Model-Based Assurance Case+ (MBAC+): Tutorial on Modeling Radiation Hardness Assurance Activities

Rebekah Austin¹ⁿ², Ken A. LaBel², Mike J. Sampson², John Evans³, Art Witulski, Brian Sierawski¹, Gabor Karsai¹, Nag Mahadevan¹, Ron Schrimpf¹, Robert Reed¹

1. Vanderbilt University; 2. NASA GSFC, 3. NASA HQ

This work is supported by NEPP and the NASA Reliability and Maintainability Program under Grant and Cooperative Agreement Number NNX16AR25G and NASA/JPL Subcontract Number 1568812

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Abbreviations and Acronyms

AMSAT: Radio Amateur Satellite Corporation
BN: Bayesian Network
COTS: Commercial Off-The-Shelf
ETW: Electronics Technology Workshop
GSN: Goal Structuring Notation
ITAR: International Traffic in Arms Regulations
JPL: Jet Propulsion Laboratory
MBAC+: Model-Based Assurance Case +
MBSE: Model-Based Systems Engineering
NASA: National Aeronautics and Space Administration
NEPP: NASA Electronic Parts and Packaging
R&M: Reliability & Maintainability
RHA: Radiation Hardness Assurance
SEAM: Systems Engineering and Assurance Models
SEFI: Single-Event Functional Interrupt
SEL: Single-Event Latch-up
SEU: Single-Event Upset
SRAM: Static Random Access Memory
SysML: Systems Modeling Language
TID: Total Ionizing Dose
WDI: Watch-dog Input
WDO: Watch-dog Output
WDT: Watch-dog Timer
WebGME: Web-based Generic Modeling Environment

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
NEPP Small Mission History and Workshops

- **FY13**
  - Began discussions at https://nepp.nasa.gov/workshops/etw2013/talks.cfm
  - Held internal NASA meeting: EEE Parts for Class D Missions and CubeSats
    - Joint meeting supported by OSMA and OCE

- **FY14**
  - Discussion at annual workshop and (open) small mission workshop
    - https://nepp.nasa.gov/workshops/etw2014/talks.cfm
    - https://nepp.nasa.gov/workshops/eeesmallmissions/talks.cfm
    - NEPP plans updated based on feedback

- **FY15**
  - https://nepp.nasa.gov/workshops/etw2015/talks.cfm

- **FY16**
  - https://nepp.nasa.gov/workshops/etw2016/talks.cfm

- **FY17 (talks to be posted in the next few weeks)**
  - https://nepp.nasa.gov/workshops/etw2017/
NEPP - Small Mission Efforts

FY18 task area ideas: automotive, avionics, and autonomous vehicles resilience

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Model-Based Systems Engineering (MBSE) for Mission Assurance (MA) - aka MBMA

- Led by NASA/OSMA Reliability and Maintainability (R&M) Program
  - NEPP co-funds efforts that are EEE parts related (tasks listed below)

- Completed tasks (assurance case)
  - Vanderbilt University: Goal structuring notation (GSN) exemplar for single event effects (SEE) in a CubeSat electronics board

- Current tasks
  - Vanderbilt University:
    - Bayesian nets for CubeSat electronics (radiation)
    - On-line sysML/GSN tool for CubeSat electronics
      - TO BE DEMOED on July 18, 2017 at IEEE NSREC conference

- FY18 tasks (proposed)
  - Vanderbilt University:
    - Integrate Bayesian nets with on-line tool and complete assurance case
  - TBD:
    - Exemplar for EEE parts reliability (non-radiation)

A Vision for Model Based Assurance
- John Evans, NASA/OSMA

Note: Mission Assurance Improvement Workshop (MAIW) is developing a MBSE for MA best practices document
Best Practices and Guidelines

- **Current tasks**
  - Radiation hardness assurance (RHA) for Small Missions
    - NASA/GSFC: Michael Campola
  - Board-level proton testing
    - JPL: Steve Guertin
  - Body of knowledge (BOK) on best practices for EEE part reliability via board testing
    - NASA/GSFC (Lentech): Ed Wyrwas

