NASA/TM- 20250009586

Model-Based SMA Initiative Phase 2 Report: Safety

Nancy J. Lindsey, Goddard Space Flight Center, Greenbelt, MD

Miranda Cooter, Goddard Space Flight Center, Greenbelt, MD

Nobel Sindjui, Goddard Space Flight Center, Greenbelt, MD

Austin Hodges, Axient, Wallops Flight Facility, Wallops Island, VA

October 2025

NASA STI Program Report Series

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

.

NASA/TM- 20250009586

Model-Based SMA Initiative Phase 2 Report: Safety

Nancy J. Lindsey, Goddard Space Flight Center, Greenbelt, MD

Miranda Cooter, Goddard Space Flight Center, Greenbelt, MD

Nobel Sindjui, Goddard Space Flight Center, Greenbelt, MD

Austin Hodges, Axient, Wallops Flight Facility, Wallops Island, VA

National Aeronautics and
Space Administration

Goddard Space Flight Center
Greenbelt, Maryland 20771]

October 2025

The use of trademarks or names of manufacturers in this report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.

Available from:

NASA STI Program / Mail Stop 050
NASA Langley Research Center
Hampton, VA 23681-2199

Model-Based SMA Initiative
Phase 2 Report: Safety

Nancy J. Lindsey[1], Miranda Cooter[1], Nobel Sindjui[1], and Austin Hodges[2]
1 Goddard Space Flight Center, Greenbelt, MD 20771
2 Axient, Wallops Flight Facility, Wallops Island, VA 23337

EXECUTIVE SUMMARY & CONCLUSIONS

In order to include Safety in Model Based Safety and Mission Assurance (MBSMA), an agency-sponsored team at Goddard Space Flight Center (GSFC) has completed a Safety study of modeling and testing as part of the Model-Based Safety and Mission Assurance Initiative (MBSMAI). In this study, GSFC Reliability experts developed a safety model of the Europa mission propulsion subsystem using a representative Commercial Off-The-Shelf tool, MADE (Maintenance Aware Design Environment from PHM Technology-Siemens). MADE was selected since its counterpart, SysML, does not have a safety plugin. If SysML adds capability as a follow-on action, we hope to test and compare with MADE. Since propulsion is/is one of the greatest contributors to hazards in satellite spacecraft, due to more inherent hazards than other subsystems and higher severity of hazards on average, it was chosen to demonstrate the possibility of modeling systems safety as a proof of concept. The model and its ability to support Systems Safety Analysis were then evaluated for accuracy, consistency, and efficiency in supporting traditional Safety and Mission Assurance (SMA) analysis and milestone artifact generation risks assessment and communication.

Based on the modeling results and experiences in this study, the following is found in regard to modeling and modeling environments (modeling tools with associated safety embellishments/accessories – See Section 5): Model-Based Engineering is valid and useable for Safety Engineering for NASA SMA if adequate modeling processes and environment are established. Thus far, MADE is the only SMA-capable tool and provided the best current and future efficiency/consistency/accuracy possibilities for system-safety analysis at the time of this study (See Table 3).

Further, it was determined that 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 81): 1) Create a multi-discipline mission-specific modeling team (Systems Engineering (SE) and SMA at a minimum); 2) Clearly define modeling responsibilities (e.g., SEs model requirements, Designers model structure (Functional Block Diagram/Wire Diagram), System Safety Engineer (SSEs) model hazards (categories, mechanisms, causes, linkages, verifications, and controls), and 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.

Therefore, this study team recommends this study's results, recommendations, and guidance (See Appendix B) be used by NASA to advance the modeling scope and depth used for model-based SMA analysis, establish SMA-to-SE/SE-to-SMA modeling collaboration and transition points, adapt/reshape traditional products while maintaining validity, and advance Model-Based tool capabilities. NASA subject matter experts and PHM/MADE are continuing to collaborate on modelling environment optimizations (See Section 4 and Table 3) to ensure accuracy/ efficiency/consistency returns are maximized for future NASA missions.

However, the results and recommendations presented herein are based solely on System Safety discipline needs and were derived from modelling a small subsystem. Thus, the authors also recommend that this study continue to test additional SMA disciplines and more complex systems to assist NASA/GSFC in developing a unified model-based engineering approach and determining the best tool set to support that approach. Thus, the next phase planned for MBSMAI will evaluate Software Assurance and/or Quality Engineering analysis compatibility.

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]

The System Safety Division at NASA/Goddard Space Flight Center (GSFC) provides 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. The formality and extent of system safety analyses depends on the system, launch vehicle type, and whether the mission is crewed or uncrewed. GSFC's missions are typically uncrewed science missions launching on an Expendable Launch Vehicle (ELV), and it is in that context that this study was completed.

For the typical, uncrewed science mission, PSMs ensure that the payloads and spaceflight hardware are safe for launch through hazard analysis processes per range safety standards, including NASA-STD-8719.24 [9], which is the primary range safety source that applies to uncrewed launches from a NASA facility. Additionally, their role for "in-house" work is to ensure the safety of personnel during development, integration, test, and shipment at their center via hazard analysis and safety requirement compliance.

1.1 Hazard Analysis

A PSM or SSE determines whether a potential hazard exists using several types of System Safety analyses and produces products documenting these analyses and the system hazards. Such analyses mature throughout the phases of a project and are based on the design. Each type of hazard analysis has a different focus in terms of phase and configuration. Examples include the System/Subsystem Hazard Analysis (SHA), focuses on hazards inherent in the system, the Operations Hazard Analysis (OHA), which focuses on hazards that occur during the Integration and Test Phase, and the Operating and Support Hazard Analysis (O&SHA), which focuses on operations at the launch site. Although not a formal deliverable product, a Safety Fault Tree Analysis (FTA) is often used to verify fault tolerance and to understand system interactions from a safety perspective.

Typically, hazard analyses begin with a Preliminary Hazard List (PHL), which is then expanded into a Preliminary Hazard Analysis (PHA). These analyses ensure that the project or program maintains safety from concept through launch. The analyses show how vehicle requirements (e.g., range safety), on-orbit safety requirements (for manned vehicles), as well as operational safety requirements (e.g., the safety of personnel involved in building a product) are met. Hazards that cannot be eliminated are controlled and tracked. Often, hazards identified early in the process can be eliminated by design changes.

Hazard Reports (HRs) are formal documents that identify hazards along with associated causes and controls (e.g., mitigations) and verifications (e.g., closure records) and establish how the control will be realized for the product.

1.2 Safety Requirements

The NASA-STD-8719.24 Annex contains over 5000 requirements, which must be considered by each payload on a launch vehicle. Each requirement is marked either "Compliant (C)," "Not Applicable (N/A)," "Information/Title (I)", "Tailored (T)" or "Noncompliant (NC)". Based on the assessment against the requirements, the system may require design modifications, additional barriers, and/or controls.

Many safety 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, NASA-STD-8719.24 Annex and its referenced requirement documents often stipulate the degree of fault tolerance (e.g., 2-fault or 3-fualt tolerant) as a means of preventing a catastrophic or critical hazard.

1.3 Safety Fault Tolerance and Inhibits

PSMs or SSEs use a variety of tools to analyze system faults that could lead to a hazard. A commonly used technique is the Safety Fault Tree, a qualitative fault tree that looks at how many failures can occur before the hazard is realized. The analysis postulates the realization of the hazard as the top-level event using a deductive analysis process, to trace the hazard to its lowest component in the design. Using this method, SSEs can determine how many interim failures/faults are required to realize a hazard, often referred to as the degree of fault tolerance. An advantage to this type of analysis is that it can also identify issues in the system

design that can be mitigated before implementation (e.g., hardware built).

A fault tree is derived from the design and thus changes with the design. System engineers and discipline engineers (e.g., Design and Specialty engineering) assist with the analysis to determine the design's fault tolerance to the realization of a severe hazard. Ideally, the design is modified during this process to eliminate hazards where possible or to reduce the likelihood of a hazard occurring. These modifications to reduce the likelihood often add features (hardware or software) to a design to prevent an action or to increase the number of faults that must occur before the realization of a hazard. These are sometimes referred to as "Inhibits," since they prevent or inhibit an action or actions that could result in a hazard (e.g., thruster activation, boom deployment.). Typically, 3 inhibits are needed for dual fault tolerance (for a catastrophic hazard) and 2 inhibits are needed for single fault tolerance (for a critical hazard).

1.4 Safety Products

Formal analyses must be documented within a Safety Data Package (SDP, sometimes referred to as a Missile System Prelaunch Safety Package (MSPSP)). A suggested outline for this document is defined for uncrewed missions in the NASA-STD-8719.24 Annex and consists of a descriptive narrative of the system and safety features, hazard analyses based on pre-launch processing and launch hazard reports. In addition to the components listed above, the SDP or safety-database entries include:

a. Safety Requirements Compliance Checklist (SRCC)using the NASA-STD-8719.24 Annex as a basis, summarizing compliance and identifying any range safety requirements that are non-compliant or required 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.

The SDP and its associated documents are delivered to the launch vehicle provider as proof that the system has been analyzed and is safe for launch. It also demonstrates compliance to the requisite requirements and provides information that might be needed if there is a mishap or close call.

2.0 TEST METHODOLOGY

While System Safety analyses are traditionally performed on all systems across all mission phases, this study's focus was limited to one mission phase and subsystem relevant operation (i.e., pre-launch consumable (pressurant, oxidizer, propellent/fuel) loading), and the production of HA, SRCC, and SDP, since similar assessments would be done at each mission phase [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.

Additionally, during phase one of the MBSMA Initiative (MBSMAI) it was learned that one subsystem would be sufficient to demonstrate SMA-discipline feasibility. Therefore, a single model from the models available from the first phase of MBSMAI (Europa Propulsion, Sounding Rocket, and ISS-CapBrIC [1]) was selected for this study phase. The Europa Propulsion subsystem, shown in Figure 1, was chosen, since it has the highest contributors to safety hazards of the subsystems previously modeled.

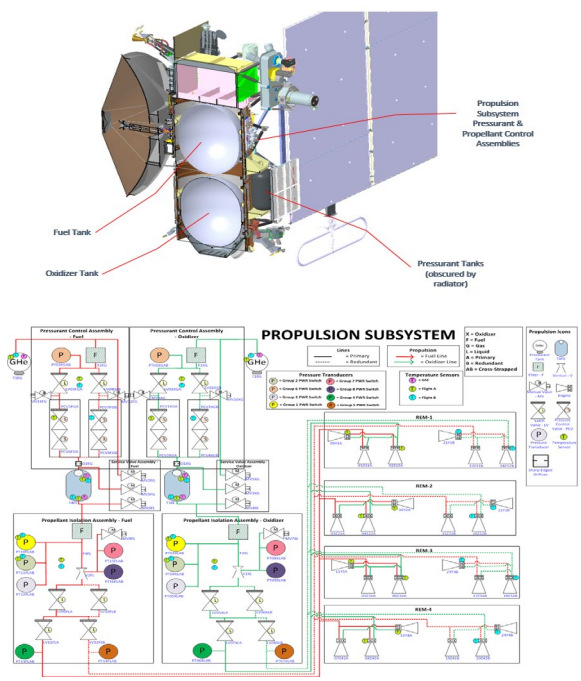


Figure 1: EUROPA Propulsion Subsystem [7]

2.1 Testing Process

The System Safety analyses process used in this study phase was as follows:

1) Identify what hazard categories might be present by component
2) Postulate and characterize the hazards present for each category (Table 1)
    - Likelihood
    - Severity/Consequence
    - Causes
    - Controls
    - Verification Methods
    - Verifications
3) Associate and Link Hazard Causes to Components and Failure Modes (Figure 11, Figures 16-25, and Table 1)
4) Verify Inhibit sufficiency
5) Generate Safety (SDP) and Hazard Reports (HRs)
6) Iterate modeling/assessment

Further, this study tested if modeling tools could be used produce a Safety Requirements Compliance Checklist (SRCC), which identifies applicability, compliance, non-compliance or tailoring for NASA STD 8719.24; elevates the understanding of hazard dependencies; and facilitates inhibit sufficiency verification/evaluation. The latter was done by generating safety fault trees and 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

2.2 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), 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 tool listed 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 representative tool selected was MADE and the second was SysML/ MagicDraw (SysML based tool from NoMagic) with Tietronix Reliability plugins and associated stereotypes [3, 4].

When the 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 one or more tools from the original set that could also support Safety, including 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 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), for 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.

2.2.1 MADE

The modeling tool Maintenance Aware Design Environment (MADE) provides a suite of software tools that can be used to design, assess, and optimize 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. 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 Society of Automotive Engineers (SAE) ARP 4761 - "Guidelines and

Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment" [6]. 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 [6]. 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].

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 that induce safety impacts are added with specific verification methods (analysis, 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 the 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.

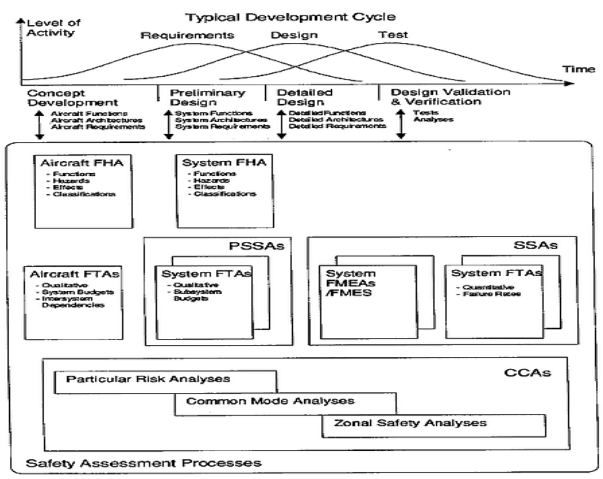


Figure 2: SAE Safety Assessment Process Overview [6]

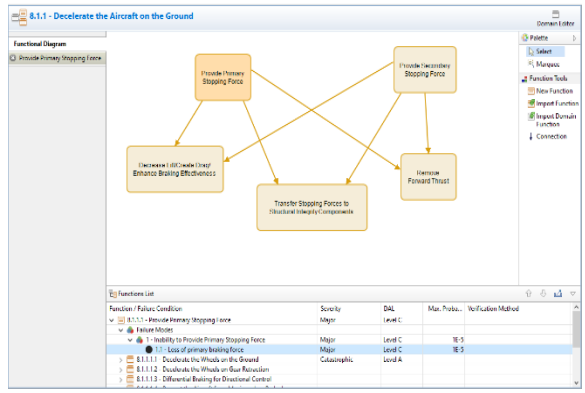


Figure 3: MADE Functional Diagram (FD) with failure conditions [4]

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 only model-based 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 one or more signals, energy, and/or material flow state changes (either continuously or discretely) into the system. During these simulations MADE propagates the injected settings through the system and shows the results graphically to the user (Figure 6).

2.2.2 SysML/MagicDraw

Reserved for update when SysML/MagicDraw system safety capability is realized.

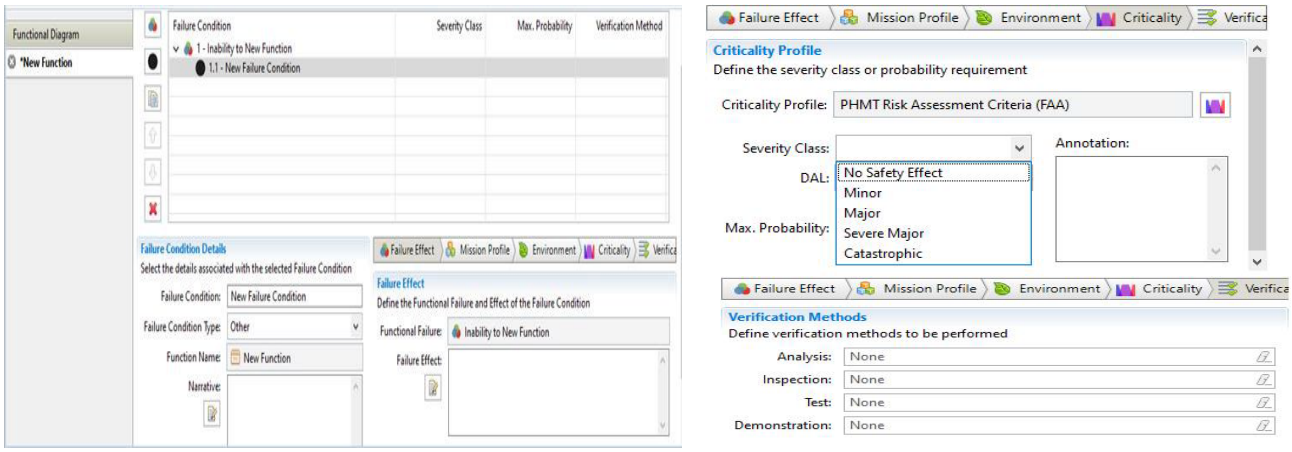


Figure 4: MADE Hazard Properties Input Fields [4]

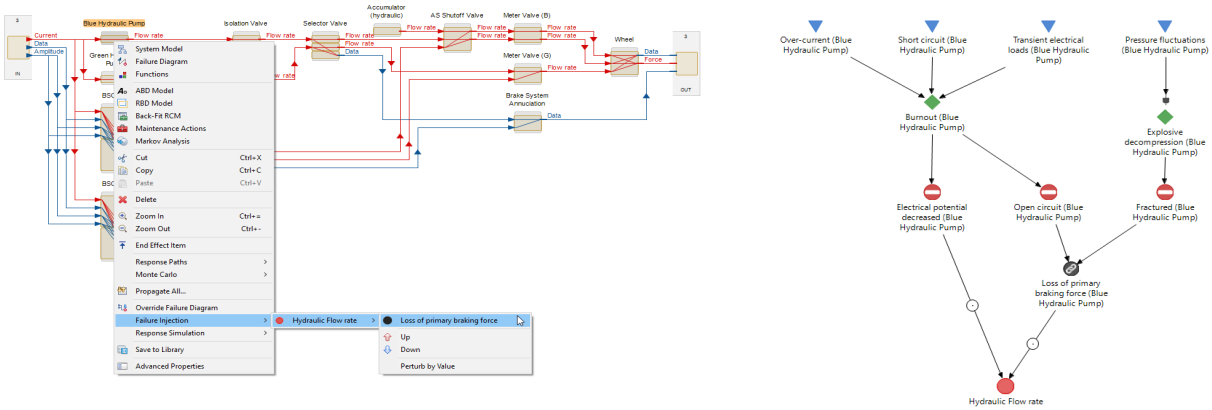


Figure 5: Hazard Enhanced Functional Block Diagram and Failure Diagram (*MADE* aircraft model [8])

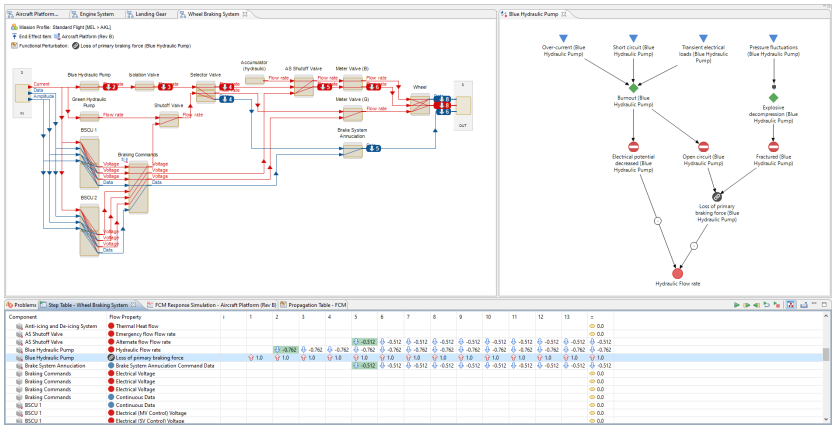


Figure 6: *MADE* Simulation Results (MADE aircraft model [8])

3 MODELS AND RESULTS

3.1 Europa Propulsion

Using the recommended modeling techniques shown in Appendix B, modelers in this study were able to create a fully operational Europa Propulsion safety model, including elements of the ground support equipment, used at launch and test facilities.

3.1.1 MADE Functional Modleing

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 (See Figures A1 – A9 in Appendix A)[1]. In addition, the mission time of 12 years was entered into the MADE mission profile for quantification purposes, while the component/system duty cycles were adjusted individually. For example, tanks, service valves, and pressure transducers 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, and latch valves, were assigned duty cycles less than 1% relative to the entire mission lifetime, based on the expected mission usage.

For this system safety phase of the MBSMAI study, four additional systems were added to the model: the Ground Support Equipment (GSE), the Propulsion Module Electronics (PME), the Diode Box, and an Enable Plug to represent upstream system topologies, as shown in Figures 7 and 8 (and Appendix A) The modeling of these systems was limited to the Subsystem Level (or "black box" level) elements with only the signals, power flows, and material flows needed to activate the Europa propulsion system.

3.1.1.1 GSE-PGSE MADE Functional Modeling

The GSE modeling element is an upper-level modeling construct that houses the Propulsion Ground Support Equipment (PGSE) and provides signal aggregation (e.g., four PCA-Latch-Valve and eight PIA-Latch-Valve signals were combined into a single Fire Thruster Signal). As modeled, the GSE element provides two electrical aggregated signals/data outputs (blue lines in Figure 7), one power output flow (red line in Figure 7), and four material flows (green lines in Figure 7) from the PGSE. One signal is the command "firing" of thrusters, and the other signal is the command "arm" of thrusters (blue lines in Figure 7). One power output flow (red line in Figure 7) sends power to the PME, Diode Box, and downstream propulsion components. Four material Fuel/Oxidizer output flows (green lines in Figure 7) send material to the Fuel tank, Oxidizer tank, pressurant tanks, and respective service valves. Modeling of the flows was manually defined according to the physical signal type to be provided by the PGSE to the downstream component.

The PGSE consists of electronics to emulate the on-board Command and Data Handling (C&DH) system as well as a pressure cart that controls the flow and pressure of propellent material (i.e., fuel, pressurant, and oxidizer) being loaded. It provides all the individual external signals and power flows to the GSE-modeling construct that operationally would come from the spacecraft's C&DH subsystem and provides the material flows for loading the propulsion subsystem. As modeled, the PGSE has sixty electrical, four power, and four material signals input. Of the sixty electrical signals, forty-eight are manually defined as thruster signals, four as PCA Latch Valve signals, and eight as PIA Latch Valve signals. The Fire component element aggregates the PCA and PIA Latch Valve signals into a single Fire Thruster signal output (Figure 9 and A80). The Arm component element aggregates the REMs signals into a single Arm Thruster signal output (Figure 9). The four power signals are generic in accordance with the library element and are combined by the Power Supply component to provide a single power signal. However, since the PGSE has no-internal modeling, material-flows were automatically combined by MADE based on material-type. This resulted in two flows, gas and liquid within the PGSE. These were then separated into the four output flows from the GSE (oxidizer pressurant, fuel pressurant, fuel, and oxidizer) (Figure 9) to appropriately model the material provided to downstream components.

3.1.1.2 Propulsion Module (PME and Diode Box) MADE Functional Modeling

The Propulsion Module is an interface unit between the C&DH and the propulsion subsystem. It consists of the PME and the Diode Box. The PME is responsible for controlling spacecraft thruster operations (as well as other spacecraft functions that were not related to this study's test case and were not modelled) by generating coordinated pulses to engines and using hardware logic to control PCV pulses based on Pressure Transducer measurements for the propulsion subsystem. Whereas the Diode box provides cross-strapped power interfaces to propulsion components, kickback suppression for the propulsion subsystem, and electrical isolation of cross-strapped power and telemetry signals. As modeled, the PME has four output power services, which provide power to the REM thrusters, Pressure Transducers, PCA Latch Valves, and the PIA Latch Valves (red lines in Figure 8) via the Diode Box. These are made electrically isolated and cross-strapped by the Diode Box to the appropriate downstream propulsion components. Therefore, the PME was modeled with sixty-eight electrical signals/data outputs that represent the command-lines to the REM thrusters, PCA Latch Valves, and the PIA Latch Valves (blue lines in Figure 8) that go through the Diode Box to implement parallel signal distribution to the downstream propulsion

components (See also Figure A13).

GSE

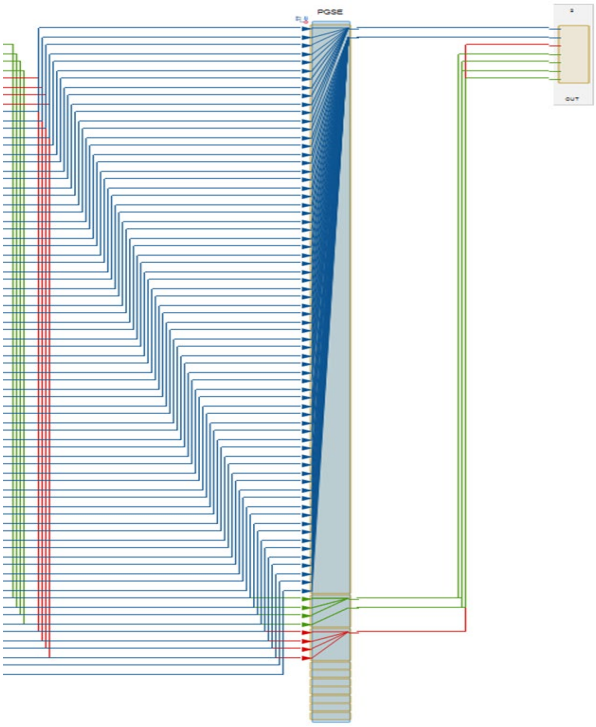


Figure 7:MADE EUROPA GSE

Propulsion Module

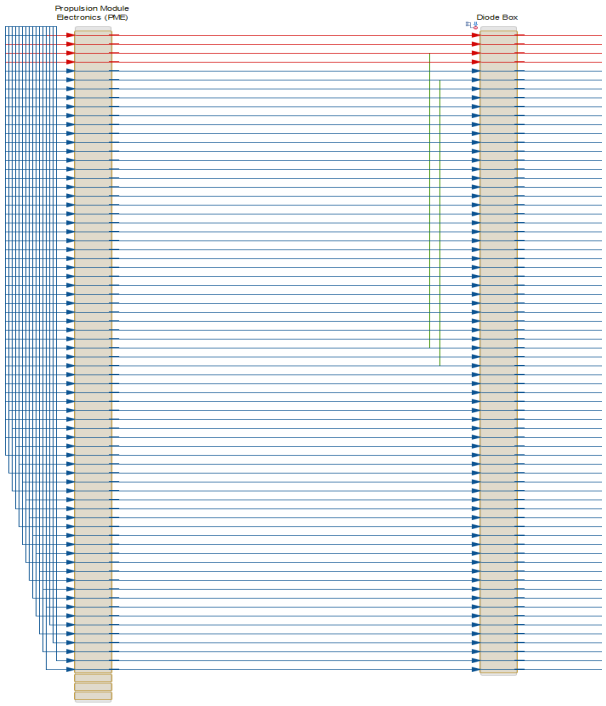


Figure 8:MADE EUROPA Propulsion Module

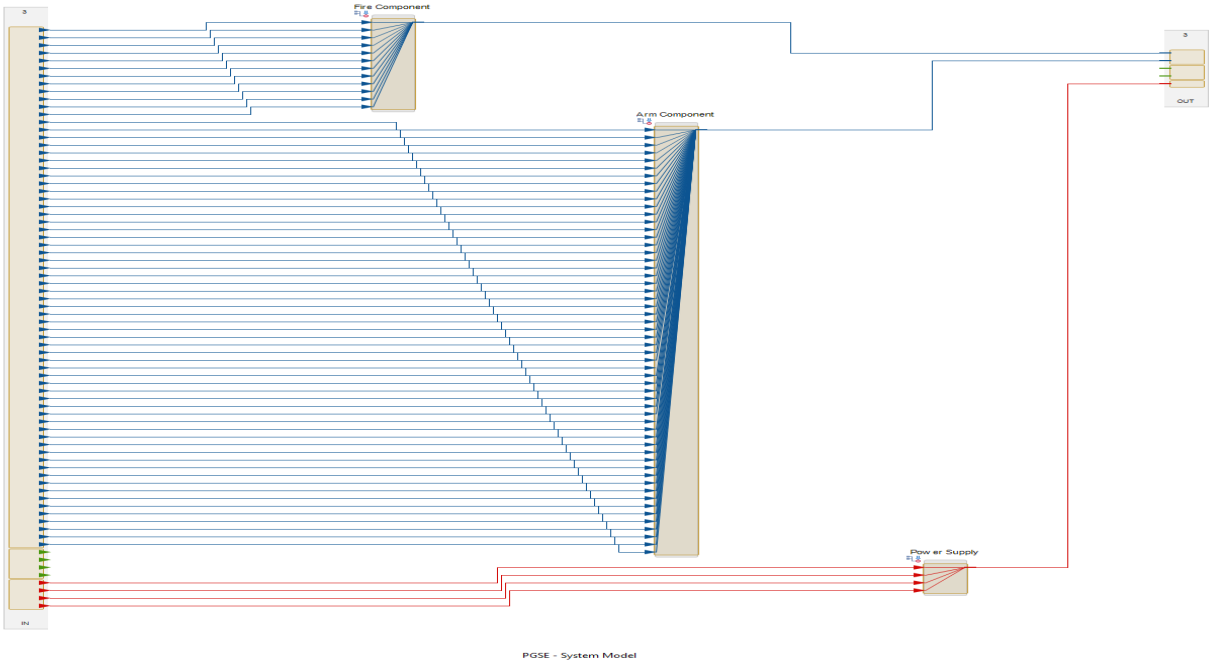


Figure 9: MADE EUROPA PGSE

3.1.1.3 Enable Plug

An enable plug is a safety feature that completes a circuit for deployment or activation of thruster valves. Without the plug installed, the signal cannot be sent to fire a thruster. In the Europa propulsion design, there are enable plugs between each REM and its power source (Figure 10), however a single enable plug was modeled to emulate the function of these plugs. For modeling purposes, the location of the Enable Plug was set between the Diode Box and the power supply for thrusters in the Propulsion system to control power reaching all REM thrusters. The Enable Plug was modeled as a single power output flow from the MADE component library with predefine flow and functional properties.

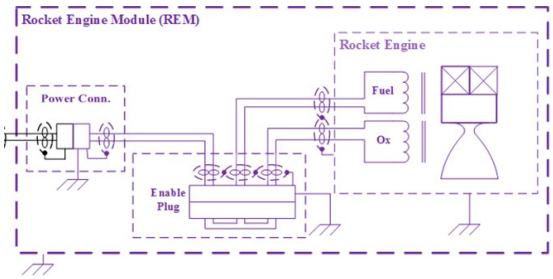


Figure 10: EUROPA Enable Plug

3.1.2 MADE Hazard Modleing

As mentioned in section 2.1.1, MADE's approach to safety analysis is an SAE ARP 4761 based approach while GSFC's safety approach is based upon MIL-STD-882 and follows NASA STD 8719.24. Specifically, GSFC's safety process consists of first identifying all the components in a system, subsystem, or testing facility and then associating these components with the applicable GSFC standard hazard categories. Therefore, to perform NASA safety analyses in MADE, hazard categories were entered as *Functions* and hazards were equated to *Functional Failures* and hazard causes to *Failure Conditions* in the model's *Functional Diagram* based on system safety engineering analysis. To perform this analysis, a table of modelling elements and hazard categories were used to identify relevance and track modeling, as indicated in Figure 11.

Relevance was assessed by evaluating each modeling element's capability of creating a hazard based on the implications noted for each category (the text box descriptions in Figure 12). As a result, the *Functional Diagram* for Europa propulsion (Figure 13) has twelve hazard categories of which ten are used for Europa propulsion.

Hazard Categories																
Green X = represents components belonging to the hazard's category **Blank Space** = no connection Component	Acceleration/Decelerations	Contamination/Corrosion	Electrical/Grounding	Control Systems	Explosives	Fire/Explosion	Human Factors	Leaks/Spills	System Life Cycle	Materials	Mechanical	Physiological	Pressure/Hydraulic	Radiation	Structural	Temperature
Fuel Tank		X			N/A: Fuel Encompassed in Tank	X		X			Assumes tanks are already integrated, no separate lifting	X	X		X	
Oxidizer Tank		X				X		X				X	X		X	
Pressurant Tank - Fuel												X	X		X	
Pressurant Tank - Oxidizer												X	X		X	
Latch Valves						X		X			N/A Covered elsewhere		X			
Pressurant Control Valves						X							X			
Service Valve						X		X					X			
Thrusters						X		X			N/A Covered elsewhere					X
Harness			See PME	See PME		See PME										
PME			X	X		X		Covered in Component				Covered in Component				
PGSE			X	X		X	N/A Covered Elsewhere	X			X	N/A: Not responsible for launch site tanks				
Filter								Filters are part of tanks				Filters are part of tanks	Filters are part of tanks			

Figure 11: GSFC Component vs Hazard Category Table, populated for EUROPA Propulsion

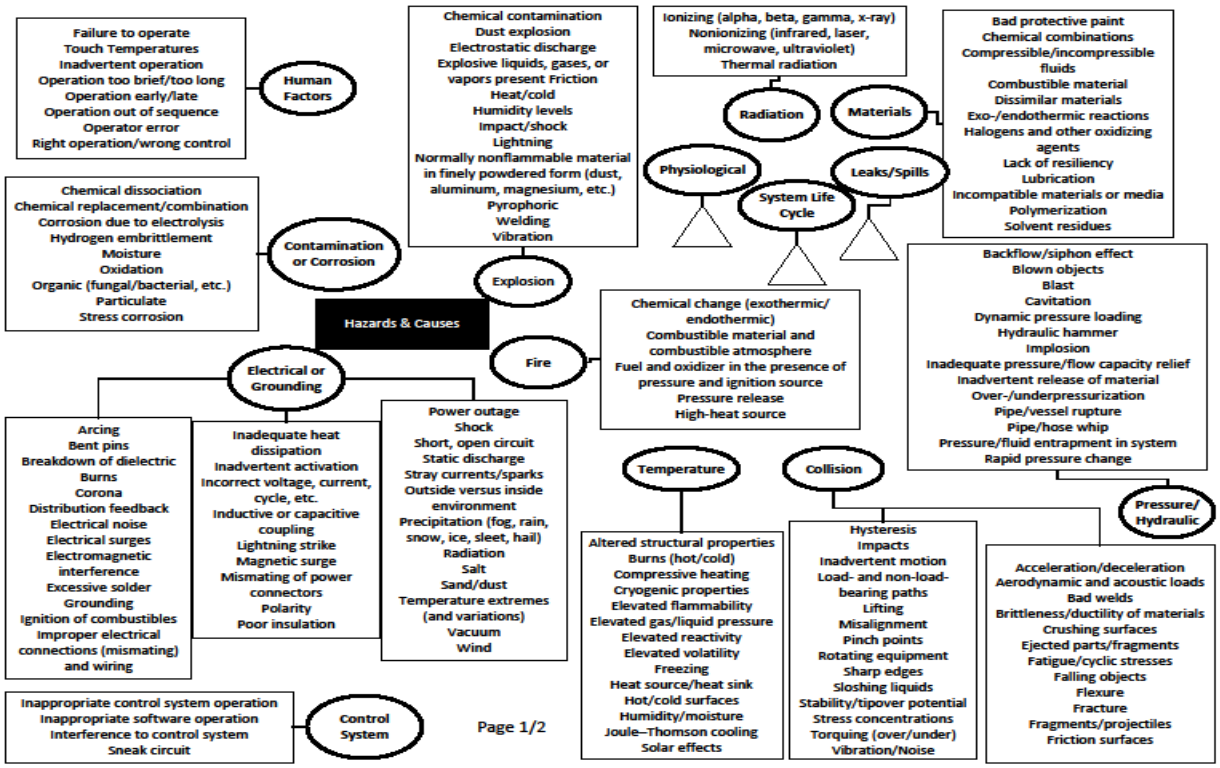


Figure 12: GSFC Hazard Category and Implications
(Double click on figure to open pdf)

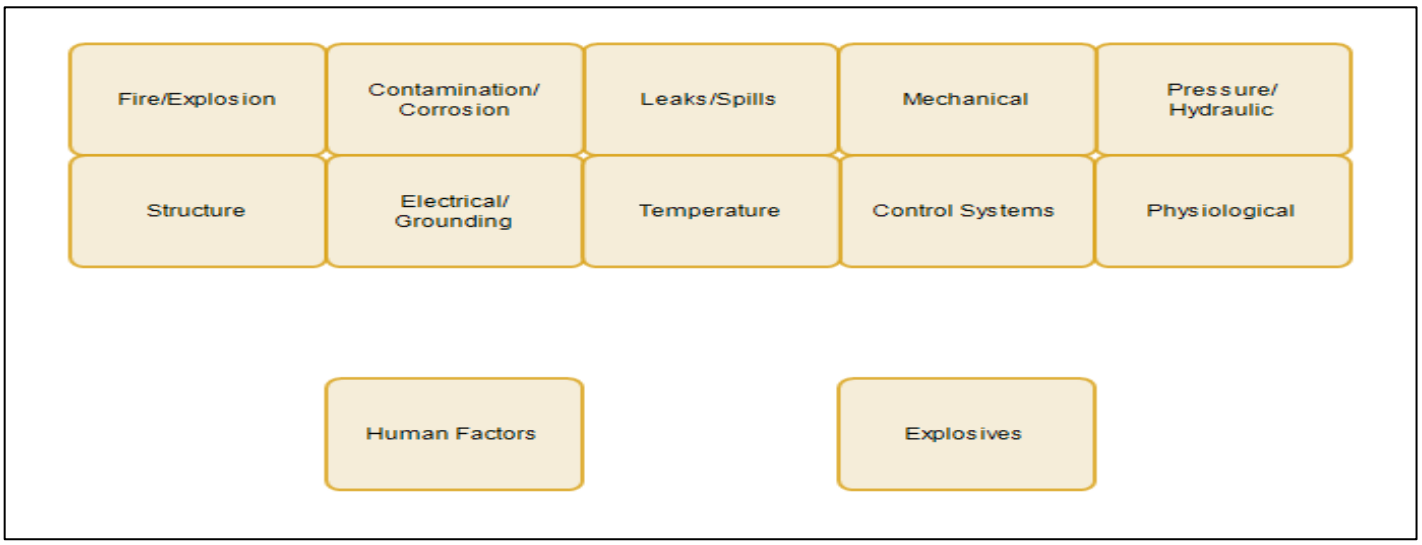


Figure 13: MADE EUROPA *Functional Diagram*

Further analysis of each hazard included evaluating the hazard's causes, severity, maximum probability, hazard controls, and verification methods to address all risks pertaining to the hazard. Specifically, the following elements were then manually entered for each hazard (See Figures 16-25 and safety-parameters (Table 1) or the EUROPA propulsion HA report (Figure 26)): the hazard name/title, hazard description (as modeling element narratives), hazard causes, verification methods, hazard controls (as modeling element annotations), effect and severity of the hazard (all hazard causes were given the NASA catastrophic effect definition (except for one, which was given major) and the catastrophic severity level values), likelihood of occurrence (Maximum Probability of each hazard's occurrence was given a default value of $1*10^{-4}$ unless it could be proven otherwise), and applicable mission phases/environments (pre-launch in all cases for this study – See Figure 15) as shown below:

- For the Fire/Explosion hazard category, the hazards assessed were: "Propellent (MMH) Release," "Oxidizer (MON-3) Release," "Inability to Isolate Fuel (MMH) from Oxidizer (MON-3)," Inadvertent firing of Thruster," and "Electrical Overheating/Short Circuit." Each one was assigned causes (e.g., "Harness Short Circuit"), each with a severity of catastrophic, based on the assessment of potential safety impacts and the default likelihood cited above. Hazard control(s), such as "Test all harness circuits during integration" and verification method(s), such as "All circuits tested during integration," were added to each control to complete the hazard modeling (See Figure 16). All hazard modeling assignments and parameters can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 6 and 10-14).

- For the Leaks/Spills hazard category, hazards assessed were "Propellant (MMH) Release" and "Oxidizer (MON-3) Release," as shown in Figure 17. 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 to fuel and oxidizer components. Each of these causes was also assigned a severity, default likelihood, control(s), and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling. All hazard modeling assignments and parameters can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 6-7 and 15-18).

FUNCTION	Electrical/Grounding		
FUNCTIONAL FAILURE	1 - Electrical/Grounding Faults		
FC ID FAILURE CONDITION	1.1 Electrical Surges	1.2 Improper Electrical Connections (mismating) and Wiring	1.3 Improper/Multiple Grounding planes
NARRATIVE	permit anomalous overvoltages and overcurrents to be present, that could cause short circuits, open circuits, or sparks which ignite flammable atmospheres	permit anomalous circuits to be present, that could cause short circuits, open circuits, or sparks which ignite flammable atmospheres	could permit arcing to be present, that causes short circuits, open circuits, or sparks which ignite flammable atmospheres
FAILURE CONDITION TYPE[1]	Other	Other	Other
MISSION PROFILE	3: Pre Launch	3: Pre Launch	3: Pre Launch
ENVIRONMENT	Regular load	Regular load	Regular load
EFFECT	Death or permanent total disability of personnel, irreversible significant environmental impact, and loss of equipment in excess of $10M.	Death or permanent total disability of personnel, irreversible significant environmental impact, and loss of equipment in excess of $10M.	Death or permanent total disability of personnel, irreversible significant environmental impact, and loss of equipment in excess of $10M.
PHMT RISK ASSESSMENT CRITERIA (FAA) SEVERITY CLASSIFICATION	Catastrophic	Catastrophic	Catastrophic
DEVELOPMENT ASSURANCE LEVEL (DAL)	Level A	Level A	Level A
MAX. PROBABILITY[2]	1E-4	1E-4	1E-4
ANNOTATION[3]	1.1.1 Equipment used for connecting EGSE to power supply is UL or CE certified 1.1.2 EGSE procedures include detailed instructions on use of equipment.	1.2.1. Design of EGSE and electrical connections will comply with NEC 1.2.2. Detailed procedures written to ensure connection process is correct 1.2.3. Connector caps provided to protect from FOD	1.3.1 EGSE design ensures correct grounding for ground and flight hardware 1.3.2. EGSE provides detailed procedures for grounding
VERIFICATION METHODS	Inspection: 1.1.1.1 Review EGSE UL certification (or equivalent); 1.1.2.1 Review Electrical procedures to ensure that they contain sufficiently detailed operating instructions	Inspection: 1.2.1.1 Complies with NEC (including fusing, grounding, and wire sizing); 1.2.1.2 Verify EGSE UL certified (or equivalent); 1.2.2.1 Procedures show that EGSE connected to facility ground prior to application of power; 1.2.2.2 Inspect setup prior to activation of EGSE with voltages in excess of 50 V AC designed to provide personnel protection from accidental contact; 1.2.3.1 Conduct GSE bent pin/Foreign debris contamination inspection prior to connection; 1.2.3.2 GSE bent pin/foreign debris contamination inspection prior to connection	Inspection: 1.3.1.1 Review Design to ensure proper grounding for EGSE and flight hardware; 1.3.1.2 QA ensures EGSE built in accordance with design; 1.3.2.1 Review procedures for grounding; 1.3.2.2 Inspect connections prior to power on

Table 1: Table of Safety Modeling Entries
(Double click on figure to open pdf)

- For the Structure hazard category, the hazard assessed was "Fractured/Mechanically Failed Flight Hardware," as shown in Figure 18. 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," and "Unbalanced heating of COPVs." Each of these causes was assigned a severity level, a default likelihood, control(s), and verification(s) in the same manner as shown for Fire/Explosion to complete modeling. All hazard modeling assignments and parameters can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 7 and 27).

- For the Electrical/Grounding hazard category, the hazard "Electrical/Grounding Faults" was modeled. Its hazard causes were "Electrical Surges," "Improper Electrical Connections (mismating) and Wiring," and "Improper/ Multiple Grounding planes," as shown in Figure 19. Again, each of these causes was assigned a severity, a default likelihood, control(s), and verification(s) in the same manner as shown for Fire/Explosion. All hazard modeling assignments and parameters can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 6 and 9).

- For the Pressure/Hydraulic hazard category, 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 by including a severity, control(s), a default likelihood, and verification method(s) in the same manner as shown for Fire/Explosion to complete modeling, as shown in Figure 20. All hazard modeling assignments and parameters can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 7 and 20-23).

- For the Contamination/Corrosion hazard category, the hazards assessed were "Propellent Release" and "Oxidizer Release" caused by "Mishandling," "Overpressure/improper fill," Incompatible materials," and "Defective manufacturing/mechanical failure" of tanks /lines for each hazard respectively, as shown in Figure 21. Each of these tank/line causes was then assigned a severity, default likelihood, control, and verification in the same manner as shown for Fire/Explosion to complete modeling. All hazard modeling assignments and parameters can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 7 and 24-25).

- For the Mechanical hazard category, 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," as shown in Figure 22. These were then assigned a severity, a default likelihood, verification(s) and control(s), in the same manner as shown for Fire/Explosion to complete modeling. All hazard modeling assignments and parameters can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 7 and 19).

- For the Temperature hazard category, 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 COPVs," as shown in Figure 23. Each of these causes was assigned a severity, a default likelihood, control(s), and verification(s) in the same manner as shown for Fire/Explosion to complete modeling. These details can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 7 and 24).

- For the Control Systems hazard category, 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," as shown in Figure 24. Each of these causes was again assigned a severity, default likelihood, control(s), and verification(s) in the same manner as shown for Fire/Explosion to complete modeling. These details can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 6 and 9).

- For the Physiological hazard category, the hazards assessed were "Asphyxiates" and "Irritates". The hazard causes identified for the "Asphyxiates" hazard by the team's system safety expert were "Helium Pressurant (for Fuel) rich atmosphere" and "Helium Pressurant (for Oxidizer) rich atmosphere"; the hazard causes identified for "Irritates" by the team's system safety expert were "Propellant (MMH) rich atmosphere" and "Oxidizer (MON-3) rich atmosphere." All hazards and hazard causes are as shown in Figure 25. Each of these causes was assigned a severity, default likelihood, control(s), and verification(s) in the same manner as shown for Fire/Explosion to complete modeling. These details can be found in Table 1 and the EUROPA propulsion HA report (Figure 26, pages 7-8 and 27-28).

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 (See Figures A12 – A80 in Appendix A). For example, for the hazard category of "Fire/Explosion" (shown as the brown hexagon in Figure 14), 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 14) for that component as failure conditions (black circles). This modeling results in these hazard causes being reported in the failure scenarios of model-based FTAs and appear as failure-mode function information in the FMECA (image on the right of Figure 14), which is advantageous to overall system analysis and communication, 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.

