# System Safety Analysis of Complex NASA Systems with Model-Based Engineering

Nancy J. Lindsey, Miranda Cooter, Austin M. Hodges and Nobel Sindjui;
Goddard Space Flight Center, Greenbelt, MD 20771

Key Words: Hazard Analysis (OHA/O&SHA), Hazard Fault Tree, Model-Based Mission Assurance, Range Safety, Maintenance Aware Design environment (MADe), SysML/MagicDraw

**ABSTRACT**

The emergence of model-based engineering is transforming design and analysis methodologies [5]. A recognized benefit of model-based engineering is the existence of a "single source of truth" about the system that becomes the authoritative source of data and information for designers, analysts, and developers. This promotes consistency and efficiency as the design emerges and can be used to further optimize the design. Integrating System Safety Engineers to the "single source of truth" will ensure that the outputs of their assessments and analyses are relevant to the design as it evolves. Use of an integrated system model enables near immediate evaluation of a design change as well as development of operational processes for risk assessment and communication. Such models can enable efficient and timely analysis of system hazards (e.g., hazard fault tree analysis and procedure simulations) and produce complete, accurate, and more consistent products (e.g., hazard reports and safety requirement evaluations).

Therefore, an agency-sponsored team at Goddard Space Flight Center (GSFC) recently completed a System Safety Study of modeling and testing capabilities as part of a Model-Based Safety and Mission Assurance Initiative (MBSMAI). Using an existing model developed for reliability analyses [1], GSFC modeling and system safety experts performed system safety analysis/modeling and produced safety products. The team evaluated model-based feasibility to support System Safety Engineering, developed safety analysis modeling processes, and identified tool capability advancement/development needs. These study results indicate *model-based engineering is valid and useable for System Safety Engineering for NASA if adequate modeling processes and environment are established.*

## *1 BACKGROUND*

*System Safety is the application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost* [2].

### *1.1 System Safety Engineering*

The System Safety Divisions at NASA/Goddard Space Flight Center (GSFC) provide safety engineering and management to programs and projects on several levels. A Project Safety Manager (PSM) is assigned to and responsible for managing and/or providing system safety engineering support on a given program or project. PSMs are the lead, and frequently the only System Safety Engineer (SSE) on a project. Safety is often primarily viewed as personnel safety, but PSMs also consider hardware, especially for expensive assets and facilities. PSMs ensure that the payloads and spaceflight hardware are safe for launch through hazard analysis processes per range safety

standards, primarily NASA-STD-8719.24 [9], which applies to uncrewed launches from a NASA facility. Additionally, their role for "in-house" work is to ensure the safety of personnel during the course of development, integration, test, and shipment at their center.

During the hazard analysis process an SSE determines whether or not a potential hazard exists via several types of System Safety Engineering analyses. These are Hazard Analyses (e.g., Hazard Analysis (HA), Operations Hazard Analysis (OHA), or Operating and Support Hazard Analysis (O&SHA)), and/or Fault Tree Analysis (FTA). Such analyses are documented within a Safety Data Package (SDP), which consists of a descriptive narrative of the system and safety features, hazard analyses which may include Hazard Reports (HRs), and compliance to range safety requirements called a Safety Requirements Compliance Checklist (SRCC). A brief overview of these key analysis types and products follows.

Hazard analyses begin with a Preliminary Hazard List (PHL) that evolves into Preliminary Hazard Analysis (PHA) and culminates with the final HRs that document how the project or program is meeting launch vehicle (e.g., range safety) requirements, on-orbit safety requirements (for manned vehicles), as well as operational safety (e.g., the safety of personnel involved in building a product) for those hazards that cannot be eliminated. HRs are formal documents that identify hazards along with associated causes and controls (e.g., mitigations) and verifications (e.g., closure records) that establish how the control will be realized for the product.

Many of the launch vehicle and on-orbit requirements are based on fault tolerance. Fault tolerance is the number of faults needed to cause the postulated hazard. For launch vehicles or systems where a failure might result in injury or death to personnel or destruction of a NASA facility, safety inhibits are used to attain the necessary fault tolerance. In general, three safety inhibits correspond to 2-fault tolerance and two safety inhibits correspond to 1-fault tolerance. Requirements documents often stipulate fault tolerance as a means of preventing a catastrophic or critical hazard. SSEs use a variety of tools to analyze system faults that could lead to a hazard. A commonly used technique is the qualitative fault tree. This postulates a hazard or fault as the top-level event, and using a deductive analysis process, traces the hazard to its lowest component in the design. Using this method, SSEs can determine the degree of fault tolerance against a hazard as well as identify issues in the system design that can be addressed to prevent a hazard.

In order to demonstrate compliance to on-orbit and/or range safety requirements, SSEs generate a Safety Data Package (SDP), which is sometimes referred to as a Missile System Prelaunch Safety Package (MSPSP). The safety data package includes:

1) A description of the product being evaluated including how the product will be processed at the launch facility
2) A Hazard analysis of the product by phase, often focusing on design inhibits to establish single or dual fault tolerance
3) Hazard Reports that document hazard causes, controls, and verifications
4) In addition to the components listed above, the SDP or safety-database entries include:
    a. Safety Requirements Compliance Checklist (SRCC) against NASA-STD-8719.24 Annexes, identifying any requirements that are non-compliant or require tailoring [9].
    b. Ground Operations Plan (GOP), which identifies the ground flow from delivery to the launch site through launch and identifies hazardous procedures.

c. An Operating and Support Hazard Analysis (O&SHA), which examines procedurally controlled activities during launch processing.
d. A Verification Tracking Log (VTL) which ensures that all controls are verified according to the Hazard Reports.

## *2 TEST METHODOLOGY*

The test methodology used to assess MBSMA for System Safety was to target analysis types described above (HA, OHA, O&HSA, SRCC, and SDP) and use models from the first phase of the MBSMA Initiative (MBSMAI), which focused on Reliability modeling (Europa Propulsion, Sounding Rocket, and ISS-CapBrIC, from NASA-TM-20205009990 [1]). However, since the MBSMAI phase 1 study indicated that the type of system did not impact results, this System Safety scope was limited to one subsystem. The Europa Propulsion subsystem, shown in Figure 1, was chosen since it has the highest contributors to safety hazards out of the other subsystems previously modeled.

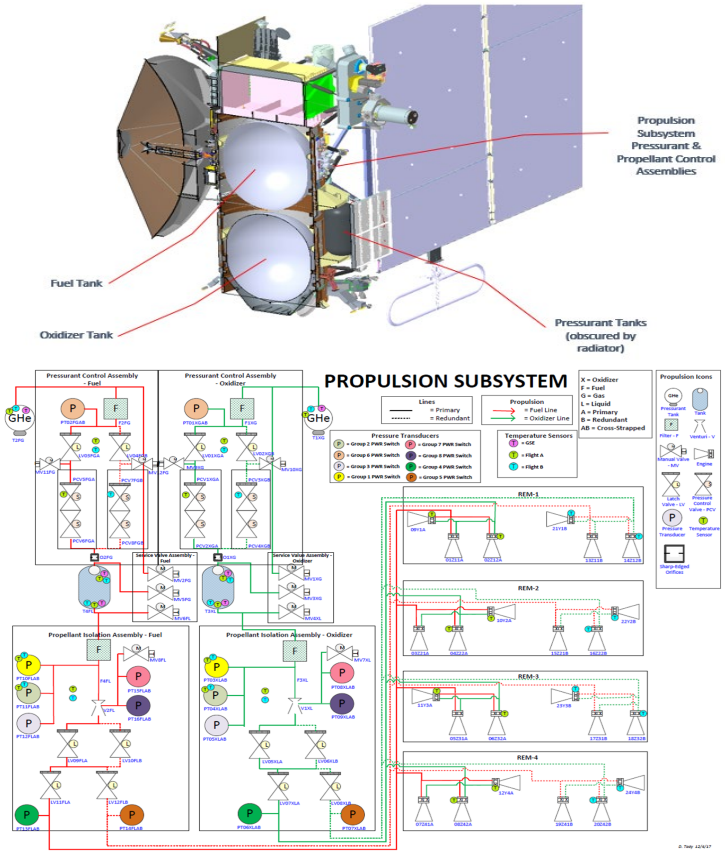


*Figure 1: Europa Propulsion Subsystem [7]*

In addition, while System Safety analyses are traditionally performed across all mission phases, this study's focus was limited to one mission phase (i.e., pre-launch and consumable (pressurant, oxidizer, propellent/fuel) loading) since similar assessments would be done at each mission phase, and one mission phase would be sufficient to demonstrate if modeling satisfied traditional System Safety methods [9]. This enabled a complete evaluation of the artifact production, artifact quality,

and artifact compatibility with risk assessment and hazard reporting, as compared to traditional products, within the relatively short period of this study. Note: Traditional safety assessments are done on complete systems and across all mission phases.