- **Planned tasks**
  - EEE Parts assurance for small missions
    - TBD (overdue)
  - Work with NASA/GSFC and NASA STMD for release of CubeSat tool
    - R-GENTIC (Michael Campola)
      - R – Radiation GuidelinEs for Notional Threat Identification and Classification
    - Plan is to make available via the web (NEPP website) and demo at IEEE NSREC

---

**NEPP Notional EEE Parts Assurance**

- Tailored Risk Acceptance

Note: MAIW is developing a CubeSat Best Practices for Mission Success (Test) document

---

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Non-Mil/Aero EEE Parts

• Automotive grade
  – Began FY15
    • Snapshot of representative part types under evaluation for reliability
  – Began FY16
    • Support of NASA Engineering Safety Center (NESC) automotive grade tests (limited electrical tests and a few radiation tests)
  – Plans
    • Guideline/lessons learned
    • Resilience/soft error rate – challenge in finding a partner
    • Have begun partnership with The Aerospace Corp

• COTS
  – Testing of COTS has been a cornerstone of the NEPP Program including processors, memories, FPGAs, power devices, etc…
    • Multiple on “CubeSat” class electronics - see presentations at weblinks on chart 2.
      – Example: radiation data on TI MSP430 processors
  – Plans
    • Discuss FY18 tasks for “CubeSat” class EEE parts
    • Plastic encapsulated device guideline

• NEPP radiation data can be found at
  – http://nepp.nasa.gov
  – Or via IEEE search
NEPP CubeSat Success and Databases

• Mission Success Analysis (Prof. Michael Swartwout/SLU)
  – NEPP has been funding on-going tracking of CubeSat mission success with newer emphasis on root-cause (improved assurance practices)
    • Note: Prof. Swartwout is teaching a short course session on this topic at IEEE NSREC on July 17, 2017

• CubeSat Databases
  – JPL: two studies (need to update studies or tie into other studies)
    • Kit manufacturer EEE parts approaches
    • What EEE parts NASA (and JPL) are using in CubeSats
  – JPL: Limited evaluation of CubeSat kit electronics boards
  – JPL Action: integrate databases with The Aerospace Corp, SPOON database and with success study (if possible)
    • New: discuss with Ames (Small Spacecraft Virtual Institute)
• Single event effect (SEE) reliability analysis
  – NASA/GSFC (Melanie Berg/AS&D) - Current effort focused on developing model for treating SEE in a manner similar to reliability (i.e., how many 9’s rather than a SEE rate)
  – Planned task is integration with MBMA tools approach

• Working groups
  – NEPP working group meets monthly on “CubeSat databases”
    • The Aerospace Corp and Prof. Swartwout participate
  – Support of MAIW (by invitation meetings with public document release)
“A Working List of Priorities"

- Key thought: What do we need to do to enable “higher reliability” small (cost-effective) missions?
  - NEPP website is expected to go through a major overhaul in the next few months
    - Improved access to “bigger thoughts” (guidelines, best practices)
    - COTS data, and so on
      - Improve “COTS” data sharing
      - Extend COTS testing
      - Extend model-based mission assurance
        - Guidance on “tailoring” of approaches
      - Best practices are OVERDUE for EEE parts
      - What can we learn (or jointly learn) from resilience approaches?

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Model-Based Assurance Case+ (MBAC+): Tutorial on Modeling Radiation Hardness Assurance Activities

Rebekah Austin

This work is supported by NEPP and the NASA Reliability and Maintainability Program under Grant and Cooperative Agreement Number NNX16AR25G and NASA/JPL Subcontract Number 1568812

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Radiation Reliability Assessment of CubeSat SRAM Experiment Board

• Assessment completed on 28nm SRAM SEU experiment

• Reasons for integrated modeling
  - Use commercial off-the-shelf (COTS) parts
  - System mitigation of SEL
  - High risk acceptance

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
At the end of this tutorial you will:

• Understand the reasons for modeling a radiation hardness assurance case for a system

• Understand the basics of graphical argument representation and system modeling with block diagrams and fault propagation

• Have seen a simple example for single-event latch-up (SEL) mitigation on commercial off-the-shelf (COTS) parts

• Know the basics about using modelbasedassurance.org to model assurance cases for radiation reliability
Integrated System Design for Radiation Environments

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Integrated System Design for Radiation Environments

Vanderbilt Engineering

Requirements

System Modeling Language (SysML)

Goal Structuring Notation (GSN)

Design

Bayesian Networks (BN) Model

Reliability

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Integrated System Design for Radiation Environments

- Reasons for Activity interaction
  - Commercial parts (COTS)
  - Document-centric work flow to model-based system engineering
  - System mitigation (for COTS)
  - Shorter schedules for small spacecraft

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Model-Based Assurance Case + (MBAC+)

- **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
What is System Engineering and Assurance Models (SEAM)?

