Reliability Analysis of Complex NASA Systems with Model-Based Engineering

Nancy J. Lindsey, Mahdi Alimardani, and Luis D. Gallo
Goddard Space Flight Center, Greenbelt, MD 20771

Key Words: Reliability, FMEA/FMECA, Risk Assessment, Fault Tree, Reliabilty Prediction, Reliability Block Diagram, Probabilistic Risk Assessment, Limited Life Items, Model-Based Mission Assurance, NASA, Goddard Space Flight Center

SUMMARY & CONCLUSIONS

The emergence of model-based engineering, with Model-Based Systems Engineering (MBSE) leading the way, is transforming design and analysis methodologies. [7] The recognized benefits to systems development include moving from document-centric information systems and document-centric project communication to a model-centric environment in which control of design changes in the life cycles is facilitated. In addition, a "single source of truth" about the system, that is up-to-date in all respects of the design, becomes the authoritative source of data and information about the system. This promotes consistency and efficiency in regard to integration of the system elements as the design emerges and thereby may further optimize the design. Therefore Reliability Engineers (REs) supporting NASA missions must be integrated into model-based engineering to ensure the outputs of their analyses are relevant and value-needed to the design, development, and operational processes for failure risks assessment and communication.

Effective model-based Reliability must be analyst/ modeler-agnostic while still efficiently producing complete, accurate, and more consistent Reliability Artifacts (e.g., Failure Modes, Effects, and Criticality Analysis (FMECA), Limited Life Analysis (LLA), Fault Tree Analysis (FTA), Maintainability/Availability Analysis and Probabilistic Risk Assessment (PRA)) than traditional methods to allow engineers greater time for analysis, risk assessment, system behavior investigation (simulation), and risk-based project decision-making support. However, to achieve this, a robust and unified modeling process that includes considerations from all disciplines must be developed, implemented, and tested.

In order to include Reliability, a discipline of Mission Assurance, in the development of this unified modeling process, an agency-sponsored team at Goddard Space Flight Center (GSFC) has completed the Reliability study of modeling and testing as part of the Model-Based Safety and Mission Assurance Initiative (MBSMAI). In this study, GSFC Reliability experts developed models of mission subsystems (EUROPA Propulsion, Wallops Flight Facility (WFF) Sounding Rocket Attitude Control System (ACS), & International Space Station (ISS) Evaporator) using a representative Commercial Off-The-Shelf tool, MADe (Maintenance Aware Design environment from PHM Technology-Siemens), and SysML/ MagicDraw (Systems Modeling Language (SysML) based tool from NoMagic) that was supported by Reliability plugins from Tietronix Software Inc. These models and their ability to support Reliability Analysis were then evaluated for accuracy, consistency, and efficiency to better connect and define MBSE/MBSMA modeling process best practices and modeling environment necessities that support traditional SMA analyses and milestone artifact generation so that failure risks can be assessed and communicated.

Model-Based Engineering is found to be valid and useable for Reliability Engineering for NASA Safety and Mission Assurance if adequate modeling processes and environment are established.

Therefore, this study recommends that NASA use a structure modeling environment that promotes consistency, accuracy, and efficiency (See Section 4) and that modelers within NASA follow this recommended MBSMA process: 1) Establish a multi-discipline modeling team (Systems Engineering (SE) and Safety and Mission Assurance (SMA) at a minimum); 2) Establish modeling responsibilities (e.g., SE's model requirements, Designer's model structure (Functional Block Diagram/Wire Diagram), REs model failure behaviors and characteristics) and controls; 3) Complete modeling and share common data between modelling elements; 4) Produce Reliability artifacts and share resulting data between modelling elements; 5) Verify and refine modelling (and designs) until a final and acceptable result is achieved; and 6) Share modeling with future missions.

These results are being used by NASA to advance the guidance on the modeling scope and depth needed for SMA analysis compatibility, to establish SMA-to-SE/SE-to-SMA modeling collaboration and transition points, potentially reshape traditional products as required while still identifying the risks to the system performing as required over its lifecycle to satisfy mission objectives, and advance Model-Based tool capabilities. However, these results are based solely on Reliability discipline needs and were derived from small systems so it is also recommended that this study continue to test additional SMA disciplines and more complex systems as planned (See Section 5).

