Identifying where Mission Assurance can benefit from Model Based Systems Engineering

Martin S. Feather[1]
Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, 91109

John Evans[2]
NASA, Washington, DC, 20546

and

Steven L. Cornford[3]
Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, 91109

Model Based Systems Engineering (MBSE) is being introduced and used to support many aspects of the engineering of complex systems. Our focus is on space systems, with a particular interest in Mission Assurance of those systems. We seek to identify where Mission Assurance can potentially benefit when a space system is developed using an MBSE approach. To do so we consider how MBSE can help provide the evidence that Mission Assurance needs, using the recently developed NASA Reliability and Maintainability Objective Hierarchy as the exposition of those needs. We illustrate this MBSE's potential contributions using examples drawn from our prior survey of the MBSE literature addressing space mission assurance concerns. The overall conclusion we draw from this is that there are numerous ways in which MBSE may, and in some cases already does, support Mission Assurance.

Nomenclature

System conforms to design intent and performs as planned = the blue colored shading indicates its text is the wording of an "Objective" for some aspect of assurance, taken from the NASA Reliability and Maintainability Objectives Hierarchy

Identify causes of anomalies = the gold colored shading indicates its text is the wording of a "Strategy" for achieving some aspect of assurance, taken from the NASA Reliability and Maintainability Objectives Hierarchy

Reference mission + before/after = the orange colored shading indicates its text is the wording of "Context" descriptive information accompanying an Objective, taken from the NASA Reliability and Maintainability Objectives Hierarchy

Sneak circuit analysis = the box indicates its text is the wording of a form of evidence used to help fulfil an assurance Strategy, taken from the NASA Reliability and Maintainability draft standard

I. Introduction

THE primary focus of the Model Based Systems Engineering (MBSE) community has been on addressing the core competencies and activities of systems engineering – developing the means by which a system's requirements, structure, behavior, development, testing and operation can be addressed in a model-centric manner. Mission Assurance, like other engineering disciplines, can take advantage of the numerous benefits associated with MBSE (for example, the "single authoritative source of truth" that is the hallmark of MBSE). For example, it

[1] Principal, Software Assurance and Assurance Research, JPL.
[2] Program Manager for Reliability and Maintainability and Program Executive for the NASA Electronic Parts and Packaging Program at NASA HQ Office of Safety and Mission Assurance, NASA Office of Safety and Mission Assurance.
[3] Senior Engineer, Strategic Systems Office, JPL.

becomes feasible to develop automated assistance for speedily generating reliability artifacts (FMECAs, Fault Trees, etc.), as a result of which Mission Assurance is able to provide reliability feedback to the engineering process in a much timelier manner.

We term this beneficial interplay "Model Based Mission Assurance" (MBMA). Our previous examination of some of the published literature on MBMA in space systems engineering has found reports of initial explorations in this direction [1, 2]. To better understand the nature of the advances that MBMA may be expected to yield, we herein examine the kinds of evidence called for in assurance of a space system design. We identify how and where MBMA can improve the processes to generate those kinds of evidence.

The basis for our assessment is the NASA Reliability and Maintainability (R&M) "Objectives Hierarchy". This is one of several hierarchies developed to date for disciplines of safety and mission assurance, the others being a Software Assurance Hierarchy, an ELV Payload Hierarchy, and a Range Safety Hierarchy. They are introduced at: https://sma.nasa.gov/news/articles/newsitem/2014/12/04/osma-introduces-new-objectives-based-strategies

The purpose of the R&M Objectives Hierarchy is explained[3] as: *"…to define critical approaches for achieving high reliability and maintainability (R&M). It embodies the knowledge attained over years of NASA experience; yet, the hierarchy extracts essentials without prescriptive processes that may encumber creativity and effective decision-making."*

We take advantage of the non-prescriptive nature of this hierarchy to serve as a rubric with which to gauge the potential contributions of MBSE to reliability and maintainability of space systems. The structure of the remainder of this paper is as follows:

Section II: An introduction of NASA's Reliability and Maintainability Objectives Hierarchy

Section III: A description of how the hierarchy's developers mapped its leaf nodes to the kinds of assurance evidence needed to fulfil those strategies. Included is a listing of all the kinds of evidence they considered.

Section IV: Our assessment of MBSE's potential for contributing to assurance of space systems. This assessment is informed by the major themes we observed in our previous survey of the MBSE literature addressing space mission assurance concerns:

- **A.** Representation and management of systems engineering information to ensure consistency and (some aspects of) completeness.
- **B.** Support of the contractual interface between acquirer and potential providers.
- **C.** Generation of review documentation from the shared MBSE system model.
- **D.** Correctness of the MBSE models themselves.
- **E.** Automated assistance for generating reliability artifacts (FMECAs, Fault Trees, etc.).
- **F.** Representation of and reasoning about off-nominal states and behaviors.
- **G.** Support for activities post-design.

For each of these we discuss MBSE's potential contributions, in terms of the support it offers to the portions of the R&M Objectives Hierarchy overall, and the specific forms of evidence typically sought to show fulfilment of elements of that hierarchy.

Section V: Areas of assurance that to date appear to be unaddressed by MBSE.

Section VI: Brief conclusions.

Appendix: A listing of the entire R&M Objectives Hierarchy.

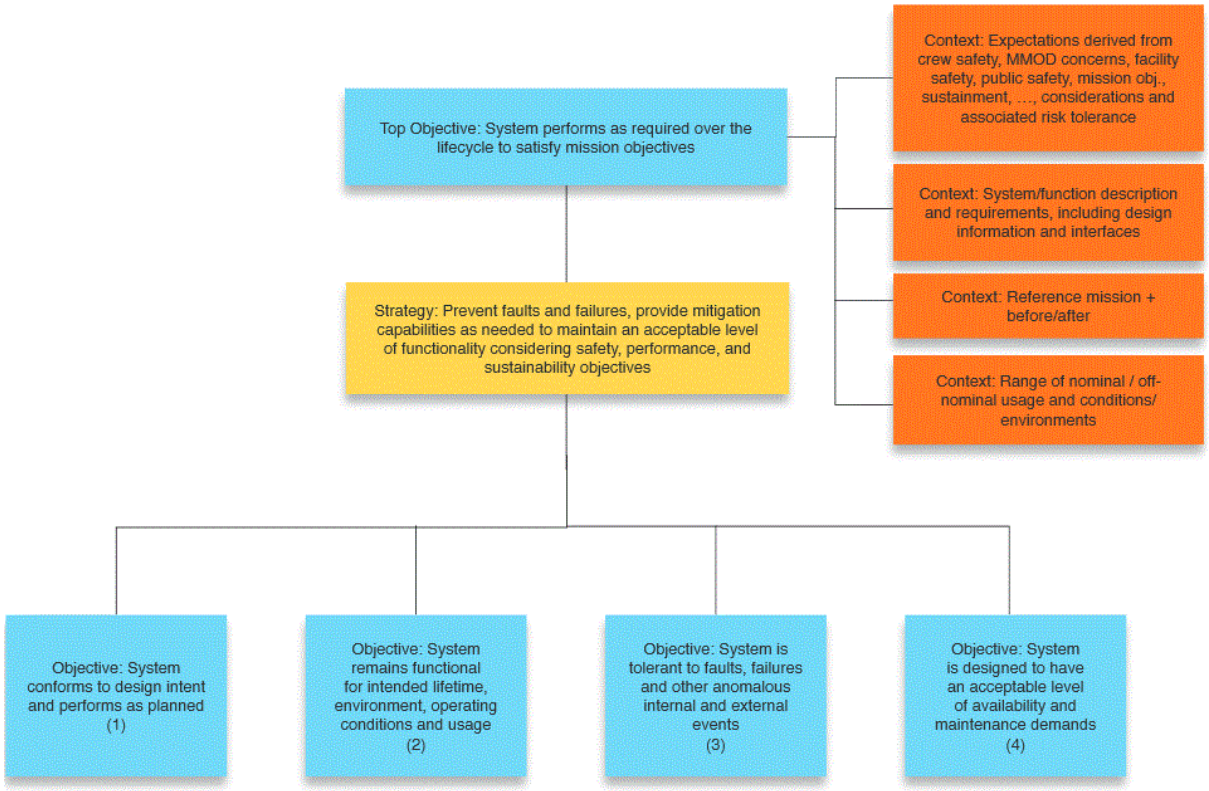

Figure 1. R&M Objectives Hierarchy: Top Level.

