MODEL BASED MISSION ASSURANCE (MBMA)

Dr. Fayssal M. Safie/APT-Research
Dr. John Evans/OSMA, NASA HQ

Model Based Systems Engineering
& Software System Safety Workshop
May 2-3, 2017
AGENDA

- Objective
- Definitions
- Why Model Based Systems Engineering (MBSE)
- Model Based Mission Assurance (MBMA)
- MBMA Case Studies
- Summary and conclusions
- References
OBJECTIVE

This presentation is intended to discuss the MBMA concept in a MBSE environment. It addresses what safety and mission assurance organizations need to do to participate and integrate in the MBSE environment (i.e. new skills, new role, training, etc...). Examples are also discussed.

Note: It is important to acknowledge the significant contribution of Dr. John Evans of NASA/OSMA his contribution to the MBMA material used in this presentation.
Definitions

Systems Engineering

- **A system** is an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

- **Systems Engineering** is an engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and stakeholder's needs are satisfied in a high quality, trustworthy, cost efficient and schedule compliant manner throughout a system's entire life cycle.
Definitions

What Is Model Based Systems Engineering (MBSE)?

- MBSE (Model Based Systems Engineering) – A formalized application of modeling to support system requirements, design, analysis, technical management, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases.

- More Specifically, MBSE is an environment that can be characterized as the collection of related processes, methods, and tools used to support the discipline of systems engineering in a “model-based” or “model-driven” context.

- MBSE is part of a long-term trend toward model-centric approaches. In particular, MBSE is expected to replace the document-centric approach that has been practiced by systems engineers in the past.
Why MBSE?

MBSE Anticipated Major Benefits

- Information consistency: reduced overhead, increased confidence
- No “where’s the latest” confusion
- Propagation of changes
- Changes tracked and versioned
- Ease of communicating and maintaining current project baseline
- Cross-training/experience for earlier-career engineers
- Enhanced stakeholder communication to enable better elicitation and validation
- Enhanced visibility into information gaps and system design integrity
- Rigorous traceability from need through solution
- Reduction in the number of requirements
- Early/on-going requirements validation and design verification
Model Based Mission Assurance

Typical Project Systems Engineering Organization

- Project Manager
  - Technical Team Review
  - Project Chief-Engineer
    - Chief System Engineer
      - Requirements Analysis
      - System Design
      - System Effectiveness
      - System Test Planning
      - System Management

- Requirements Analysis
  - Mission Analysis
  - Functional Analysis
  - Requirements Flow Down
  - Operational Scenario
  - Selection Criteria
  - Sensitivity Analysis
  - Type A Specifications
  - Operational Concept Documentation
  - Simulations
  - Trade Studies
  - Risk Analysis
  - TPM

- System Design
  - Candidate Concepts
  - System Synthesis
  - Subsystem Synthesis
  - Type B Specifications
  - Interface Control Document
  - Block Diagrams
  - Software requirements Specifications
  - Interface requirements Specifications
  - Software Configuration Mgmt. Plan
  - Software Quality Evaluation Plan
  - SW Standards & Procedures Manual
  - Subcontractor Specifications
  - Purchased Item Specifications

- System Effectiveness
  - Reliability
  - Safety
  - Logistics
  - Maintainability
  - Human Factors
  - Producibility Studies
  - LCC Estimate

- System Test Planning
  - System Test Plan
  - Performance Verification

- System Management
  - SEMP
  - WBS
  - Schedules
  - Design Reviews
  - Risk Management
  - Configuration Control
  - S/C Reviews

Managing the Systems engineering Process, CMS
Systems Modeling Language (SYSML)- ABS Example

Decisions should not be made without assurance insight and oversight.

1. Structure

- SysML, being one of the key MBSE components, has a good foundation for capturing requirements, architecture, constraints, views and viewpoints.
- It allows linking different types of models that come from different engineering disciplines.

2. Behavior

- FMEA Hazard Analysis
- activity/function

3. Requirements

- Safety Requirements and Quality Demands

3. Requirements

- Model Based Mission Assurance (MBMA) - NSC Briefing March 21, 2016, Dr. John Evans, NASA, OSMA

4. Parametrics

- Reliability Models

4. Parametrics

- Used with permission of OMG
Assurance organizations may need to define new roles, develop new skills, and train on new tools to engage in the Model Based Systems Engineering environment.
Mission Assurance products may need to be different in a model based environment (Objective Driven standards and requirement...)