Further, this study tested the capability for modeling to understand and evaluate hazard dependencies via fault trees and verify inhibit sufficiency by running simulations to determine the fault tolerance for the following cases:

1- Premature Propulsion Activation (firing)
2- Overfill of tanks/COPVs (Composite Overwrapped Pressure Vessels) for propellent/fuel, oxidizer, and pressurant
3- Inappropriate material loading procedures or loading with failures present (e.g., flow rate sent to closed system)
4- System fuel/oxidizer escapes via thrusters

### *2.1 Modeling Tools Utilized*

Although there are many model-based tools and plugins available for Model-Based Systems Engineers (MBSEs) to use today, only some have specific Mission Assurance (Reliability, Safety, Quality, and Software Assurance) functionality.

This team found at the time of this study that the following Mission Assurance enabling model-based tools were available: IBM Rational Rhapsody, SysML/MagicDraw (Systems Modeling Language (SysML) [3]) with plugins (Cameo Safety and Reliability Analyzer and/or Tietronix Reliability plugins (FaultTree, Failure Modes, Effects and Criticality Analysis (FMECA)), WebGME.org, SEAM/modelbasedassurance.org, Model Obfuscator, Methodology Wizards, Product Line Engineering, Eclipse Papyrus, and local custom-designed plugins), MADe (Maintenance Aware Design environment from PHM Technology-Siemens [4]), SCADE Suite, Reactis Suite, and PTC's model-based systems engineering solution (Windchill Modeler, Windchill Asset Library & Windchill Process Director). While this toolset 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 during phase 1 of the MBSMAI based on MBSE utilization, the apparent ease of use, and the breadth of assurance discipline coverage. The first being MADe and the second being SysML/MagicDraw (SysML based tool from NoMagic) with Tietronix Reliability plugins and associated stereotypes [3, 4].

When this team assessed the ability of those two tools to support System Safety Engineering hazard analysis (phase 2 of the MBSMAI), only MADe was found to provide adequate Safety support. The team considered adding a tool from the original set that could also support Safety including the following: IBM Rational Rhapsody, MADe, and SCADE Suite; or adding Safety only modeling tools such as HiP-HOPS (Hierarchically Performed Hazard Origin and Propagation Studies), SimulinkModels with SCADE Design Verifier, Analysis and Design Languages, FSAP/NuSMV with FSAP (Formal Safety Analysis Platform) and Safety Analysis Task (SAT) manager, or DSI's eXpress, but ultimately the team chose to execute MBSMAI phase 2 with MADe only. The decision to continue with MADe only was made for inter-study consistency (same study parameters), efficiency (no new model development), and to maintain the representative nature and breadth of assurance discipline coverage of the tools used. However, if

SysML/MagicDraw plugins are developed that support Safety analysis and modeling, MBSMAI phase 2 will be revisited for additional insights and to maintain overall MBSMAI consistency.

### *2.1.1 Maintenance Aware Design environment*

The modeling tool Maintenance Aware Design environment (MADe) provides a suite of software tools that can be used to design, assess, and optimize Safety Hazard Analyses and Hazard Mitigation Management systems. This tool is used in a wide variety of high-risk industries where safety and reliability are critical using model-based engineering techniques. The MADe safety modeling environment provides a Functional Hazard Assessment (FHA) application for the systematic examination of system functions to identify and classify hazards of functions according to their severity in accordance with SAE ARP 4761 - "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment". The SAE ARP 4761 technique starts with determining a system's functions and the elements of the design that perform those functions. Using the system functions, safety assessments (FHA and Preliminary/Final Safety Assessments) are performed and verified, as shown in Figure 2 [2]. An SAE-FHA in this process is used to identify and classify failure conditions in terms of their safety impacts (Minor, Major, Hazardous, and Catastrophic) and begins the Safety Assessment (SA). The SAE-SA is a systematic identification of how failures can cause the hazards identified in the FHA by using FTAs, FMECAs, and common cause analyses. [4]

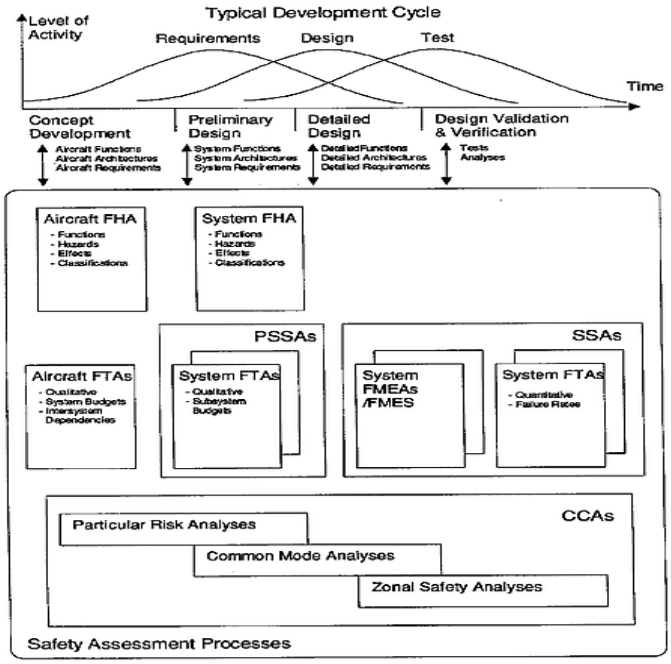


*Figure 2: SAE Safety Assessment Process Overview [6]*

In order to implement the SAE technique, MADe uses a *Functional Diagram* (Figure 3) to define the functions of the system and the *Functional Block Diagram (FBD)* to allocate specific functions to system elements (Figure 5). Therefore, each function's *failure conditions,* which induce safety impacts, are added with specific *verification methods* (analyses, inspection, test, and

demonstration), *safety severity* of the failure (No Safety Effect, Minor, Major, Severe Major, Catastrophic), *probability of occurrence* (1 to 1E-12), applicable mission phases/environments, and any applicable user annotations (Figure 4). All of these definitions are used to generate the SAE reports. Further, if a safety symptom/condition is added to safety impacted Failure Diagrams as a symptom, then a safety case FT can be generated using data from all the Failure Diagrams with that symptom.

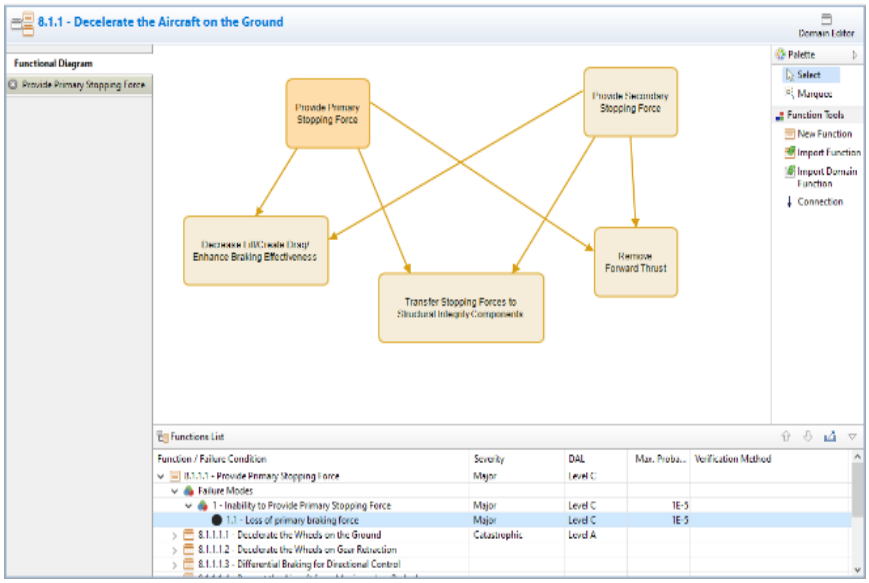


*Figure 3: MADe Functional Diagram (FD) with failure conditions [4]*

In addition, MADe also provides for the integration of safety information with other failure analyses by allowing the modeler to link the failure conditions entered in the *Functional Diagram* to the elements in its *Functional Block Diagram* (FBD - Figure 5) and automatically adds those conditions to its associated *Failure Diagram*. These additional causes are then connected to the appropriate failure faults, losses/symptoms, and/or the associated failure modes by the modeler to complete the modeling (See Figure 5). When all safety impacted causes are integrated with the failure diagrams, they will be reported in the FMECAs and FTAs; and simulation possibilities will also be expanded from fault propagation only to fault and/or hazard propagation.

MADe's simulation capability provides the user with the ability to inject failures and show the propagation graphically to the user. When this capability is used to support system safety, it provides a dynamic way to evaluate the sufficiency and independence of hazard controls/inhibits, how many inhibits must fail before a hazard would occur (i.e., Fault Tolerance), and what impacts the addition or removal of an inhibit will have on system end states. System Safety simulations are initiated by injecting single or multiple signals, energy, and/or material flow state changes to be present or absent (continuously or discretely) into the system. The MADe simulator will then propagate the injected settings through the system and show the results graphically to the user (Figure 6).