II. The Reliability and Maintainability Objectives Hierarchy

NASA's Objective Hierarchies are expressed in (a slight modification of) the Goal Structuring Notation (GSN)[4], widely used to present a "Safety Case" – a well-reasoned argument that a system achieves acceptable levels of safety. These are widely used in Europe and elsewhere to present the argument that a safety critical system (e.g., a transportation system, an industrial plant) is indeed safe to operate. The primary aspect of the GSN notation is hierarchical decomposition of an Objective into sub-Objectives such that if all of them are met, together imply the Objective is met ("Objective" here is equivalent to GSN's concept of "Goal" or equivalently "Claim"). A "Strategy" may be interposed between an Objective and the sub-Objectives to explain the decomposition to the reader. A Safety Case is used primarily for communicating ideas and information to a third party (e.g., a regulator or an independent assessor). It is primarily an informal argument, although there is interest in modeling arguments in formal logic[5].

The top of the R&M Objectives Hierarchy is shown in this notation in Fig. 1. The uppermost blue rectangle states the overall reliability and maintainability objective of a space system. The four orange rectangles to its right establish the "Context" for that system (its mission requirements, expected operating conditions, etc.) The yellow rectangle describes a "Strategy" – an approach to decomposing the topmost Objective into the four lower-level sub-Objectives, which, if all of them are met, imply the Objective above the Strategy is met. Each of the four lower-level sub-Objectives is recursively decomposed further, through a Strategy leading to lower-level Objectives, etc. For example, the leftmost of the lower-level sub-Objectives in Fig. 1 is shown as decomposed as shown in Fig. 2. The other three sub-Objectives of Fig. 1 are similarly decomposed. The entire R&M Objectives Hierarchy is listed (in a more compact form) in the Appendix.

The R&M Objectives Hierarchy is the generic starting point for constructing the assurance case for a space system. The specifics of the system (its mission requirements) are presented in the Context elements of its assurance case. The results of analyses, tests, inspections, reviews, etc., are presented as "Evidence" demonstrating fulfilment of the bottommost Strategy nodes of the R&M Objectives Hierarchy. This approach is demonstrated on an example of a spacecraft containing COTS parts, focusing on the tolerance of the spacecraft design to radiation effects[6].

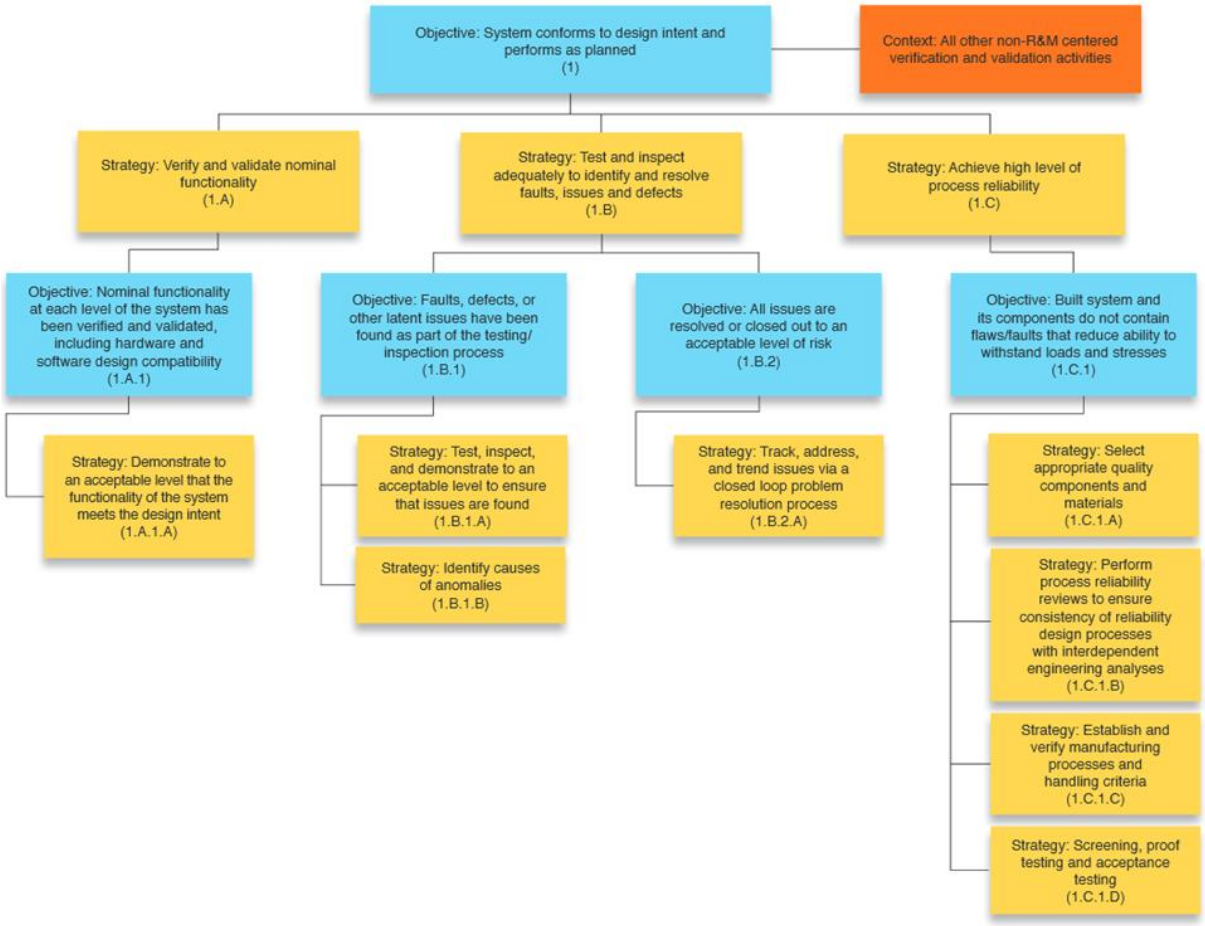

Figure 2. R&M Objectives Hierarchy: Sub-Objective 1.