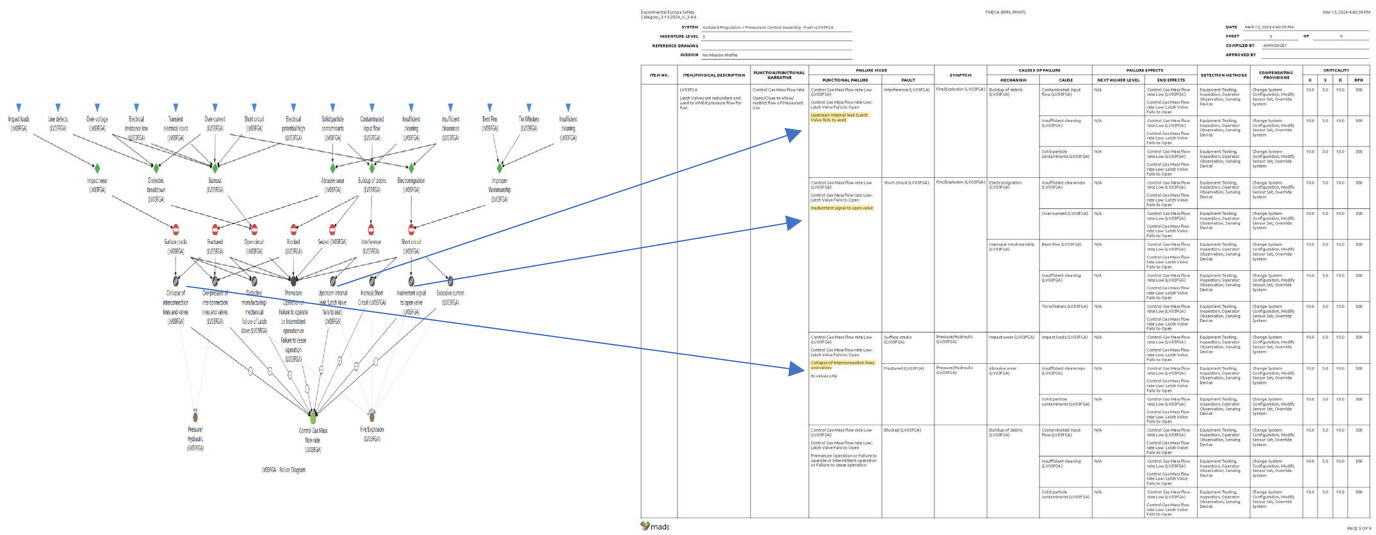


Figure 14: MADE Failure Diagram Safety Causes and FMECA reporting

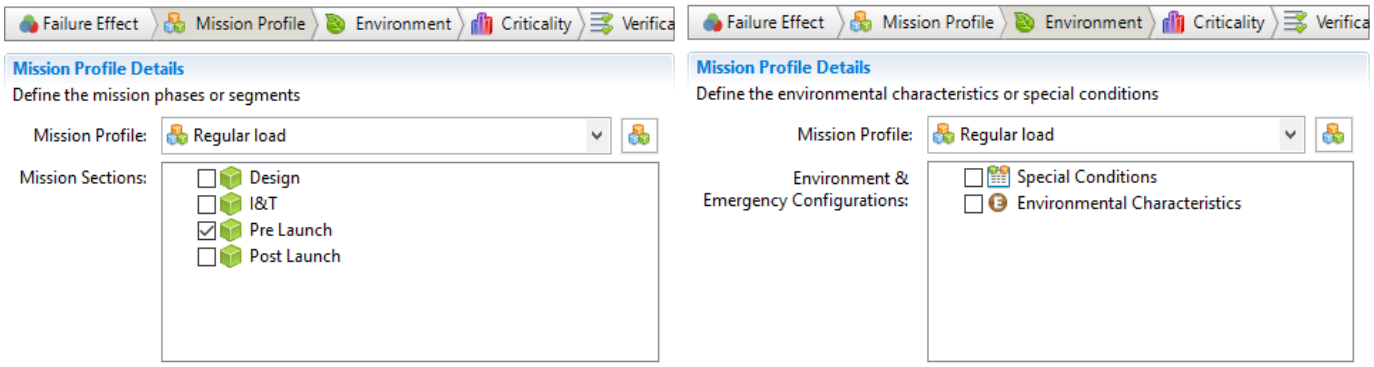


Figure 15: MADE EUROPA Mission phases/environments

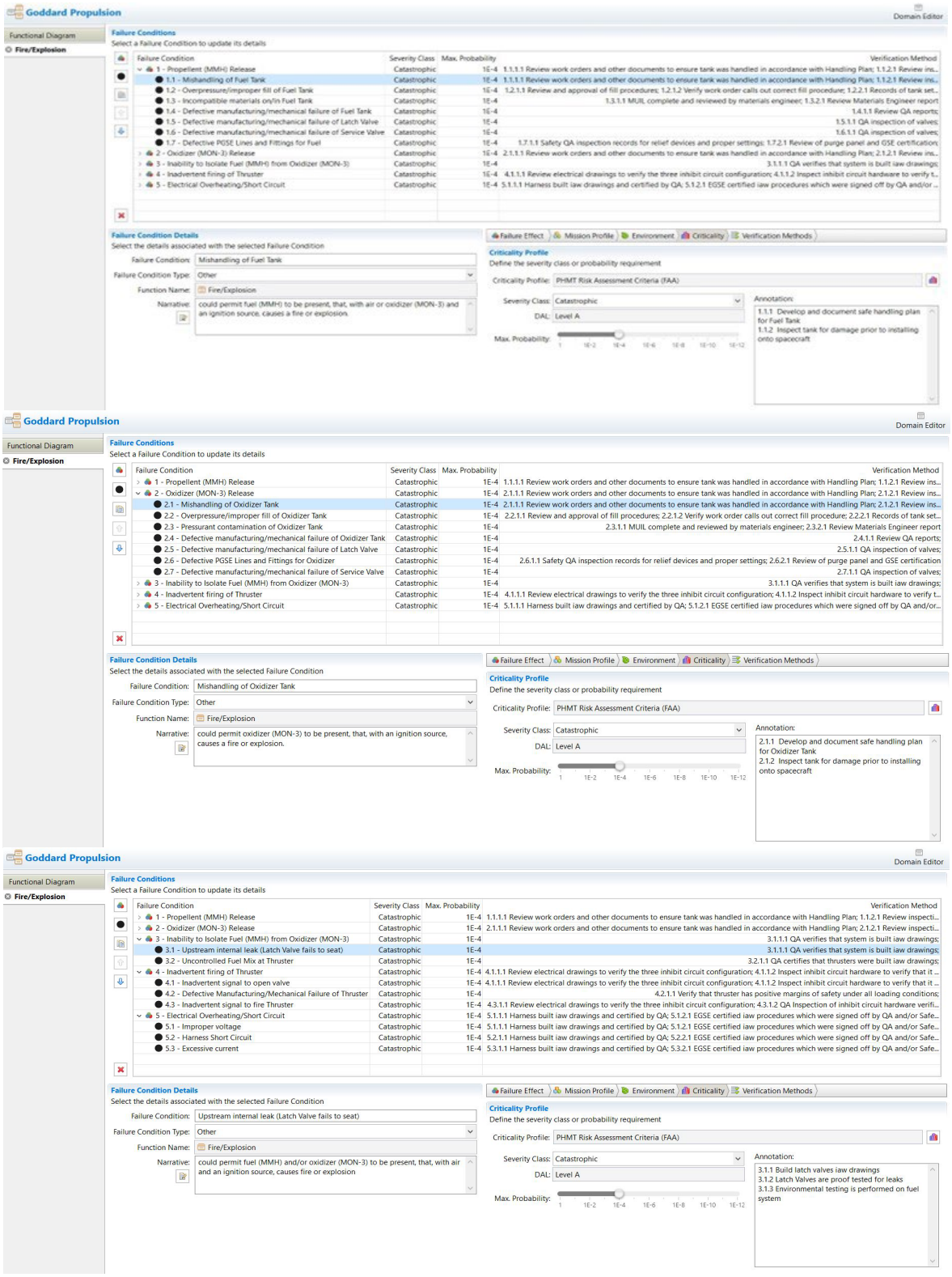
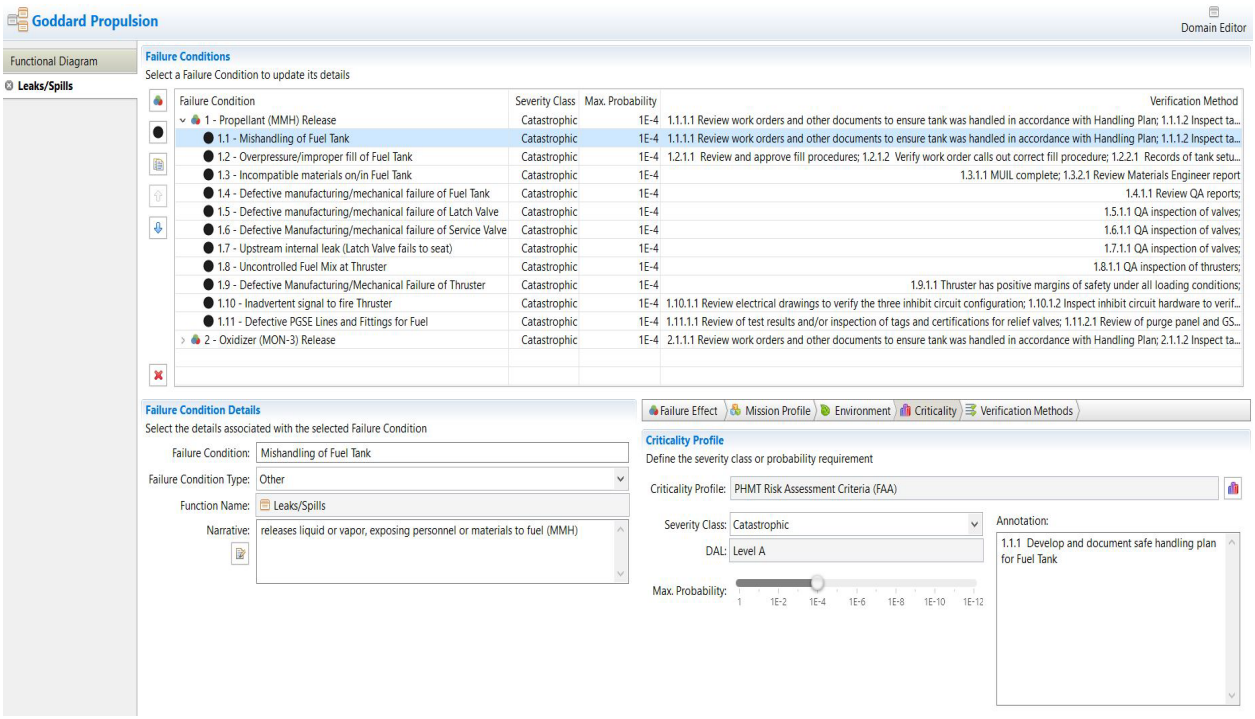


Figure 16: MADE EUROPA Fire/Explosion



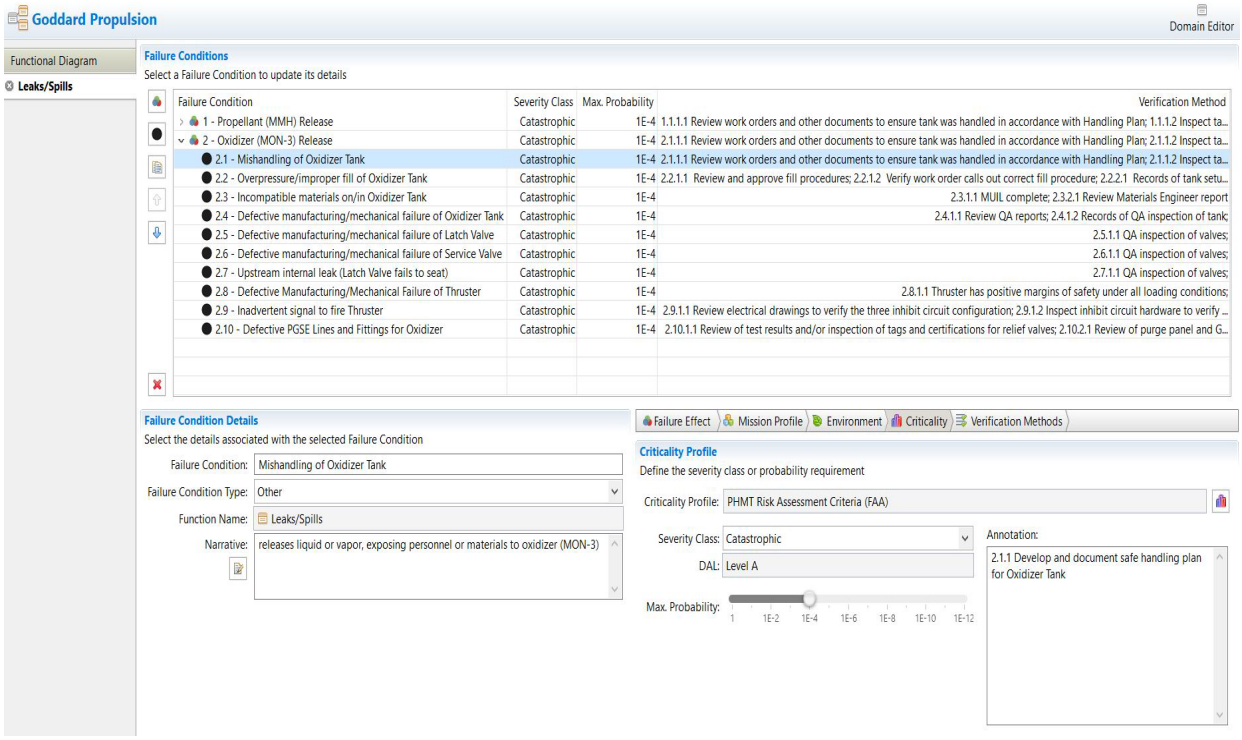


Figure 17: MADE EUROPA Leaks/Spills

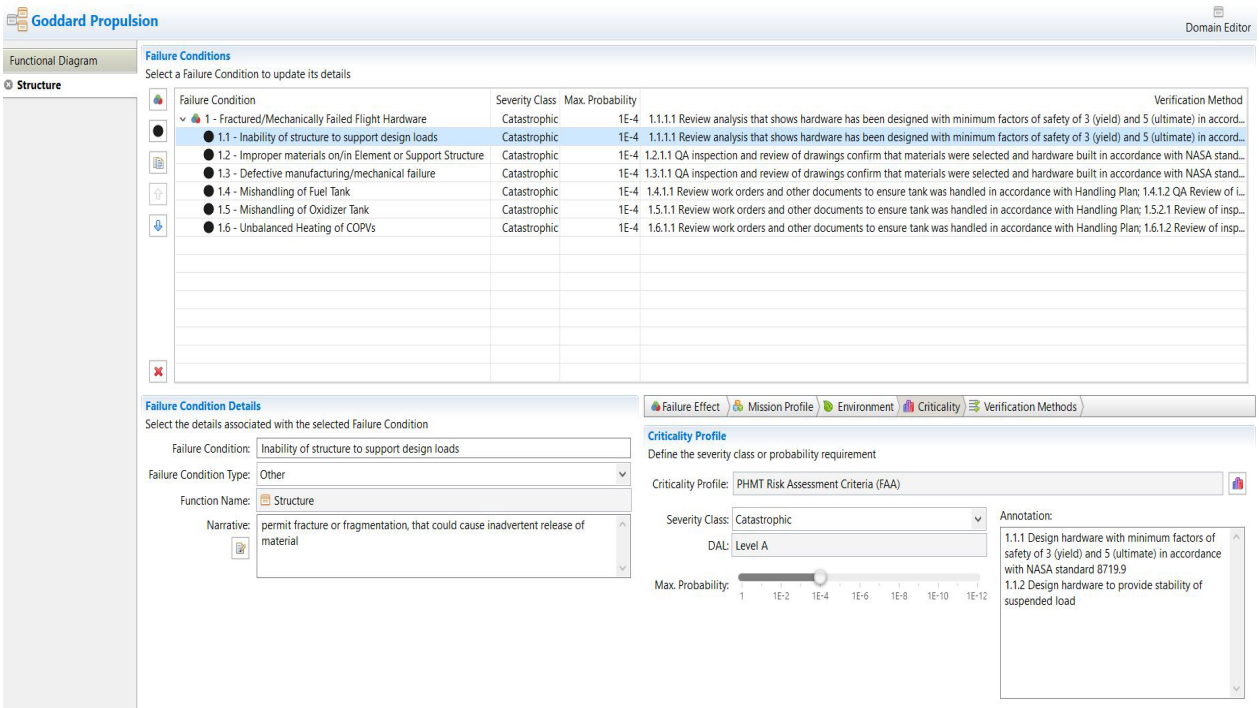


Figure 18: MADE EUROPA Structure

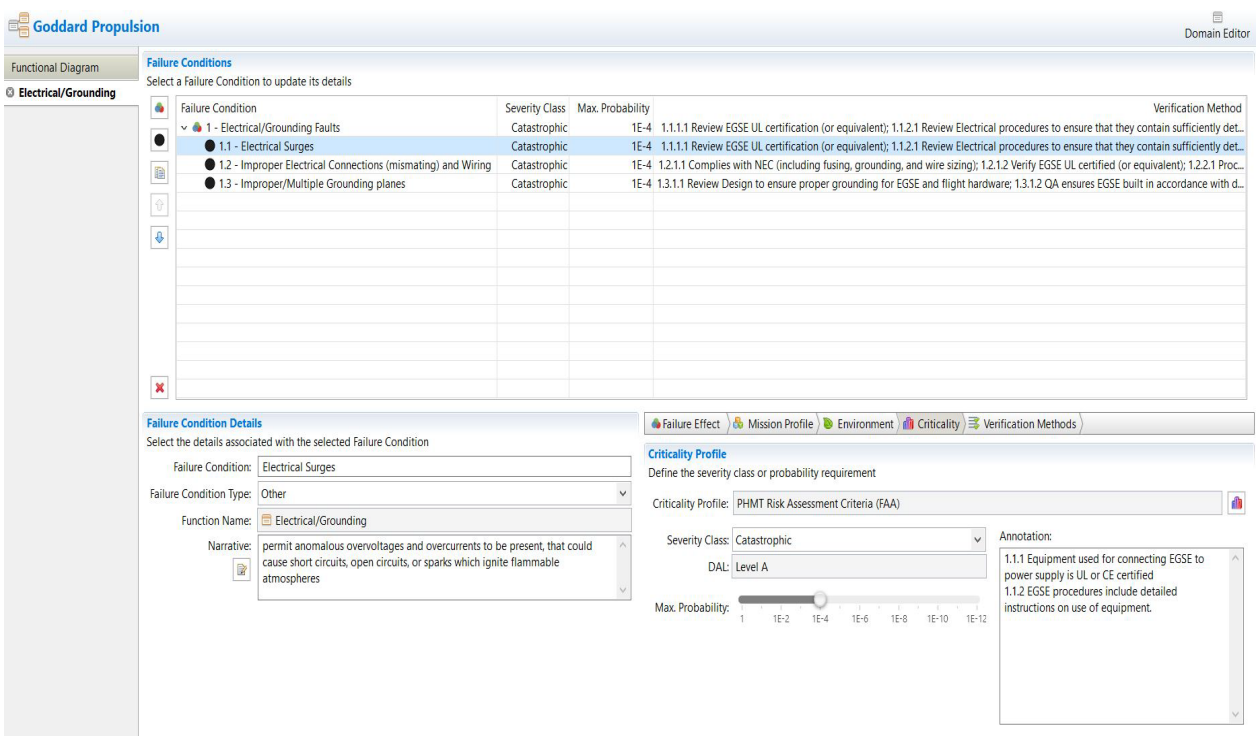


Figure 19: MADE EUROPA Electrical/Grounding

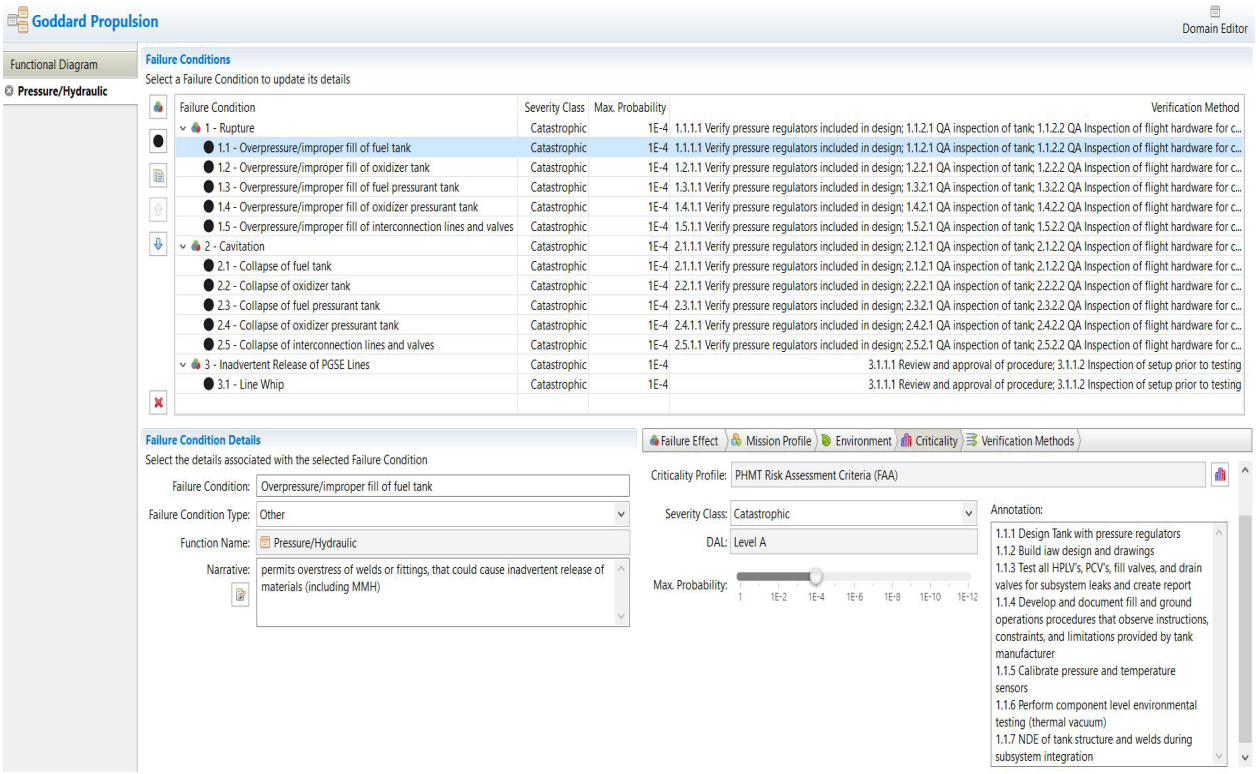


Figure 20: MADE EUROPA Pressure/Hydraulic

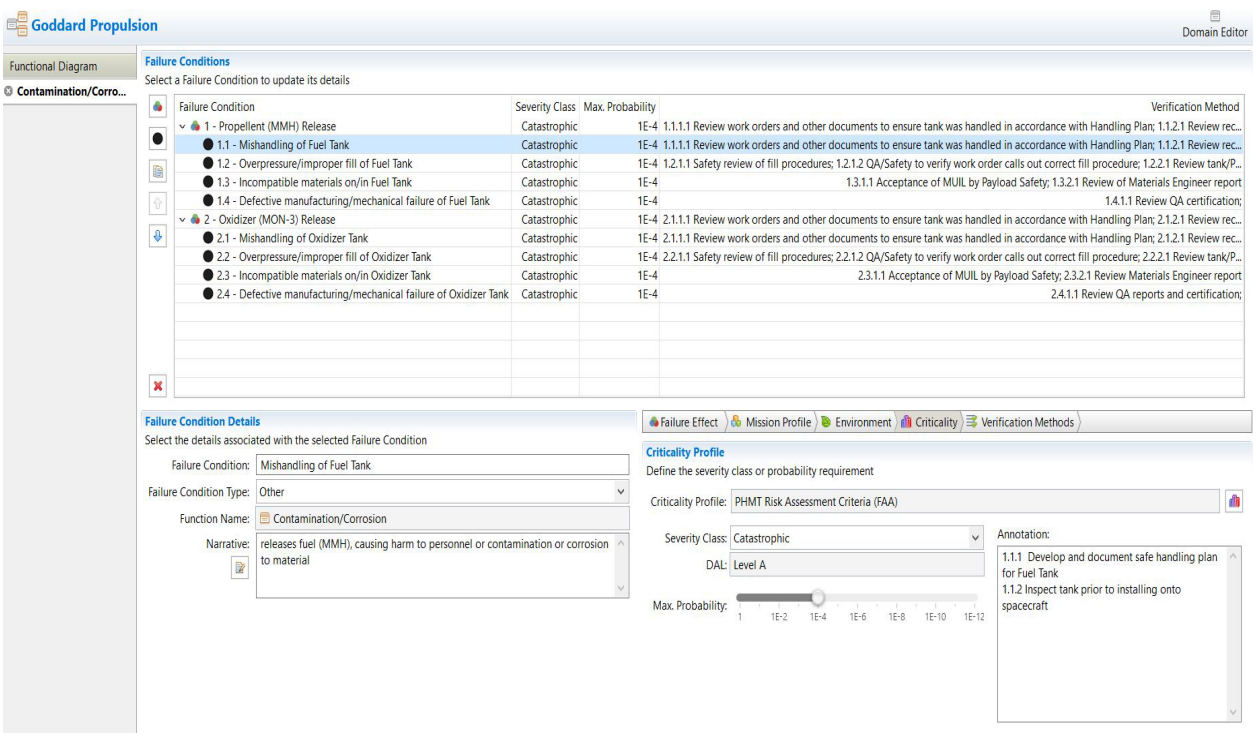


Figure 21: MADE EUROPA Contamination/Corrosion

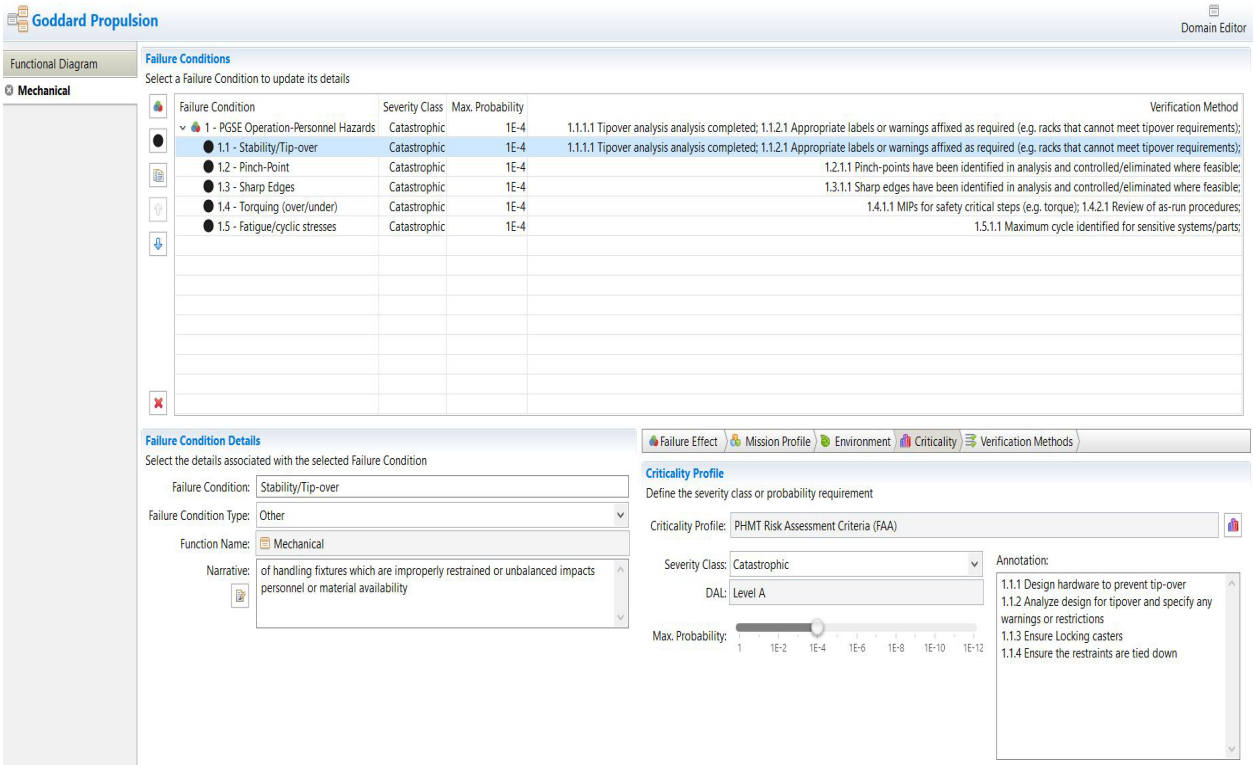


Figure 22: MADE EUROPA Mechanical

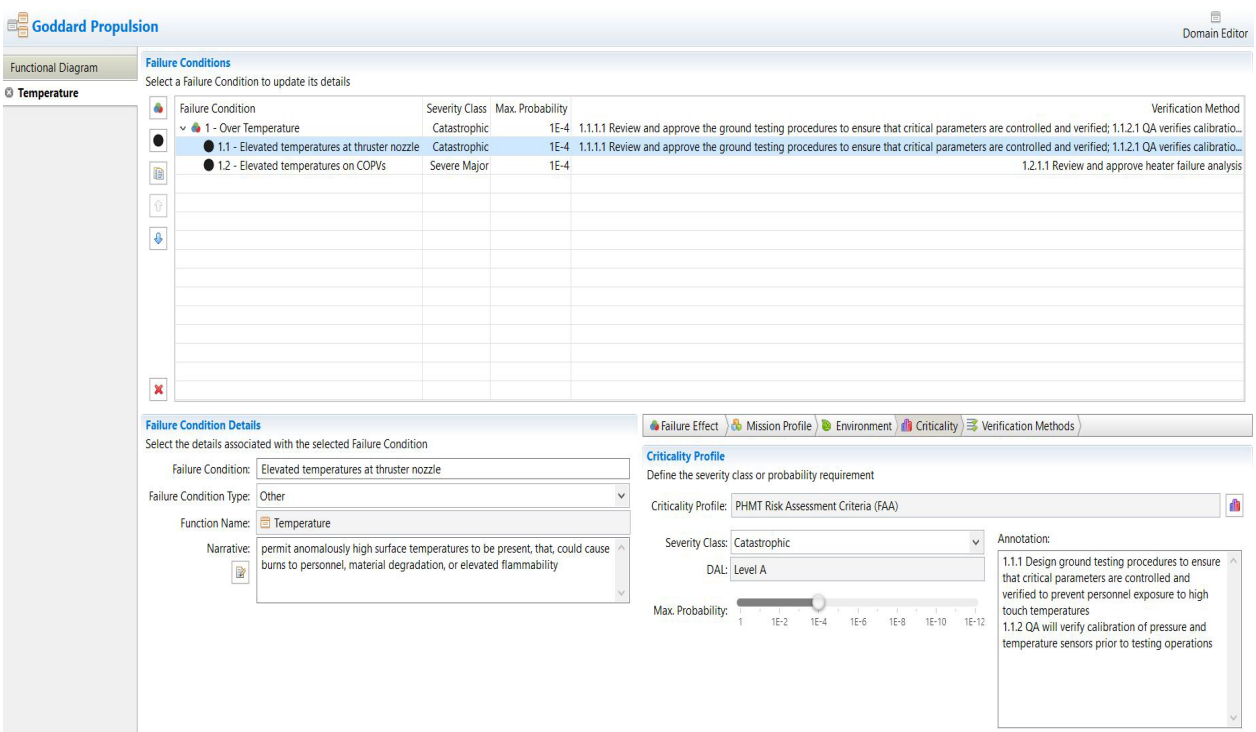


Figure 23: MADE EUROPA Temperature

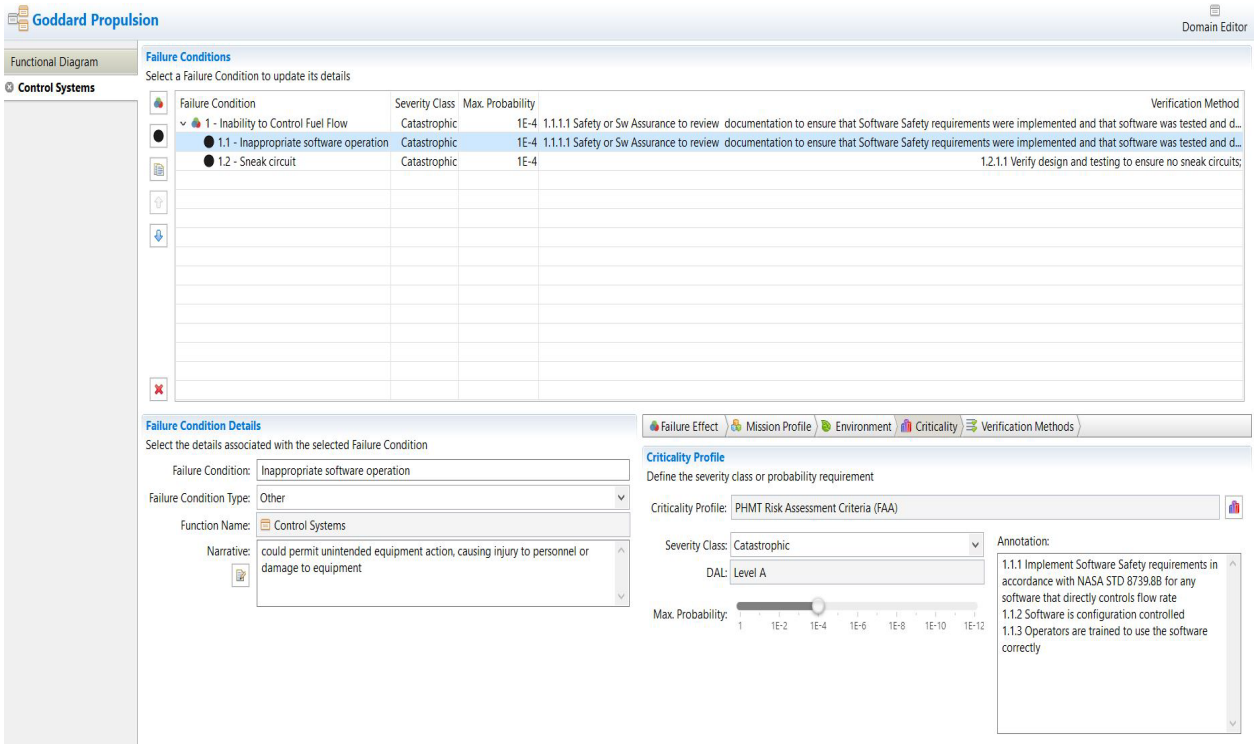


Figure 24: MADE EUROPA Control Systems

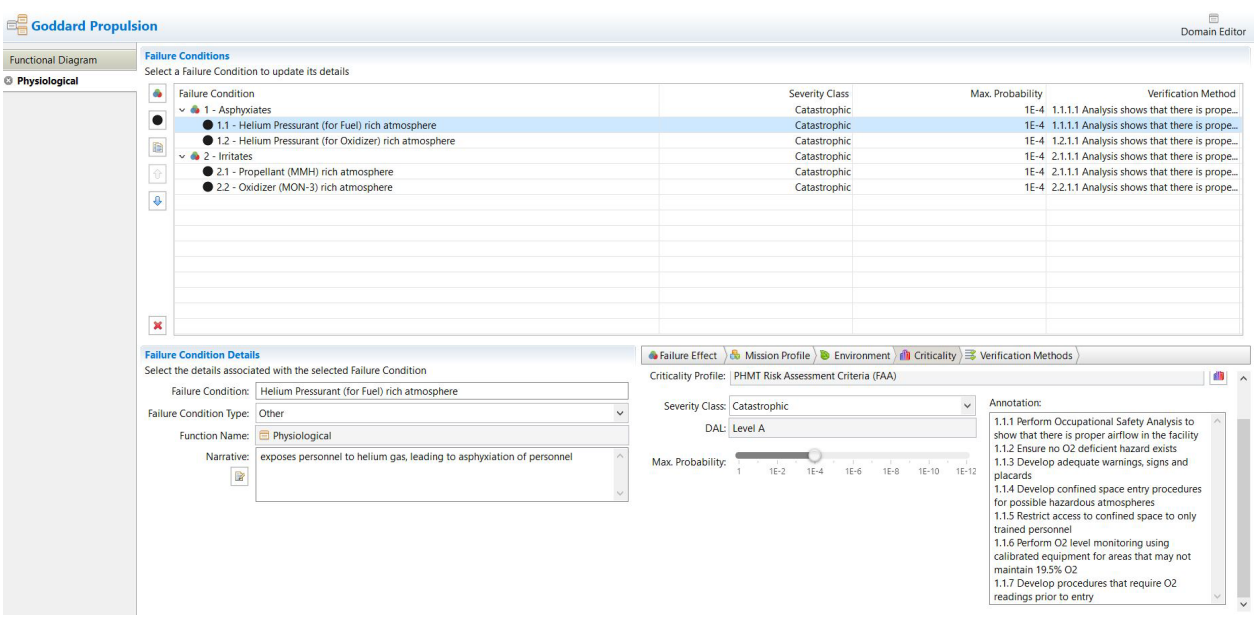


Figure 25: MADE EUROPA Physiological

3.2 SysML/MagicDraw

Reserved for update when SysML/MagicDraw system safety capability is realized.

3.3 Results and Observations

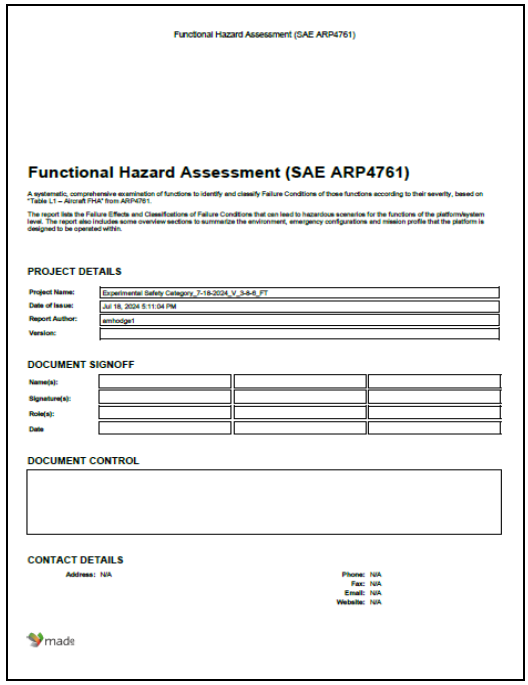
Models produced for this study (described in prior sections) were used to conduct hazard analyses and produce a set of safety products. The most hazardous case for the EUROPA Propulsion Subsystem is fueling at the launch site, so this was the selected case for modeling in this study. The model produced a Hazard Analysis (HA), a Safety Data Package (SDP) descriptive section, and a Safety Requirements Compliance Checklist (SRCC) and provided simulations to verify inhibit structures. Additionally, MADE failure diagrams were translated into a Safety Fault Tree Analysis (SFTA). These results were compared to those produced using traditional methods (Note that the SFTA is an additional product not produced in the traditional analysis).

MADE results (artifacts) are based on the same source data mentioned earlier and run for a specific/selected phase. The Functional Hazard Assessment was developed in MADE from the Functional Model (see section 3.1.2) and a hazard report was generated based on each hazard category and associated parameters (See Table 1).

3.3.1 Hazard Analysis (HA)

The MADE Propulsion Subsystem HA report (Figure 26) contains the description of the subsystem with the complete details of the mechanisms and components provided in the subsystem diagram. The subsystem description also identifies the energy hazards and introduces the system design risks and barriers designed into the system, such as redundancy or energy controls. In the later chapters of the report, there are details about the Electrical Ground Support Equipment (EGSE), Pressure Ground Support Equipment (PGSE), and how these support systems facilitate different types of tests of components and mechanisms. The last chapter discusses risks associated with Europa's propulsion system, such as rupture, leakage, mixing of fuel and oxidizer, and electrical fire. This chapter describes the relationship between the type of tests supported by GSE and hazards mitigated by these tests.

The appendix of the MADE HA report contains three tables: *Function List, Derived Safety Requirements List,* and *Functional Hazard Assessment*. These three tables are automatically generated from MADE. The *Function List* table is comprised of the main internal functions of the system. The *Derived Safety Requirements List* table connects system functions to the *Functional Failure* (hazard), *Failure Condition* (hazard description), and severity classification. The *Functional Hazard Assessment* table contains the analysis of hazard controls and verification methods and connects these items to the functions and failure conditions.


Functional Hazard Assessment (SAE ARP4761)

Functional Hazard Assessment (SAE ARP4761)

A systematic, comprehensive examination of functions to identify and classify Failure Conditions of those functions according to their severity, based on "Table L1 – Aircraft FHA" from ARP4761.

The report lists the Failure Effects and Classifications of Failure Conditions that can lead to hazardous scenarios for the functions of the platform/system level. The report also includes some overview sections to summarize the environment, emergency configurations and mission profile that the platform is designed to be operated within.

PROJECT DETAILS

Project Name:	Experimental Safety Category_7-18-2024_V_3-8-6_FT
Date of Issue:	Jul 18, 2024 5:11:04 PM
Report Author:	emhodge1
Version:	

DOCUMENT SIGNOFF

Name(s):			
Signature(s):			
Role(s):			
Date			

DOCUMENT CONTROL

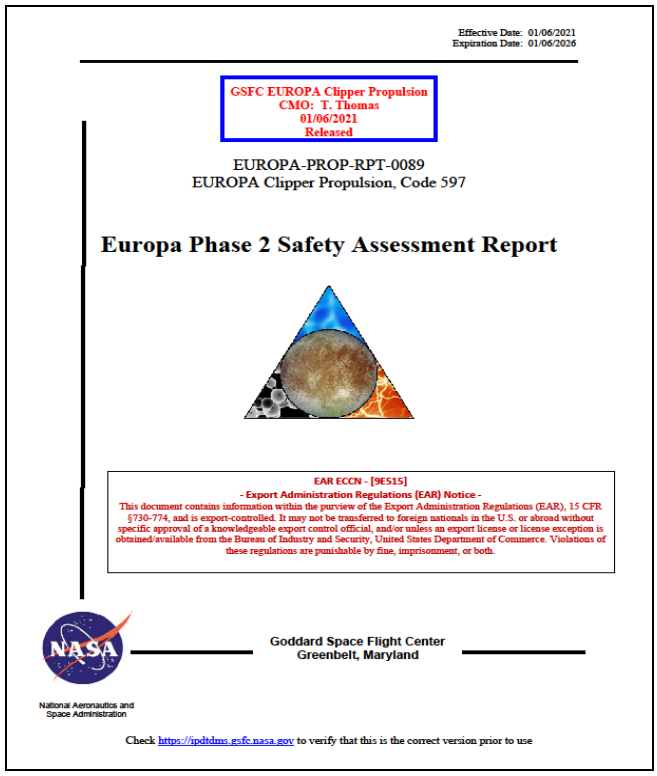
CONTACT DETAILS

Address: N/A

Phone: N/A
Fax: N/A
Email: N/A
Website: N/A

made

Figure 26: MADE HA
(Double click on figure to open pdf)


Effective Date: 01/06/2021
Expiration Date: 01/06/2026

GSFC EUROPA Clipper Propulsion
CMO: T. Thomas
01/06/2021
Released

EUROPA-PROP-RPT-0089
EUROPA Clipper Propulsion, Code 597

Europa Phase 2 Safety Assessment Report

EAR ECCN - [9E515]
- Export Administration Regulations (EAR) Notice -
This document contains information within the purview of the Export Administration Regulations (EAR), 15 CFR §730-774, and is export-controlled. It may not be transferred to foreign nationals in the U.S. or abroad without specific approval of a knowledgeable export control official, and/or unless an export license or license exception is obtained/available from the Bureau of Industry and Security, United States Department of Commerce. Violations of these regulations are punishable by fine, imprisonment, or both.

Goddard Space Flight Center
Greenbelt, Maryland

National Aeronautics and Space Administration

Check https://ipdtdms.gsfc.nasa.gov to verify that this is the correct version prior to use

Figure 27: Traditional SAR
(Double click on figure to open pdf)

The main difference between the MADE Propulsion Subsystem HA report (Figure 26) and the traditional report (Chapter 5 of Figure 27) is the format of the *Functional Hazard Assessment* table that is automatically generated by MADE versus the Hazard-Report forms in the traditional report.

A new capability, not currently available in the traditional method, is MADE Simulations. Simulations model a flow or operation based on energy/material/data transfer within the system. Such simulations can emulate, for example, the flow of fuel or electricity through a system. In the case of the Europa Propulsion system, simulations demonstrated that inhibits or controls functioned as expected within the context of the model. While not a part of conducting a Hazard Analysis, simulations can be used to validate the hazard controls established through the analysis. The more complex systems of systems become, the more important it is to validate the approach to hazard controls. A capability like simulations provides this function in a way that is not currently available in other tools.

3.3.2 Compliance Matrix or SRCC Analysis

The MADE Europa compliance matrix (Figure 29) or Safety Requirements Compliance Checklist (SRCC), was generated using the *Requirements* feature in MADE and a spreadsheet version of the NASA STD 8719.24 Rev A requirements. This feature allowed each requirement to be imported and has the limited capability to manage requirements and to manually add modeling-element connections (See Figure 28), verifications, and attachments to each requirement. However, there are no connections to the verification exhibits or other modeling data elsewhere in the model, so the entries for those would have to be completed manually. Therefore, the verification field was only used to store/report tailored requirement text.

While not designed for the SRCC analysis and documentation, the study team was able to use the *Description* field to hold NASA STD requirement text, the *Classification* field for compliance standing, and the Prerequisite field for tailored requirement text (See Figure 28). It was noted that the *Attachment* field of this feature could have been used to record vendor standard/practice or other data if applicable, but this was not employed by this study. However, all these inputs were manual, and the final exported tables required post-processing manipulation to produce a MADE-SRCC table (Figure 29) similar to a traditional SRCC product (Figure 30), but this still did not produce an entire product. The tool is being modified to incorporate generation of this safety product and automation/integration of its assessments and data.

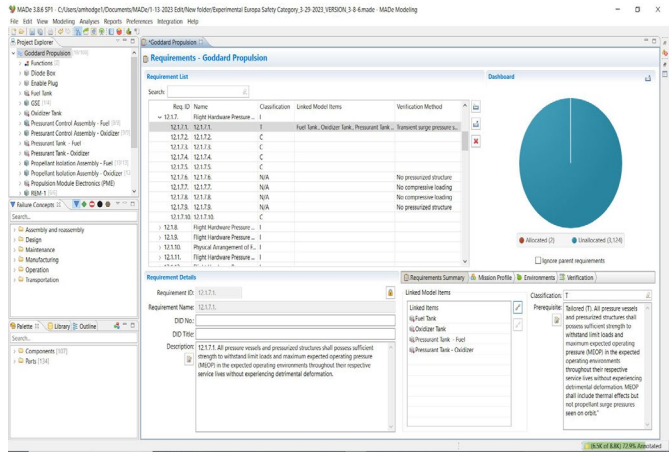


Figure 28: Tailored and Linked Europa Requirements in MADE

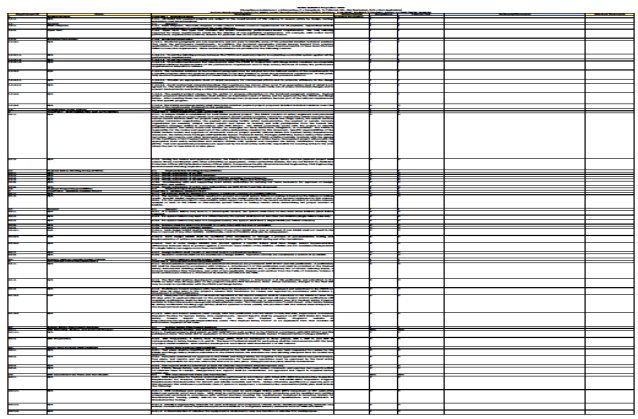


Figure 29: MADE Compliance Matrix (Double click on figure to open pdf)

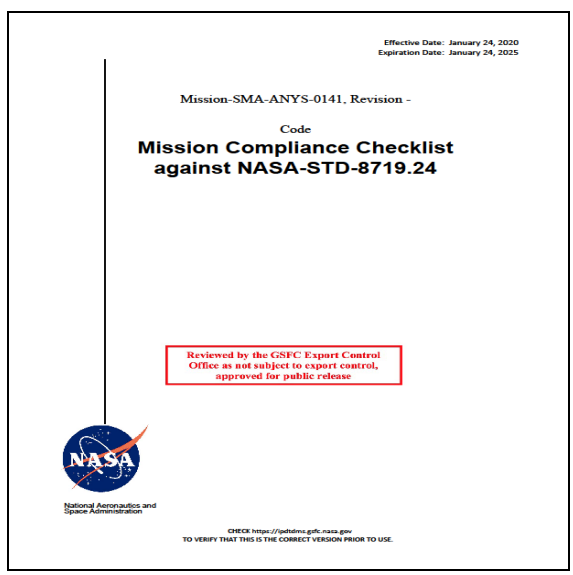


Figure 30: Genreric Traditional Full Mission Compliance Matrix Example (Double click on figure to open pdf)

3.3.3 Safety Data Package (SDP)

A Safety Data Package (SDP) includes hazard analyses as well as a description of the system (e.g., pages 2 - 8 of Figure 27) with an emphasis on system hazards and their mitigation. An SDP is intended to show what hazards exist, put them in context, and show how they are mitigated. Hazard Reports and associated analysis are part of the SDP. Additionally, the SDP describes Ground Support Equipment (GSE) and often includes a Ground Operations Plan (GOP), describing activities related to processing the spacecraft at the launch site and integration with the launch vehicle. Sometimes the GOP is a separate document, however it does become a part of the Package. Often, the SDP and/or GOP will be referenced in the compliance matrix as part of the rationale.

To create this in MADE, three documents (MADE hazard analysis report – Figure 26 and Section 3.3.1, MADE System Information Report (SIR) – Figure 31, a GOP created outside of MADE but attached to the model) would have to be combined manually and post-processed to generate a MADE SDP report. However, the ability to create an SDP automatically is being considered for future versions of MADE.

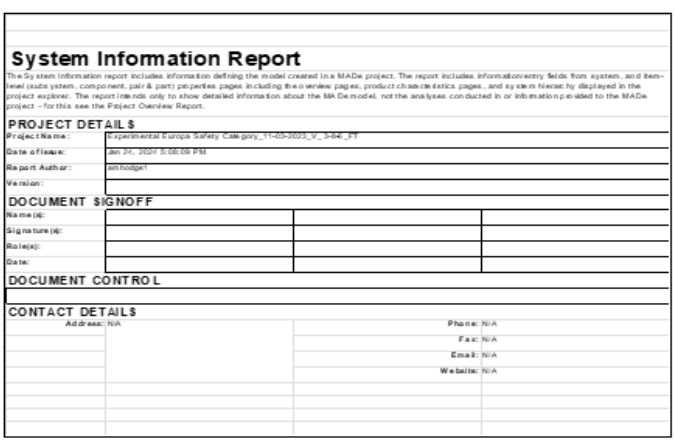
This study elected not to execute that post-processing but rather generate the individual MADE documents and assess if these would be sufficient to form an SDP. As a result, it was observed that these generated MADE documents have significant data gaps. They were missing physical and chemical properties/characteristics, sketches/schematics, diagrams, materials, design parameters, toxicity and physiological effects, and temperature/pressure limits. While it might be possible to add this data to the model, it would take significant work. This work level would be required because MADE has one descriptive field for each element, and all the text/data to fill the SDP gaps would need to be manually added and images/documents attached there, until a NASA or MADE library of the various space system components with descriptions and images is created. However, it was also observed that any uploaded images and descriptive documentation cannot be output as part of any MADE report but could be output natively. This makes using MADE features to generate an SDP of questionable efficiency.

3.3.4 Fault Analysis and Inhibit Verification

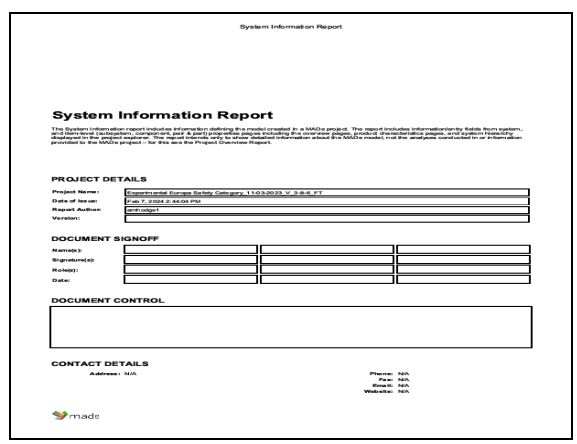
3.3.4.1 Fault Tree Analysis (FTA)

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 (Figures 33 – 42) and Windchill (Figure 32) for each hazard category (i.e., Fire/Explosion, Structure, Leaks/Spills, Electrical/Grounding, Mechanical, Pressure/Hydraulic, Contamination/Corrosion, Temperature, Control Systems, and Physiological).

The fault trees generated by MADE for each hazard appear quite different than the more traditional Windchill products. The Windchill products follow the traditional Fault Tree (Figure 32) format using standard notation. The MADE model-based FTs (Figures 33 – 42), however, shows mechanism and cause contributions as individual events without logic gates. When this is observed, it can be surmised that these representations are single events of one mechanism due to one cause. Once this is understood, the FTs are understandable and can be used to show, in a qualitative way, fault tolerance and safety mitigation sufficiency or insufficiency. This would allow a safety engineer to explain and advocate for design changes or safety mitigations that might be needed to render a system safer. While MADE provides the capability to quantify Safety Fault Trees, quantification could be misleading if not grounded in reality.