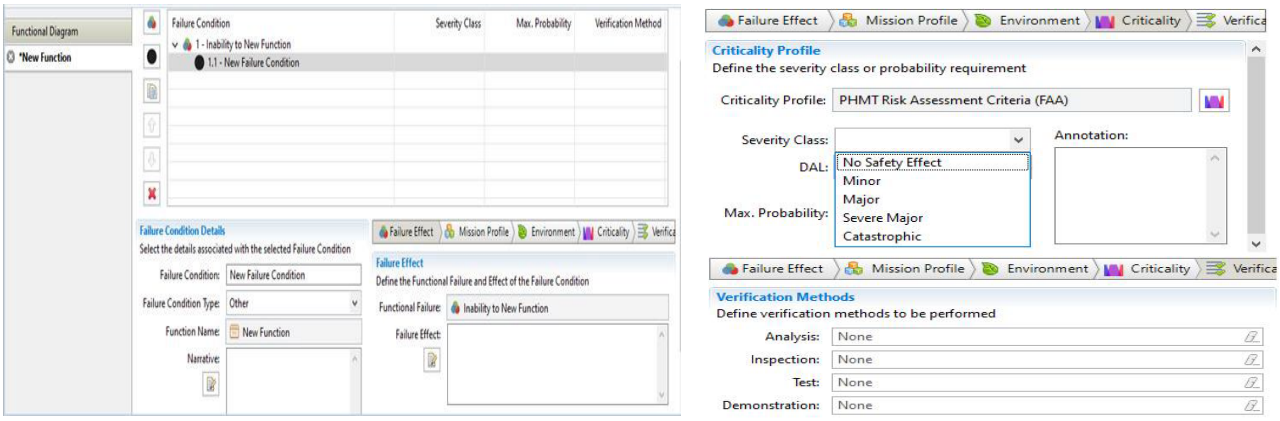


*Figure 4 – MADe Hazard Properties Input Fields [4]*

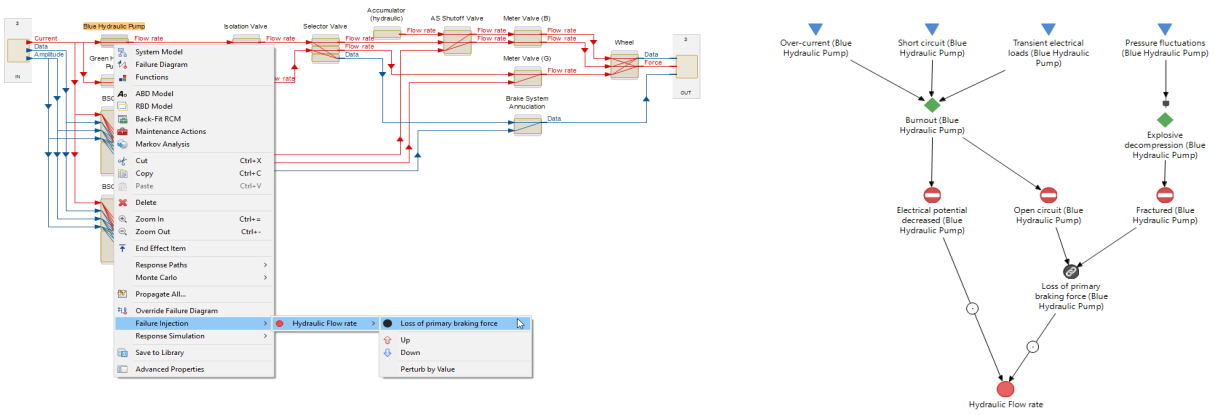


*Figure 5 – Hazard Enhanced Functional Block Diagram and Failure Diagram (MADe aircraft model [8])*

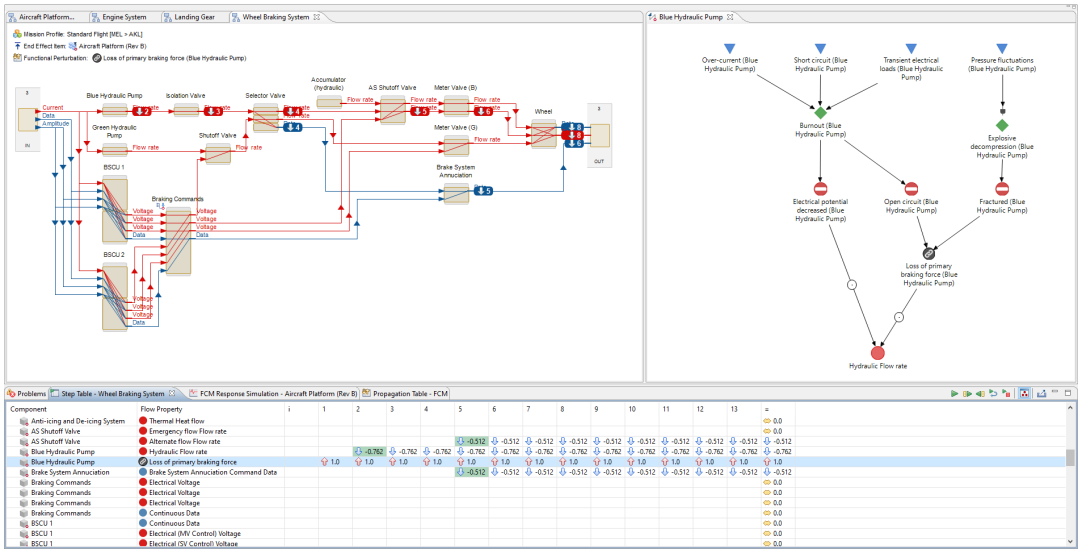


*Figure 6 – MADE Simulation Results (MADe aircraft model [8])*

# *3 MODELING AND TEST CASES*

## *3.1 Europa Propulsion Modeling and Test Cases*

When modeled in the reliability phase (phase 1) of the MBSMAI, the MADe Europa Propulsion model consisted of nine main *Functional Block Diagrams*, one at the system level and eight at the subsystem level. For this system safety phase of the MBSMAI, another system, Propulsion Ground Support Equipment (PGSE), was added to the model, as a "black-box" functional model only, in order to simulate the pre-launch consumable loading and to allow for safety analysis of pre-launch mission phase.

In addition, the mission time of twelve years was entered into the MADe *mission profile* for quantification purposes, while the component/system duty cycles (not cycle life) were adjusted individually. For example, tanks, and service valves that are not cycled on/off or open/close during the mission were assigned duty cycles of 100%. Cycled components, such as engines, pressure control valves, pressure transducers, and latch valves, were assigned duty cycles based on expected mission usage. Note: Traditional safety assessments are done based on the potential for single occurrences, so these the mission profile values are only informational to this study.

As mentioned in section 2.1.1, MADe's approach to safety analysis is based on SAE ARP 4761, while NASA's safety approach consists of first identifying what hazards might be present in the system and then associating potential hazards with components in a system, subsystem, or testing facility. Therefore, to perform NASA safety analyses in MADe, hazard categories were entered as *Functions*, hazards were equated to *Functional Failures*, and hazard causes to *Failure Conditions* in the model's *Functional Diagram* based on system safety engineering assessing the system components against the hazard categories. As a result, all hazards and associated hazard causes for each hazard category were conceptualized for each modeling element. Further analysis of each hazard included evaluating the hazard's causes, severity, and likelihood, and then postulating hazard controls and verification methods to mitigate the hazards.