III. From Strategies to Assurance Evidence

The NASA team that developed the Reliability and Maintainability Objectives Hierarchy then went on to identify the typical assurance evidence needed to fulfil each bottom level strategy. For example, for the bottom level strategy **Test, inspect, and demonstrate to an acceptable level to ensure that issues are found (1.B.1.A)** seen in Fig. 2, they identified a long list of forms of evidence: "**Testing and Analysis Methods such as: Sneak circuit analysis, EMC emissions test, EMC isolation test, EMC susceptibility test, ESD discharge test, HALT, HAST, Life testing, Regression Testing, Stress Testing, Static Code Analysis**." (Note: in this paper the names of forms evidence are listed using **boxed text**.) As the wording indicates, this is a list of *suggested* forms of assurance evidence. It may not be necessary to include *all* those forms of evidence for demonstrating satisfaction of that strategy within a specific assurance case. Nor are the forms of evidence that may be provided restricted to *only* those included in the list. Nevertheless, these lists are good collections of the forms of evidence one would typically make use of in demonstrating assurance.

Their efforts resulted in a many-to-many mapping between assurance evidence and the strategy or strategies that evidence fulfils. It is many-to-many because in many cases a strategy may be fulfilled by multiple forms of evidence (as is clear from the example above), and in some cases a form of evidence may be of use in fulfilling multiple strategies (for example, **Life testing** also shows up as a form of evidence for one of the leaf strategy nodes in the Sub-Objective 2 of the R&M Objectives Hierarchy). All the forms of evidence mentioned in their work are listed next, in alphabetical order:

Acceptance Test Plan
Accessibility Analysis
Acoustic test
Aging margins
Allocation Analysis
Ambiguity Analysis
Ambiguity Matrix
Approved parts list
Constant acceleration test
Consumables Catalog/Limited Life Items
Demonstration Testing
Derating
Design Requirement Verification Matrix
Destructive Physical Analysis
EMC emissions test
EMC isolation test
EMC susceptibility test
ESD discharge test
Environmental Stress Screening
FMEA
FMEA/CIL
FMECA
FRACAS
Failure Trending Analysis
Fatigue Analysis
Fault Tree
Fishbone Analysis
Flight Rules
Ground handling analysis
Ground handling test
HALT
HAST
Hazard Analysis
I&T Reports
Independent technical review
Insertion of data into some NASA-wide database
Inspection Criteria

Lessons Learned
Level of repair analysis
'Level of technician' analysis
Life Analysis
Life testing
Logistics/sparing analysis
Magnetic test
Maintainability Demonstration
Maintainability Design Check sheets
Maintainability Program Plan
Maintainability models
Maintenance Database
Maintenance Task Analysis
Maintenance activities block diagrams
Maintenance manual
Material and Processes Control Plan
Materials review
Mechanical shock test
Monte Carlo simulation for predicting MMH
PRA
PRACA
Parts control and traceability
Parts stress analyses
Peer technical review
Performance Trending Analysis
Physics of failure analysis
Powered-on vibration test
Process FMEA
Process capability assessment
Process variance analysis
Pyrotechnic shock test
Quantitative Reliability Modeling and Analysis
RCM Decision Logic Tree
RCM analysis
RMA Analysis

Radiation design margins
Radiation dose analysis
Random vibration test
Recapitalization Analysis (Tech refresh)
Redundancy Decomposition
Regression Testing
Reliability Block Diagram
Reliability Growth Modeling
Requirements for modularity/interoperability
Results of demonstration test
Root Cause Analysis
Sine dynamic test
Single Event Effect Analysis
Sneak circuit analysis
Software process audits
Standard Interface Requirement Document
Static Code Analysis
Stress Testing
Structural Proof Loading Test
Structural safety margins
Structural/thermal analyses
Surface charging/ESD
Technical oversight & management
Test Results
Testability analysis
Testability demonstration plan and results
Thermal margin
Thermal test
Trade Study Analysis
Training Plan and Material
Verification and Validation Testing
Voltage/temperature margin test
Worst Case Analysis

The primary purpose of the NASA team that did this work was to develop standards and guidance for deciding the extent and forms of assurance appropriate for a space system design. Thus the expected way of using their products is to work top-down through the R&M Objectives Hierarchy, applied to and instantiated with the details of the space system in question. When this process reaches the Objective Hierarchy's bottommost strategy nodes, these then map to the forms of evidence typically provided to show that part of the assurance argument. We use the results of their mapping work in the *opposite* direction. Given a form of assurance evidence, we trace "backwards" through their mapping to identify the place(s) where that evidence contributes to assurance arguments. This is the basis for our approach to assessing the potential contributions of Model Based Systems Engineering, discussed next.

IV. MBSE's Potential for Contributing to Assurance

Mission Assurance, like other engineering disciplines, can take advantage of the numerous benefits associated with MBSE including: the "single authoritative source of truth," unambiguous definition of terms and relationships, the ability to explore the data using unique viewpoints, and the ability to transform the data for ingestion into other tools. Most obviously, MBSE's emergence provides an opportunity for Mission Assurance to move from document-centric approaches, which often hinder the contribution and timely conduct of assurance activities, to objective-based products that are embedded within, and compatible with, the modeling used in an MBSE setting. To realize this improvement, mission assurance products and processes need to be able to fit within this framework. For example, safety and reliability engineers must be closely linked to the development taking place in the MBSE framework, from requirements definition through analysis, to support trade studies and design analyses that assure the required reliability and safety. The MBSE framework may demand that reliability and safety analysis and related products take on a new shape. Overall, this new environment presents an unprecedented opportunity to improve effectiveness of the reliability and safety communities.

To understand MBSE's implications for Mission Assurance, we conducted a survey of MBSE literature addressing space mission assurance concerns. Our objective was to find how MBSE approaches are being (or could be) applied to support assurance needs. Our findings[2] of where MBSE approaches are being applied to support assurance needs fell into the following seven areas:

- **A.** Representation and management of systems engineering information to ensure consistency and (some aspects of) completeness.
- **B.** Support of the contractual interface between acquirer and potential providers.
- **C.** Generation of review documentation from the shared MBSE system model.
- **D.** Correctness of the MBSE models themselves.
- **E.** Automated assistance for generating reliability artifacts (FMECAs, Fault Trees, etc.).
- **F.** Representation of and reasoning about off-nominal states and behaviors.
- **G.** Support for activities post-design.

The first four of these (A-D) are very broad in the assurance scope they cover. The remaining three (E-G) are more specific. The subsections that follow look at each of these in turn.

A. Representation and Management of Systems Engineering Information to Ensure Consistency and (some aspects of) Completeness

This rigorous foundation helps ensure consistency, and some aspects of completeness, of the systems engineering information. These desirable qualities have obvious relevance and benefit to the entire R&M Objectives Hierarchy to the extent that MBSE is carried through the mission lifecycle. It may provide specific benefit to **1.B.1.A Test, inspect, and demonstrate to an acceptable level to ensure that issues are found** through heading off subtle and hard to detect problems that stem from misinterpretations prevalent when less rigorous documentation is the norm. In the R&M mapping this item is linked to only one form of evidence, the rather broadly stated one of **Verification and Validation Testing**.

The general nature of this area meant that in our survey we were able to find repeated mentions of its benefits. Rigorously defined interfaces were often cited as beneficial for large projects. Indeed, we see from the NASA R&M mapping between evidence and strategies that evidence in the form of a **Standard Interface Requirement Document** is connected to the Strategy **4.A.3.B Design for physical and functional interchangeability with other like components and assemblies in the system**. We list two examples drawn from the literature we surveyed:

- The document[7] reporting integration of flight software developed for the James Webb Space Telescope's Integrated Science Instrument Module includes the statement:

  > Distributed software modeling was successfully demonstrated in the James Webb Space Telescope (JWST) Integrated Science Instrument Module flight software development. The use of identical CASE development tools was a major contributor to the success by reducing the model export and import issues.

