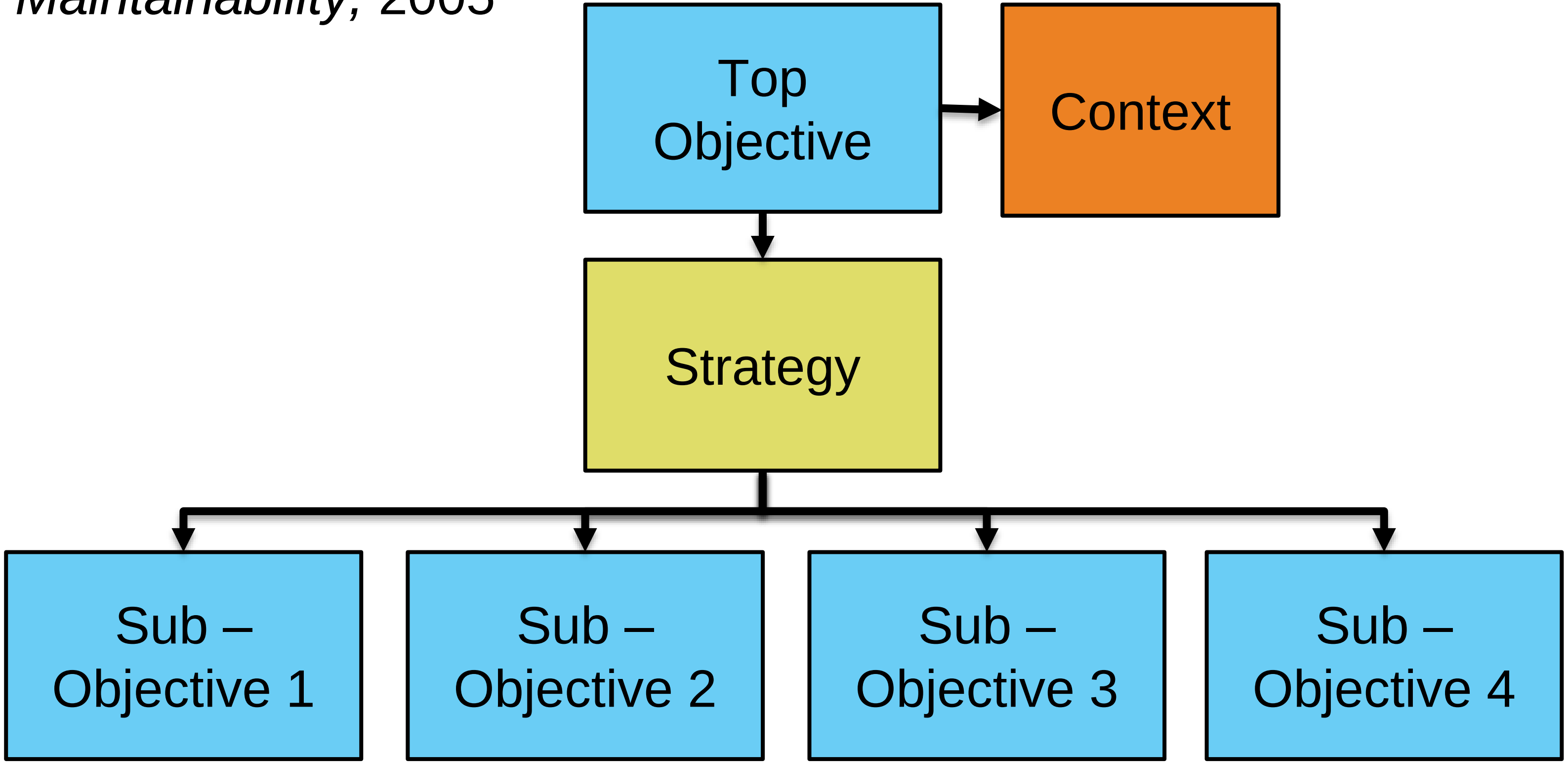
# Foundation: NASA Reliability & Maintainability (R&M) Hierarchy