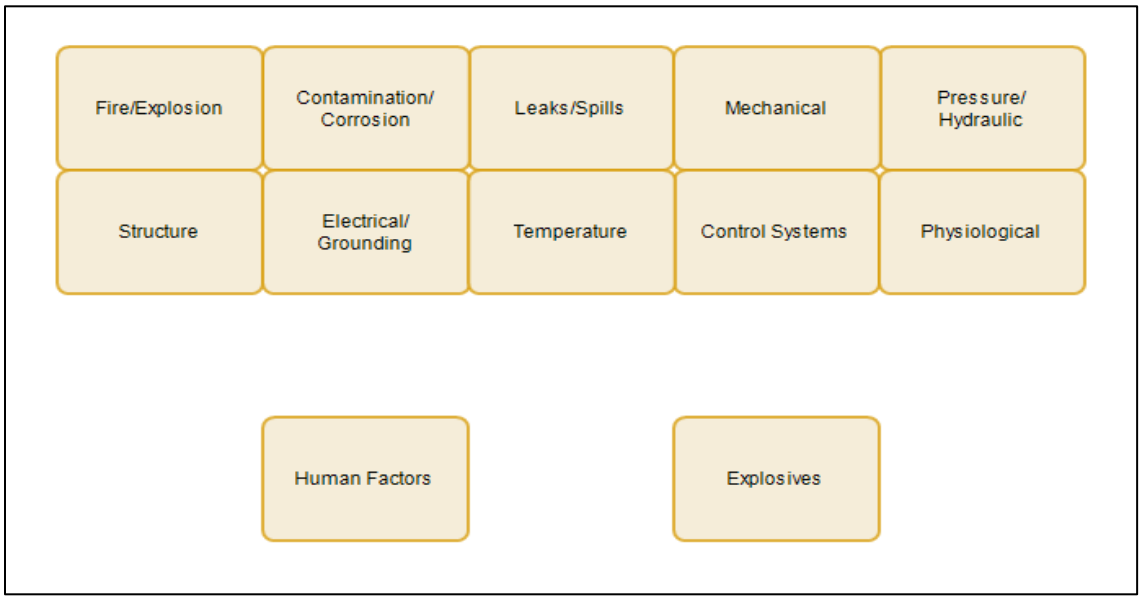


*Figure 7: MADe Europa Functional Diagram*

Twelve hazard categories were considered, ten of which were assessed against the Europa Propulsion Subsystem (see Figure 7). Once associated with a component, the following properties of the hazard were manually entered: the hazard name/title/description, hazard cause(s), verification method(s), hazard control(s), severity of the hazard, likelihood of occurrence (likelihood or maximum probability of each hazard's cause was given a default value of 1E-4 unless it could be proven otherwise), and applicable mission phases/environments (pre-launch in all cases for this study (Figure 7)). The hazards identified were as follows:

- For Fire/Explosion, the hazards assessed were: "Propellent Release", "Oxidizer Release", "Inadvertent firing of Thruster", "Inability to Inability to Isolate Fuel from Oxidizer", and "Electrical Overheating/Short Circuit". Each one was assigned causes (e.g., "Harness Short Circuit") and a severity of catastrophic, based on the assessment of potential safety impacts and the default likelihood cited above. Hazard controls, such as "Test all harness circuits during integration" and a verification method such as "All circuits tested during integration", were added to each control to complete the hazard modeling.

- For Structure, the hazard assessed was "Fractured/Mechanically Failed Flight Hardware". Its hazard causes were identified as "Inability of structure to support design loads", "Improper materials on/in Element or Support Structure", "Defective manufacturing/mechanical failure", "Mishandling of Fuel Tank", "Mishandling of Oxidizer Tank" and "Unbalanced heating of COPVs". Each of these causes were assigned a severity level, a default likelihood, control(s), and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling.

- For Leaks/Spills, hazards assessed were "Propellant Release" and "Oxidizer Release". Causes such as "Mishandling", "Overpressure/improper fill", "Incompatible materials", "Defective manufacturing/mechanical failure", "Upstream internal leak", "Uncontrolled Fuel Mix at Thruster", "Inadvertent signal to fire Thruster", and "Defective PGSE Lines and Fittings" were assigned fuel and oxidizer components. Each of these causes were also assigned a severity, default likelihood, control(s), and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling.

- For Electrical/Grounding, the hazard "Electrical/Grounding Faults" was modeled. Its hazard causes were "Electrical Surges", "Improper Electrical Connections (mismating) and Wiring", and "Improper/Multiple Grounding planes". Again, each of these causes was assigned a severity, default likelihood, control(s), and verification method(s) in the same manner as shown for Fire/Explosion.

- For Pressure/Hydraulic, the hazards assessed were "Rupture", "Cavitation", and "Inadvertent Release of PGSE Lines". The causes modeled for each of these hazards were "Overpressure/improper fill", "Collapse", and "Line Whip" respectively. These were then further modeled with a severity, control(s), and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling.

- For Contamination/Corrosion, the hazards assessed were "Propellent Release" and "Oxidizer Release" caused by mishandling/overpressures of tanks/lines and

material/defective tanks/lines. Each of these tank/line causes were then assigned a severity, default likelihood, control, and verification in the same manner as shown for Fire/Explosion to complete modeling.

- For Mechanical, the hazard assessed was "PGSE Operation-Personnel Hazards". The hazard causes identified by the team's system safety expert were "Stability/Tip-over", "Pinch-Point", "Sharp Edges", "Torquing (over/under)", and "Fatigue/cyclic stresses". These were also further modeled with a severity, default likelihood, control(s), and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling.

- For Temperature, the hazard assessed was "Over temperature". The hazard causes identified by the team's system safety expert were "Elevated temperatures on thruster nozzle" and "Elevated temperatures on Pressurant COPVs". Each of these causes was assigned a severity, default likelihood, control, and verification in the same manner as shown for Fire/Explosion to complete modeling.

- For Control Systems, the hazard assessed was "Inability to Control Fuel Flow". The hazard causes identified by the team's system safety expert were "Inappropriate software operation" and "Sneak circuit". Each of these causes were again assigned a severity, default likelihood, control(s), and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling.

- For Physiological, the hazard assessed were "Asphyxiates" and "Irritates". The hazard causes identified for the "Irritates" hazard by the team's system safety expert were "Propellant rich atmosphere", "Oxidizer rich atmosphere", "Pressurant (for Fuel) rich atmosphere", and "Pressurant (for Oxidizer) rich atmosphere". Each of these causes were assigned a severity, default likelihood, control(s), and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling.

In addition, to fully capture the safety analysis of the Europa Propulsion subsystem, hazard causes were added and linked to the *Failure Diagram* of each applicable modeling element. For example, for the hazard category of "Fire/Explosion" (shown as the brown hexagon in Figure 8), the causes "Defective manufacturing/mechanical failure of Latch Valve", "Upstream internal leak (Latch Valve fails to seat)", and "Inadvertent signal to Open Valve", would be linked to the latch valve, and modeled in the MADe *Failure Diagrams* (Figure 8) for that component as a failure conditions (black circles). This modeling results in these hazard causes being reported in the failure scenarios of FTAs and appear as failure mode function-information in the FMECA (Figure 8), which is advantageous to overall system analysis, but is not relevant to the system safety focus of this phase of the study. This capability will be assessed outside this phase of the study.

### *3.2 System Safety Hazard Analysis Test Cases*

#### *3.2.1 System Safety Hazard Fault Trees*

A common hazard analysis method uses qualitative FTA to understand and visualize hazard inhibits and controls present in a system. Therefore, fault trees were developed in MADe and Windchill for each hazard category (i.e., Fire/Explosion, Structure, Leaks/Spills,

Electrical/Grounding, Mechanical, Pressure/Hydraulic, Contamination/Corrosion, Temperature, Control Systems, and Physiological) in this phase of MBSMAI.

### *3.2.2 System Safety Hazard Analysis Simulations*

In the pre-launch and launch phases of a mission, there are specific scenarios that must be prevented during consumable loading, launch, and ascent. These scenarios, if allowed, would result in a catastrophic or critical hazard. This MBSMAI study phase used the simulation capability of MADe to demonstrate the resilience and sufficiency of hazard controls/inhibits and thus validate the safety of the design of the Europa Propulsion subsystem for the following propulsion specific scenarios for each propulsion hazard analysis case:

Case 1: Premature Propulsion Activation (Firing). Six scenarios were used to demonstrate the response of the propulsion subsystem when signals are sent from the PGSE (three with the enable plug disconnected and three with it connected). The enable plug disconnected scenarios were the following: the PGSE sending only power, only the "Arm" command, and only the "Fire" command. Then a repeat of the previous three scenarios but with the enable plug installed. This was done to validate fault tolerance and inhibit sufficiency.

Case 2: Overfill of tanks/COPVs (fuel, oxidizer, pressurant). PGSE flow rates without termination were used to determine if any Europa propulsion tank can be overfilled.

Case 3: Inappropriate material loading procedures or material loading with failures present (e.g., a flow rate sent to closed system). Two scenarios were used to demonstrate the response of the propulsion subsystem when material (fuel or oxidizer) flows from the service valve and there is a tank fill-valve failure (e.g., stuck closed). This was done in MADe by activating the flow rate to each tank from the appropriate service valve while the tank's function to store fuel was deactivated.

Case 4: System fuel/oxidizer escapes via thrusters. Twenty scenarios were successfully used to demonstrate the response of the propulsion subsystem when material (fuel or oxidizer) flows from the fuel and oxidizer tank to the Propellant Isolation Assemblies (PIAs) while there are latch valve failures. These scenarios consisted of failing each latch valve, shown in Figure 9, separately and then in pairs for fuel and oxidizer to determine leakage.