- The document[8], describing work on large scale telescope projects, includes the statement:

  > A major issue for us is to understand very well both external and internal interfaces among components of the as-is system, to evaluate the impact of the changes in the to-be system to avoid any interface backward incompatibility. MBSE is helping us substantially in this task.

B. Support of the Contractual Interface between Acquirer and Potential Providers

When NASA acquires a system or service from a provider (system developer, or supplier of a service), the goals and strategies of the R&M Objectives Hierarchy cover the kinds of assurance information that the provider will need to communicate to the acquirer to allow the latter to gauge the acceptability of the system. NASA plans for this

information to be conveyed through a "Risk-Informed Safety Case (RISC)." As explained in the NASA System Safety Handbook [9] this is a specialization of the "safety case" construct:

> The term "risk-informed" is used here to emphasize that a determination of adequate safety is the result of a deliberative decision making process that necessarily entails an assessment of risks and tries to achieve a balance between the system's safety performance and its performance in other areas. The RISC, which evolves over the course of the system life cycle, supports decision making at system life-cycle reviews and other major decision points.

First, however, it is necessary for the acquirer to inform the would-be provider(s) of what is being sought. This is shown as the "**Elicit Top-Level Objectives…**" step in Fig. 3.

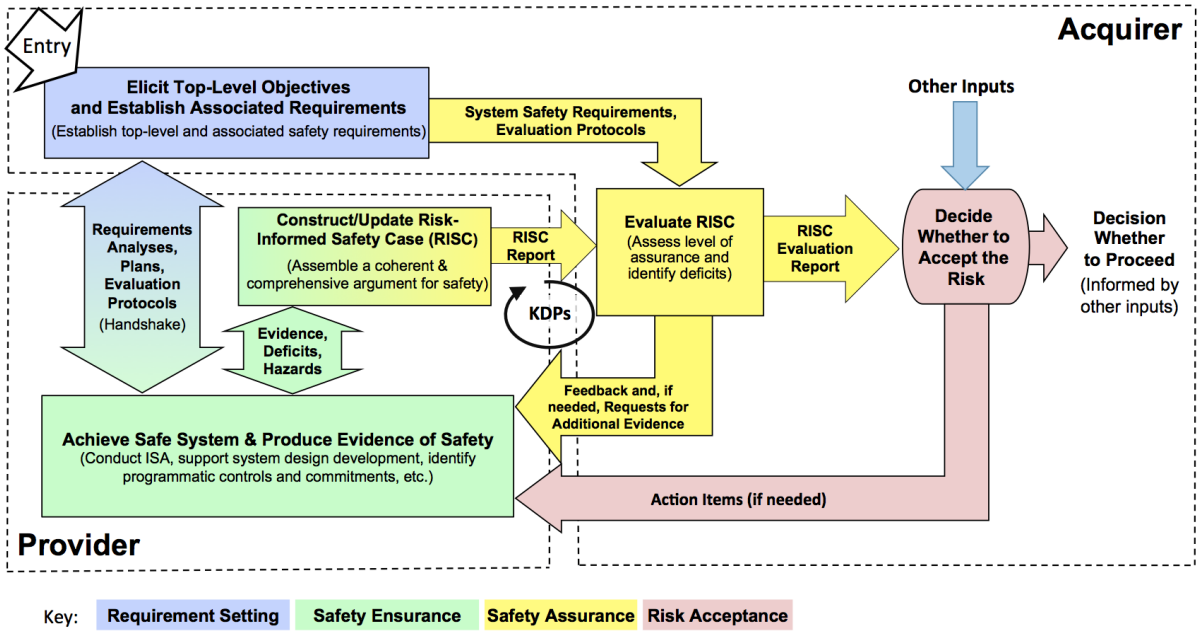

Figure 3. The NASA System Safety Framework[9]

In the R&M Objectives Hierarchy the location for this information is in the four context elements accompanying the top objective of the R&M hierarchy (Fig. 4), rather than within the goals and strategies themselves. In keeping with the spirit of the hierarchy, these describe *what* information is to be provided, not the form it must take. Hence a key precept of MBSE – that there are advantages to information taking the form of semantically precise models rather than documents composed of natural language and somewhat imprecise diagrams – has potential here too.

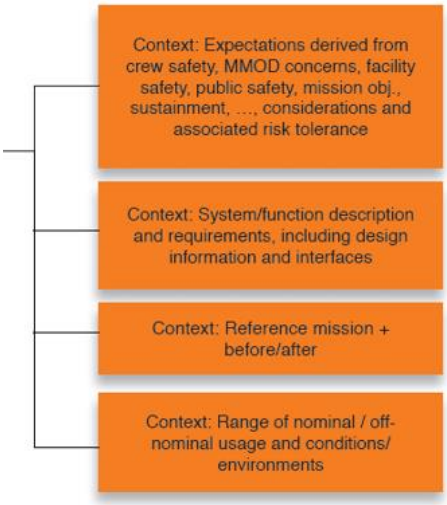

Figure 4. The Context elements at the top of the R&M Objectives Hierarchy

In the course of our survey we did not find this topic discussed for space systems (admittedly we do not claim our survey to be in any sense "complete"). We did, however, find the use of MBSE in the contracting phase discussed in the context of defense system procurement[10], specifically focusing on *"… the transition of models created by the customer (acquirer) during the capability definition phase to the supplier during the tendering process and the use and maintenance of these models through the system architectural design and detailed development phases.*" The discussion considered the information that should be in a model-based "Request For Tender," in which the acquirer puts forth the description for what's being sought, and the information in a model-based "Tender" in which the would-be provider responds with their proposed solution. The paper makes the point that "*MBSE has been applied across the contractual boundary for over twenty years in environments where mutual trust is well developed and mutual goals are well understood*" but goes on to state that "*If a competitive environment cannot be avoided,*

our findings to date indicate that MBSE-based tendering looks viable but its feasibility will be a function of how well the parties can either limit the scope of the models to sharable information or the ability of all parties to segment and configuration-manage their models" (e.g., a prospective provider might wish to limit the exchange of proprietary information prior to becoming selected as the provider).

C. Generation of Review Documentation from the Shared MBSE System Model

Preliminary results from ongoing NASA applications show evidence of benefits to the R&M Objectives Hierarchy strategy **1.A.1.A Demonstrate to an acceptable level that the functionality of the system meets the design intent.** Traditional review materials (text and tabular documents) are being generated from the system models rather than hand-composed, ensuring those materials reflect the consistency of MBSE's "single authoritative source of truth." By generating traditional review materials, this allows review boards to continue to deal with familiar materials – they need not be trained to read and comprehend MBSE models. Anecdotal reports from projects using MBSE in this way suggest that review boards do observe the increased quality (particularly consistency) of the review materials. In the longer term there is hope that reviews themselves shift to take advantage of MBSE models by examining the models themselves, not just the static outputs that cen be generated from those models.