Excel Version (Diode Box Only)



PDF Version (Full Model)

Figure 31: MADE SIR
(Double click on figures to open pdf/Excel)

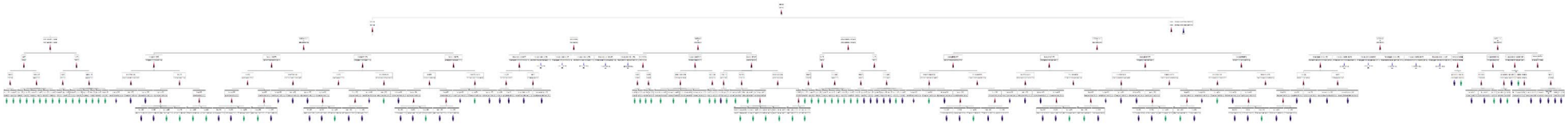


Figure 32:Fire/Explosion Hazard FT – Traditional Example (Windchill)
(double click to open pdf)

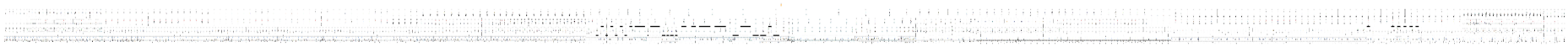


Figure 33: Fire/Explosion Hazard Tree *(MADE)*
(double click to open pdf)

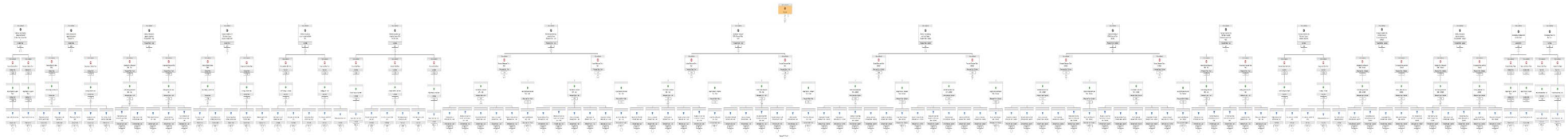


Figure 34: Structure Hazard Tree *(MADE)*
(double click to open pdf)

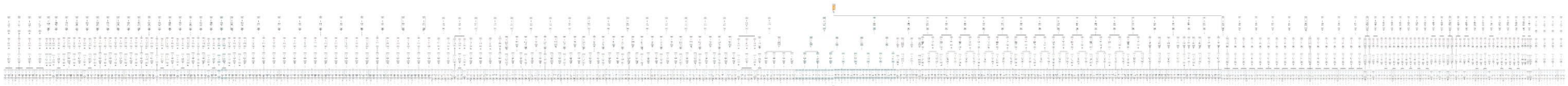


Figure 35: Leaks/Spills Hazard Tree *(MADE)*
(double click to open pdf)

Figure 36: Electrical/ Grounding Hazard Tree *(MADE)*
(double click to open pdf)

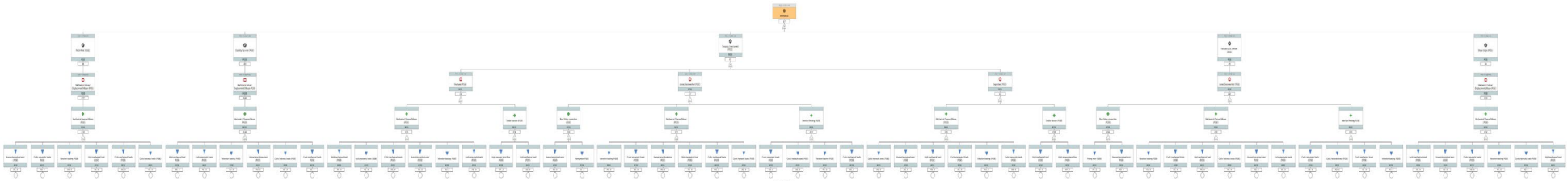


Figure 37: Mechanical Hazard Tree *(MADE)*
(double click to open pdf)

Figure 38: Pressure/Hydraulic Hazard Tree *(MADE)*
(double click to open pdf)

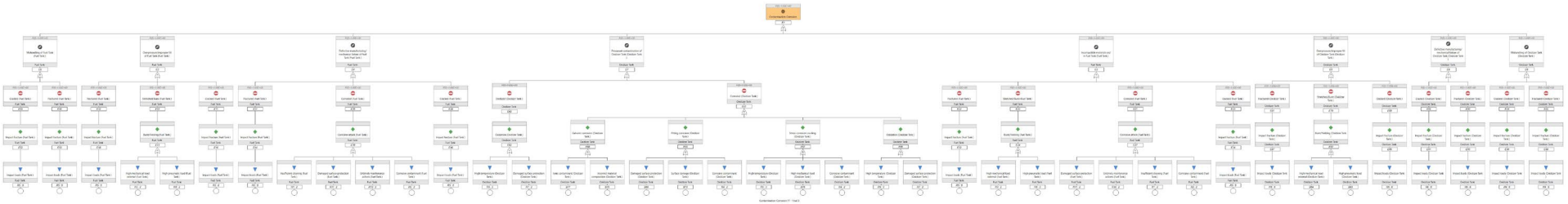


Figure 39: Contamination/Corrosion Hazard Tree *(MADE)*
(double click to open pdf)

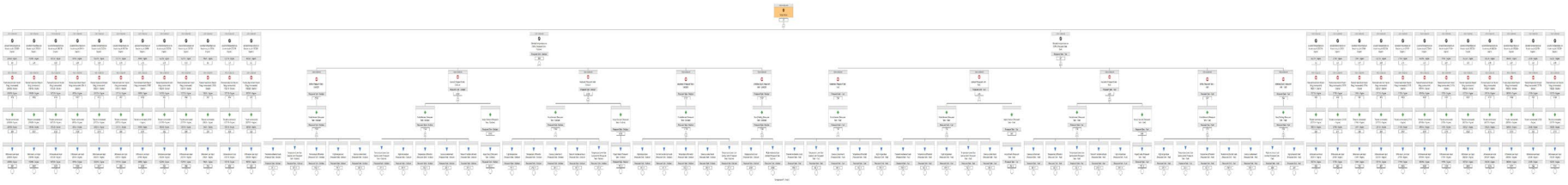


Figure 40: Temperature Hazard Tree (MADE)
(double click to open pdf)

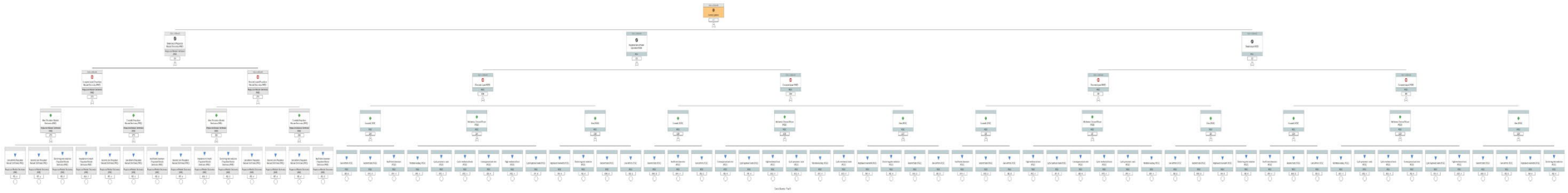


Figure 41: Control Systems Hazard Tree *(MADE)*
(double click to open pdf)

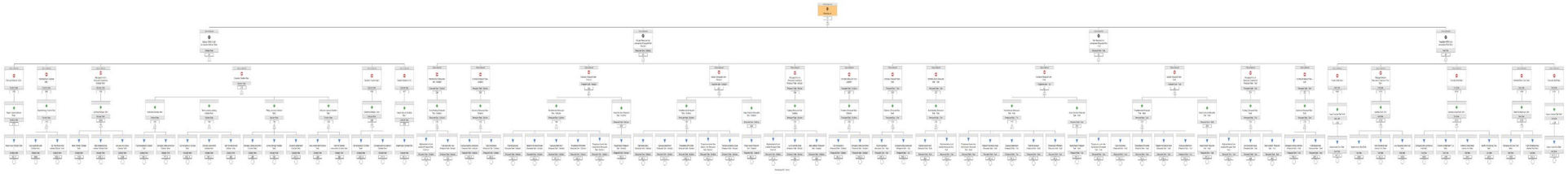


Figure 42: Physiological Hazard Tree *(MADE)*
(double click to open pdf)

3.3.4.2 Inhibit Verifications: Simulation Scenarios

In the Pre-launch phase of mission, there are specific scenarios that need to be prevented in accordance with safety engineering guidelines. The simulation capability of the MADE software and the following simulation scenarios/cases were used to demonstrate the resilience and sufficiency of hazard controls/inhibits and thus validate the safety compliance of the design of the Europa Propulsion system :

Case 1 - Premature Propulsion Activation (Firing). The following scenarios were used to demonstrate the response of the propulsion system when power is supplied, and signals are sent from the GSE for activation. Six simulations (Figures 43-48). were executed. For this series of simulations, an "up arrow" indicates that the component has been perturbed or given a value of 0.4 in the positive direction. With the enable plug disconnected (indicated by a "down arrow"), power was activated by the GSE (indicated by an "up arrow"), and the thrusters displayed no response (indicated by "side-to-side arrow") as shown in Figure 43. In addition to the power being activated, the "Arm" command was activated by the GSE (indicated by an "up arrow"), and the thrusters displayed no response (indicated by "side-to-side arrow"), as shown in Figure 44.

When "power," and the "Arm," and "Fire" commands were activated by the GSE (indicated by 3 "up arrows"), the thrusters displayed no response (indicated by a "side-to-side arrow") as shown in Figure 45. All three cases showed the thrusters did not activate, as the enable plug is a sufficient inhibit against premature signal activation. The previous three simulation scenarios were repeated with the exception that the enable plug was connected. In these cases, activation of the power (indicated by an "up arrow") displayed no response (indicated by a "side-to-side arrow") from the thrusters, as shown in Figure 46. Activation of both "power" and the "Arm" command led to a no response from the thrusters, as shown in Figure 47. When "power" and the "Arm," and "Fire" commands were activated, the thrusters responded by activating (indicated by an "up arrow"), as shown in Figure 48. This final scenario shows that the thruster needs to receive three signals ("power," "Arm" command, "Fire" command) with the enable plug connected for activation to occur, or operational commencement of firing. These three signals act as inhibits along with enable plugs to prevent premature thruster activation. These simulations verified that there are four inhibits in place to prevent premature thruster activation.

Case 2 - Overfill of tanks (fuel, oxidizer, pressurant). For the Europa propulsion, a tank overfill cannot be simulated due to a lack of accumulation capability in the MADE software.

Case 3 - Inappropriate material loading procedures or loading with failures present (e.g., flow rate sent to closed system). The following 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 failure. Two simulations (Figures 49-50) were executed. For this series of simulations, an "up arrow" indicates that the component has been set to "open," or given a value of 1 in the positive direction, while a "down arrow" indicates that the component has been set to "closed," or given a value of 1 in the negative direction. Fuel was activated (indicated by an "up arrow") from the fuel service valve, while the fuel tank was deactivated (indicated by a "down arrow") to show that it had failed. The simulation (Figure 49) showed a "no response" (indicated by a "side-to-side arrow"), which means that fuel will not leak further than the fuel tank. The second simulation was a repeat of this fuel scenario except using Oxidizer and Oxidizer components (See Figure 50), and the same results were obtained. Overall, these simulations indicated that there will be no downstream effect to the propulsion subsystem safety from anomalous material loading.

Case 4 - System fuel/oxidizer escapes via thrusters. The following scenarios were used to demonstrate the response of the propulsion system when material (fuel or oxidizer) flows from the fuel and oxidizer tank to the Propellant Isolation Assembly (PIA) for fuel or oxidizer if there are latch-valve (as shown by the block diagram in Figure 1) failures. Fuel latch valve inhibit-failure simulations involve the following latch valves: LV09FLA, LV10FLB, LV11FLA, and LV12FLB. Oxidizer latch valve inhibit failure simulations involve the following latch valves: LV05XLA, LV06XLB, LV07XLA, and LV08XLB. Twenty-eight simulations were executed that used either single latch-valve or double-latch or triple-valve inhibit failures with the fuel or oxidizer tanks activated/perturbed (indicated by an "up arrow" or a value of 1 in the positive direction) to allow fuel or oxidizer to flow for the simulation. A summary of the simulated states, perturbation type, and system end effect for all components in the Fuel PIA can be found in Table 1.

The first set of eight simulations used only single latch-valve inhibit failures (as indicated by an "up arrow" or value of 1 or 2 in the positive direction) for the Fuel and Oxidizer PIAs. Each of the single fuel latch-valve inhibit failure/opening simulations showed no flow through the undisturbed/closed latch valves (as indicated by a "side-to-side arrow" that represents a non-operational valve), indicating that fuel did not leak past the failed valve, as shown by the "side-to-side arrows" on the green lines in Figures 50 - 57.

The next set of twelve simulations consisted of combinations of double-Fuel or -Oxidizer PIA latch-valve inhibit failures/openings. The double-latch-valve failure combinations of LV09FLA and LV10FLB or LV11FLA and LV12FLB resulted in the loss of fuel flow to the thrusters. Similarly, the double-latch-valve failure combinations of LV05XLA and LV06XLB or LV07XLA and LV08XLB resulted in the loss of oxidizer flow to the thrusters. The other eight oxidizer double-latch-valve failure combinations of PIA

latch valves proves that fuel or oxidizer cannot enter the thrusters, validating that the inhibits behave as expected and do not allow fuel to exit the system, as shown in Figures 58 - 69.

The final set of eight simulations consisted of combinations of Fuel or Oxidizer PIA latch-valve inhibit failures/openings to simulate triple-latch-valve inhibit failures (openings) (as indicated by a "down arrow" on one valve or value of 1 or 2 in the negative direction while the others were open as indicated by an "up arrow"). In these cases, fuel or oxidizer did flow further downstream through the remaining latch valves until either exited the PIA, as shown by the "up arrows" on the green lines in Figures 70 – 77, but the thruster valves prevented any leak/spill further downstream.

Note: Two additional simulations were used to verify that individual inhibit failure case results were not an artifact of modeling issues and that nominal fuel and oxidizer flow is possible to thrusters if all inhibits are removed (enabling operational thruster firing), as shown in Figure 79.

The simulations can provide confirmation that the inhibits function as designed or show that an additional inhibit is needed. Since they are directly tied to the model and the model is derived directly from the design, a digital twin, the simulation feature can directly demonstrate the inhibit design. Using a simulation is much more accurate and less time consuming than the traditional method of tracing inhibits through a complex design.

3.3.5 Other types of Hazard Analysis

Hazard analyses are performed within system boundaries or mission phases. The analyses described in this report are for a propulsion system at the launch site after fueling, but study observations indicate that this tool could be used for any type of hazard analysis by modeling proper system boundaries, vehicle configuration, and ancillary hardware (i.e., lifting hardware, ground support equipment, etc.) that interacts with a system. For example:

- A hazard analysis performed in support of Integration and test (called an Operational Hazard Analysis (OHA)) will have different boundaries and hazards than operations but would be supported by the same capabilities and methods used in this study.
- A hazard analysis preformed on a process such as hazardous operations at the launch site would be an Operational and Support Hazard Analysis (O&SHA), a highly detailed analysis of that process. For the propulsion system of this study, the O&SHA would look at the process of fueling and would be supported by the same capabilities and methods used in this study.

Again, simulations can provide confirmation that the inhibits function as designed or show that an additional inhibit is needed in these analyses as well. Additionally, since an O&SHA is a detailed look at a process or procedure (e.g., fueling), the use of simulations can greatly enhance the effectiveness of process development and these types of hazard analysis and represent an improvement over existing methods.

Table 1: Propellant Isolation Assembly (PIA) Inhibit Simulations

Open Component Name (s)	Closed Component Name (s)	System Flow Results	Figure Reference Number
Fuel Tank	N/A	This is a prerequisite for all simulations involving fuel flow	N/A
Oxidizer Tank	N/A	This is a prerequisite for all simulations involving oxidizer flow	N/A
LV05XLA	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 51
LV06XLA	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 52
LV07XLA	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 53
LV08XLA	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 54
LV09FLA	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 55
LV10FLB	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 56

Open Component Name (s)	Closed Component Name (s)	System Flow Results	Figure Reference Number
LV11FLA	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 57
LV12FLB	N/A	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 58
LV05XLA, LV06XLA	LV07XLA, LV08XLA	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 59
LV05XLA LV07XLA	LV06XLA, LV08XLA, REMs	Insufficient oxidizer reaches thrusters; Oxidizer hazard is controlled by thrusters	Figure 60
LV05XLA, LV08XLA	LV06XLA, LV07XLA, REMs	Insufficient oxidizer reaches thrusters; Oxidizer hazard is controlled by thrusters	Figure 61
LV06XLA, LV07XLA	LV05XLA, LV08XLA, REMs	Insufficient oxidizer reaches thrusters; Oxidizer hazard is controlled by thrusters	Figure 62
LV06XLA, LV08XLA	LV05XLA, LV07XLA, REMs	Insufficient oxidizer reaches thrusters; Oxidizer hazard is controlled by thrusters	Figure 63
LV07XLA, LV08XLA	LV05XLA, LV06XLA	Oxidizer does not reach thrusters; Oxidizer hazard is controlled by valves	Figure 64
LV09FLA, LV10FLB	LV11FLA, LV12FLB	Fuel does not reach thrusters; Fuel hazard is controlled by valves	Figure 65
LV09FLA, LV11FLA	LV10FLB, LV12FLB, REMs	Insufficient fuel reaches thrusters; Fuel hazard is controlled by thrusters	Figure 66
LV09FLA, LV12FLB	LV10FLB, LV11FLA, REMs	Insufficient fuel reaches thrusters; Fuel hazard is controlled by thrusters	Figure 67
LV10FLB, LV11FLA	LV09FLA, LV12FLB, REMs	Insufficient fuel reaches thrusters; Fuel hazard is controlled by thrusters	Figure 68
LV10FLB, LV12FLB	LV09FLA, LV11FLA, REMs	Insufficient fuel reaches thrusters; Fuel hazard is controlled by thrusters	Figure 69
LV11FLA, LV12FLA	LV09FLA, LV10FLB	Fuel does not reach thrusters; Fuel hazard is controlled by valves	Figure 70
LV06XLA, LV07XLA, LV08XLA	LV05XLA, REMs	Oxidizer reaches thrusters; Oxidizer hazard controlled by thrusters	Figure 71
LV05XLA, LV07XLA, LV08XLA	LV06XLA, REMs	Oxidizer reaches thrusters; Oxidizer hazard controlled by thrusters	Figure 72
LV05XLA, LV06XLA, LV08XLA	LV07XLA, REMs	Oxidizer reaches thrusters; Oxidizer hazard controlled by thrusters	Figure 73
LV05XLA, LV06XLA, LV07XLA	LV08XLA, REMs	Oxidizer reaches thrusters; Oxidizer hazard controlled by thrusters	Figure 74
LV10FLA, LV11FLA, LV12FLA	LV09FLA, REMs	Fuel reaches thrusters; Fuel hazard controlled by thrusters	Figure 75
LV09FLA, LV11FLA, LV12FLA	LV10FLB, REMs	Fuel reaches thrusters; Fuel hazard controlled by thrusters	Figure 76
LV09FLA, LV10FLA, LV12FLA	LV11FLA, REMs	Fuel reaches thrusters; Fuel hazard controlled by thrusters	Figure 77
LV09FLA, LV10FLA, LV11FLA	LV12FLB, REMs	Fuel reaches thrusters; Fuel hazard controlled by thrusters	Figure 78
All Latch Valves	N/A	Fuel reaches thrusters and firing commence; Fuel hazard not controlled by thrusters or valves; Firing enabled	Figure 79

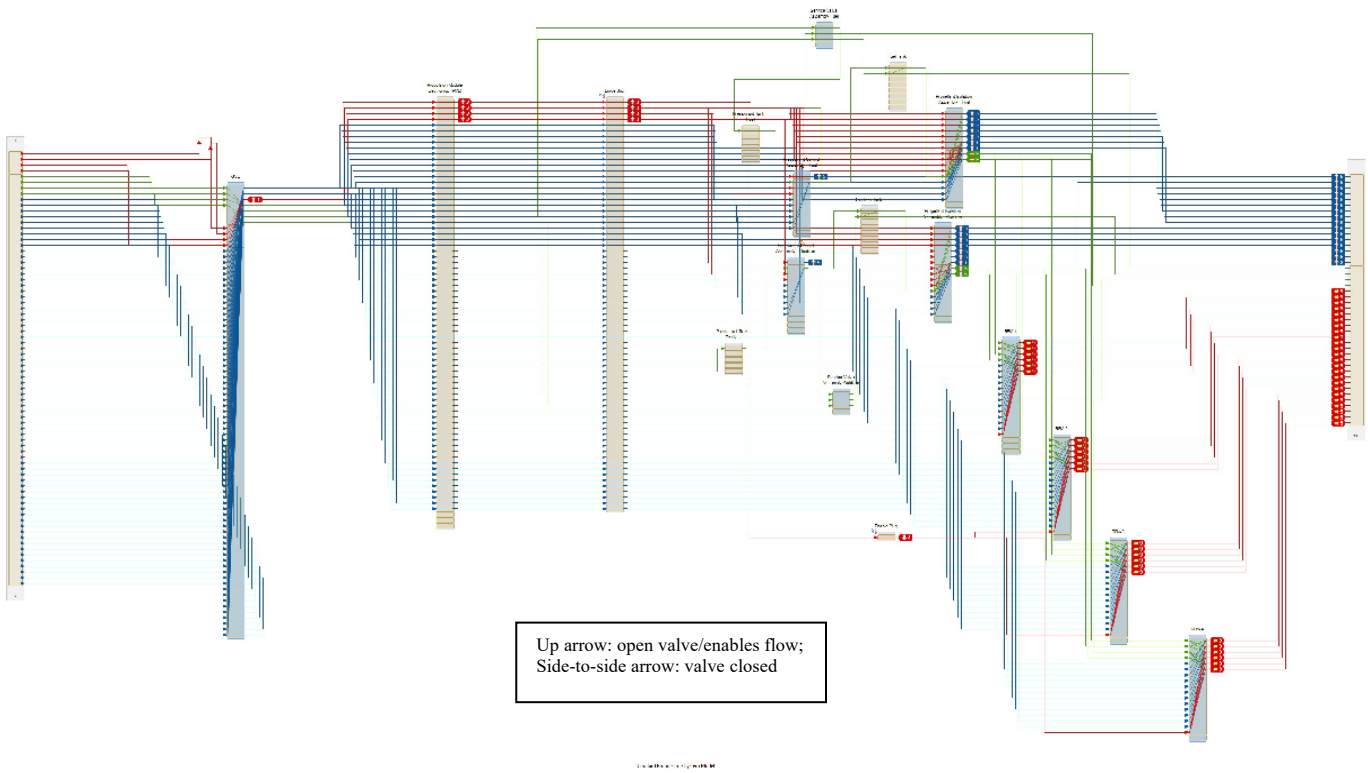


Figure 43: MADE EUROPA inhibit model Case 1.1: Enable off/out with Power on *(double click image for larger view)*

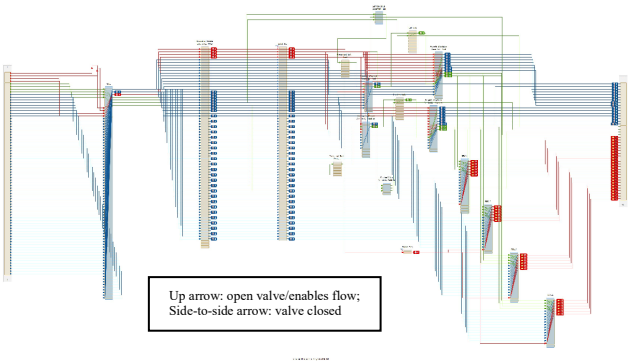


Figure 44: MADE EUROPA inhibit model Case 1.2: Enable off/out with power and arm *(double click image for larger view)*

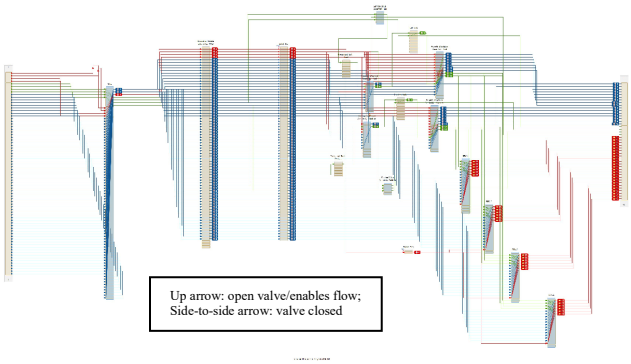


Figure 45: MADE EUROPA inhibit model Case 1.3: Enable off/out with power, arm, and fire *(double click image for larger view)*

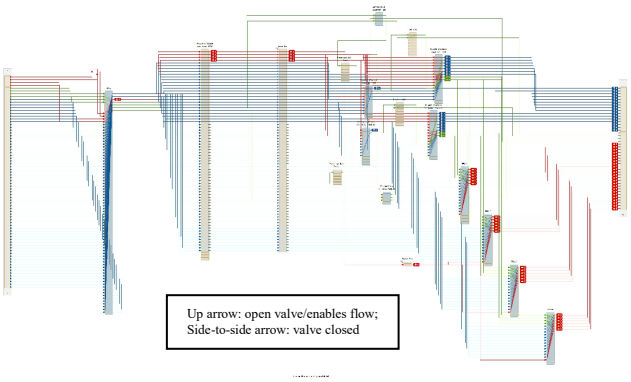


Figure 46: *MADE* EUROPA inhibit model Case 1.4: Enable on/in and power *(double click image for larger view)*

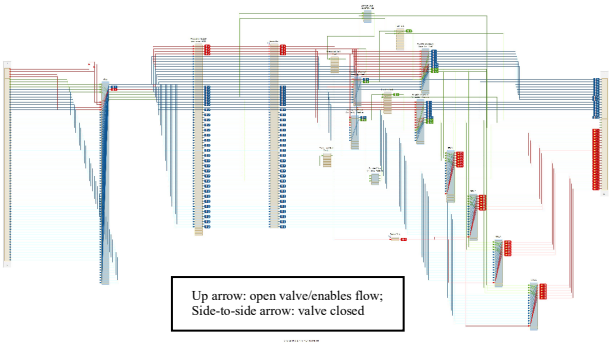


Figure 47: MADE EUROPA inhibit model Case 1.5: Enable on/in with power and arm *(double click image for larger view)*

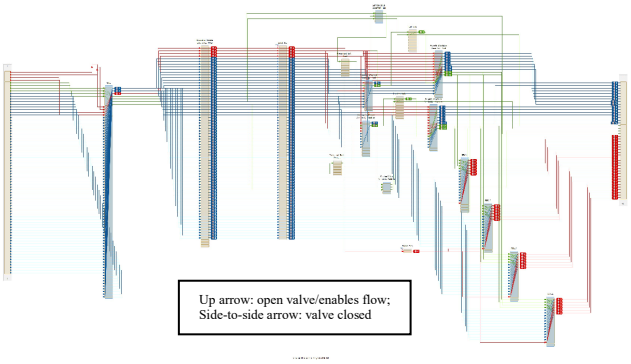


Figure 48: MADE EUROPA inhibit model Case 1.6: Enable on/in with power, arm, and fire *(double click image for larger view)*

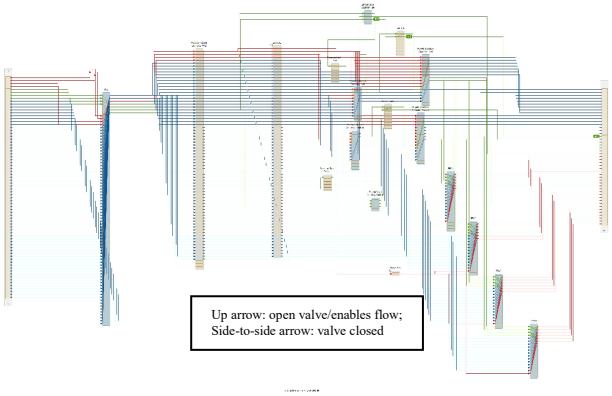


Figure 49: MADE EUROPA inhibit model Case 3.1: Flow Fuel Internally *(double click image for larger view)*

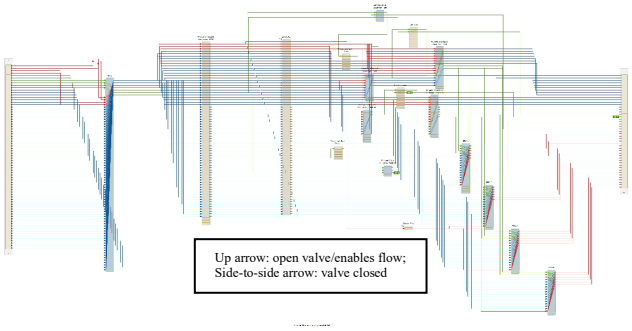


Figure 50: MADE EUROPA inhibit model Case 3.2: Flow Oxidizer Internally *(double click image for larger view)*

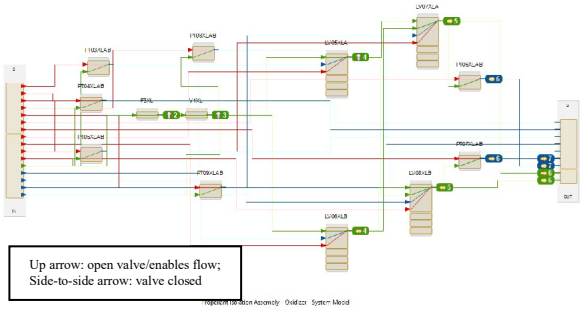


Figure 51: MADE EUROPA inhibit model Case 4.1: LV05XLA Open *(double click image for larger view)*

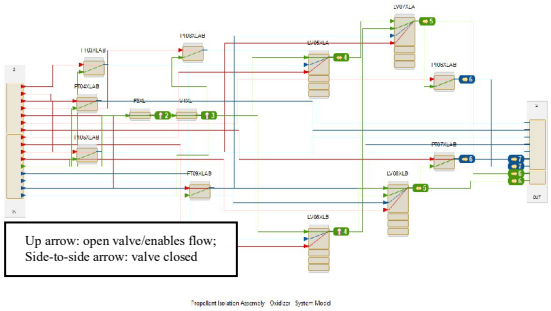


Figure 52: MADE EUROPA inhibit model Case 4.2: LV06XLA Open (double click image for larger view)

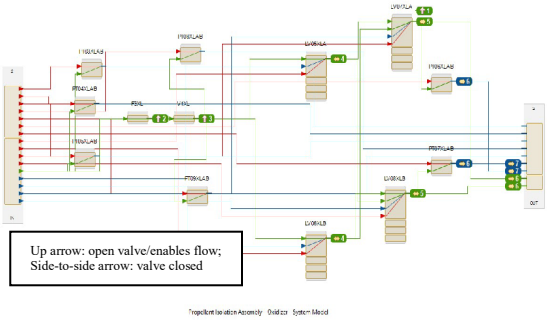


Figure 53: MADE EUROPA inhibit model Case 4.3: LV07XLA Open *(double click image for larger view)*

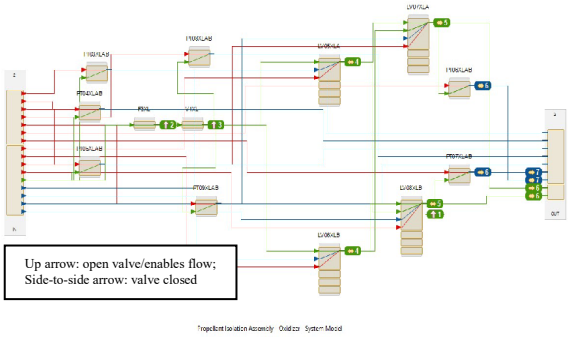


Figure 54: MADE EUROPA inhibit model Case 4.4: LV08XLA Open *(double click image for larger view)*

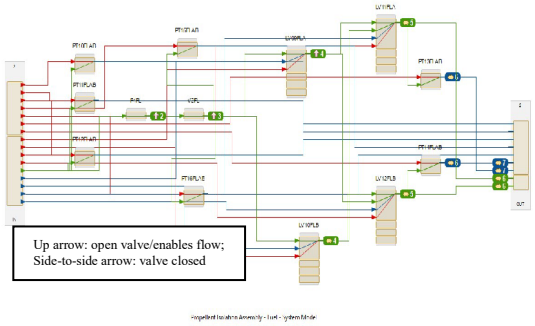


Figure 55: MADE EUROPA inhibit model Case 4.5: LV09FLA Open *(double click image for larger view)*

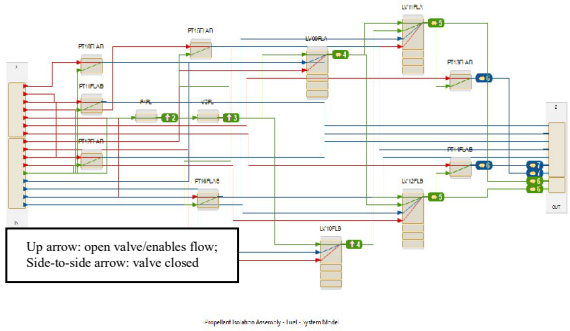


Figure 56: MADE EUROPA inhibit model Case 4.6: LV10FLA Open *(double click image for larger view)*

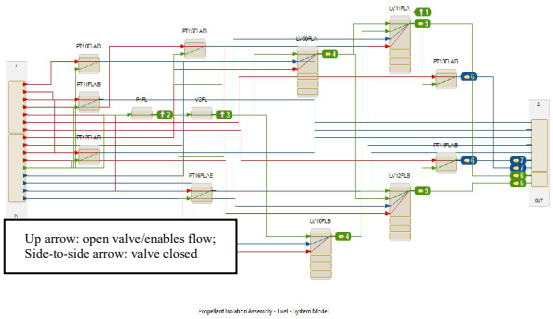


Figure 57: MADE EUROPA inhibit model Case 4.7: LV11FLA Open *(double click image for larger view)*

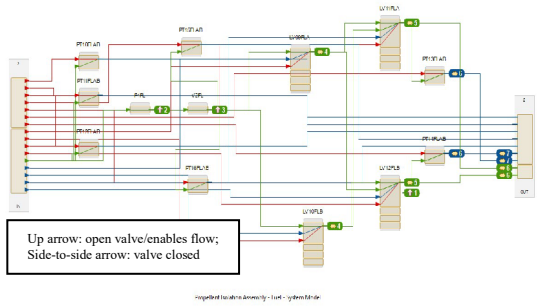


Figure 58: MADE EUROPA inhibit model Case 4.8: LV12FLA Open *(double click image for larger view)*

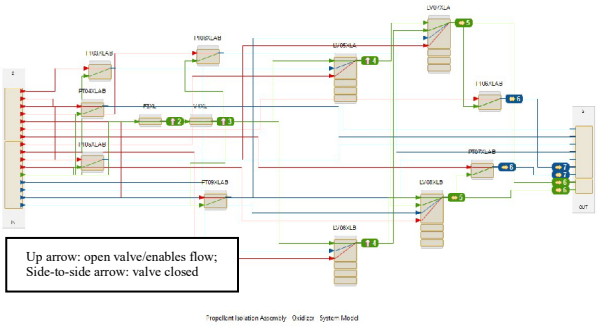


Figure 59: MADE EUROPA inhibit model Case 4.9: LV05XLA & LV06XLA Open *(double click image for larger view)*

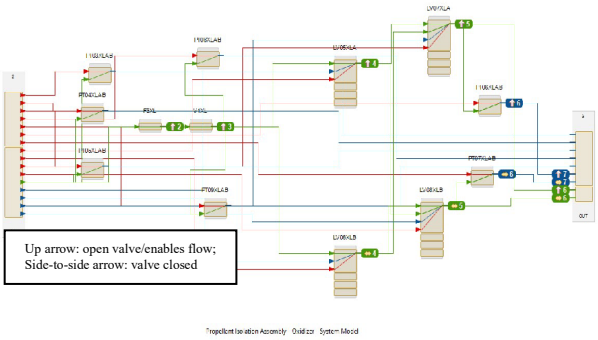


Figure 60: MADE EUROPA inhibit model Case 4.10: LV05XLA & LV07XLA Open *(double click image for larger view)*

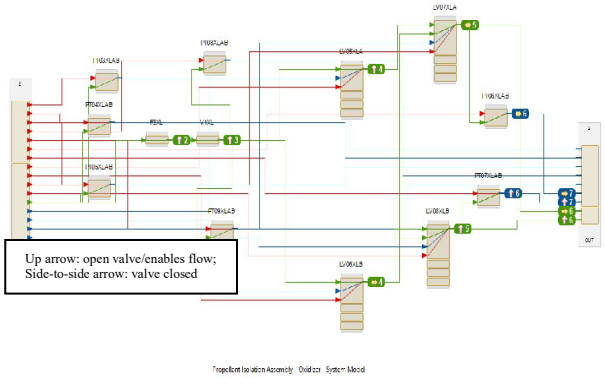


Figure 61: MADE EUROPA inhibit model Case 4.11: LV05XLA & LV08XLA Open *(double click image for larger view)*

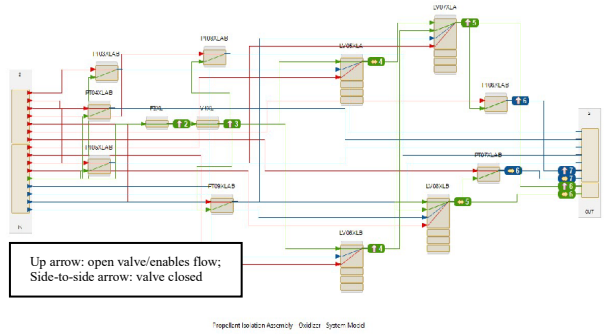


Figure 62: MADE EUROPA inhibit model Case 4.12: LV06XLA & LV07XLA Open *(double click image for larger view)*

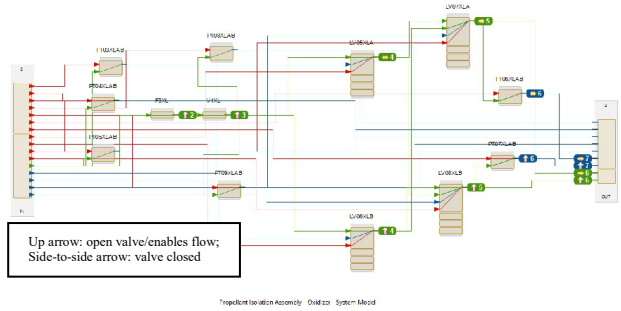


Figure 63: MADE EUROPA inhibit model Case 4.13: LV06XLA & LV08XLA Open *(double click image for larger view)*

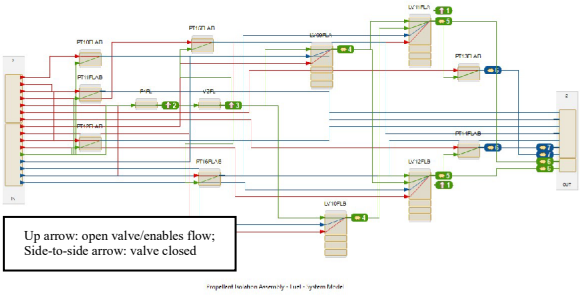


Figure 64: MADE EUROPA inhibit model Case 4.14: LV07XLA & LV08XLA Open *(double click image for larger view)*

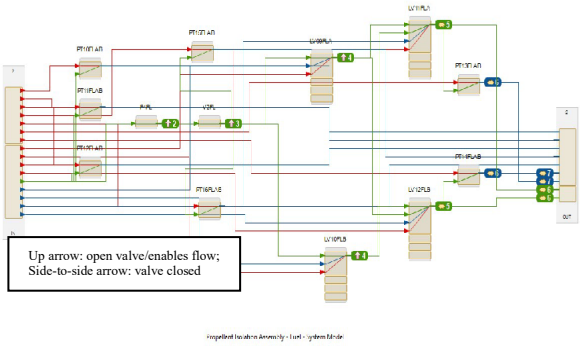


Figure 65: MADE EUROPA inhibit model Case 4.15: LV09FLA & LV10FLA Open *(double click image for larger view)*

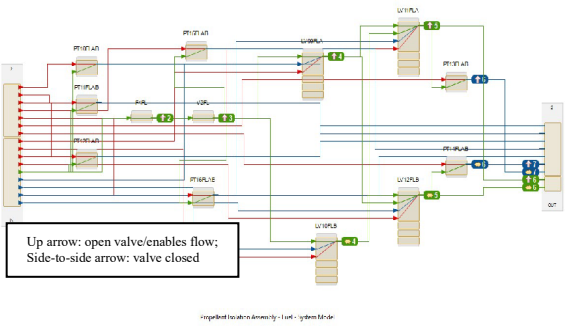


Figure 66: MADE EUROPA inhibit model Case 4.16: LV09FLA & LV11FLA Open *(double click image for larger view)*

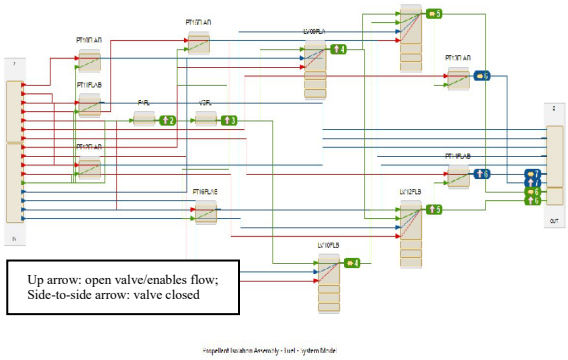


Figure 67: MADE EUROPA inhibit model Case 4.17: LV09FLA & LV12FLA Open *(double click image for larger view)*

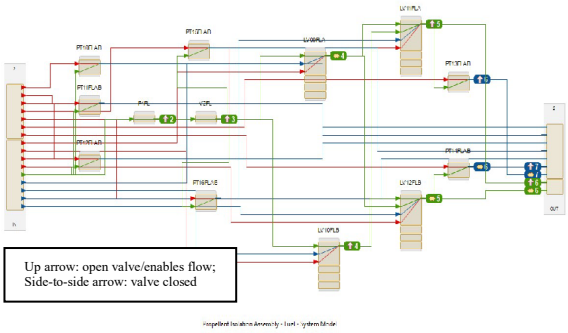


Figure 68: MADE EUROPA inhibit model Case 4.18: LV10FLA & LV11FLA Open *(double click image for larger view)*

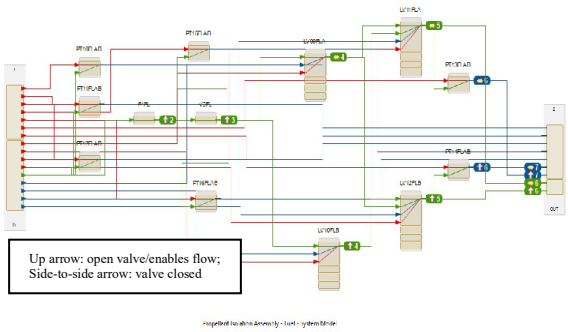


Figure 69: MADE EUROPA inhibit model Case 4.19: LV10FLA & LV12FLA Open *(double click image for larger view)*

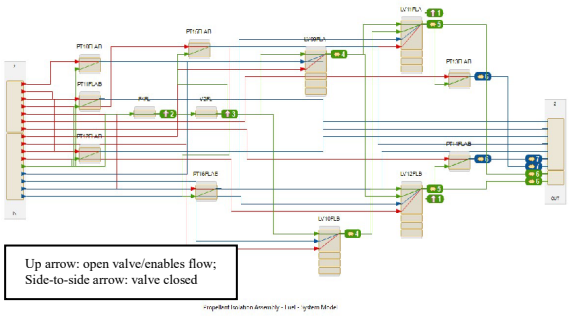


Figure 70: MADE EUROPA inhibit model Case 4.20: LV11FLA & LV12FLA Open *(double click image for larger view)*

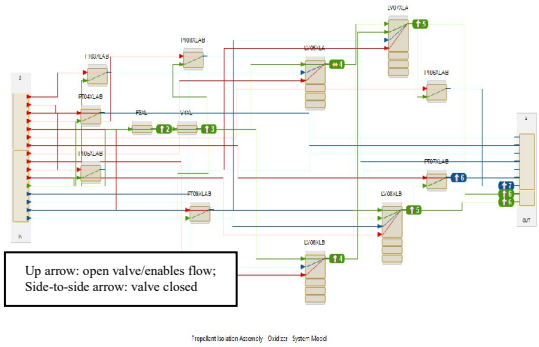


Figure 71: MADE EUROPA inhibit model Case 4.21: Only LV05XLA Closed *(double click image for larger view)*

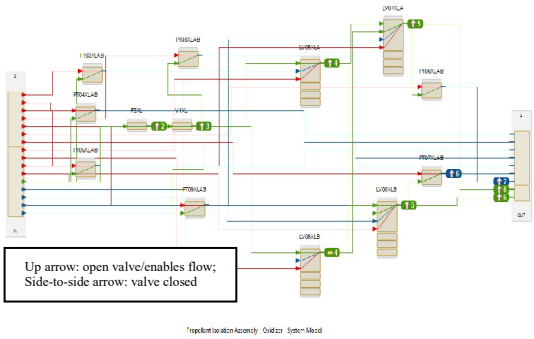


Figure 72: MADE EUROPA inhibit model Case 4.22: Only LV06XLA Closed (double click image for larger view)

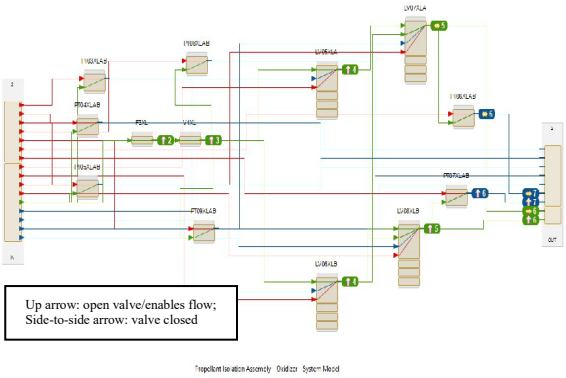


Figure 73: MADE EUROPA inhibit model Case 4.23: Only LV07XLA Closed *(double click image for larger view)*

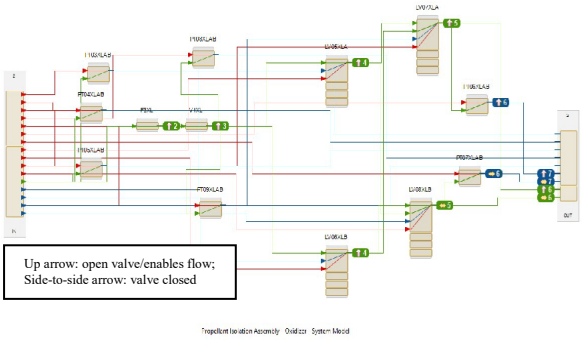


Figure 74: MADE EUROPA inhibit model Case 4.24: Only LV08XLA Closed *(double click image for larger view)*

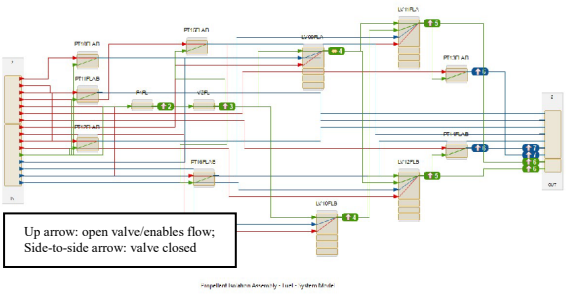


Figure 75: MADE EUROPA inhibit model Case 4.25: Only LV09FLA Closed *(double click image for larger view)*

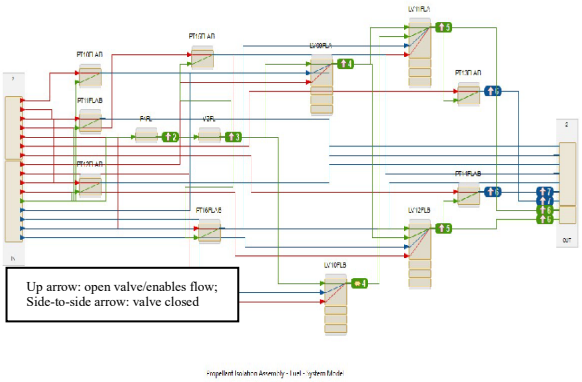


Figure 76: MADE EUROPA inhibit model Case 4.26: Only LV10FLA Closed *(double click image for larger view)*

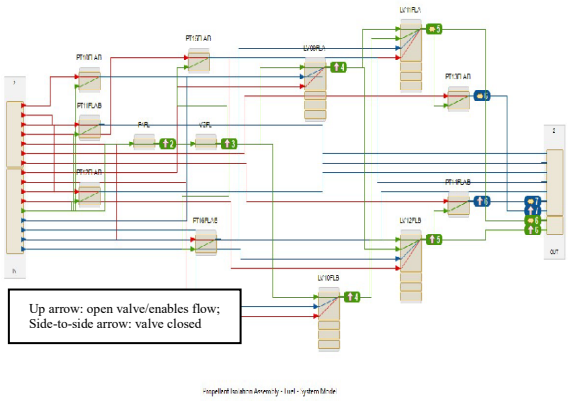


Figure 77: MADE EUROPA inhibit model Case 4.27: Only LV11FLA Closed (double click image for larger view)

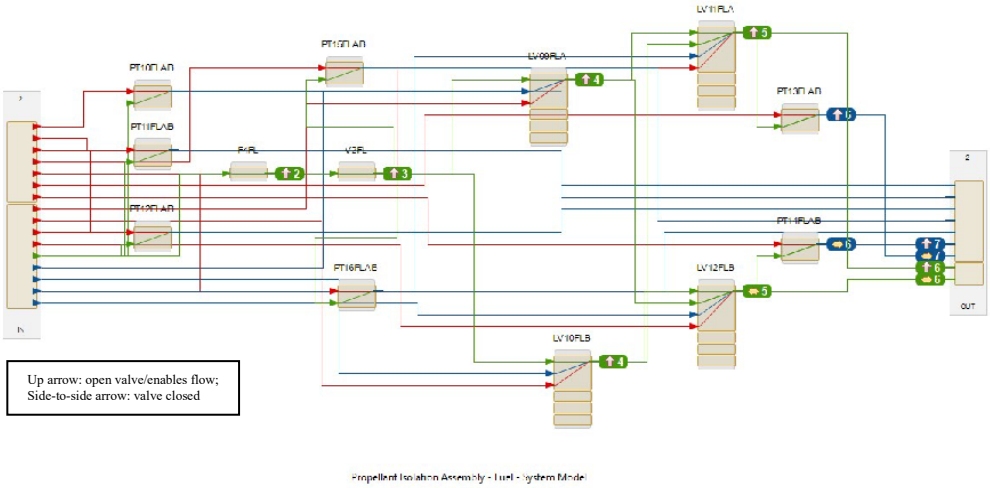


Figure 78: MADE EUROPA inhibit model Case 4.28: Only LV12FLA Closed *(double click image for larger view)*

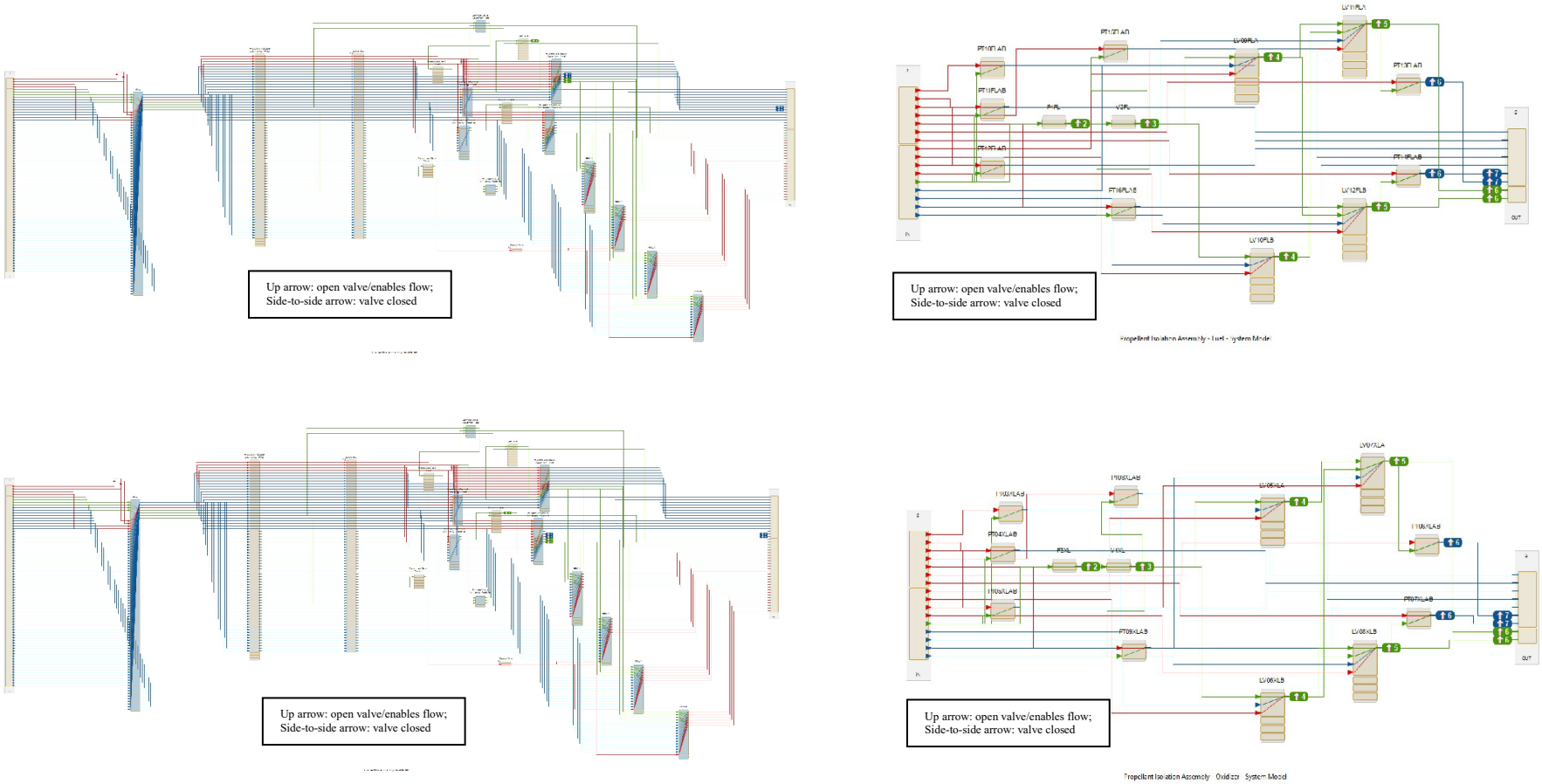


Figure 79: MADE EUROPA Nominal (non-inhibited) Fuel (Upper Images) and Oxidizer (Lower Images) Operating States for Reference
(double click images for larger view)

4 STUDY FINDINGS AND 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 mapped 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 reliability 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 MBSMAI Phase 2 study finds that it is feasible to use MADE models to conduct and document Hazard Analyses (HAs), develop a Safety Data Package (SDP), and use MADE simulations to enhance Operations and Support Hazard Analyses (O&SHA) and demonstrate inhibit-sufficiency/fault-tolerance analysis. Furthermore, this study finds that MADE can 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 further develop these capabilities.

As the scope of this study phase 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 analysis methods, terminology, and documentation formats. While the techniques are similar, the MADE products produced required some postprocessing to better match NASA products. Specific artifact and simulation findings are provided below and in Table 2.

I. MADE was found to have the ability to generate portions of a Safety Data Package (SDP) with some limitations (See Table 2). Currently, descriptive entries must be manually entered, or supporting images/documentation can be uploaded to the various components of the model or the top/full model. However, supporting images and documents cannot be output in any MADE report but can be output natively. For the study's SDP document, the EUROPA Propulsion System traditional SDP descriptive text was copied and pasted into MADE, and the model's System Information Report (SIR) was produced as an output. Since the descriptive portion of the SDP is a narrative and not an analysis, the SIR Figure 31, provided the narrative verbatim from what was provided without the images. Since the SDP is expected to be a narrative description of a system with images, illustrations, and diagrams to show the key features and safety-related functions of the system, the lack of supporting image outputs in the SIR means that extensive post-processing is required to produce an SDP. Such post processing includes locating and working with images generated outside of MADE from other sources or downloading them from MADE. As a result, the analyst would have to compile and annotate the images manually. The inability of MADE to reproduce stored images in any reports greatly reduces the value of using MADE to produce SDPs. Because of the lack of existing libraries and the reality that narratives must be manually input into the program and all images and image editing must be done outside MADE, the SDP generation process with MADE is rendered more burdensome and less efficient than traditional methods.