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

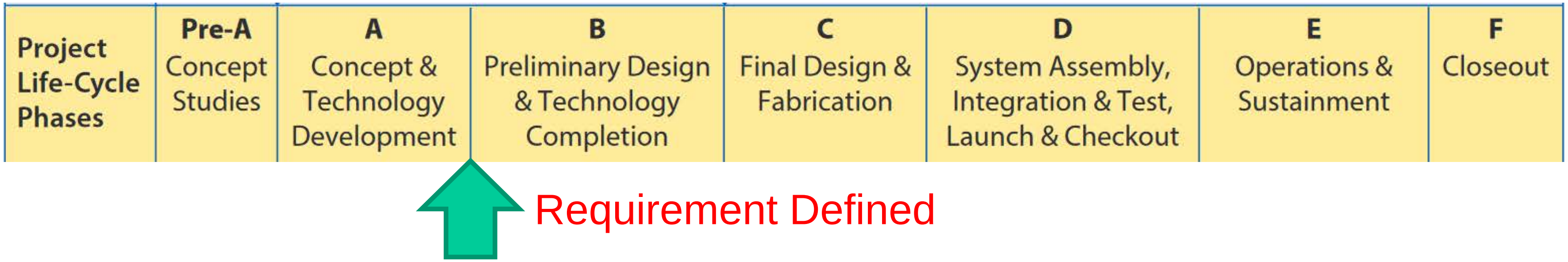


# Foundation: NASA Reliability & Maintainability (R&M) Hierarchy

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



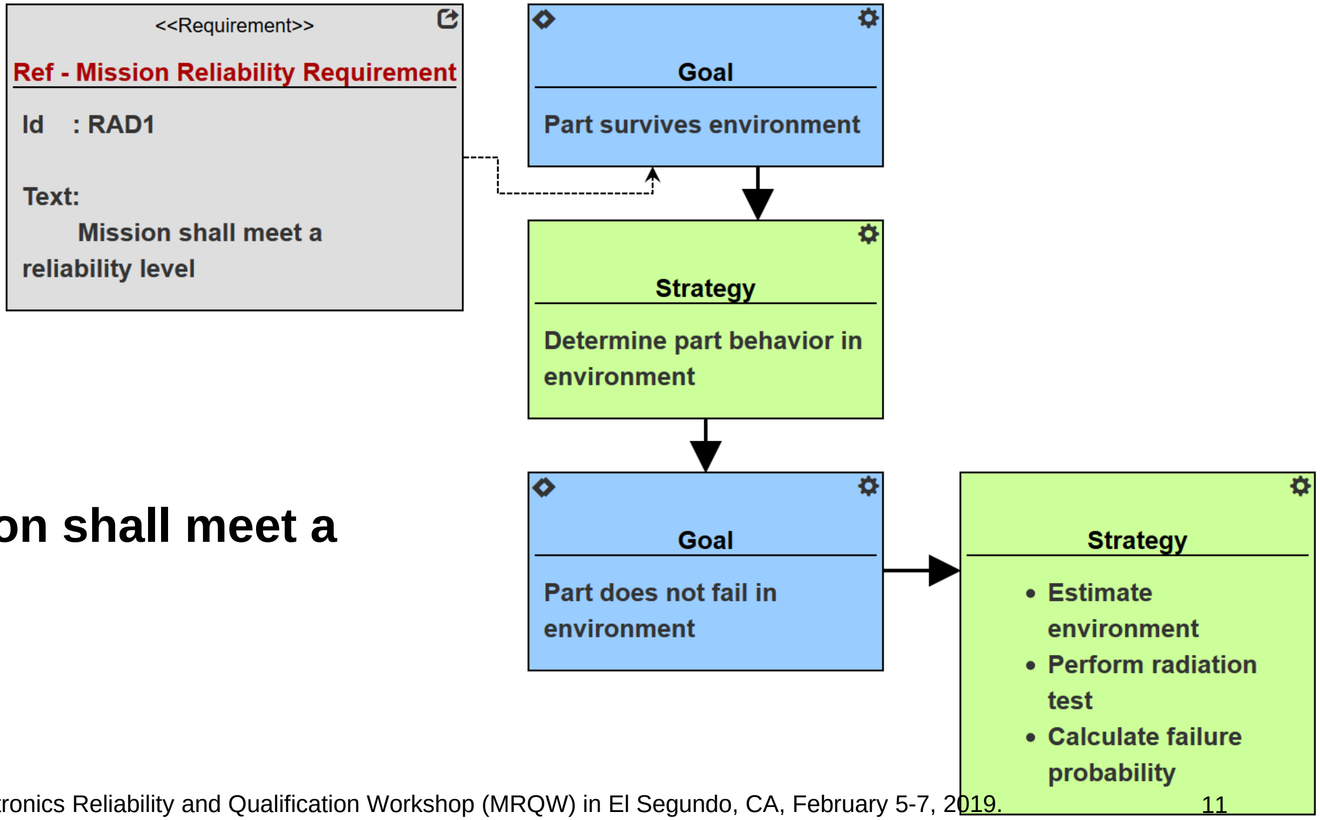
# Today's Example: Total Ionizing Dose Requirement



