National Aeronautics and Space Administration

Reliability Analysis of Complex NASA Systems with Model Based Engineering

Nancy J. Lindsey, Risk & Reliability Branch Head — NASA/GSFC
Mahdi Alimardani, Reliability Engineer — NASA/GSFC
Luis D. Gallo, Reliability Engineer — NASA/GSFC

Sponsored by NASA/HQ : John Evans and Anthony DiVenti

RAMS 2020 - PAPER ID 71
Model-based System Engineering for Reliability Analysis

Jan 29th 2020
SESSION – 12

MBSMA

www.nasa.gov

MBSMA Initiative Pathfinder Partner Project Objectives

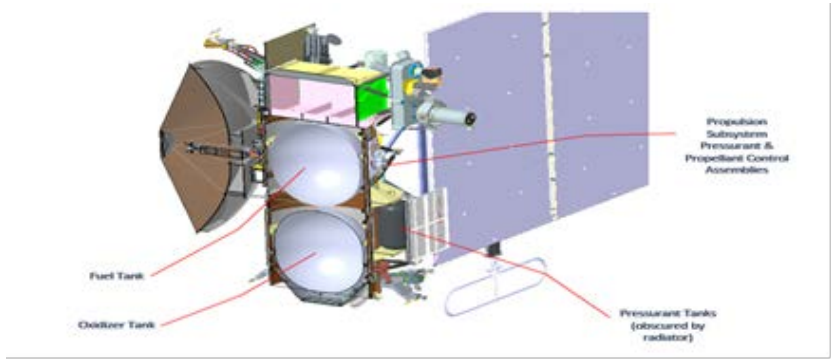
- Investigate methodologies for the deployment of Model Based SMA/MA:
  - Reliability (e.g., FMECA, LLA, FTA, PRA, Maintainability, Availability)
  - System Safety (e.g., MSPSP, Hazard Analysis)
  - Software Assurance (e.g., Control/Testing Plans, Process/Supplier Risks, Software FMECA/FTA)
  - Quality Assurance (e.g., Control/Testing Plans, Process/Supplier Risks, Parts/Materials Approvals, Mission Assurance Requirements, PRACA/FRACAs)

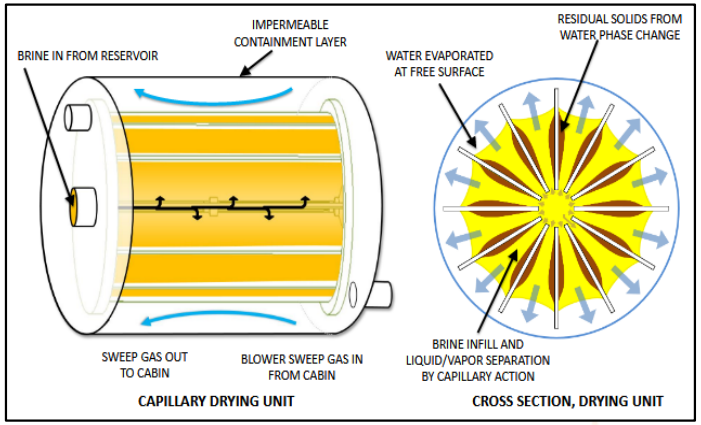
- Provide Recommendations, Guidance, and Risk-Based Strategies for MBSMA/MA and MBSE Collaboration

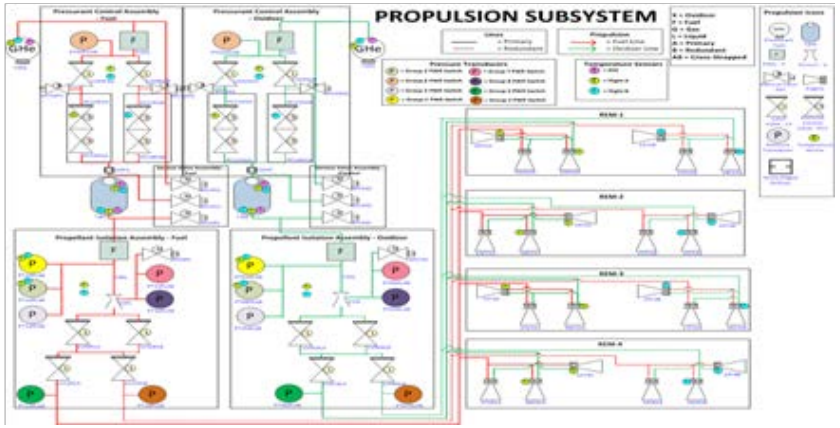
Is Model-Based Engineering valid and useable for Reliability Engineering for NASA mission Safety and Mission Assurance ?

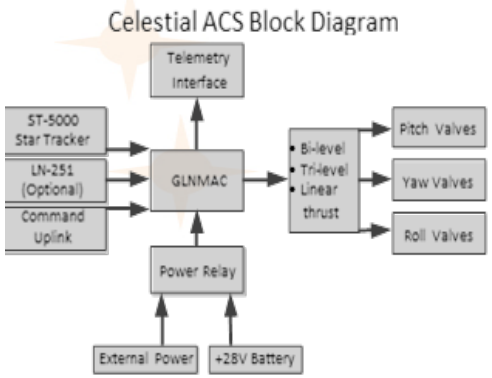
MBSMAI Methodology

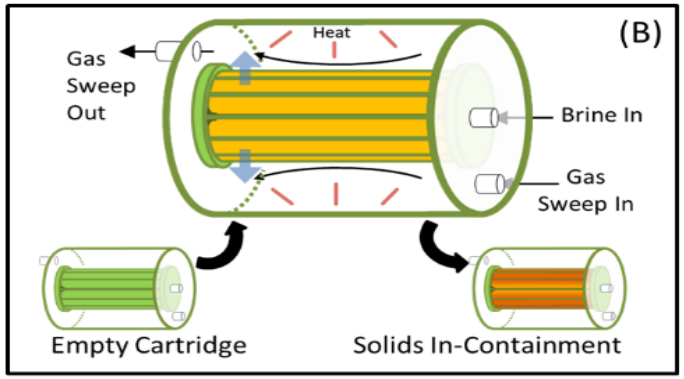
Use three mission test cases to evaluate the ability of Model-Based Engineering to support Reliability Analyses of Probability Analysis (PA)) Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), and Limited Life Analysis (LLA).



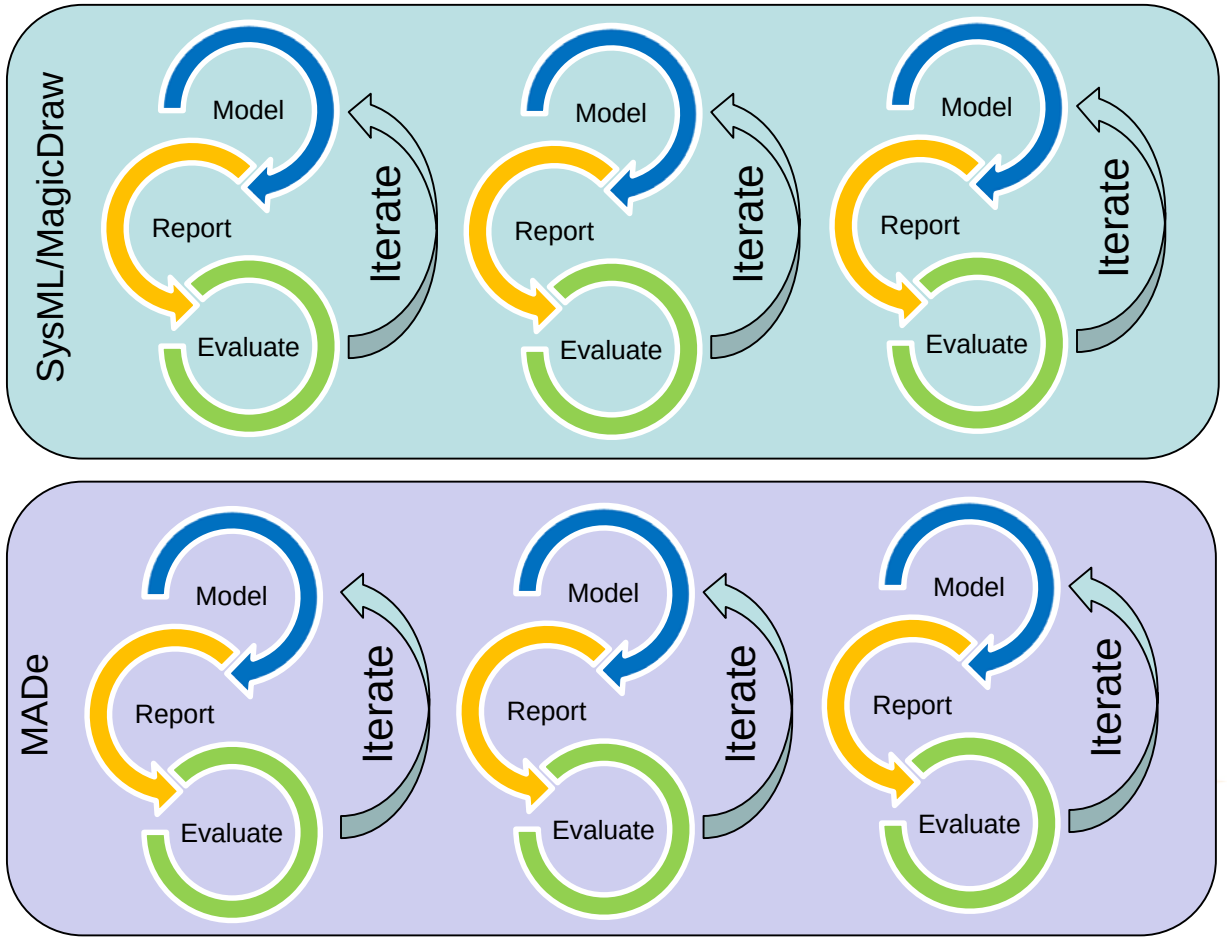








MBSMAI Methodology

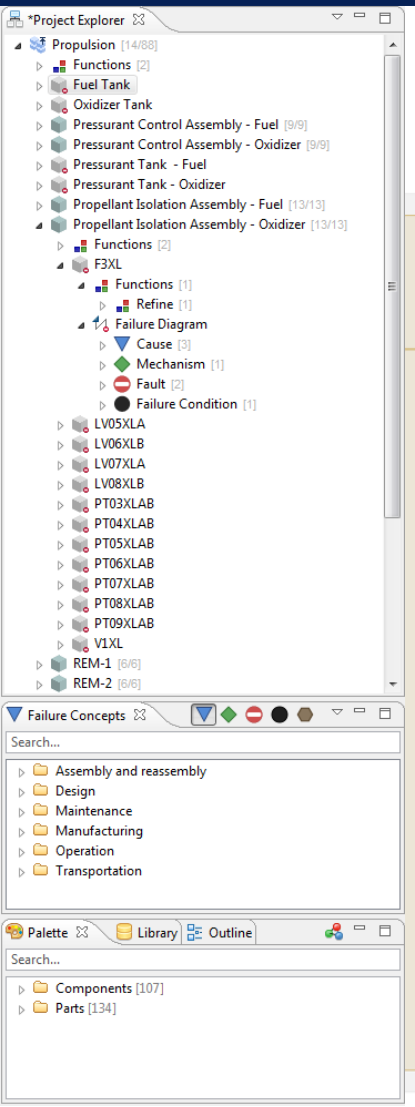


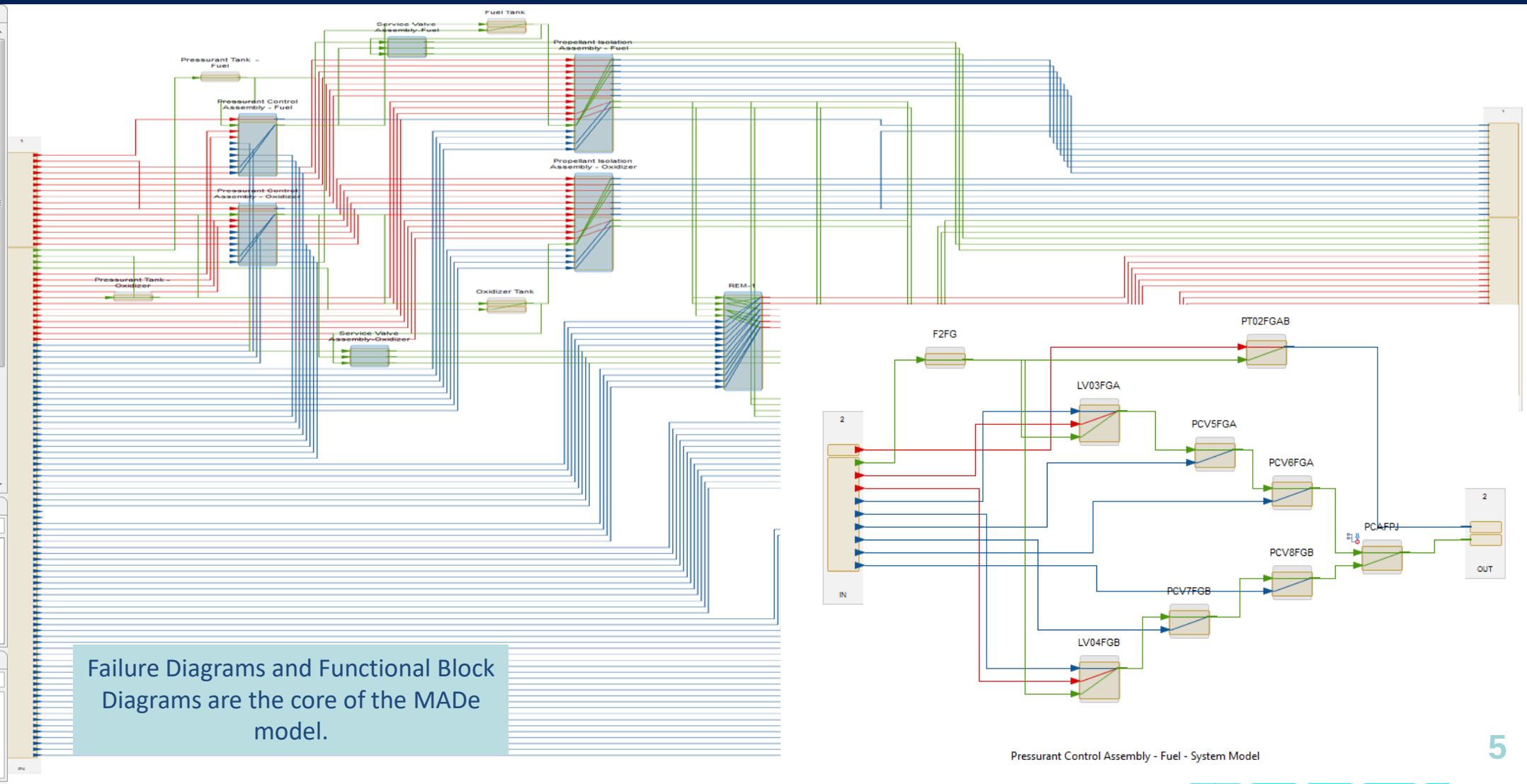
Modeling Process Guidance

Optimal Modeling Environment Requirements*

* Tool readiness was also assessed.

MBSMAI Phase 1: EUROPA Propulsion Modeling

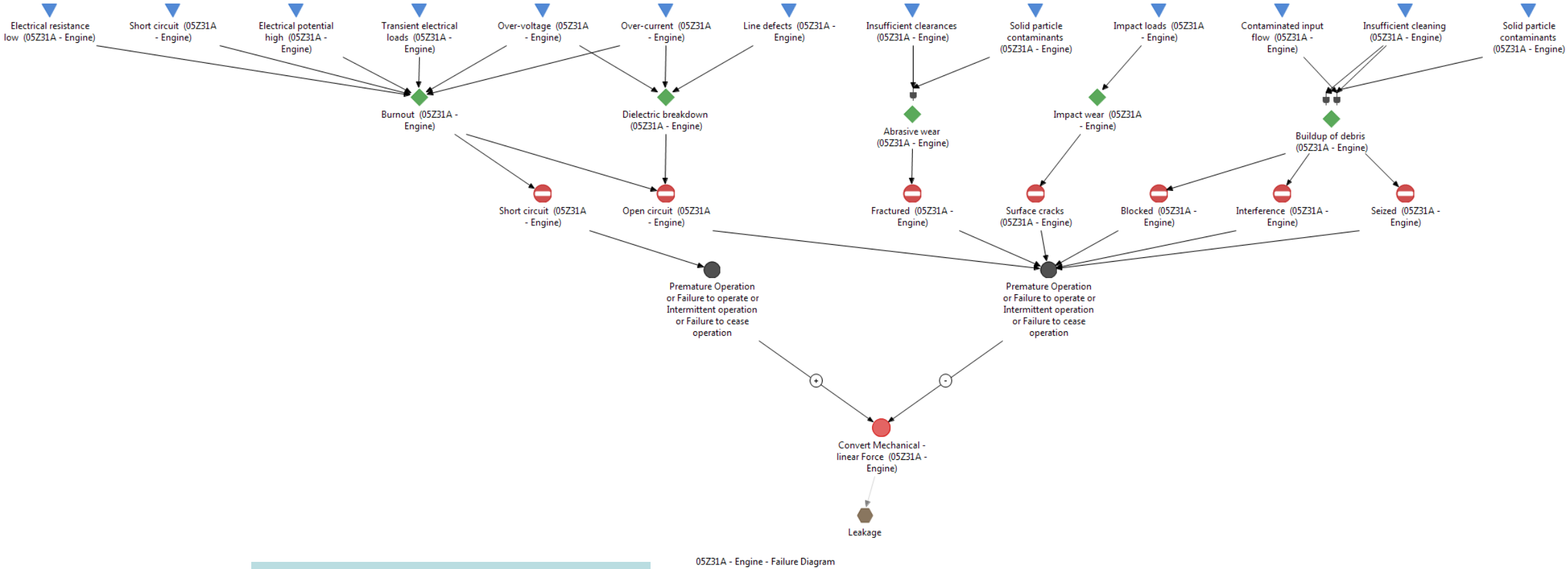




Failure Diagrams and Functional Block Diagrams are the core of the MADe model.