II. Product Hazard Analysis Reports (HAR) generated by MADE (Figure 26) are very detailed and, since the model provides a direct tie to the components, the modeler can 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 HAR. 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. Currently, the HAR requires post-processing for clarity and to ensure that the verifications were entered correctly, since they are manually entered into a field within the model. The report's columns must also be relabeled to better annotate the HAR in the context of GSFC methods. Also, the HAR includes much more detail than traditional HARs, since they have access to every component identified within the model. Additionally, the MADE-generated HAR defines the criticality levels differently than the traditional method. A NASA Hazard Report uses 5 levels of criticality vs 10 levels for MADE. Even with the need for extensive post-processing and increased detail, the HARs were found to be valid for System Safety use.

III. The use of MADE's Requirements feature and the generation of a MADE requirements table (Figure 29) showed that MADE could generate a Range Safety Compliance Assessments (Safety Requirements Compliance Checklist (SRCC)) supporting table with manual inputs. While not designed for SRCC generation and documentation, the study team was able

to use it to perform those functions (See Figure 28). It was noted that the attachment field has built-in fields and features to indicate compliance/tailoring.

IV. PSMs or SSEs use the qualitative Safety Fault Tree (SFT) to analyze system faults that could lead to a hazard. A quantitative value is generally not generated or used. MADE was found to have the ability to generate and quantify SFT [or Hazard Tree (HT)] with a hazard as the top event and to include safety causes in its failure fault trees using the model's *Failure Diagrams* (Appendix A, Figures A12 – A80) and MADE's *Fault Analysis tool* (fault tree development tool), and the *model-based fault tree logic* option, an inherent feature within MADE. The result was that the MADE SFTs were found to be informative for hazard cause analysis/validation and modeling verification and were generally consistent with SFTs developed in Windchill (See Figure 32), based on MADE modeled safety data in this study.

However, since MADE SFTs are produced using the *model-based logic* option, they have some of the same logic issue as other FTs created with this option. This issue is that some events decomposed without "logic gates" (And, Or, etc.) between the superior and subordinate events (e.g., failure modes, mechanisms, causes), which indicates an error in the tree's Boolean logic and is shown as stacked events instead of one event (which during Phase 1 of this study were observed to be treated that way quantitatively [1]). This issue has been raised to PHM Technology, and it was recommended that MADE consider improving their model-based FT/SFT generation using standardized gate logic similar to the format produced in Windchill (see Figure 32 and Figure 80 for examples). As a result, this study team was assured that a solution should be expected in future versions.

In addition, MADE reporting was found to be able to produce concise and readable FT reports (e.g., the pdf shown with the Figure 80 MADE FT) for most failures and hazards, and online viewing of all fault trees for engineering insights was issue-free. The notable exception was the inability of MADE to output a Fire-Explosion Hazard Tree Report, presumably because the tree was too wide, or the file is too large for successful generation. In addition, reports were found to have some transfer-gate labels (for indicating what page to transfer the reader to) missing, and event names/numbers are not searchable. These issues were found to make it more difficult to match the transfer gate targets on following pages to the transfer gates on the top-level tree and traverse the tree. It was also found in those reports that were producible that the wider fault trees got "cut off" or "ran off the page," versus having transfer gates for the additional gates of the tree. This makes the reporting for these trees flawed and ineffective. However, these issues have been raised to PHM Technology, and a solution for future versions should be expected in time.

V. MADE was found to offer the PSMs or SSEs a new capability to demonstrate processes and operations and analyze system faults that could lead to a hazard using simulation. MADE simulations in this study (6 Premature Propulsion Activation, 2 Inappropriate material loading procedures or loading with failures, and 20 System fuel/oxidizer escapes) provided a visual indication of the effectiveness, fault tolerance, resilience and sufficiency of hazard controls/inhibits and validated the safety of the design of the Europa Propulsion system under failure conditions. Interactive simulations will be helpful for future analyses of all types. In particular, the simulations can help not only the safety of hazardous procedures but that of any procedure or energy flow within the model (fuel, power or mechanism).

VI. While most of the MADE's Safety output products required post-processing for NASA use, MADE's simulation capability provides a unique and advantageous feature, currently unavailable in traditional NASA/GSFC safety methods. Simulations were found to enhance safety-inhibit and fault-tolerance understanding (See Figure 43-79), however a specific simulation report is not available at this time (although the results can be captured in a movie or Excel table).

In this study it was found that MADE does not currently have the following abilities:

- Generating a complete safety hazard list or report in the NASA format (NF 1825[10]). Currently, the report structure doesn't match NASA's or MIL-STD-882.
- Generating a NASA Range Safety Requirements report.
- Generating custom HARs (e.g., organized by functional failure instead of functions or with analysis scope limitations).
- Allowing users to select verifications or controls from built-in libraries. They currently must be entered manually (and controls do not have their own specific field).
- Allowing users to select NASA hazard categories from MADE defaults, which while similar, are not aligned with NASA categories. Currently, NASA-specific modeling of hazard categories must be manually entered/modeled.
- Autonomously reflecting edits of hazards (e.g., hazard causes / failure conditions) in the failure diagrams.
- Directly importing/outputting text and images for an integrated System Safety Data Package descriptive section.
- Importing 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.

4.2 SysML/MagicDraw

Reserved for update when SysML/MagicDraw system safety capability is realized.

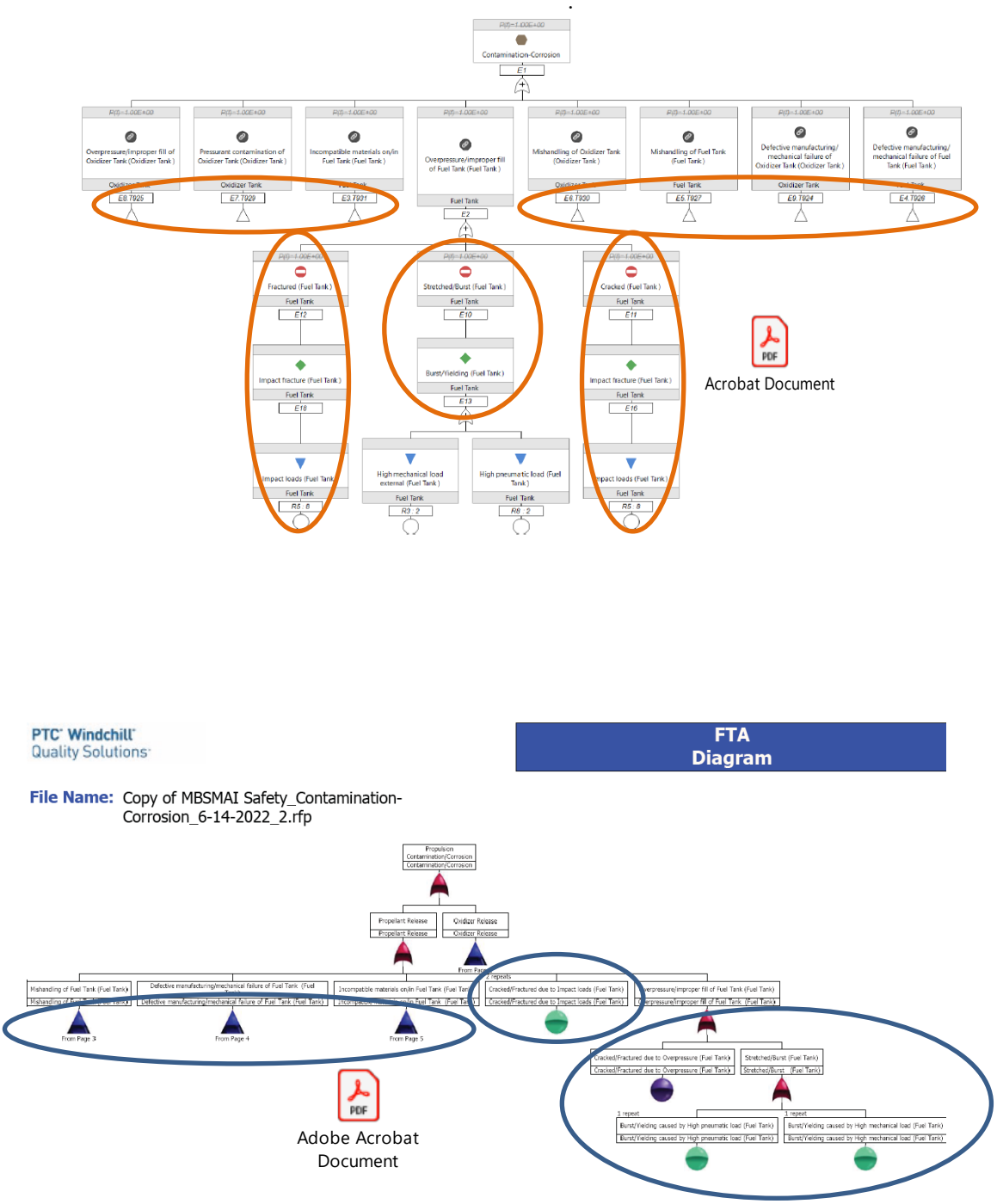


Figure 80: Hazard Tree Issues (Click on icons open full reports)

Table 2: MADE Evaluation

✓ = Status Quo
✓+ = Significant Improvement over traditional method
✓- = Worse than traditional method
NA = Not Applicable

Tool: MADE **Analysis:** Hazard Analysis based on NASA-STD 8719.24 & NPR 8715.7 and MAR DID	**Innate capability of the Tool**	**Consistency from Model to Model**	**Accuracy**	**Analysis complete and mission relevant?**	**Consistent with GSFC practices and ratings?**	**Can a safety assessment be succinctly represented by outputs?**	**Can Outputs support PSWG discussions/ evaluations?**	**Workload More or less than traditional approach?**	**Lessons Learned and Recommendations**
Hazard Identification	✓ Manual Process to add into the *Functional Diagram*.	✓ Can be kept consistent since it is a manual input, but it is dependent upon Analyst's ability to do so.	✓ Analyst dependent	✓ Analyst dependent	✓ Process is the same, but nomenclature is different because it's based on an FAA Standard. (Ref Table 1)	✓ Hazard statements are manually entered.	✓ Hazard statements are manually entered.	✓ Different nomenclature could drive initial delays due to having to correlate the nomenclature with NASA's terminology.	Map the hazard categories to functions, functional failure (hazard), and failure conditions (cause).
Hazard Category	✓ Manual Process to add into the *Functional Diagram*.	✓ Can be kept consistent since it is a manual input, but it is dependent upon Analyst's ability to do so.	✓ Analyst dependent	✓ Analyst dependent	✓ Process is the same, but nomenclature is different because it's based on an FAA Standard. (Ref Table 1)	✓ Hazard statements are manually entered	✓ Hazard statements are manually entered	✓- Must generate the categories and then map them.	Libraries and copying from model to model can mitigate manual entry tasks
Hazard Severity	✓	✓ Analyst dependent	✓ Analyst dependent	✓ Analyst dependent	✓- Severity labels are different since it's based on the SAE Standard.	✓	✓	✓	The ability to match the GSFC severity scale (NASA-STD8719.24: negligible, marginal, critical, catastrophic vs. minor, major, severe major, catastrophic) could be provided as an option.
Hazard Likelihood	✓	✓ Analyst dependent	✓ Analyst dependent	✓ Analyst dependent	✓ Likelihood values are modeled differently. They are set within each cause and then calculated for the Hazard.	✓	✓	✓	Each cause likelihood can be set to any value between 1 to 1E-12 but NASA hazard reports normally use an A-E scale as defined in NASA-STD-8719.24: A – $3x10^{-2}$ to $3x10^{-1}$ B – $3x10^{-3}$ to $3x10^{-2}$ C – $3x10^{-4}$ to $3x10^{-3}$ D – $8x10^{-5}$ to $3x10^{-4}$ E – $1x10^{-6}$ to $8x10^{-5}$
Hazard Cause(s)	✓ Manual identification	✓ Can be kept consistent since it is a manual input, but it is dependent upon Analyst's ability to do so.	✓ Analyst dependent	✓ Analyst dependent	✓ Analyst dependent	✓ Only if linked to modeling elements	✓	✓- Linking elements is an extra effort beyond the traditional method	Libraries and copying from model to model can mitigate manual tasks
Hazard Controls	✓ Manual Process to add controls based on cause	✓ Can be kept consistent since it is a manual input, but it is dependent upon Analyst's ability to do so.	✓ Analyst dependent	✓ + Model can be used to generate fault trees to validate controls.	✓ Manual process, Analyst dependent	✓- A field named Hazard Controls does not exist. We used an existing field with a different name.	✓	✓ Same.	Libraries and copying from model to model can mitigate manual tasks Renaming or adding a field for "Hazard Controls"

Tool: MADE **Analysis:** Hazard Analysis based on NASA-STD 8719.24 & NPR 8715.7 and MAR DID	**Innate capability of the Tool**	**Consistency from Model to Model**	**Accuracy**	**Analysis complete and mission relevant?**	**Consistent with GSFC practices and ratings?**	**Can a safety assessment be succinctly represented by outputs?**	**Can Outputs support PSWG discussions/ evaluations?**	**Workload More or less than traditional approach?**	**Lessons Learned and Recommendations**
Hazard Control Validation to demonstrate Effectiveness of Control(s) (e.g. Fault Tolerance based on inhibits)	✓+ Can generate fault tree directly from model. Tool has error checking.	✓+ Generated from the model upon request	✓+ Improved accuracy because it can be validated against the model itself.	✓+ Model allows user to simulate the failure to make sure that the control addresses the hazard.	✓+ Improvement over current practices.	✓+ Fault tree can be represented as Excel or pdf. Simulation can be output as a movie or event table	✓+ New output. What If scenarios can be run through the model	✓+ Once is complete with hazards identified, process is automatic	Instead of screen capture, could provide a movie file. This is a new capability that would enhance the current discussions with Systems Team and Safety Team and introduces the potential for validation via modeling, fault trees, and simulations which tie directly to the design.
Hazard Control verifications	✓- Entered manually and no specific field.	✓ Entered manually, Analyst dependent	✓ Entered manually. Analyst dependent	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓- Must be post-processed.	✓	✓- Post processing is time consuming	Add a verification field which can support multiple verifications for a single control. Add a means of attaching verification artifacts and map to verification
Hazard Verification Status	✓- Entered manually and no specific field.	✓ Entered manually - consistency dependent on analyst	✓ Accuracy is dependent on operator's knowledge of the model.	✓ Analysis complete w/ manual inputs.	✓ Manual process	✓- Must be post-processed.	✓	✓- Post processing is time consuming	Add a verification tracking field which can support multiple verifications for a single control. Add a means of attaching verification artifacts and map to verification
Supporting documentation, attachments, links to SDP, other artifacts or sources	✓ Attachments are possible, but are included in output	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Manual. Output not available for attachments.	✓ Manual. Output not available for attachments.	✓- Output not available for attachments and especially images.	✓- Output not available for attachments and especially images.	✓- Post process outputs to add in attachments and images.	Allow attachments and images to be output inline with analysis. Libraries and copying from model to model can mitigate manual tasks
Produce GSFC Formatted Hazard Report (based on NEF 1825)	✓- Produces reports iaw SAE ARP4761	✓	✓- Produces reports iaw SAE ARP4761	✓- Produces reports iaw SAE ARP4761	✓- Produces reports iaw SAE ARP4761	✓ Assessment is represented iaw SAE ARP4761	✓- Produces reports iaw SAE ARP4761	✓- Extensive post-processing to transform into proper Format.	Add an option to use GSFC formatting
Produce GSFC Formatted Hazard Report (based on NASA Std)	✓- Produces reports iaw SAE ARP4761	✓	✓- Produces reports iaw SAE ARP4761	✓- Produces reports iaw SAE ARP4761	✓- Produces reports iaw SAE ARP4761	✓ Assessment is represented iaw SAE ARP4761.	✓- Produces reports iaw SAE ARP4761	✓- Extensive post-processing to transform into proper Format.	Add an option to use GSFC formatting.

Tool: MADE **Analysis:** SRCC Based on NASA-STD 8719.24 Annex, NPR 8715.7, and MAR DID **Requirements assessment based on NASA STD 8719.24 (e.g. SRCC)**	**Innate capability of the Tool**	**Consistency from Model to Model**	**Accuracy**	**Analysis complete and mission relevant?**	**Consistent with GSFC practices and ratings?**	**Can a safety assessment be succinctly represented by outputs?**	**Can Outputs support PSWG discussions/ evaluations?**	**Workload More or less than traditional approach?**	**Lessons Learned and Recommendations**
Requirements are present	✓ Must be ingested from Excel	✓	✓	NA This does not apply to importing requirements	✓+ Provides requirements management tool which is not currently available	NA This does not apply to outputting reports	NA This does not apply to outputting reports	✓ Same as the current because requirements must be ingested each time	Current tool capabilities require importing the requirements for every system. An improvement would be to provide the requirements as part of the tool. Renaming or tailoring fields to be consistent with the requirements would be helpful. This is another area where libraries would be helpful.

Tool: MADE **Analysis:** SRCC Based on NASA-STD 8719.24 Annex, NPR 8715.7, and MAR DID **Requirements assessment based on NASA STD 8719.24 (e.g. SRCC)**	**Innate capability of the Tool**	**Consistency from Model to Model**	**Accuracy**	**Analysis complete and mission relevant?**	**Consistent with GSFC practices and ratings?**	**Can a safety assessment be succinctly represented by outputs?**	**Can Outputs support PSWG discussions/ evaluations?**	**Workload More or less than traditional approach?**	**Lessons Learned and Recommendations**
Determination of Requirement Applicability	✓ Manually determined	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Analyst dependent	✓ Analyst dependent. Requirements can be linked to the model	✓- Excel post-processing required	✓ Requires manual post-processing	✓ Still requires manual editing, but in a different way.	The ability to import and export requirements with consistent fields would improve this capability. The ability to link model elements to the requirements is a big advantage over current tools.
Compliance Assessment (e.g. I, NA, C, T, NC)	✓ Manually determined	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Analyst dependent	✓ Analyst dependent	✓- Excel post-processing required.	✓ Requires manual post-processing	✓ Still requires manual editing, but in a different way.	"Classification" field was used for Compliance. A restricted field, consistent with the assessment type would be a desirable enhancement
Requirement Tailoring (i.e. write equivalent requirement)	✓ Manually determined	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Analyst dependent	✓+ Tailoring can be done within the modeling process and linked to the model	✓- Excel post-processing required.	✓ Requires manual post-processing	✓ Still requires manual editing, but in a different way.	The "Pre-requisite" field was used for tailored text.
Acceptance Rationale (applies to any Compliance assessment except "C" including NA)	✓ Manually determined	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Analyst dependent	✓+ Tailoring can be done within the modeling process and linked to the model	✓- Excel post-processing required.	✓ Requires manual post-processing	✓ Still requires manual editing, but in a different way.	The "Verification Methods" field was used for Acceptance Rationale. Merged with Supporting Rationale for this test. Recommend separating them.
Supporting Rationale documentation	✓ Manually determined	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Analyst dependent	✓+ Tailoring can be done within the modeling process and linked to the model	✓- Excel post-processing required.	✓ Requires manual post-processing	✓ Still requires manual editing, but in a different way.	The "Verification Methods" field was used for Acceptance Rationale. Merged with Supporting Rationale for this test. Recommend separating them.
Supporting documentation, attachments, links to SDP, other artifacts, or sources	✓ Manually attached or referenced	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Manual. Output not available for attachments.	✓ Manual. Output not available for attachments.	✓- Output not available for attachments and especially images.	✓- Output not available for attachments and especially images.	✓- Post process outputs to add in attachments and images.	Allow attachments and images to be output inline with analysis. Libraries and copying from model to model can mitigate manual tasks

Tool: MADE **Analysis:** Safety Assessment Report (SAR) (component)/ Safety Data Package (SDP) (for a Complete System)	**Innate capability of the Tool**	**Consistency from Model to Model**	**Accuracy**	**Analysis complete and mission relevant?**	**Consistent with GSFC practices and ratings?**	**Can a safety assessment be succinctly represented by outputs?**	**Can Outputs support PSWG discussions/ evaluations?**	**Workload More or less than traditional approach?**	**Lessons Learned and Recommendations**
Functional block diagrams (as modeled in Tool)	✓+ Very convenient drag n' drop capability with a library of predefined functional blocks.	✓ More consistency compared to manual	✓ Accuracy is dependent on operator's knowledge of the model and use of built in libraries.	✓ Valid starting point with limited manipulation and customization capabilities.	✓ More details than may usually be required for projects.	✓+ This would be a new product which could provide an enhanced understanding of the design as it applies to safety.	✓ New product which would aid in Cause and Control discussions and their correlation to design	NA New product. No additional effort required since this is a feature of the tool/model	Very effective and easy to navigate. Learning curve will become flat very quickly. Consistent with remainder of model – 1-truth. Pictorial output generated by tool feature
Supporting images, attachments and descriptions from existing documentation output	✓ Manually attached or referenced	✓ Entered manually, Analyst dependent	✓ Entered manually, Analyst dependent	✓ Manual. Output not available for images or attachments.	✓ Manual. Output not available for images or attachments.	✓- Output not available for attachments and especially images.	✓- Output not available for attachments and especially images.	✓- Post process outputs to add in attachments and images.	Allow attachments and images to be output inline with analysis. Libraries and copying from model to model can mitigate manual tasks
Hazard Analysis Results Summary	✓- Achievable with extensive post-processing of Excel Hazard Report Output (See Hazard Analysis Table above).	✓ Analyst Dependent	✓ Analyst Dependent	✓ Analyst Dependent	✓- Produces reports iaw SAE ARP4761 instead of NASA Format Extensive post-processing required.	✓ Achievable with extensive post-processing.	✓ Analyst Dependent	✓ Work load is similar.	Add an option to provide summary of Hazard Reports in a standard GSFC format (NF1825[10]).
Stored Energy Assessment	✓ Analyst Dependent. Functional Block Diagrams can provide this information	✓ Analyst Dependent.	✓ Analyst Dependent	✓ Analyst Dependent	✓ Analyst Dependent	✓ Analyst Dependent. Appropriate text must be added to model description for this to be available	✓ Analyst Dependent	✓ Similar. Must be included in model, but once this is done, may be less.	Recommend adding a checkbox when developing the model to indicate a stored energy device. Currently Analyst must add "stored energy device" in text description to identify.
Integrated system description in a safety context, data sources used, images and attachments produced as a report	✓- System produces a System Information Report (SIR). However, only manually entered descriptions are included.	✓- Manually produced outside the model by combining SIR, Hazard Reports & Summary, Stored Energy information, custom text and images	✓ Analyst dependent	✓ Analyst dependent.	✓ Analyst dependent	✓- Integrated output not available. Analyst can manually produce report outside the model by combining SIR, Hazard Reports & Summary, Stored Energy information, custom text and images	✓ Analyst dependent.	✓- Extensive post-processing with the potential for an increased workload.	Recommend adding the capability to integrate the SIR with other information, including attachments and images, to form a coherent report.

Table 3: Reserved for SysML/MagicDraw Evaluation

✓ = Status Quo

✓+ = Significant Improvement over traditional method

✓- = Worse than traditional method

NA = Not Applicable

Page Intentionally Left Blank

5 *DISCOVERIES AND 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 System 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 (see Table 3 for each study tool's readiness to provide the optimal MA environment):

    - 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 that 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 show 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 12 for a possible hazard library structure).

        - The library would include potential hazard 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 (e.g., procedures, control inspection, verifications) 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 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 (interactively and in a report) 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 generate an SDP package with detailed 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 81): 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.

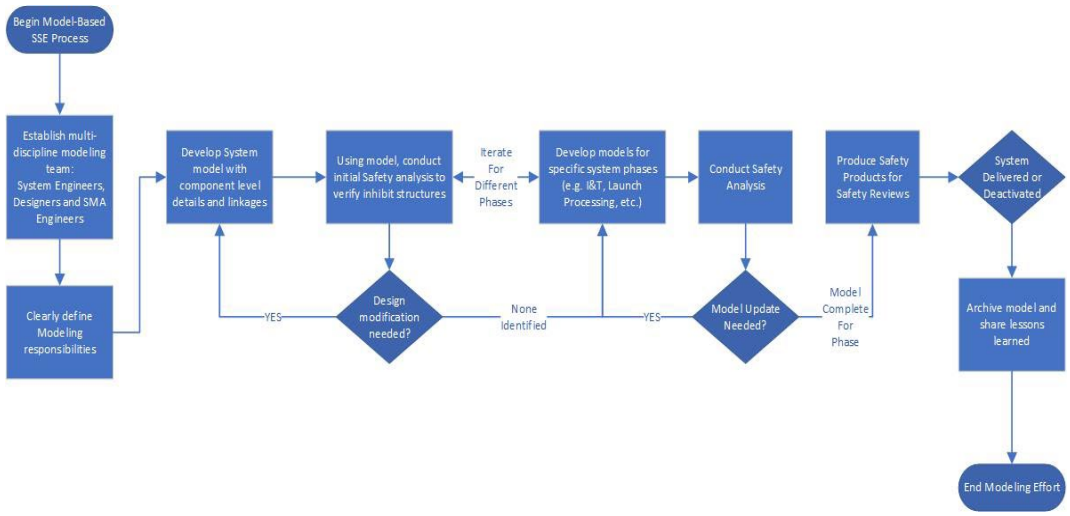


Figure 81:Notional Model-Based System Safety Process

Table 3: Environment Compliance Table

	Requirement	SysML/MagicDraw	MADE
1	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).	N/A No Safety features inherent in environment	✓ Manually defined or copied from a previous model
2	The ability to ingest and parse or allocate text, diagrams, illustrations, and images to safety products and/or models.	N/A No Safety features inherent in environment	✓- Manual ingestion of descriptive text and diagrams/images is possible at each modelling element (making parsing – irrelevant). Safety products do not utilize these inputs, and reports do not include text or images. This makes safety products incomplete for NASA.
3	An easily mastered structure and interface for efficiency.	✓- Steep Learning curve. (From Reference 1)	✓+ Easily traversed and understood by modelers and non-modelers.
4	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.	N/A Not tested in this phase	✓ Extensive libraries of generic functions and failure causes/mechanisms exist; custom libraries of components can be built, from existing models or manually, that would include safety hazard modeling. No specific hazard library at this time.
5	The ability to create a functional model of the systems for efficiency and clarity.	N/A Not tested in this phase	✓+ Functional Block Diagram is the heart of the model and relates all other model pieces. ✓ Hazard models currently need to be completed using the *Functional Diagram* that is deigned more for failure than NASA hazard modeling, so fields names are not consistent with data being entered for hazards, which can reduce clarity and require additional care to ensure accuracy/consistency.
6	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 and/or show as an error that needs to be resolved by the modeler.to enable model accuracy and efficiency.	✓- Each diagram is managed by the modelers independently; No error checking is present. Copy/pasting and deleting methods complex. (From Reference 1)	✓+ Model changes (additional components / failure causes / modes / etc.) propagate through the model well; error checking is continuous but not intrusive. ✓- Changes to the *Functional Diagram* do not currently update across the model (e.g., linked failure condition and annotation changes do not revise (or only partially revise) the corresponding failure diagrams).

Efficiency Consistency Accuracy

	Requirement	SysML/MagicDraw	MADE
7	The ability to simulate the accumulation of material or actuations on modeling elements as well as failures for efficiency and accuracy.	N/A Not tested in this phase	✓- Exceeding the capacity of a system boundary is not articulated in the model. For example, accumulating more fuel than a tank can hold will not be flagged in the model. Transfer of material is clearly modeled unless this applies to material or actuations, such as quantity, volume, or pressure, and thus appears difficult to identify, if not impossible. However, more than one failure mode can be identified. ✓ There is the capability to inject failures using the simple "Failure Injection" user-clickable interface, which shows accurate results. The results are shown via transient, on-screen model-failure impact-propagation animations and an on-screen table (that can be exported as a raw Excel file). An animation recording feature (with exporting capability) and a reporting capability would be much more efficient for sharing results with stakeholders and other models.
8	The ability to allocate requirements to a functional diagram/element to analyze whether or not safety requirements have been met.	N/A Not tested in this phase	✓ Connection capability good but controls/verifications limited – text only. ✓- Compliance is determined and entered manually only.
9	The ability to fully edit hazard-modeling elements (including identifiers) to ensure accuracy.	N/A No Safety features inherent in environment	✓ Controls missing and verifications are just textual (cannot link a verification artifact), not drop-down. Next version remedies all but attachments.
10	The ability to develop libraries of hazard categories with baseline definitions and implication data for consistency and accuracy (see Figure 12 for a possible hazard library structure with causes).	✓- Library Creation would need developed while avoiding copy/pasting/deleting issues; but models can be copied in their entirety into a new model, so a community solution is plausible. (From Reference 1)	✓- Extensive libraries of functions/causes/mechanisms exist; Custom libraries for hazards are not a current capability.

Efficiency Consistency Accuracy

	Requirement	SysML/MagicDraw	MADE
11	The ability to add models of systems or portions of systems to a library of shareable models for efficiency.	✓- Difficult; copy/pasting and deleting methods complex and may not be fully effective; but models can be copied in their entirety into a new model, so a community solution is plausible. (From Reference 1)	✓ Copy/pasting within a model is possible and error free. Possible: Custom libraries of models, failure modes, causes, functions are all possible but were not tested.
12	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.	✓- No Safety features inherent in environment	✓- Manual Only (no import) and no attachments are output in MADE reports.
13	The ability to copy hazard modeling without linkages or challenge the modeler to verify linkages if applicable.	✓- No Safety features inherent in environment	✓- Can copy hazard categories with linkages to create new ones in the model; but we cannot copy hazards or hazard causes from category to category.
14	The ability to combine models and duplicate models for reuse in future modeling efficiency.	✓- Difficult; copy/pasting and deleting methods complex and may not be fully effective; but models can be copied in their entirety into a new model, so a community solution is plausible. (From Reference 1)	✓ Inherent in the tool, there is the ability to import sub-models or component models from other models using Project Import; custom libraries can also be used to share models / portions of models, failure modes, causes, and functions across users but were not tested.
15	Provisions for model component and system consistency error checking and reporting for improved modeling accuracy.	✓- None at this time (From Reference 1)	✓ Modeling error checking is continuous but not intrusive for system flows/functions. ✓- There is no safety/hazard validity checking apparent at this time.
16	Model change control/reporting (i.e., detailed configuration control) including the ability to revert to a previous model for accuracy.	✓- None at this time (From Reference 1) Not tested in this phase	✓ Change tracking and reporting is available and is not intrusive (Data Quality Assessment (DQA) report – could be improved by labeling it a "Change Log" not "Annotations" for better understanding). Reversion would be manual only (undo changes manually or revert to a previously saved version), since automated roll-back (and undo) is not available.

Efficiency Consistency Accuracy

	Requirement	SysML/MagicDraw	MADE
17	The ability to import requirements, CAD, and BOM/part lists type data to create modeling elements or as supporting data for efficiency.	N/A Not tested in this phase	✓ Requirements can be imported, but the sorting, allocation, and labeling is manual and not intuitive. Currently MADE can import MADE.STEP files (CAD or BOM) or Teamcenter BOMs. JSON and BOM from an Excel file importing appears possible but is untested.
18	The ability to select and allocate requirements to each element or hazard for verification/compliance recording efficiency.	N/A Not tested in this phase	✓ Yes, requirements can be selected and linked/allocated to all appropriate components within the model. Verifications are not linked to other features and are textual only.
19	An export or reporting function for fault tree and simulation results for understanding and accuracy validation.	N/A Not tested in this phase	✓ FT – Images, as a single image, can only be generated via display snapping at this time (which can be difficult and can cause readability issues). Reports can be generated for failure scenarios in pdf or Excel (but not in the NASA format – See Reference 1) and for hazards (but only one hazard tree at a time and not in the NASA format). Currently, larger fault trees had pdf image-overflow issues making them incomplete. ✓ FT- Exporting for ingestion in other tools can be accomplished using comma separated format (.csv) or JSONs. ✓- Simulations are available, easy to follow, and provide good insights, but no report is available to document/share results easily. Simulation step results can only be exported to an Excel or CSV at this time. Having a recording and report capability would be better.
20	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.	N/A Not tested in this phase	✓+ Easily traversed and understood by modelers and non-modelers.
21	The ability to produce a preliminary hazard assessment and subsequent hazard reports using NASA-defined severities and likelihoods.	✓- No Safety features inherent in environment;	✓- ✓Safety reports do not currently use NASA terminology or format. Significant post-processing is needed to bring to the NASA format. The Excel/table style is a plus. Custom report generation would be helpful to remedy this issue.

Efficiency Consistency Accuracy

	Requirement	SysML/MagicDraw	MADE
22	The ability to produce a fault tree (interactively and in a report) with a hazard as the top-level event (pulling causes and contributions from all system elements) and precise Boolean logic for accuracy.	✓- Fault Tree logic issues. (From Reference 1)	✓ Logic validated for each hazard, but trees did show stacked events that should be combined for additional accuracy (See Section 3.3.4.1). Hazard fault trees were not quantified in this study, since that was validated in Reference 1. Reporting is available see requirement 19.
23	The ability to produce a compliance checklist per NASA-STD-8719.24.	✓- No Safety features inherent in environment	✓ The capability to manually verify requirements and generate a requirements report is available, but the process is very manual, and verifications are not pulled from other modeling features.
24	The ability to hold and generate an SDP package with detailed information in the NASA format (Per Attachment 1, Vol 3 of NASA STD 8719.24)	✓- No Safety features inherent in environment	✓- The holding of descriptive text and diagrams/images for an SDP is possible at each modelling element (See Requirement 2). However, the current (3.8.7 SP1) System Information Report (SIR) does not meet NASA STD for an SDP, as it only provides a modeling view of the system, and the descriptive data held is not included in the SIR (See Section 3.3.3).
25	The ability to export to NASA databases directly.	N/A Not tested in this phase	✓ All MADE analyses are able to be exported in comma separated format (.csv), which should be able to be imported into databases. This was not tested during this study. Nevertheless, since NASA's ELV Database (ELV) just stores documents, it can be inferred that the MADE reports (in pdf or Excel formats) should be able to be delivered and stored manually (no direct link like traditional delivery). However, NASA's Human Flight Databases store an entry for each individual hazard, which could be manually entered from modeling reports. But it would be best if those could be imported from the model, versus manually entered. Import testing from MADE to the JSC -Hazard System would need to be conducted using csv or JSON or other formats to determine feasibility.
26	Performance that shortens analysis time while maintaining consistency and accuracy between models.	✓- No Safety features inherent in environment	✓ Potential for analysis time savings once NASA process/outputs are available, but no efficiency or penalty was apparent at this time. Accuracy/Consistency improvement potential exists but can only be realized by using model-reuse and library-use/creation capability.

Efficiency Consistency Accuracy

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. Consequently, 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, it would be best if NASA subject-matter experts and PHM continue to collaborate on modelling environment optimizations (see Section 4 and Table 3 for tool needs) to ensure positive returns (i.e., improved efficiency, consistency, accuracy) are maximized to support future NASA missions, since MADE is the only SMA-capable tool to provide both safety and reliability engineering capabilities and positive returns, as of the conclusion of this study.

Additionally, this study's results, recommendations, and guidance (see Appendix B) are provided to NASA to advance SMA analysis compatibility, to establish SMA-to-SE/SE-to-SMA modeling collaboration and transition points and to 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 to advance Model-Based tool capabilities.

For these reasons, GSFC is planning, to execute more phases of this study to assist NASA/GSFC in developing a unified Model-Based engineering approach and determine the best tool set to support that approach. The next phase of the MBSMAI will evaluate Software Assurance and/or Quality Engineering Analysis compatibility.

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, "System Safety Handbook," NASA/SP-2014-612 Vol 2, November 2014.
[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 Propulsion Critical Design Review Package (EUROPA-PROP-REVW-0006)," 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] NASA Payload Safety Hazard Report (NF1825), available via https://forms.neacc.nasa.gov/documents/11002/305376/NF1825.pdf?download=true&v=1.1

INDEX

EXECUTIVE SUMMARY & CONCLUSIONS ……1
BACKGROUND 2
1.1 Hazard Analysis 2
1.2 Safety Requirements 2
1.3 Safety Fault Tolerance and Inhibits 2
1.4 Safety Products 3
TEST METHODOLOGY..... 3
2.1 Testing Process 3
2.2 Modeling Tools Utilized..... 4
2.2.1 MADE 4
2.2.2 SYSML/MAGICDRAW 5
MODELS AND RESULTS..... 7
3.1 EUROPA PROPULSION..... 7
3.1.1 MADE Functional Modleing..... 7
3.1.1.1 GSE-PGSE Functional Modeling..... 7
3.1.1.2 PME/Diode Box Functional Modeling.. 7
3.1.1.3 Enable Plug..... 9
3.1.2 MADE Hazard Modleing 9
3.2 SYSML/MAGICDRAW 20
3.3 Results and Observations 20
3.3.1 Hazard Analysis (HA) 20
3.3.2 Compliance Matrix or SRCC Analysis 21
3.3.3 Safety Data Package (SDP) 22
3.3.4 Fault Analysis and Inhibit Verification 22
3.3.5 Other types of Hazard Analysis 27
STUDY FINDINGS AND EVALUATIONS 37
4.1 MADE..... 37
4.2 *SYSML/MAGICDRAW*..... 38
DISCOVERIES AND RECOMMENDATIONS..... 45
Optimal Modeling Environment Needs……...45
Modeling process and controls ……46
CONCLUSIONS & PATH FORWARD..... 52

Table of Figures

Figure 1: EUROPA Propulsion Subsystem 3
Figure 2: SAE Safety Assessment Process Overview 5
Figure 3: MADE *Functional Diagram* (FD) 5
Figure 4: MADE Hazard Properties Input Fields 6
Figure 5: Hazard Enhanced Functional Block/Failure Diagrams 6
Figure 6: MADE Simulation Results 6
Figure 7:MADE EUROPA GSE..... 8
Figure 8:MADE EUROPA Propulsion Module 8
Figure 9: MADE EUROPA PGSE..... 8
Figure 10: EUROPA Enable Plug 9
Figure 11: MADE EUROPA Component vs Hazard Category 9
Figure 12: MADE EUROPA Hazard Category/Implications 10
Figure 13: MADE EUROPA *Functional Diagram*..... 10
Figure 14: MADE Failure Diagram Safety/FMECA reporting 13
Figure 15: MADE EUROPA Mission phases/environments 13
Figure 16: MADE EUROPA Fire/Explosion 14
Figure 17: MADE EUROPA Leaks/Spills 15
Figure 18: MADE EUROPA Structure 16
Figure 19: MADE EUROPA Electrical/Grounding 16
Figure 20: MADE EUROPA Pressure/Hydraulic 17
Figure 21: MADE EUROPA Contamination/Corrosion..... 17
Figure 22: MADE EUROPA Mechanical..... 18
Figure 23: MADE EUROPA Temperature 18
Figure 24: MADE EUROPA Control Systems 19
Figure 25: MADE EUROPA Physiological..... 19
Figure 26: MADE HA..... 20
Figure 27: Traditional SAR 20
Figure 28: Tailored/Linked Europa Requirement in MADE 21
Figure 29: MADE Compliance Matrix..... 21
Figure 30: Genreric Traditional Compliance Matrix Example 21
Figure 31: MADE SIR 22
Figure 32:Fire/Explosion Hazard FT – Traditional..... 23
Figure 33: Fire/Explosion Hazard Tree (MADE) 23
Figure 34: Structure Hazard Tree (MADE) 23
Figure 35: Leaks/Spills Hazard Tree (MADE) 23
Figure 36: Electrical/ Grounding Hazard Tree (MADE) 24
Figure 37: Mechanical Hazard Tree (MADE) 24
Figure 38: Pressure/Hydraulic Hazard Tree (MADE) 24
Figure 39: Contamination/Corrosion Hazard Tree (MADE) 24
Figure 40: Temperature Hazard Tree (MADE)..... 25
Figure 41: Control Systems Hazard Tree (MADE) 25
Figure 42: Physiological Hazard Tree (MADE) 25
Figure 43: MADE EUROPA inhibit model Case 1.1 29
Figure 44: MADE EUROPA inhibit model Case 1.2..... 29
Figure 45: MADE EUROPA inhibit model Case 1.3..... 29
Figure 46: MADE EUROPA inhibit model Case 1.4..... 30
Figure 47: MADE EUROPA inhibit model Case 1.5 30
Figure 48: MADE EUROPA inhibit model Case 1.6 30
Figure 49: MADE EUROPA inhibit model Case 3.1 30
Figure 50: MADE EUROPA inhibit model Case 3.2..... 30
Figure 51: MADE EUROPA inhibit model Case 4.1..... 30
Figure 52: MADE EUROPA inhibit model Case 4.2..... 31
Figure 53: MADE EUROPA inhibit model Case 4.3 31
Figure 54: MADE EUROPA inhibit model Case 4.4..... 31
Figure 55: MADE EUROPA inhibit model Case 4.5..... 31
Figure 56: MADE EUROPA inhibit model Case 4.6..... 31
Figure 57: MADE EUROPA inhibit model Case 4.7 31
Figure 58: MADE EUROPA inhibit model Case 4.8..... 32
Figure 59: MADE EUROPA inhibit model Case 4.9..... 32
Figure 60: MADE EUROPA inhibit model Case 4.10 32
Figure 61: MADE EUROPA inhibit model Case 4.11..... 32
Figure 62: MADE EUROPA inhibit model Case 4.12..... 32
Figure 63: MADE EUROPA inhibit model Case 4.13..... 32
Figure 64: MADE EUROPA inhibit model Case 4.14 33
Figure 65: MADE EUROPA inhibit model Case 4.15..... 33
Figure 66: MADE EUROPA inhibit model Case 4.16..... 33
Figure 67: MADE EUROPA inhibit model Case 4.17..... 33
Figure 68: MADE EUROPA inhibit model Case 4.18 33
Figure 69: MADE EUROPA inhibit model Case 4.19..... 33
Figure 70: MADE EUROPA inhibit model Case 4.20 34
Figure 71: MADE EUROPA inhibit model Case 4.21 34
Figure 72: MADE EUROPA inhibit model Case 4.22 34
Figure 73: MADE EUROPA inhibit model Case 4.23..... 34
Figure 74: MADE EUROPA inhibit model Case 4.24..... 34
Figure 75: MADE EUROPA inhibit model Case 4.25 34
Figure 76: MADE EUROPA inhibit model Case 4.26 35
Figure 77: MADE EUROPA inhibit model Case 4.27..... 35
Figure 78: MADE EUROPA inhibit model Case 4.28..... 35
Figure 79: MADE EUROPA Nominal Operating States 36
Figure 80: Hazard Tree Issues (Click on icons open full reports) 39
Figure 81: Notional Model-Based System Safety Process 46

Figure A1: EUROPA Propulsion System MADE Model 56
Figure A2: MADE EUROPA Pressurant Control Assembly – Fuel 57
Figure A3: MADE EUROPA Pressurant Control Assembly – Oxidizer 58
Figure A4: MADE EUROPA Propellant Isolation Assembly – Fuel 59
Figure A5: MADE EUROPA Propellant Isolation Assembly – Oxidizer 60
Figure A6: MADE EUROPA REM System Model (Qty 4 one for each REM) 61
Figure A7: MADE EUROPA Service Valve Assembly – Fuel 62
Figure A8: MADE EUROPA Service Valve Assembly - Oxidizer 62
Figure A9: MADE EUROPA MV2FG 62
Figure A10: MADE EUROPA GSE System Model 63
Figure A11: PGSE System Model 63
Figure A12: PME *Failure Diagram* 64
Figure A13: Diode Box *Failure Diagram* 65
Figure A14: Fuel Tank *Failure Diagram* 66
Figure A15: Oxidizer Tank *Failure Diagram* 67
Figure A16: Fuel Pressurant Tank *Failure Diagram* 68
Figure A17: Oxidizer Pressurant Tank *Failure Diagram* 69
Figure A18: MADE EUROPA PCA – Fuel - F2FG *Failure Diagram* 70
Figure A19: MADE EUROPA PCA – Fuel-LV03FGA *Failure Diagram* 71
Figure A20: MADE EUROPA PCA – Fuel-LV04FGA *Failure Diagram* 71
Figure A21: MADE EUROPA PCA – Fuel-PCV5FGA *Failure Diagram* 72
Figure A22: MADE EUROPA PCA – Fuel-PCV6FGA *Failure Diagram* 72
Figure A23: MADE EUROPA PCA – Fuel-PCV7FGA *Failure Diagram* 72
Figure A24: MADE EUROPA PCA – Fuel-PCV8FGA *Failure Diagram* 73
Figure A25: MADE EUROPA PCA – Fuel-PT02FGAB *Failure Diagram* 74
Figure A26: MADE EUROPA PCA – Oxidizer-F1XG *Failure Diagram* 75
Figure A27: MADE EUROPA PCA – Oxidizer-LV01XGA *Failure Diagram* 76
Figure A28: MADE EUROPA PCA – Oxidizer-LV02XGA *Failure Diagram* 76
Figure A29: MADE EUROPA PCA – Oxidizer-PCV1XGA *Failure Diagram* 77
Figure A30: MADE EUROPA PCA – Oxidizer-PCV2XGA *Failure Diagram* 77
Figure A31: MADE EUROPA PCA – Oxidizer-PCV3XGB *Failure Diagram* 78
Figure A32: MADE EUROPA PCA – Oxidizer-PCV4XGB *Failure Diagram* 78
Figure A33: MADE EUROPA PCA – Oxidizer-PT01XGAB *Failure Diagram* 79
Figure A34: MADE EUROPA PIA – Fuel – F4FL *Failure Diagram* 80
Figure A35: MADE EUROPA PIA – Fuel – LV09FLA *Failure Diagram* 81
Figure A36: MADE EUROPA PIA – Fuel – LV10FLB *Failure Diagram* 81
Figure A37: MADE EUROPA PIA – Fuel – LV11FLA *Failure Diagram* 82
Figure A38: MADE EUROPA PIA – Fuel – LV12FLB *Failure Diagram* 82
Figure A39: MADE EUROPA PIA – Fuel – PT10FLAB *Failure Diagram* 83
Figure A40: MADE EUROPA PIA – Fuel – PT11-16FLAB *Failure Diagram* 84
Figure A41: MADE EUROPA PIA – Fuel – V2FL *Failure Diagram* 85
Figure A42: MADE EUROPA PIA – Oxidizer – F3X *Failure Diagram* 86
Figure A43: MADE EUROPA PIA – Oxidizer – LV05XLA *Failure Diagram* 87
Figure A44: MADE EUROPA PIA – Oxidizer – LV06XLB *Failure Diagram* 87
Figure A45: MADE EUROPA PIA – Oxidizer – LV07XLA *Failure Diagram* 88
Figure A46: MADE EUROPA PIA – Oxidizer – LV08XLB *Failure Diagram* 88
Figure A47: MADE EUROPA PIA – Oxidizer – PT03XLAB *Failure Diagram* 89
Figure A48: MADE EUROPA PIA – Oxidizer – PT04-09XLAB *Failure Diag* 90
Figure A49: MADE EUROPA PIA – Oxidizer – V1XL *Failure Diagram* 91
Figure A50: MADE EUROPA REM-1 (01Z11A Engine) *Failure Diagram* 92
Figure A51: MADE EUROPA REM-1 (02Z12A Engine) *Failure Diagram* 92
Figure A52: MADE EUROPA REM-1 (09Y1A Engine) *Failure Diagram* 93
Figure A53: MADE EUROPA REM-1 (13Z11B Engine) *Failure Diagram* 93
Figure A54: MADE EUROPA REM-1 (14Z12B Engine) *Failure Diagram* 94
Figure A55: MADE EUROPA REM-1 (21Y1B Engine) *Failure Diagram* 94
Figure A56: MADE EUROPA REM-2 (03Z21A Engine) *Failure Diagram* 95
Figure A57: MADE EUROPA REM-2 (04Z22A Engine) *Failure Diagram* 95
Figure A58: MADE EUROPA REM-2 (10Y2A Engine) *Failure Diagram* 96
Figure A59: MADE EUROPA REM-2 (15Z21B Engine) *Failure Diagram* 96
Figure A60: MADE EUROPA REM-2 (16Z22B Engine) *Failure Diagram* 97
Figure A61: MADE EUROPA REM-2 (22Y2B Engine) *Failure Diagram* 97
Figure A62: MADE EUROPA REM-3 (05Z31A Engine) *Failure Diagram* 98
Figure A63: MADE EUROPA REM-3 (17Z31B Engine) *Failure Diagram* 99
Figure A64: MADE EUROPA REM-3 (06Z32A Engine) *Failure Diagram* 99
Figure A65: MADE EUROPA REM-3 (19Z32B Engine) *Failure Diagram* 100
Figure A66: MADE EUROPA REM-3 (11Y3A Engine) *Failure Diagram* 100
Figure A67: MADE EUROPA REM-3 (23Y3B Engine) *Failure Diagram* 101
Figure A68: MADE EUROPA REM-4 (07Z41A Engine) *Failure Diagram* 101
Figure A69: MADE EUROPA REM-4 (08Z42A Engine) *Failure Diagram* 102
Figure A70: MADE EUROPA REM-4 (12Y4A Engine) *Failure Diagram* 102
Figure A71: MADE EUROPA REM-4 (19Z41B Engine) *Failure Diagram* 103
Figure A72: MADE EUROPA REM-4 (20Z42B Engine) *Failure Diagram* 103
Figure A73: MADE EUROPA REM-4 (24Y4B Engine) *Failure Diagram* 104
Figure A74: MADE EUROPA Service Valves – Fuel (MV2FG) *Failure Diag* 105
Figure A75: MADE EUROPA Service Valves – Fuel (MV5FG) *Failure Dia* 105
Figure A76: MADE EUROPA Service Valves – Fuel (MV6FL) *Failure Dia* 105
Figure A77: MADE EUROPA Service Valves – Fuel (MV1XG) *Failure Dia* 106
Figure A78: MADE EUROPA Service Valves – Fuel (MV3XG) *Failure Dia* 106
Figure A79: MADE EUROPA Service Valves – Fuel (MV4XL) *Failure Dia* 106
Figure A80: MADE EUROPA PGSE *Failure Diagram* 107