1 BACKGROUND

"Reliability engineering provides the theoretical and practical tools whereby the probability and capability of parts, components, products and systems to perform their required functions in specified environments for the desired period of operation without failure" is assessed. [9]

1.1 Reliability Engineering

Reliability engineering at NASA/GSFC involves risk assessment and analyses, to assess and manage mission "lifetime" engineering risks of failure, failure recovery, and the identification of mitigations/corrective actions and their impacts. Although stochastic parameters define and affect reliability, reliability engineering is not solely mathematics and statistics (Probability Analysis (PA)); it also is the analysis of risks through Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Limited Life Analysis (LLA), Single Point Failure Analysis, Availability/ Maintainability Analysis, and Probabilistic Risk Assessment (PRA). As a result this SMA discipline is an integral part of NASA/GSFC's Continuous Risk Management (CRM) (See Figure 1). In continuous risk management risks are identified and analyzed/ researched then a plan is developed to handle (e.g., mitigate, watch, accept, or escalate) the risks and ultimately the risks are monitored for occurrence and or modification.

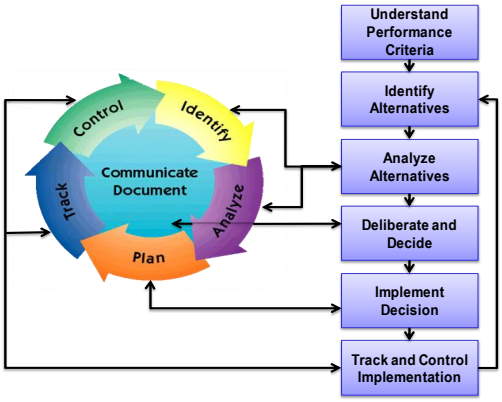

Figure 1- RIDM-CRM Risk Management Process Flow [1]

2 TEST METHODOLOGY

The test methodology used to assess MBSMA for Reliability was to target analysis types for this initial evaluation phase that are commonly used on all mission classes (FMECA, FTA, LLA, PA) to enable complete evaluation and the production of artifacts, initial findings on quality and compatibility with risk assessment and hazard reporting, and modeling guidance within the relatively short time period of this study. Test case scope was also limited to one subsystem for each model for the same reason while the types of missions and subsystems were varied (1 Mechanical subsystem for a robotic mission, 1 Electronic subsystem for a sounding rocket, and 1 Electromechanical subsystem for a human mission) to avoid bias or limitations in findings and/or guidance. Additionally, PRA and Availability/Maintainability Analyses were excluded from this study since these analyses are highly dependent on the Fault Tree (FT) and PA results (that were already being studied), the PRA's inherent complexity, and the data needs of Maintainability/Availability that are not supported by the limited test cases of this study. Whereas a more expansive test case of an entire observatory/mission or serviceable system would enable these additional analyses to be addressed and provide sufficient evaluation insights.

2.1 Modeling Tools Utilized

Although there are many model-based tools and plugins available for MBSEs to use today only some have specific Mission Assurance (Reliability, Safety, Quality, and Software Assurance) functionality. This team found these to be IBM Rational Rhapsody, SysML/MagicDraw with plugins (Cameo Safety and Reliability Analyzer, and/or Tietronix Reliability plugins (FaultTree, FMECA)), WebGME.org, SEAM/ modelbasedassurance.org, Methodology Wizards, Model Obfuscator, Product Line Engineering, Eclipse Papyrus, and local custom-designed plugins), MADe, SCADE Suite, Reactis Suite, and PTC's model-based systems engineering solution (Windchill Modeler, Windchill Asset Library & Windchill Process Director). While this tool set is not huge it would be impossible to model, evaluate, and develop recommendations based on each in this study. Therefore the study team selected two representative tools based on MBSE utilization, apparent ease of use, and the breadth of assurance discipline coverage. The first being SysML/MagicDraw (A Systems Modeling Language (SysML) based tool from NoMagic) with Tietronix Reliability plugins and the second being Maintenance Aware Design environment (MADe).

2.1.1 MADe

The modeling tool Maintenance Aware Design environment (MADe) provides a suite of software tools that can be used to design, assess and optimize Prognostics and Health Management systems for use in a wide variety of high-risk industries where safety and reliability are critical, using model-based engineering techniques. The MADe modelling environment, shown in Figure 2, provides specific analysis workflows for reliability, including Reliability Allocation, Reliability Block Diagrams, Markov Analysis, and Reliability/Availability Analysis with multiple failure distribution methodologies to produce and validate the reliability requirements for a system at each stage of the design process. These analyses allow for on-demand generation of FMEA, FMECA, and Common Mode Analysis and Functional Fault Tree Analysis reports.