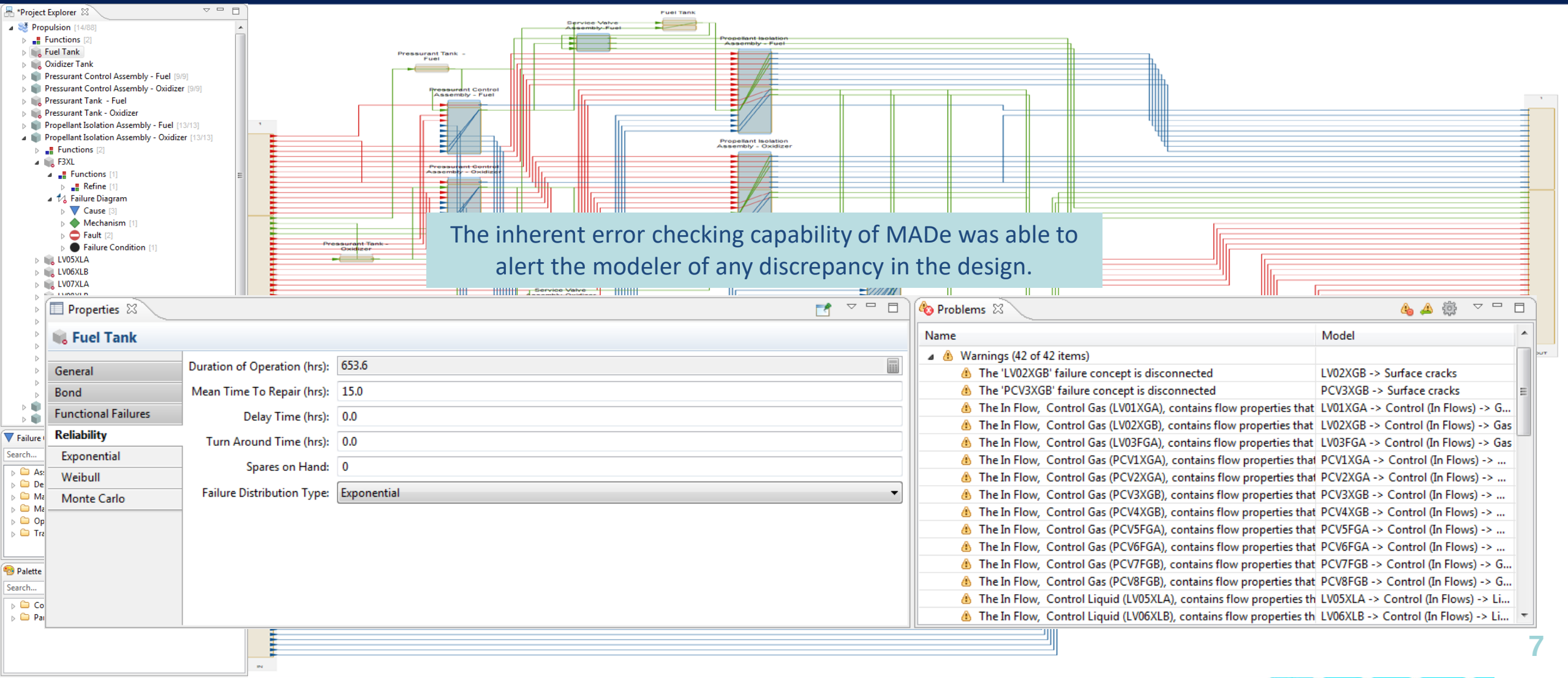
Pressurant Control Assembly - Fuel - System Model

MBSMAI Phase 1: EUROPA Propulsion Modeling



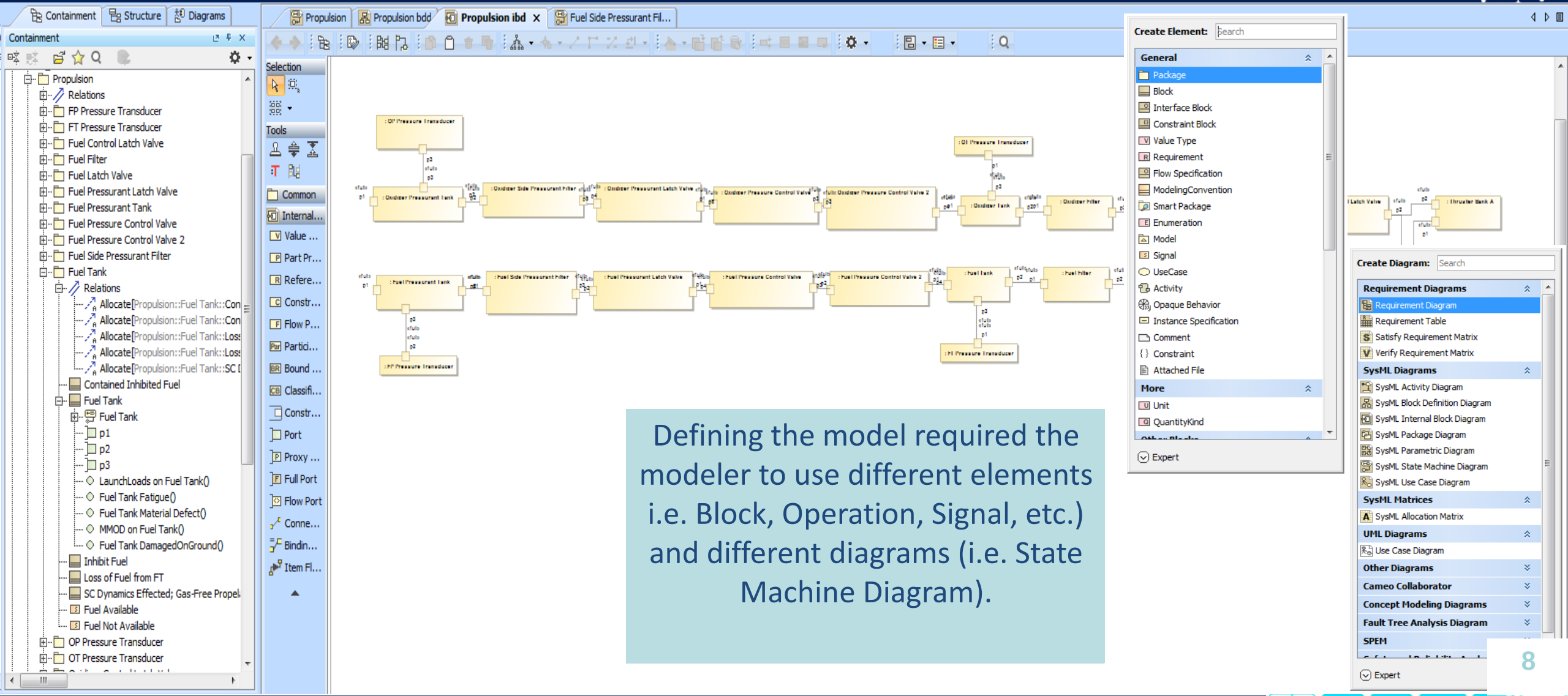
Failure Diagrams and Functional Block Diagrams are the core of the MADe model.

MBSMAI Phase 1: EUROPA Propulsion Modeling



The inherent error checking capability of MADe was able to alert the modeler of any discrepancy in the design.

MBSMAI Phase 1: EUROPA Propulsion Modeling

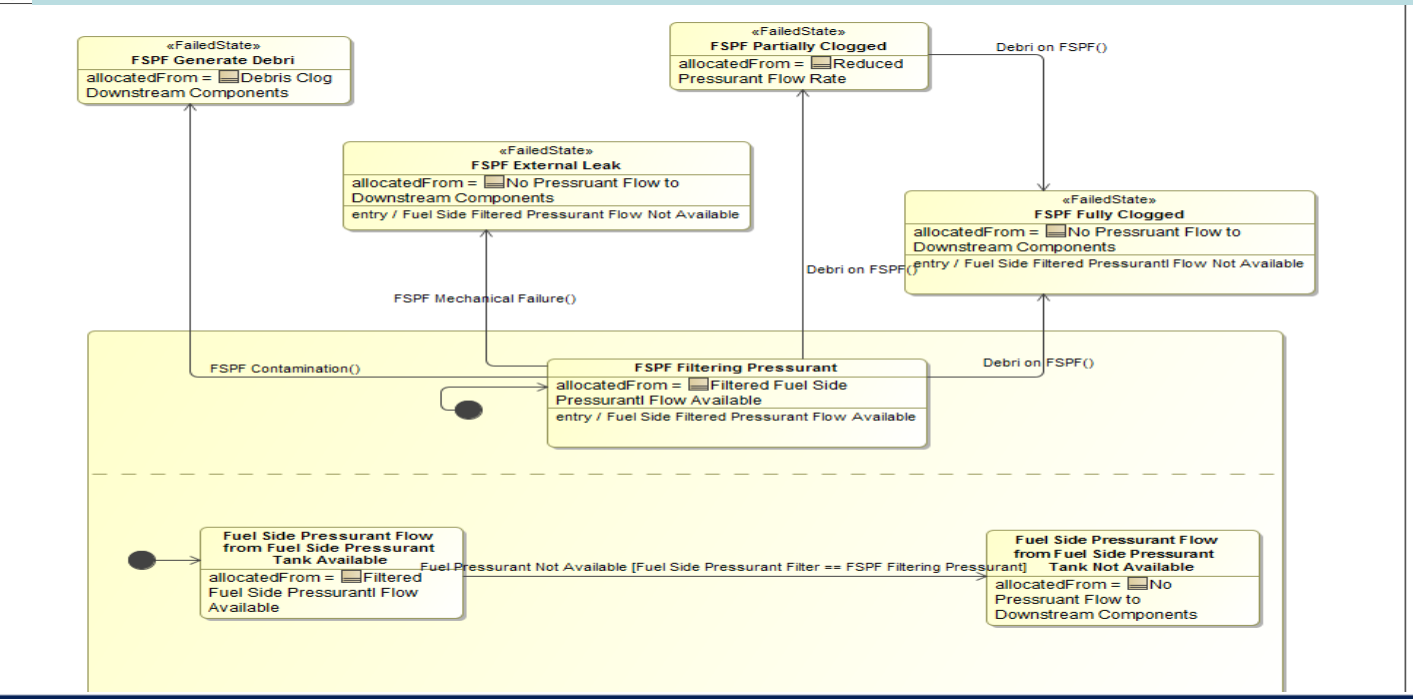


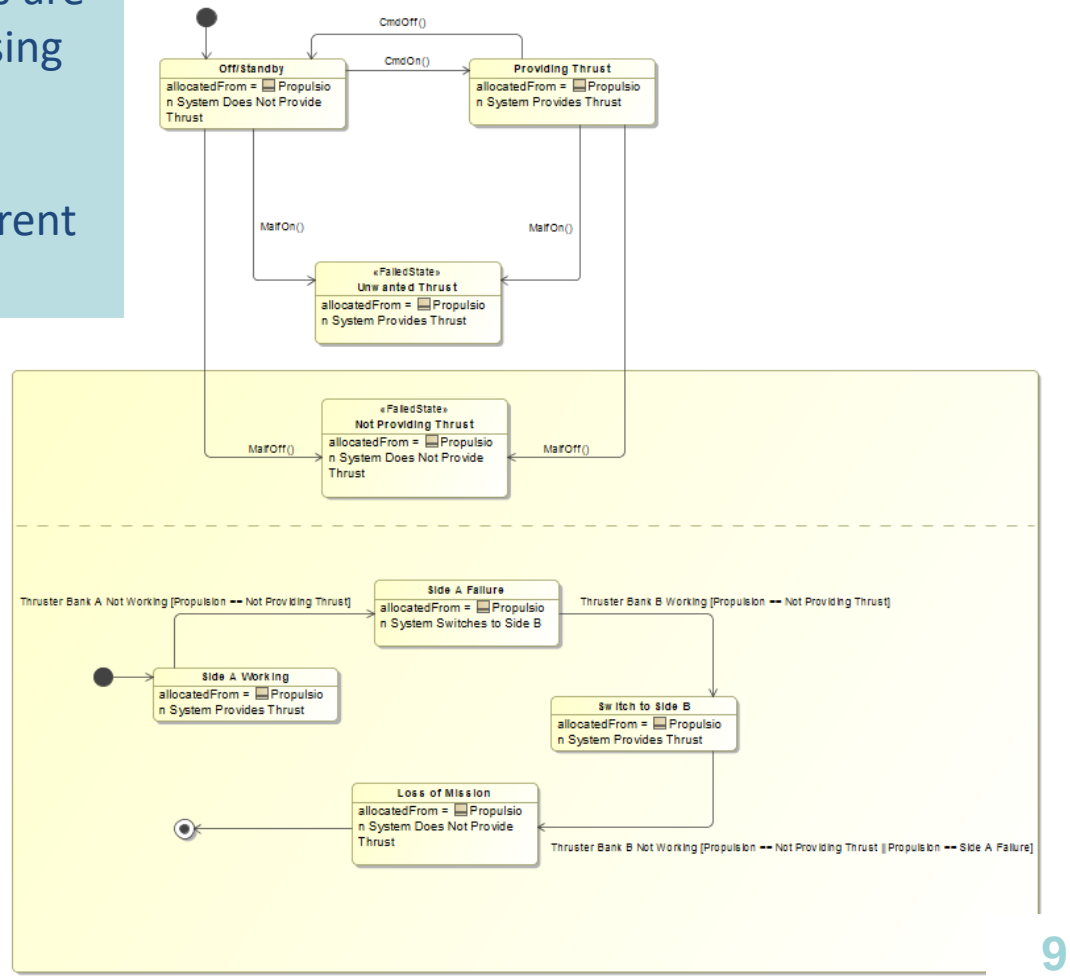
Defining the model required the modeler to use different elements i.e. Block, Operation, Signal, etc.) and different diagrams (i.e. State Machine Diagram).

MBSMAI Phase 1: EUROPA Propulsion Modeling

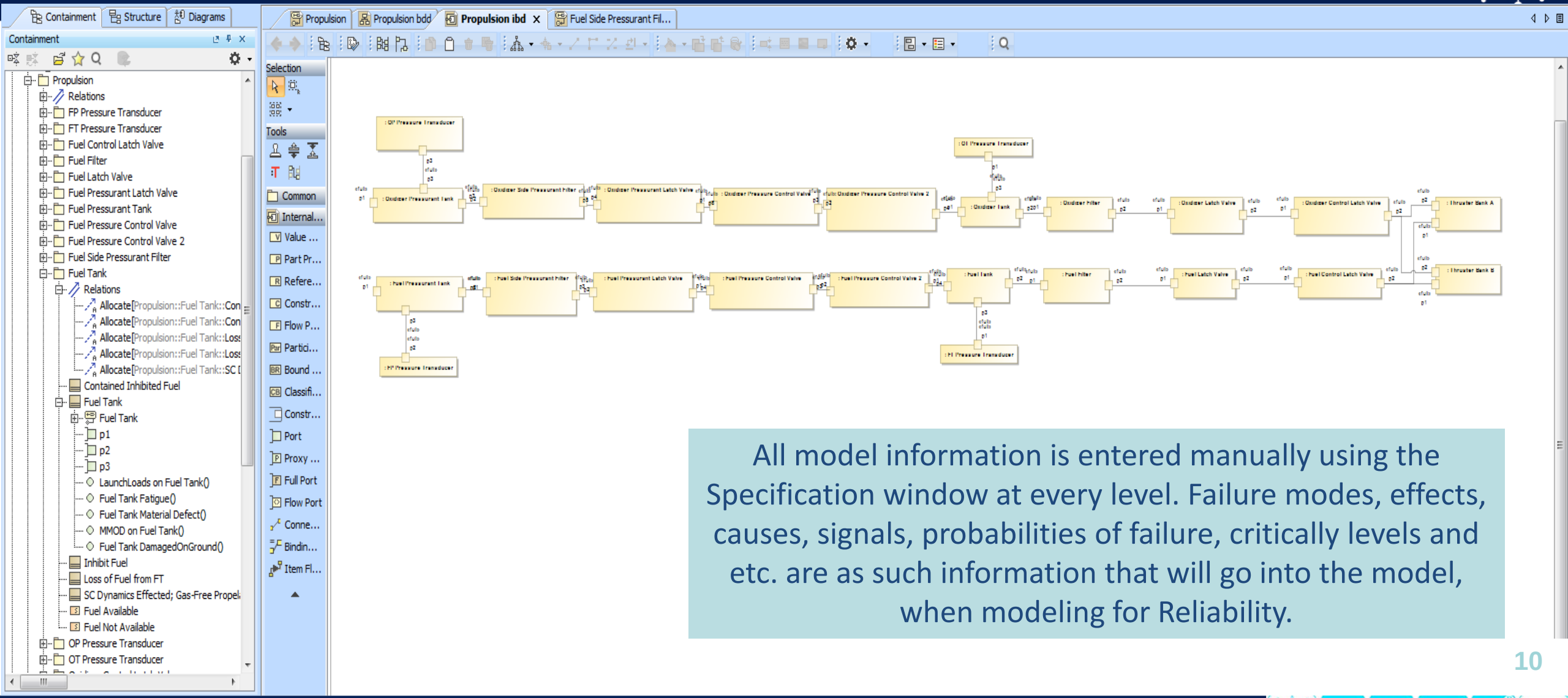
Defining Orthogonal State Machines with appropriate Guard Conditions are required in order to define Redundancy in SysML/MagicDraw when using Tietronox Plugin.