Appendix A : MBSMAI Models

MADE: All the functional block diagrams and failure diagrams

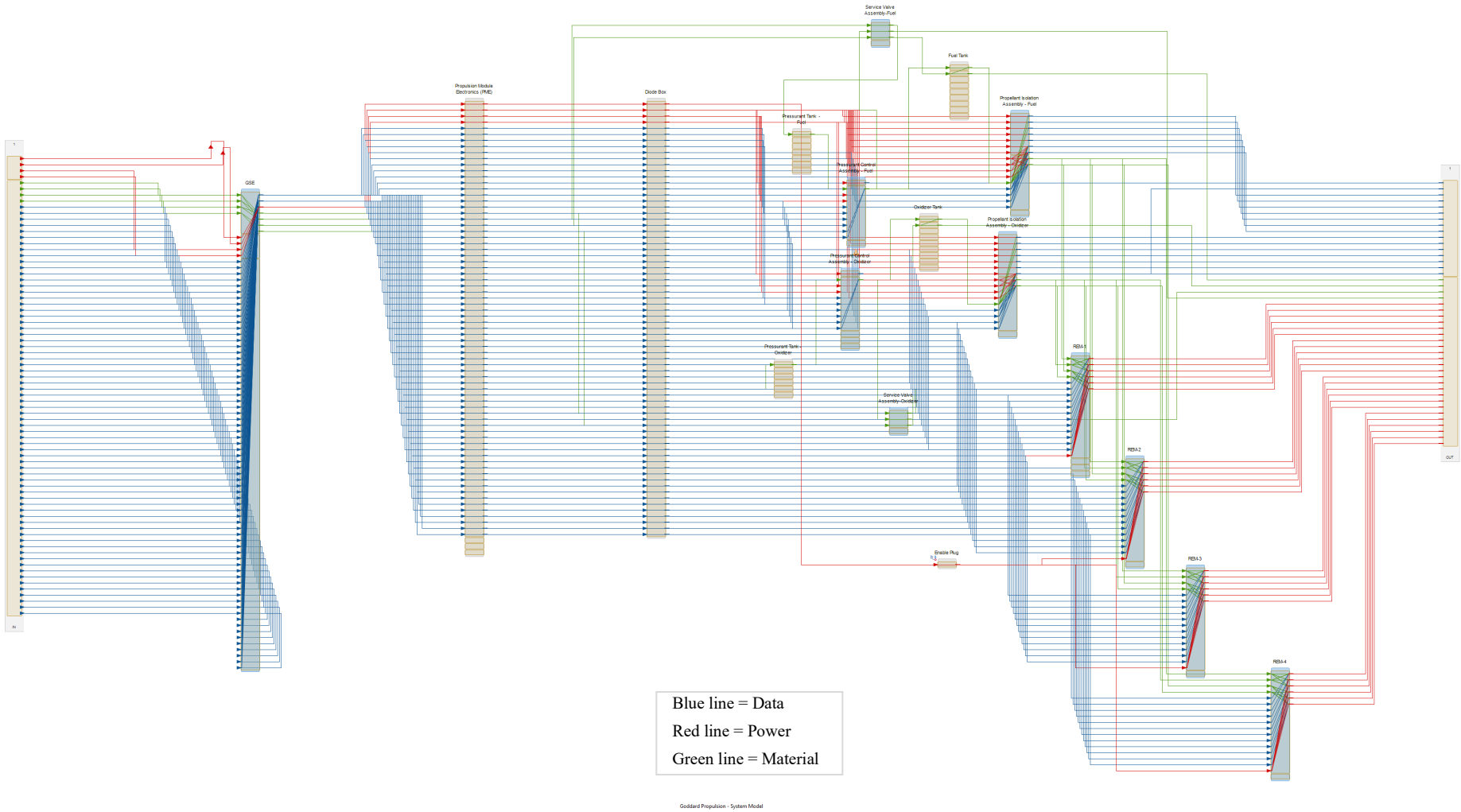


Figure A1: EUROPA Propulsion System MADE Model

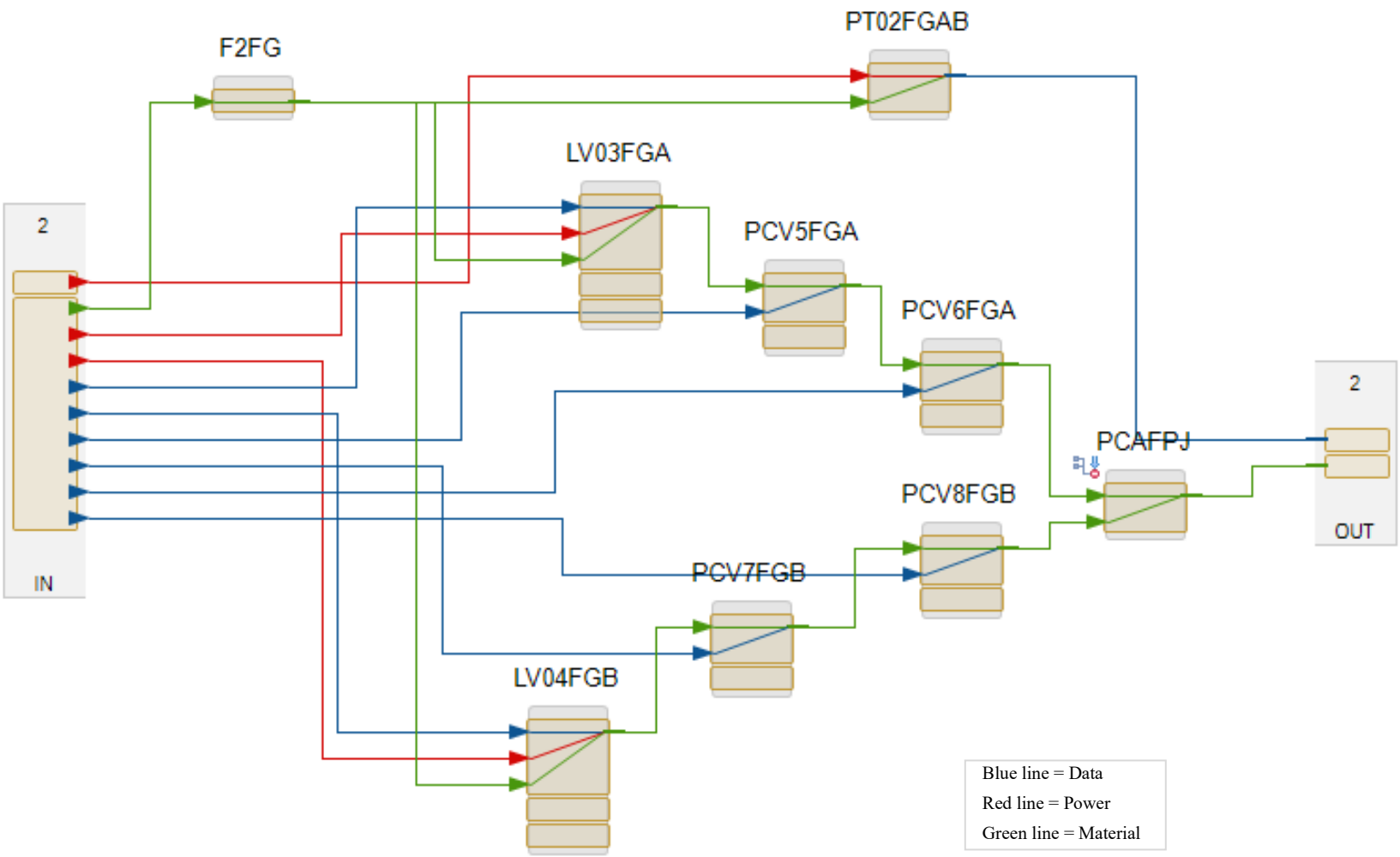


Figure A2: MADE EUROPA Pressurant Control Assembly – Fuel

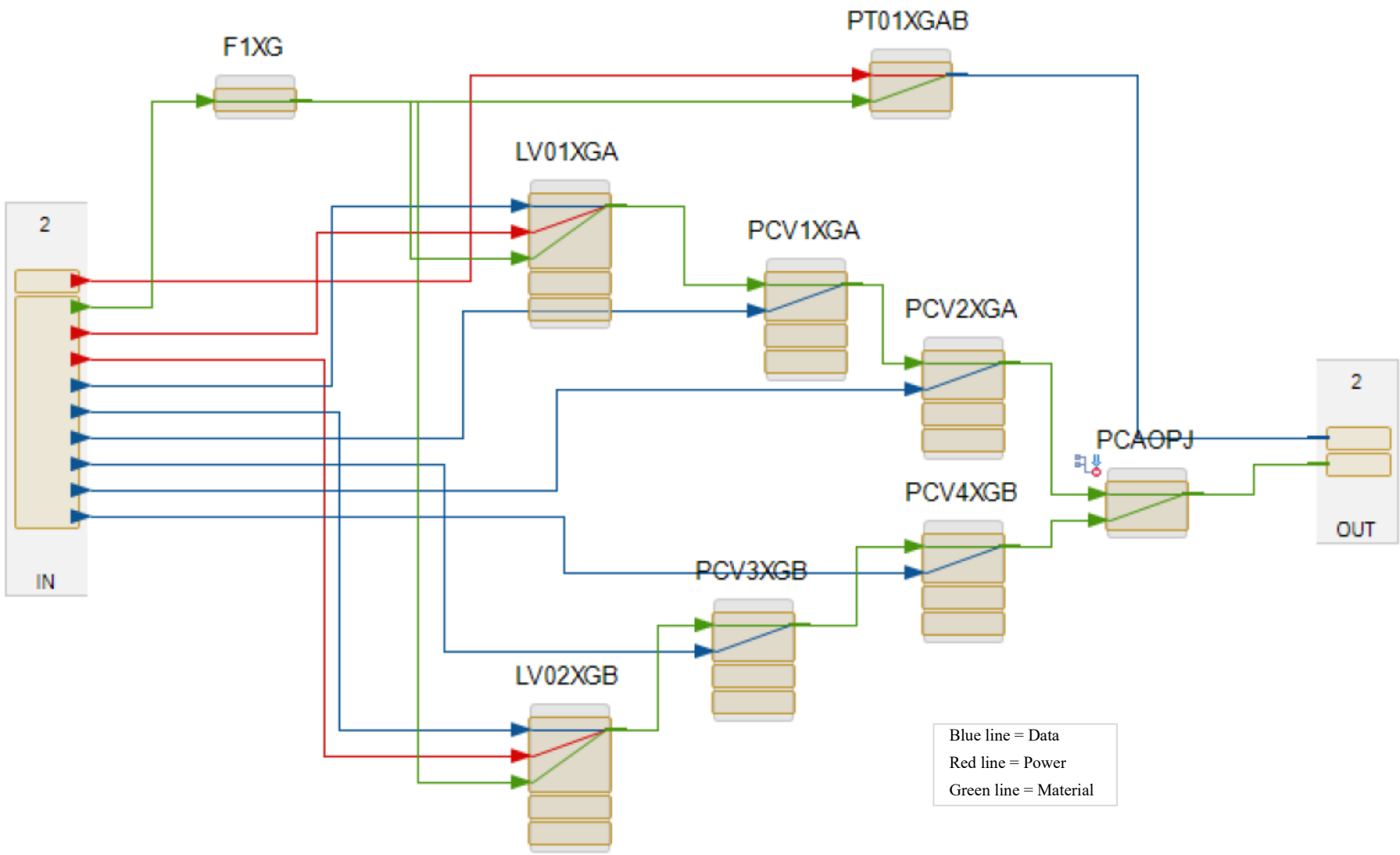


Figure A3: MADE EUROPA Pressurant Control Assembly – Oxidizer

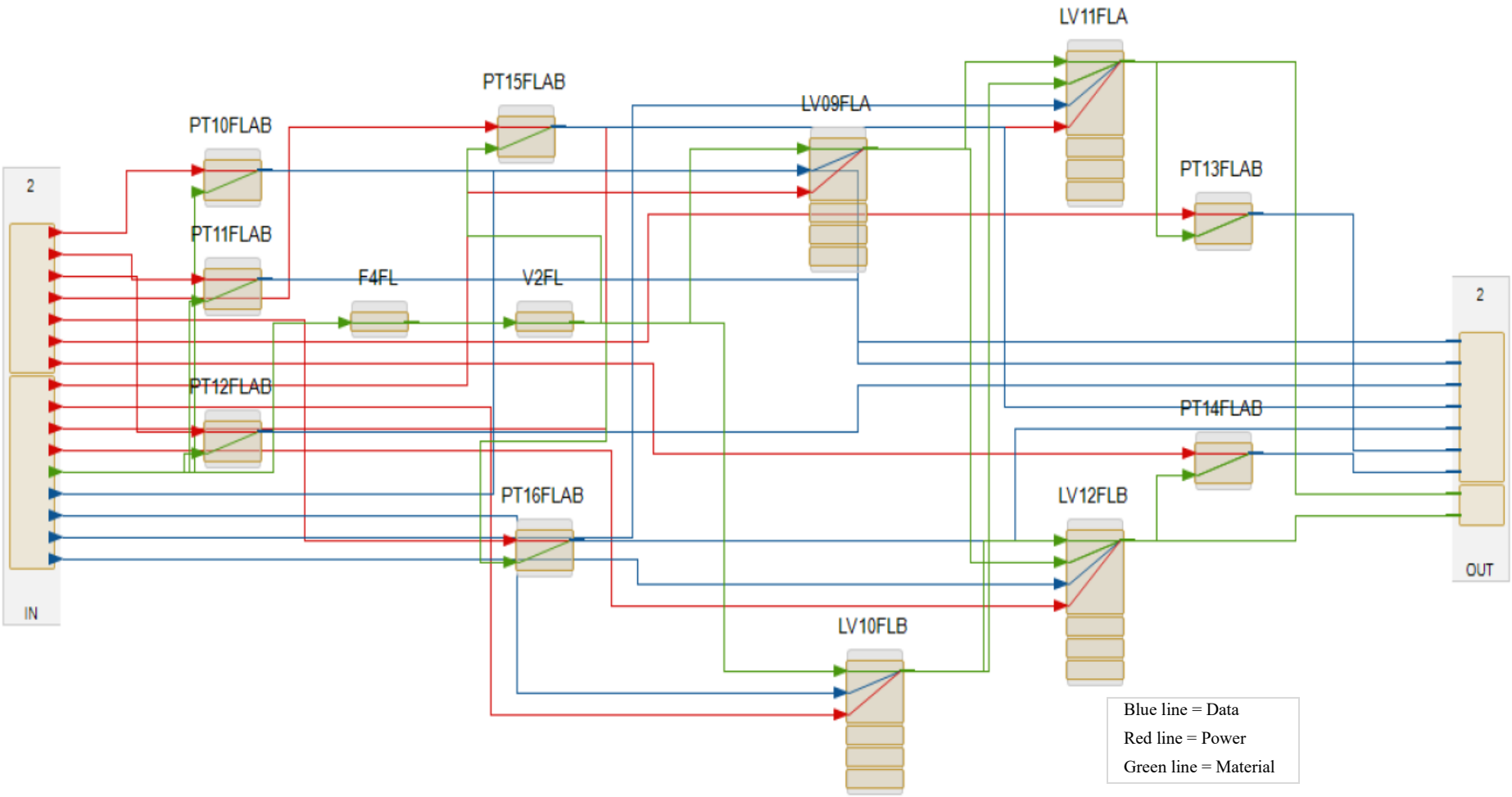


Figure A4: MADE EUROPA Propellant Isolation Assembly – Fuel

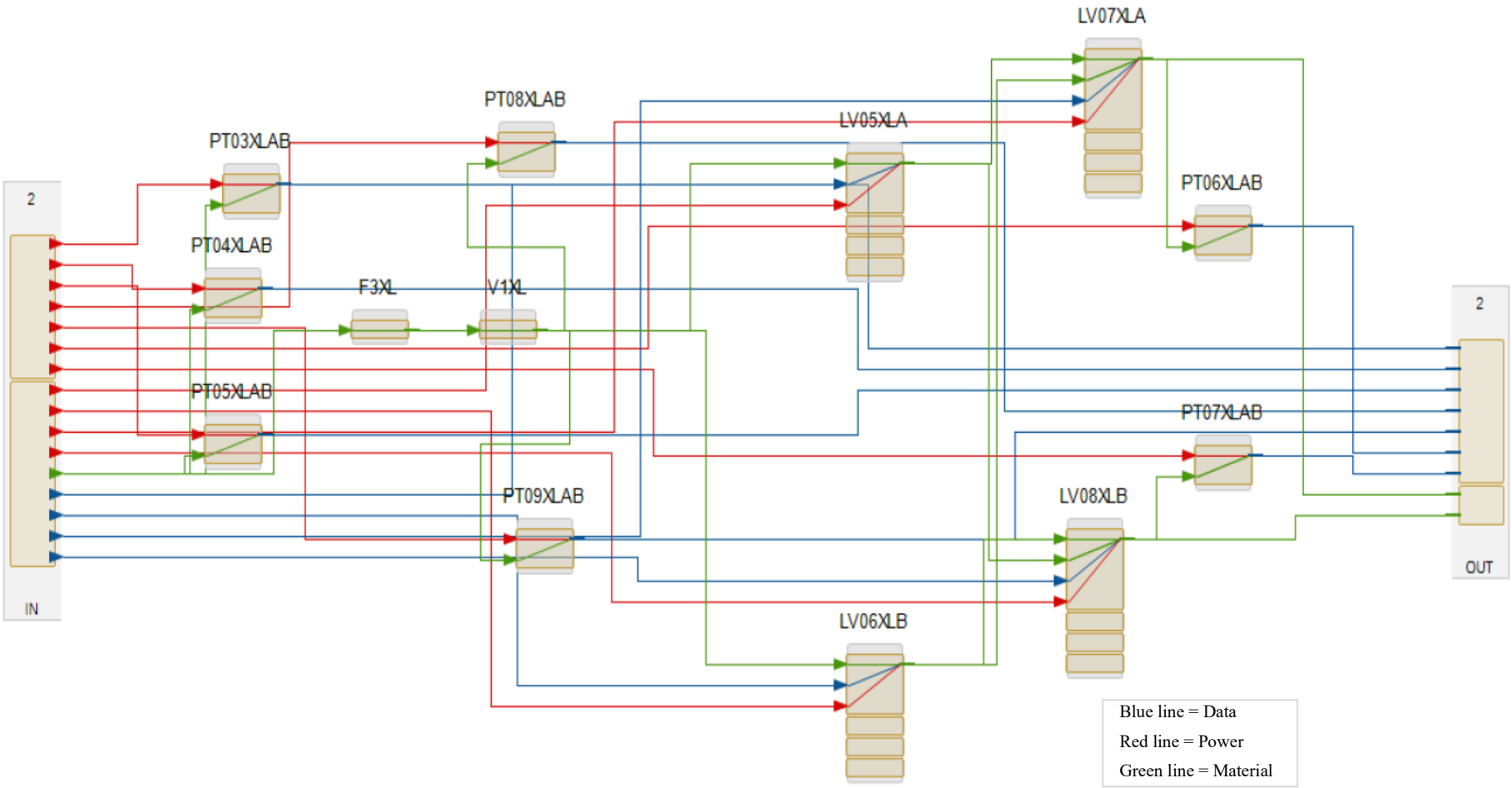


Figure A5: MADE EUROPA Propellant Isolation Assembly – Oxidizer

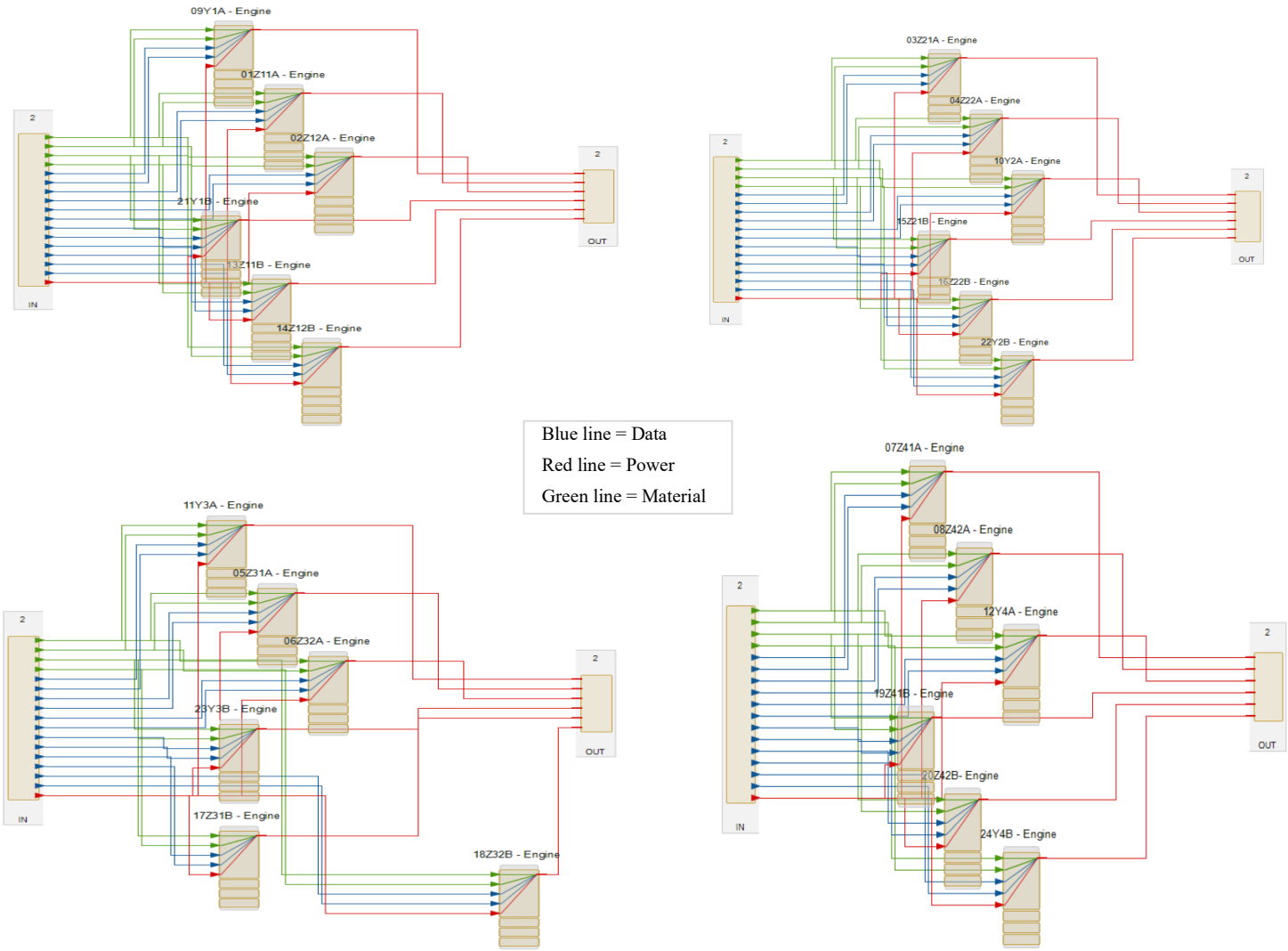


Figure A6: MADE EUROPA REM System Model (Qty 4 one for each REM)

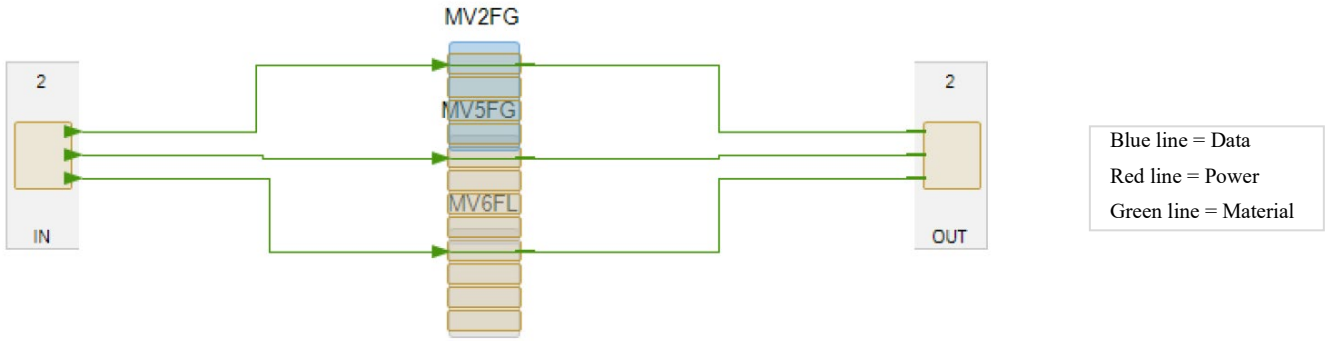


Figure A7: MADE EUROPA Service Valve Assembly – Fuel

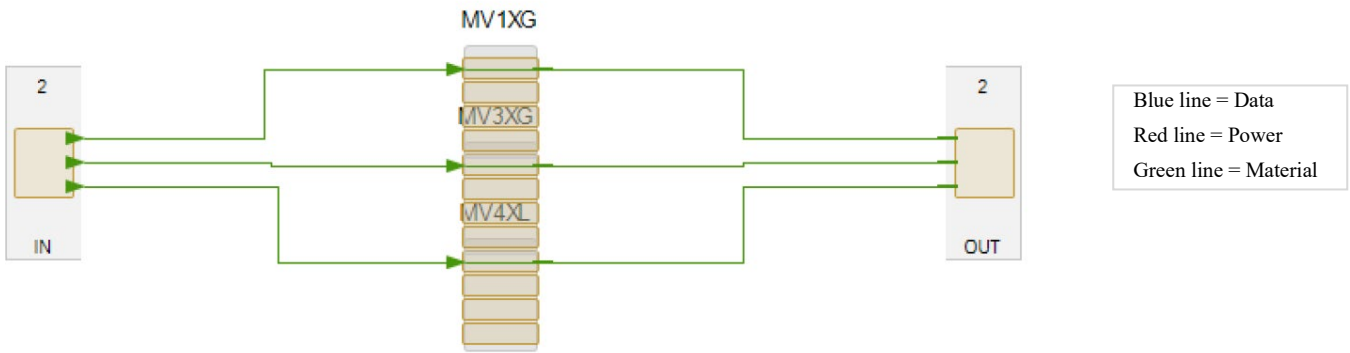


Figure A8: MADE EUROPA Service Valve Assembly - Oxidizer

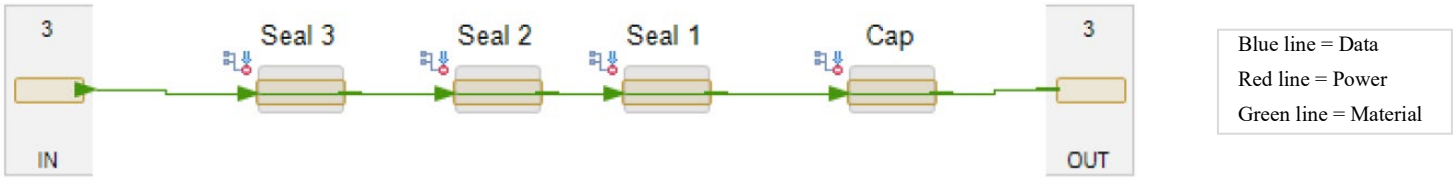


Figure A9: MADE EUROPA Mechanical Valve 2FG (MV2FG)

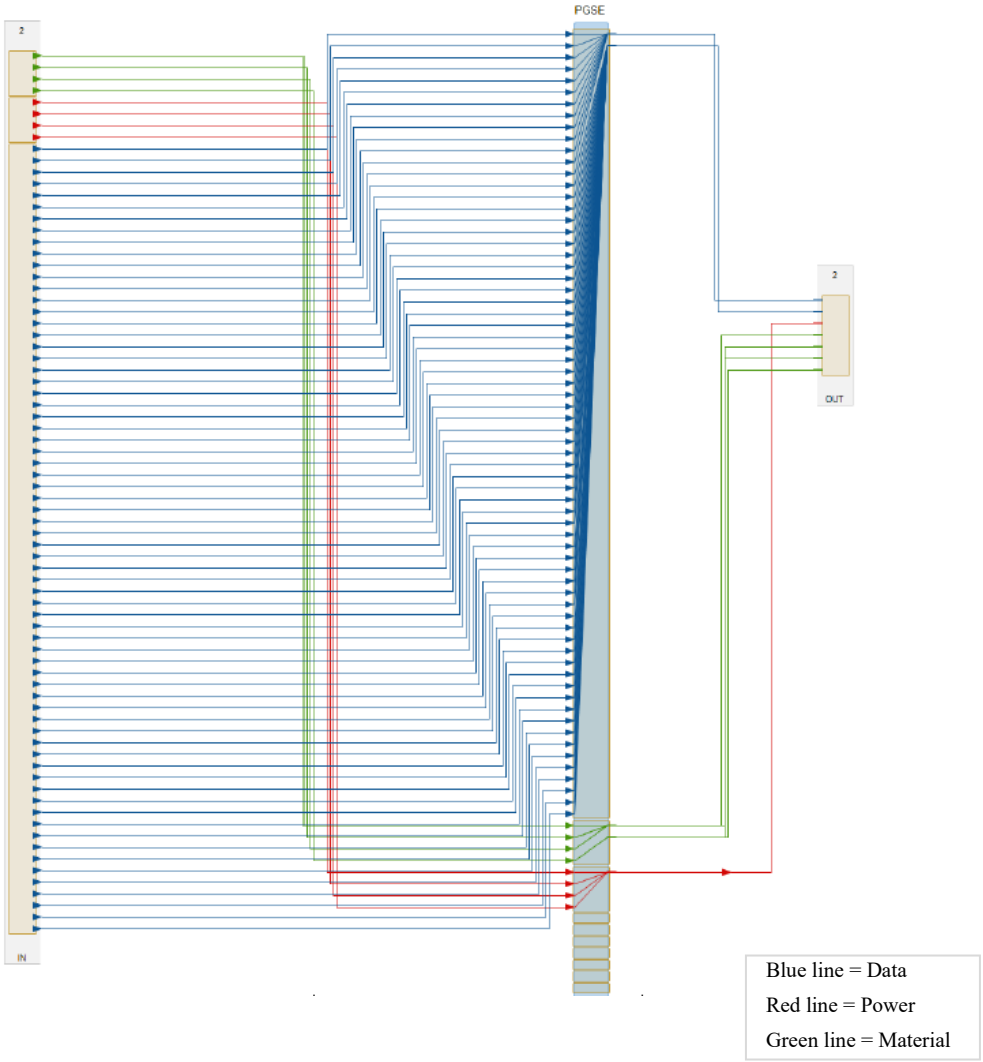


Figure A10: MADE EUROPA GSE System Model

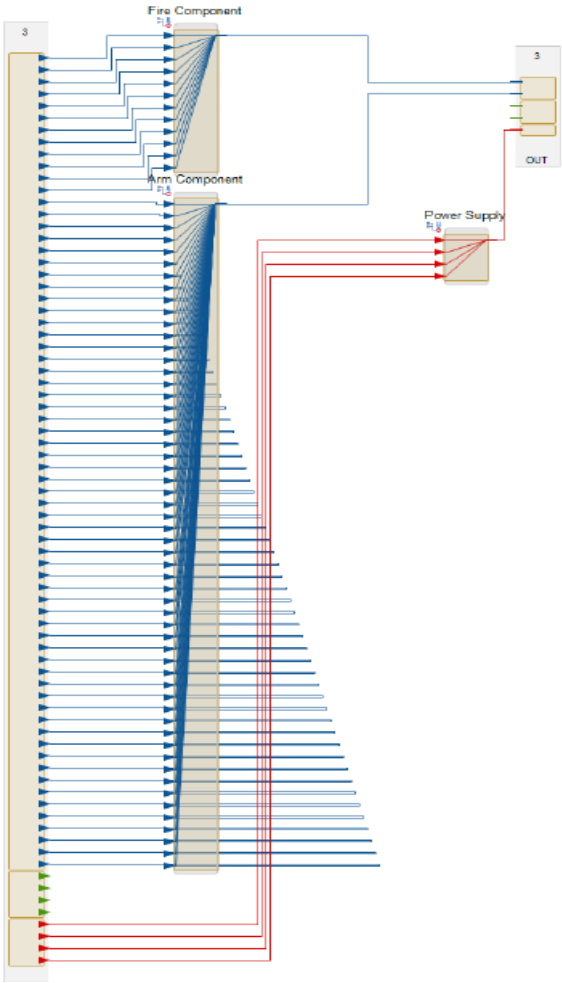


Figure A11: PGSE System Model

Failure Diagrams

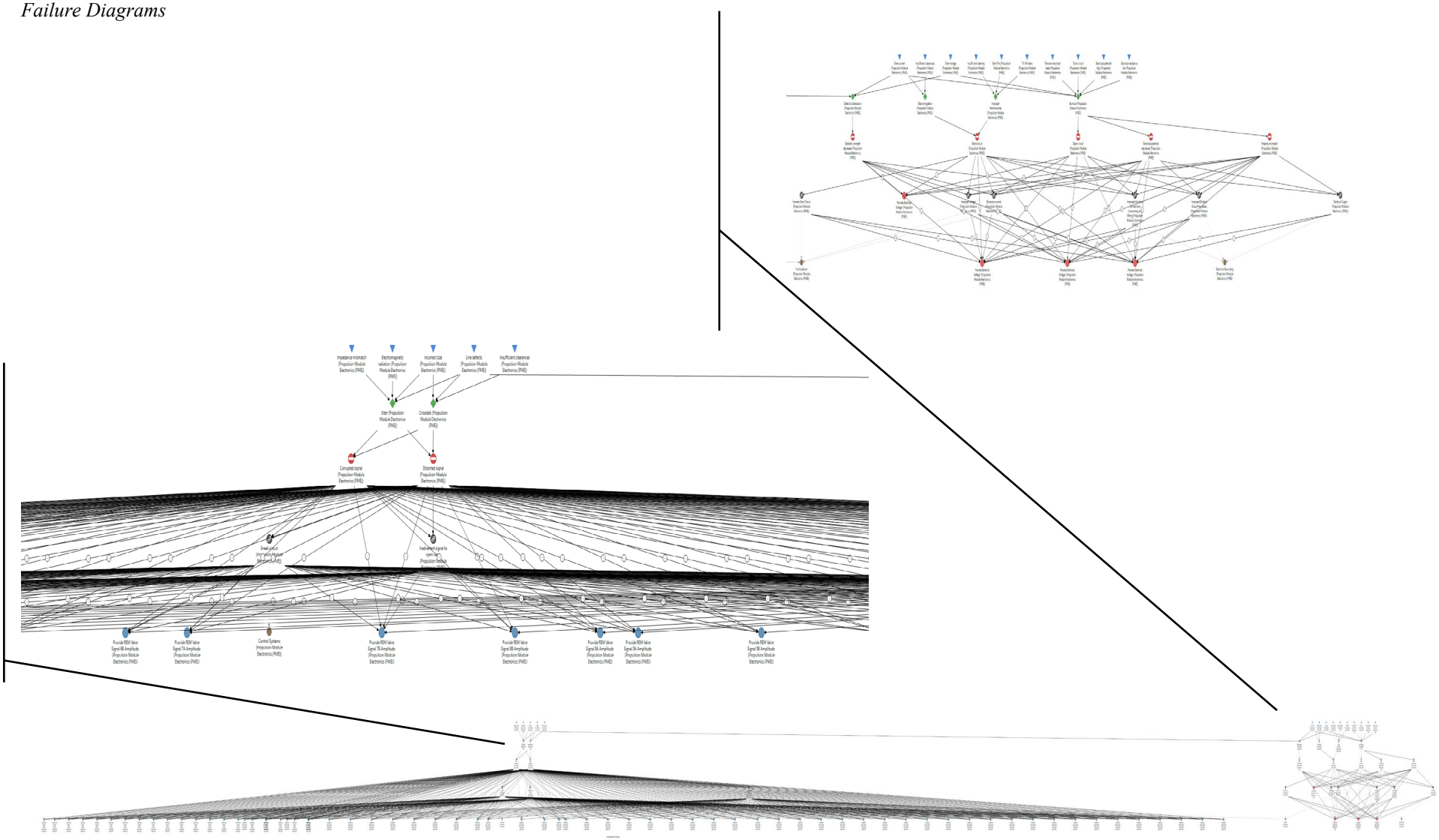


Figure A12: PME Failure Diagram

Diode Box (Failure space black box modeled only)

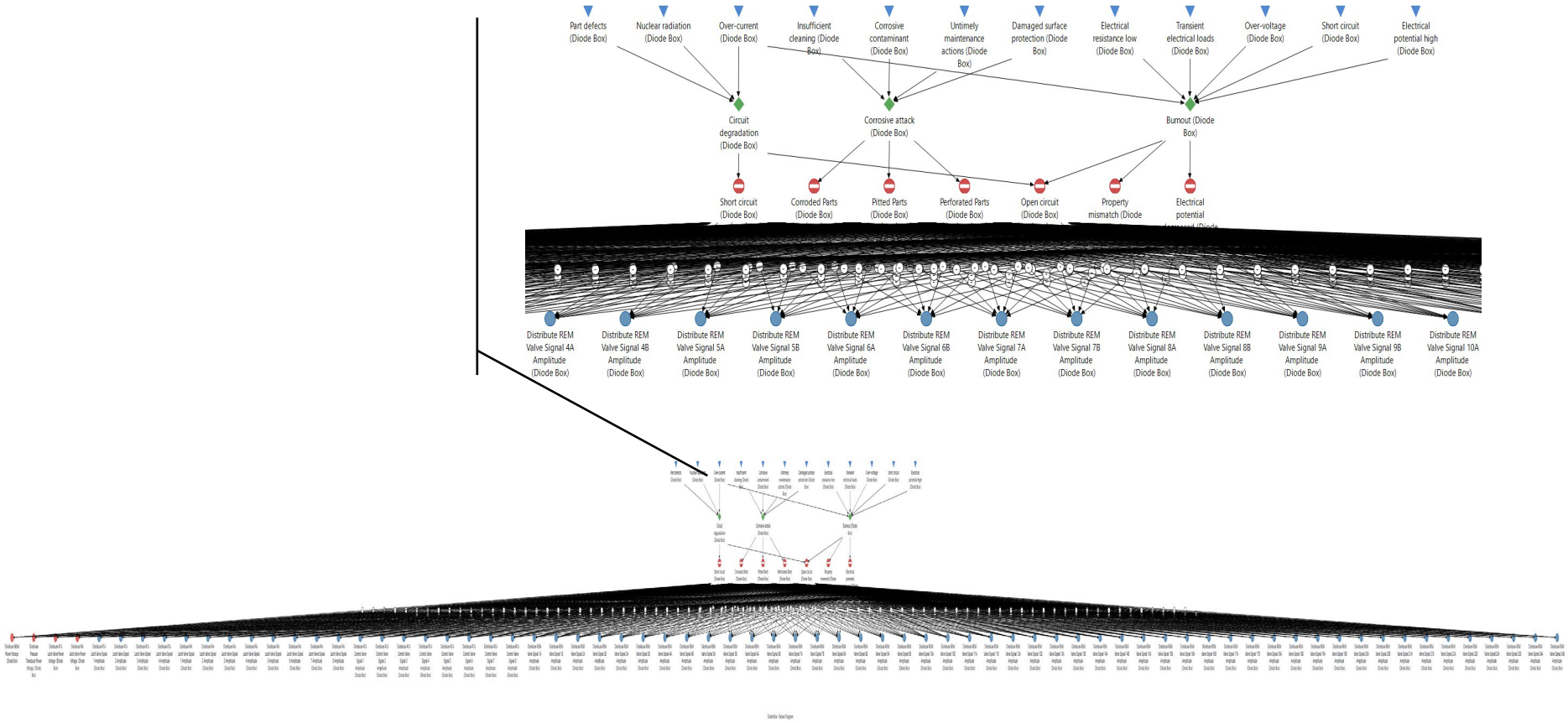


Figure A13: Diode Box Failure Diagram (with magnified partial view)

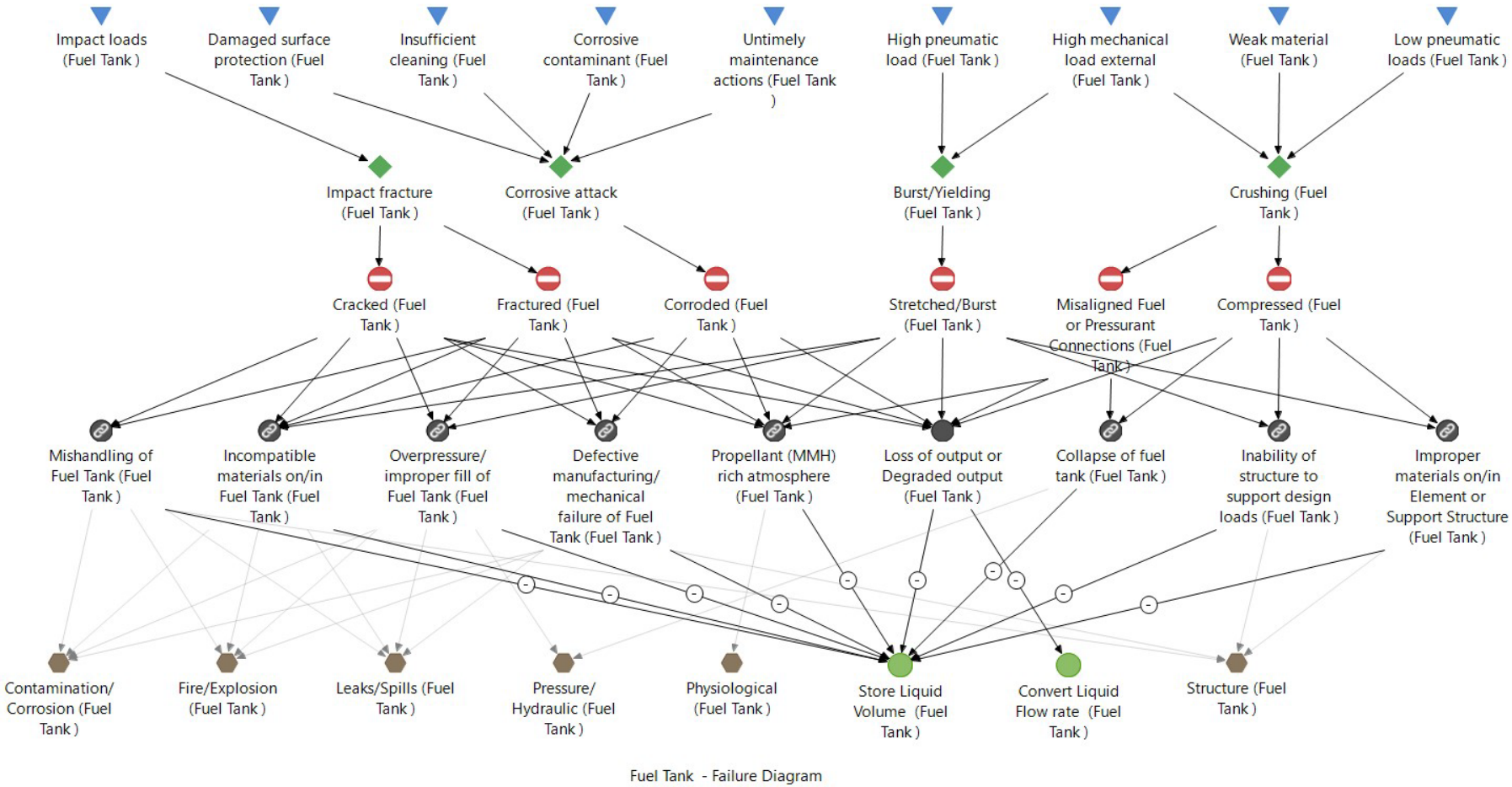


Figure A14: Fuel Tank Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Propellent Rich Atmosphere from Store Liquid to avoid erroneous or duplicative entries in reliability outputs)

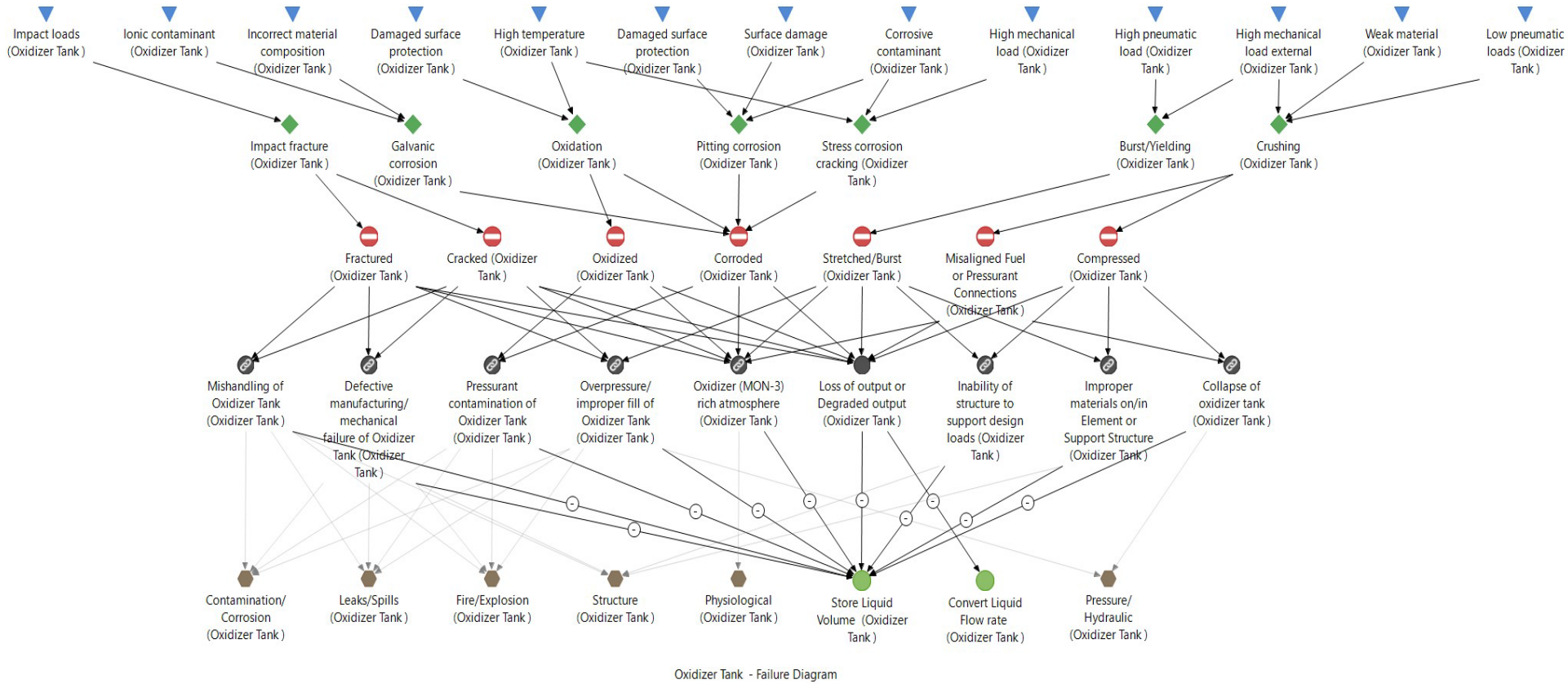


Figure A15: Oxidizer Tank Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Oxidizer Rich Atmosphere from Store Liquid to avoid erroneous or duplicative entries in reliability outputs)

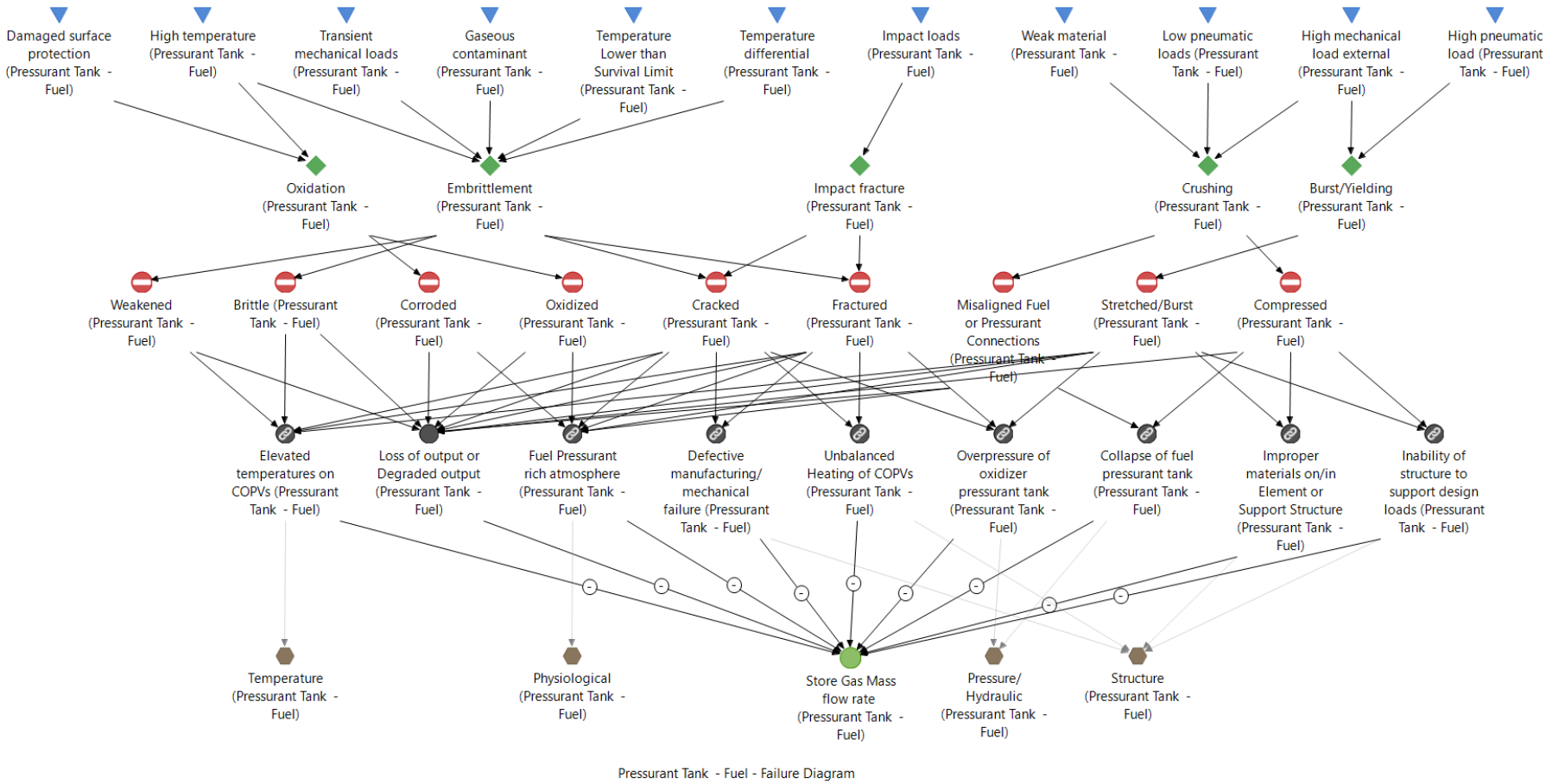


Figure A16: Fuel Pressurant Tank Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Fuel Pressurant Rich Atmosphere from Store Gas to avoid erroneous or duplicative entries in reliability outputs)

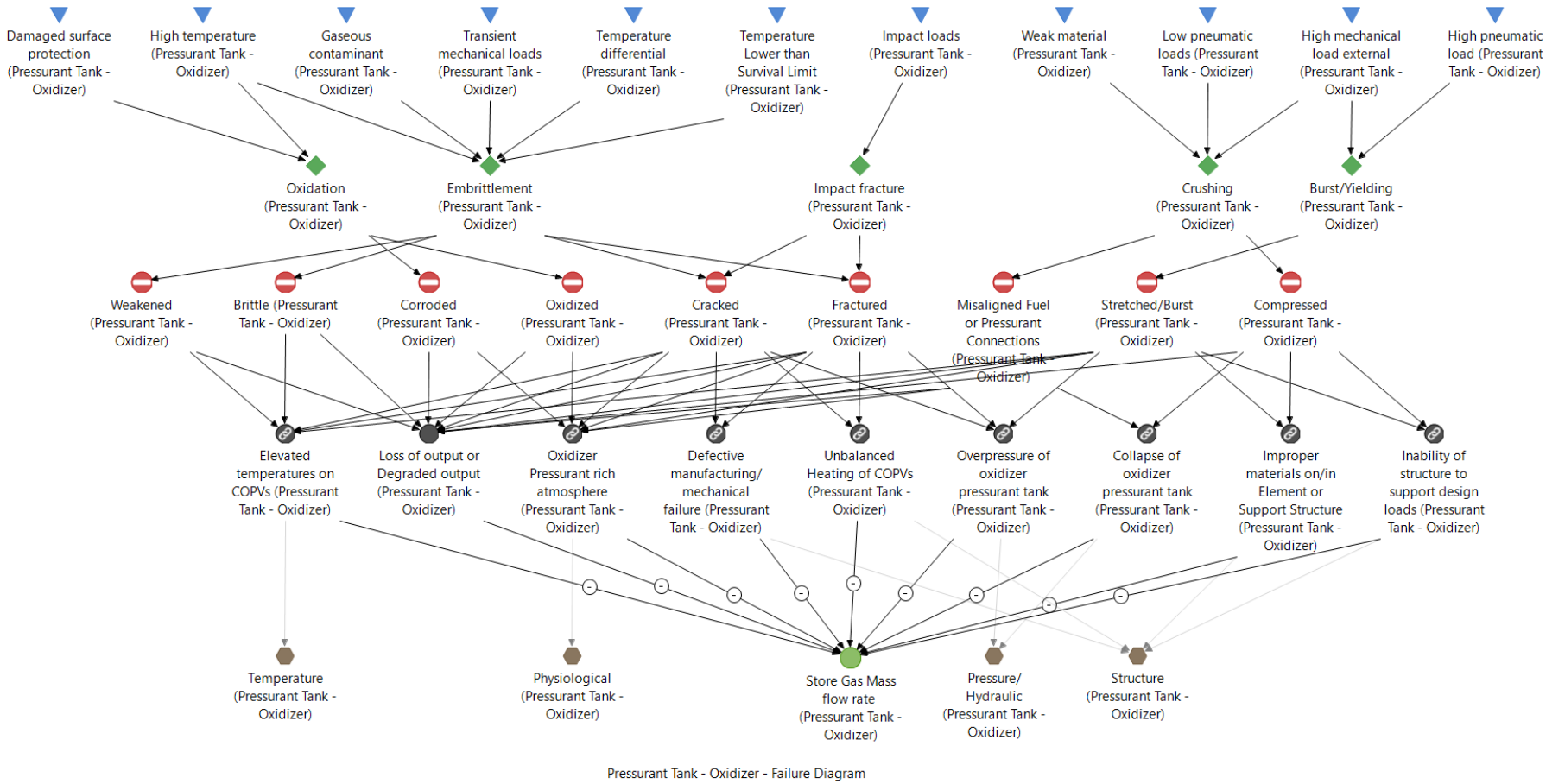


Figure A17: Oxidizer Pressurant Tank Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Oxidizer Pressurant Rich Atmosphere from Store Gas to avoid erroneous or duplicative entries in reliability outputs)