A MADe model of a system uses a graphical Functional Block Diagram and automates the propagation of functional failures in a system to establish syndromes or signatures of failure based on the underlying physics of failure. This information is used to generate and optimize diagnostic sensor placement based on the probability of detection (PoD) of potential failures. Additionally the propagation and sensor information can be utilized to ensure Fault Detection and Isolation and life/maintenance/diagnostic rule implementation is balanced with cost, weight, risks, and produce diagnostic rules based on the selected combination of sensors.

.

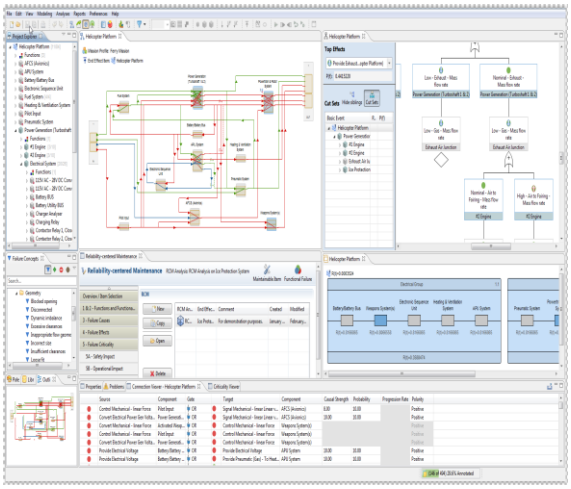

Figure 2 – MADe Modeling Environment [3]

2.1.2 SysML/MagicDraw

This study's Systems Modeling Language (SysML/ MagicDraw) modeling tool (v19.0), was an extension of UML 2.0, with Tietronix plug-ins (FaultTree (18.0), FMECA (18.0), MBSE Plugin (18.0), Methodology Wizards (19.0SP2), Model Obfuscator (19.0), & Product Line Engineering (19.0SP2)) designed to support modeling for System Engineering and Reliability. It is a general purpose graphical modeling language for analyzing, designing and verifying complex systems that may include hardware, software, information, personnel, procedures and facilities. A SysML system model consists of Functional/Behavioral Model, Performance Model, Structure/Component Model, and Other Engineering Analysis Models (Figure 3) to integrate system requirements with engineering disciplines. In order to perform SMA analyses the SysML plugins of FMECA, FTA, and PRA (developed by NoMagic, CAMEO, Tietronix, and modeling teams) must be executed against the SysML system model.

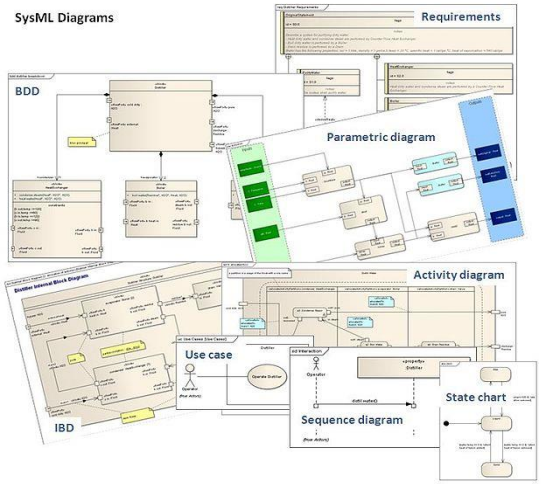

Figure 3: SysML Diagrams [2]

3 TEST CASES AND RESULTS

3.1 EUROPA Propulsion (Mechanical) Test Case

The EUROPA propulsion subsystem, shown in Figure 4, provided by GSFC, will be used on a Europa Flyby Mission spacecraft to the Jupiter system to perform repeated close flybys of the giant planet's large moon Europa to investigate its potential habitability. The spacecraft would collect information on Europa's ice shell thickness, composition and surface geomorphology.

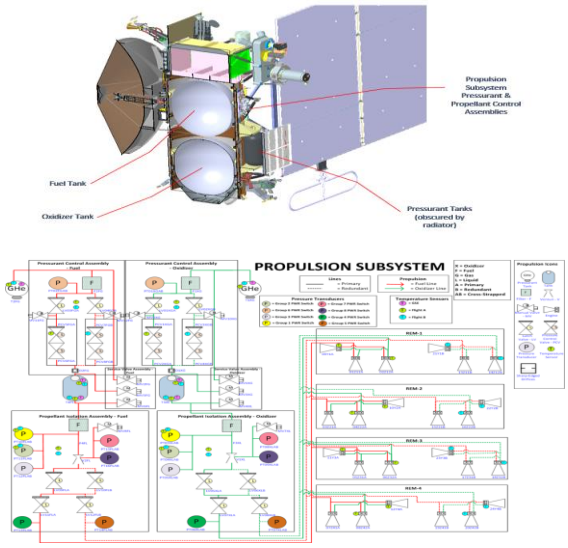

Figure 4 – EUROPA Propulsion System [8]