Appropriate signal were defined in order to connect the model at different levels.



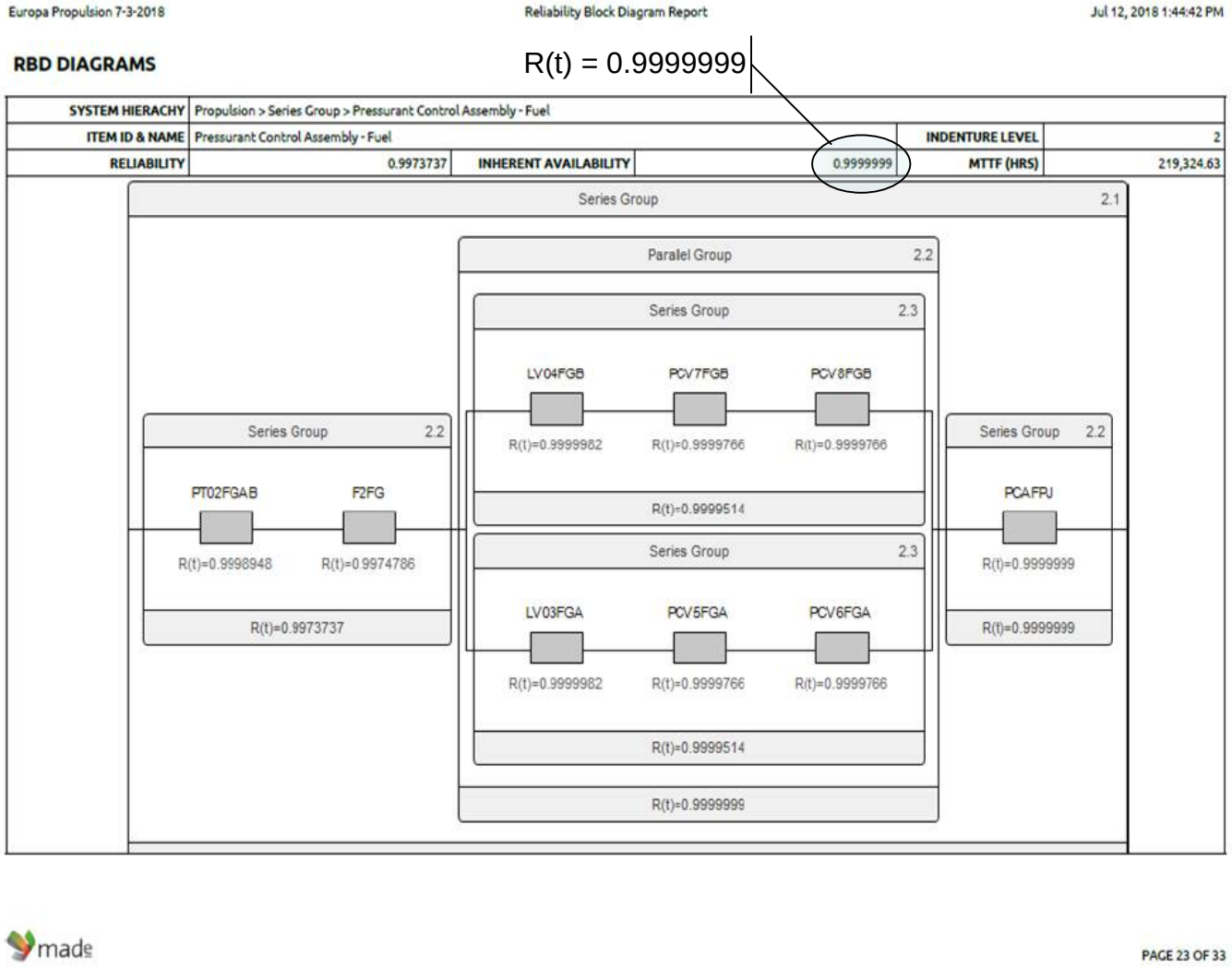


MBSMAI Phase 1: EUROPA Propulsion Modeling



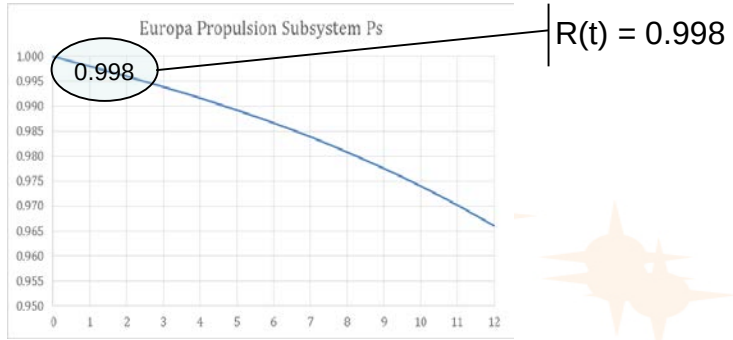
All model information is entered manually using the Specification window at every level. Failure modes, effects, causes, signals, probabilities of failure, critically levels and etc. are as such information that will go into the model, when modeling for Reliability.

MBSMAI Phase 1: EUROPA Model Probability Analysis Evaluation



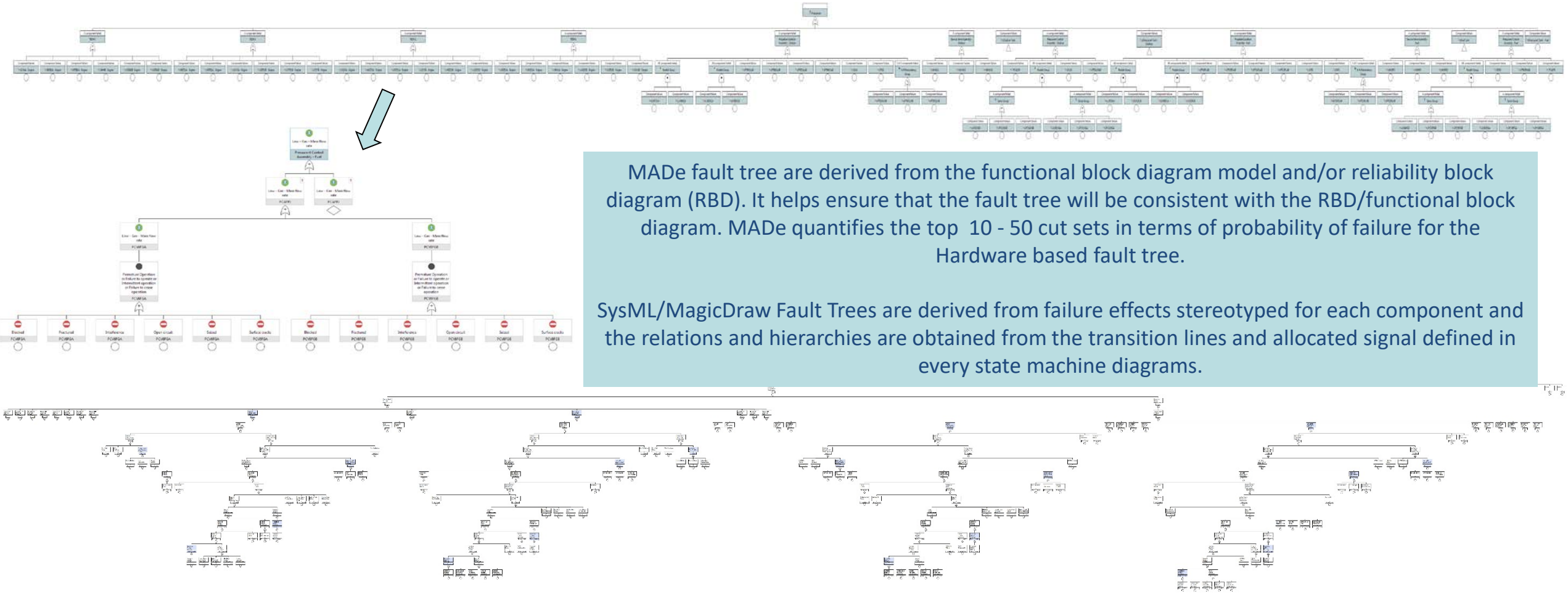
The Probability of failure reported for the entire Europa Propulsion Subsystem at 12 Yrs. (0.0387234) by the MADe fault tree module corresponds to the Probability of Success/Reliability reported by the MADe RBD module (0.9612766).

MADe RBD prediction results matches to about 5 decimal places to the traditional method on a component per component basis



SysML/MagicDraw with Tietronix plugins does not currently support Probability Analysis. However, custom Plugins have been developed by individual enterprises.

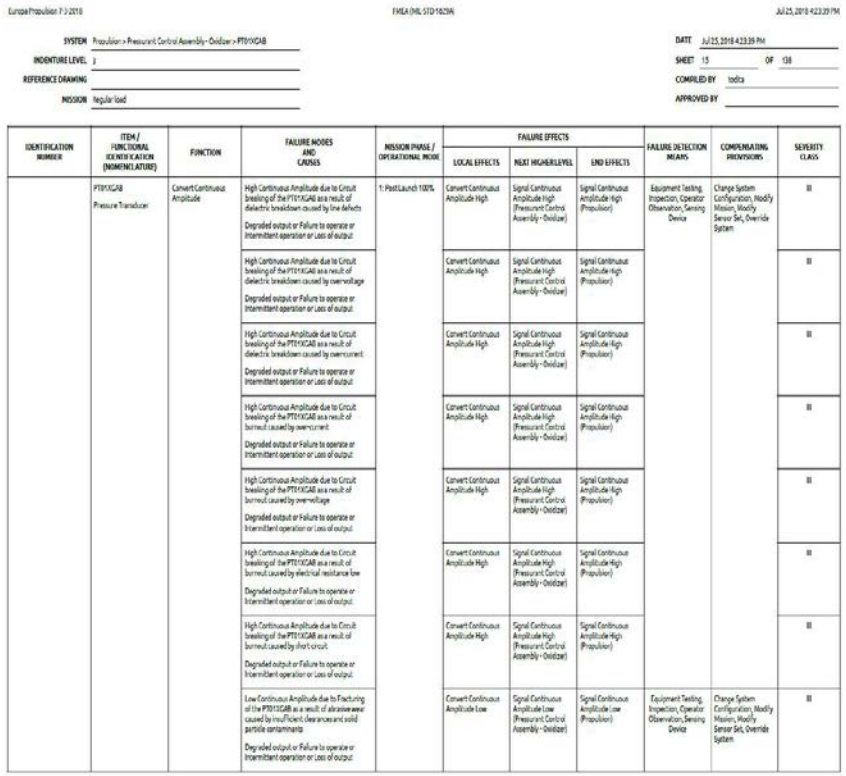
MBSMAI Phase 1: EUROPA Model Fault Tree Evaluation



MADe fault tree are derived from the functional block diagram model and/or reliability block diagram (RBD). It helps ensure that the fault tree will be consistent with the RBD/functional block diagram. MADe quantifies the top 10 - 50 cut sets in terms of probability of failure for the Hardware based fault tree.

SysML/MagicDraw Fault Trees are derived from failure effects stereotyped for each component and the relations and hierarchies are obtained from the transition lines and allocated signal defined in every state machine diagrams.

MBSMAI Phase 1: EUROPA Model Failure Modes Effects and Criticality Analysis (FMECA)



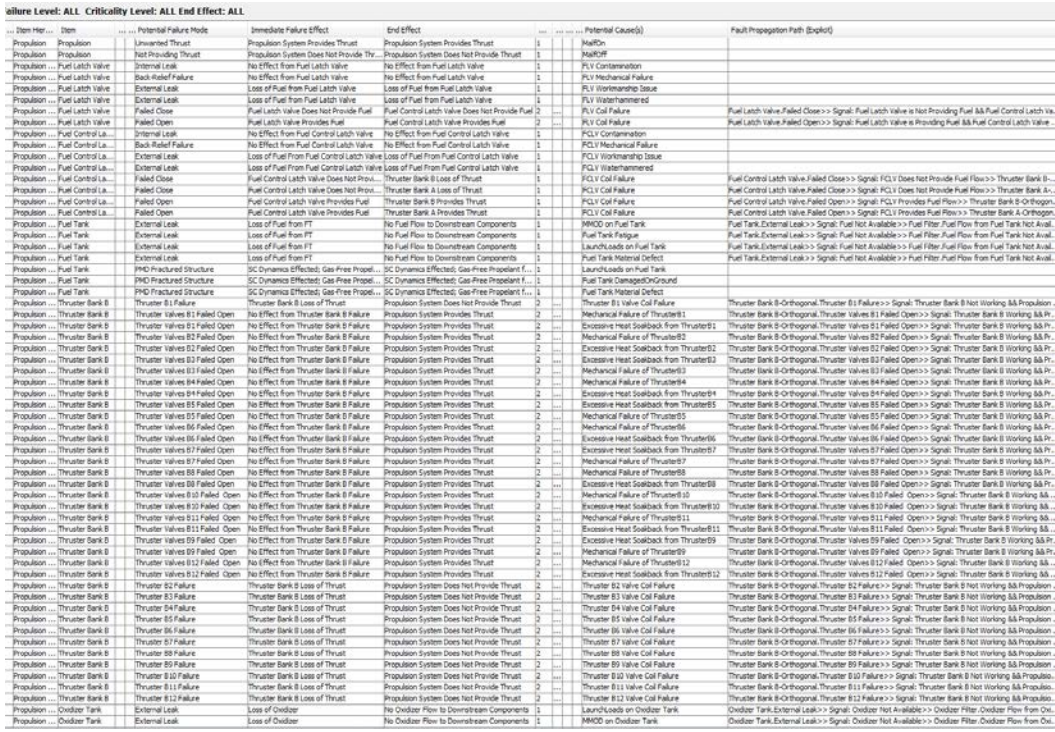
SYSTEM: Propulsion > Pressurant Control Assembly - Oxidizer > PT01XGAB
INDENTURE LEVEL: 3
REFERENCE DRAWING:
MISSION: Regular load
DATE: Jul 25, 2018 4:23:39 PM
SHEET: 15 OF 138
COMPILED BY: todra
APPROVED BY:

IDENTIFICATION NUMBER	ITEM / FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE / OPERATIONAL MODE	FAILURE EFFECTS: LOCAL EFFECTS	FAILURE EFFECTS: NEXT HIGHER LEVEL	FAILURE EFFECTS: END EFFECTS	FAILURE DETECTION MEANS	COMPENSATING PROVISIONS	SEVERITY CLASS
	PT01XGAB Pressure Transducer	Convert Continuous Amplitude	High Continuous Amplitude due to Circuit breaking of the PT01XGAB as a result of dielectric breakdown caused by line defects Degraded output or Failure to operate or Intermittent operation or Loss of output	1: Post Launch 100%	Convert Continuous Amplitude High	Signal Continuous Amplitude High (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)	Equipment Testing, Inspection, Operator Observation, Sensing Device	Change System Configuration, Modify Mission, Modify Sensor Set, Override System	III
			High Continuous Amplitude due to Circuit breaking of the PT01XGAB as a result of dielectric breakdown caused by overvoltage Degraded output or Failure to operate or Intermittent operation or Loss of output		Convert Continuous Amplitude High	Signal Continuous Amplitude High (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			III
			High Continuous Amplitude due to Circuit breaking of the PT01XGAB as a result of dielectric breakdown caused by overcurrent Degraded output or Failure to operate or Intermittent operation or Loss of output		Convert Continuous Amplitude High	Signal Continuous Amplitude High (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			III
			High Continuous Amplitude due to Circuit breaking of the PT01XGAB as a result of burnout caused by overcurrent Degraded output or Failure to operate or Intermittent operation or Loss of output		Convert Continuous Amplitude High	Signal Continuous Amplitude High (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			III
			High Continuous Amplitude due to Circuit breaking of the PT01XGAB as a result of burnout caused by overvoltage Degraded output or Failure to operate or Intermittent operation or Loss of output		Convert Continuous Amplitude High	Signal Continuous Amplitude High (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			III
			High Continuous Amplitude due to Circuit breaking of the PT01XGAB as a result of burnout caused by electrical resistance low Degraded output or Failure to operate or Intermittent operation or Loss of output		Convert Continuous Amplitude High	Signal Continuous Amplitude High (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			III
			High Continuous Amplitude due to Circuit breaking of the PT01XGAB as a result of burnout caused by short circuit Degraded output or Failure to operate or Intermittent operation or Loss of output		Convert Continuous Amplitude High	Signal Continuous Amplitude High (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			III
			Low Continuous Amplitude due to Fracturing of the PT01XGAB as a result of abrasive wear caused by insufficient clearances and solid particle contaminants Degraded output or Failure to operate or Intermittent operation or Loss of output		Convert Continuous Amplitude Low	Signal Continuous Amplitude Low (Pressurant Control Assembly - Oxidizer)	Signal Continuous Amplitude Low (Propulsion)	Equipment Testing, Inspection, Operator Observation, Sensing Device	Change System Configuration, Modify Mission, Modify Sensor Set, Override System	III

FMECAs correlated well to the defined models. Format and content short comings can be overcome manually.