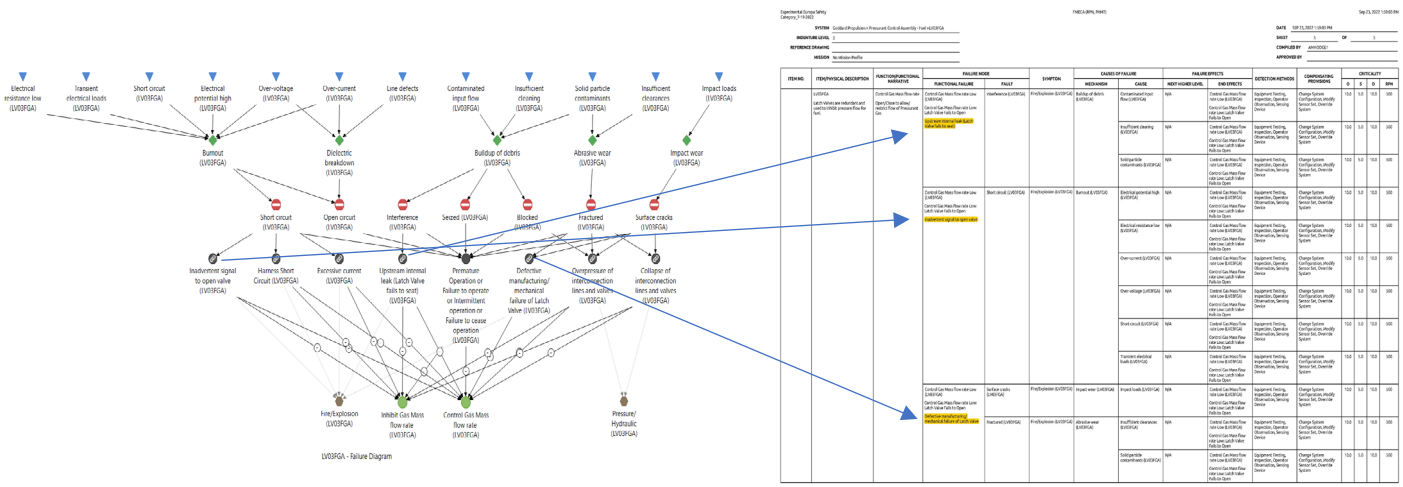


*Figure 8: MADe Failure Diagram Safety Causes and FMECA reporting*

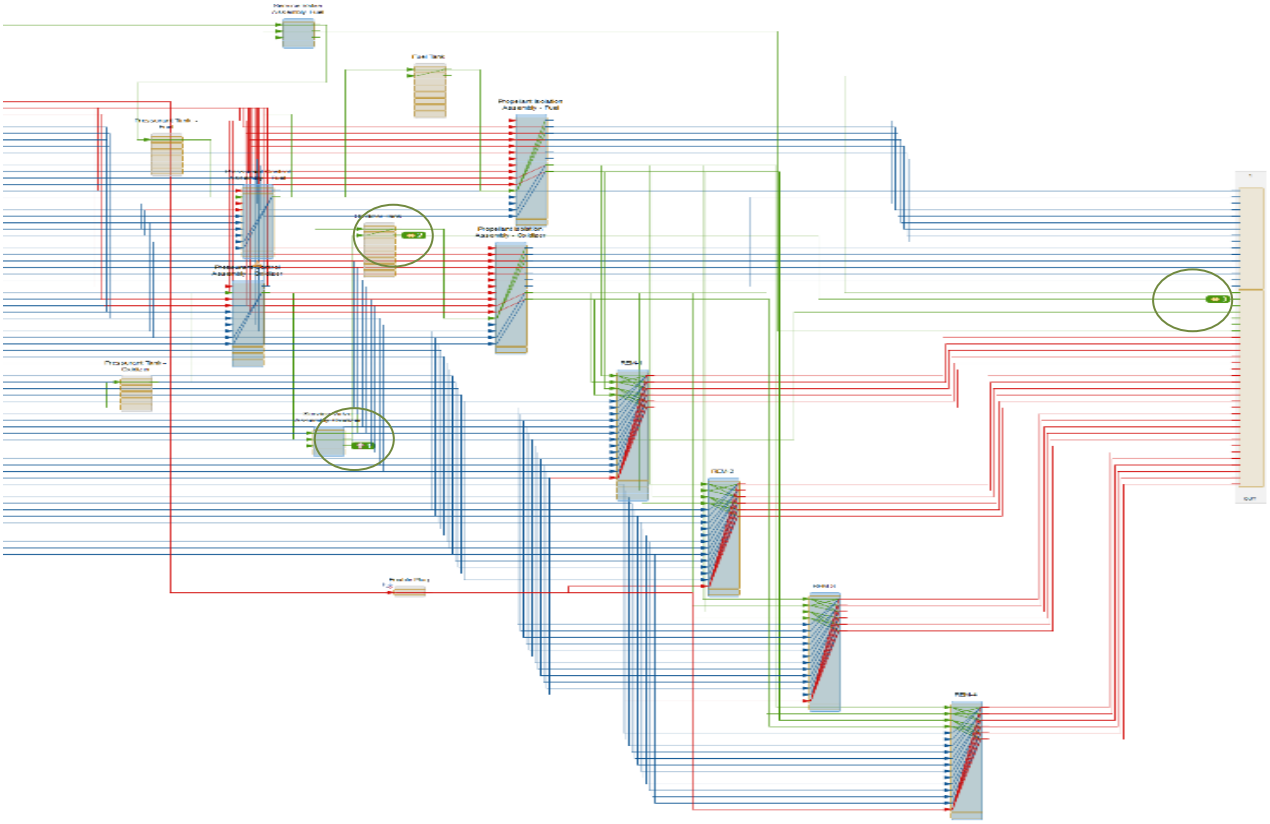

*Figure 9: Example MADe Simulation Response*

# *4 SYSTEM SAFETY RESULTS AND COMPATIBILITY EVALUATIONS*

## *4.1 MADe*

In order to more closely match the NASA/GSFC safety assessment process, the team used MADe's *Functional Diagram - Functions* to represent hazard categories as described above. Using this approach, safety hazards and causes were postulated by subsystem and linked to the categories in an analyst-dependent manner similar to the traditional process [9]. With the additional linking of hazard causes (*Failure Conditions*) to *Failure Diagrams*, Reliability and Safety assessments became integrated, which is not always possible in the traditional process. Additionally, descriptive narratives, controls, and verifications were manually added; however, the MBSMAI phase 1 study demonstrated that developing a library to aid the analyst in entering these types of details reduces the need for such manual inputs. Therefore, this study phase finds that it is plausible to use MADe models to conduct Hazard Analyses (HAs) and Operations Hazard Analyses (OHAs); develop a Safety Data Package (SDP); and use MADe simulations to provide Operating and Support Hazard Analysis (O&SHA) and inhibit-sufficiency/fault-tolerance analysis. Furthermore, this study finds that MADe cannot generate hazard-by-hazard Safety-FTs and Range Safety Compliance Assessments (Safety Requirements Compliance Checklist (SRCC)), but the team is working with the MADe designers to develop these capabilities.

As the scope of this study was limited to the pre-launch phase for the Europa Propulsion subsystem and PGSE only, the HA, SRCC, and SDP were similarly limited to the propulsion subsystem and the analyses described herein. Since MADe was developed to support SAE ARP4761 rather than NASA standards, MADe products reflect the SAE rather than the NASA techniques. While the techniques are similar, the MADe products produced required some postprocessing to better match NASA products. Specific artifact and simulation findings provided below and in Reference 10.

I. MADe has the ability to generate an SDP report. Currently, descriptive entries must be manually entered. For this analysis, the Europa Propulsion subsystem SDP descriptive text was copied and pasted into MADe and the descriptive report was produced as an output. Since the descriptive portion of the SDP is a narrative and not an analysis, it is expected that the narrative will either need to be ingested or entered in directly and matched to the various components. Currently, an SDP is written as a narrative description of a system with images, illustrations, and diagrams to show the key features and safety-related functions of the system and is typically delivered as a document. Except for the ability to upload images and diagrams, writing the narrative within MADe is not much different than the current traditional method.

II. Product Hazard Analysis Reports generated by MADe are very detailed and, since the model provides a direct tie to the components, the modeler has the ability to directly consider the influence of lower-level components on the hazard. Due to the level of detail in the reports, they can appear to be redundant in terms of causes. Like the hazard causes (*Failure Conditions*), hazard controls and verifications are entered manually to complete the hazard data for the HA report. In the future, this could become a library of data that would be selected and applied when needed, thus improving consistency and decreasing analyst dependencies. Even given the post-processing needs and increased detail, the HA reports were found to be valid for System Safety use.

III. An OHA is a hazard analysis that focuses on hazards that occur during integration and test (I&T). Since this study focused only on the pre-launch phase of operations, I&T facilities and dependencies were not modeled or included, and OHA capabilities were not evaluated. However, MADe does have the ability to represent different components and configurations for different mission phases. Were the I&T phase modeled, a Hazard Analysis similar to the one completed in this study could be conducted and produced. Results and observations would therefore be expected to be similar to those mentioned above for Hazard Analysis Reports.

