A Vision for Spaceflight Reliability: NASA’s Objectives Based Strategy

Frank Groen, John Evans – NASA OSMA
Tony Hall – ISL

Presented at RAMS 2015
NASA Challenges

Small Sats

Commercial Crew

Mars

Europa and Beyond
Our products may need to be different in a model-based environment.

NASA OCE direction will enable model-centric capability.

Decisions should not be made without our insight and oversight.

Safety Requirements and Quality Demands

Reliability Models

FMEA Hazard Analysis
Mission Assurance Challenges

- NASA’s Mission Assurance faces challenges
  - Changing missions
  - Changing acquisition models
  - Changing engineering practices
  - Changing technology

- We must reconsider our practices to stay relevant
  - Don’t necessarily hang on to ‘proven’ practices
  - Consider the intent behind R&M methods and techniques
“Subset of Considerations”

- Focus on the *what*:
  - Emphasize R&M objectives and related strategies
  - Leave choice of methods and techniques to implementing organizations
  - Allow for innovation and adaptation to new engineering practices
Decomposition of R&M Objectives

R&M Objectives Structure – Top-Level

Top Objective: system performs as required over the lifecycle to satisfy mission objectives

Strategy: prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives

Objective: system conforms to design intent and performs as planned (1)
Objective: system remains functional for intended lifetime, environment, operating conditions and usage (2)
Objective: system is tolerant to faults, failures and other anomalous internal and external events (3)
Objective: system is designed to have an acceptable level of availability and maintenance demands (4)

Context: Expectations derived from crew safety, MMOD concerns, facility safety, public safety, mission obj., sustainment, ..., considerations and associated risk tolerance
Context: System/function description and requirements, including design information and interfaces
Context: Reference mission + before/after
Context: Range of nominal / off-nominal usage and conditions/environments

sma.nasa.gov
Objective: System remains functional for intended lifetime, environment, operating conditions and usage (2)

Strategy: Understand failure mechanisms, eliminate and/or control failure causes, degradation and common cause failures, and limit failure propagation to reduce likelihood of failure to an acceptable level (2.A)

Objective: System and its components meet quantifiable reliability criteria (2.B.1)

Strategy: Determine reliability allocation (2.B.1.A)

Objective: System or its elements are designed to withstand nominal and extreme loads and stresses (radiation, temperature, pressure, mechanical, ...) for the life of the mission (2.A.1)

Strategy: Apply design standards to incorporate margin to account for variable and unknown stresses (2.A.1.A)

Strategy: Evaluate and control nominal stresses and related failure causes (2.A.1.B)

Strategy: Evaluate and control potential for extreme stresses and related failure causes (2.A.1.C)

Strategy: Perform qualification testing and life demonstration to verify design for intended use (2.A.1.D)

Strategy: Evaluate and control coupling factors and shared causes between redundant (or dependent) components (2.A.2.A)

Objective: System remains functional for intended lifetime, environment, operating conditions and usage (2)

Strategy: Assess quantitative reliability measures and recommend or support changes to system design and/or operations (2.B)

Objective: System or its elements are not susceptible to common-cause failures (2.A.2)

Strategy: Evaluate and control nominal stresses and related failure causes (2.A.1.B)

Strategy: Evaluate and control potential for extreme stresses and related failure causes (2.A.1.C)

Strategy: Support design trades based on reliability analysis (2.B.1.C)

Strategy: Plan and perform life testing (2.B.1.D)

Strategy: Track and monitor reliability performance over time (2.B.1.E)

Context: Description of operating environment, including static, cyclical, and randomly varying loads

Objective: System and its elements are designed to withstand nominal and extreme loads and stresses (radiation, temperature, pressure, mechanical, ...) for the life of the mission (2.A.1)

Strategy: Apply design standards to incorporate margin to account for variable and unknown stresses (2.A.1.A)

Strategy: Evaluate and control nominal stresses and related failure causes (2.A.1.B)

Strategy: Evaluate and control potential for extreme stresses and related failure causes (2.A.1.C)

Strategy: Perform qualification testing and life demonstration to verify design for intended use (2.A.1.D)
Laying the Foundation

- Logically decompose top-level R&M objective
  - Use elements of the Goal Structuring Notation
  - Structure shows why strategies are to be applied

- Structure forms basis for a proposed R&M standard
  - Specifies the technical considerations to be addressed by projects
  - Forms basis for evaluation of plans, design, and assurance products
Summary

- Changes in missions, acquisition/engineering practices, and technology challenge proven R&M practices

- Define R&M objectives and strategies to enable adaptation and innovation

- Logically decompose the top-level R&M objective to identify the elements of an R&M argument
Final Thoughts

• MBSE is not the rationale for the proposed approach, but is considered to help devise R&M tools and methods within MBSE contexts.

• Community will have to work towards open standards for documenting R&M arguments and evidence
  – As part of broader assurance framework
  – Enable infrastructure of MBSE-compatible R&M tools