Likelihood of Occurrence	5							
	4							
	3							
	2							
	1							
	< 1							
Criticality Risk Matrix	Severity Category	4	3	3	2/2R	2	1R	1/1S
	Severity Value	1	2	3		4		5
	Relative Severity of Failure Modes							

There currently is no SPF or CIL report from MADe or SysML/MagicDraw.

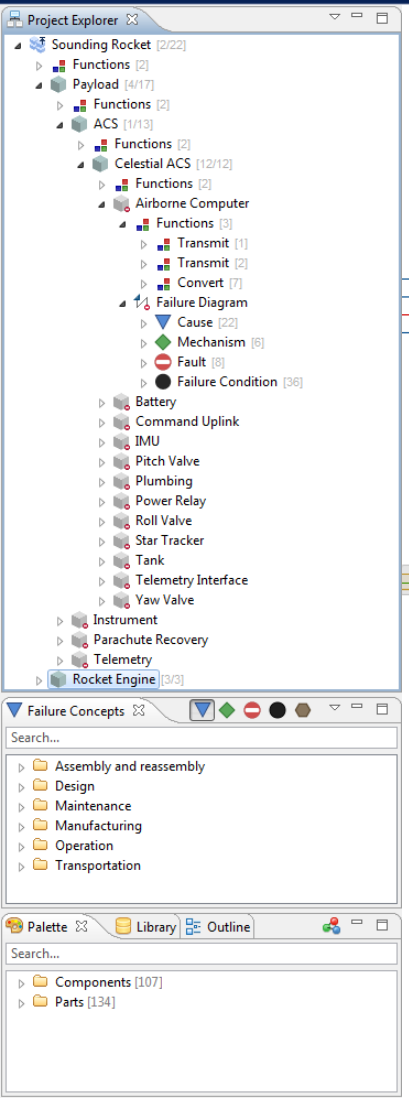


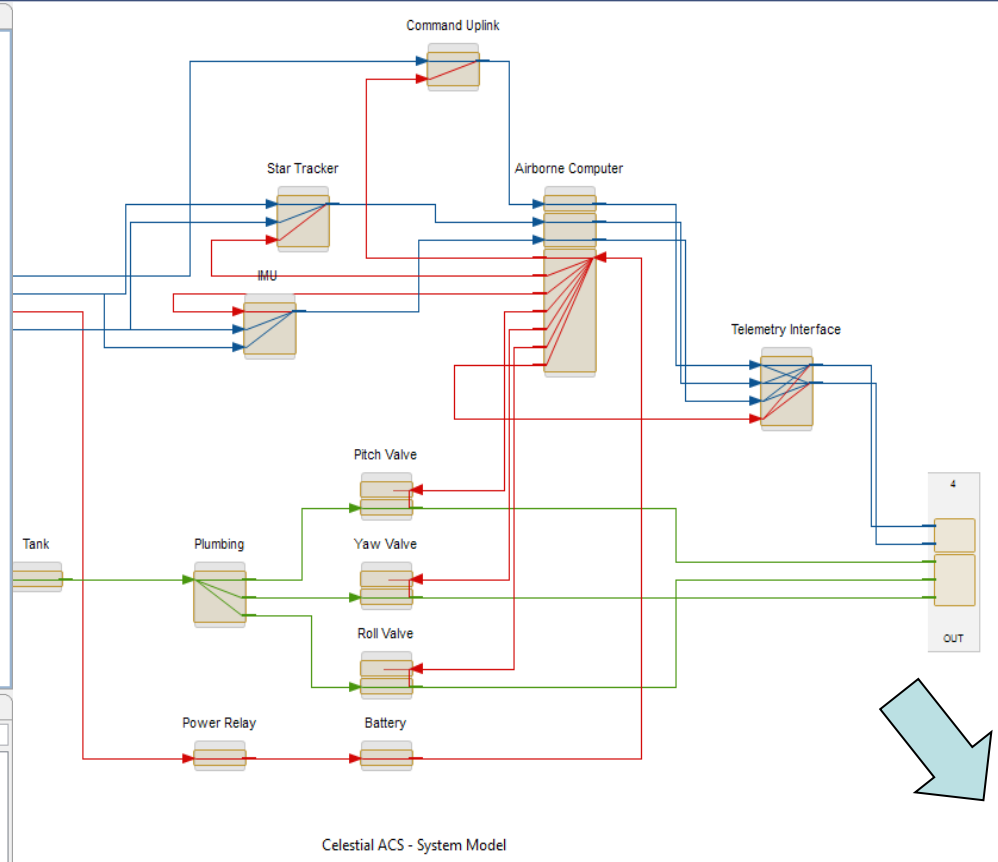
ailure Level: ALL Criticality Level: ALL End Effect: ALL

Item Hier...	Item	Potential Failure Mode	Immediate Failure Effect	End Effect	Potential Cause(s)	Fault Propagation Path (Explicit)
Propulsion	Propulsion	Unwanted Thrust	Propulsion System Provides Thrust	Propulsion System Provides Thrust	MaiFOn	
Propulsion	Propulsion	Not Providing Thrust	Propulsion System Does Not Provide Thr...	Propulsion System Does Not Provide Thrust	MaiFOff	
Propulsion ...	Fuel Latch Valve	Internal Leak	No Effect from Fuel Latch Valve	No Effect from Fuel Latch Valve	FLV Contamination	
Propulsion ...	Fuel Latch Valve	Back-Relief Failure	No Effect from Fuel Latch Valve	No Effect from Fuel Latch Valve	FLV Mechanical Failure	
Propulsion ...	Fuel Latch Valve	External Leak	Loss of Fuel from Fuel Latch Valve	Loss of Fuel from Fuel Latch Valve	FLV Workmanship Issue	
Propulsion ...	Fuel Latch Valve	External Leak	Loss of Fuel from Fuel Latch Valve	Loss of Fuel from Fuel Latch Valve	FLV Waterhammered	
Propulsion ...	Fuel Latch Valve	Failed Close	Fuel Latch Valve Does Not Provide Fuel	Fuel Control Latch Valve Does Not Provide Fuel	FLV Coil Failure	Fuel Latch Valve.Failed Close>> Signal: Fuel Latch Valve is Not Providing Fuel && Fuel Control Latch Va...
Propulsion ...	Fuel Latch Valve	Failed Open	Fuel Latch Valve Provides Fuel	Fuel Control Latch Valve Provides Fuel	FLV Coil Failure	Fuel Latch Valve.Failed Open>> Signal: Fuel Latch Valve is Providing Fuel && Fuel Control Latch Valve ...
Propulsion ...	Fuel Control La...	Internal Leak	No Effect from Fuel Control Latch Valve	No Effect from Fuel Control Latch Valve	FCLV Contamination	
Propulsion ...	Fuel Control La...	Back-Relief Failure	No Effect from Fuel Control Latch Valve	No Effect from Fuel Control Latch Valve	FCLV Mechanical Failure	
Propulsion ...	Fuel Control La...	External Leak	Loss of Fuel From Fuel Control Latch Valve	Loss of Fuel From Fuel Control Latch Valve	FCLV Workmanship Issue	
Propulsion ...	Fuel Control La...	External Leak	Loss of Fuel From Fuel Control Latch Valve	Loss of Fuel From Fuel Control Latch Valve	FCLV Waterhammered	
Propulsion ...	Fuel Control La...	Failed Close	Fuel Control Latch Valve Does Not Provi...	Thruster Bank B Loss of Thrust	FCLV Coil Failure	Fuel Control Latch Valve.Failed Close>> Signal: FCLV Does Not Provide Fuel Flow>> Thruster Bank B-...
Propulsion ...	Fuel Control La...	Failed Close	Fuel Control Latch Valve Does Not Provi...	Thruster Bank A Loss of Thrust	FCLV Coil Failure	Fuel Control Latch Valve.Failed Close>> Signal: FCLV Does Not Provide Fuel Flow>> Thruster Bank A-...
Propulsion ...	Fuel Control La...	Failed Open	Fuel Control Latch Valve Provides Fuel	Thruster Bank B Provides Thrust	FCLV Coil Failure	Fuel Control Latch Valve.Failed Open>> Signal: FCLV Provides Fuel Flow>> Thruster Bank B-Orthogon...
Propulsion ...	Fuel Control La...	Failed Open	Fuel Control Latch Valve Provides Fuel	Thruster Bank A Provides Thrust	FCLV Coil Failure	Fuel Control Latch Valve.Failed Open>> Signal: FCLV Provides Fuel Flow>> Thruster Bank A-Orthogon...
Propulsion ...	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	MMOD on Fuel Tank	Fuel Tank.External Leak>> Signal: Fuel Not Available>> Fuel Filter.Fuel Flow from Fuel Tank Not Avail...
Propulsion ...	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	Fuel Tank Fatigue	Fuel Tank.External Leak>> Signal: Fuel Not Available>> Fuel Filter.Fuel Flow from Fuel Tank Not Avail...
Propulsion ...	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	LaunchLoads on Fuel Tank	Fuel Tank.External Leak>> Signal: Fuel Not Available>> Fuel Filter.Fuel Flow from Fuel Tank Not Avail...
Propulsion ...	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	Fuel Tank Material Defect	Fuel Tank.External Leak>> Signal: Fuel Not Available>> Fuel Filter.Fuel Flow from Fuel Tank Not Avail...
Propulsion ...	Fuel Tank	PMD Fractured Structure	SC Dynamics Effected; Gas-Free Propel...	SC Dynamics Effected; Gas-Free Propellant F...	LaunchLoads on Fuel Tank	
Propulsion ...	Fuel Tank	PMD Fractured Structure	SC Dynamics Effected; Gas-Free Propel...	SC Dynamics Effected; Gas-Free Propellant F...	Fuel Tank DamagedOnGround	
Propulsion ...	Fuel Tank	PMD Fractured Structure	SC Dynamics Effected; Gas-Free Propel...	SC Dynamics Effected; Gas-Free Propellant F...	Fuel Tank Material Defect	
Propulsion ...	Thruster Bank B	Thruster B1 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B1 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B1 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster Valves B1 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B1	Thruster Bank B-Orthogonal.Thruster Valves B1 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B1 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B1	Thruster Bank B-Orthogonal.Thruster Valves B1 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B2 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B2	Thruster Bank B-Orthogonal.Thruster Valves B2 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B2 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B2	Thruster Bank B-Orthogonal.Thruster Valves B2 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B3 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B3	Thruster Bank B-Orthogonal.Thruster Valves B3 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B3 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B3	Thruster Bank B-Orthogonal.Thruster Valves B3 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B4 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B4	Thruster Bank B-Orthogonal.Thruster Valves B4 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B4 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B4	Thruster Bank B-Orthogonal.Thruster Valves B4 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B5 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B5	Thruster Bank B-Orthogonal.Thruster Valves B5 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B5 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B5	Thruster Bank B-Orthogonal.Thruster Valves B5 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B6 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B6	Thruster Bank B-Orthogonal.Thruster Valves B6 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B6 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B6	Thruster Bank B-Orthogonal.Thruster Valves B6 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B7 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B7	Thruster Bank B-Orthogonal.Thruster Valves B7 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B7 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B7	Thruster Bank B-Orthogonal.Thruster Valves B7 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B8 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B8	Thruster Bank B-Orthogonal.Thruster Valves B8 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B8 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B8	Thruster Bank B-Orthogonal.Thruster Valves B8 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B10 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B10	Thruster Bank B-Orthogonal.Thruster Valves B10 Failed Open>> Signal: Thruster Bank B Working && ...
Propulsion ...	Thruster Bank B	Thruster Valves B10 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B10	Thruster Bank B-Orthogonal.Thruster Valves B10 Failed Open>> Signal: Thruster Bank B Working && ...
Propulsion ...	Thruster Bank B	Thruster Valves B11 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B11	Thruster Bank B-Orthogonal.Thruster Valves B11 Failed Open>> Signal: Thruster Bank B Working && ...
Propulsion ...	Thruster Bank B	Thruster Valves B11 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B11	Thruster Bank B-Orthogonal.Thruster Valves B11 Failed Open>> Signal: Thruster Bank B Working && ...
Propulsion ...	Thruster Bank B	Thruster Valves B9 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B9	Thruster Bank B-Orthogonal.Thruster Valves B9 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B9 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B9	Thruster Bank B-Orthogonal.Thruster Valves B9 Failed Open>> Signal: Thruster Bank B Working && Pr...
Propulsion ...	Thruster Bank B	Thruster Valves B12 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Mechanical Failure of Thruster B12	Thruster Bank B-Orthogonal.Thruster Valves B12 Failed Open>> Signal: Thruster Bank B Working && ...
Propulsion ...	Thruster Bank B	Thruster Valves B12 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	Excessive Heat Soakback from Thruster B12	Thruster Bank B-Orthogonal.Thruster Valves B12 Failed Open>> Signal: Thruster Bank B Working && ...
Propulsion ...	Thruster Bank B	Thruster B2 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B2 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B2 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B3 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B3 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B3 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B4 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B4 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B4 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B5 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B5 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B5 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B6 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B6 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B6 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B7 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B7 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B7 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B8 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B8 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B8 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B9 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B9 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B9 Failure>> Signal: Thruster Bank B Not Working && Propulsion ...
Propulsion ...	Thruster Bank B	Thruster B10 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B10 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B10 Failure>> Signal: Thruster Bank B Not Working && Propulsio...
Propulsion ...	Thruster Bank B	Thruster B11 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B11 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B11 Failure>> Signal: Thruster Bank B Not Working && Propulsio...
Propulsion ...	Thruster Bank B	Thruster B12 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	Thruster B12 Valve Coil Failure	Thruster Bank B-Orthogonal.Thruster B12 Failure>> Signal: Thruster Bank B Not Working && Propulsio...
Propulsion ...	Oxidizer Tank	External Leak	Loss of Oxidizer	No Oxidizer Flow to Downstream Components	LaunchLoads on Oxidizer Tank	Oxidizer Tank.External Leak>> Signal: Oxidizer Not Available>> Oxidizer Filter.Oxidizer Flow from Oxi...
Propulsion ...	Oxidizer Tank	External Leak	Loss of Oxidizer	No Oxidizer Flow to Downstream Components	MMOD on Oxidizer Tank	Oxidizer Tank.External Leak>> Signal: Oxidizer Not Available>> Oxidizer Filter.Oxidizer Flow from Oxi...

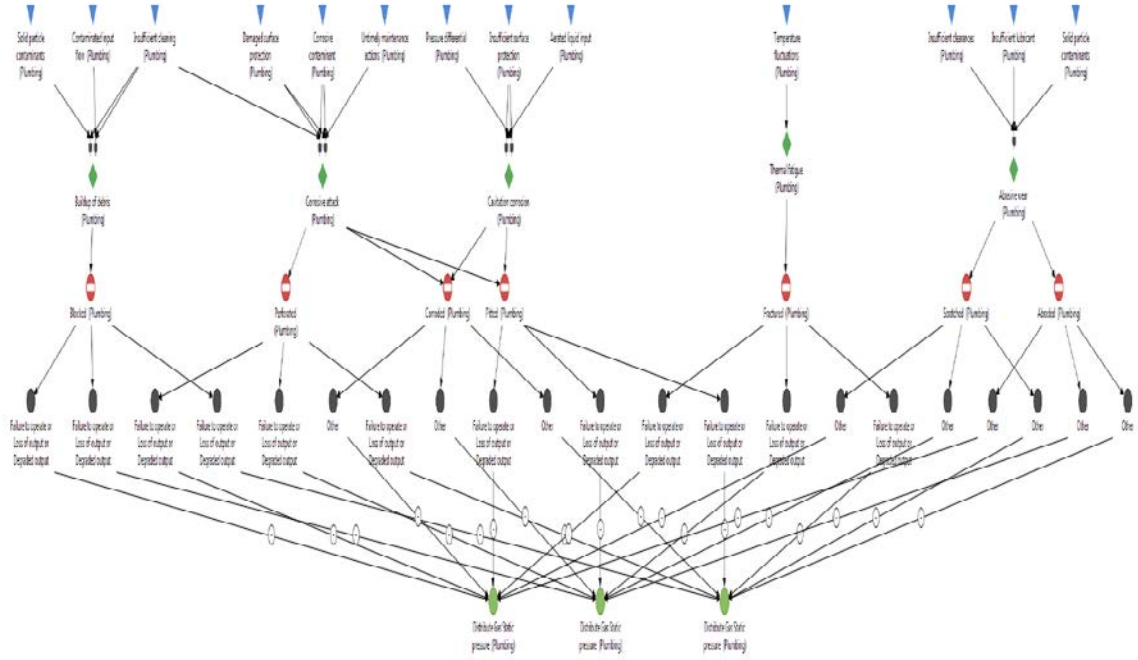
146	**Oxidizer Pressurant Tank Pressure Transducer (PT01XGAB)**	Drift	Component random failure	All	Information only, reduced visibility into pressurant system status	System operates nominally	Ground trending	No response necessary?		2		.	146
147	*Oxidizer Pressurant Tank Pressure Transducer (PT01XGAB)*	No output or False high/low	Component random failure	All	Information only, loss of pressurant system status	System operates nominally	Ground trending	No response necessary?		2		.	147
148	*Oxidizer Pressurant Tank Pressure Transducer (PT01XGAB)*	External leak	Mechanical failure	Launch, Cruise, JOI	Uncontrolled loss of pressurant (eventual complete mission ending loss of pressurant), cannot supply adequate flow rate for thrusting	Loss of mission	Detection by GNC through torque impact	No effective mitigation		6		SPF	148
149	*Oxidizer Pressurant Tank Pressure Transducer (PT01XGAB)*	*External leak*	*Mechanical failure*	Tour	*Uncontrolled loss of pressurant (eventual complete mission ending loss of pressurant), cannot supply adequate flow rate for thrusting*	Loss of remainder of mission	Detection by GNC through torque impact	No effective mitigation		5		SPF	149