The R&M mapping contains several forms of more specific review evidence:

- **Materials review** is connected to the strategy **1.C.1.A. Select appropriate quality components and materials**
- **Independent technical review**, **Peer technical review** and **Software process audits** all connect to the strategy **1.C.1.B Perform process reliability reviews to ensure consistency of reliability design processes with interdependent engineering analyses**

D. Correctness of the MBSE Models

Since the system design information is captured in models, it is crucial that they be correct, with obvious relevance across the entirety of the R&M Objectives Hierarchy. Surprisingly, model correctness received scant mention in the documents we examined in our survey.

We did encounter mention of the checking of MBSE models for criteria of completeness and consistency. These kinds of checks help ensure the models are semantically well-formed, but do not ensure model validity – i.e., that the models capture the designers' intent.

Note that NASA's Modeling and Simulation standard[11] is focused on primarily models of physical phenomena, models based on data from observations of those phenomena. As such it does not directly address the kinds of engineering models developed in MBSE to represent candidate system designs (although it does apply to models of the space environment in which those systems will operate, and to models of physical phenomena such as wear out degradation and failure).

E. Automated Assistance for Generating Reliability Artifacts (FMECAs, Fault Trees, etc.)

Not surprisingly, reliability artifacts such as FMECAs and Fault Trees play a prominent role in providing evidence to demonstrate satisfaction of the R&M Objectives Hierarchy. Fig. 5 shows the mapping of the 13 types of reliability-specific artifacts listed by the NASA R&M team to the leaf Strategies of the R&M hierarchy. As can be seen, the artifacts map to 20 of the 42 leaf Strategies, in some cases with two or three of the artifacts mapping to the same Strategy.

In our survey of MBSE literature we found repeated examples of MBSE proposed to be (in some cases already being) used to provide automated assistance to generation of various kinds of reliability artifacts. For example:

- Automated help for generating a FMEA is illustrated on a system of a satellite, its ground control system, and its ground users[12]
- FMEA synthesis for failure mode analysis (and derivations of other analysis artifacts not specifically called out in the NASA R&M evidence artifacts, such as an AADL model for architectural analysis) are illustrated on aspects of a ramjet powered vehicle[13,14]
- Generation of FMECAs and Fault Trees illustrated on the "Common Cabin Air Assembly" (to provide life-critical air circulation in the ISS) and on the "Cascade Distillation System" (wastewater processing for a water recovery system as might be used on a lunar outpost or mission to Mars)[15,16]

F. Representation of, and Reasoning about, Off-nominal States and Behaviors

Off-nominal behavior, of particular interest to R&M practitioners, has begun to be explored in the context of MBSE. Its representation often goes hand-in-hand with generation of reliability artifacts, discussed above.

The ability to reason over such artifacts is key. MBSE helps this through its focus on carefully crafted rigorous computer-based representations of information, in particular MBSE's representation of *behavioral* information[17]. In the past it has been challenging for mission assurance to provide rapid feedback in this area, because of the time it took to assemble an analyzable model from the wide variety of representations, formal and semi-formal, in use. MBSE helps through its emphasis on an agreed-upon and shared ontology (using the information science definition of the word, e.g., "*To support the sharing and reuse of formally represented knowledge among AI systems, it is useful to define the common vocabulary in which shared knowledge is represented. A specification of a representational vocabulary for a shared domain of discourse — definitions of classes, relations, functions, and other objects – is called an ontology*"[18]).

	1.A.1.A Demonstrate to an	1.B.1.A Test, inspect, and	1.B.1.B Identify causes of	1.B.2.A Track, address, and trend	1.C.1.A Select appropriate quality	1.C.1.B Perform process	1.C.1.C Establish and verify	1.C.1.D Screening, proof testing	2.A.1.A Apply design standards to	2.A.1.B Evaluate and control	2.A.1.C Evaluate and control	2.A.1.D Perform qualification	2.A.2.A Evaluate and control	2.B.1.A Determine reliability	2.B.1.B Estimate reliability based	2.B.1.C Support design trades	2.B.1.D Plan and perform life	2.B.1.E Track and monitor	3.A.1.A Provide similar or	3.A.2.A Separate redundant	3.A.2.B Isolate and contain faults	3.A.2.C Evaluate and control	3.A.3.A Provide fault	3.A.4.A Plan contingency or other	4.A.1.A Design to facilitate on-	4.A.1.B Design to minimize	4.A.1.C During design, consider	4.A.1.D Use standardization to	4.A.1.E Perform RCM (on	4.A.1.F Perform maintainability	4.A.1.G Provide demonstration	4.A.2.A Identify and optimize the	4.A.2.B Incorporate fault	4.A.2.C Develop test-point-	4.A.2.D Design-in self-diagnostics	4.A.3.A Design the system to	4.A.3.B Design for physical and	4.A.3.C Incorporate modular	4.A.4.A Establish capabilities and	4.A.4.B Periodically analyze test	4.A.4.C Periodically review and	4.A.4.D Ensure availability of data
FMEA													■							■		■	■	■																			
FMEA/CIL																															■		■	■	■								
FMECA																					■			■																			
Fault Tree			■										■									■																					
Fishbone Analysis			■																																								
Hazard Analysis																						■	■																				
PRA																								■																			
Process FMEA							■																		■	■	■																
Quantitative Reliability Modeling and															■																												
Redundancy Decomposition/RBD/FTA																			■																								
Reliability Growth Modeling																		■																									
Root Cause Analysis			■																																								
Worst Case Analysis											■	■																															

Figure 5. Mapping of reliability artifacts (rows) R&M Objectives Hierarchy leaf Strategies (columns)

The areas where this has potential to help include:

- generation of the reliability artifacts discussed in the previous section,
- development of models on which to perform other kinds of analysis, and
- generation of simulations and other executable models that can be run extensively prior to testing with actual hardware. Hardware testing is generally expensive, so simulations and executable models can tease out problems early leaving testing to focus on confirmation of the most critical areas of remaining uncertainty, and testing is not always even possible (e.g., it may not be possible to test in zero-g in advance of the actual mission), so in those cases simulations and executable models may be the only option.

Representation and reasoning underpins each of these areas. Fig. 5 earlier showed the mapping of reliability artifacts to the R&M Objectives Hierarchy's leaf Strategies, for which representation of off-nominal conditions is obviously crucial. Fig. 6 shows the mapping of the other kinds of analysis artifacts (other than explicit failure analysis), and of specific types of testing, to the same leaf Strategies.

Examples of this from our survey of MBSE literature include:

- Execution of a Stateflow model of NASA's Ares & Orion communication during abort was used to verify fault management behavior[19]
- Use of an AADL model (semi-automatically derived from the MBSE representation in SysML) to analyze real-time computational aspects of a system[20]; similar use of an AADL model is seen for analyses of end-to-end data flow and latency of command flow for a space mission[21]
- Use of AltaRica ("a tool and language implementing mode automata") to model fault propagation[12, 13]

G. Support for Activities Post-design

While much of the focus of MBSE is on the design phase of systems engineering, its fundamental principle of capturing and utilizing a range of pertinent information in a formal representation has also been applied to later development phases, notably testing and operations. In these later phases there can be a huge amount of engineering detail. Applications of MBSE in these phases – at least in the reports we have seen – do not attempt to encompass

this level of detail, but rather concentrate on the overall management (planning and execution) of testing, training and operations.