Model Based Mission Assurance (MBMA) - NSC Briefing March 21, 2016, Dr. John Evans, NASA, OSMA
“...NASA OSMA has developed an approach...to provide for flexibility ... while focusing on a vision that is rooted in technical objectives rather than specifying specific products and processes. This approach uses the development of objectives hierarchies with supporting strategies for implementation. The results promise the potential of improved effectiveness, flexibility, and compatibility with Model Based Systems Engineering (MBSE)...”

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

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

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)

https://sma.nasa.gov/docs/default-source/News-Documents/r-amp-m-hierarchy.pdf?sfvrsn=4
R&M Objectives Hierarchy (Continued)

SUB – OBJ. 2

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

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

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)

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

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

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)

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

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

https://sma.nasa.gov/docs/default-source/News-Documents/r-amp-m-hierarchy.pdf?sfvrsn=4
Tying Design, Reliability & Safety Analyses

Linking designs to reliability analysis, reliability analysis to safety analysis, and safety analysis to designs

1. Integrating Safety and Reliability Analysis into MBSE Toolkit
   https://www.youtube.com/watch?v=NwuTV5-HAws
Safety and Reliability analyses are an integral part of a program Design Analysis Cycles (DAC):

- Launch System Architecture Assessments
- Requirements evaluation and refinement
- Assessment of progress toward program Goals
The ARES V launch vehicle is actually two vehicles in one since it serves both an ascent, or Earth launch function, and a trans-lunar injection (TLI), or Earth orbit departure function.
MBMA Case Studies - THE ARES V CASE
The ARES V Vehicle Concept Assessment Methodology
MBMA Case Studies - THE ARES V CASE

The ARES V Vehicle Concept Assessment Methodology

Initial Vehicle Sizing

- INTROS (MERS)

Structural Sizing

- LVA

Build and Assess Load Cases

- LVA

Structural Analysis

- LVA

Displacement & Internal Forces

- LVA

Material Property Database

Sizing Code

- LVA

Updated Structural Weights

- LVA

Cost Analysis

- NAFCOM

Reliability Analysis

- SPREAD

Propulsion Database

Aerodynamic Database

APAS/Wind Tunnel Data

Trajectory/Performance Analysis

- POST

Closed Vehicle Concept

Iterate As Necessary
MBMA Case Studies - THE ARES V CASE
The ARES V Reliability Model Structure

Reliability Model Structure Schematic
MBMA Case Studies - THE ARES V CASE
The ARES V Reliability Methodology

**Mission Profile**

<table>
<thead>
<tr>
<th>Event</th>
<th>Time (sec)</th>
<th>Alt (km)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liftoff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Q</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRB Separation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shroud Separation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Engine Cutoff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDS Ignition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDS Engine Cutoff</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Vehicle Configuration**

**Subsystem Parameters**

The Process

Ares V Subsystem Data

Reliability Database

Reliability Algorithms

Mission Performance Data

System Analysis Integration

Reliability Evaluation Results

Advanced Concepts
Office Design
Input
MBMA Case Studies - THE ARES V CASE
Within Concept Trade - Earth Departure Stage (EDS)

Performance-based reliability analysis provided supporting data in key architecture, element, subsystem, and component design decisions.

Earth Departure Stage

Solar Array to Fuel Cells
**MBMA Case Studies - THE ARES V CASE**  
**Reliability & Safety Predictions**

### Reliability and Safety Analyses Output

<table>
<thead>
<tr>
<th></th>
<th>Mean Failure Probability</th>
<th>MFBF (1 in)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRB (2)</td>
<td>8.2118E-04</td>
<td>1,218</td>
</tr>
<tr>
<td>Core Stage engine CAT</td>
<td>1.1877E-03</td>
<td>842</td>
</tr>
<tr>
<td>Core Stage engine NCAT</td>
<td>6.9917E-03</td>
<td>143</td>
</tr>
<tr>
<td>Core Stage APUS</td>
<td>2.3230E-05</td>
<td>43,048</td>
</tr>
<tr>
<td>Core Stage TCS</td>
<td>1.0800E-09</td>
<td>&gt;1,000,000</td>
</tr>
<tr>
<td>Core Stage PMS</td>
<td>2.0907E-05</td>
<td>47,831</td>
</tr>
<tr>
<td>Core Stage TVC</td>
<td>2.2080E-04</td>
<td>4,529</td>
</tr>
<tr>
<td>Core Stage Separation</td>
<td>7.4003E-05</td>
<td>13,513</td>
</tr>
<tr>
<td>EDS engine CAT</td>
<td>1.0841E-04</td>
<td>9,224</td>
</tr>
<tr>
<td>EDS engine NCAT</td>
<td>5.9000E-04</td>
<td>1,695</td>
</tr>
<tr>
<td>EDS engine airstart</td>
<td>3.6000E-04</td>
<td>2,778</td>
</tr>
<tr>
<td>EDS APU</td>
<td>6.1794E-05</td>
<td>16,183</td>
</tr>
<tr>
<td>EDS TCS</td>
<td>1.0800E-09</td>
<td>&gt;1,000,000</td>
</tr>
<tr>
<td>EDS RCS</td>
<td>6.2540E-04</td>
<td>1,599</td>
</tr>
<tr>
<td>EDS TVC</td>
<td>3.6810E-05</td>
<td>27,167</td>
</tr>
<tr>
<td>Shroud</td>
<td>3.2464E-04</td>
<td>3,080</td>
</tr>
</tbody>
</table>