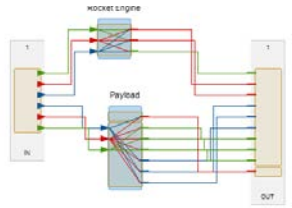
MBSMAI Phase 1: Sounding Rocket Modeling



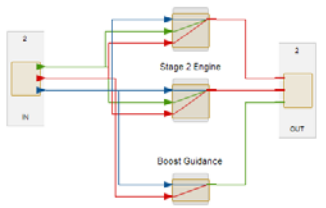


Celestial ACS - System Model

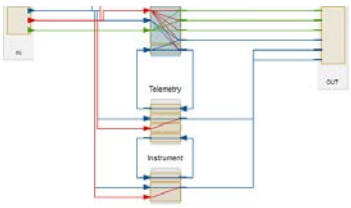




Sounding Rocket - System Model

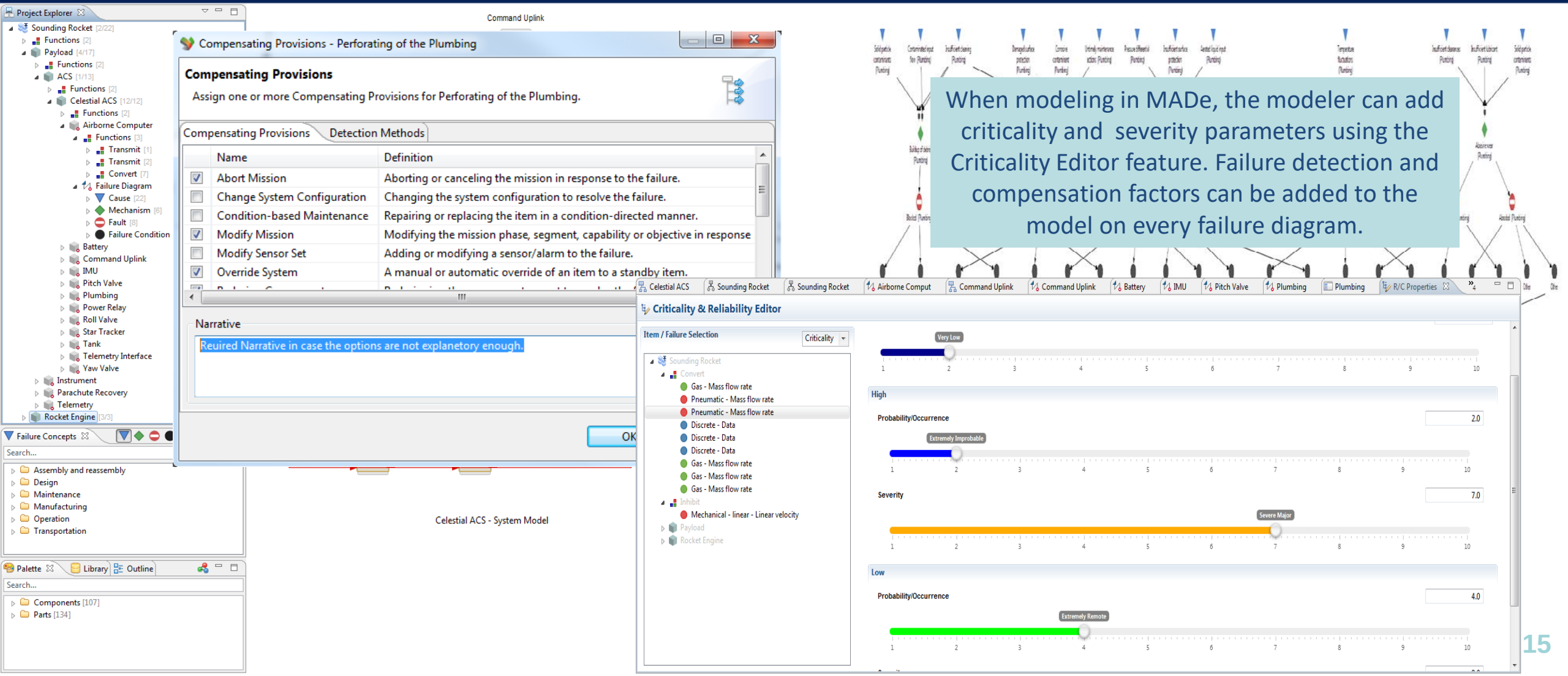


Rocket Engine - System Model



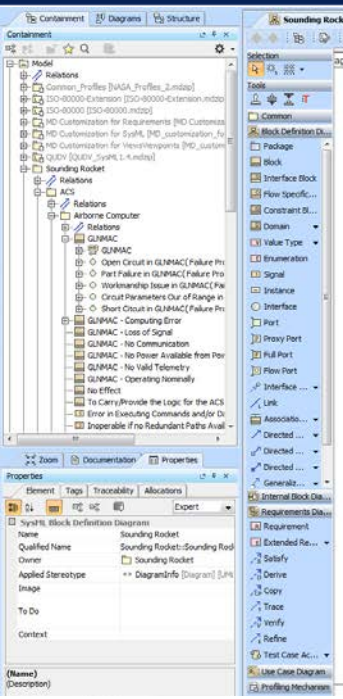
Payload - System Model

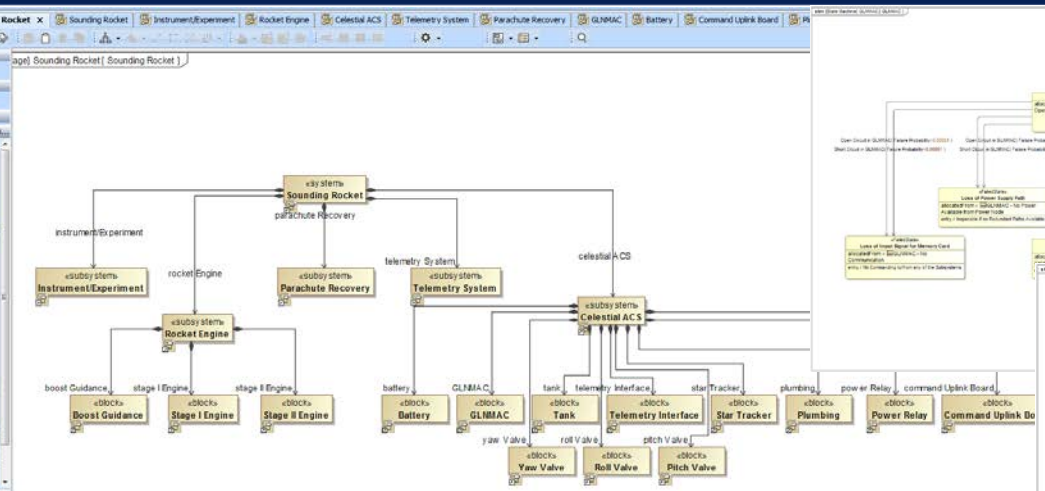
MBSMAI Phase 1: Sounding Rocket Modeling

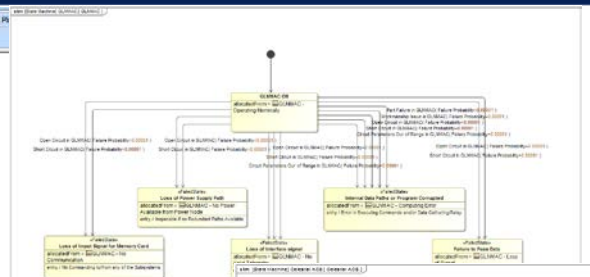


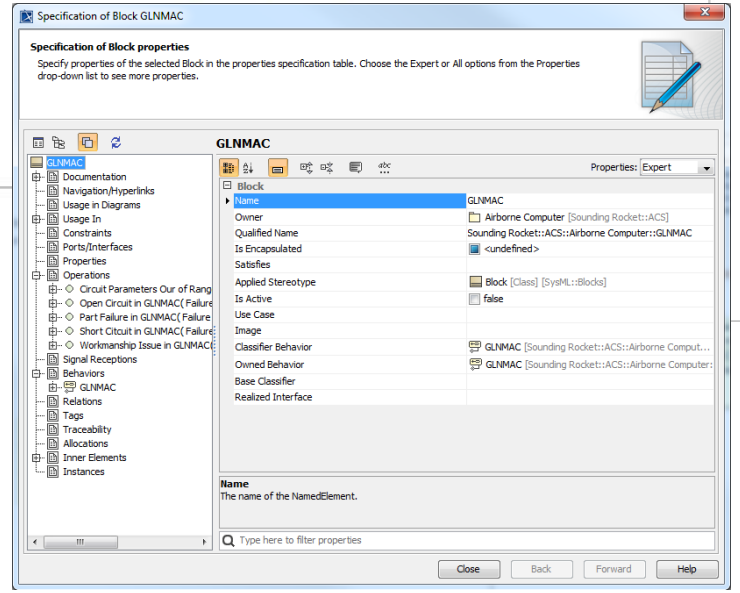
When modeling in MADe, the modeler can add criticality and severity parameters using the Criticality Editor feature. Failure detection and compensation factors can be added to the model on every failure diagram.

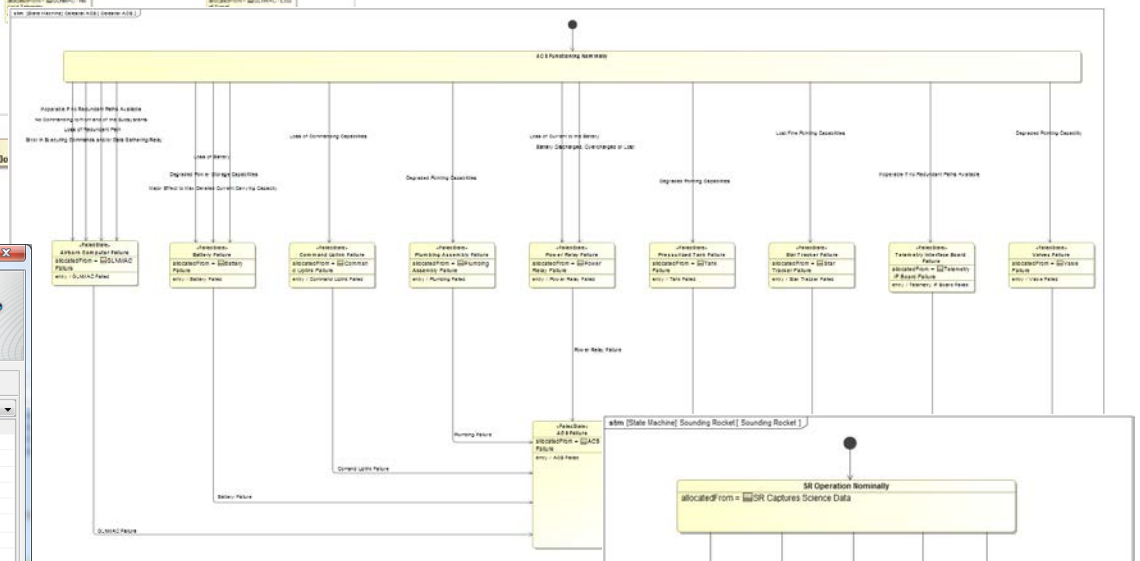
MBSMAI Phase 1: Sounding Rocket Modeling

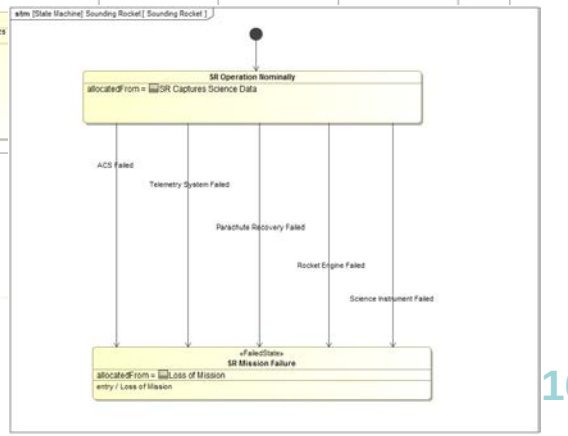








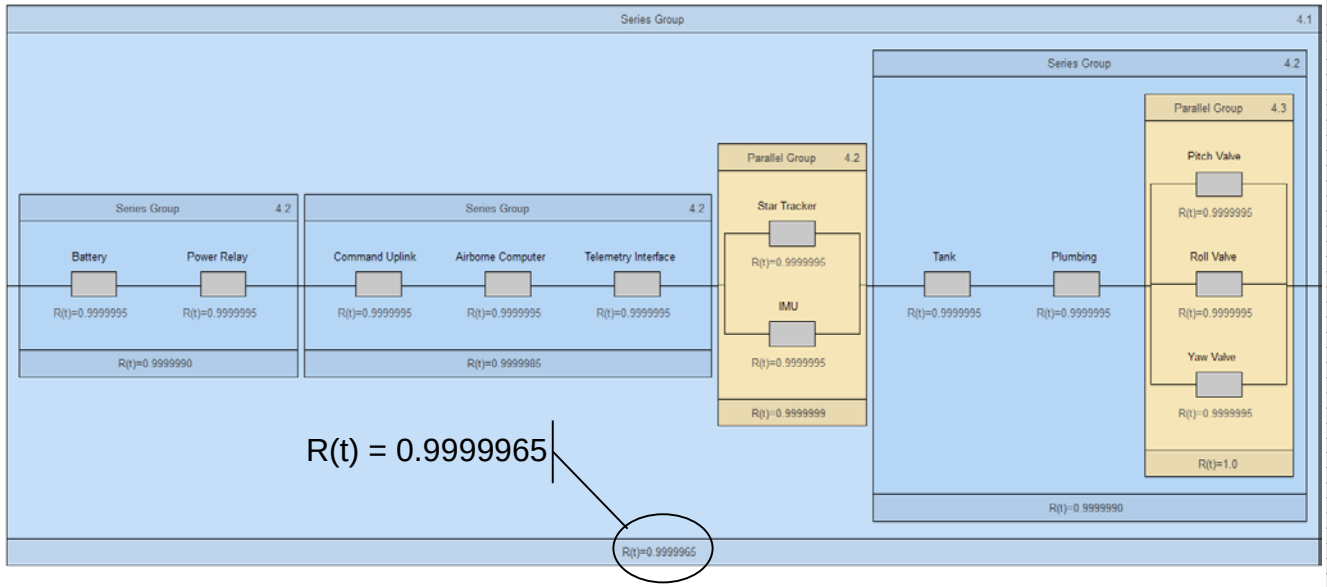




State Machines are the core of the model when modeling in SysML/MagicDraw for Tietronix and we need a state machine at every level.

All model information was entered manually using the Specification window at every level. Failure modes, effects, causes, signals, probabilities of failure, critically levels and etc. are as such information that will go into the model, when modeling for Reliability.