IV. An O&SHA report is intended to describe and analyze hazardous procedures used at the launch site for which there are procedure-based controls. Since Europa's Propulsion subsystem is a part of a spacecraft and not the end product, an O&SHA was not produced. However, some simulations were run to demonstrate the inhibit features present in the subsystem. Such simulations successfully showed that simulating such operations in MADe would greatly aid in conducting an O&SHA and validating the hazardous procedures.

V. Safety inhibits are developed as part of the system or subsystem design to prevent deactivating a safety feature prematurely. As a part of conducting the Hazard Analysis, inhibits are verified, since each potential category is considered down to the lowest component. Deployments, use of thrusters, or opening of fill and drain valves are examples of systems that must work on orbit but must be prevented from working during launch and ascent. Fault trees are often used to validate inhibits.

   The MADe model's *Failure Diagrams* served as a guide for a hazard Fault Tree (FT) development in Windchill that was capable of verifying inhibits/controls. Even though the FTs developed in Windchill (See Figure 10) were not consistent methodologically with typical Reliability or Safety-FT analysis, they each contained a structure consistent with the MADe model's safety data and can provide needed SSE insights pictorially (Windchill FT reports are not concise and readable at this time).

   While MADe has a *Fault Analysis tool* (fault tree development tool), an inherent feature within MADe, which was able to include safety causes in its failure fault trees. It was not able to produce satisfactory hazard-oriented safety fault trees (note: a feature to resolve this is under development by PHM). However, MADe is able produce concise and readable FT-reports and online viewing of all FT-types for engineering insights.

VI. The MADe simulation capability was able to demonstrate the resilience and sufficiency of hazard controls/inhibits and validate the safety of the design of the Europa Propulsion subsystem under failure conditions using the following scenarios for each case as follows:

   Case 1: Premature Propulsion Activation (Firing). Six scenarios were used to successfully demonstrate the fault tolerance and inhibit sufficiency when propulsion subsystem signals are sent from the PGSE (three with the enable plug disconnected and three with it connected). Results with the enable plug disconnected showed that even if only power was activated by the PGSE, the thrusters displayed no response; if only the "Arm" command was activated by the PGSE, the thrusters displayed no response; and if "Power" and the "Arm" and "Fire" commands were sent by the PGSE, the thrusters

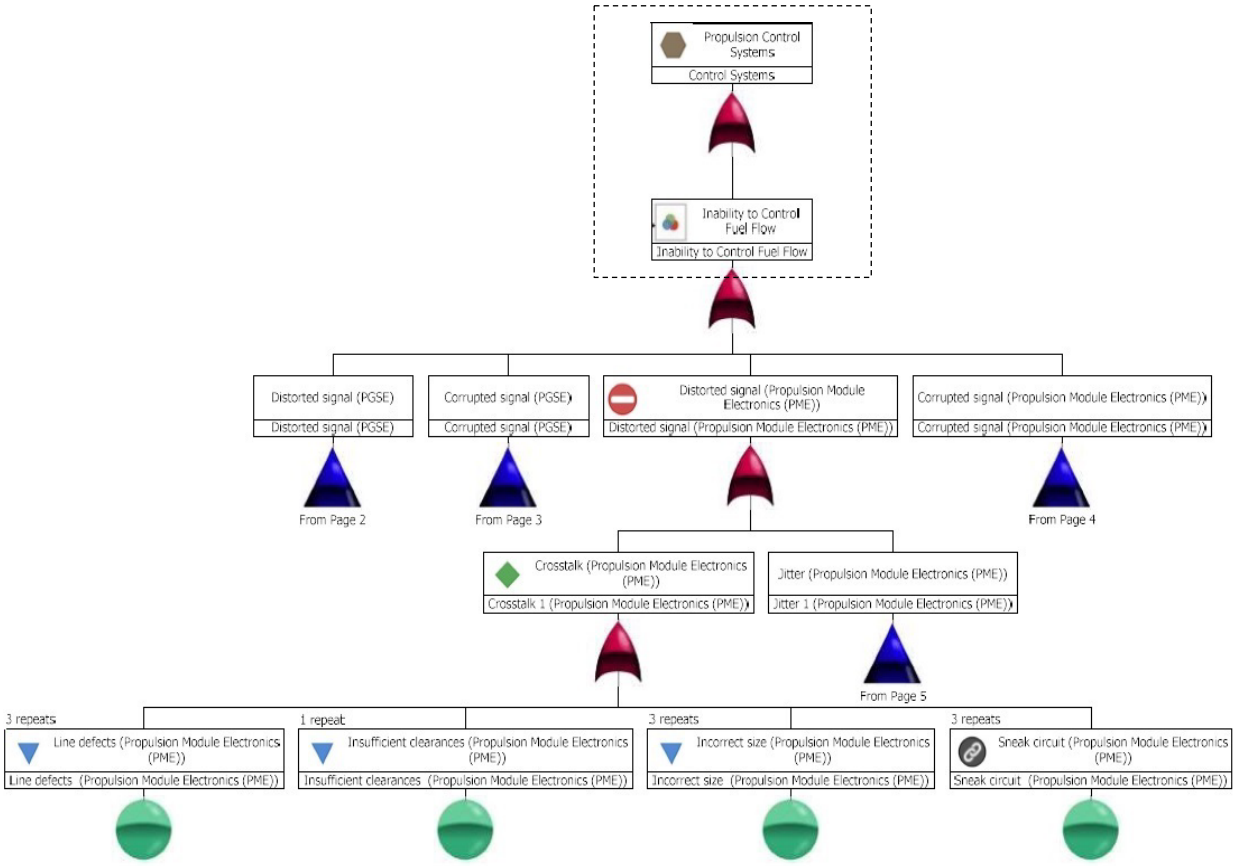


Figure 10: Example Safety Fault Tree (Page 1 of Control System Hazard Only)

displayed no response. All three cases showed that the thrusters were not activated and that the enable plug is a sufficient inhibit against premature signal activation. A repeat of the previous three scenarios were simulated with the exception that the enable plug was connected. Results indicated that activation of the power initiated no response from the thrusters; activation of either power or the "Arm" command separately led to a no response from the thrusters; but if the "Power", and the "Arm" and "Fire" commands were sent the thruster response was to activate. This final scenario validated that premature propulsion activation ("Power" and "Arm"/ "Fire" commands) is more than two-fault tolerant with the enable plug connected.

Case 2: Overfill of tanks/COPVs (fuel, oxidizer, pressurant). Europa propulsion tank overfill could not be simulated due to a lack of material-accumulation-simulation capability in MADe.

Case 3: Inappropriate material loading procedures or loading with failures present (e.g., flow rate sent to closed system). The two simulation scenarios used to demonstrate the response of the propulsion subsystem when material (fuel or oxidizer) flows from the service valve and there is a tank storage failure (e.g., fill-valve stuck closed) successfully showed the safety risk. In the simulation, fuel/oxidizer flow was activated (up arrow) from the service valve while each tank was deactivated (arrow down) to show that it had failed. The results of each simulation (Figure 9) showed no response (side-to-side arrow), which means that fuel/oxidizer will leak at the tanks only.

Case 4: System fuel/oxidizer escapes via thrusters. Twenty scenarios (including both single and double latch valve failures) were successfully used to demonstrate the response of the propulsion subsystem when material (fuel or oxidizer) flows from the fuel and oxidizer tank to the Propellant Isolation Assemblies (PIAs) while there are latch valve failures. Results showed that for a single latch valve failure (LV05XLA, LV06XLB, LV07XLA, LV08XLB, LV09XLA, LV10XLB, LV11XLA, or LV12XLB shown in Figure 1), no thruster change occurred. This indicates that neither fuel nor oxidizer would leak further than the individual valves that had a failure. Similarly, cross-side latch valve failure combinations (e.g., LV05XLA with LV06XLB) showed no leakage beyond the upper-most failed valve. However, the scenarios where both latch valves fail on a single side (e.g., LV05XLA with LV07XLA) showed that fuel would flow to the thruster and cause a hazard if the thruster valve is open.

While most of the MADe report-products required post-processing for NASA use, MADe's simulation capability was considered a unique and advantageous feature that is currently unavailable in traditional NASA/GSFC safety methods. Simulations were found to enhance safety inhibit and fault tolerance understanding (See Figure 9 and Reference 10), but a specific simulation report is not available at this time. The current interactive simulations would be helpful for future analyses and could help verify/validate the safety of hazardous procedures used in pre-launch processing as well as during other phases of system development.