When modelled in MADe the Europa Propulsion model consists of 9 main functional block diagrams, 1 at System level and 8 at Subsystem level. For instance, the Propellant Isolation Fuel Assembly Model consists of 13 components, 8 of which had their functions and flows manually defined and the remaining 5 components were modeled using predefined components already available in MADe Pallete library and modified to represent the functions and other parameters of our interest. Each of these 13 components is supported by a failure diagram that contains all potential failure modes, effect, causes, and detection and compensation factors. In addition to these components that have a failure diagram, all other components that are being analyzed at their lowest level should contain a failure diagram. As modelled, the electrical failure mechanisms and causes in the propulsion components were auto populated by MADe as a default on the failure diagrams; mechanical failure mechanisms needed to be added to the library component failure diagram manually (one time operation). All subsystem blocks in the Propulsion model, including the Propellant Isolation Fuel Assembly, Propellant Isolation Oxidizer Assembly, Pressurant Control Fuel Assembly, Pressurant Control Oxidizer Assembly, and Engine Assemblies include failure diagrams for all the components within them. Having functions and flows defined at every level is necessary, as the failure propagations carry over to the next level using the predetermined flows, according to the propagation logic between model levels.

When modeled in SysML/MagicDraw the Europa Propulsion model does not have multiple Functional Block Diagrams, like the MADe model; instead it uses multiple State Machine Diagrams to define the system. In this test case a wiring diagram developed during modeling was used by the modeler to understand what State Machines would be required. Therefore 24 state machines, along with their corresponding states were defined and functions, causes, immediate effects and signals were allocated to every state machine diagram to define the propulsion model. While a Wiring Diagram can be helpful to the modeler to represent actual connectivity pattern of the component it is not connected to the State Machines and it is not necessary for the purpose of generating Reliability artifacts. [10]

3.2 Sounding Rocket (Electronic)Test Case

A sounding rocket test case was selected to model the Celestial ACS (CACS) Subsystem of a Wallops Flight Facility Sounding Rocket as defined in the Wallops Sounding Rocket Handbook [4]. A sounding rocket carries experiments to altitudes between 50 and 1,500 km and flies nearly parabolic trajectories while its Celestial ACS is used to align sounding rocket payloads towards celestial targets. This attitude control subsystem is used for flights investigating targets that can either be acquired and tracked with a star tracker or pointed at by using nearby celestial targets as a reference. The subsystem is composed of the elements shown in the Figure 5.

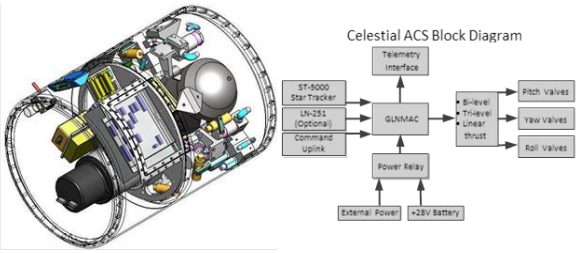

Figure 5 – Sounding Rocket Subsystem [10]

Therefore the Sounding Rocket MADe model consists of 4 main functional block diagrams, one at the System level, two at the Subsystem and one at the component level for CASC. The CASC Model consists of 12 components, 5 of which had their functions and flows manually defined while the remaining 7 components were modeled using predefined components already available in the MADe Pallete library and modified to represent the functions and other parameters of our interest. Each of the 12 components, is supported by a failure diagram that contains all potential failure modes, effects, causes, detection, and compensation factors. These failure diagrams were then used by the MADe analysis engine to derive parent failure relationships. No intermediate or parent failure diagrams were needed since MADe rolls-up failure characteristics from the lowest level modelled. Consequently, to complete the model the other subsystems in the Payload that were not decomposed, the Telemetry System, Recovery System and Instrument Block, and the Rocket Engine and its three forming subsystems; Boost Guidance, Stage I and Stage II Engine, also had a failure diagram assigned to them. While functions and flows were defined at every level so that the failure propagations are carried to the next level using MADe's propagation logic. [10]