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

Ref - Mission Reliability Requirement

Id : RAD1

Text:

Mission shall meet a reliability level

Goal

Part survives environment

Strategy

Determine part behavior in environment

Goal

Part does not fail in environment

Strategy

- Estimate environment
- Perform radiation test
- Calculate failure probability

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

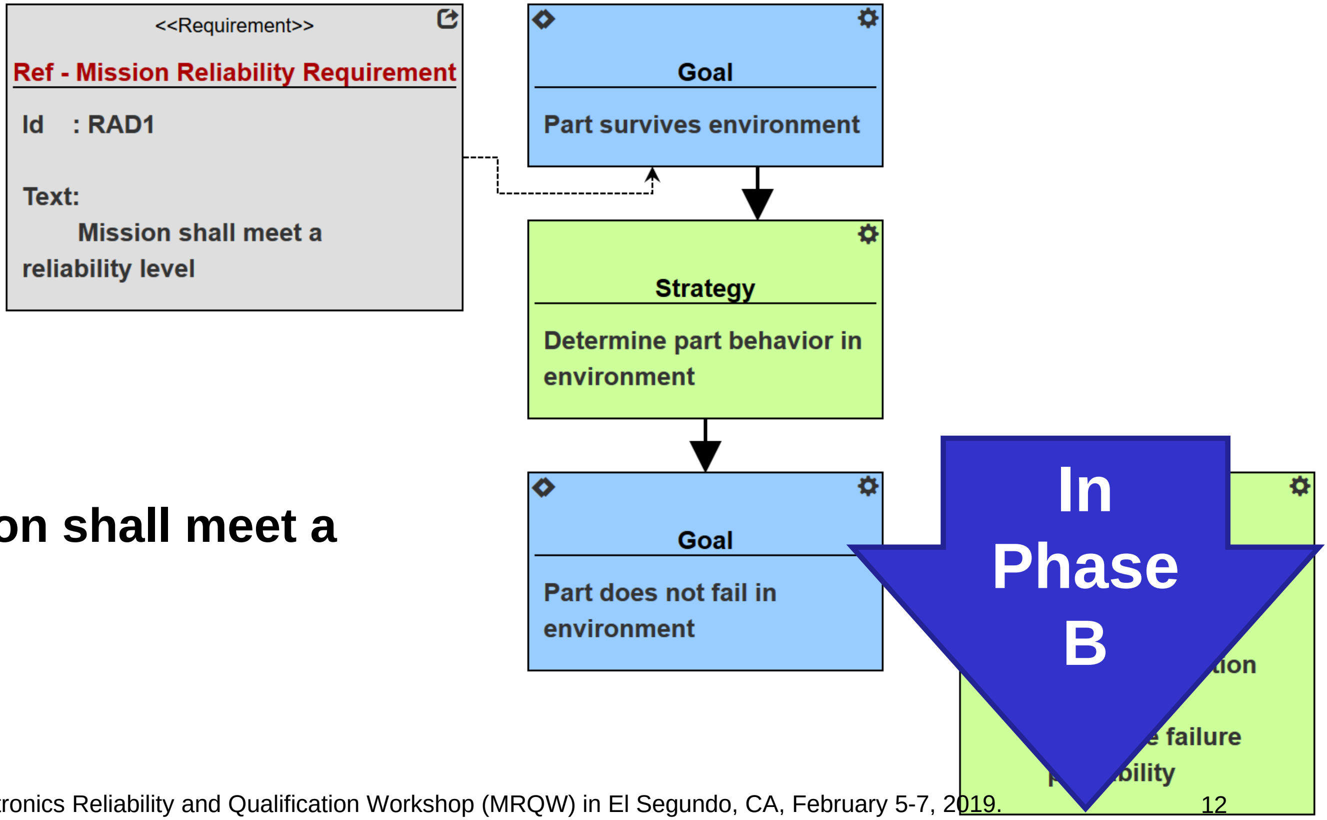
# Today’s Example: Total Ionizing Dose Requirement