Examples of this from our survey of MBSE literature include:

- The Large Synoptic Survey Telescope (LSST) reported[22] having used MBSE to "to document the verification planning phases." To do so, they extended the MBSE representation to include concepts of the verification phase (e.g., verification requirement, verification method, success criteria)
- An assessment of the NASA Ground Systems Development and Operations' (GSDO) plan made use of MBSE techniques to represent the information (primarily physical and logical interfaces) they then assessed[7]
- The OSIRIS-REx mission used MBSE to "generate a consistent architecture across all ground system elements, to manage all OSIRIS-REx ground system requirements easily in one location, to perform verification and validation of these requirements, and to validate the ground system operations timeline…"[23]

Fig. 7 shows the mapping of testing management artifacts (rather than of specific types of testing, which were in the previous figure) to the same leaf Strategies.

V. Unaddressed Areas

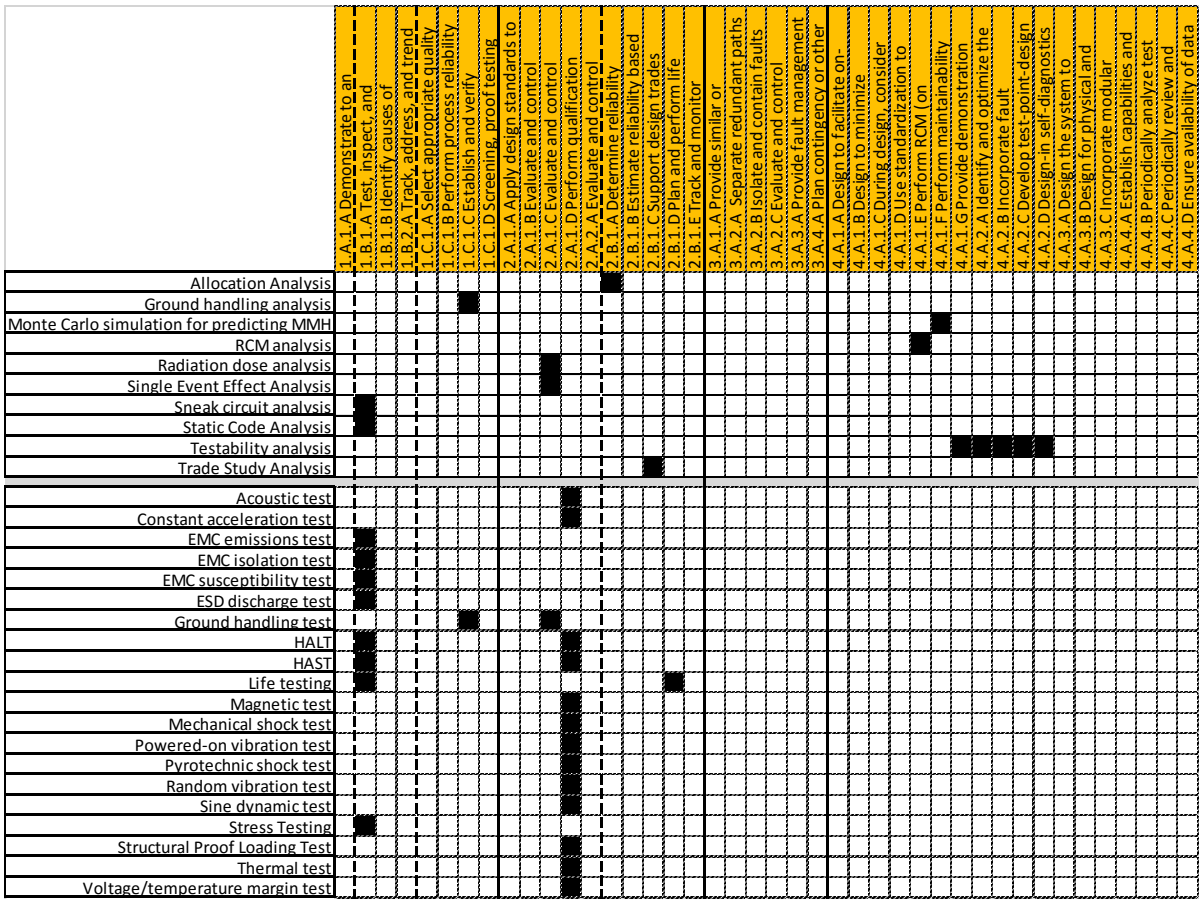

Figure 6. Mapping of analysis and specific test artifacts (rows) to R&M Objectives Hierarchy leaf Strategies (columns)

The previous sections showed mappings to the R&M Objectives Hierarchy leaf Strategies from:

- Reliability artifacts
- Analysis and specific test artifacts
- Test management artifacts

Together these indicate where MBSE approaches may support generation of the artifacts needed to show fulfilment of many of the leaf Strategies of the R&M Objectives Hierarchy. In our survey of MBSE literature on

	1.A.1.A Demonstrate to an	1.B.1.A Test, inspect, and	1.B.1.B Identify causes of	1.B.2.A Track, address, and trend	1.C.1.A Select appropriate quality	1.C.1.B Perform process reliability	1.C.1.C Establish and verify	1.C.1.D Screening, proof testing	2.A.1.A Apply design standards to	2.A.1.B Evaluate and control	2.A.1.C Evaluate and control	2.A.1.D Perform qualification	2.A.2.A Evaluate and control	2.B.1.A Determine reliability	2.B.1.B Estimate reliability based	2.B.1.C Support design trades	2.B.1.D Plan and perform life	2.B.1.E Track and monitor	3.A.1.A Provide similar or	3.A.2.A Separate redundant paths	3.A.2.B Isolate and contain faults	3.A.2.C Evaluate and control	3.A.3.A Provide fault management	3.A.4.A Plan contingency or other	4.A.1.A Design to facilitate on-	4.A.1.B Design to minimize	4.A.1.C During design, consider	4.A.1.D Use standardization to	4.A.1.E Perform RCM (on	4.A.1.F Perform maintainability	4.A.1.G Provide demonstration	4.A.2.A Identify and optimize the	4.A.2.B Incorporate fault	4.A.2.C Develop test-point-design	4.A.2.D Design-in self-diagnostics	4.A.3.A Design the system to	4.A.3.B Design for physical and	4.A.3.C Incorporate modular	4.A.4.A Establish capabilities and	4.A.4.B Periodically analyze test	4.A.4.C Periodically review and	4.A.4.D Ensure availability of data
Acceptance Test Plan								■																																			
Demonstration Testing																	■																										
Design Requirement Verification Matrix																					■																						
Failure Trending Analysis																		■																									
I&T Reports																																■											
Inspection Criteria								■																																			
Maintainability Demonstration																									■	■				■	■							■					
Performance Trending Analysis																		■																									
Regression Testing		■																																									
Reliability Growth Modeling																		■																									
Results of demonstration test																															■												
Test Results												■																															
Testability demonstration plan and results																															■	■	■	■	■								
Verification and Validation Testing	■																																										

Figure 7. Mapping of test management artifacts (rows) to R&M Objectives Hierarchy leaf Strategies (columns)

(predominantly) space systems engineering we found instances of studies, ranging from theoretical, through pilot and actual applications, of MBSE approaches for these purposes. We now consider the opposite question – which of the leaf Strategies of the R&M Objectives Hierarchy are *not* mapped to by any of these artifacts? A preliminary investigation has identified the following 12 leaf Strategies (out of the total of 42 leaf strategies in all):