MBSMAI Phase 1: Sounding Rocket Probability Analysis Evaluation



ACS

Subsystem / Component Name	Qty	Model	MTTF/ Char Life / Lognormal Mean	Failure Rate / Shape / Lognormal Std Dev	Relative Duty Cycle	Component Reliability (for time in years) 5.70E-05	1	1	Redundancy Configuration	Subsytem Reliability (for time in years) 5.70E-05	1	1
Star Trackers	1			**0.00000017**	100%	0.999999915	0.998511908	0.998511908	Single String	0.999999915	0.998511908	0.998511908
Star Tracker Head (Mini Star Tracker)	1	E	38461538.46	0.000000026		0.999999987	0.999772266	0.999772266	Single String	0.999999915	0.998511908	0.998511908
Star Tracker Processor (Mini Star Tracker)	1	E	6944444.444	0.000000144		0.999999928	0.998739355	0.998739355				
Command Uplink	1			**2.05538E-07**	100%	0.999999897	0.998201111	0.998201111	Single String	0.999999897	0.998201111	0.998201111
Avionics Board - Medium Complexity	1	E	4865292.2	2.05538E-07		0.999999897	0.998201111	0.998201111				
Telemetry Interface	1				100%	0.999999726	0.995210152	0.995210152	Single String	0.999999726	0.995210152	0.995210152
Avionics Board - High Complexity	1	E	1824484.5	5.481E-07		0.999999726	0.995210152	0.995210152	Single String	0.999999726	0.995210152	0.995210152
IMU	1				100%	0.999999989	0.999799719	0.999799719	Single String	0.999999989	0.999799719	0.999799719
NG Scalable SIRU	1	E	43734201.02	2.28654E-08		0.999999989	0.999799719	0.999799719	Single String	0.999999989	0.999799719	0.999799719
Airborne Computer	1			**5.55045E-07**	100%	0.999999723	0.995149609	0.995149609	Single String	0.999999723	0.995149609	0.995149609
Avionics Board - High Complexity	1	E	1824484.5	5.481E-07		0.999999726	0.995210152	0.995210152	Single String	0.999999723	0.995149609	0.995149609
Memory	1	E	218986859.7	4.56648E-09		0.999999998	0.999959998	0.999959998				
Power control circuit	1	E	420466859.9	2.37831E-09		0.999999999	0.999979166	0.999979166				
Power	1				100%	0.999999873	0.997776719	0.997776719	Single String	0.999999873	0.997776719	0.997776719
Relays	1	E	71013886.22	1.40818E-08		0.999999993	0.999876651	0.999876651	Single String	0.999999873	0.997776719	0.997776719
Battery in LEO (the entire battery; not technology specific)	1	E	4166666.667	0.00000024		0.99999988	0.997899808	0.997899808				
Delta V	1				100%	0.999999697	0.994693998	0.994693998	Single String	0.999999697	0.994693998	0.994693998
Tank	1	E	5959577.615	1.67797E-07		0.999999916	0.998531177	0.998531177	Single String	0.999999697	0.994693998	0.994693998
Plumbing	1	E	61103138.13	1.63658E-08		0.999999992	0.999856646	0.999856646				
Thruster Valve	3	E	7089554.5	1.41053E-07		0.999999789	0.9963	0.9963				

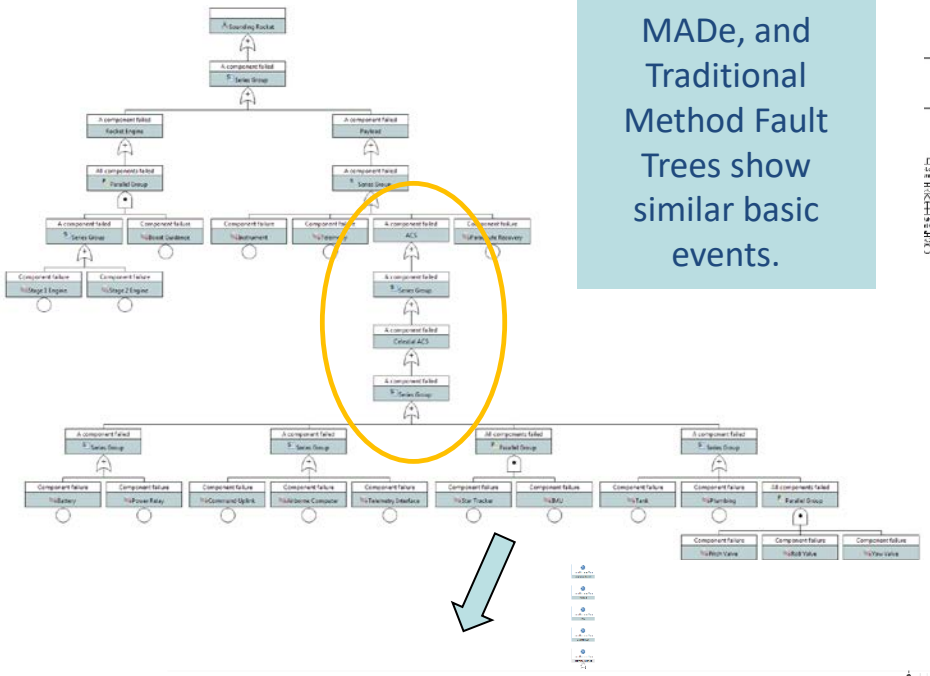
R(t) = 0.999998923

ACS Total			
	0.000057 years	1 years	1 years
Max Redundancy	0.99999882	0.97951332	0.97951332
Min Redundancy	0.999998923	0.98127853	0.98127853

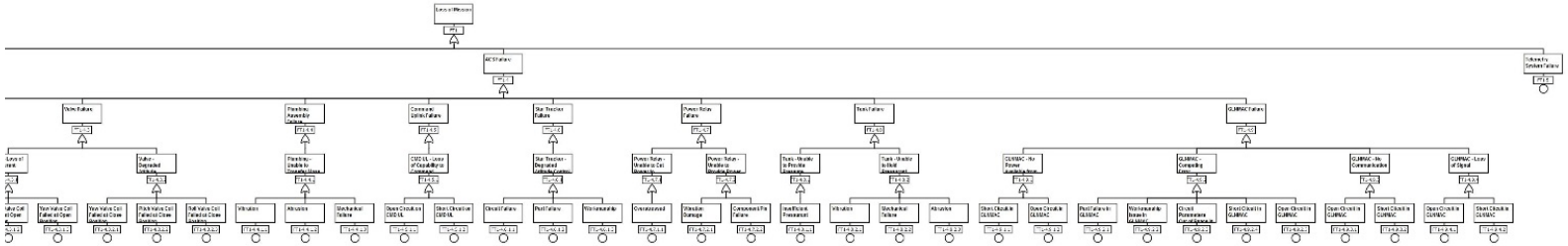
The Probability of failure reported for the Sounding Rocket MADe model corresponds to the Probability of Success/Reliability of the traditional method at the component level; mission life probabilities also compare favorably if the duration and duty cycles assumed for each are the same.

SysML/MagicDraw with Tietronix plugins does not currently support Probability Analysis. However, custom Plugins have been developed by individual enterprises.

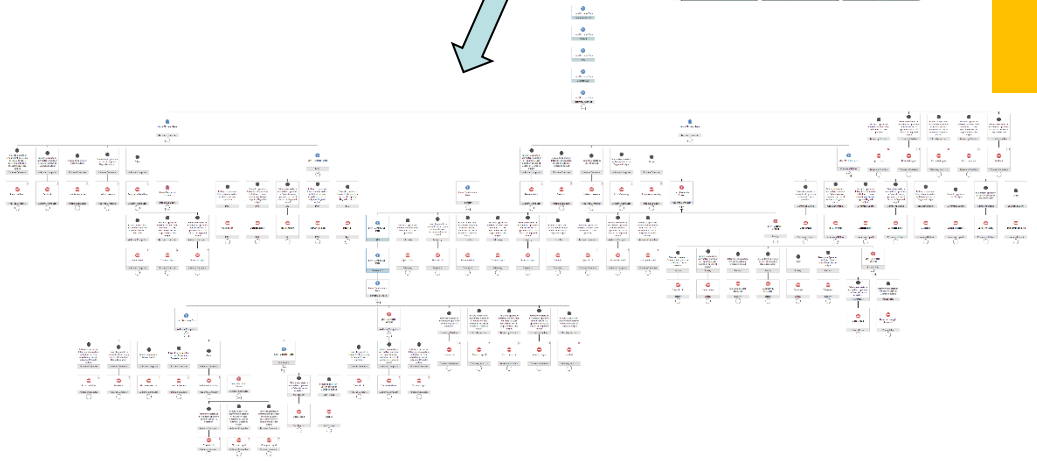
MBSMAI Phase 1: Sounding Rocket Fault Tree Evaluation



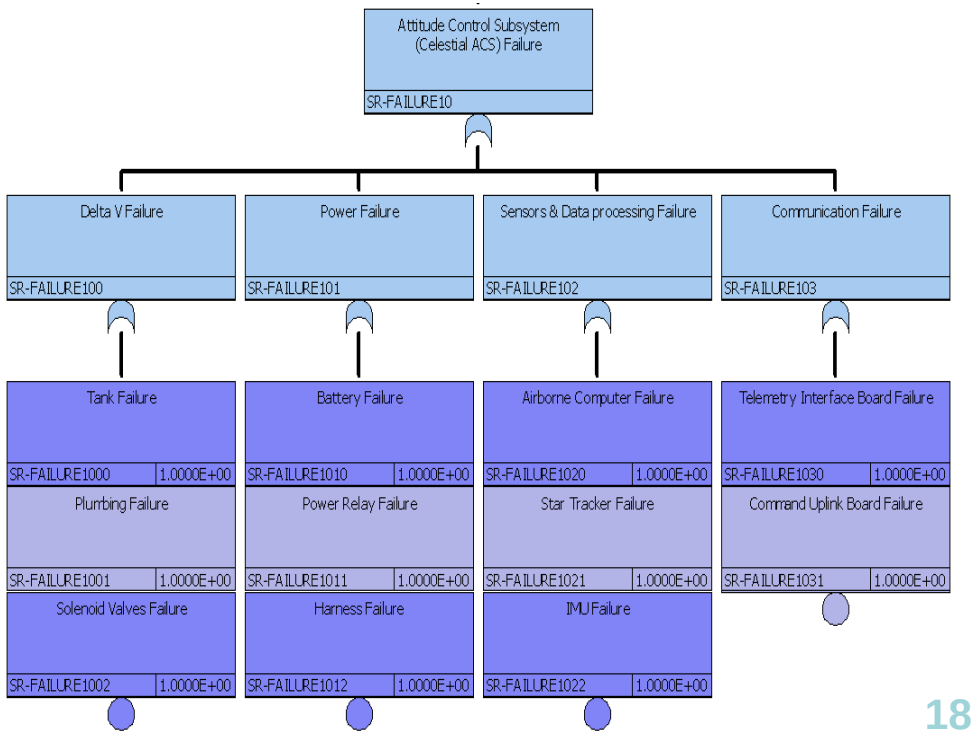
MADe, and Traditional Method Fault Trees show similar basic events.



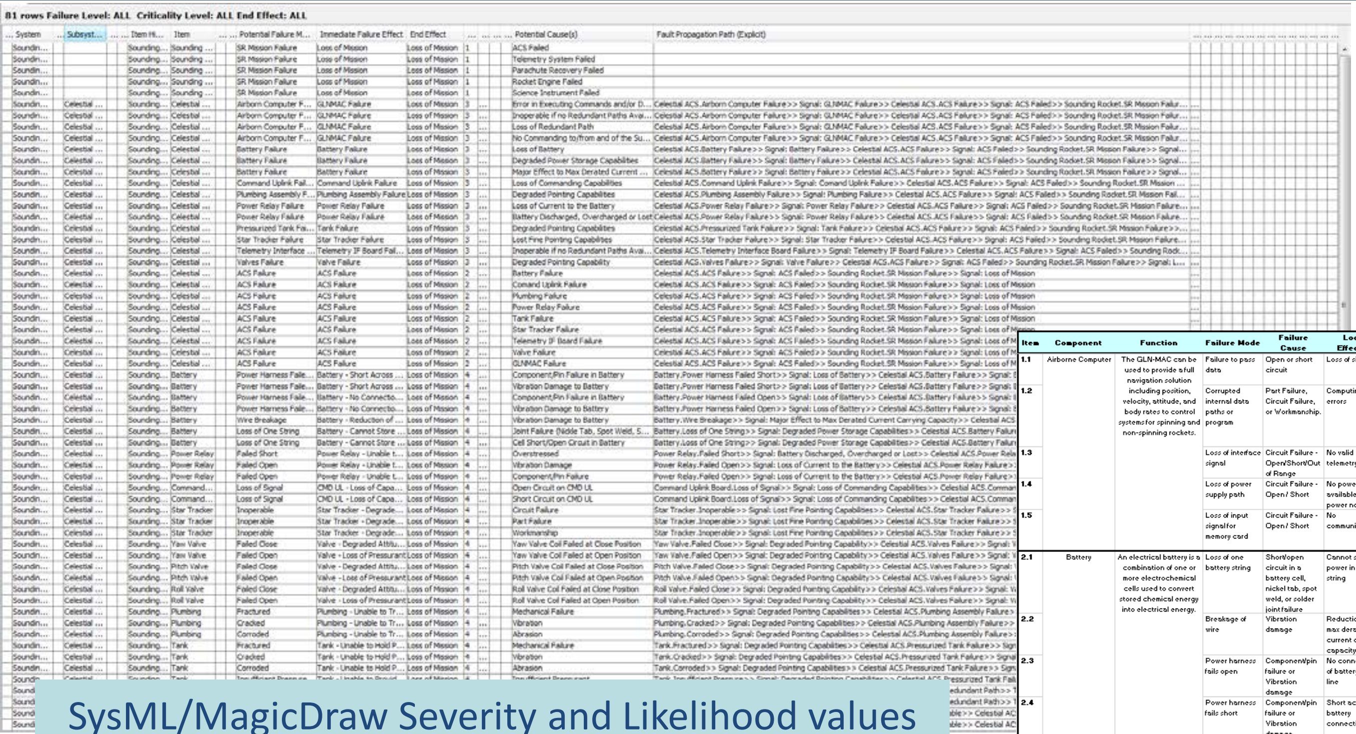
SysML/MagicDraw Fault Trees also contain Boolean logic errors (i.e., events decomposed into to subordinate events without a combining logic or gate, and logic gates with only one input) but perform accurate Boolean math.

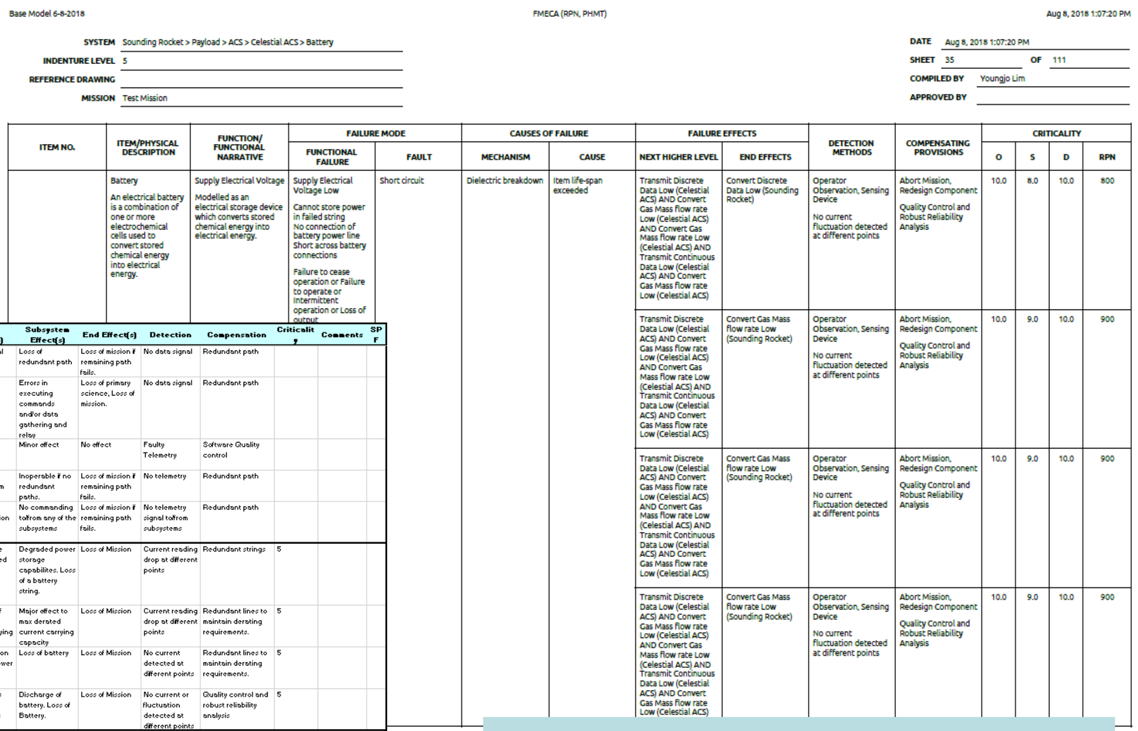


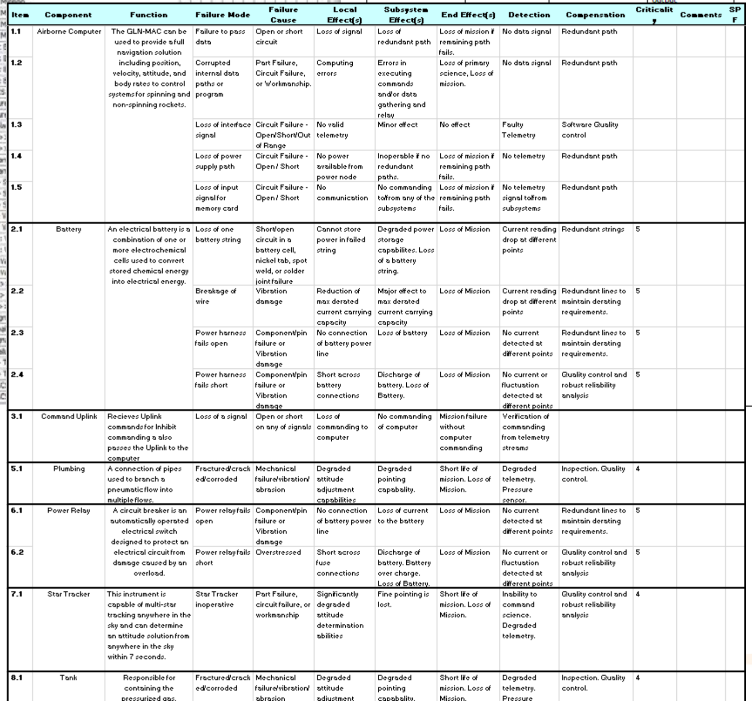
SysML/MagicDraw FT output from the Tietronix Plugin shows immediate Failure Causes as the basic event not hardware failure since State Diagrams were optimized for the FMECA.