*Vanderbilt University School of Engineering*

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

**Ref - Mission Reliability Requirement**

**Id : RAD1**

**Text:**
**Mission shall meet a reliability level**

Goal
Part survives environment
Strategy
Determine part behavior in environment
Goal
Part does not fail in environment
ion
e failure
p bility
In Phase B

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

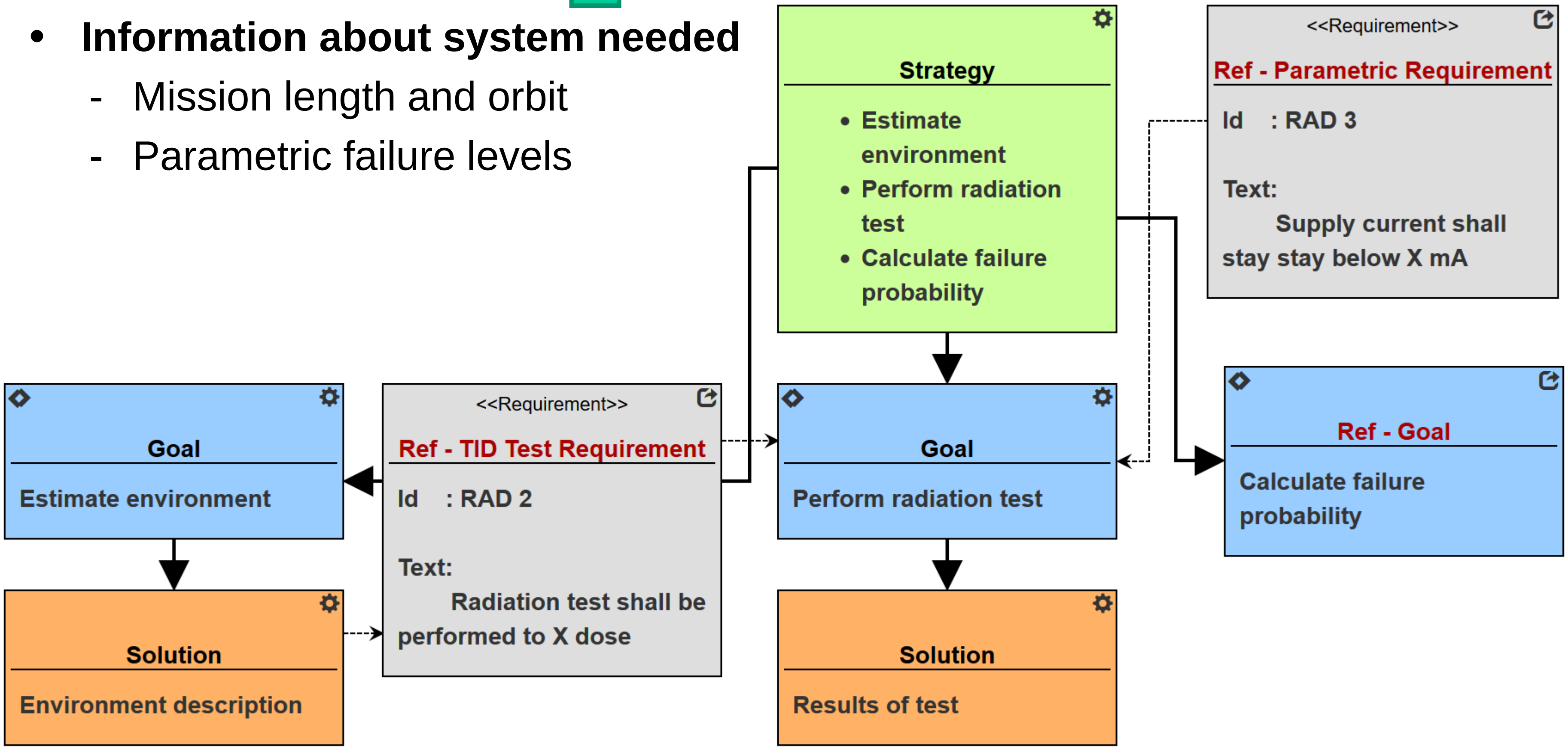
# Today's Example: Total Ionizing Dose Requirement