- **1.B.2.A Track, address, and trend issues via a closed loop problem resolution process**
- **1.C.1.A Select appropriate quality components and materials**
- **1.C.1.B Perform process reliability reviews to ensure consistency of reliability design processes with interdependent engineering analyses**
- **2.A.1.A Apply design standards to incorporate margin to account for variable and unknown stresses**
- **2.A.1.B Evaluate and control nominal stresses and related failure causes**
- **4.A.1.D Use standardization to limit the number of feasible design options and encourage the use of common items, procedures, processes, tools, etc**
- **4.A.3.A Design the system to accommodate future technology or changes in application over the design life via maintenance activities**
- **4.A.3.B Design for physical and functional interchangeability with other like components and assemblies in the system**
- **4.A.4.A Establish capabilities and processes to collect and store operational history, health status, degradation, diagnostic, and maintenance data**
- **4.A.4.B Periodically analyze test and operational history, health status, degradation, diagnostic, and maintenance data to determine maintainability performance and trends**
- **4.A.4.C Periodically review and update maintenance strategy and activities**
- **4.A.4.D Ensure availability of data to future programs and projects**

Quite a few of the above are "process" related (e.g., 1.C.1.B) for which MBSE might offer only indirect support, rather than assist in the generation of artifacts that show fulfilment of these strategies. At first glance none of the above look like they will be *disadvantaged* by the advent of MBSE, so it is plausible to think that MBSE will be compatible with them, and as we learn to utilize MBSE, it may be that we find it has contributions to offer for some of them. As NASA continues to move into the Model-based future, MBMA must address the gaps identified and begin to perform increasingly challenging test cases, to enable the revisions and updates necessary for complete and "perfect" integration.

VI. Conclusion

Our examination of the prospective benefits of Model Based Systems Engineering to space systems' Mission Assurance shows there to be multiple opportunities for such benefits to be realized. Key to these opportunities is MBSE's use of a notation that is both formal (semantically rigorous) and well-suited to the expression of systems engineering information. For assurance in particular, this means that systems engineering information is readily available in a form amenable to automated processing. We see the most prominent assurance uses of this form of information in a trend towards automated support for generation of reliability artifacts (FMECAs, Fault Trees, etc.), made possible by MBSE's formal (semantically rigorous) representation of system information. There is clearly scope for further valuable work in this direction. We see indications of another class of advantages, those deriving from MBSE in the area of space systems' engineering activities past the design stage. We find examples where MBSE helps planning, managing and assessing V&V program for a complex system, and to help manage the planning for complex systems operations.

The approach we followed to reach our insights was to consider the kinds of evidence needed by assurance, and examine whether and how MBSE might support the contribution of such evidence. An alternative approach to assessing the value of MBSE would be to query a broad range of practitioners for their experiences. Such a survey approach was followed to assess the contributions of Model Based (Software) Engineering (MBE) to the development of embedded software systems[24]. Model Based *Software* Engineering is in many ways a precursor of Model Based *Systems* Engineering. For example, the Systems Modeling Language (OMG SysML™), designed for representing *systems* engineering information, is an outgrowth of an earlier language, the Unified Modeling Language (UML) developed to be a standard language for *software* engineering. We note that in the aforementioned survey, respondents were overwhelmingly positive in their indications of the effect of MBE on "Quality," "Reliability," "Maintainability" and "Safety." Since it is only relatively recently that MBSE has begun to be used in space systems' engineering, it is perhaps too early to conduct a comparable survey for MBSE. However, given the growth of interest in and application of MBSE in the space community[25], in a few years' time such a survey would be worthwhile.

Appendix

The whole of the R&M Objectives Hierarchy is listed below, using indentation to compactly indicate the hierarchical structure.

Blue shading = its text is the wording of an "Objective
Gold shading = its text is the wording of a "Strategy"
Orange shading = its text is the wording of "Context"

System performs as required over the lifecycle to satisfy mission objectives
- Expectations derived from crew safety, MMOD concerns, facility safety, public safety, mission obj., sustainment, …, considerations and associated risk tolerance
- System/function description and requirements, including design information and interfaces
- Reference mission + before/after
- Range of nominal / off-nominal usage and conditions/environments
- Prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives
  - 1: System conforms to design intent and performs as planned
    - All other non-R&M centered verification and validation activities
    - 1.A: Verify and validate nominal functionality
      - 1.A.1: Nominal functionality at each level of the system has been verified and validated, including hardware and software design compatibility
        - 1.A.1.A: Demonstrate to an acceptable level that the functionality of the system meets the design intent
    - 1.B: Test and inspect adequately to identify and resolve faults, issues and defects
      - 1.B.1: Faults, defects, or other latent issues have been found as part of the testing/inspection process
        - 1.B.1.A: Test, inspect, and demonstrate to an acceptable level to ensure that issues are found
        - 1.B.1.B: Identify causes of anomalies
      - 1.B.2: All issues are resolved or closed out to an acceptable level of risk
        - 1.B.2.A: Track, address, and trend issues via a closed loop problem resolution process

1.C: Achieve high level of process reliability

1.C.1: Built system and its components do not contain flaws/faults that reduce ability to withstand loads and stresses

1.C.1.A: Select appropriate quality components and materials

1.C.1.B: Perform process reliability reviews to ensure consistency of reliability design processes with interdependent engineering analyses

1.C.1.C: Establish and verify manufacturing processes and handling criteria

1.C.1.D: Screening, proof testing and acceptance testing

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

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

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

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

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

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

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

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

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

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

2.B.1.A: Determine reliability allocation

2.B.1.B: Estimate reliability based on applicable performance data, historical data of similar systems, and/or physics-based modeling

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

2.B.1.D: Plan and perform life testing

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

3: System is tolerant to faults, failures and other anomalous internal and external events

Hardware and software interactions and interfaces

3.A: Assure that system includes necessary barriers and mitigations to keep anomalous events from compromising the ability to meet mission objectives

3.A.1: System has multiple means of accomplishing functions that are critical to mission objectives including safety

3.A.1.A: Provide similar or dissimilar functional redundancy

3.A.2: Physical and functional pathways for fault propagation or combination are limited

3.A.2.A: Separate redundant paths functionally and physically

3.A.2.B: Isolate and contain faults

3.A.2.C: Evaluate and control shortest path to worst case effects (e.g. hazardous events)

3.A.3: System is able to recover from anomalies affecting functions that are important to top-level expectations.

