Model Based Mission Assurance: Emerging Opportunities for Robotic Systems

Tony DiVenti, Branch Head – Reliability and Risk Analysis (371), NASA Goddard Space Flight Center
John W. Evans, Office of Safety and Mission Assurance, NASA HQ

The emergence of Model Based Systems Engineering (MBSE) in a Model Based Engineering framework has created new opportunities to improve effectiveness and efficiencies across the assurance functions. The MBSE environment supports not only system architecture development, but provides for support of Systems Safety, Reliability and Risk Analysis concurrently in the same framework. Linking to detailed design will further improve assurance capabilities to support failures avoidance and mitigation in flight systems. This also is leading new assurance functions including model assurance and management of uncertainty in the modeling environment. Further, the assurance cases, a structured hierarchal argument or model, are emerging as a basis for supporting a comprehensive viewpoint in which to support Model Based Mission Assurance (MBMA).
Model Based Mission Assurance

Tony DiVenti, Branch Head – Reliability and Risk Analysis (Code 371), Goddard Space Flight Center

John W. Evans, Office of Safety and Mission Assurance, NASA HQ
MBSE – How does SMA fit in

Assurance products modified to fit into a model based environment

Facilitates and strengthens SMA’s Insight, Oversight, Risk Assessment capabilities, and Technical Authority role

Safety Requirements and Quality Demands

FMEA & Hazard Analysis

Reliability Models
MBMA – Model Based Mission Assurance

[Diagram showing the process of MBMA with various steps like evidence build, assurance analyses, system models, and assurance objectives.]
Example - MBSE FMEA

Courtesy Lui Wang
Johnson Space Center

Magic Draw Plug-Ins

FMECA Output

SysML Models

Failure Modes and Effects Criticality Analysis

<table>
<thead>
<tr>
<th>System</th>
<th>Subsystem</th>
<th>LRU/Assembly Type</th>
<th>LRU/Assembly Name</th>
<th>Item Function</th>
<th>Potential Failure Mode</th>
<th>Immediate Failure Effect</th>
<th>End Effect</th>
<th>Number of Independent Failures</th>
<th>Other Independent Failures</th>
<th>CRIT LEVEL</th>
<th>SEV</th>
<th>Potential Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FanCan</td>
<td>ECLSS</td>
<td>CCAA</td>
<td>CCAA1</td>
<td>CCAA1 Circulates Air</td>
<td>Failed Off</td>
<td>Loss of CCAA1 air Circulation</td>
<td>Loss of CCAA1 air Circulation</td>
<td>1</td>
<td>Internal Malfunction</td>
<td>1</td>
<td>Internal Malfunction</td>
<td></td>
</tr>
<tr>
<td>FanCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU1</td>
<td>MBSU1_<strong>Power</strong></td>
<td>Failed Off</td>
<td>Loss of MBSU1 output_power</td>
<td>Loss of MBSU1 output_power</td>
<td>2</td>
<td>MBSU1 Failed Off</td>
<td>1</td>
<td>Insert MBSU1 Malfunction</td>
<td></td>
</tr>
<tr>
<td>FanCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU1</td>
<td>MBSU1_<strong>Power</strong></td>
<td>Failed Off</td>
<td>Loss of MBSU1 output_power</td>
<td>Loss of CCAA1 air Circulation</td>
<td>1</td>
<td>Insert MBSU1 Malfunction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FanCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU2</td>
<td>MBSU2_<strong>Power</strong></td>
<td>Failed Off</td>
<td>Loss of MBSU2 output_power</td>
<td>Loss of MBSU2 output_power</td>
<td>2</td>
<td>MBSU2 Failed Off</td>
<td>1</td>
<td>Insert MBSU2 Malfunction</td>
<td></td>
</tr>
<tr>
<td>FanCan</td>
<td>Power Subsystem</td>
<td>MBSU</td>
<td>MBSU2</td>
<td>MBSU2_<strong>Power</strong></td>
<td>Failed Off</td>
<td>Loss of MBSU2 output_power</td>
<td>Loss of MBSU2 output_power</td>
<td>2</td>
<td>MBSU2 Failed Off</td>
<td>1</td>
<td>Insert MBSU2 Malfunction</td>
<td></td>
</tr>
<tr>
<td>FanCan</td>
<td>Power Subsystem</td>
<td>PDU</td>
<td>PDU1</td>
<td>PDU_<strong>Power</strong></td>
<td>Failed Off</td>
<td>Loss of PDU output_power</td>
<td>Loss of CCAA1 air Circulation</td>
<td>1</td>
<td>Insert PDU Malfunction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FanCan</td>
<td>Power Subsystem</td>
<td>PDU</td>
<td>PDU1</td>
<td>PDU_<strong>Power</strong></td>
<td>Failed Off</td>
<td>Loss of PDU output_power</td>
<td>Loss of CCAA1 air Circulation</td>
<td>1</td>
<td>Insert PDU Malfunction</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CRIT LEVEL: Criticality Level
SEV: Severity
Potential Causes: Detailed causes and effects of the failure modes.
Example - CDS System Fault Tree

Courtesty Lui Wang
Johnson Space Center

sma.nasa.gov
Future Example - Physics of Failure Model Integration

FY16 Planned Collaboration – UMD Center for Advanced Life Cycle Engineering (CALCE)

Simulation Assisted Reliability Assessment (SARA®) Software

- GSFC has access to CALCE SARA® software to perform in depth parts reliability analysis
- A system model that links to SARA® could produce more accurate reliability analyses
- MBSE provides a framework to support this activity
Objectives Based Assurance

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
   Context: Expectations derived from crew safety, MMOD concerns, facility safety, public safety, mission obj., sustainment, ..., considerations and associated risk tolerance

Objective: system remains functional for intended lifetime, environment, operating conditions and usage
   Context: System/function description and requirements, including design information and interfaces

Objective: system is tolerant to faults, failures and other anomalous internal and external events
   Context: Reference mission + before/after

Objective: system is designed to have an acceptable level of availability and maintenance demands
   Context: Range of nominal / off-nominal usage and conditions/ environments
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

- MBSE provides an unprecedented opportunity to integrate SMA and Engineering Analysis concurrently as part of a common modeling framework.
- MBMA, part of the MBSE environment, facilitates and enhances SMA’s analytical and risk assessment capabilities.
- MBSE and MBMA fully supports GSFC’s Risk Based SMA Approach and the Agency’s R&M Objectives Structure and as part of a larger Safety/Assurance Case.