*Vanderbilt University School of Engineering*

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

Radiation Test Performed

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



**Strategy**

- Estimate environment
- Perform radiation test
- Calculate failure probability

<<Requirement>>

**Ref - Parametric Requirement**

Id : RAD 3

Text: Supply current shall stay stay below X mA

**Goal**

Estimate environment

<<Requirement>>

**Ref - TID Test Requirement**

Id : RAD 2

Text: Radiation test shall be performed to X dose

**Goal**

Perform radiation test

**Ref - Goal**

Calculate failure probability

**Solution**

Environment description

**Solution**

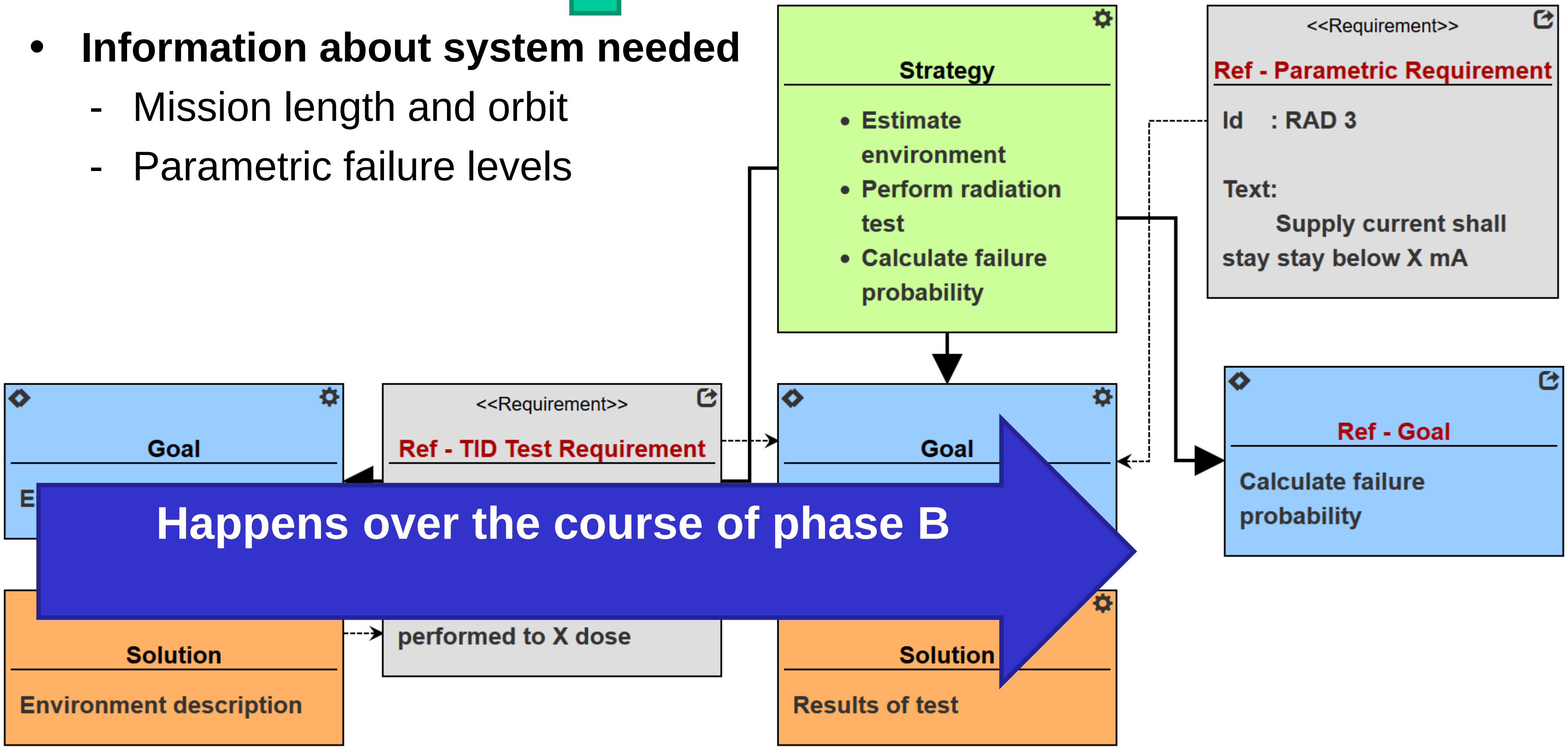
Results of test