MBSMAI Phase 1: Sounding Rocket Model Failure Modes Effects and Criticality Analysis (FMECA) Evaluation



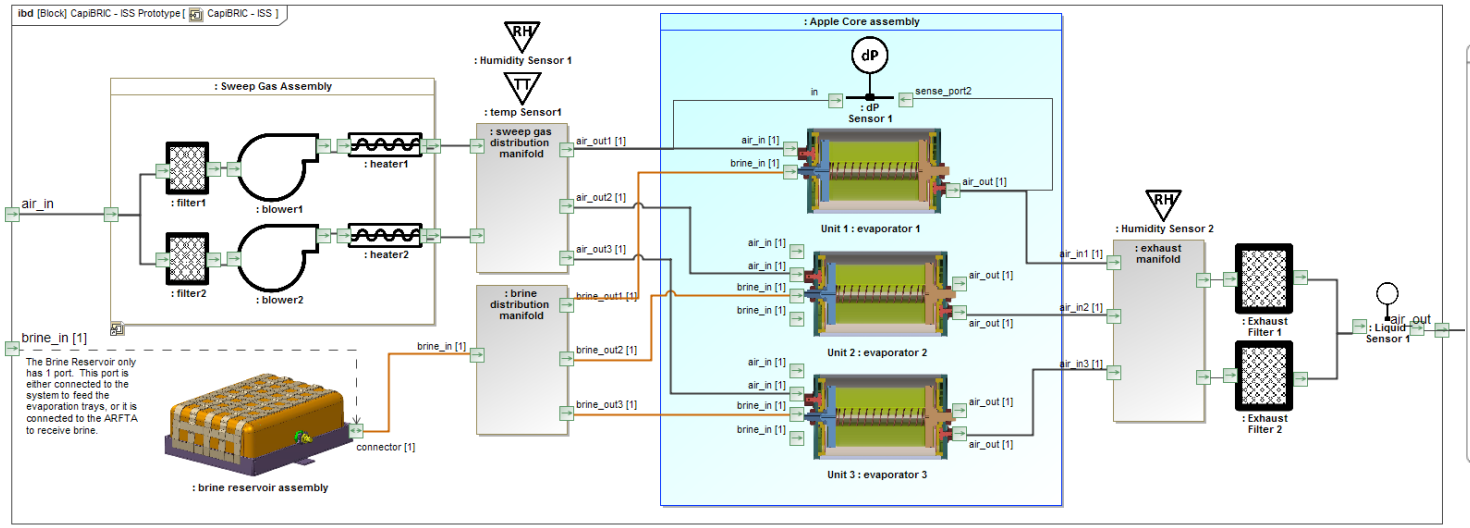


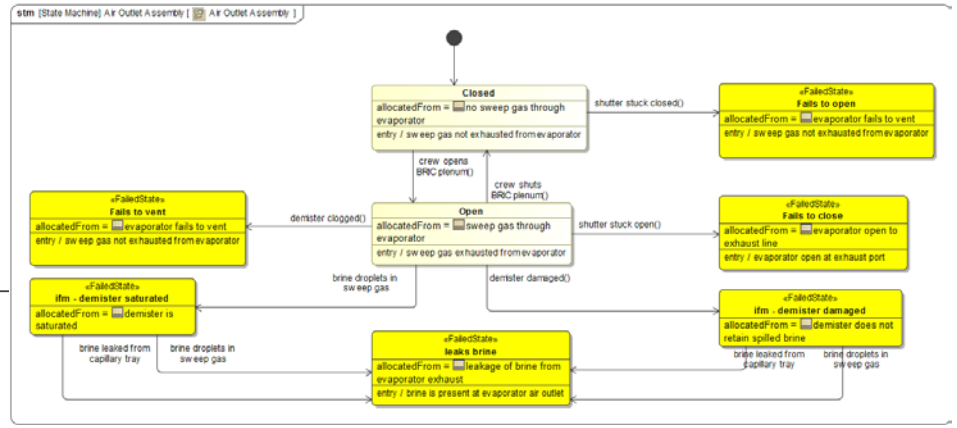


SysML/MagicDraw Severity and Likelihood values are entered manually and can correlate to the GSFC Risk definitions. To have a complete FMECA all thinking and data entry for to calculate RPN would be done at manually at the modeling stage and the plugin will extract the data and tabulate it for the user.

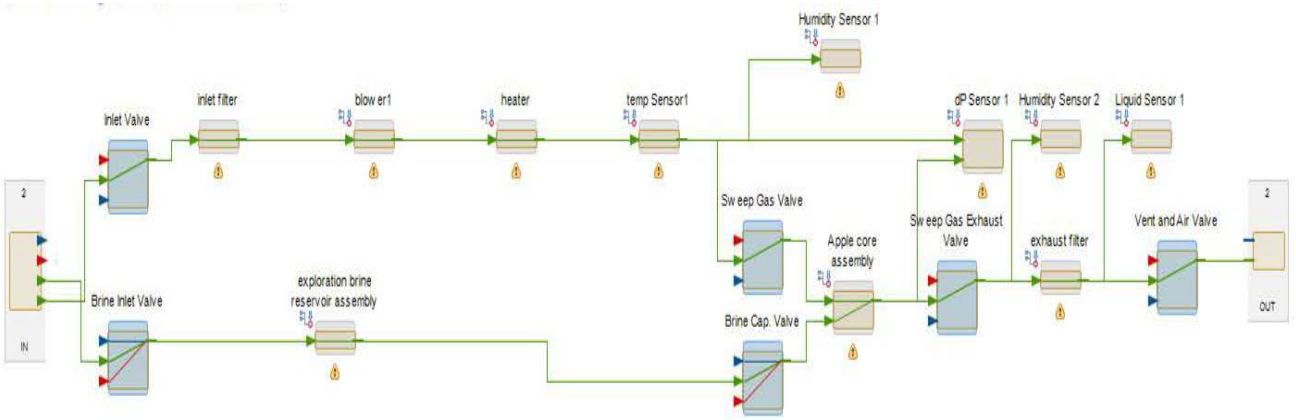
Narrative additions were used to clarify MADe FMECA outputs but tool modifications may be required to synthesize/input mission consequences more autonomously.

MBSMAI Phase 1: HUMAN SYSTEM – CapiBRIC Modeling

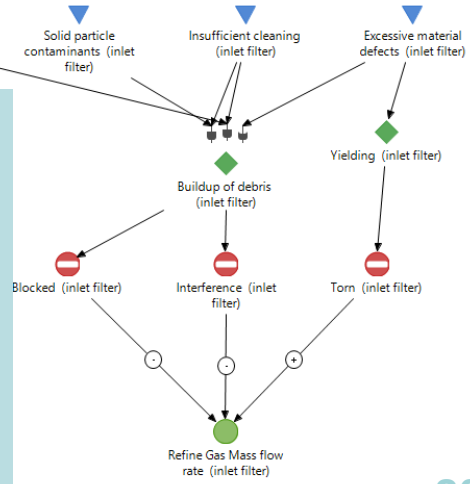




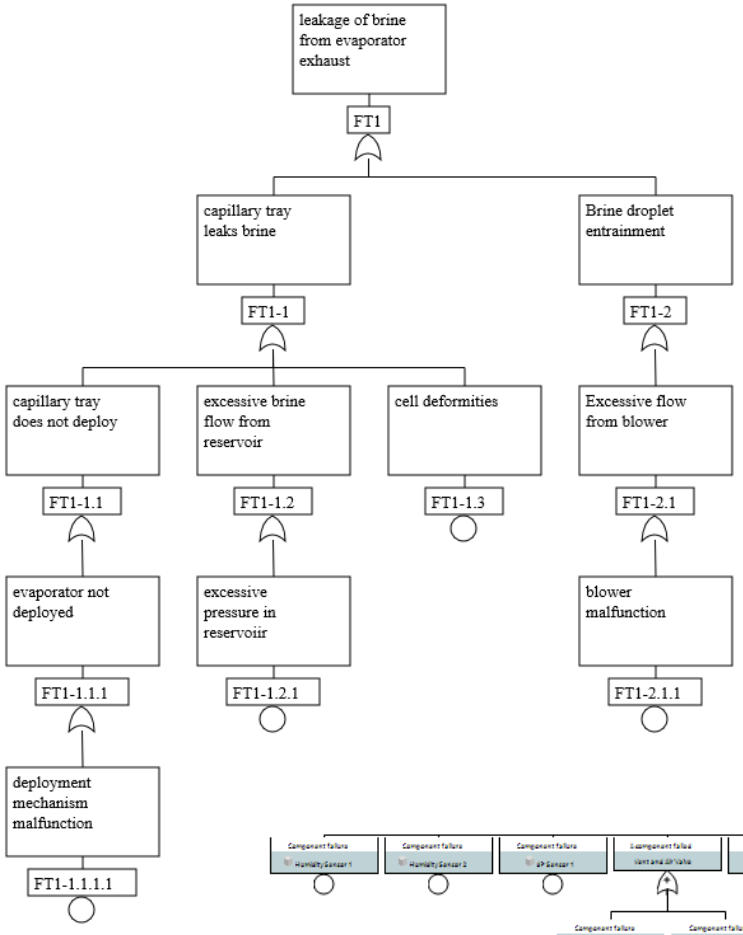
The CapiBRIC SysML model in SysML/MagicDraw provided by JSC consisted of a Block Definition Diagram, a wiring Diagram and 13 state machines



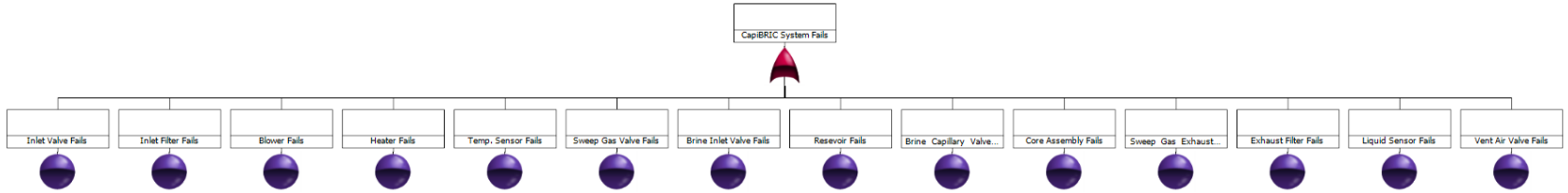
In MADe a limited model was developed that consisted of 1 main functional block diagram and 1 failure diagram.



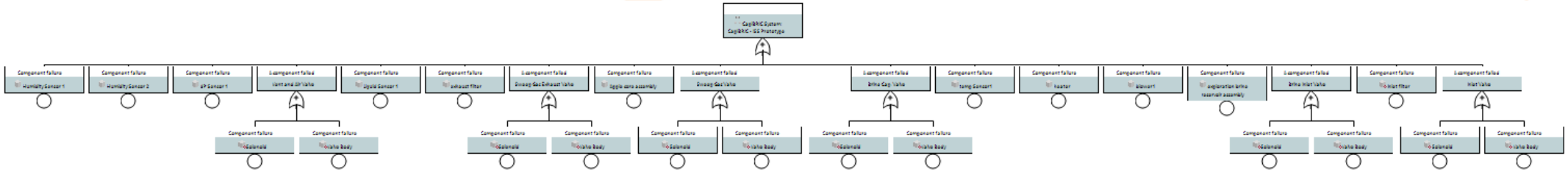
MBSMAI Phase 1: CapiBRIC Model Fault Tree Evaluation



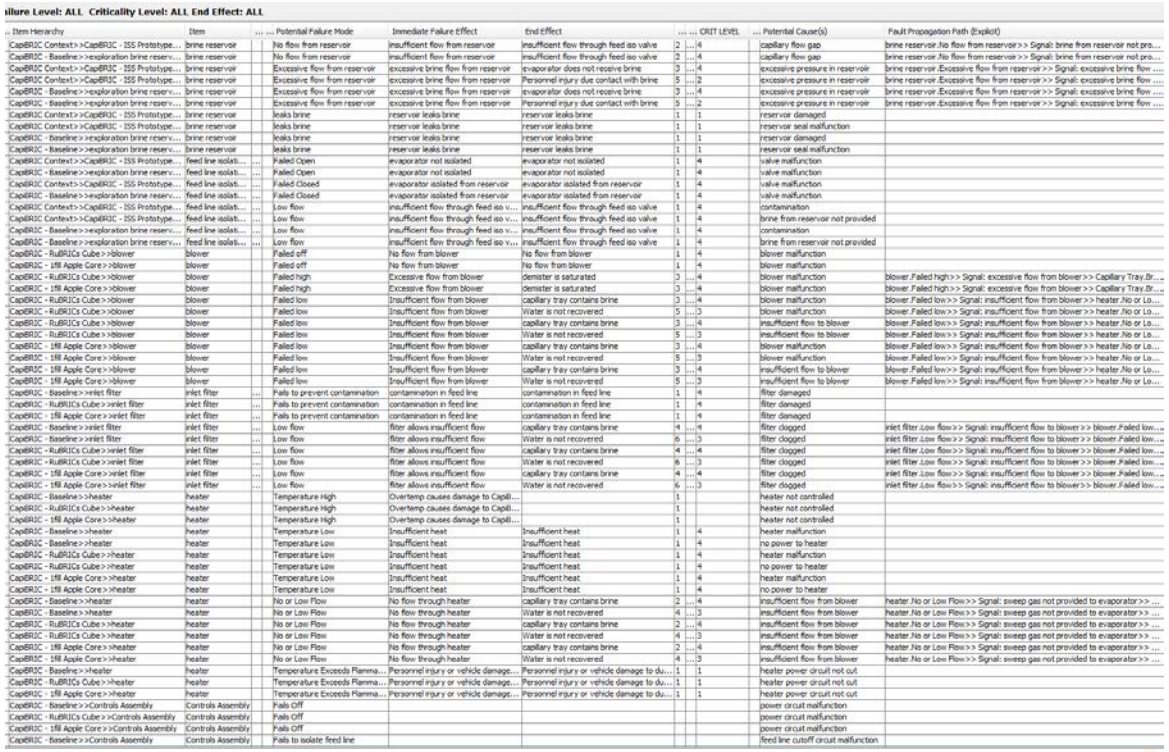
Traditional fault tree method was used to confirm that the hardware fault tree quantification in MADe was equivalent to those in traditional software tool.



The SysML/MagicDraw CapiBRIC model was provided to the MBSMAI model development and evaluation team and not developed internally so the model structure is similar but not exactly the same as that in MADe or traditional analysis performed by the team



MBSMAI Phase 1: CapiBRIC Model Failure Modes Effects and Criticality Analysis (FMECA) Evaluation