3.A.3.A: Provide fault management (detection, active isolation, recovery) capabilities

3.A.4: System can degrade or lose functions without significantly impacting top-level expectations (through contingency operations)

3.A.4.A: Plan contingency or other off nominal operations

4: System is designed to have an acceptable level of availability and maintenance demands

4.A: Evaluate, control, and monitor the ease of maintaining, restoring, or changing system capability and total maintenance demands

4.A.1: Maintenance and repair activity can be performed within available resources (cost, time)

4.A.1.A: Design to facilitate on-orbit and ground maintenance and check out

4.A.1.B: Design to minimize maintenance complexity for reduction of maintenance time and training requirements

4.A.1.C: During design, consider tool selection, transport, stowage, ease of use, and criticality as well as complexity of robotic maintenance capability where feasible

4.A.1.D: Use standardization to limit the number of feasible design options and encourage the use of common items, procedures, processes, tools, etc

4.A.1.E: Perform RCM (on orbit/ground support systems) during design to optimize the design for maintainability

4.A.1.F: Perform maintainability simulation and analysis as needed to support design and logistic support analysis

4.A.1.G: Provide demonstration testing to verify 'detect, diagnose, isolate' capability of systems and confirm corrective and preventive maintenance task actions and analysis

4.A.2: System provides clear indication of health status, degradations, and diagnostic information

4.A.2.A: Identify and optimize the testability and diagnostics characteristics to support the maintainability requirements

4.A.2.B: Incorporate fault detection/isolation/recovery at the lowest practical level to support the maintainability requirements

4.A.2.C: Develop test-point-design strategies to minimize access time and system intrusion

4.A.2.D: Design-in self-diagnostics for assemblies to minimize maintenance/recovery time and false alarms

4.A.3: System design allows for reconfiguration, upgrade, or growth opportunities during the mission

4.A.3.A: Design the system to accommodate future technology or changes in application over the design life via maintenance activities

4.A.3.B: Design for physical and functional interchangeability with other like components and assemblies in the system

4.A.3.C: Incorporate modular designs to facilitate remove-and-replace maintenance and allow flexibility in the design

4.A.4: Maintainability performance is validated and optimized during operations based on available maintenance data

4.A.4.A: Establish capabilities and processes to collect and store operational history, health status, degradation, diagnostic, and maintenance data

4.A.4.B: Periodically analyze test and operational history, health status, degradation, diagnostic, and maintenance data to determine maintainability performance and trends

4.A.4.C: Periodically review and update maintenance strategy and activities

4.A.4.D: Ensure availability of data to future programs and projects

Acknowledgments

This research was carried out at NASA HQ and at the Jet Propulsion Laboratory, California Institute of Technology under a contract with the National Aeronautics and Space Administration, sponsored by the NASA Office of Safety and Mission Assurance. This activity was managed locally at JPL through the Assurance and Technology Program Office.

References

[1]Evans, J., Cornford, S., and Feather, M. S., "Model Based Mission Assurance (MBMA): NASA's Assurance Future," *2016 Annual Reliability and Maintainability Symposium (RAMS)*. IEEE, 2016.

[2]Cornford, S. L., and Feather, M. S., "Model Based Mission Assurance in an MBSE Framework: State-of-the-Art Assessment," NASA/CR-2016-219272, 2016.

[3]Groen, F. J., Evans, J., and Hall, A. J., "A Vision for Spaceflight Reliability: NASA's Objectives Based Strategy," *2016 Annual Reliability and Maintainability Symposium (RAMS)*. IEEE, 2016.

[4]Kelly, T., and Weaver, R., "The goal structuring notation–a safety argument notation," *Proceedings of the dependable systems and networks 2004 workshop on assurance cases*. 2004.

[5]Habli, I., and Kelly, T., "Balancing the Formal and Informal in Safety Case Arguments," *VeriSure: Verification and Assurance Workshop*, colocated with Computer-Aided Verification (CAV), 2014.

[6]Witulski, A., Austin, R., Evans, J., Mahadevan, N., Karsai, G., Sierawaski, B., and Reed, R., "Goal Structuring Notation in a Radition Hardening Assurance Case for COTS-Based Spacecraft," *GOMAC Tech 2016 Government Microcircuits Applications and Critical Technologies Conference*. IEEE, 2016.

[7]Aguilar, M, L., "Assess/Mitigate Risk through the Use of Computer-Aided Software Engineering (CASE) Tools," NASA/TM-2013-218031, 2013.

[8]Karban, R., Andolfato, L., Bristow, P., Chiozzi, G., Esselborn, M., Schilling, M., Schmid, C., Sommer, H., and Zamparelli, M., "Model Based Systems Engineering for Astronomical Projects," *SPIE Astronomical Telescopes+Instrumentation. International Society for Optics and Photonics*, 2014.

[9]Dezfuli, H., Benjamin, A., Everett, C., Feather, M., Rutledge, P., Sen, D., & Youngblood, R., "NASA System Safety Handbook. Volume 2: System Safety Concepts, Guidelines, and Implementation Examples," NASA/SP-2014-612, 2014.

[10]Do, Q., Cook, S., & Lay, M., "An investigation of MBSE practices across the contractual boundary," *CSER 2014*, Redondo Beach, CA, March 2014.

[11]"Standard for Models and Simulations," NASA-STD-7009, 2009.

[12]Hecht, M., Dimpfl, E., & Pinchak, J., "Automated Generation of Failure Modes and Effects Analysis from SysML Models," *2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. IEEE, 2014.

[13]David, P., Idasiak, V., & Kratz, F., "Improving Reliability Studies With SysML," *Reliability and Maintainability Symposium (RAMS)*. IEEE, 2009.

[14]Cressent, R., David, P., Idasiak, F., & Kratz, F., "Dependability analysis activities merged with system engineering, a real case study feedback," *Advances in Safety, Reliability and Risk Management*: ESREL 2011.

[15]Wang, L., Izygon, M., Okon, S., Bareh, M., Castet, J-F., Nunes, J., & Fesq, L., "Model Based System Engineering Methodology for Fault Management System Design" *NASA/JPL Symposium and Workshop on Model-Based System Engineering*, Pasadena, CA; 2015.

[16]Sargusingh, M. K., Callahan, M. R., & Okon, S., "Cascade Distillation System Design for Safety and Mission Assurance," *45th Int. Conf. on Environmental Systems*, Bellevue, Washington, 2015.

[17]J-F Castet et al, "Ontology and Modeling Patterns for State-Based Behavior Representation," *AIAA SciTech*, Kissimmee, FL, 2015.

[18]Gruber, T. R., "A translation approach to portable ontology specifications," *Knowledge Acquisition*, 5 (2), 1993.

[19]Aguilar, M., Bonanne, K,. Favretto, J. A., Jackson, M. M., Jones, S. L., Mackey, R. M., Sarrel, M. A., and Simpson, K. A., B. M., Claver, C., and Angeli, G., "Review of Ground Systems Development and Operations (GSDO) Tools for Verifying Command and Control Software." NASA/TM-2014-218278, June 2014.

[20]Cressent, R., David, P., Idasiak, F., & Kratz, F., "Increasing Reliability of Embedded Systems in a SysML Centered MBSE Process: Application to LEA Project," *1st M-BED workshop*, during DATE 2010, Dresden, Germany, 2010.

[21]Fernández, M. M. "Using AADL to Enable MBSE for NASA Space Mission Operations" *SpaceOps Conference*, Pasadena, 2014.

[22]Selvy, B. M., Claver, C., and Angeli, G., "Using SysML for Verification and Validation Planning on the Large Synoptic Survey Telescope (LSST)," *SPIE Astronomical Telescopes + Instrumentation*, pp. 91500N-91500N. International Society for Optics and Photonics, 2014.

[23]Wibben, F. R., and Furfaro, F., "Model-Based Systems Engineering approach for the development of the science processing and operations center of the NASA OSIRIS-REx asteroid sample return mission," *Acta Astronautica* 115, 2015, 147-159.

[24]Liebel, G., Marko, N., Tichy, M., Leitner, A., and Hansson, J., "Model-based engineering in the embedded systems domain: an industrial survey on the state-of-practice," *Software & Systems Modeling*, 2016. 1-23.

[25]Lin, C., Fradet, R., and Dvorak, D., "NASA/JPL Symposium & Workshop on Model-Based Systems Engineering" Jan. 2015.