**Ascent LOM (Loss of Mission)** | 1.1452E-02 | 87

### Safety Condition

1. Inability to rendezvous with Orion and continue mission
2. Inability to perform mission critical operations in LEO
3. Undesired vehicle translation or rotation in LEO
4. Undesired vehicle translation or rotation during lunar coast
5. Undesired vehicle rotation during TLI burn
6. Uncontained release of energy and debris in LEO
7. Vehicle enters off nominal cis-lunar trajectory
8. Uncontained release of energy and debris during lunar coast
9. Uncontained release of energy and debris during TLI burn

### Likelihood Estimate

<table>
<thead>
<tr>
<th>Consequence Level</th>
<th>Greater than 1 in 100</th>
<th>Greater than 1 in 1,000</th>
<th>Greater than 1 in 10,000</th>
<th>Greater than 1 in 100,000</th>
<th>Greater than 1 in 1,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Consequence Level
Can We Customize Reliability and Safety Analyses to Fit in The MBSE Environment?

- Can reliability and safety analyses can be customized to fit in a MBSE?
- Can MBSE provide the frame of work to support Reliability and safety analyses?

Reliability and safety predictions output

<table>
<thead>
<tr>
<th>Component</th>
<th>Mean Failure Probability</th>
<th>Failure Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRB (2)</td>
<td>8.2118E-04</td>
<td>1.218</td>
</tr>
<tr>
<td>Core Stage engine CAT</td>
<td>1.1877E-03</td>
<td>842</td>
</tr>
<tr>
<td>Core Stage engine NCAT</td>
<td>6.9917E-03</td>
<td>143</td>
</tr>
<tr>
<td>Core Stage APU</td>
<td>2.3230E-05</td>
<td>43,048</td>
</tr>
<tr>
<td>Core Stage TCS</td>
<td>1.0800E-09</td>
<td>&gt;1,000,000</td>
</tr>
<tr>
<td>Core Stage PMS</td>
<td>2.0907E-05</td>
<td>47,831</td>
</tr>
<tr>
<td>Core Stage TVC</td>
<td>2.2080E-04</td>
<td>4,529</td>
</tr>
<tr>
<td>Core Stage Separation</td>
<td>7.4003E-05</td>
<td>13,513</td>
</tr>
<tr>
<td>EDS engine CAT</td>
<td>1.0841E-04</td>
<td>9,224</td>
</tr>
<tr>
<td>EDS engine NCAT</td>
<td>5.9000E-04</td>
<td>1,695</td>
</tr>
<tr>
<td>EDS engine airstart</td>
<td>3.6000E-04</td>
<td>2,778</td>
</tr>
<tr>
<td>EDS APU</td>
<td>6.1794E-05</td>
<td>16,183</td>
</tr>
<tr>
<td>EDS TCS</td>
<td>1.0800E-09</td>
<td>&gt;1,000,000</td>
</tr>
<tr>
<td>EDS PMS</td>
<td>5.7845E-06</td>
<td>172,876</td>
</tr>
<tr>
<td>EDS RCS</td>
<td>6.2540E-04</td>
<td>1,599</td>
</tr>
<tr>
<td>EDS TVC</td>
<td>3.6810E-05</td>
<td>27,167</td>
</tr>
<tr>
<td>Shroud</td>
<td>3.2464E-04</td>
<td>3,080</td>
</tr>
<tr>
<td>Ascent LOM (Loss of Mission)</td>
<td>1.1452E-02</td>
<td>87</td>
</tr>
</tbody>
</table>