ilure Level: ALL Criticality Level: ALL End Effect: ALL

Item Hierarchy	Item	...	...	Potential Failure Mode	Immediate Failure Effect	End Effect	...	...	CRIT LEVEL	...	Potential Cause(s)	Fault Propagation Path (Explicit)
CapiBRIC Context>>CapiBRIC - ISS Prototype...	brine reservoir			No flow from reservoir	insufficient flow from reservoir	insufficient flow through feed iso valve	2	...	4		capillary flow gap	brine reservoir.No flow from reservoir>> Signal: brine from reservoir not pro...
CapiBRIC - Baseline>>exploration brine reserv...	brine reservoir			No flow from reservoir	insufficient flow from reservoir	insufficient flow through feed iso valve	2	...	4		capillary flow gap	brine reservoir.No flow from reservoir>> Signal: brine from reservoir not pro...
CapiBRIC Context>>CapiBRIC - ISS Prototype...	brine reservoir			Excessive flow from reservoir	excessive brine flow from reservoir	evaporator does not receive brine	3	...	4		excessive pressure in reservoir	brine reservoir.Excessive flow from reservoir>> Signal: excessive brine flow ...
CapiBRIC Context>>CapiBRIC - ISS Prototype...	brine reservoir			Excessive flow from reservoir	excessive brine flow from reservoir	Personnel injury due contact with brine	5	...	2		excessive pressure in reservoir	brine reservoir.Excessive flow from reservoir>> Signal: excessive brine flow ...
CapiBRIC - Baseline>>exploration brine reserv...	brine reservoir			Excessive flow from reservoir	excessive brine flow from reservoir	evaporator does not receive brine	3	...	4		excessive pressure in reservoir	brine reservoir.Excessive flow from reservoir>> Signal: excessive brine flow ...
CapiBRIC - Baseline>>exploration brine reserv...	brine reservoir			Excessive flow from reservoir	excessive brine flow from reservoir	Personnel injury due contact with brine	5	...	2		excessive pressure in reservoir	brine reservoir.Excessive flow from reservoir>> Signal: excessive brine flow ...
CapiBRIC Context>>CapiBRIC - ISS Prototype...	brine reservoir			leaks brine	reservoir leaks brine	reservoir leaks brine	1		1		reservoir damaged	
CapiBRIC Context>>CapiBRIC - ISS Prototype...	brine reservoir			leaks brine	reservoir leaks brine	reservoir leaks brine	1		1		reservoir seal malfunction	
CapiBRIC - Baseline>>exploration brine reserv...	brine reservoir			leaks brine	reservoir leaks brine	reservoir leaks brine	1		1		reservoir damaged	
CapiBRIC - Baseline>>exploration brine reserv...	brine reservoir			leaks brine	reservoir leaks brine	reservoir leaks brine	1		1		reservoir seal malfunction	
CapiBRIC Context>>CapiBRIC - ISS Prototype...	feed line isolati...		...	Failed Open	evaporator not isolated	evaporator not isolated	1		4		valve malfunction	
CapiBRIC - Baseline>>exploration brine reserv...	feed line isolati...		...	Failed Open	evaporator not isolated	evaporator not isolated	1		4		valve malfunction	
CapiBRIC Context>>CapiBRIC - ISS Prototype...	feed line isolati...		...	Failed Closed	evaporator isolated from reservoir	evaporator isolated from reservoir	1		4		valve malfunction	
CapiBRIC - Baseline>>exploration brine reserv...	feed line isolati...		...	Failed Closed	evaporator isolated from reservoir	evaporator isolated from reservoir	1		4		valve malfunction	
CapiBRIC Context>>CapiBRIC - ISS Prototype...	feed line isolati...		...	Low flow	insufficient flow through feed iso v...	insufficient flow through feed iso valve	1		4		contamination	
CapiBRIC Context>>CapiBRIC - ISS Prototype...	feed line isolati...		...	Low flow	insufficient flow through feed iso v...	insufficient flow through feed iso valve	1		4		brine from reservoir not provided	
CapiBRIC - Baseline>>exploration brine reserv...	feed line isolati...		...	Low flow	insufficient flow through feed iso v...	insufficient flow through feed iso valve	1		4		contamination	
CapiBRIC - Baseline>>exploration brine reserv...	feed line isolati...		...	Low flow	insufficient flow through feed iso v...	insufficient flow through feed iso valve	1		4		brine from reservoir not provided	
CapiBRIC - RuBRICs Cube>>blower	blower			Failed off	No flow from blower	No flow from blower	1		4		blower malfunction	
CapiBRIC - 1fil Apple Core>>blower	blower			Failed off	No flow from blower	No flow from blower	1		4		blower malfunction	
CapiBRIC - RuBRICs Cube>>blower	blower			Failed high	Excessive flow from blower	demister is saturated	3	...	4		blower malfunction	blower.Failed high>> Signal: excessive flow from blower>> Capillary Tray.Br...
CapiBRIC - 1fil Apple Core>>blower	blower			Failed high	Excessive flow from blower	demister is saturated	3	...	4		blower malfunction	blower.Failed high>> Signal: excessive flow from blower>> Capillary Tray.Br...
CapiBRIC - RuBRICs Cube>>blower	blower			Failed low	Insufficient flow from blower	capillary tray contains brine	3	...	4		blower malfunction	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - RuBRICs Cube>>blower	blower			Failed low	Insufficient flow from blower	Water is not recovered	5	...	3		blower malfunction	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - RuBRICs Cube>>blower	blower			Failed low	Insufficient flow from blower	capillary tray contains brine	3	...	4		insufficient flow to blower	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - RuBRICs Cube>>blower	blower			Failed low	Insufficient flow from blower	Water is not recovered	5	...	3		insufficient flow to blower	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - 1fil Apple Core>>blower	blower			Failed low	Insufficient flow from blower	capillary tray contains brine	3	...	4		blower malfunction	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - 1fil Apple Core>>blower	blower			Failed low	Insufficient flow from blower	Water is not recovered	5	...	3		blower malfunction	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - 1fil Apple Core>>blower	blower			Failed low	Insufficient flow from blower	capillary tray contains brine	3	...	4		insufficient flow to blower	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - 1fil Apple Core>>blower	blower			Failed low	Insufficient flow from blower	Water is not recovered	5	...	3		insufficient flow to blower	blower.Failed low>> Signal: insufficient flow from blower>> heater.No or Lo...
CapiBRIC - Baseline>>inlet filter	inlet filter		...	Fails to prevent contamination	contamination in feed line	contamination in feed line	1		4		filter damaged	
CapiBRIC - RuBRICs Cube>>inlet filter	inlet filter		...	Fails to prevent contamination	contamination in feed line	contamination in feed line	1		4		filter damaged	
CapiBRIC - 1fil Apple Core>>inlet filter	inlet filter		...	Fails to prevent contamination	contamination in feed line	contamination in feed line	1		4		filter damaged	
CapiBRIC - Baseline>>inlet filter	inlet filter		...	Low flow	filter allows insufficient flow	capillary tray contains brine	4	...	4		filter clogged	inlet filter.Low flow>> Signal: insufficient flow to blower>> blower.Failed low...
CapiBRIC - Baseline>>inlet filter	inlet filter		...	Low flow	filter allows insufficient flow	Water is not recovered	6	...	3		filter clogged	inlet filter.Low flow>> Signal: insufficient flow to blower>> blower.Failed low...
CapiBRIC - RuBRICs Cube>>inlet filter	inlet filter		...	Low flow	filter allows insufficient flow	capillary tray contains brine	4	...	4		filter clogged	inlet filter.Low flow>> Signal: insufficient flow to blower>> blower.Failed low...
CapiBRIC - RuBRICs Cube>>inlet filter	inlet filter		...	Low flow	filter allows insufficient flow	Water is not recovered	6	...	3		filter clogged	inlet filter.Low flow>> Signal: insufficient flow to blower>> blower.Failed low...
CapiBRIC - 1fil Apple Core>>inlet filter	inlet filter		...	Low flow	filter allows insufficient flow	capillary tray contains brine	4	...	4		filter clogged	inlet filter.Low flow>> Signal: insufficient flow to blower>> blower.Failed low...
CapiBRIC - 1fil Apple Core>>inlet filter	inlet filter		...	Low flow	filter allows insufficient flow	Water is not recovered	6	...	3		filter clogged	inlet filter.Low flow>> Signal: insufficient flow to blower>> blower.Failed low...
CapiBRIC - Baseline>>heater	heater			Temperature High	Overtemp causes damage to Capil...		1				heater not controlled	
CapiBRIC - RuBRICs Cube>>heater	heater			Temperature High	Overtemp causes damage to Capil...		1				heater not controlled	
CapiBRIC - 1fil Apple Core>>heater	heater			Temperature High	Overtemp causes damage to Capil...		1				heater not controlled	
CapiBRIC - Baseline>>heater	heater			Temperature Low	Insufficient heat	Insufficient heat	1		4		heater malfunction	
CapiBRIC - Baseline>>heater	heater			Temperature Low	Insufficient heat	Insufficient heat	1		4		no power to heater	
CapiBRIC - RuBRICs Cube>>heater	heater			Temperature Low	Insufficient heat	Insufficient heat	1		4		heater malfunction	
CapiBRIC - RuBRICs Cube>>heater	heater			Temperature Low	Insufficient heat	Insufficient heat	1		4		no power to heater	
CapiBRIC - 1fil Apple Core>>heater	heater			Temperature Low	Insufficient heat	Insufficient heat	1		4		heater malfunction	
CapiBRIC - 1fil Apple Core>>heater	heater			Temperature Low	Insufficient heat	Insufficient heat	1		4		no power to heater	
CapiBRIC - Baseline>>heater	heater			No or Low Flow	No flow through heater	capillary tray contains brine	2	...	4		insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>> ...
CapiBRIC - Baseline>>heater	heater			No or Low Flow	No flow through heater	Water is not recovered	4	...	3		insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>> ...
CapiBRIC - RuBRICs Cube>>heater	heater			No or Low Flow	No flow through heater	capillary tray contains brine	2	...	4		insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>> ...
CapiBRIC - RuBRICs Cube>>heater	heater			No or Low Flow	No flow through heater	Water is not recovered	4	...	3		insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>> ...
CapiBRIC - 1fil Apple Core>>heater	heater			No or Low Flow	No flow through heater	capillary tray contains brine	2	...	4		insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>> ...
CapiBRIC - 1fil Apple Core>>heater	heater			No or Low Flow	No flow through heater	Water is not recovered	4	...	3		insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>> ...
CapiBRIC - Baseline>>heater	heater			Temperature Exceeds Flamma...	Personnel injury or vehicle damage...	Personnel injury or vehicle damage to du...	1		1		heater power circuit not cut	
CapiBRIC - RuBRICs Cube>>heater	heater			Temperature Exceeds Flamma...	Personnel injury or vehicle damage...	Personnel injury or vehicle damage to du...	1		1		heater power circuit not cut	
CapiBRIC - 1fil Apple Core>>heater	heater			Temperature Exceeds Flamma...	Personnel injury or vehicle damage...	Personnel injury or vehicle damage to du...	1		1		heater power circuit not cut	
CapiBRIC - Baseline>>Controls Assembly	Controls Assembly			Fails Off							power circuit malfunction	
CapiBRIC - RuBRICs Cube>>Controls Assembly	Controls Assembly			Fails Off							power circuit malfunction	
CapiBRIC - 1fil Apple Core>>Controls Assembly	Controls Assembly			Fails Off							power circuit malfunction	
CapiBRIC - Baseline>>Controls Assembly	Controls Assembly			Fails to isolate feed line							feed line cutoff circuit malfunction	

It is currently unclear if a SysML model FMECA can be customized to characterize severity/likelihood for risk assessment. SysML/MagicDraw FMECAs were generated at the system, and all other lower levels using Tietronix FMEA Plugin. MagicDraw Tietronix generated FMECAs were found to correspond well with traditional artifacts in content and format when the state machines were defined accordingly.

ITEM/PHYSICAL DESCRIPTION	FUNCTION/ FUNCTIONAL NARRATIVE	FAILURE MODE		CAUSES OF FAILURE		FAILURE EFFECTS		DETECTION METHODS	COMPENSATING PROVISIONS	CRITICALITY			
		FUNCTIONAL FAILURE	FAULT	MECHANISM	CAUSE	NEXT HIGHER LEVEL	END EFFECTS			O	S	D	RPN
inlet filter	Refine Gas Mass flow rate	Refine Gas Mass flow rate High	Torn	Yielding	Excessive material defects	Convert air_out Temperature High (CapiBRIC System: CapiBRIC - ISS Prototype) AND Convert air_out Mass flow rate High (CapiBRIC System: CapiBRIC - ISS Prototype)	Refine Gas Mass flow rate High			10.0	10.0	10.0	1000
		Refine Gas Mass flow rate Low	Blocked	Buildup of debris	Excessive material defects	Convert air_out Temperature Low (CapiBRIC System: CapiBRIC - ISS Prototype) AND Convert air_out Mass flow rate Low (CapiBRIC System: CapiBRIC - ISS Prototype)	Refine Gas Mass flow rate Low			10.0	10.0	10.0	1000
					Insufficient cleaning AND Contaminated input flow	Convert air_out Temperature Low (CapiBRIC System: CapiBRIC - ISS Prototype) AND Convert air_out Mass flow rate Low (CapiBRIC System: CapiBRIC - ISS Prototype)	Refine Gas Mass flow rate Low			10.0	10.0	10.0	1000
					Solid particle contaminants AND Insufficient cleaning	Convert air_out Temperature Low (CapiBRIC System: CapiBRIC - ISS Prototype) AND Convert air_out Mass flow rate Low (CapiBRIC System: CapiBRIC - ISS Prototype)	Refine Gas Mass flow rate Low			10.0	10.0	10.0	1000
			Interference	Buildup of debris	Excessive material defects	Convert air_out Temperature Low (CapiBRIC System: CapiBRIC - ISS Prototype) AND Convert air_out Mass flow rate Low (CapiBRIC System: CapiBRIC - ISS Prototype)	Refine Gas Mass flow rate Low			10.0	10.0	10.0	1000
					Insufficient cleaning AND Contaminated input flow	Convert air_out Temperature Low (CapiBRIC System: CapiBRIC - ISS Prototype) AND Convert air_out Mass flow rate Low (CapiBRIC System: CapiBRIC - ISS Prototype)	Refine Gas Mass flow rate Low			10.0	10.0	10.0	1000

MADe FMECAs were generated at the system, and fully decomposed levels using a simple override/mode setting. MADe FMECAs were found to relatively correspond well with traditional artifacts in content and format once optional mission specific narratives were added.

IS MODEL-BASED ENGINEERING VALID AND USEABLE FOR RELIABILITY ENGINEERING?

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

Recommended Process Guidance for Cross-Discipline Model-Based Engineering

Pre- Requisite: Establish Modelling process and controls

1) Establish a multi-discipline modeling team (Systems Engineering (SE) and SMA at a minimum);
2) Establish modeling responsibilities (e.g., SE's model requirements, Designer's model structure (Functional Block Diagram/Wire Diagram), REs model failure behaviors and characteristics) and controls;
3) Complete modeling and share common data between modelling elements;
4) Produce Reliability artifacts and share resulting data between modelling elements;
5) Verify and refine modelling (and designs) until a final and acceptable result is achieved;
6) Share modeling with future missions.

Recommended Optimal Modeling Environment Requirements for Cross-Discipline Model-Based Engineering

The Modeling environment/tool shall:

- Be easily mastered structure and interface for efficiency.
- Support for the development of models from the traditional reliability artifacts rather than only deriving the artifacts from the models for efficiency via model re-use.
- Have the ability to create a functional model of the systems for efficiency and clarity.
- Have the ability to ensure that changes to one diagram (e.g., adding a component) propagates to other parts/diagrams of the model automatically or at least shows as an error that needs to be resolved by the modeler.
- Have the ability to allocate requirements to a functional diagram/element for consistent and accurate effect assessment.
- Include modeling diagrams that connect hierarchically to each other for efficiency and clarity which will allow non-modelers to easily traverse and drill down within the model for understanding and accuracy validation.
- Have Libraries of standard components with baseline failure and function data for consistency and accuracy.
- Have Libraries of standard failure mechanisms and causes for consistency and efficiency.
- Have the ability to combine models and duplicate modeling for efficiency.
- Include Model component and system error checking for accuracy.
- Include Model change control/reporting for accuracy.
- Have performance that shortens analysis time while maintaining consistency and accuracy between models.
- Have the ability to add models of systems or portions of systems to a library of shareable models for efficiency.

Recommended Optimal Modeling Environment Requirements for Cross-Discipline Model-Based Engineering

The Modeling environment/tool shall:

- Have the ability to produce a FMECA with NASA defined levels and characterization factors, a Fault tree with precise Boolean logic for accuracy, life assessments at the component and system level, and availability assessments at the component and system level.
- Have the ability to perform maintainability assessments interconnected with maintenance/sparing plans at the component and system level.
- Have the ability to import requirements, CAD and BOM/part lists type data to create modeling elements or as supporting data for efficiency.
- Have the ability to select requirements allocated to each element as the effects and functions for accuracy and efficiency.
- Include an export function to other modeling formats and reliability tools (e.g., Windchill Prediction tool (formerly Relex), Saphire, QRAS, etc.)
- Have the ability to perform probability analysis using at least 217F, Telecordia, FIDES, PRISM, and/or enterprise custom databases (SEAM). Or import data from reliability tools (e.g., Windchill Prediction tool, etc.) for accuracy and efficiency.
- Have the ability to import results (e.g., radiation effects, life expectancy data, traditional analysis data) from other models or sources for efficiency and accuracy.

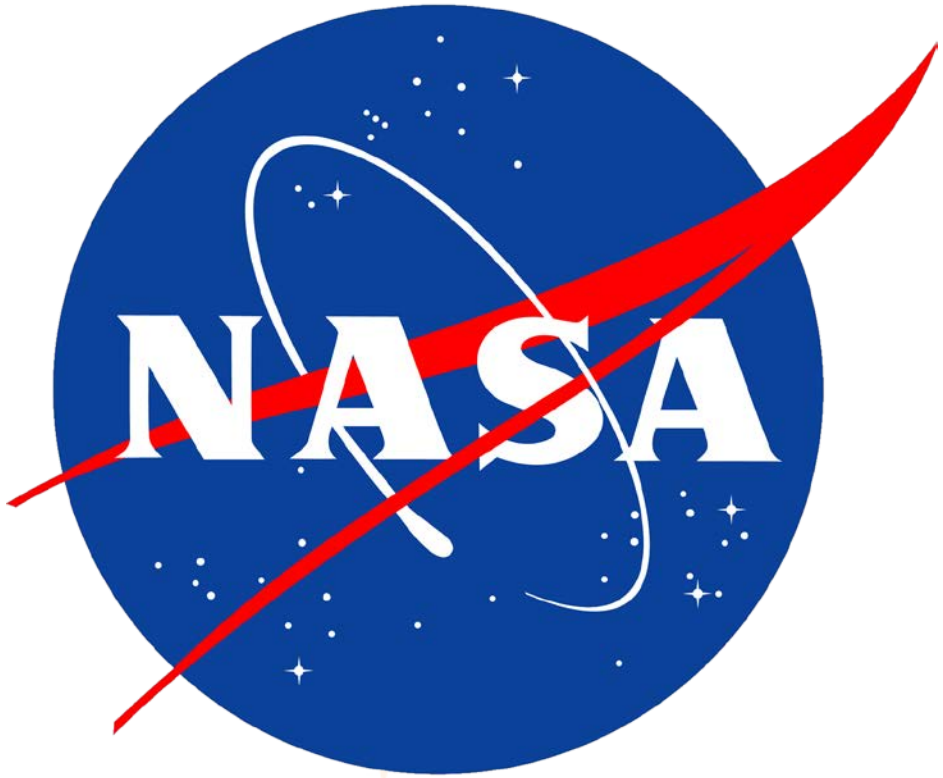
Conclusion and Path Forward

Conclusions

- Model-Based Organizations, including NASA, must decide for themselves how to implement model-based engineering in a way that makes sense for all their engineering, assurance, operational, and production elements. Therefor it is essential to the subject matter experts from each element as early as possible.
- Not all tools are ready to support all disciplines.

Path Forward

- Conduct Phase 2 of this study in which evaluations and testing will consist of follow-on Reliability evaluations with more complex system/model (e.g., Cubesat Mission) and Safety Analyses.
- Work with tool vendor's to customize tools for even more compatibility with SMA disciplines.
- Conduct Phase 3 of this study which will evaluate Software Assurance and Quality Engineering Analysis compatibility.


NASA