As noted in the in Europa modelling section, the Sounding Rocket SysML/MagicDraw model does not include multiple Functional Block Diagrams. Instead a Block Definition Diagram (BDD), which defines the "Ownership" of the created blocks and shows the hierarchical relationship of blocks and 20 State Machines were defined to represent the Sounding Rocket. The model's Block Definition Diagram was helpful to the modeler to represent actual connectivity patterns of the components but it is not connected to the State Machines directly and it is not necessary for the purpose of generating Reliability artifacts in SysML/MagicDraw. Conversely in SysML/MagicDraw are essential to conducting Reliability analyses in SysML/MagicDraw. Therefore the state machines of the Sounding Rocket model (20), along with their corresponding states were defined and functions, causes, immediate effects and signals were allocated to every state machine diagram in a similar way to traditional FMECA generation. Next level effects were then automatically carried over to the subsequent level using the signal element and the results are shown in a FMEA column. Probability of failure was assigned to every cause (Operations Element) and the plugin calculated the P*f* using the Boolean Logic. [10]

3.3 ISS-Evaporator Test Case

The ISS-Evaporator test case used a JSC developed SysML model of a design solution for ISS (International Space Station) brine evaporation (CapiBRIC - Capillary-Based Brine Residual In-Containment) [5, 6] to further model and test. The CapiBRIC system uses unique containment geometry, capillary flow, and static phase separation to enable water evaporation in a microgravity environment. CapiBRIC contains a capillary drying unit within a drying chamber (See Figure 6). This design allows water to be recovered from the clean water vapor evaporating from the free surfaces while leaving waste brine solids behind. In this way CapiBRIC is designed to help mitigate limitations of the current ISS water recovery system that causes unfeasible water storage issues for long duration space missions.

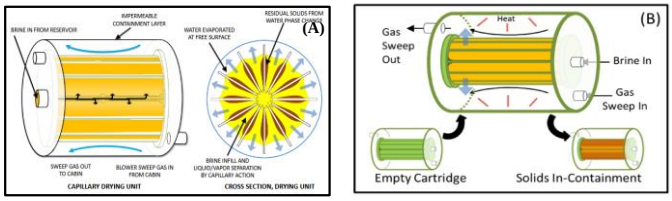

Figure 6 – ISS- Evaporator System (CapiBRIC) [5, 6]

The CapiBRIC SysML model in MagicDraw provided by JSC consisted of a Block Definition Diagram, a wiring Diagram and 13 state machines for the air outlet, blower, inlet assembly, reservoir, tray, filters, heaters, shells and controls with corresponding states (nominal, intermittent and/or failed states), functions, causes, immediate effects and signals to define the system in a model. In addition, a probability of failure was assigned to every cause (Operations Element) and

Criticality Levels (1-10) were assigned to every potential effect to calculate the level of risk in the failure case.

For testing purposes, when the ISS CapiBRIC was modelled in MADe a limited model was developed that consisted of 1 main functional block diagram and 1 failure diagram. As in other MADe models the 17 components of the functional block diagram, were modeled using predefined components and modified to represent the functions, flows and other parameters of interest. Additionally a single failure diagram of the inlet filter of the CapiBRIC system was added, containing all potential failure modes, effect, and causes to enable Reliability testing.

3.4 Reliability Analysis Compatibility Evaluations

3.4.1 MADe

The MADe models generated in this study show that it is possible to generate accurate predictions, consistent FMECA reports, logical Fault Trees, and expected Availability/ Probability Analysis results from a single set of model-based information given adequate tool computational support. Further study participants found the MADe tool's Reliability reports corresponded well to traditional reliability artifacts as shown below and in Reference 10.

I. MADe FMECAs were generated at the system and fully decomposed levels using a simple override/mode setting. MADe FMECAs were found to correspond relatively well with traditional artifacts in content and format once optional mission specific narratives were added. While consistent with traditional artifact format, the MADe FMECA has different Severity and Likelihood ratings from the GSFC 5x5 risk definitions, however post report generation corrections or specific rating selection rules or vendor NASA/GSFC customization can mitigate this issue. In addition, there is currently no CIL/FT or SPF report from MADe (but one is planned) but the viewer function can be used to generate a CIL report separately and the SPFs can manually be extracted from the FMECA table. Even given these caveats the MADe FMECAs were found to be valid for Reliability discipline use.

II. MADe fault trees are derived from the functional block diagram model and/or reliability block diagram (RBD), which helps ensure that the fault tree will be consistent with the RBD/functional block diagram. MADe is capable of generating 2 types of fault trees: Hardware and Functional but neither's report is automated and they are limited to some extent. For example MADe will only quantify the top 10 - 50 cut sets in terms of probability of failure in its hardware-based fault tree. MADe Hardware Fault Trees will also show unnecessary intermediate OR gates if grouping of components is used in the RBD, but this can be eliminated by simply adjusting how components are grouped. Even with these limitations. MADe Hardware FTs produced in this study were found to be consistent with GSFC's traditional FTs and had accurate Boolean logic, which should make them transferrable to other reliability tools like Sapphire or PTC Windchill Quality Solution (WQS). While MADe's Functional FTs of this study were found to correctly indicate the system's failure responses based on the functional dependencies (Flows) established in the model, they were not formally evaluated in this study.