In this study, it was observed that MADe does not currently have the following abilities:

- Automatically generate a hazard-by-hazard Safety-FT. Currently, the Reliability-FT can be automatically generated, but safety data is comingled within that tree.
- Generating a complete safety hazard list or report in the NASA format.
- Formulating and managing a Range Safety Requirements compliance matrix.
- Generate either custom HA report and/or NASA HA. Currently, the report structure doesn't match NASA's or MIL-STD-882.
- Allow users to select verifications or controls from built-in libraries, they currently must be entered manually.
- Allow user to select NASA hazard categories from MADe defaults, which while similar, are not aligned with NASA categories. Currently, NASA specific modeling of hazard categories and severity definitions, from NF 1825 or ISS/ARTEMIS hazard database(s), must be manually entered/modeled. Note: It would be more efficient if MADe was able to upload these definitions/categories, or interface with the NASA databases to directly input hazard categories and output analysis results as a part of the safety documentation and/or into NASA databases.
- Autonomously reflect edits of hazards (e.g., hazard causes/failure conditions) in the failure diagrams.
- Directly import text or images for an integrated System Safety Data Package descriptive section.
- Import legacy and offline data into the safety model.

MADe does not currently have a dedicated module for Safety Analysis. It is comingled with the Reliability module which limits the terminology and concepts available.

## *5 DISCOVERIES & RECOMMENDATIONS*

While model-based safety analysis is feasible, the authors, based on modeling results and experiences in this study, have several insights and recommendations for improving available tools and methods, as shown below:

1) Model-Based functional models need extensive component details 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) and to support simulations.

2) A single system model should be built that includes lower-level components as well as connections representing all functions (e.g., power, signal, material transfers). This model should be validated against the system by the Systems Engineers and used to conduct SMA analyses including validating and verifying hazard analyses as well as safety requirements for manufacturing, pre-launch processing and launch.

3) Any lack of standardization or framework within a 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 without modeling experience, 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.

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

    - Support for the development of models from the traditional system safety artifacts rather than only deriving the artifacts from the models for efficiency via model re-use (import existing hazard analyses and/or SDPs).
    - The ability to ingest and parse or allocate text, diagrams, illustrations, and images to safety products and/or models.
    - The ability to reuse component level models for consistency and to take advantage of subsystems which have already been validated to ensure efficiency and accuracy.
    - 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 or deleting a failure condition) propagate to other parts/diagrams of the model automatically (including link breaks) and/or shows as an error that needs to be resolved by the modeler.
    - The ability to simulate the accumulation of material or actuations on modeling elements as well as failures for efficiency and accuracy.
    - The ability to allocate requirements to a functional diagram/element to analyze whether or not safety requirements have been met.
    - The ability to fully edit hazard-modeling elements (including identifiers) to ensure accuracy.

- The ability to develop libraries of hazard categories with baseline definitions and implication data for consistency and accuracy (see Figure 11 for a possible hazard library structure).

    - Potential element causes or element types (graphical hazard tree for input)
    - The library could extend to controls and verifications
    - As the library is built, the speed and efficiency of conducting the analyses will improve since manual inputs are reduced.

- The ability to add models of systems or portions of system models to a library of shareable models for efficiency.
- The ability to input/import results and tracking/verification supporting data (i.e., procedures, control inspection, verifications, etc.) for safety report production efficiency and accuracy.
- The ability to copy hazard modeling without linkages or challenge the modeler to verify linkages, if applicable.
- The ability to combine models and duplicate models for reuse in future modeling efficiency.
- Provisions for model component and system consistency error checking and reporting for improved modeling accuracy.
- Model change control/reporting (i.e., detailed configuration control), including the ability to revert to a previous model 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 and allocate requirements to each element or hazard for verification/compliance recording efficiency.
- An export or reporting function for fault tree and simulation results for understanding and accuracy validation.
- Modeling diagrams that connect hierarchically to each other allowing non-modelers to easily traverse and drill down within the severities and likelihoods model for understanding and accuracy validation.
- The ability to produce a preliminary hazard assessment and subsequent hazard reports using NASA-defined severities and likelihoods.
- The ability to produce a fault tree with a hazard as the top-level event (pulling causes and contributions from all system elements) and precise Boolean logic for accuracy.
- The ability to produce a compliance checklist per NASA-STD-8719.24.
- The ability to hold and report SDP package information in the NASA format.
- The ability to export to NASA databases directly.
- Performance that shortens analysis time while maintaining consistency and accuracy between models.

5) Modeling process and controls are needed prior to generating any models to ensure and validate model accuracy. Hence, a key recommendation of this study is that the following modeling process guidance be established (as shown in Figure 12): 1) Create a multi-discipline mission specific modeling team (SE and SMA at a minimum); 2) Clearly define modeling responsibilities (e.g., SEs model requirements; Designers

model structure (Functional Block Diagram/Wire Diagram); SSEs model hazards (categories, mechanisms, causes, and linkages), verifications, and controls; REs model failure behaviors, characteristics, and mitigations (and assist with safety-cause linking); 3) Complete modeling and share common data between modeling elements; 4) Produce System Safety artifacts (and simulation results) and share resulting data between modeling elements; 5) Verify and refine modeling (and designs) until a final and acceptable result is achieved; and 6) Share modeling with future missions.

The results and recommendations presented herein are based solely on System Safety discipline needs and were derived from a small subsystem. Thus, the authors also recommend that this study continue to test additional SMA disciplines and more complex systems.