Safety Condition

1. Inability to rendezvous with Orion and continue mission
2. Inability to perform mission critical operations in LEO
3. Undesired vehicle translation or rotation in LEO
4. Undesired vehicle translation or rotation during lunar coast
5. Undesired vehicle rotation during TLI burn
6. Uncontained release of energy and debris in LEO
7. Vehicle enters off nominal cis-lunar trajectory
8. Uncontained release of energy and debris during lunar coast
9. Uncontained release of energy and debris during TLI burn

Integrating Safety and Reliability Analysis into MBSE Toolkit
https://www.youtube.com/watch?v=NwuTV5-HAws
A FMECA Synthesis Example

Courtesy Lui Wang
Johnson Space Center

Magic Draw Plug-Ins

FMECA Output

<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 Inoperative</th>
<th>Other Inoperative Failures</th>
<th>CRIT LEVEL</th>
<th>SEV</th>
<th>Potential Causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FanInCan</td>
<td>ECS9</td>
<td>CCA1</td>
<td>CCA1</td>
<td>Circulates Air</td>
<td>Failed Off</td>
<td>Loss of CCA1 air Circulation</td>
<td>Loss of CCA1 air Circulation</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>InternalMail</td>
<td></td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBU</td>
<td>MBU1</td>
<td></td>
<td>Failed Off</td>
<td>Loss of MBU1 output power</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBU</td>
<td>MBU1</td>
<td>MBU1 Distribute Power</td>
<td>Failed On</td>
<td>MBU1 Output Power On</td>
<td></td>
<td>2</td>
<td>MBU1 Failed Off</td>
<td>1</td>
<td>MBU1FRCOn</td>
<td></td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBU</td>
<td>MBU1</td>
<td>MBU1 Distribute Power</td>
<td>Failed On</td>
<td>Loss of ability to manage MBU1 loads</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBU</td>
<td>MBU2</td>
<td>MBU1 Distribute Power</td>
<td>Failed Off</td>
<td>Loss of MBU1 output power</td>
<td>Loss of CCA1 air Circulation</td>
<td>2</td>
<td>MBU1 Failed Off</td>
<td>1</td>
<td>MBU1FRCOn</td>
<td></td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBU</td>
<td>MBU2</td>
<td>MBU1 Distribute Power</td>
<td>Failed Off</td>
<td>Loss of MBU2 output power</td>
<td>Loss of CCA1 air Circulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>MBU</td>
<td>MBU2</td>
<td>MBU1 Distribute Power</td>
<td>Failed Off</td>
<td>Loss of MBU2 output power</td>
<td>Loss of CCA1 air Circulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FanInCan</td>
<td>Power Subsystem</td>
<td>PDU</td>
<td>PDU1</td>
<td>PDU Distribute Power</td>
<td>Failed Off</td>
<td>Loss of PDU output power</td>
<td>Loss of CCA1 air Circulation</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>InternalMail</td>
<td></td>
</tr>
</tbody>
</table>

SysML Models
Summary & Conclusion

- MBSE can provide the frame of work to support Model Based Mission Assurance activities.
- Mission Assurance Community must get engaged and integrate with the MBSE communities.
- Assurance organizations may need to define new roles, develop new skills, and their products may need to be different in a model based environment.
References

- Goddard Space Flight Center (GSFC) MBSE Workshop, February 17-18, 2016, (See Link 1 Below).
- Integrating Safety and Reliability Analysis into MBSE Toolkit, (See Link 3 Below)
- Reliability and Maintainability Objective Driven Hierarchy (NASA, OSMA), (See Link 4 Below).
- Model Based Mission Assurance (MBMA) - NSC Briefing March 21, 2016, Dr. John Evans, NASA, OSMA
- MBSE presentation to MSFC S&MA, Joe Hale/Fayssal Safie, April 27, 2016

1. [https://drive.google.com/open?id=0Bw3ikr90G7CVR01Wd0hTWjN5NjA](https://drive.google.com/open?id=0Bw3ikr90G7CVR01Wd0hTWjN5NjA)
2. [https://drive.google.com/drive/folders/0B3hsmXWocH2JZVpTSzdzaUxYQzA](https://drive.google.com/drive/folders/0B3hsmXWocH2JZVpTSzdzaUxYQzA)
3. [https://www.youtube.com/watch?v=NwuTV5-Haws](https://www.youtube.com/watch?v=NwuTV5-Haws)