III. MADe Probability Analysis results show that MADe RBD prediction results match to about 5 decimal places with the traditional method on a component per component basis and mission life probabilities compared favorably if the duration and duty cycles assumed for each are the same. In addition the probability of failure reported in the system fault tree module corresponds to the probabilities reported by the MADe Probability Analysis /RBD module. However, the calculations for applying environmental/ temperature/stress factors for deriving failure rate based can only be based on MIL-HDBK-217F (217F) or manually entered at this time.

IV. MADe Availability was tested in lieu of life analysis since MADe has built in operational availability capability. A small 4 antenna test case model was created so that results could be verified with traditional calculations. This model was built much like a reliability block diagram, where each component was defined with common failure distributions (Exponential or Weibull) and mean down time. Results showed that there would be 1000 hour mean down time and 1million hour MTTF for each antenna which matched previous traditional calculations. However, these values were generated by analytical method and not simulation so mean down time is a point estimate (i.e. single value as opposed to distribution). Thus the complexity of the Availability calculation is less than current reliability tools. (e.g., Raptor) but could be useful in maintenance planning.

In this study it was observed that MADe does not currently have the following abilities but it does have a Maintenance Cost and Task Analysis and Prognostics and Health Monitoring Reliability support capabilities that will need to be tested in a later phase of this study:

- An import/export of failure rates from parts lists.
- A method to connect requirements directly to Reliability artifacts.
- Limited Life Analysis (LLA) report but this may be derived from elements of the maintenance analysis capability that is yet untested.

3.4.2 SysML/MagicDraw

The SysML/MagicDraw models generated with the Tietronix plugins in this study showed that it is possible to generate functional or failure causality Fault Trees with probabilities and Functional FMECAs. Study participants found:

I. SysML/MagicDraw FMECAs were generated at the system, and all other lower levels using Tietronix FMEA Plugin. MagicDraw/Tietronix generated FMECAs were found to correspond well with traditional artifacts in content and format when the state machines were defined accordingly. Therefore this study's state machines were optimized for FMECA outputs, but this was found to adversely impact FT artifacts due to state machine interdependency; and Severity and Likelihood ratings were added to the Effects to match the GSFC 5x5 risk definitions. However, the generated SysML/MagicDraw FMECA reports are limited to a single format but can be edited manually outside the model to clarify effects for further use. Conversely, there is currently no CIL or SPF report available but data may be deduced from the FMECA worksheet. Even with the state-machine inter-dependency and report limitations SysML/MagicDraw FMECAs were found to be a sufficient for Reliability discipline use.

II. SysML/MagicDraw Fault Trees are derived from failure effects stereotyped for each component and the relations and hierarchies are obtained from the transition lines and allocated signal defined in every state machine diagram. However, the artifacts of this study indicate that these Fault Trees contain Boolean logic errors (i.e., events decomposed into subordinate events without a combining logic or gate, and logic gates with only one input) that will need correction outside the model for Reliability discipline engineers to use for further analysis. In addition, since this study's state machines were optimized to produce an accurate FMECA, the fault tree output was found to be hardware/ subsystem-function-based versus component/hardware-failure based as is traditional for GSFC Reliability. In order to change the output to be hardware-style or traditional with component failure rates, a second set of state machines, model, or truth would have to be created. This is not the case for MADe, since it produces both functional and hardware fault trees from the information in the reliability block diagram and the functional block diagram.

III. SysML/MagicDraw Probability Analysis can only be performed using the PRA option of the Tietronix FTA module. Therefore quantifications are per failure cause and allocated to each transition line at the lowest level. Study results show that Tietronix FT Boolean math calculated the next higher-level probability of failures accurately using the lower level P*f* inputs. Overall MagicDraw FTAs quantifications were found valid for Reliability discipline use. However, component per component and mission life probabilities were not available.

This study also found that SysML/MagicDraw with Tietronix plugin does not currently support:

- RBD analysis capability so that probability prediction at the component and system level can be estimated.
- Life analysis support capabilities so that Limited Life Analysis (LLA) can be performed.
- Critical Items List (CIL) support capabilities for full FMECA functionality.
- Maintainability or Availability Analysis

4 DISCOVERIES & RECOMMENDATIONS

Based the modeling results and experiences in this study the following is found:

1) Model-Based functional models need more details than traditional block diagrams to make them complete (e.g., Propulsion Latch Valves need power/command inputs and telemetry outputs to fully characterize their functionality and a traditional block diagram may not have this level of detail in just one source).