• A set of modeling languages in one environment used to implement MBAC+

• These modeling languages allow for reliability activities and requirements to become part of the Model-Based System Engineering (MBSE) paradigm
  - Move from document-based reliability to objective-based reliability
  - Takes Radiation Hardness Assurance activities from being a process that results in *unlinked and unrelated* documents and integrates those activities into the overall system design process
What is SEAM? Cont.

- SEAM is built using WebGME tool
- Models include:
  - Goal Structuring Notation (GSN)
  - System model (SysML)
  - Fault Propagation
  - Function/Behavior Models
- Allows for links across models
- Links to external documents

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Overall RHA Process

Flight Program RHA Managed via Lead Radiation Engineer

Environment Definition

Project Requirements and Specifications

Design Evaluation

In-Flight Evaluation

External Environment

Environment in the presence of the spacecraft

Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Technology Hardness

Design Margins

Box/system Level

Parts List Screening

Radiation Characterizations, Instrument Calibration, and Performance Predictions

Mitigation Approaches and Design Reliability

Technology Performance

Anomaly Resolution

Lessons Learned

Iteration over project development cycle

Cradle to Grave!

Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014
Overall RHA Process

Flight Program RHA Managed via Lead Radiation Engineer

Context

Environment Definition

External Environment

Environment in the presence of the spacecraft

Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Technology Hardness

Design Margins

Box/system Level

Project Requirements and Specifications

Design Evaluation

Parts List Screening

Radiation Characterizations, Instrument Calibration, and Performance Predictions

Mitigation Approaches and Design Reliability

In-Flight Evaluation

Technology Performance

Anomaly Resolution

Lessons Learned

Iteration over project development cycle

Cradle to Grave!

Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014
Overall RHA Process

Flight Program RHA Managed via Lead Radiation Engineer

Context
- Environment Definition
  - External Environment
    - Environment in the presence of the spacecraft
  - Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Goals
- Project Requirements and Specifications
  - Technology Hardness
  - Design Margins
  - Box/system Level

Design Evaluation

In-Flight Evaluation

Parts List Screening
- Radiation Characterizations, Instrument Calibration, and Performance Predictions
- Mitigation Approaches and Design Reliability

Technology Performance
- Anomaly Resolution
- Lessons Learned

Iteration over project development cycle

Cradle to Grave!

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Overall RHA Process

Flight Program RHA Managed via Lead Radiation Engineer

Context
- Environment Definition
  - External Environment
- Environment in the presence of the spacecraft
- Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Goals
- Project Requirements and Specifications
  - Technology Hardness
  - Design Margins
- Box/system Level

Solutions
- Design Evaluation
  - Parts List Screening
- Radiation Characterizations, Instrument Calibration, and Performance Predictions
- Mitigation Approaches and Design Reliability

In-Flight Evaluation
- Technology Performance
  - Anomaly Resolution
- Lessons Learned

Iteration over project development cycle
Cradle to Grave!

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Overall RHA Process

Flight Program RHA Managed via Lead Radiation Engineer

Context
- Environment Definition
  - External Environment
    - Environment in the presence of the spacecraft
  - Component Mechanical Modeling – 3D ray trace, Monte Carlo, NOVICE, etc.