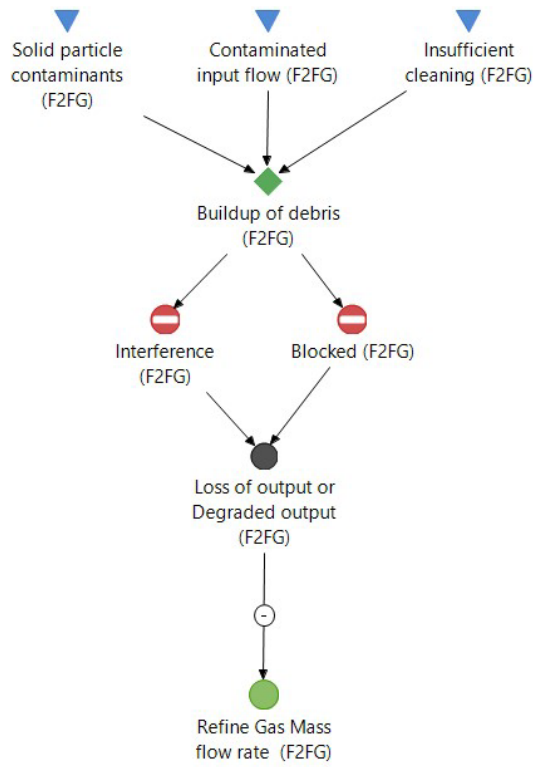


Figure A18: MADE EUROPA PCA – Fuel - F2FG Failure Diagram

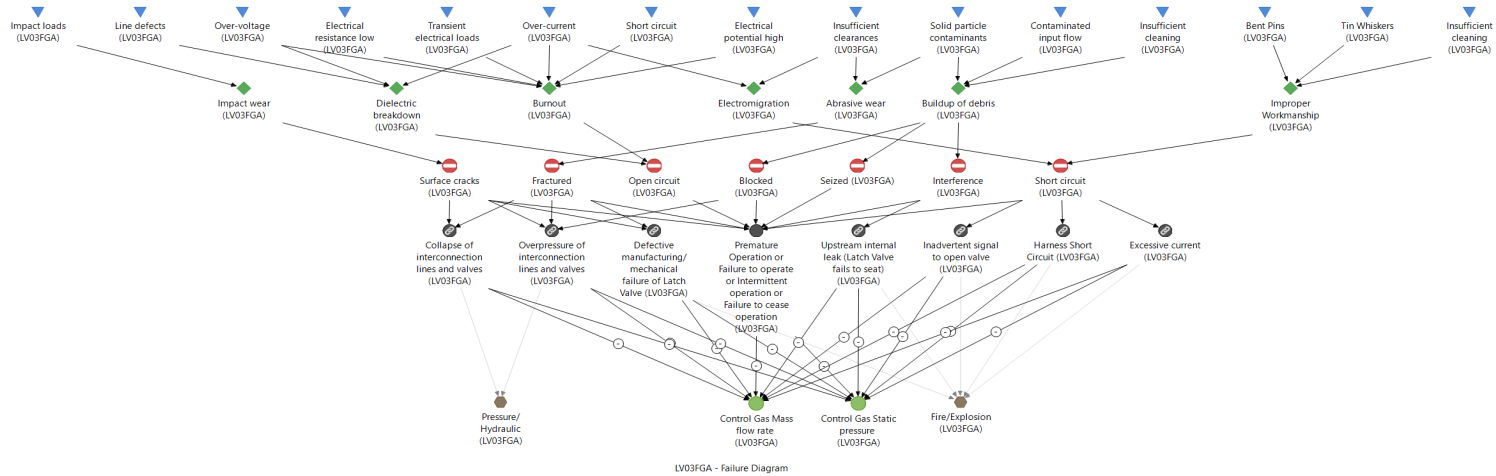


Figure A19: MADE EUROPA PCA – Fuel-LV03FGA Failure Diagram

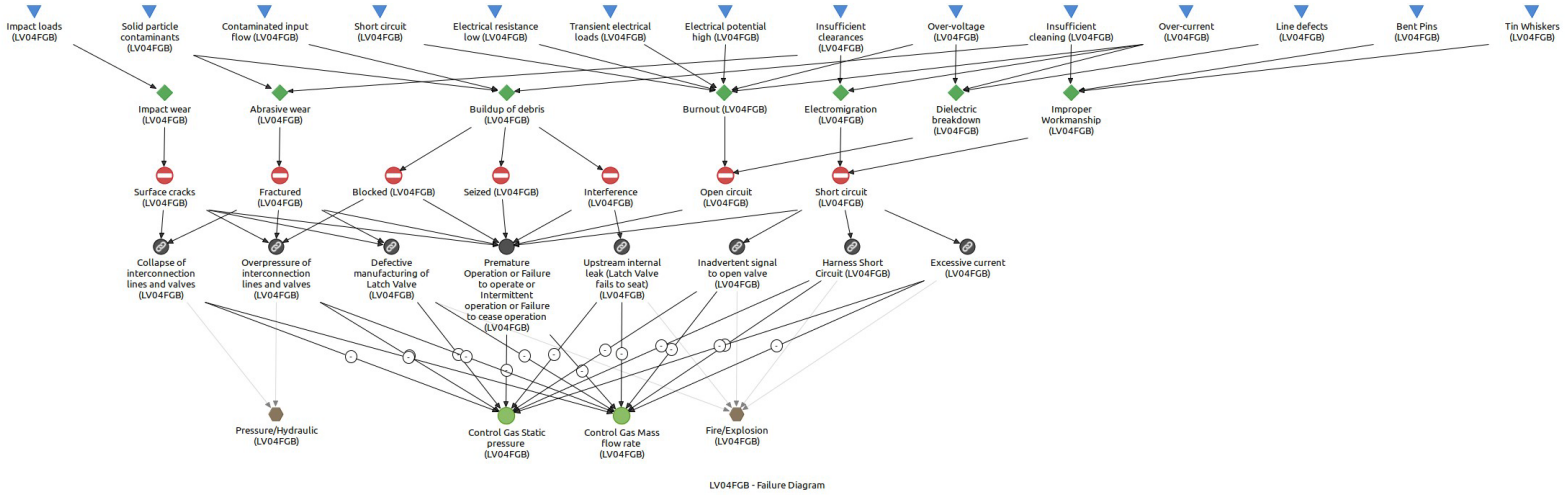


Figure A20: MADE EUROPA PCA – Fuel-LV04FGA Failure Diagram

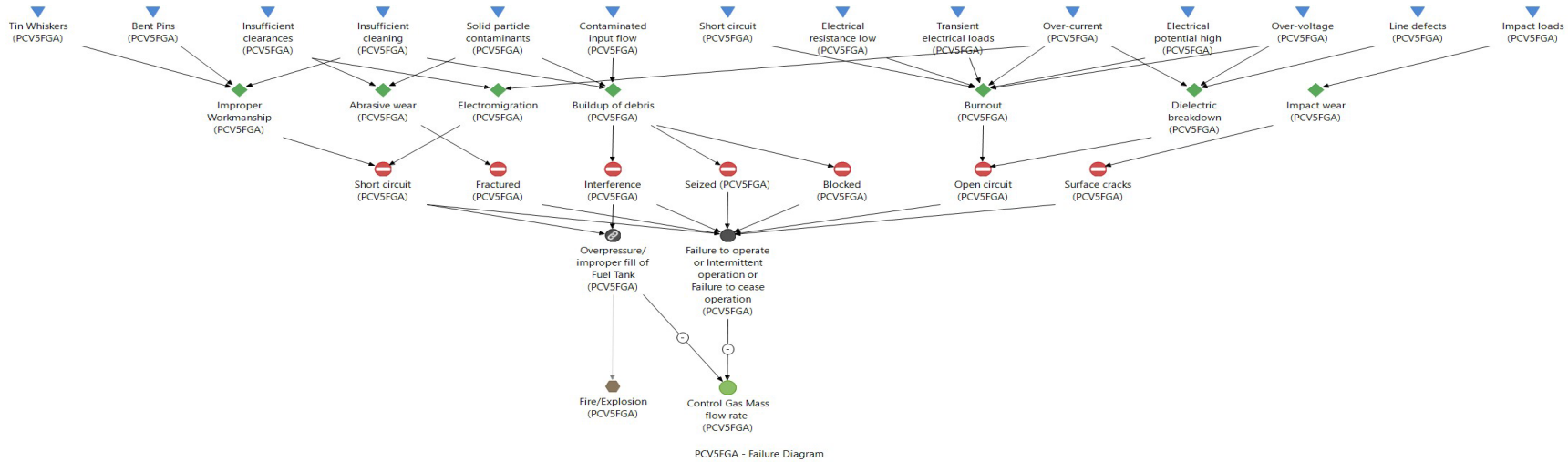


Figure A21: MADE EUROPA PCA – Fuel-PCV5FGA Failure Diagram

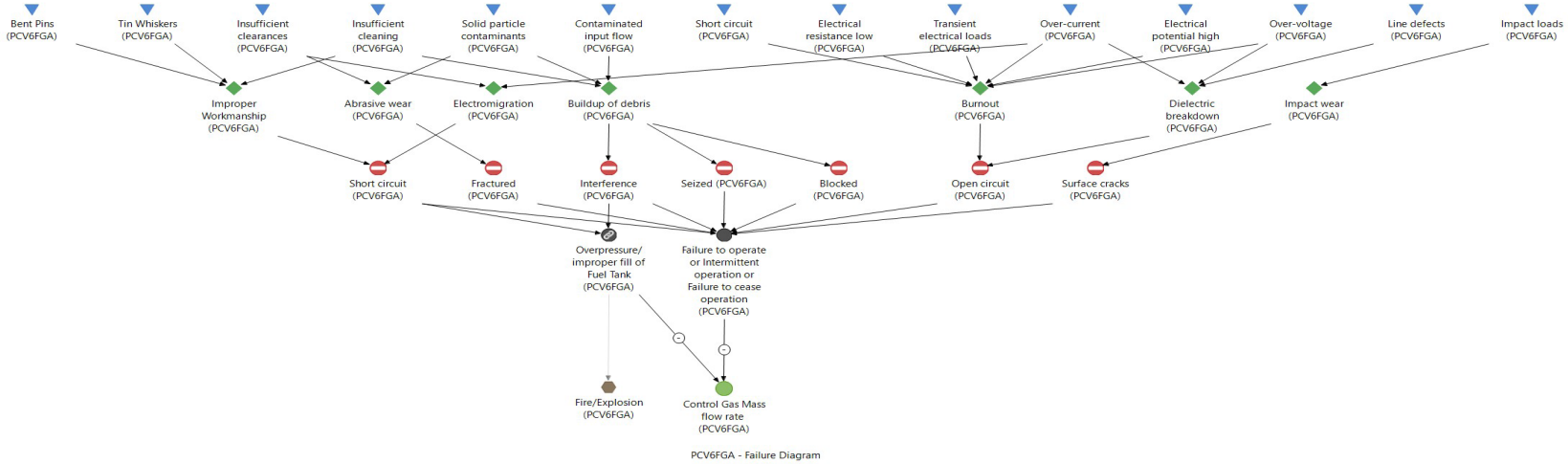


Figure A22: MADE EUROPA PCA – Fuel-PCV6FGA Failure Diagram

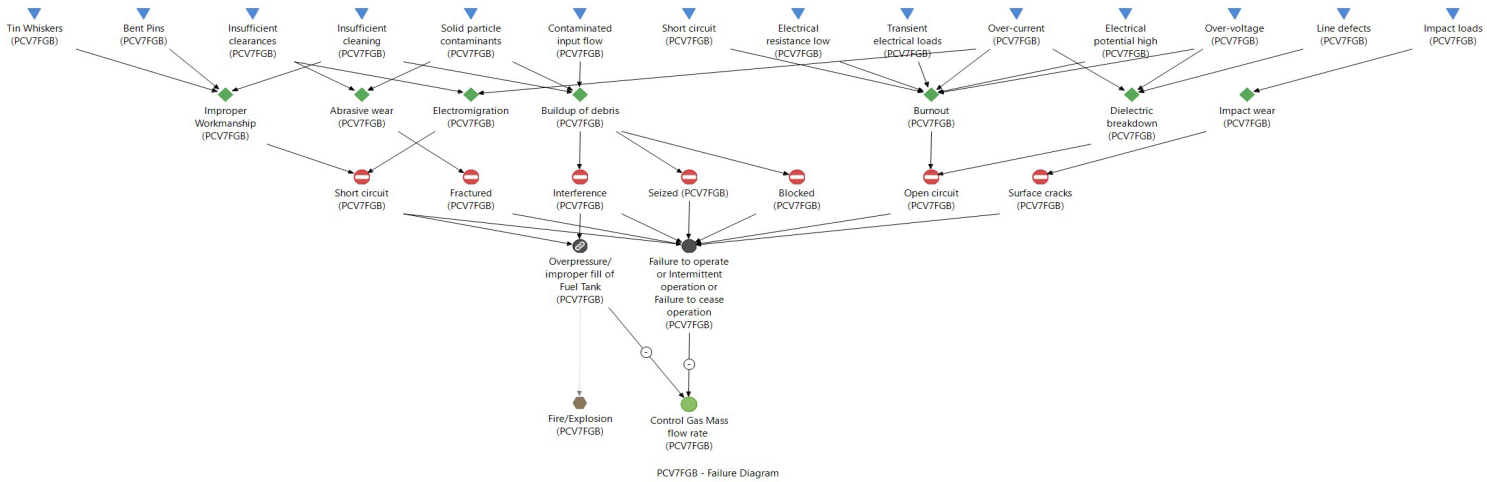


Figure A23: MADE EUROPA PCA – Fuel-PCV7FGA Failure Diagram

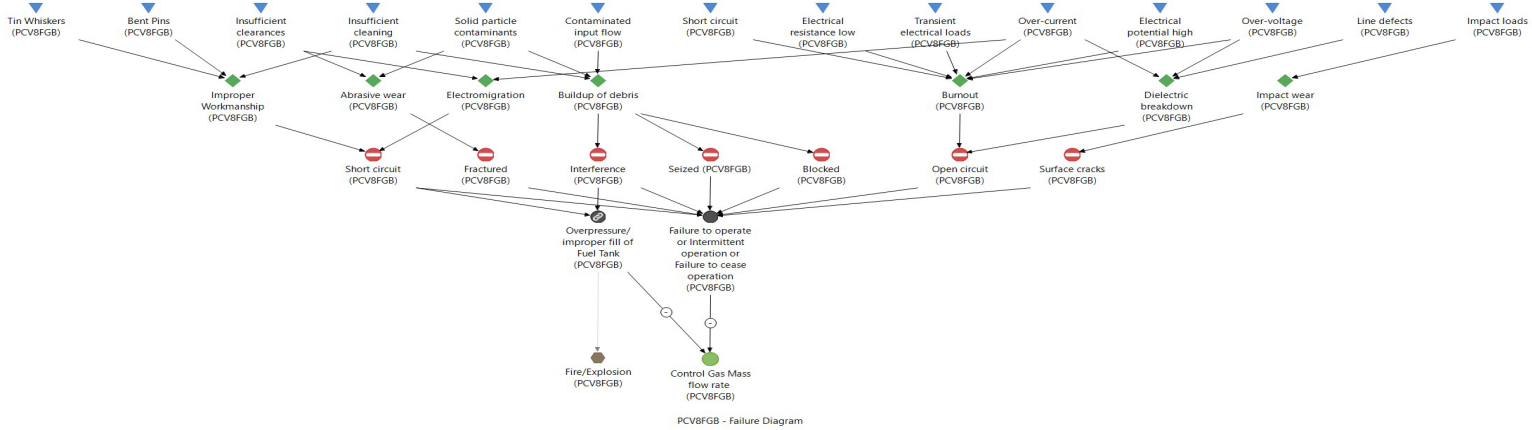


Figure A24: MADE EUROPA PCA – Fuel-PCV8FGA Failure Diagram

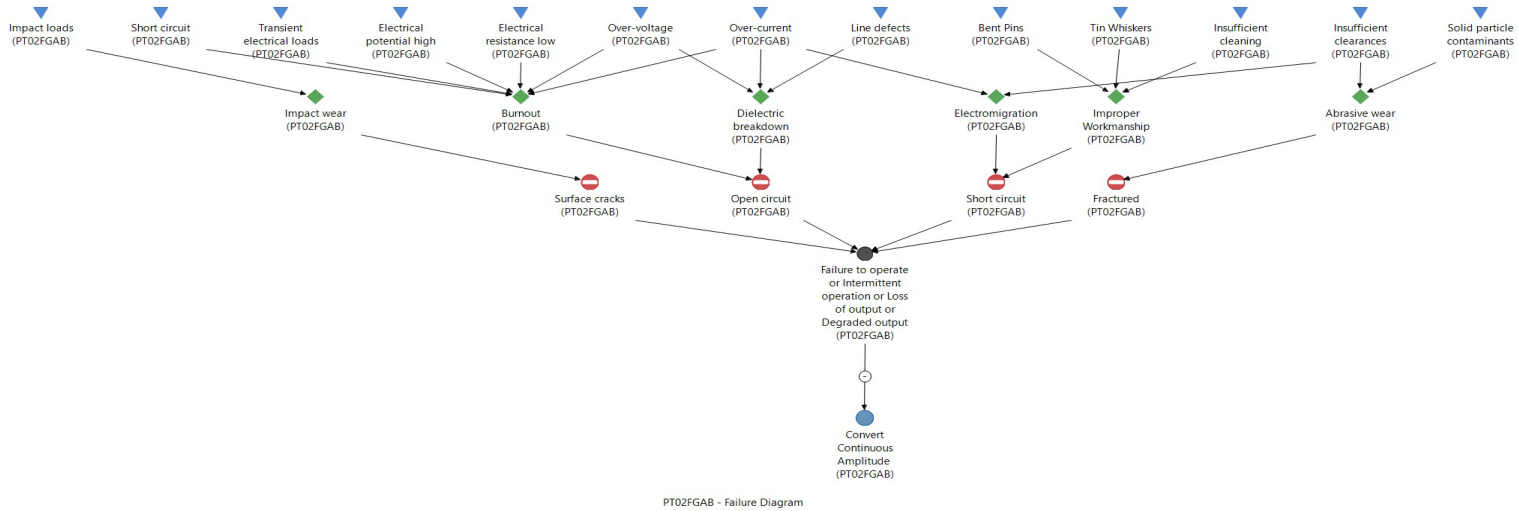


Figure A25: MADE EUROPA PCA – Fuel-PT02FGAB Failure Diagram

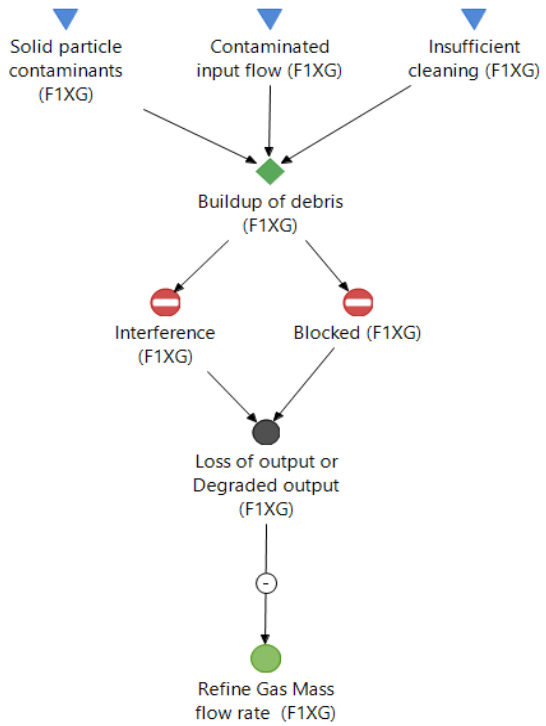


Figure A26: MADE EUROPA PCA – Oxidizer-F1XG Failure Diagram

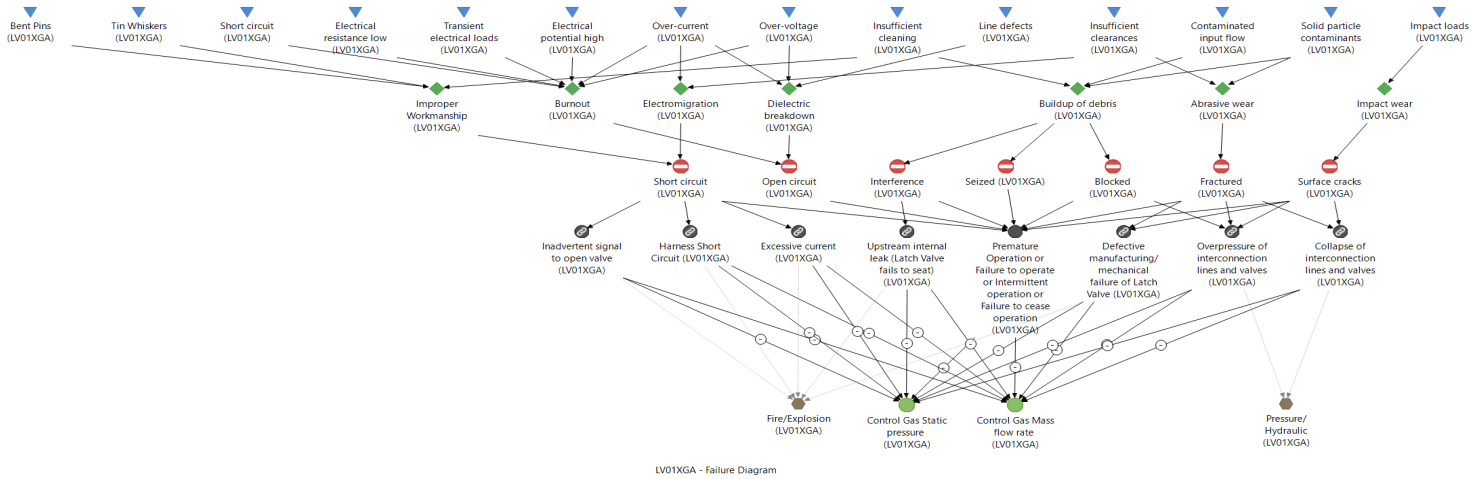


Figure A27: MADE EUROPA PCA – Oxidizer-LV01XGA Failure Diagram

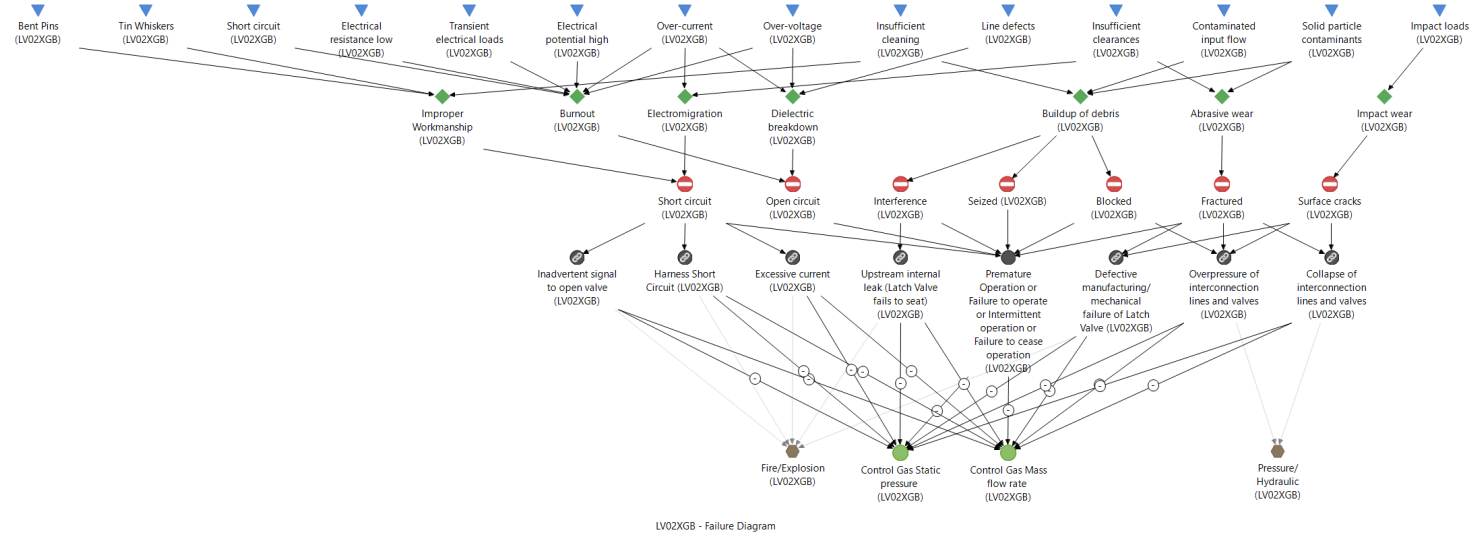


Figure A28: MADE EUROPA PCA – Oxidizer-LV02XGA Failure Diagram

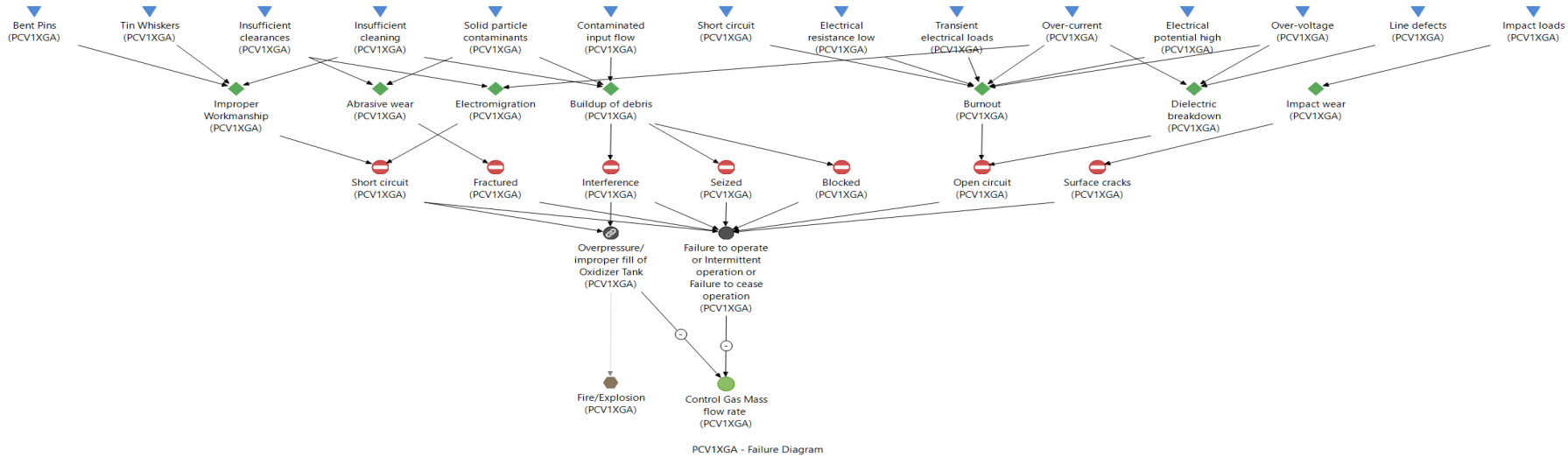


Figure A29: MADE EUROPA PCA – Oxidizer-PCV1XGA Failure Diagram

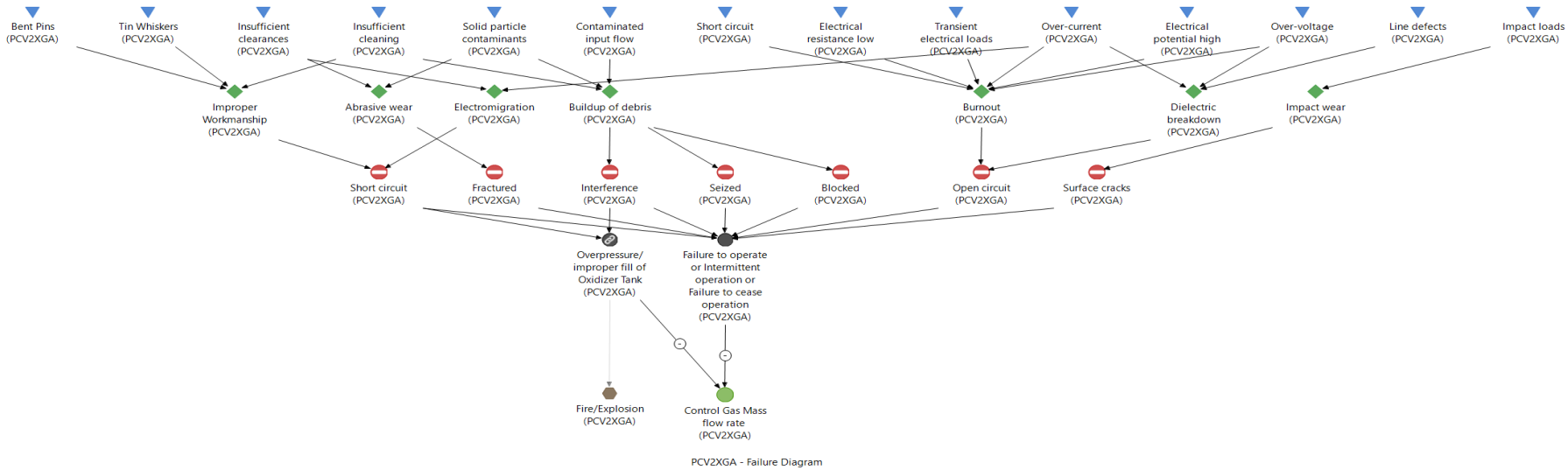


Figure A30: MADE EUROPA PCA – Oxidizer-PCV2XGA Failure Diagram

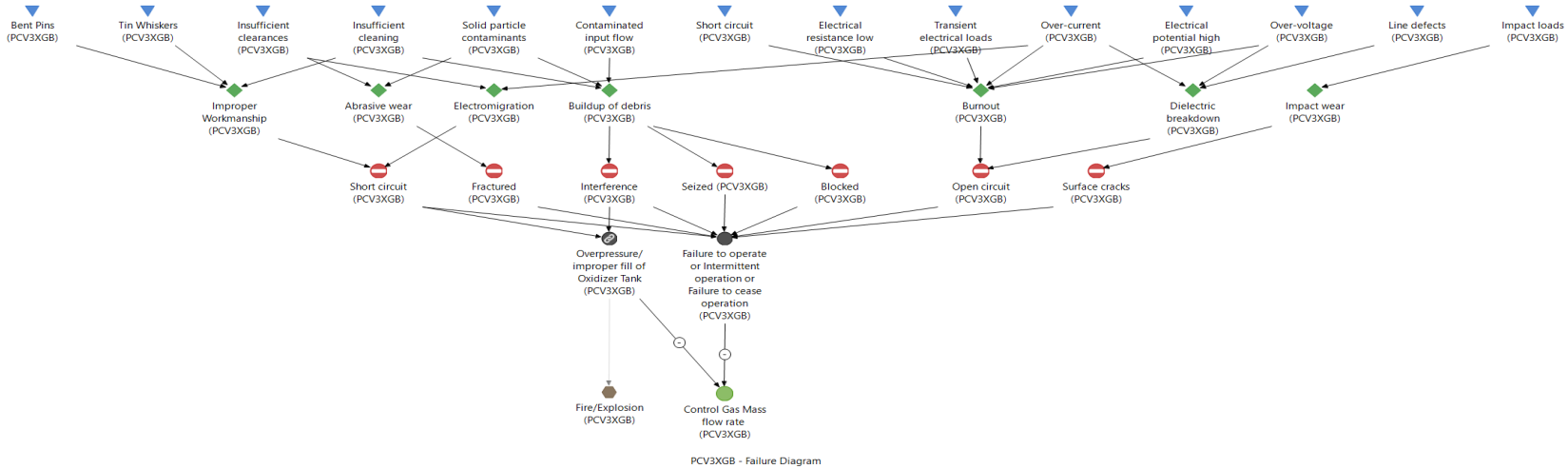


Figure A31: MADE EUROPA PCA – Oxidizer-PCV3XGB Failure Diagram

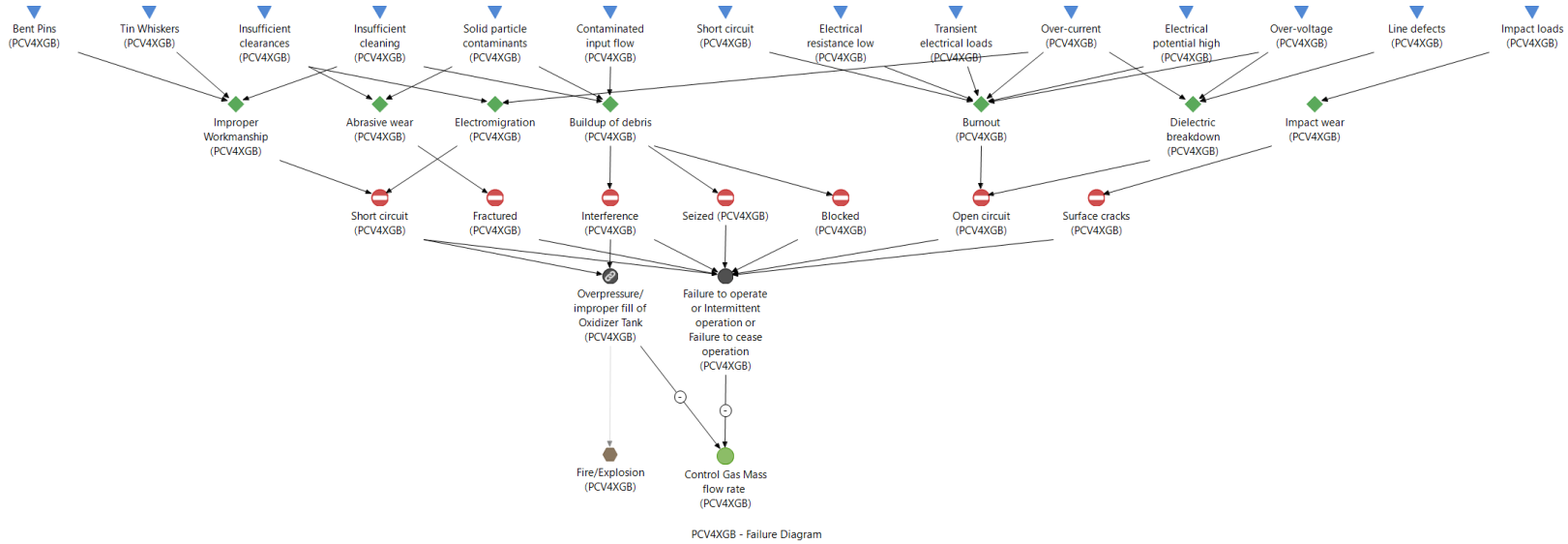


Figure A32: MADE EUROPA PCA – Oxidizer-PCV4XGB Failure Diagram

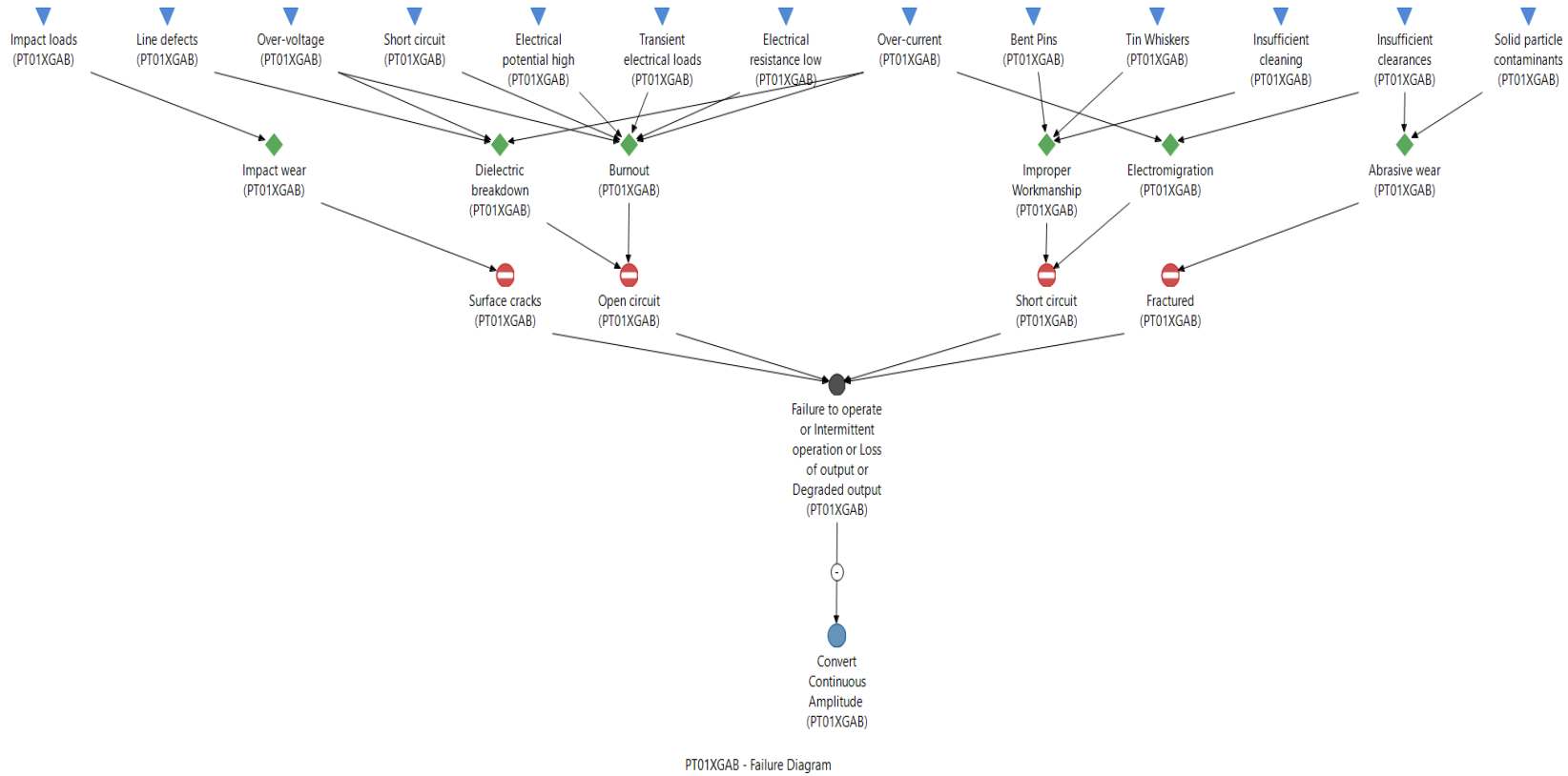


Figure A33: MADE EUROPA PCA – Oxidizer-PT01XGAB Failure Diagram

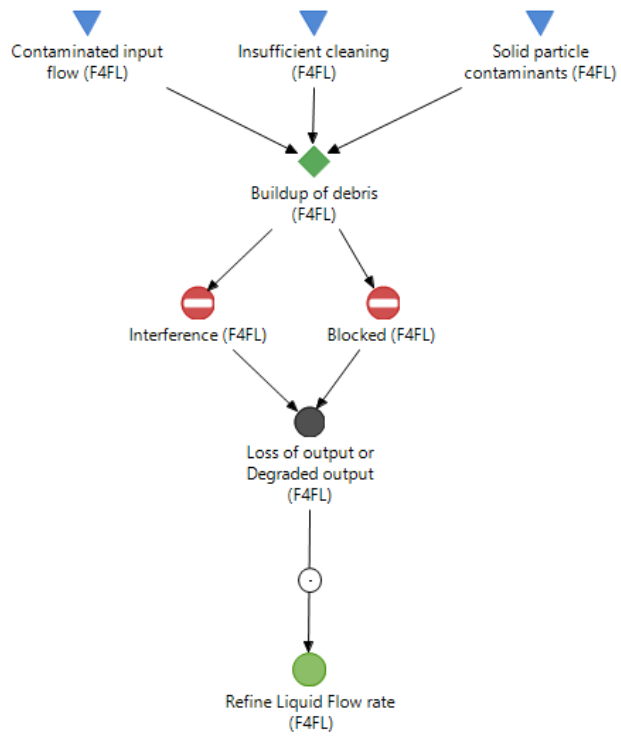


Figure A34: MADE EUROPA PIA – Fuel – F4FL Failure Diagram

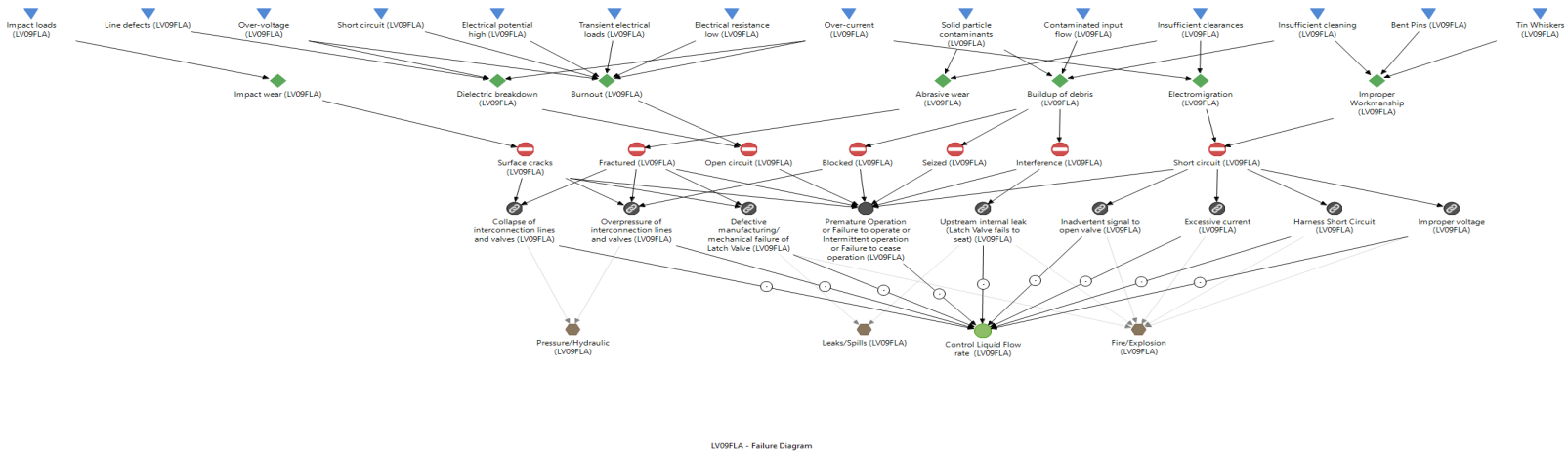


Figure A35: MADE EUROPA PIA – Fuel – LV09FLA Failure Diagram

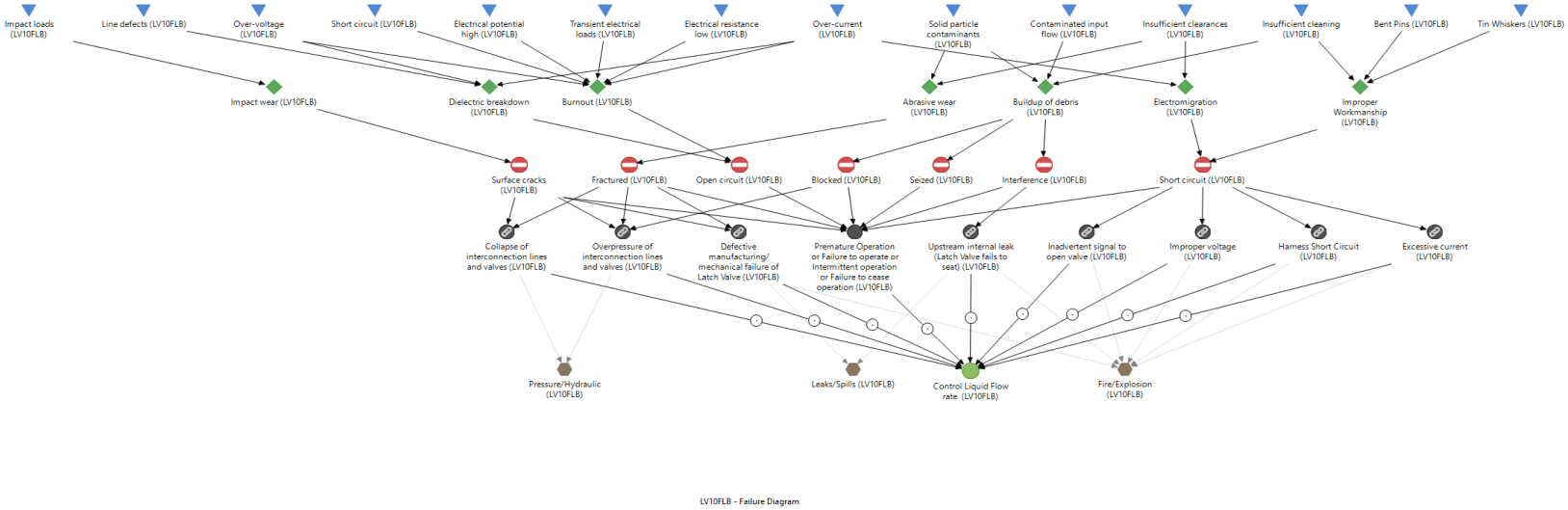


Figure A36: MADE EUROPA PIA – Fuel – LV10FLB Failure Diagram

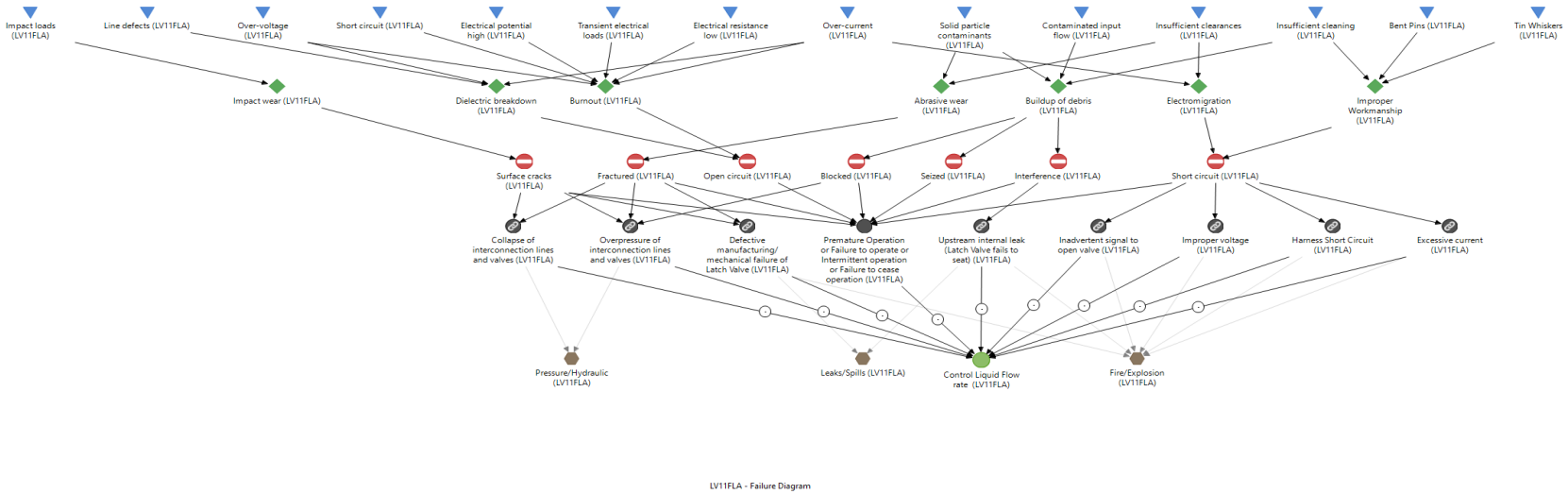


Figure A37: MADE EUROPA PIA – Fuel – LV11FLA Failure Diagram

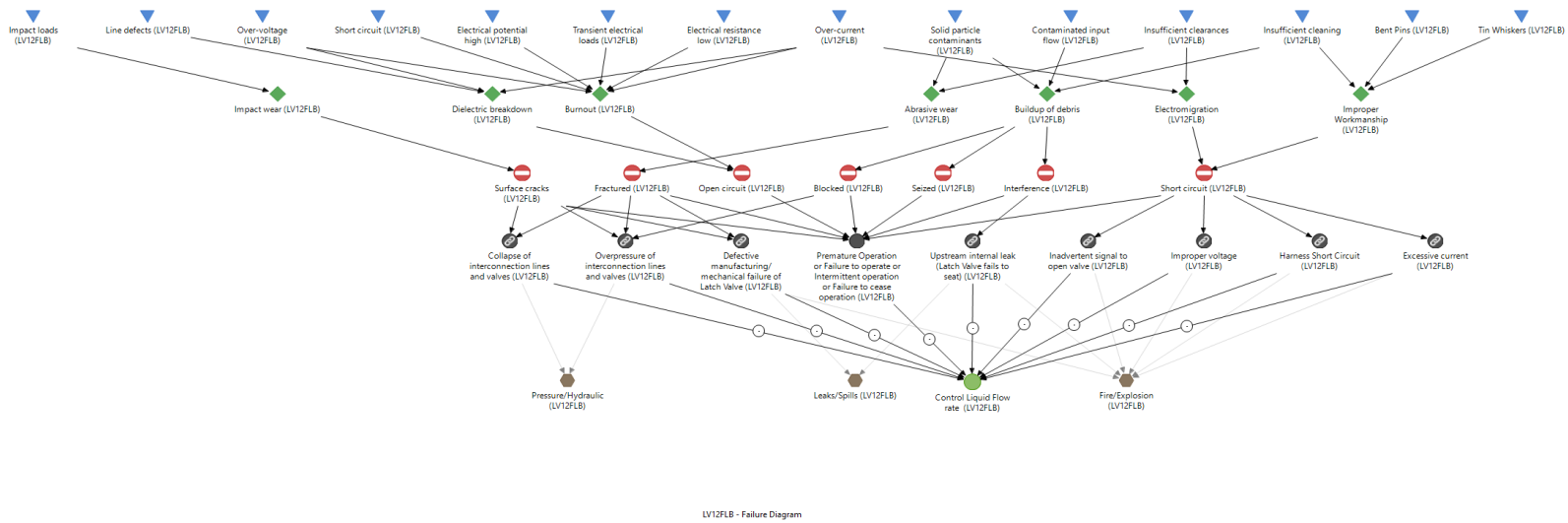


Figure A38: MADE EUROPA PIA – Fuel – LV12FLB Failure Diagram

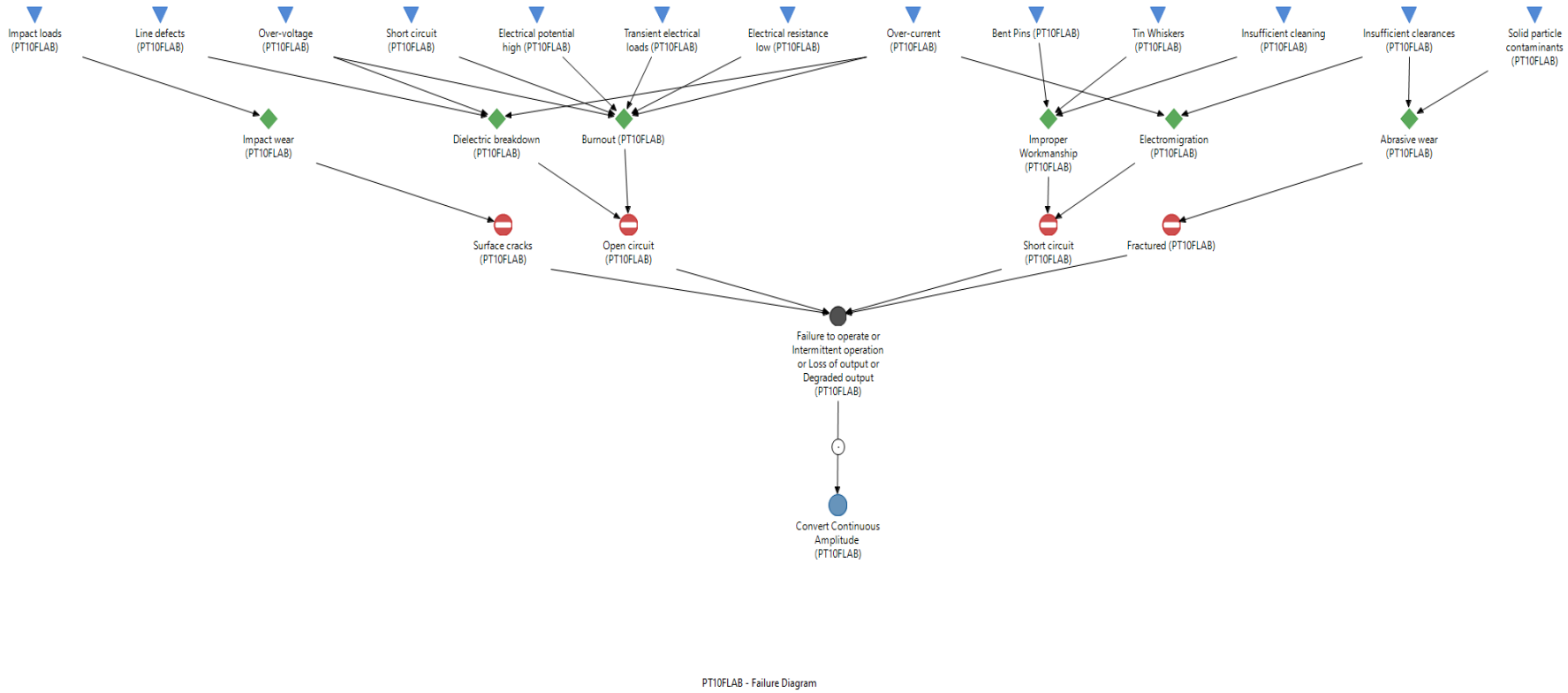