# Today’s Example: Total Ionizing Dose Requirement

*Vanderbilt University School of Engineering*

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

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



**Strategy**

- Estimate environment
- Perform radiation test
- Calculate failure probability

<<Requirement>>

**Ref - Parametric Requirement**

**Id : RAD 3**

**Text:**
**Supply current shall stay stay below X mA**

**Goal**

**E**

<<Requirement>>

**Ref - TID Test Requirement**

**performed to X dose**

**Goal**

**Ref - Goal**

**Calculate failure probability**

**Solution**

**Environment description**

**Solution**

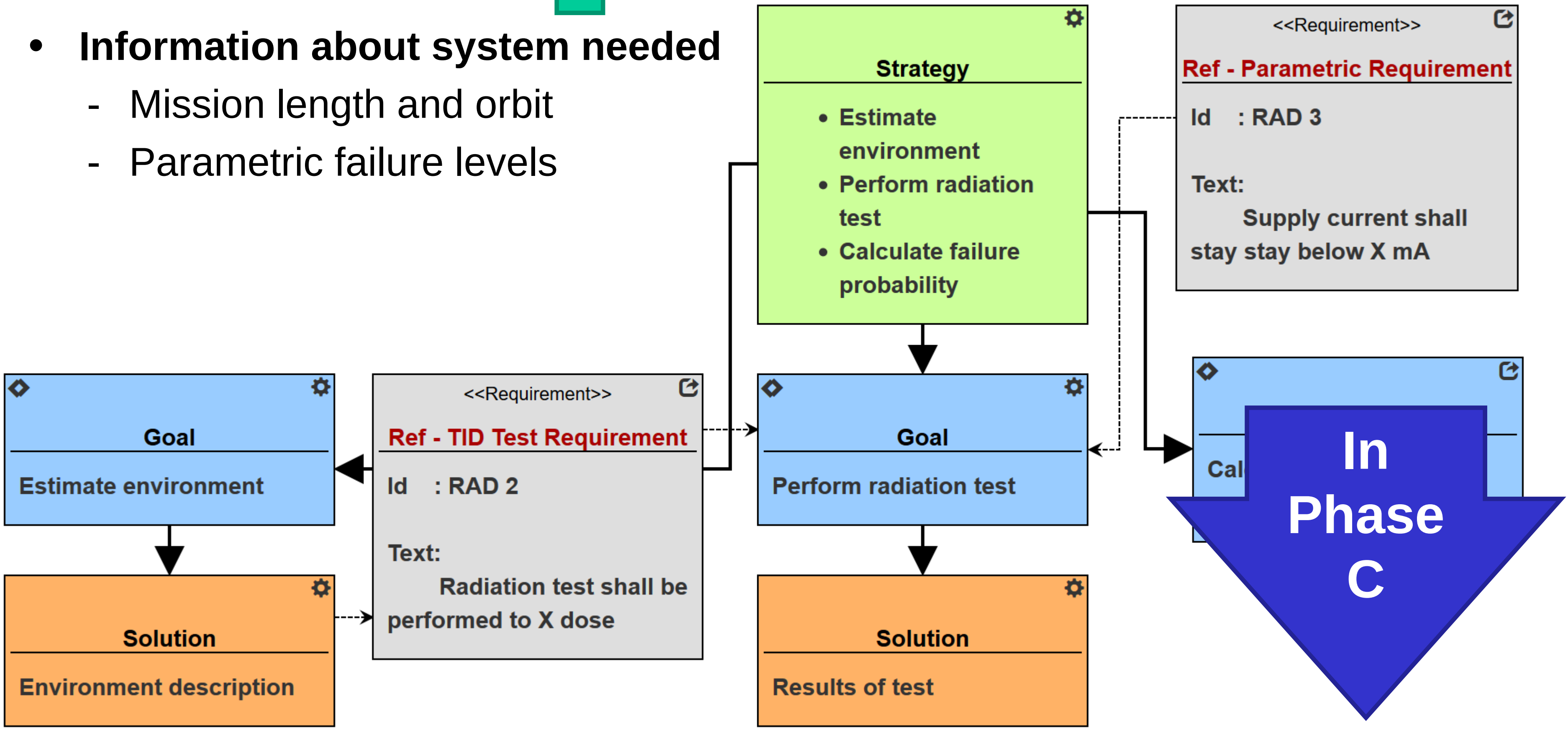