Goals
- Project Requirements and Specifications
  - Technology Hardness
  - Design Margins
  - Box/system Level

Solutions
- Design Evaluation
  - Parts List Screening
  - Radiation Characterizations, Instrument Calibration, and Performance Predictions

Strategies
- Validation of Modeling
  - Technology Performance
    - Anomaly Resolution
    - Lessons Learned

Kenneth LaBel at the NASA Electronic Parts and Packaging (NEPP) Electronics Technology Workshop (ETW), Greenbelt, MD, June 17-19, 2014

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Foundation: NASA Reliability & Maintainability (R&M) Hierarchy

- Basis of NASA-STD-8729.1 (R&M Standard) that will be released later this year
- Incorporates R&M into MBSE
- Moves to objectives-based reliability requirements
Graphical Assurance Cases

Argument: “A connected series of claims intended to support an overall claim.” [1]

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.” [1]

Goal Structuring Notation (GSN): Visual Representation of an Argument

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Goal Structuring Notation (GSN): Visual Representation of an Argument

Strategy: Reasoning step, nature of argument

Supported by: Inferential or evidential relationships

Solution: Items of evidence. Test reports linked.

Goal: Claims of the argument
Goal Structuring Notation (GSN): Visual Representation of an Argument

**Assumption:**
Needed for goal or strategy to be valid

**Context:**
How the claim or reasoning step should be interpreted. Can be linked to documents or other models.

**Justification:**
Explain why a claim or argument is acceptable

**In Context of:**
Contextual relationships

**M of N options:**
M out of N paths can be completed to prove goal

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Goal Structuring Notation (GSN): Visual Representation of an Argument

Goal: Claims of the argument

Assumption: Needed for goal or strategy to be valid

Strategy: Reasoning step, nature of argument

M of N options: M out of N paths can be completed to prove goal

Supported by: Inferential or evidential relationships

Solution: Items of evidence. Test reports linked.

Justification: Explain why a claim or argument is acceptable

In Context of: Contextual relationships

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
Goal Structuring Notation (GSN): Visual Representation of an Argument

- **Goal**: Claims of the argument
- **Strategy**: Reasoning step, nature of argument
- **Solution**: Items of evidence
- **Context**: How the claim or reasoning step should be interpreted
- **Justification**: Explains why a claim or argument is acceptable
- **Assumption**: Needed for goal or strategy to be valid

**Undeveloped entity symbol**: Indicates the line of reasoning is not complete

**M of N options**: M out of N paths can be complete to prove goal

**Supported by**: Inferential or evidential relationships

**In context of**: Contextual relationships
System Modeling Language (SysML)

- Graphical modeling language that supports specification, analysis, design, verification, and validation of systems
  - Systems include hardware, software, data, personnel, procedures, and facilities
- MBAC+ just uses the Block Diagram modeling standard from SysML at the moment

**Block**: Block name::Library Part

**Port**: Shows power or signal flow
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

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
CubeSat SRAM Experiment Board

SRAM

Logic Translation

Addr, Data, Control

Addr, Data, Control

uController

Power Domain Color Key:

Blue: Spacecraft 3V

Orange: 3V_switch

Green: 3V_uC

Red: SRAM Voltages

Core Regulator

I/O Regulator

Logic Regulator

Load Switch B

Load Switch B

Load Switch B

Quad Flip-Flop

Load Switch A

Load Switch A

WDI

WDO

WDT

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
CubeSat SRAM Experiment Board

Power Domain Color Key:
- **Blue**: Spacecraft 3V
- **Green**: 3V_uC
- **Orange**: 3V_switch
- **Red**: SRAM Voltages

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
1) Determine mission objective and fill in top-level of R&M Template
2) Create functional decomposition of system
MBAC+ Modeling Flow

1) Start

2) Define Goals

3) Create SysML Block Diagram

To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
5) Complete assurance case based on system design and test results
To be presented by Rebekah Austin and Ken LaBel at the 2017 Institute of Electrical and Electronics Engineers (IEEE) Nuclear and Space Radiation Effects Conference (NSREC), New Orleans, Louisiana, July 17-21, 2017.
1) R&M Hierarchy as seed model
2) Use R&M Hierarchy as a template for example radiation reliability assurance case
3) Link SysML blocks to assurance case
4) Show team assignment and group working capabilities
Site Infrastructure

- The contents of the modelbasedassurance.org website have been prepared for the Radiation Effects research community for informational purposes that are not export controlled. Your privacy and security are important to us; please do not upload any data that is controlled unclassified information, export controlled, or considered to be intellectual property.

- You can make your own site (internal server, amazon gov cloud, etc.) if you want to include Export/ITAR material. Contact us.