2) The lack of standardization and framework within any modeling environment will provide more liberty in the modeling process to generate findings/results/artifacts but the results may not necessarily be accurate when done by discipline engineers and "Modeling Expert" intervention may be required as an additional step to ensure accuracy and consistency. Although this additional step may increase the confidence in the model it is in contradiction with other goals of Model-Based Engineering to reduce time and cost factors.

3) The optimal modeling environment for Systems Engineering and Mission Assurance should be developed or purchased and include:

- Support for the development of models from the traditional reliability artifacts rather than only deriving the artifacts from the models for efficiency via model re-use.
- An easily mastered structure and interface for efficiency.
- The ability to create a functional model of the systems for efficiency and clarity.
- The ability to ensure that changes to one diagram (e.g., adding a component) propagates to other parts/diagrams of the model automatically or at least shows as an error that needs to be resolved by the modeler.
- The ability to allocate requirements to a functional diagram/element for consistent and accurate effect assessment.
- Libraries of standard components with baseline failure and function data for consistency and accuracy.
- Libraries of standard failure mechanisms and causes for efficiency.
- The ability to add models of systems or portions of systems to a library of shareable models for efficiency.
- The ability to import results (e.g., radiation effects, life expectancy data, traditional analysis data) from other models or sources for efficiency and accuracy.
- The ability to combine models and duplicate modeling for efficiency.
- Model component and system error checking for accuracy.
- Model change control/reporting for accuracy.
- The ability to import requirements, CAD and BOM/part lists type data to create modeling elements or as supporting data for efficiency.
- The ability to select requirements allocated to each element as the effects and functions for accuracy and efficiency.
- An export function to other modeling formats and reliability tools (e.g., Windchill Prediction tool (Relex), Saphire, QRAS, etc.)
- Modeling diagrams that connect hierarchically to each other for efficiency and clarity which will allow non-modelers to easily traverse and drill down within the model for understanding and accuracy validation.
- The ability to produce a FMECA with NASA defined levels and characterization factors.
- The ability to produce a Fault tree with precise Boolean logic for accuracy.
- The ability to produce life assessments at the component and system level.
- The ability to perform availability assessments at the component and system level.
- The ability to perform maintainability assessments interconnected with maintenance/sparing plans at the component and system level.
- The ability to perform probability analysis using at least 217F, Telecordia, FIDES, PRISM, and/or enterprise custom databases. Or import data from reliability tools (e.g., Windchill Prediction tool, etc.) for accuracy and efficiency.
- Performance that shortens analysis time while maintaining consistency and accuracy between models.

4) Modelling process and controls are needed prior to generating any models to ensure model accuracy. Therefore it is recommended that the following modeling process guidance has been developed by this initiative: 1) Establish a multi-discipline modeling team (Systems Engineering (SE) and Safety and Mission Assurance (SMA) at a minimum); 2) Establish modeling responsibilities (e.g., SE's model requirements, Designer's model structure (Functional Block Diagram/Wire Diagram), REs model failure behaviors and characteristics) and controls; 3) Complete modeling and share common data between modelling elements; 4) Produce Reliability artifacts and share resulting data between modelling elements; and 5) Verify and refine modelling (and designs) until a final and acceptable result is achieved; and 6) Share modeling with future missions.

5 CONCLUSIONS & PATH FORWARD

Model-Based Engineering is found to be valid and useable for Reliability Engineering for NASA Safety and Mission Assurance if adequate modeling processes and environment are established. It should be noted that every organization employing model-based engineering for design, SMA, systems engineering, and project management, including NASA, must decide for itself how to implement model-based engineering in a way that makes sense for all their engineering, assurance, operational, and production elements. However, this study concludes that it is essential to involve the subject matter experts from each element as early as possible to avoid developing or buying model-based tools or strategies that lead to misleading or invalid results.

Therefore these results and recommendations are being used by NASA to advance the guidance on the modeling scope and depth needed for SMA analysis compatibility, to establish SMA-to-SE/SE-to-SMA modeling collaboration and transition points, potentially reshape traditional products as required while still identifying the risks to the system performing as required over its lifecycle to satisfy mission objectives, and advance Model-Based tool capabilities.