**Results of test**

**Happens over the course of phase B**

# Today’s Example: Total Ionizing Dose Requirement

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

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



**Strategy**

- Estimate environment
- Perform radiation test
- Calculate failure probability

<<Requirement>>

**Ref - Parametric Requirement**

Id : RAD 3

Text:

Supply current shall stay stay below X mA

**Goal**

Estimate environment

<<Requirement>>

**Ref - TID Test Requirement**

Id : RAD 2

Text:

Radiation test shall be performed to X dose

**Goal**

Perform radiation test

**Solution**

Environment description

**Solution**

Results of test

In Phase C

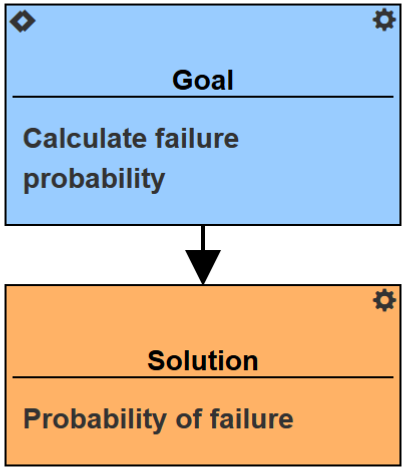
# Today’s Example: Total Ionizing Dose Requirement