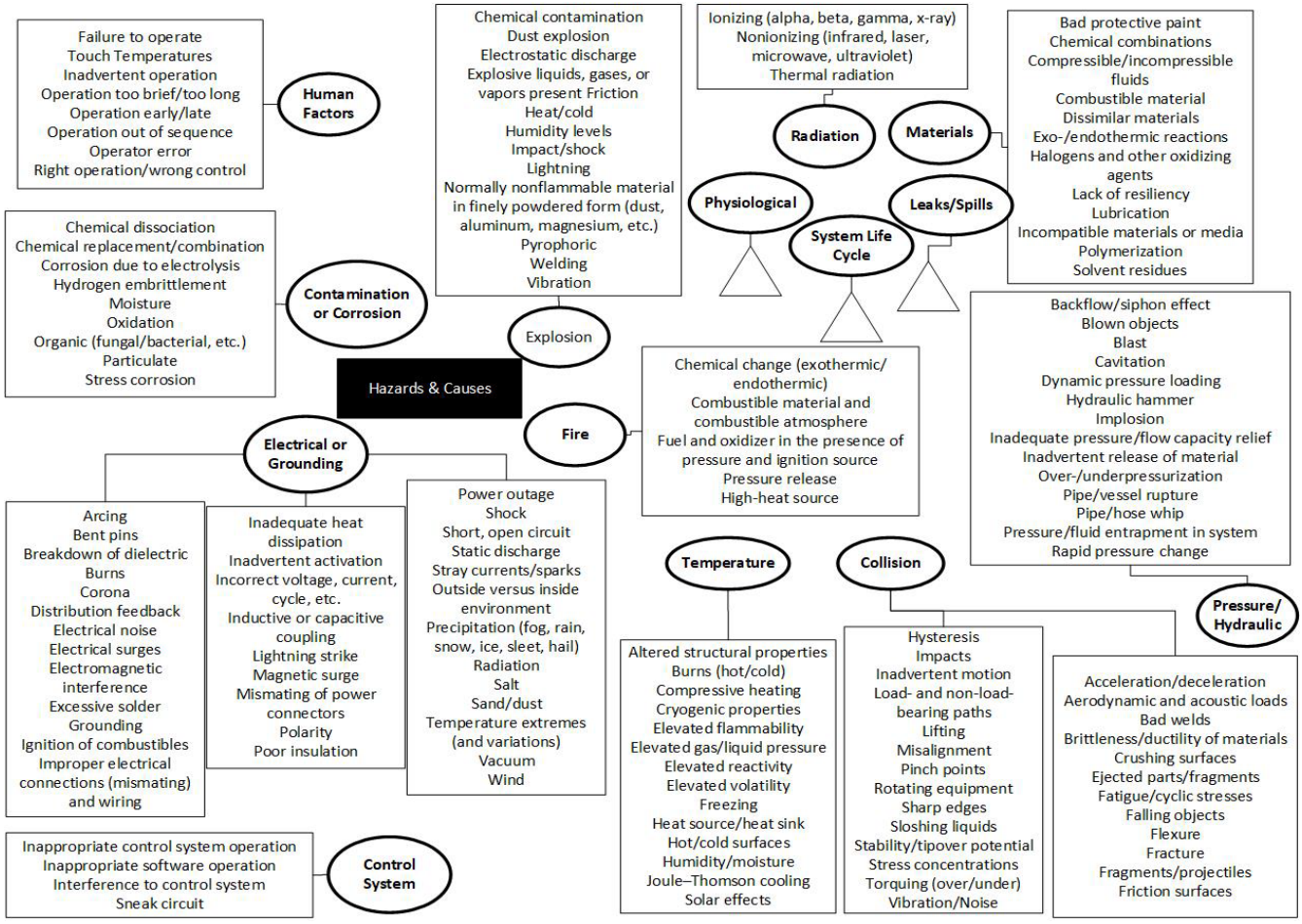


Figure 11: Prototype Hierarchical Hazard and Cause Structure

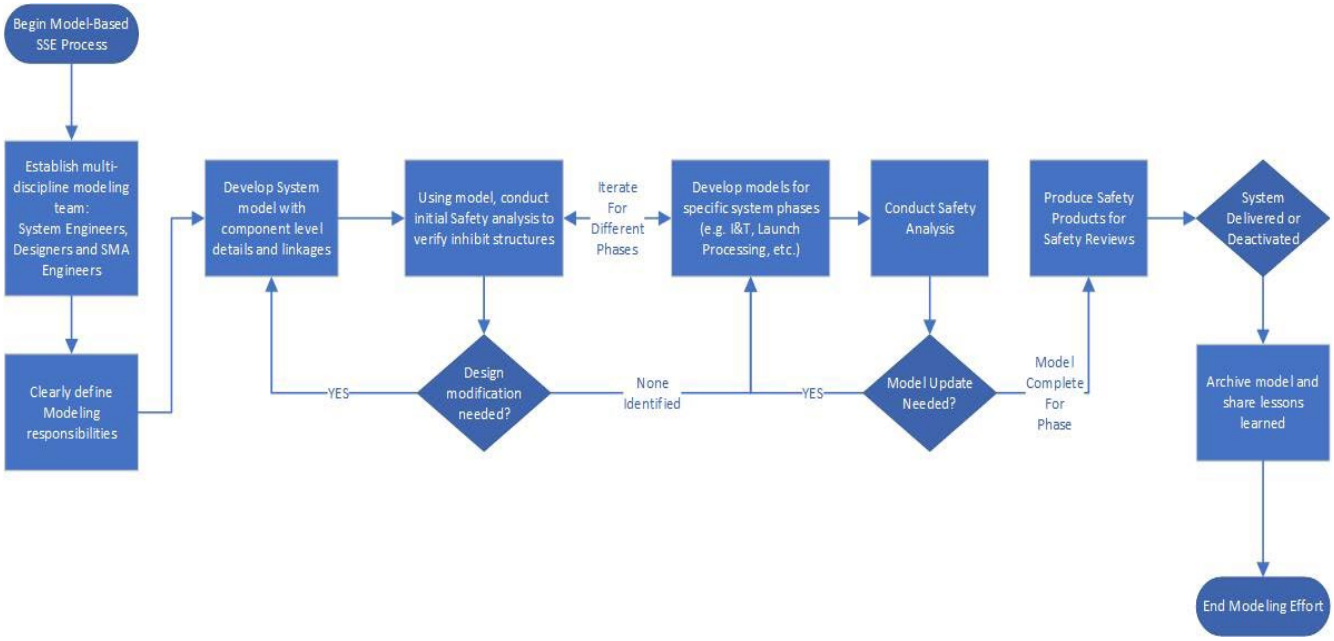


Figure 12: Notional Model-Based System Safety Process

## *6 CONCLUSIONS & PATH FORWARD*

Model-Based Engineering is found to be valid and useable for System Safety Engineering 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 one more phase of this study to assist NASA/GSFC in developing a unified Model-Based engineering approach and determining the best tool set to support that approach. The next phase of the MBSMAI will evaluate Software Assurance and Quality Engineering Analysis compatibility.

## *ACKNOWLEDGEMENT*

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

## *REFERENCES*


[1] N. J. Lindsey, M. Alimardani, L. D. Gallo, Y. Lim, and T. Odita, "Model-Based SMA Initiative Phase 1 Report: Reliability" (NASA-TM-20205009990), GSFC Risk & Reliability Branch, Greenbelt, MD, USA, 2019.

[2] NASA, "Software Safety and Software Assurance Standard," NASA STD 8739.8, June 10, 2020.

[3] "Systems Modeling Language," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Systems_Modeling_Language. [Accessed 15 Apr 2019 - 2022].

[4] "MADe Software Official Website," PHM Technology, [Online]. Available: https://www.phmtechnology.com/. [Accessed 21 Jan 2019- 24 Mar 2022].

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

[6] SAE International, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment" (SAE ARP4761), https://subscriptions.techstreet.com/products/303161. [Accessed 3/21/22]

[7] "EUROPA Fluid Schematic" (EUROPA-PROP-DESC-0002), GSFC EUROPA Project, Greenbelt, MD, USA, 2018.

[8] PHM Technology, "MADe Aircraft Model," Evan Apostolou-to-Nancy Lindsey email 11/1/2021.

[9] NASA, NASA Expendable Launch Vehicle Payload Safety Requirements NASA-STD-8719.24 with Change 3, 08-26-2011

[10] N. J. Lindsey, A. M Cooter, L. N. Sindjui, and A. Hodges, "GSFC/NASA Model-Based SMA Initiative Phase 2 Report: System Safety" (draft), GSFC Risk & Reliability Branch, Greenbelt, MD, USA, 2022.


## *BIOGRAPHIES*


Nancy J Lindsey
Goddard Space Flight Center (Code 370)
8800 Greenbelt Road
Greenbelt, MD 20771 e-mail: nancy.j.lindsey@nasa.gov


Nancy J Lindsey has spent 37+ years in aviation and aerospace engineering performing a variety of engineering tasks, including systems, system safety, quality, and reliability engineering, across the entire gamut of space vehicle life cycles and program types including Defense & Commercial Communications Missions, Space-based Astronomical Observatories, Ground Systems, and Earth Science Monitoring Systems. She is currently the Reliability, Maintainability and Availability (RMA) Subject Matter Expert at the NASA Goddard Space Flight Center in Greenbelt MD and the deputy R&M Technical Fellow at NASA Headquarters. Mrs. Lindsey has a Bachelor of Science undergraduate degree in Computer Science & Aeronautical Engineering which was earned at Embry-Riddle Aeronautical University in Daytona Beach, Florida, was trained in Flight Medicine and F-14 flight by the US Navy, and has a Master of Science degree in Space Studies, from the University of North Dakota. Nancy's independent research efforts can be viewed via website: www.rcktmom.com.

Ann Miranda Cooter
Goddard Space Flight Center (Code 360)
8800 Greenbelt Road
Greenbelt, MD 20771 e-mail: ann.m.cooter@nasa.gov

Ann Miranda Cooter's career in aerospace engineering includes a wide variety of engineering assignments in the USA and abroad. Her career began with building finite element models and developing methods for coupling, analyzing, and validating spacecraft models in NASTRAN to structurally qualify satellites. She spent 2 years conducting thermo-elastic modeling in Toulouse, France. Following her sojourn in France, Ms. Cooter joined the Hubble Space Telescope safety team, and was awarded a Silver Snoopy for her work on Servicing Mission 4. She is currently a Senior Project Safety Manager on multiple projects at Goddard Space Flight Center. Ms. Cooter has a Bachelor of Science in Mechanical Engineering from the University of Tennessee, Knoxville, a Graduate Certificate in Space Operations from Capital Technology University, and a Master of Science in Information Technology from the University of Maryland, Global Campus.

Austin Michael Hodges
Goddard Space Flight Center (Code 371)
8800 Greenbelt Road
Greenbelt, MD 20771 e-mail: austin.m.hodges@nasa.gov

Austin Michael Hodges has spent 2 years working in aerospace and mechanical engineering performing different safety and reliability work for government contractors working directly for NASA customers. He has interned for Flight Safety performing Risk-Based Flight Safety Analysis and technical writing on Expendable Launch Vehicles (ELVs). He has performed Quantity Distance (QD) Analysis and Risk-Based Explosive Safety Analysis. He has worked in novel Reliability projects including Data Mining Failure Modes and Effects Analyses (FMEAs), creating fault trees, writing controls/verifications, performing experimental software analysis, and writing technical papers in support of the Digital Transformation (DT) Initiative and the Model-Based Safety and Mission Assurance Initiative (MBSMAI). Mr. Hodges graduated with a Bachelor of Science (B.S.) in Aerospace Engineering from West Virginia University in May of 2020.

Lionel Nobel Sindjui
Goddard Space Flight Center (Code 371)
8800 Greenbelt Road
Greenbelt, MD 20771 e-mail: lionel-nobel.w.sindjui@nasa.gov

Lionel-nobel Sindjui received a BS in Mechanical Engineering in 2015, and a Master of Engineering in Mechanical Engineering in 2018, both from the University of Maryland College Park. He is currently working as Reliability Engineer at NASA Goddard Space Flight Center (GSFC). During his time at NASA GSFC, he has worked continuously to improve the printed circuit board assurance process and test the capacities of Model Base Engineering tools for NASA missions. This includes providing finite element analysis techniques to simulate Printed Circuit Board (PCB) environmental conditions and modeling analysis to test the design architecture of NASA projects.