Figure A39: MADE EUROPA PIA – Fuel – PT10FLAB Failure Diagram

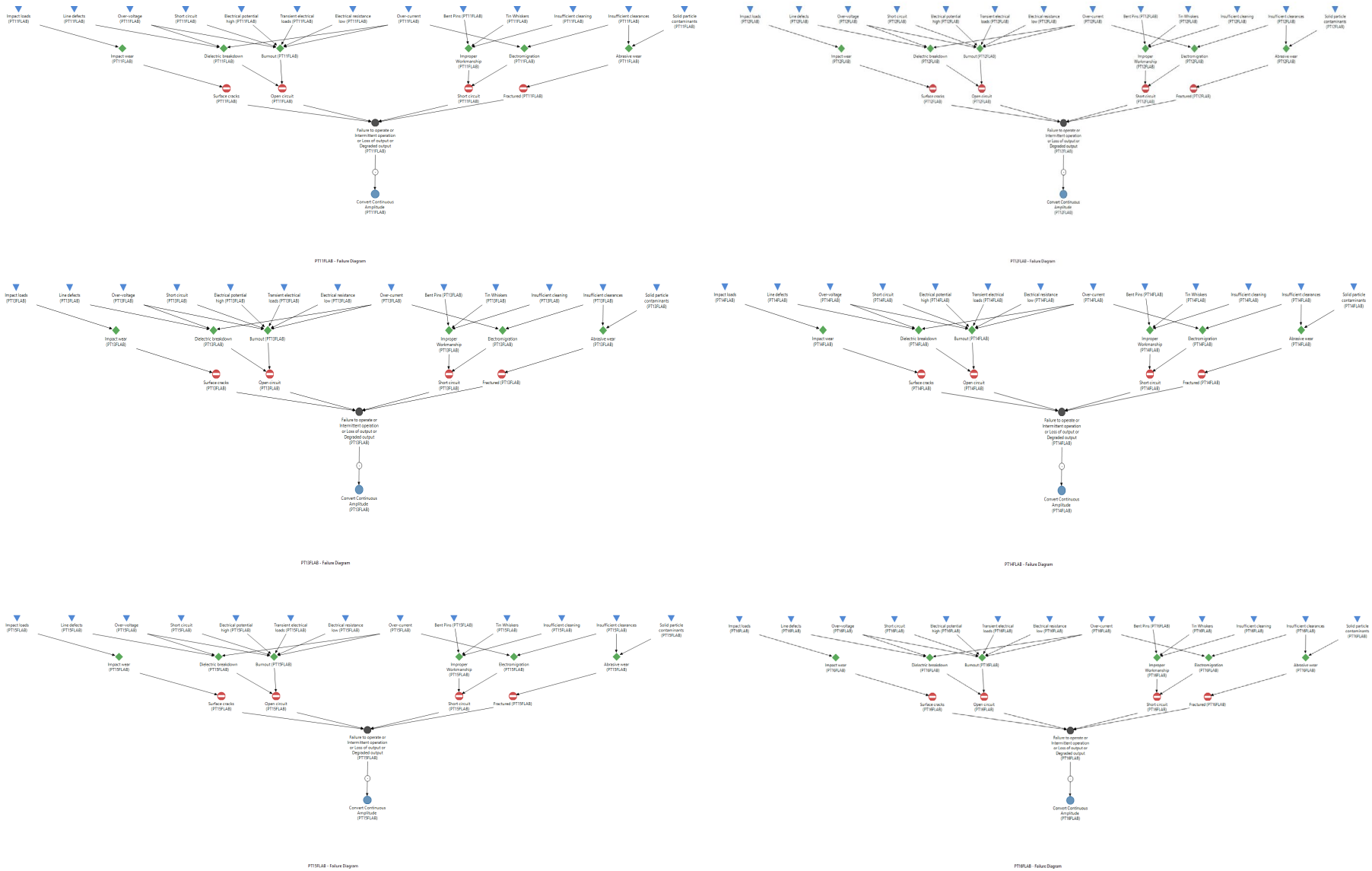


Figure A40: MADE EUROPA PIA – Fuel – PT11FLAB-PT16FLAB Failure Diagram

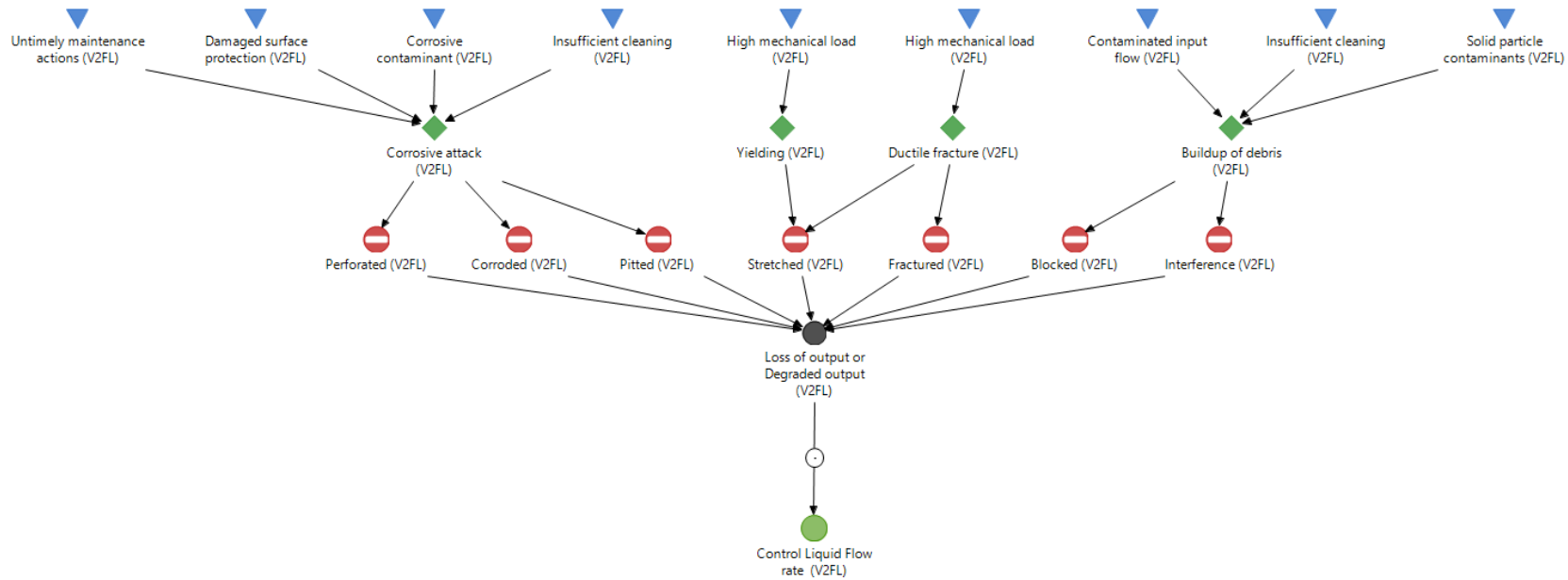


Figure A41: MADE EUROPA PIA – Fuel – V2FL Failure Diagram

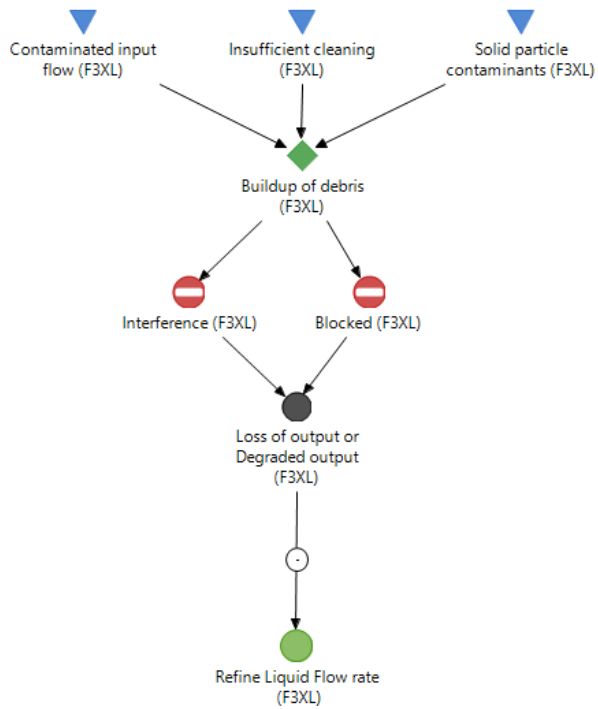


Figure A42: MADE EUROPA PIA – Oxidizer – F3XL

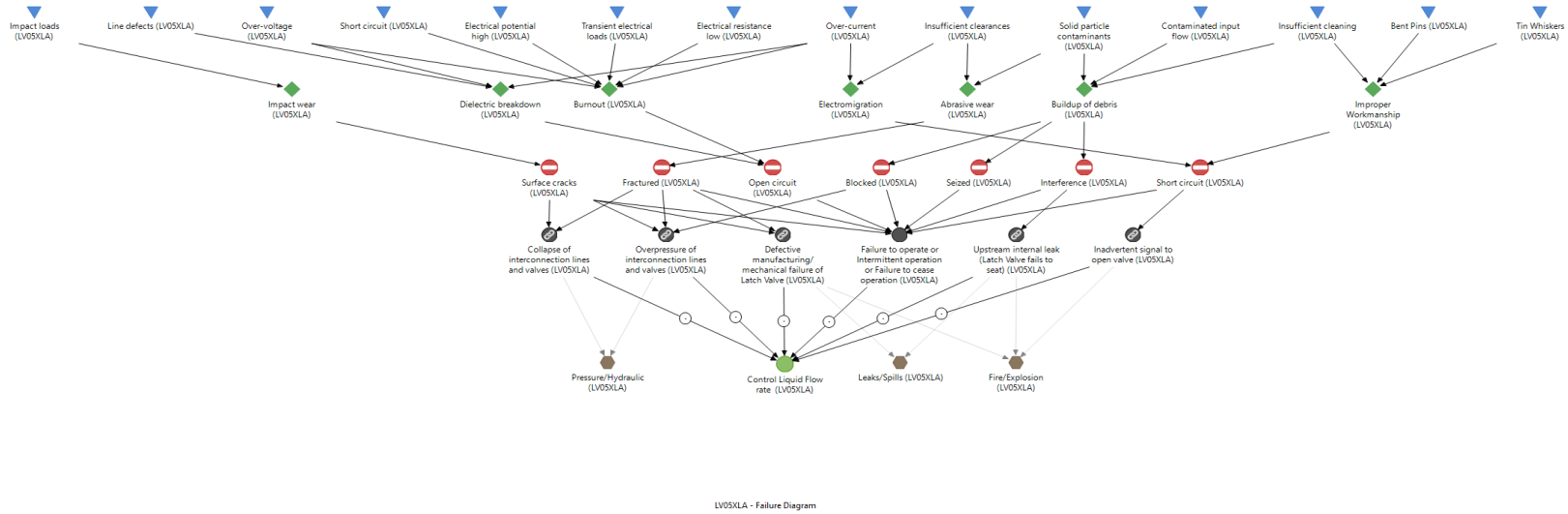


Figure A43: MADE EUROPA PIA – Oxidizer – LV05XLA

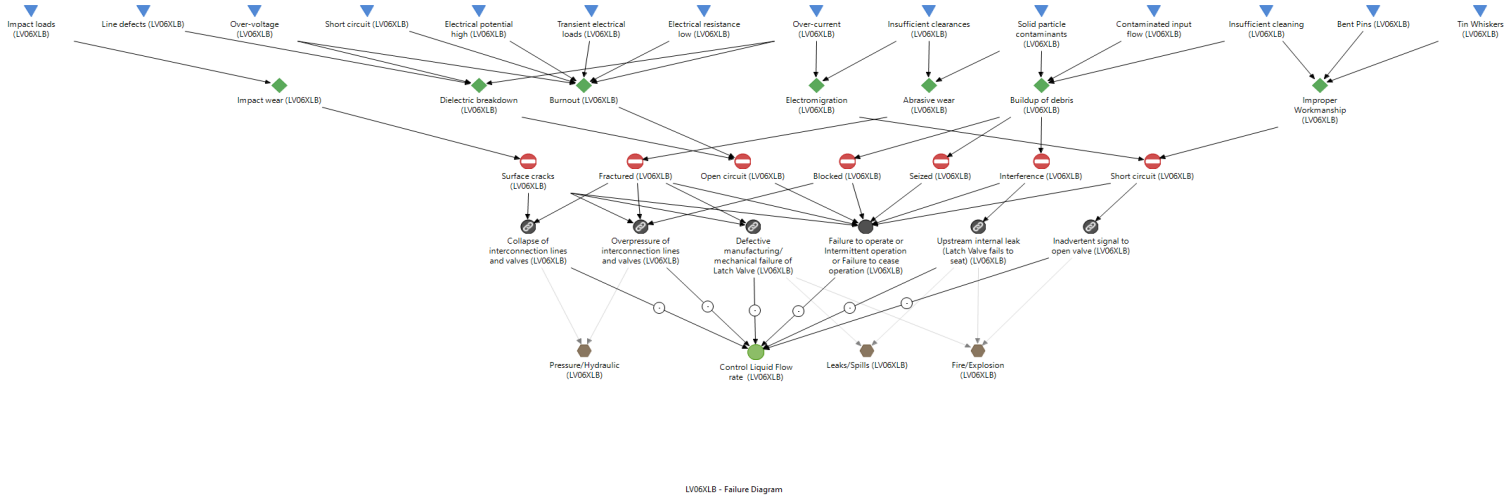


Figure A44: MADE EUROPA PIA – Oxidizer – LV06XLB

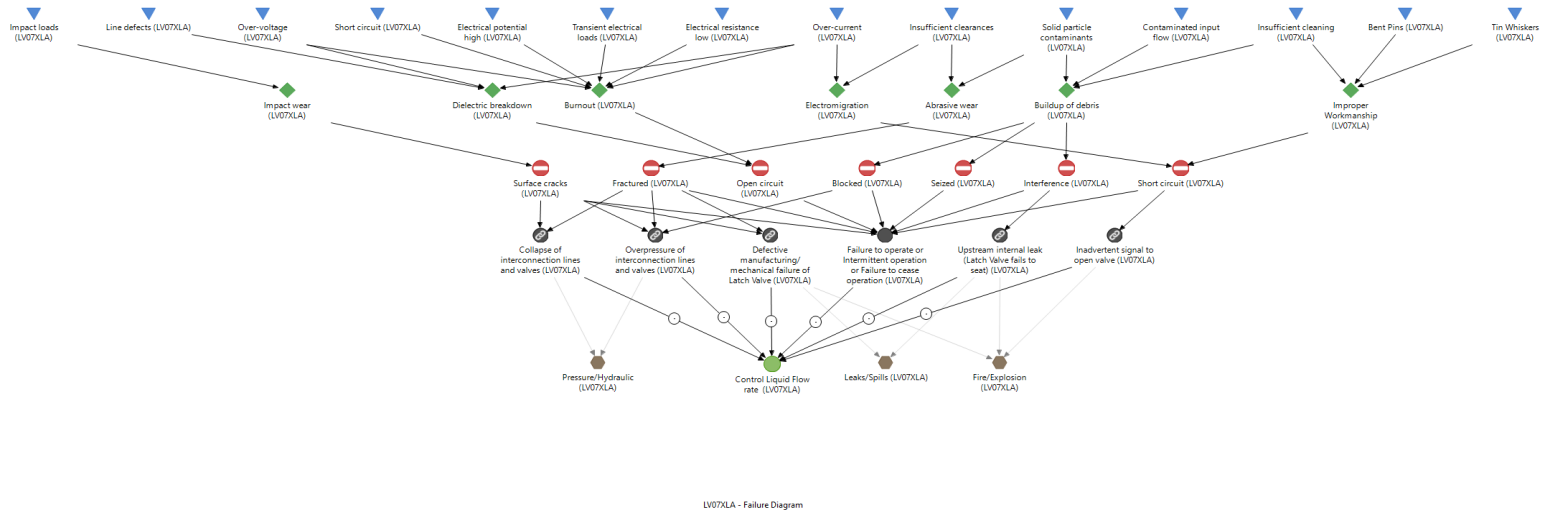


Figure A45: MADE EUROPA PIA – Oxidizer – LV07XLA

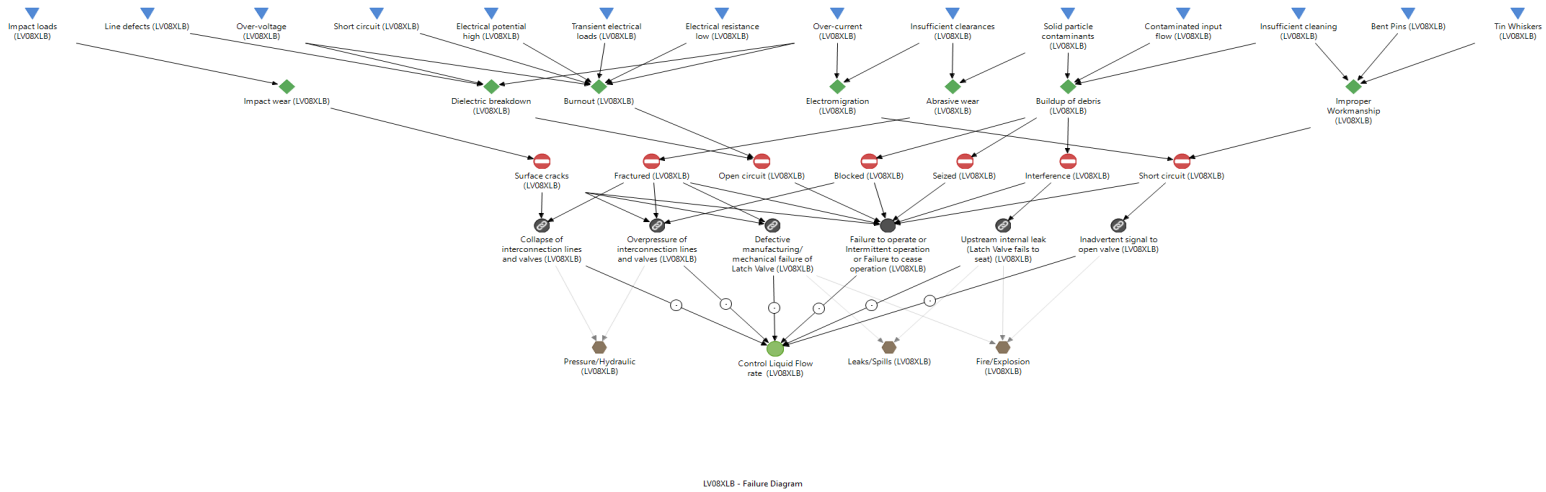


Figure A46: MADE EUROPA PIA – Oxidizer – LV08XLB

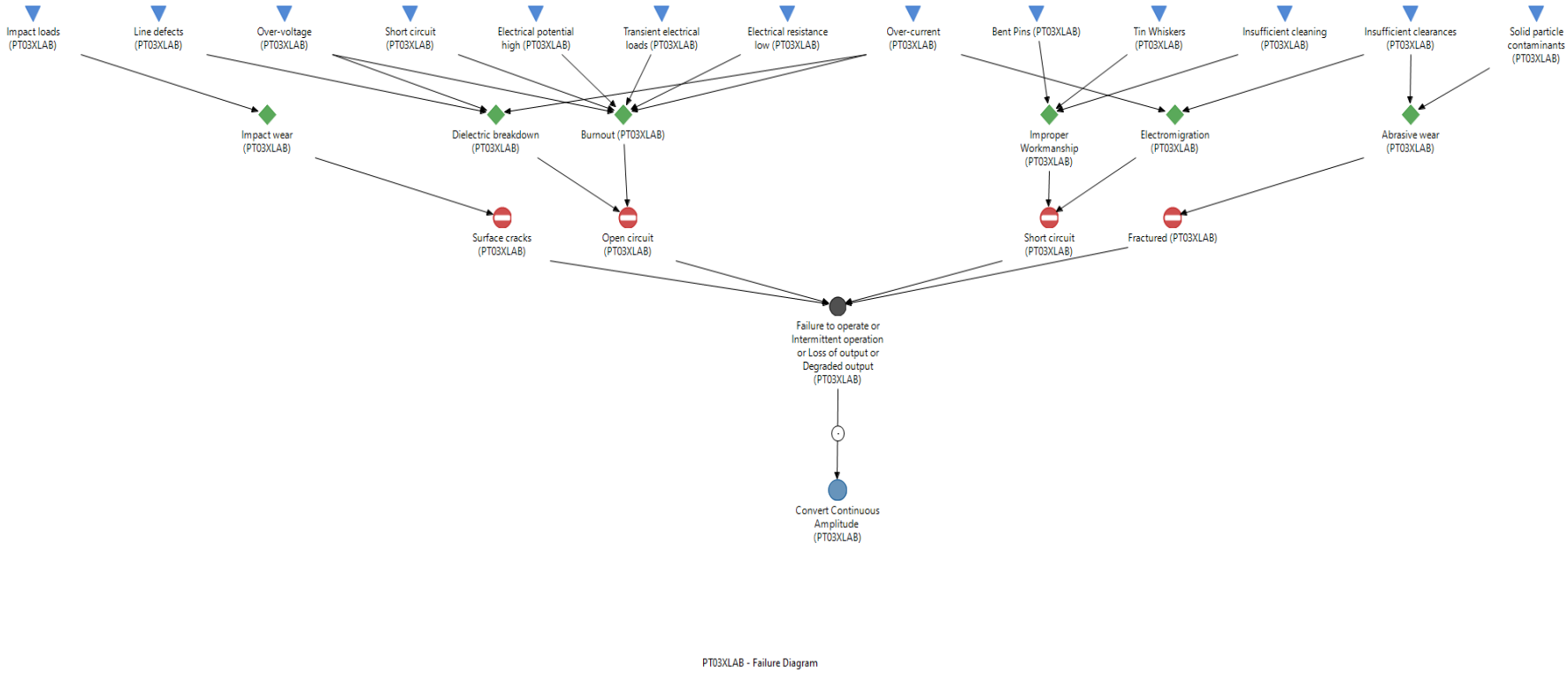


Figure A47: MADE EUROPA PIA – Oxidizer – PT03XLAB

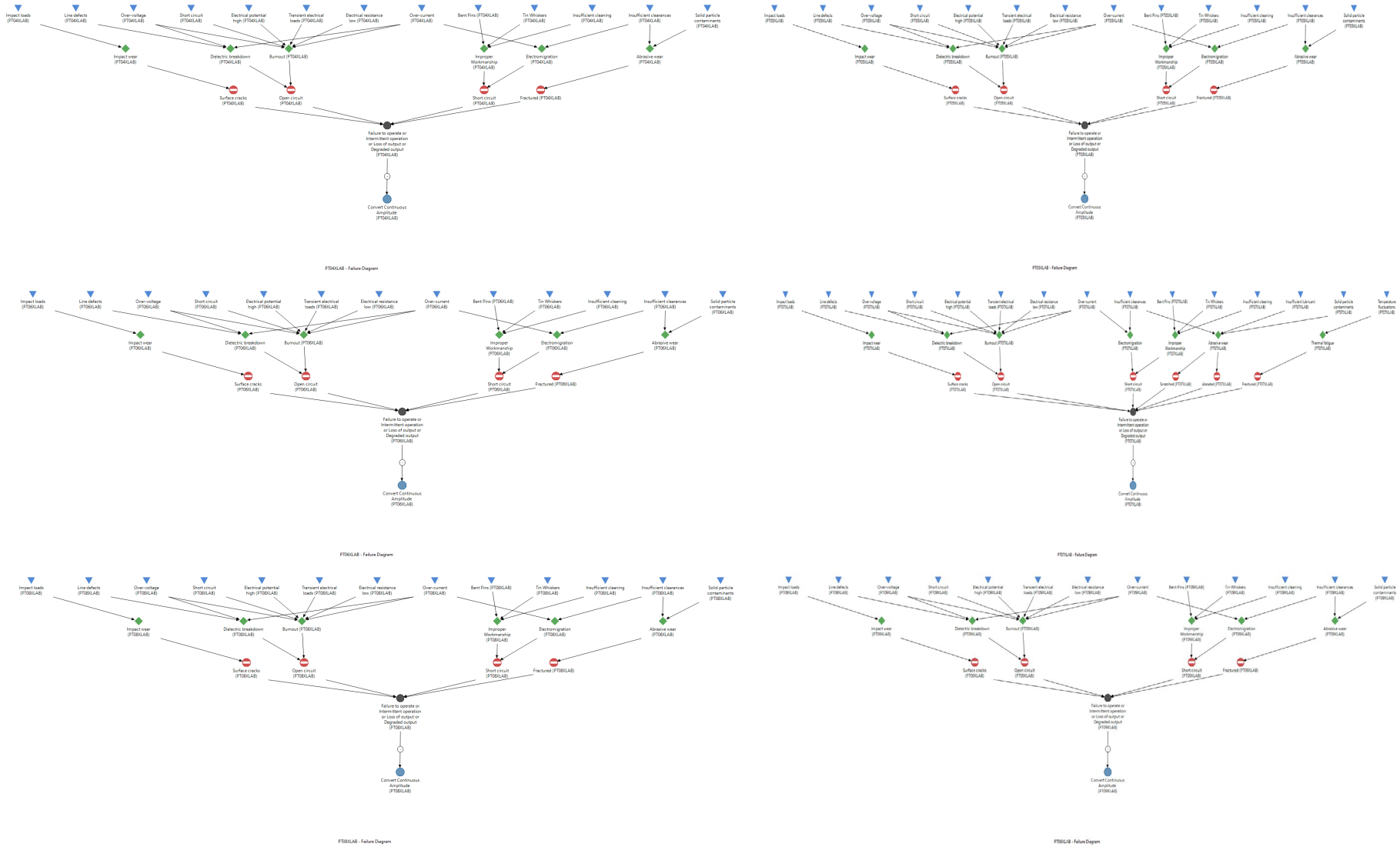


Figure A48: MADE EUROPA PIA – Oxidizer – PT04XLAB-PT09XLAB Failure Diagram

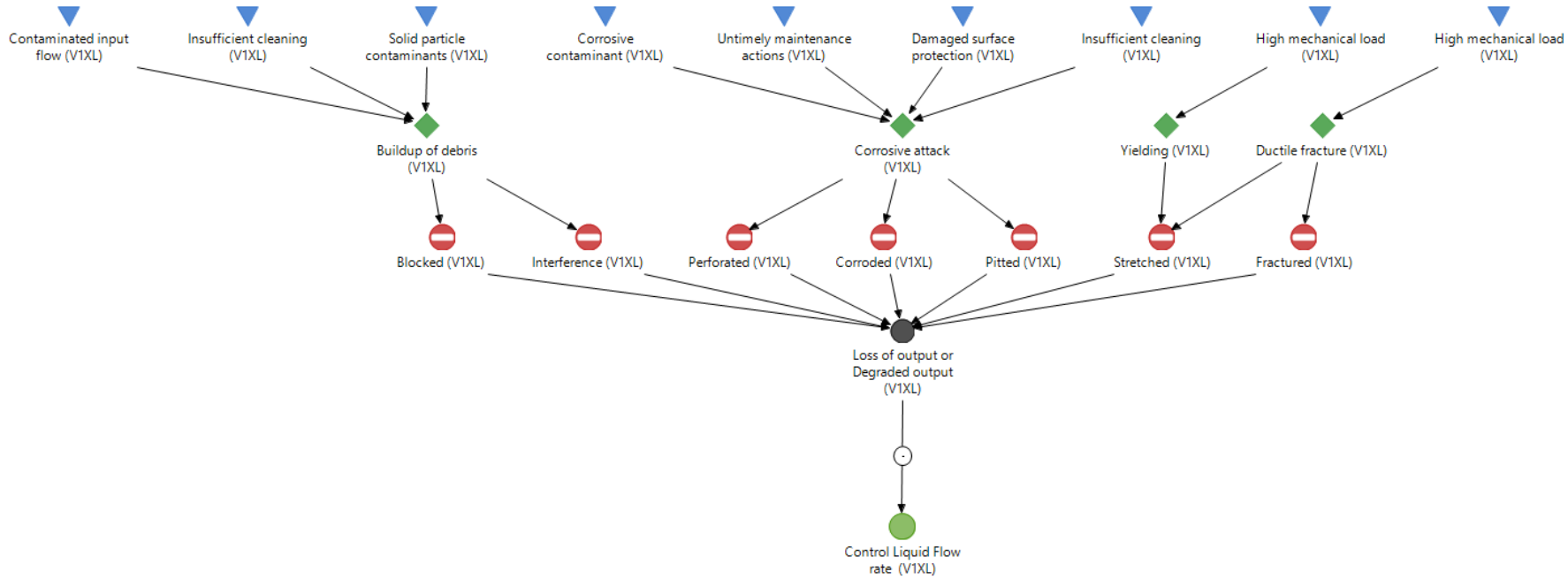


Figure A49: MADE EUROPA PIA – Oxidizer – V1XL Failure Diagram

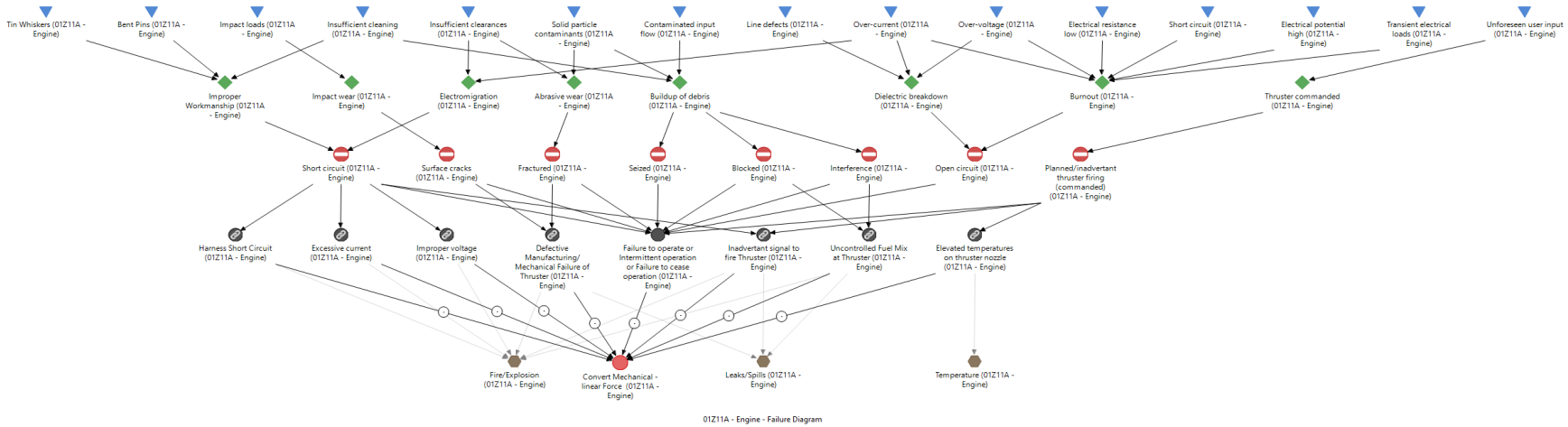


Figure A50: MADE EUROPA REM-1(01Z11A Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

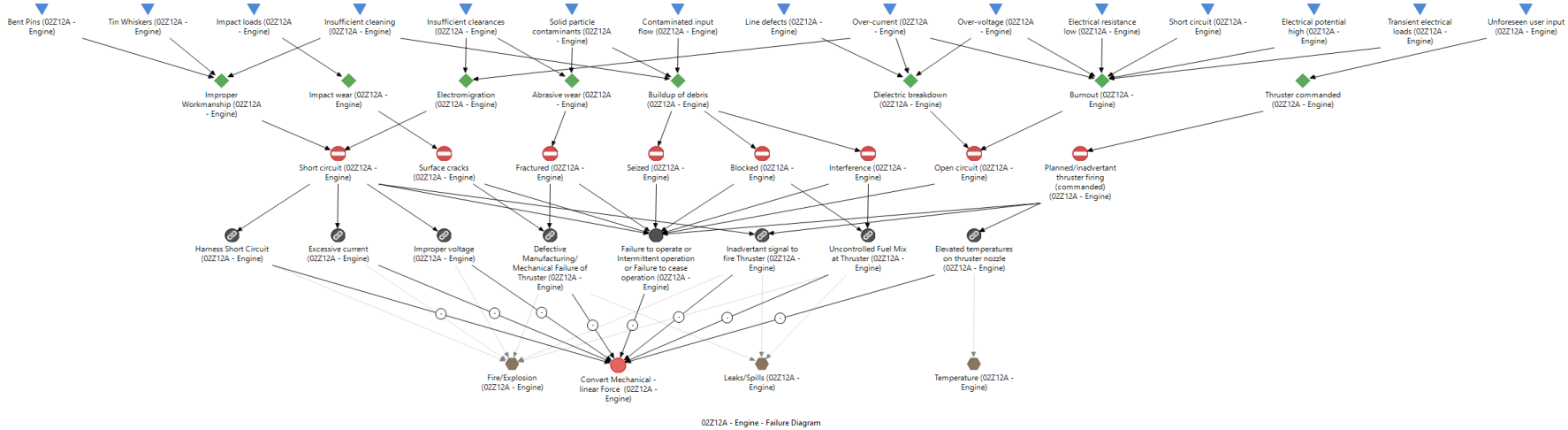


Figure A51: MADE EUROPA REM-1 (02Z12A Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

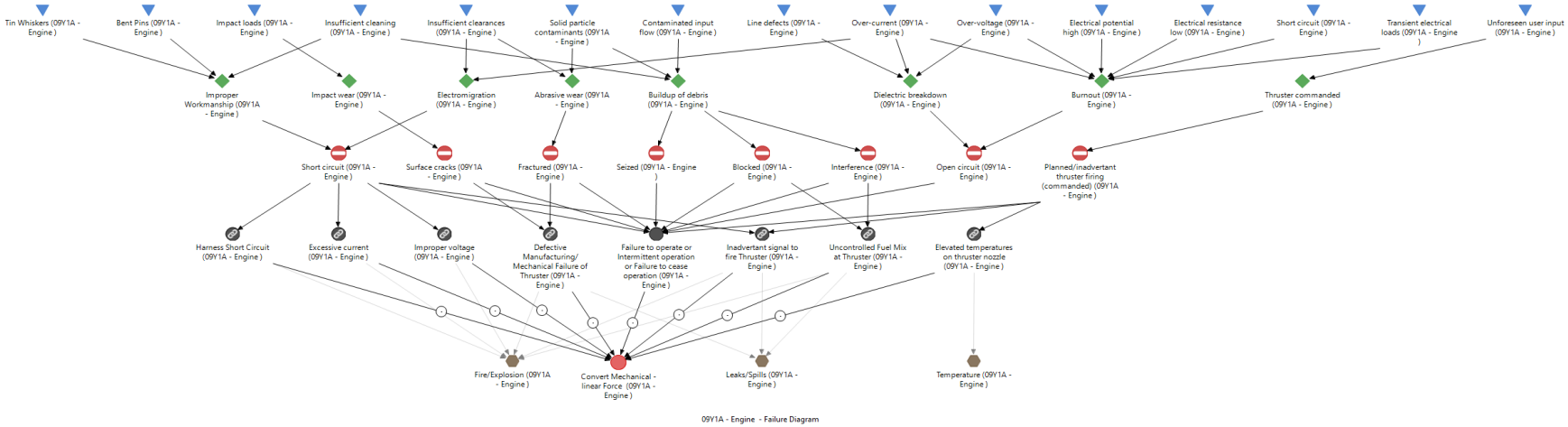


Figure A52: MADE EUROPA REM-1 (09Y1A Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

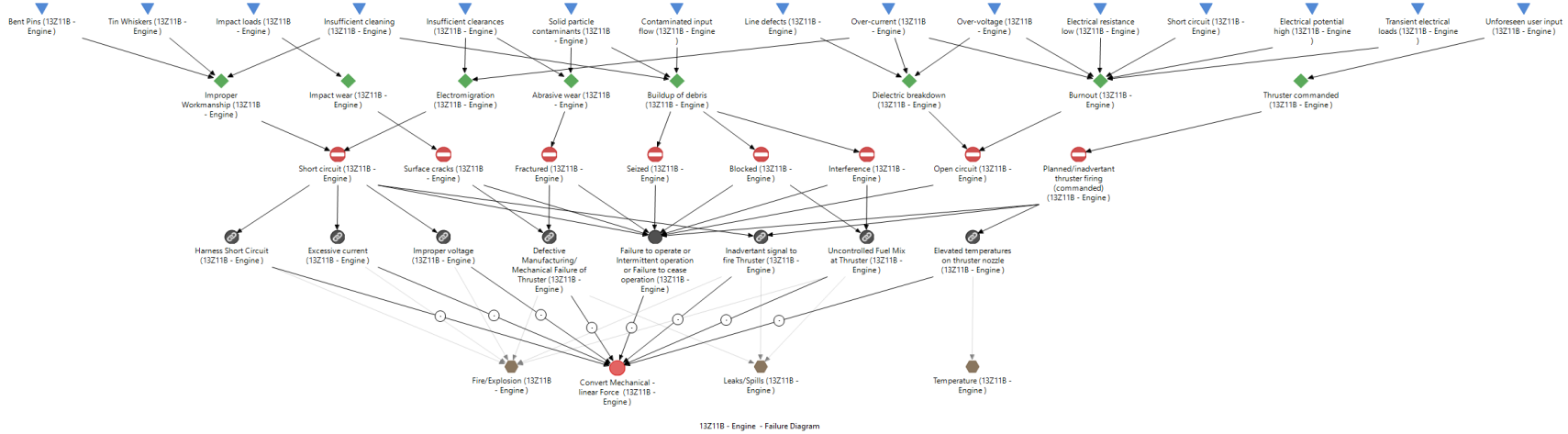


Figure A53: MADE EUROPA REM-1(13Z11B Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

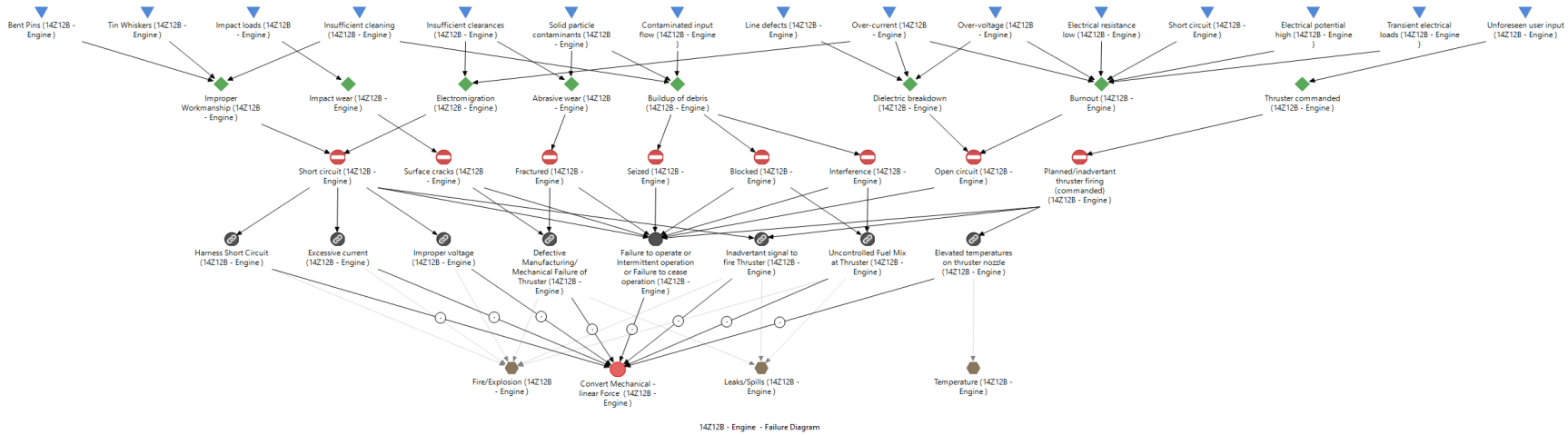


Figure A54: MADE EUROPA REM-1 (14Z12B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

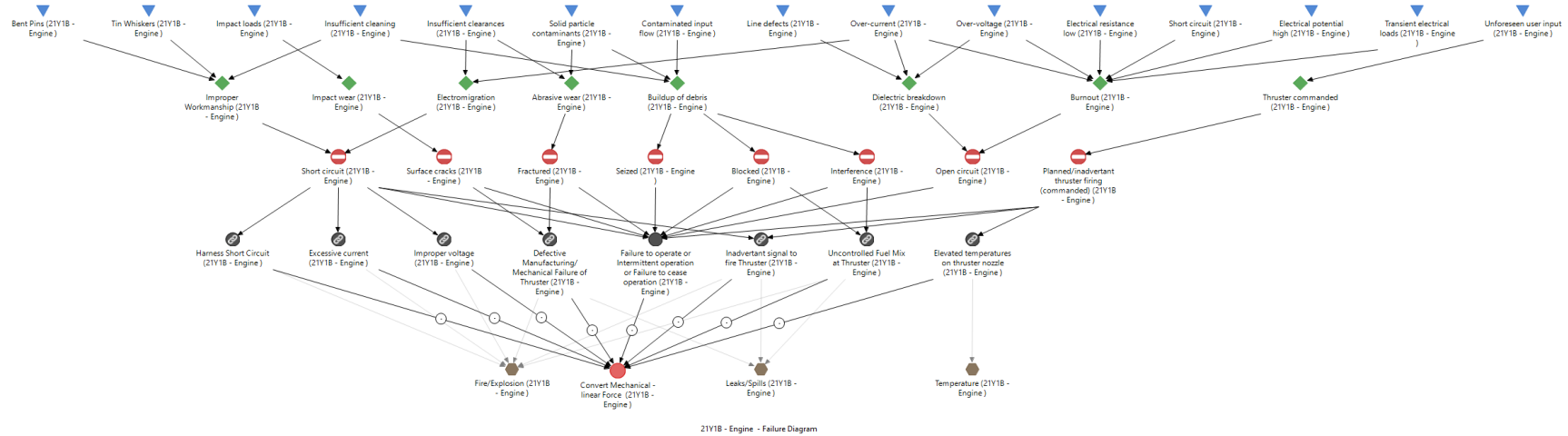


Figure A55: MADE EUROPA REM-1(21Y1B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

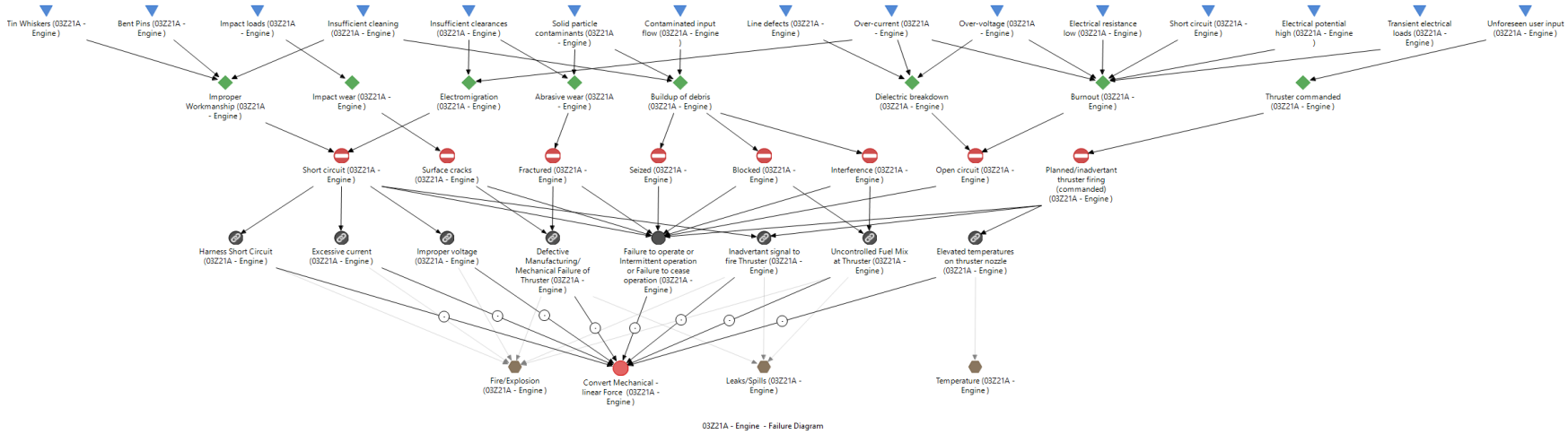


Figure A56: MADE EUROPA REM-2 (03Z21A Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

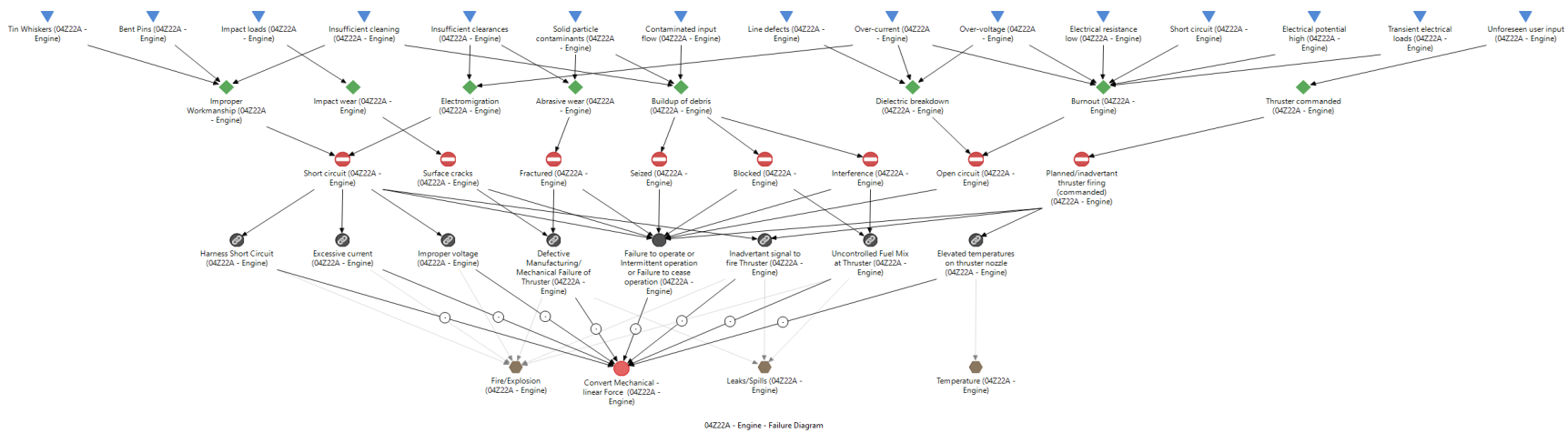


Figure A57: MADE EUROPA REM-2 (04Z22A Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

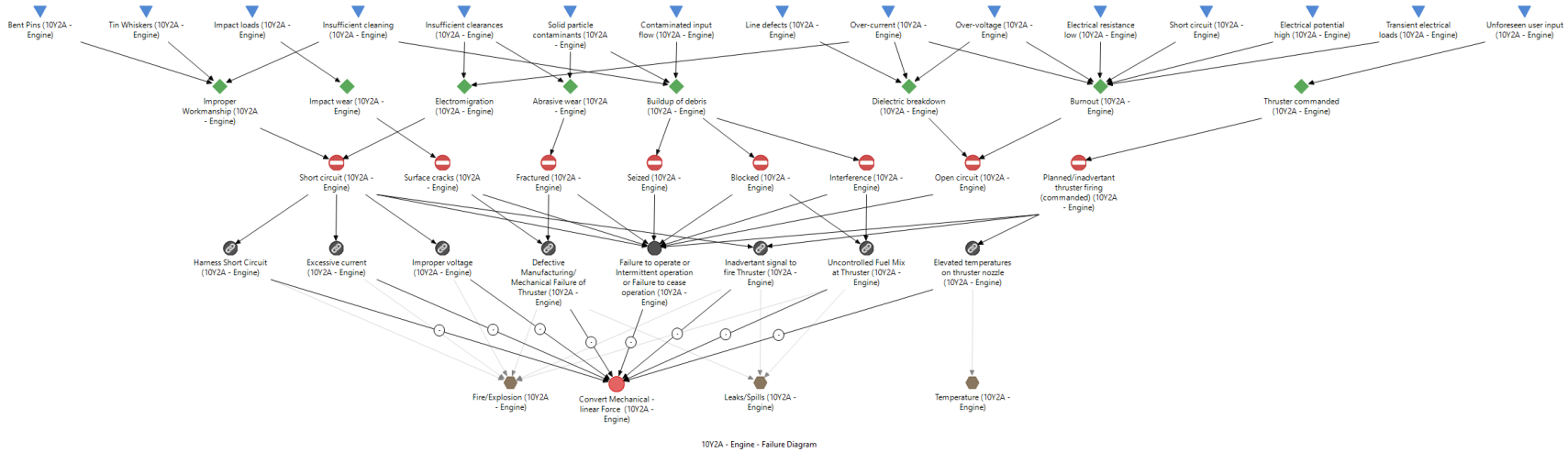


Figure A58: MADE EUROPA REM-2 (10Y2A Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