For this reason GSFC plans, with their Headquarters sponsor, to execute 2 more phases of this study to assist NASA/GSFC to develop a unified Model-based engineering approach and determine the best tool set to support that approach. The first being Phase 2 in which evaluations and testing will consist of follow-on Reliability evaluations with more complex system/model (e.g., CubeSat Mission) to enable more multifaceted reliability (e.g., Life, Maintainability/ Availability, Probabilistic Risk Assessment) and Safety Analyses. While Phase 3 will evaluate Software Assurance and Quality Engineering Analysis compatibility.

REFERENCES

[1] "Goddard Procedural Requirements for Risk Management; GPR 7120.4D," Code 300/Safety and Mission Assurance Directorate, Goddard Space Flight Center, Greenbelt, MD, USA, 2012.

[2] "Systems Modeling Language," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Systems_Modeling_Language. [Accessed 15 Apr 2019].

[3] "MADe Software Official Website," PHM Technology, [Online]. Available: https://www.phmtechnology.com/. [Accessed 21 Jan 2019].

[4] "NASA Sounding Rockets User Handbook," Sounding Rockets Program Office, Sub-orbital and Special Orbital Projects Directorate, Wallops Island, VA, USA, 2015.

[5] M. J. Sargusingh, S. Pensinger and M. R. Callahan, "CapiBRIC – Capillary-Based Brine Residual In-Containment for Secondary Water Recovery," EISD Technology Showcase, 2015.

[6] M. R. Callahan and M. J. Sargusingh, "Design Status of the Capillary Brine Residual in," in 46th International Conference on Environmental Systems, Vienna, Austria, 2016.

[7] S. Friedenthal, R. Griego and M. Sampson, "INCOSE Model Based Systems Engineering (MBSE) Initiative," in INCOSE 2007 Symposium, San Diego, CA, USA, 2007.

[8] "EUROPA Propulsion Critical Design Review Package (EUROPA-PROP-REVW-0006)," GSFC EUROPA Project, Greenbelt, MD, USA, 2018.

[9] D. B. Kececioglu, Reliability Engineering Handbook, vol. 1, Lancaster, PA, USA: DESTech Publications, Inc., 2002.

[10] N. J. Lindsey, M. Alimardani and L. D. Gallo, "GSFC/NASA Model-Based SMA Initiative Phase 1 Report: Reliability," GSFC Risk & Reliability Branch, Greenbelt, MD, USA, 2019.

ACKNOWLEDGEMENT

We thank sponsors John Evans and Anthony DiVenti, NASA Headquarters, for their support, insights, and funding this research.

BIOGRAPHIES

Nancy J Lindsey
Goddard Space Flight Center (Code 371)
8800 Greenbelt Road
Greenbelt, MD 20771 e-mail: nancy.j.lindsey@nasa.gov

Nancy J. Lindsey has spent 30+ years in aviation and aerospace engineering performing a variety of reliability, assurance, and systems engineering tasks across the entire gamut of space vehicle life cycles and program types including Defense and Commercial Communications Missions, Space-based Astronomical Observatories, and Earth Science Monitoring Systems. She is a recognized innovator at GSFC based and is currently the Branch Head for the Risk & Reliability Branch at the NASA GSFC in Greenbelt MD. She has a Bachelor of Science degree in Computer Science & Aeronautical Engineering and a Master's of Science degree in Space Studies. Nancy's independent research efforts can be viewed via website: www.rcktmom.com.

Mahdi Alimardani
Goddard Space Flight Center (Code 371)
8800 Greenbelt Road
Greenbelt, MD 20771 e-mail: mahdi.alimardani@nasa.gov

Mahdi Alimardani is a Reliability Engineer at NASA Goddard Space Flight Center. He has experience working for different companies in aviation and aerospace segments. At NASA he has worked on various NASA missions including; Earth Observing System (EOS) Extended Mission Operation, PACE and Landsat 9 Earth Observing Satellite mission and Lucy Space Exploration Mission as reliability Engineer and is the reliability lead for the L'Ralph Instrument. Mr. Alimardani is currently pursuing his Doctorate in Industrial and Systems Engineering.

Luis Gallo
Goddard Space Flight Center (Code 371)
8800 Greenbelt Road
Greenbelt, MD 20771 e-mail: luis.d.gallo@nasa.gov

Luis Gallo has spent 10 years in aerospace engineering and is the lead reliability engineer for the Europa Propulsion Subsystem and Co-Lead on the Model-Based Safety and Mission Assurance effort at the Goddard Space Flight Center. Mr. Gallo has a Bachelor of Science degree Electrical Engineering from Florida International University.