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



**Goal**

**Calculate failure probability**

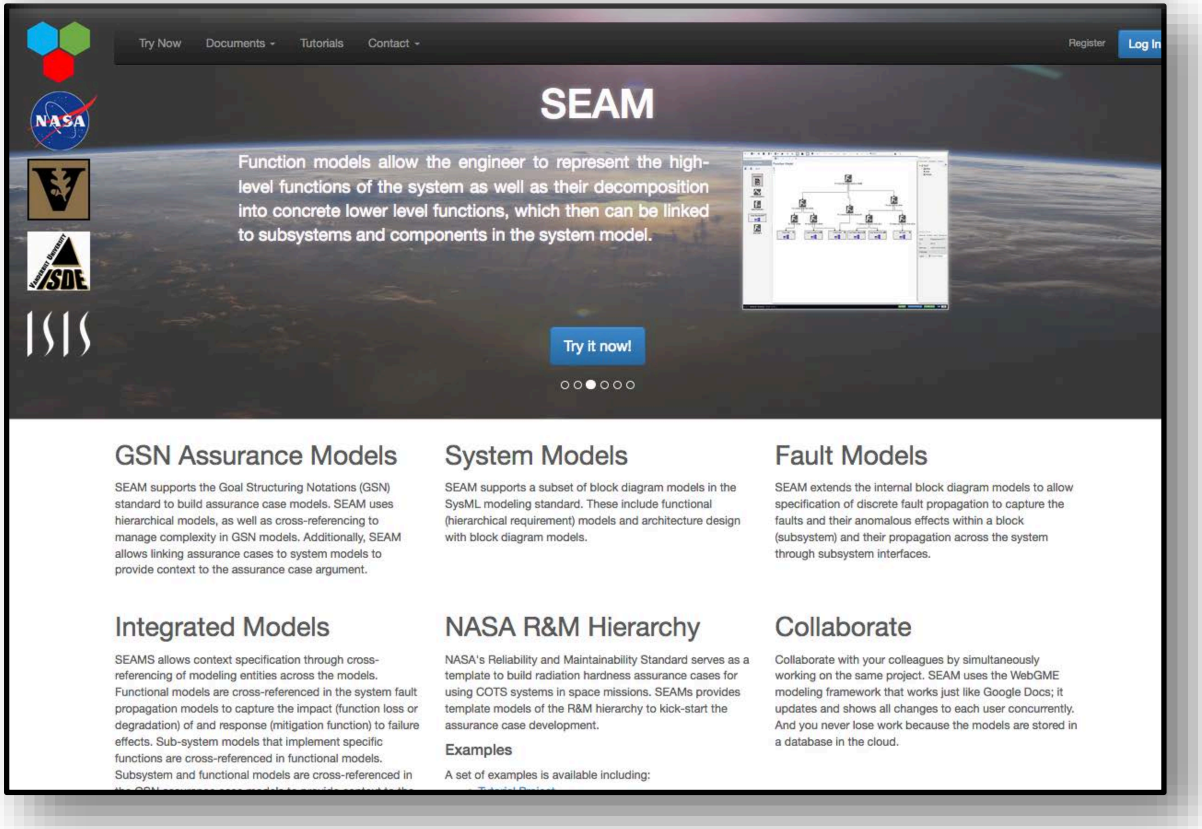
**Solution**

**Probability of failure**

# System Engineering and Assurance Modeling (SEAM) Platform

- **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/



## SEAM

Function models allow the engineer to represent the high-level functions of the system as well as their decomposition into concrete lower level functions, which then can be linked to subsystems and components in the system model.

### 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. Subsystem and functional models are cross-referenced in

### 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

A set of examples is available including:

### 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.

# 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**