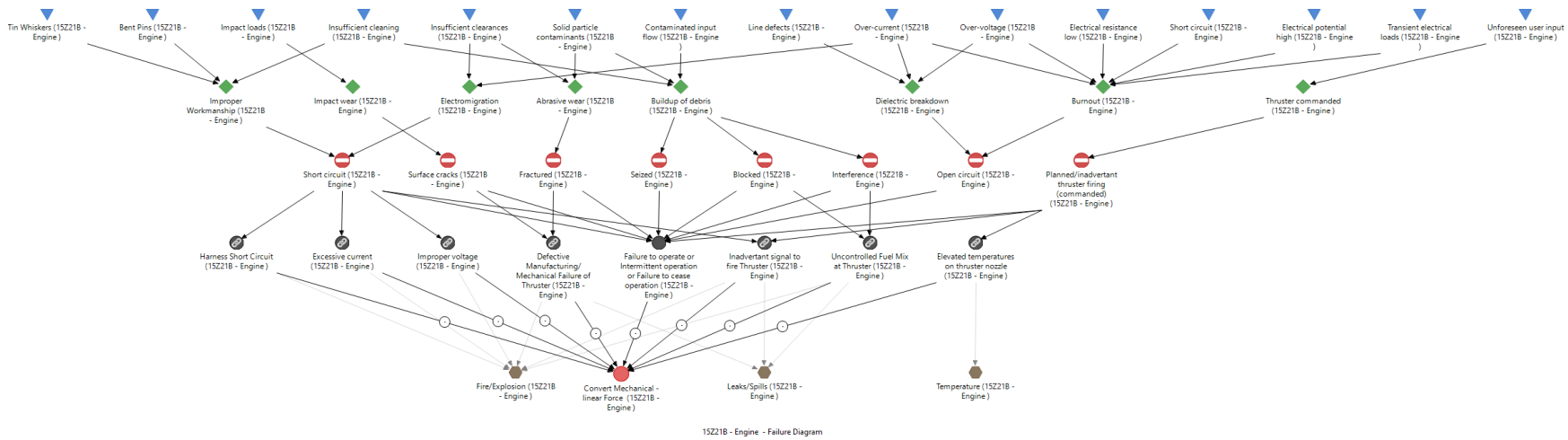


Figure A59: MADE EUROPA REM-2 (15Z21B Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

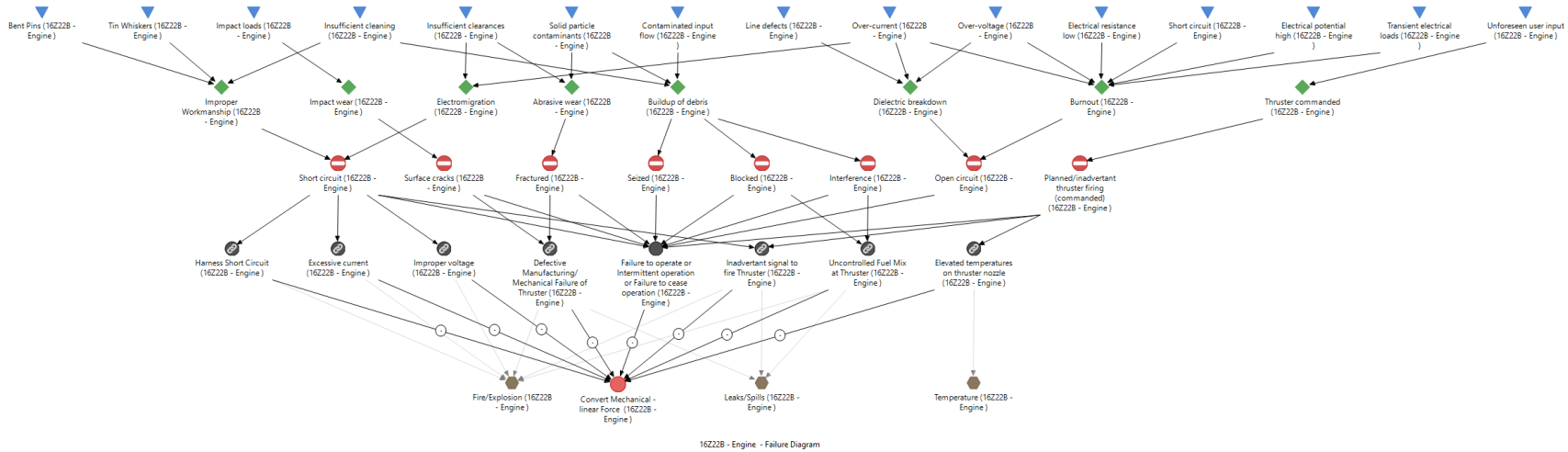


Figure A60: MADE EUROPA REM-2 (16Z22B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

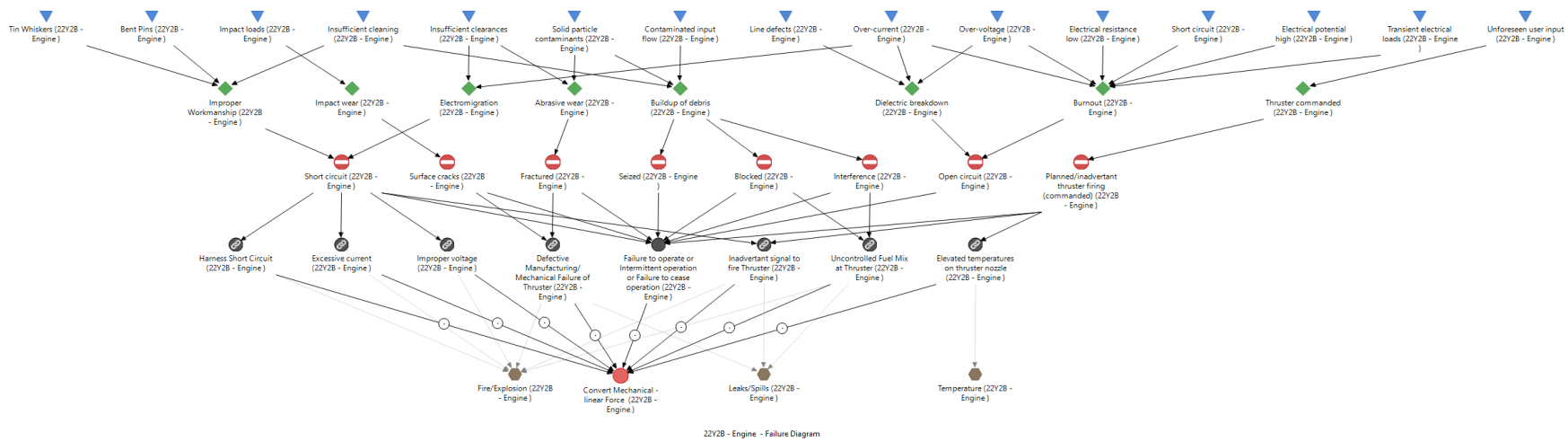


Figure A61: MADE EUROPA REM-2 (22Y2B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

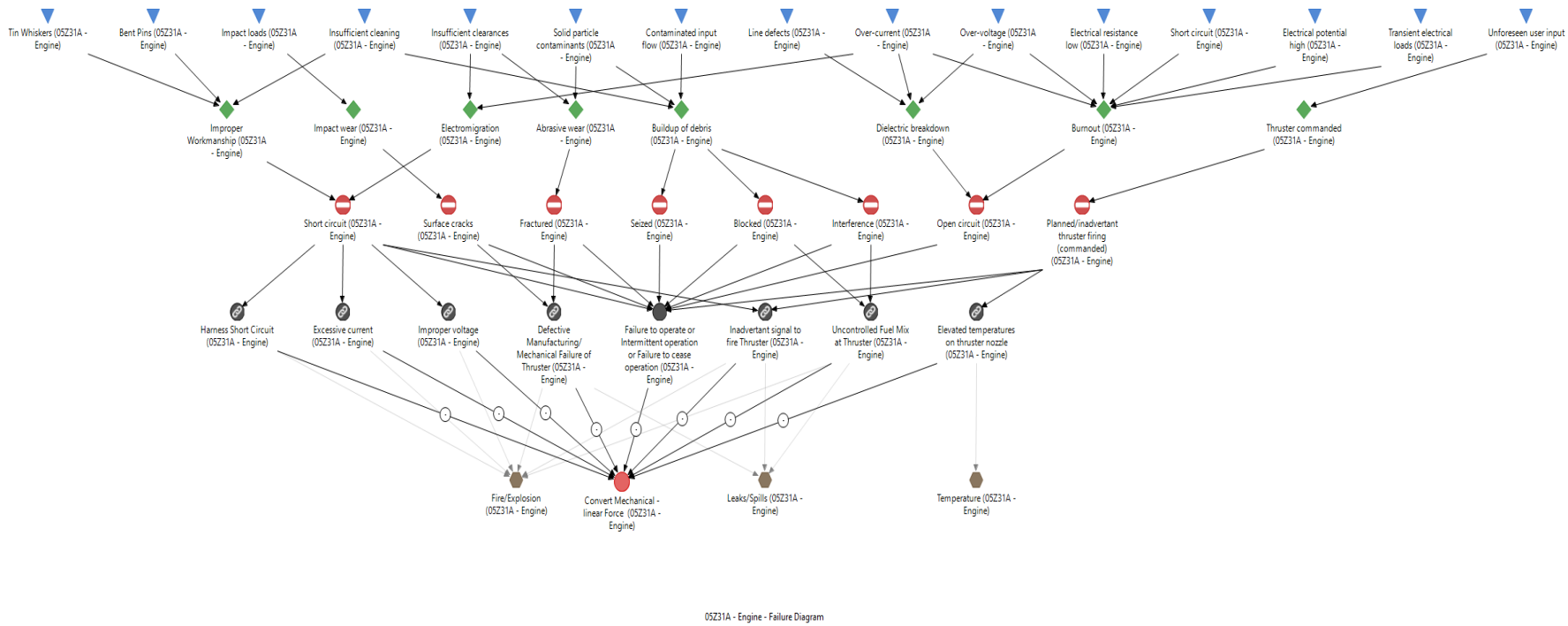


Figure A62: MADE EUROPA REM-3 (05Z31A Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

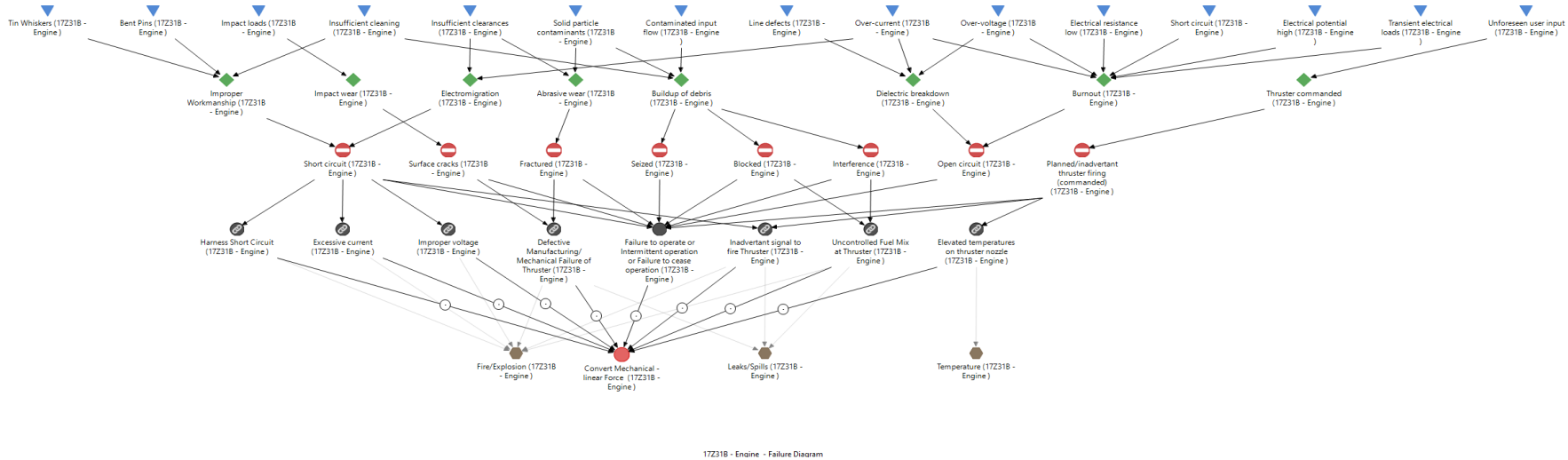


Figure A63: MADE EUROPA REM-3 (17Z31B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

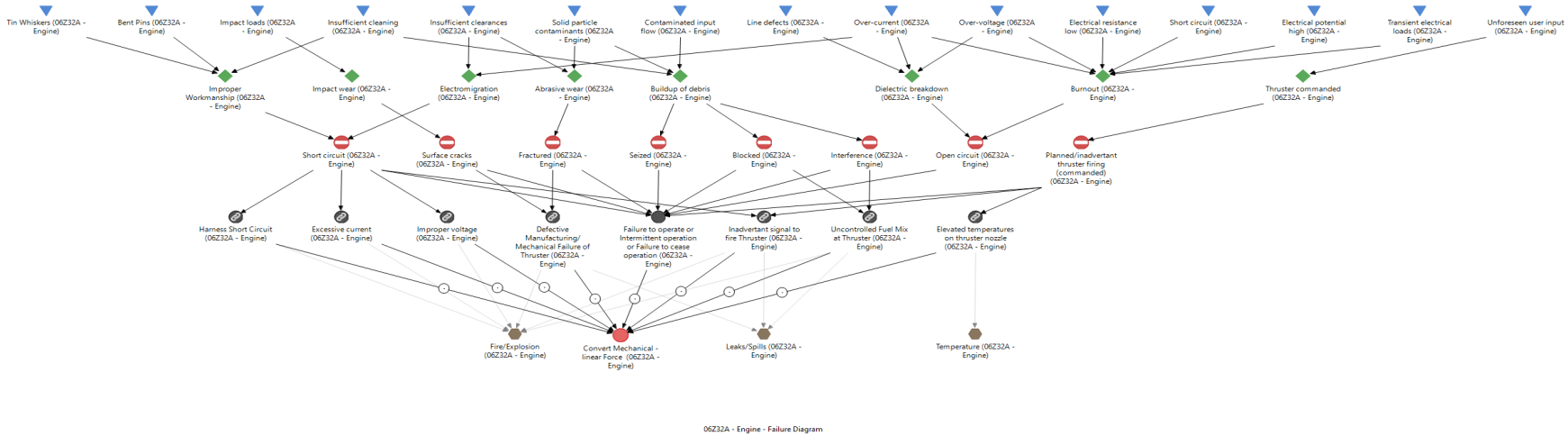


Figure A64: MADE EUROPA REM-3 (06Z32A Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

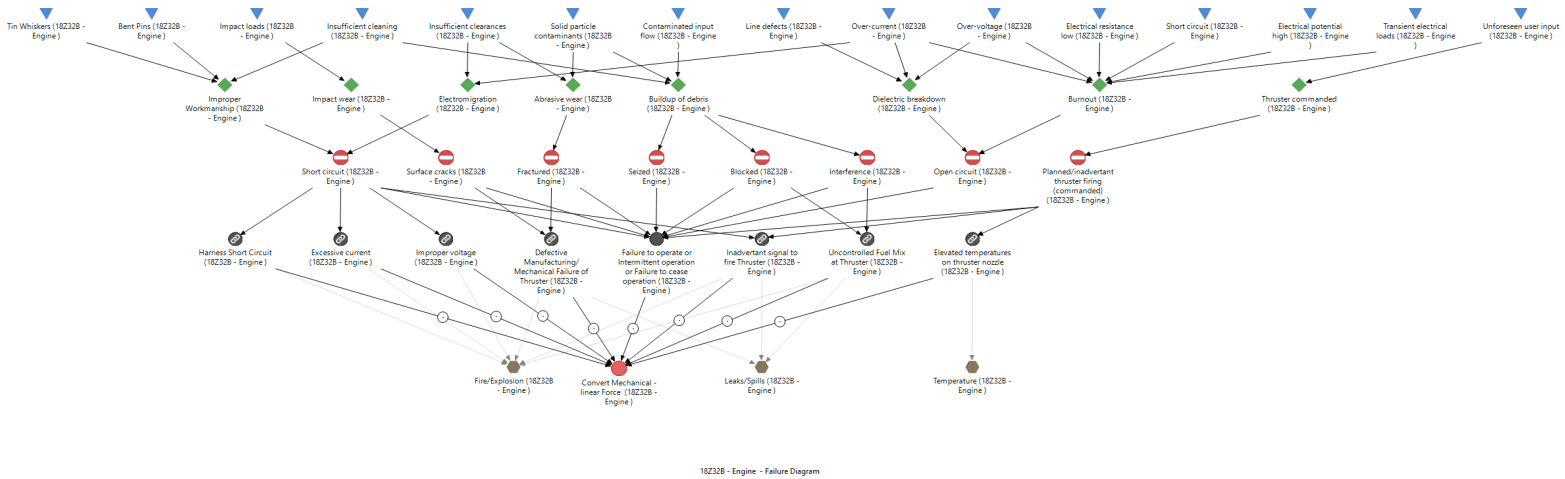


Figure A65: MADE EUROPA REM-3 (19Z32B Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

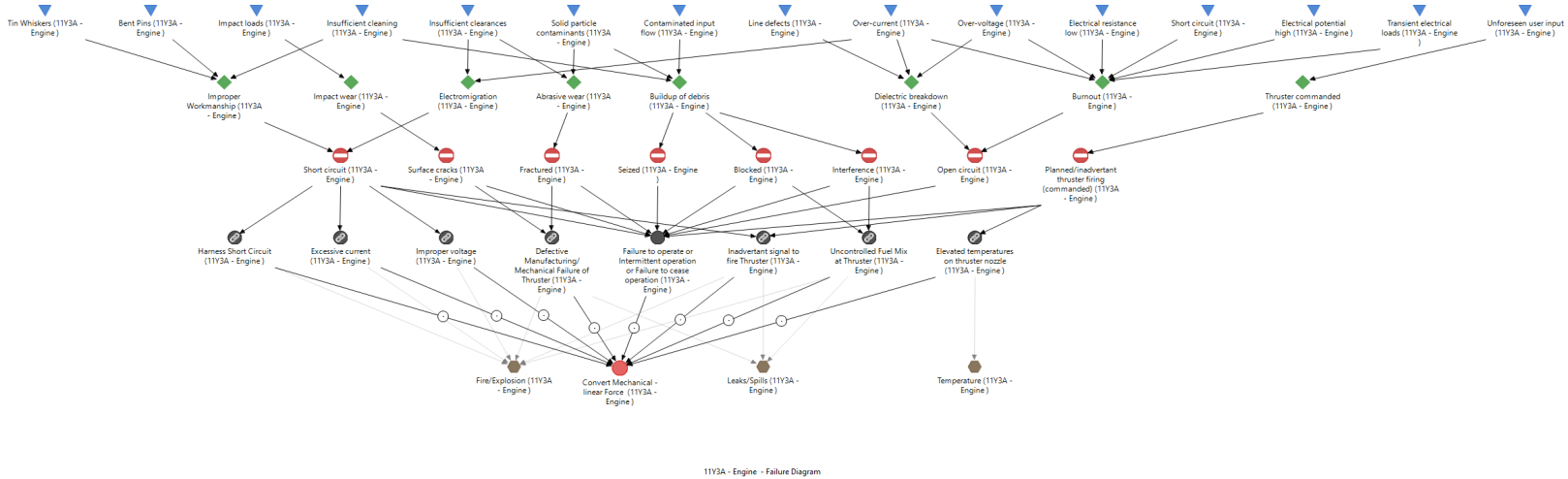


Figure A66: MADE EUROPA REM-3 (11Y3A Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

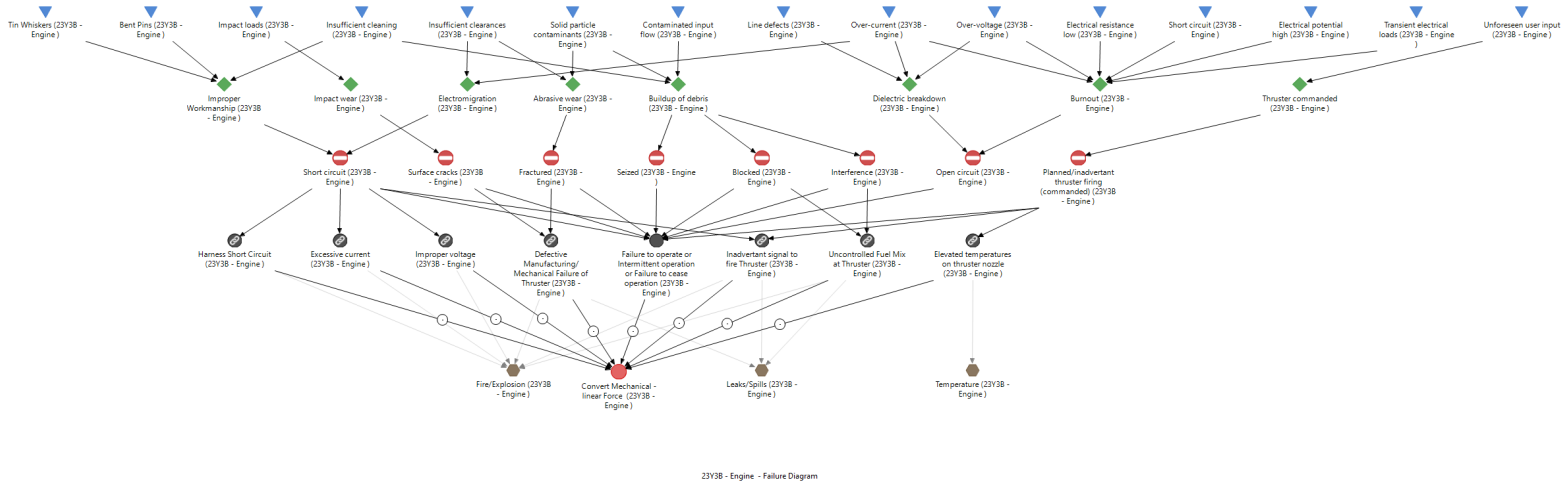


Figure A67: MADE EUROPA REM-3 (23Y3B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

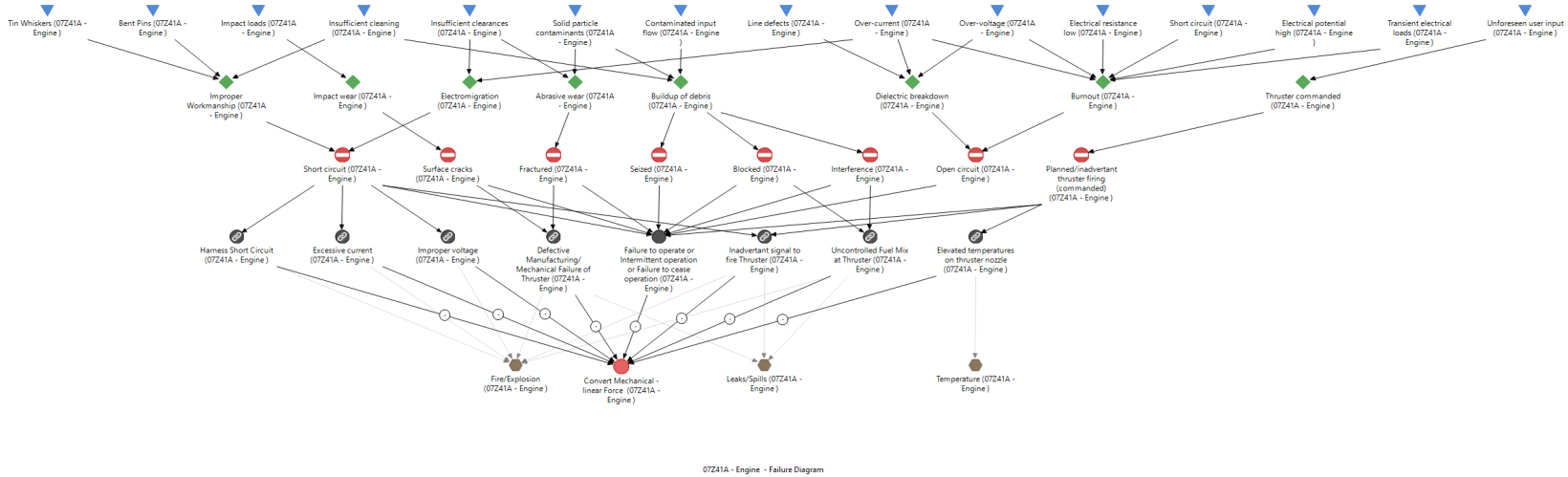


Figure A68: MADE EUROPA REM-4 (07Z41A Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

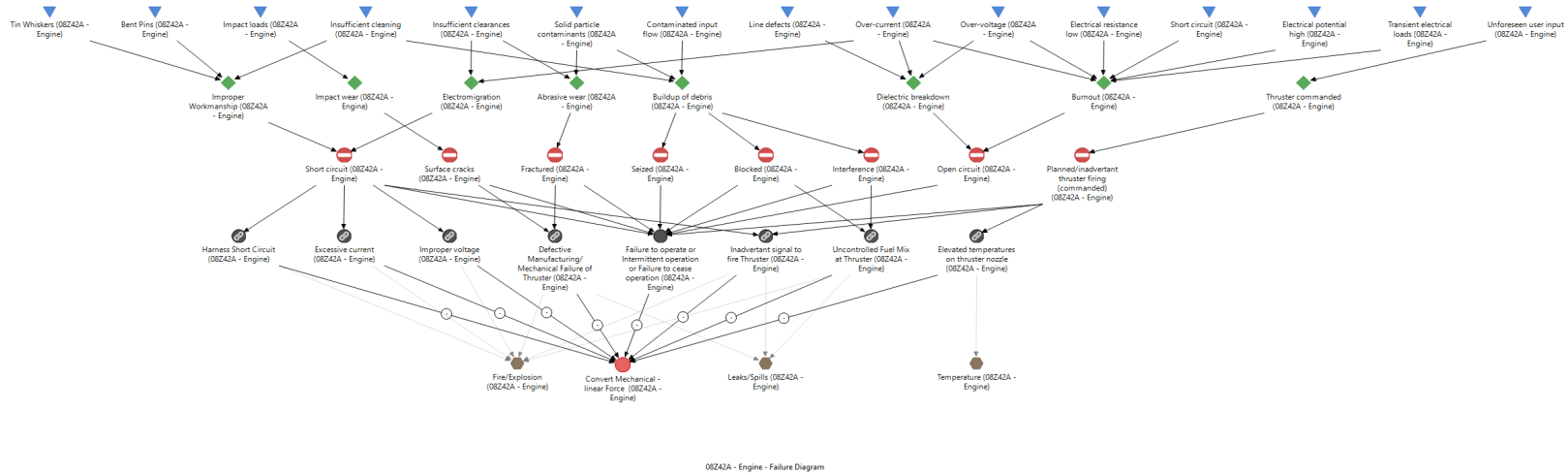


Figure A69: MADE EUROPA REM-4 (08Z42A Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

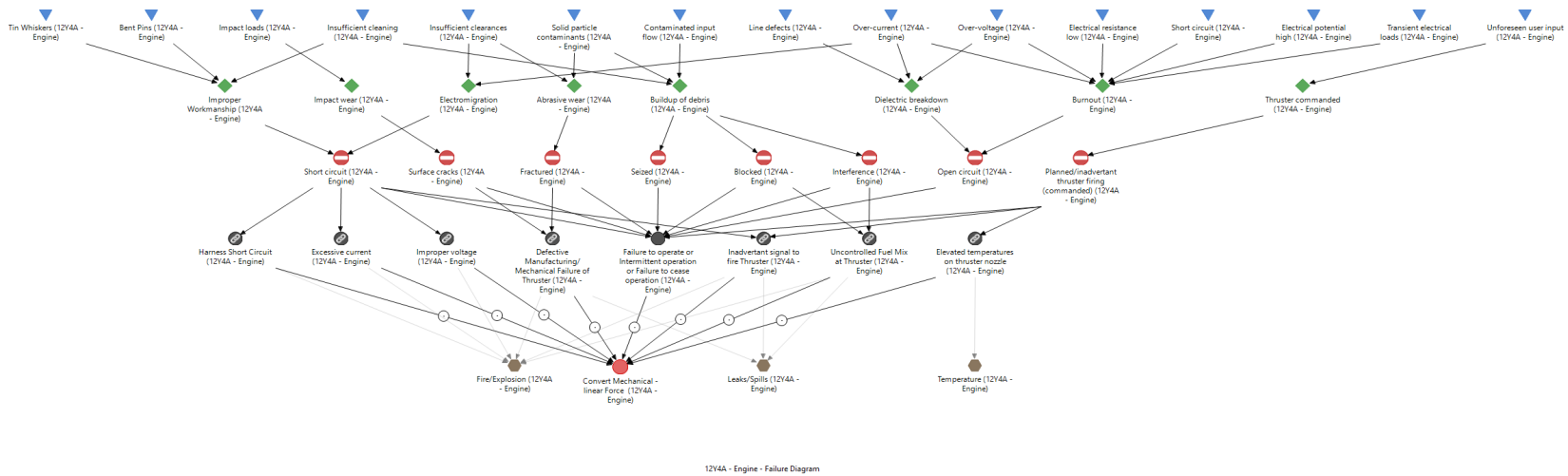


Figure A70: MADE EUROPA REM-4 (12Y4A Engine) Failure Diagram
(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

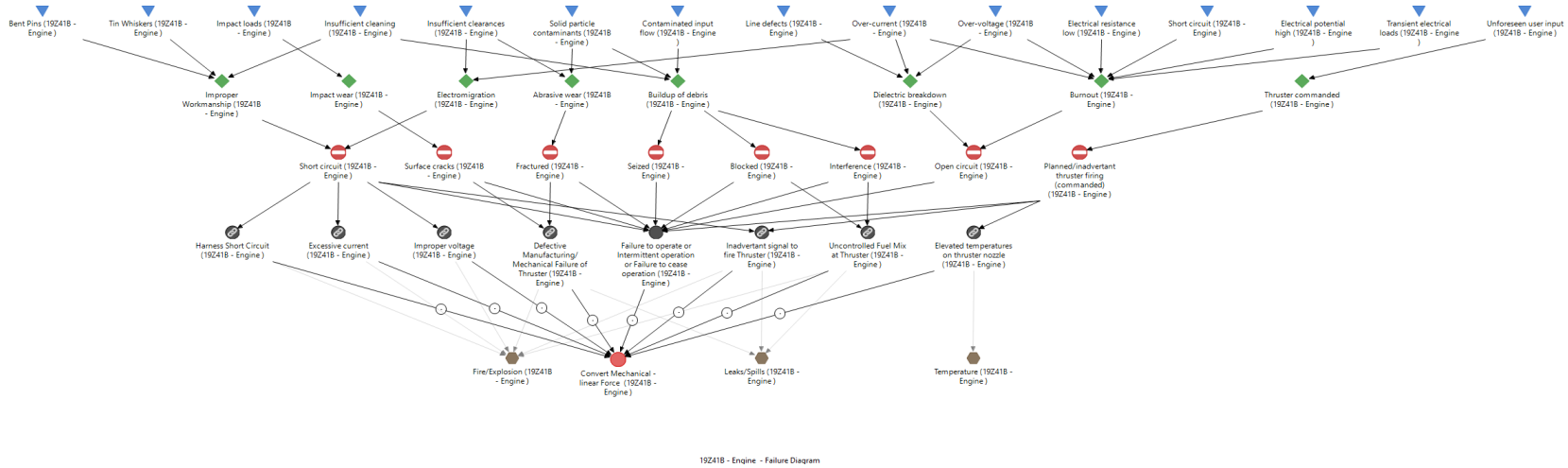


Figure A71: MADE EUROPA REM-4 (19Z41B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in Reliability outputs)

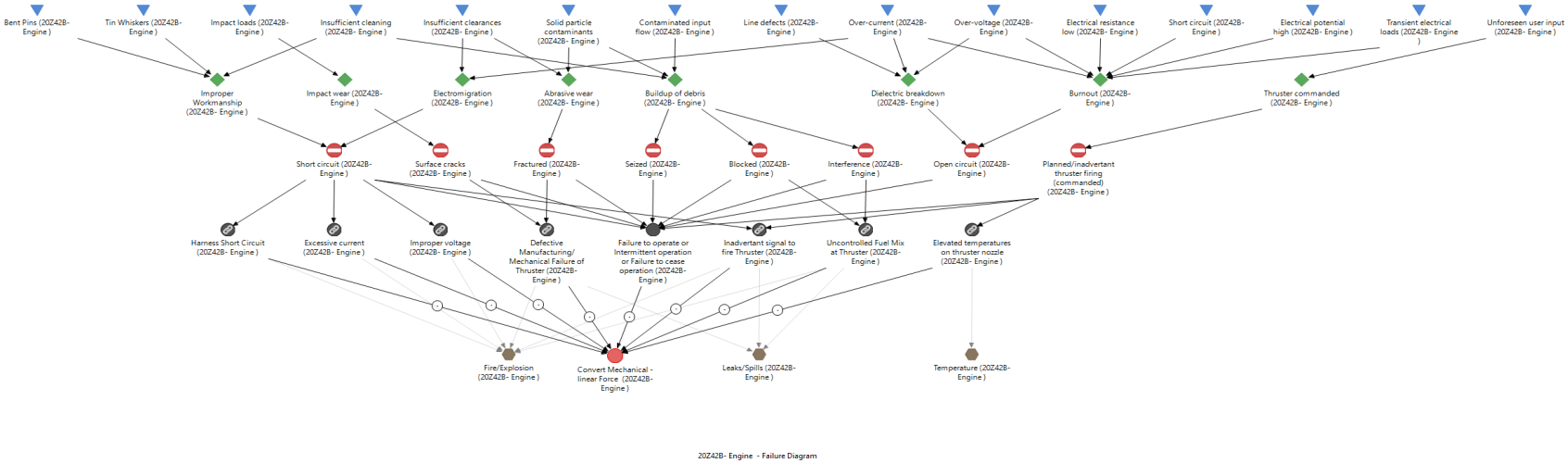


Figure A72: MADE EUROPA REM-4 (20Z42B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in Reliability outputs)

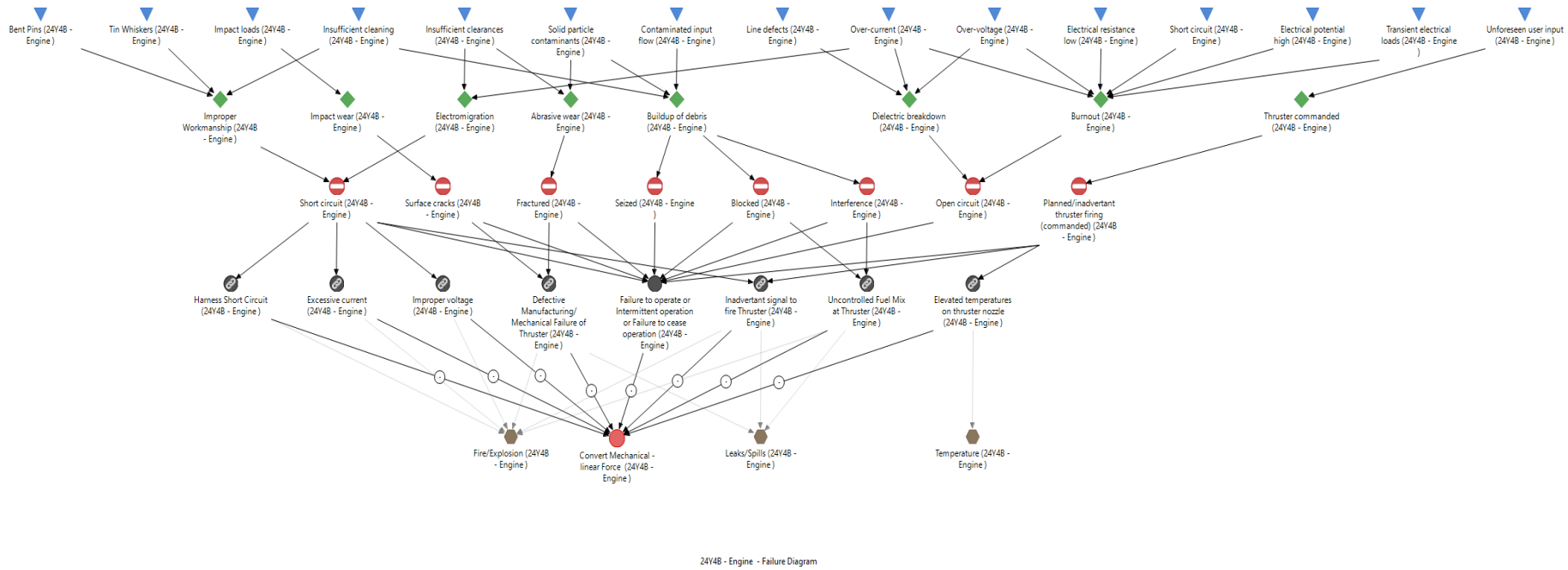


Figure A73: MADE EUROPA REM-4 (24Y4B Engine) Failure Diagram

(For reliability analyses be advised that it is advisable to disconnect Inadvertent Signal and Elevated Temperatures from Convert Mechanical Linear Force to avoid erroneous or duplicative entries in reliability outputs)

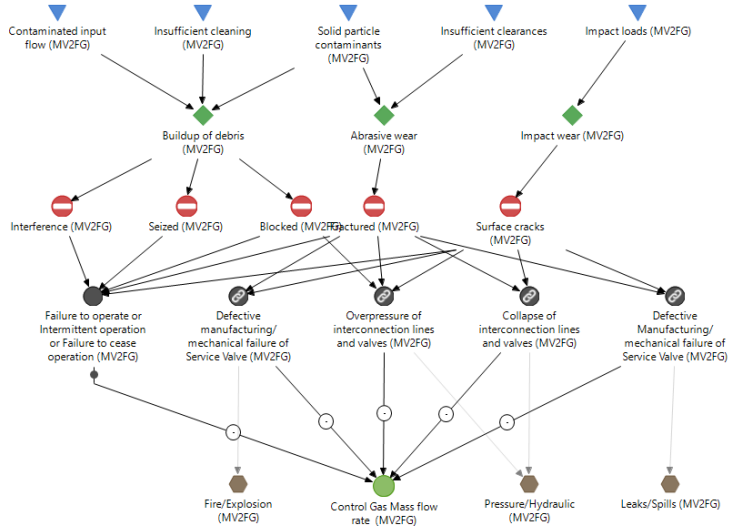


Figure A74: MADE EUROPA Service Valves – Fuel (MV2FG) Failure Diagram

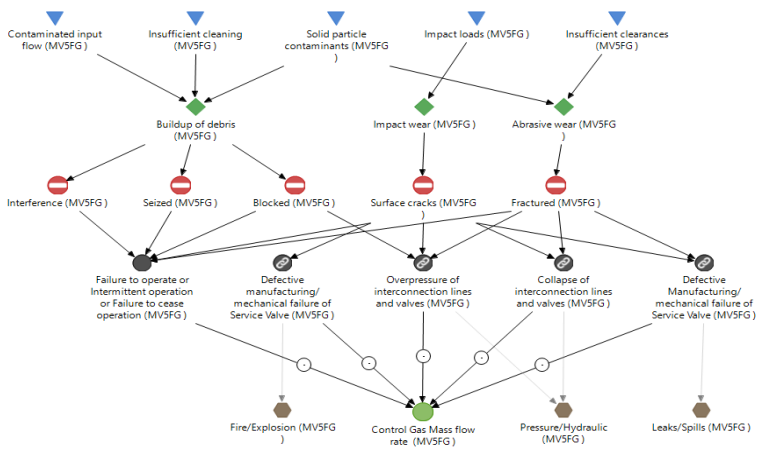


Figure A75: MADE EUROPA Service Valves – Fuel (MV5FG) Failure Diagram

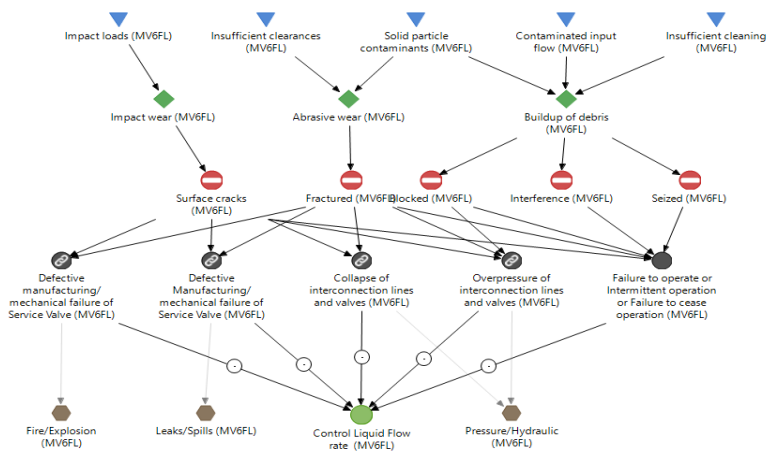


Figure A76: MADE EUROPA Service Valves – Fuel (MV6FL) Failure Diagram

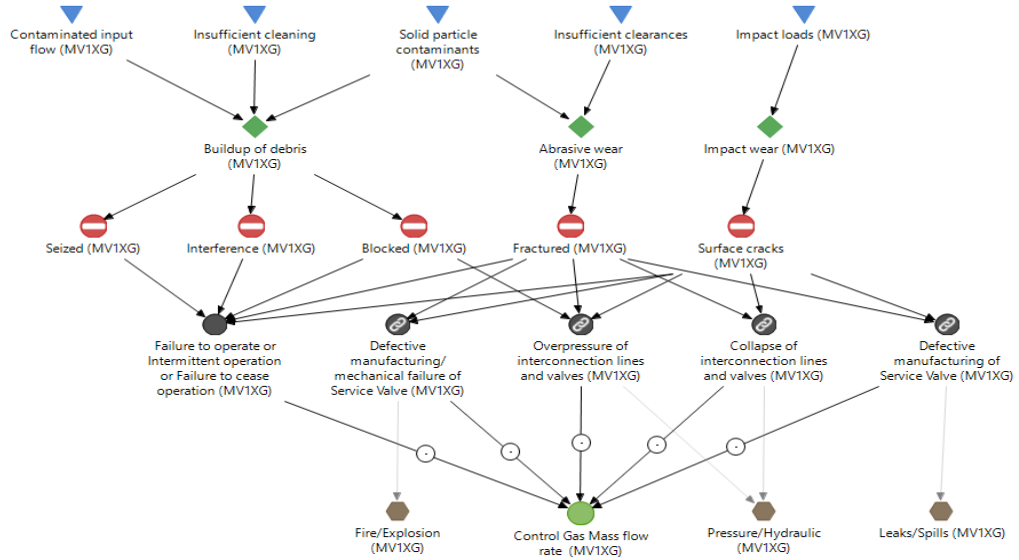


Figure A77: MADE EUROPA Service Valves – Fuel (MV1XG) Failure Diagram

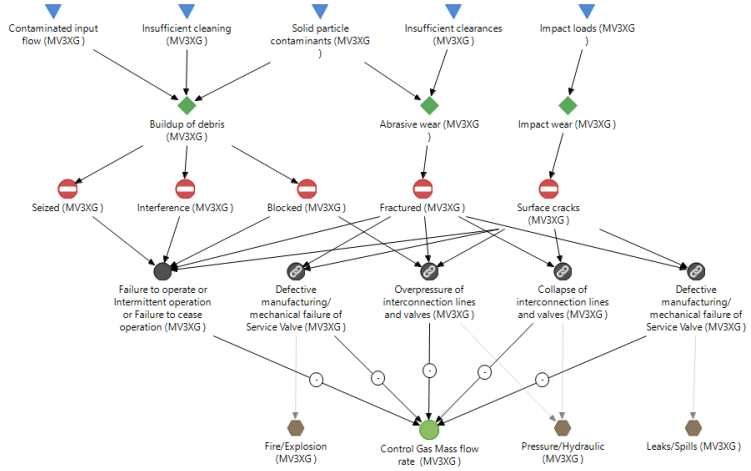


Figure A78: MADE EUROPA Service Valves – Fuel (MV3XG) Failure Diagram

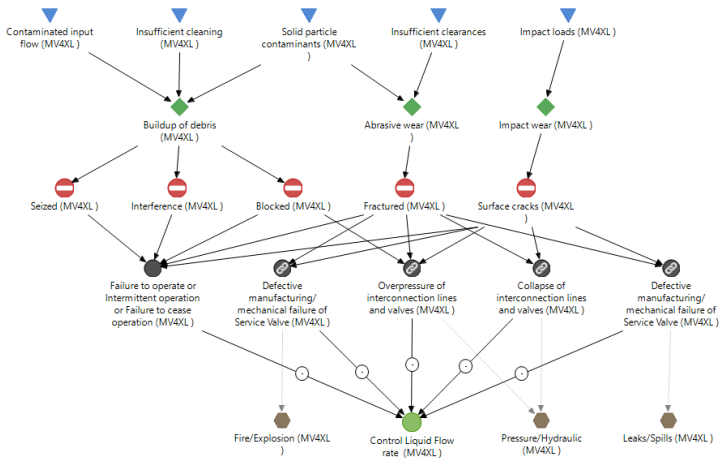


Figure A79: MADE EUROPA Service Valves – Fuel (MV4XL) Failure Diagram

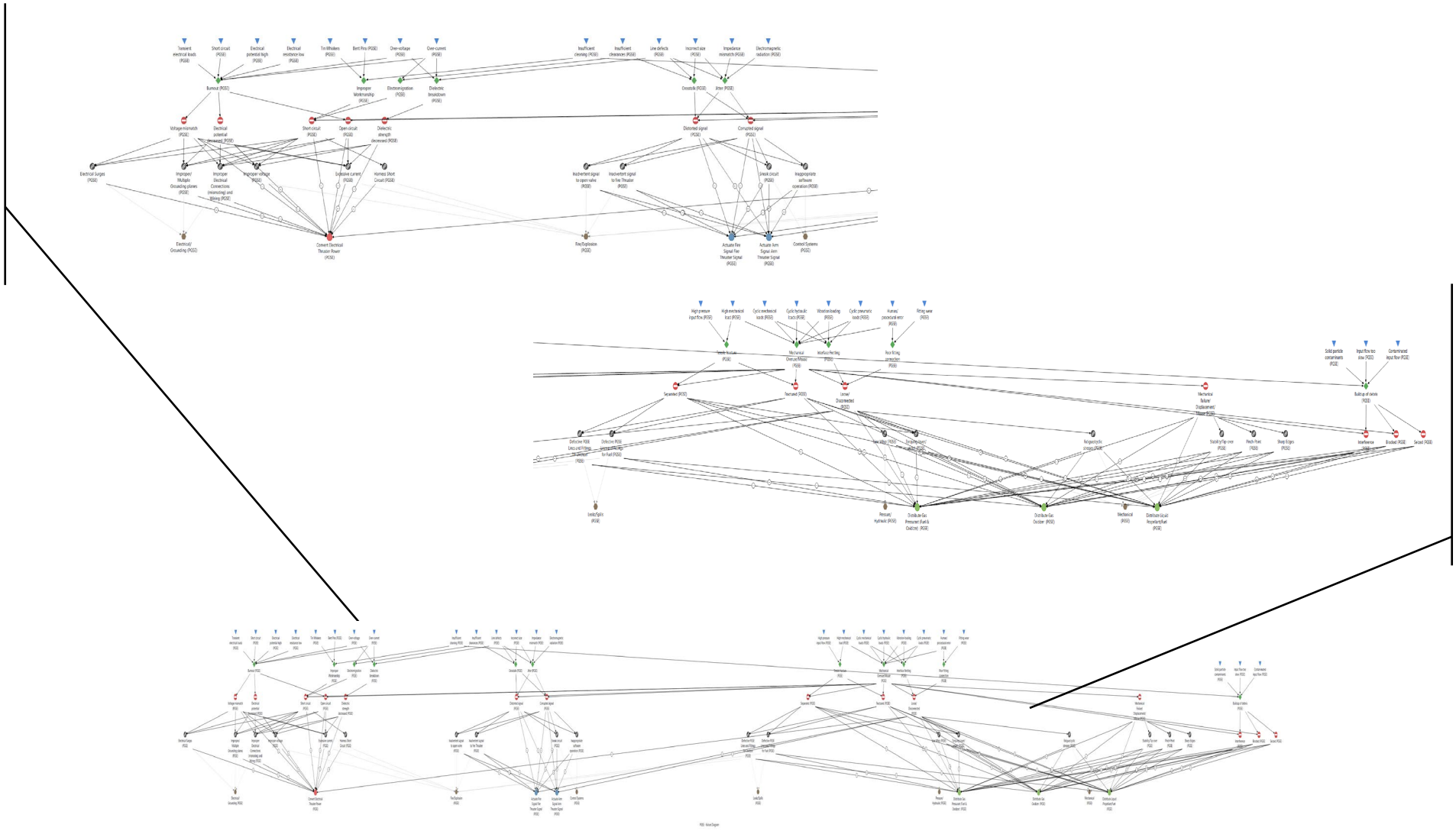


Figure A80: MADE EUROPA PGSE Failure Diagram (with magnified views)
(For reliability analyses be advised that it is advisable to disconnect Sharp Edges and Pinch Points from Distribute Liquid/Fuel to avoid erroneous or duplicative entries in reliability outputs)

SysML/MagicDraw: Reserved for update when SysML/MagicDraw system safety capability is realized.

Appendix B : Recommended MADE Modeling Techniques & Tips

MADE's main interface (Figure B1) includes a *Project Explorer* and supporting libraries (i.e., *Failure Concepts*, generic *Palette*, and a *Local Library* of user defined components), relational diagrams (functional and failure), and continuous error notification (*Problem/Connection Viewer*).

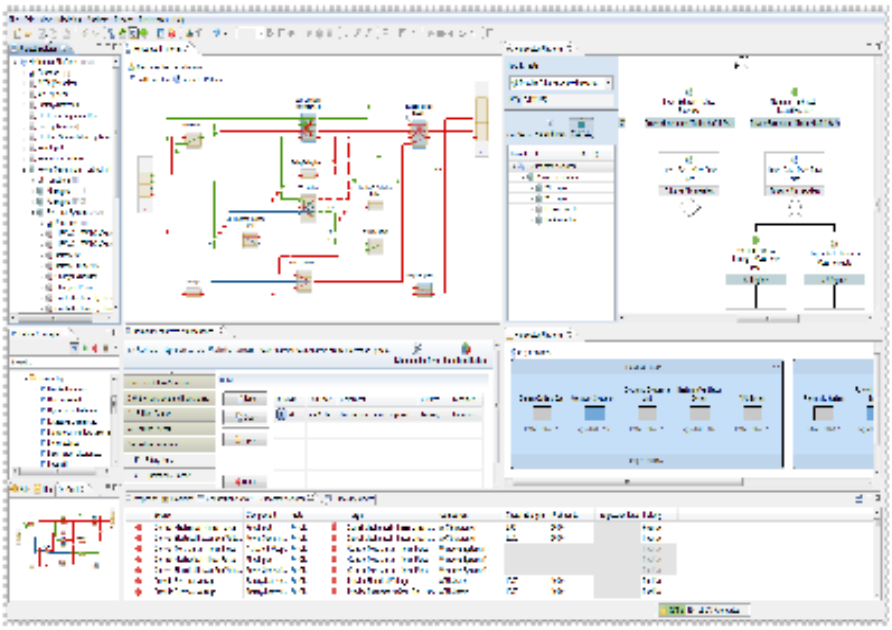


Figure B1: MADE Interface

To model a system in *MADE*, hierarchical structures and characterizations are required to constitute the model to support mission assurance activities and generate risk-based artifacts. Therefore, it is recommended that the Techniques and Tips in the subsequent sections be followed to:

I. Create/Import system hierarchy in *Project Explorer* and define *Mission Profile*.
II. Refine/Enhance *functional block diagrams* with functions, flows, supporting narratives, and documentation for each element.
III. Add/Refine and integrate mission-assurance discipline-specific modeling.
   i. Reliability, Maintainability, and Availability (RMA) Engineering - design/assurance-specific failure, maintenance, and availability characterization parameters (i.e., failure causes/mechanisms, modes, and symptoms, detection methods, compensating provisions, occurrence probability, criticality/severity of the occurrence, and spares)
   ii. System Safety - design/assurance specific hazard category and condition parameters (i.e., causes, controls, consequences, severity, occurrence, and verifications).
   iii. Software Assurance - TBD
   iv. Quality Engineering - TBD
IV. Import requirements and link them to the model for compliance assessment, verification, and tracking.
V. Verify and validate modeling with error adjudication, simulation, and peer consults.
VI. Generate mission-assurance reports/assessments and requirement verifications/compliances.
VII. Iterate and update modeling (using Steps I – VI).

Double click on figure to open pdf