National Aeronautics and Space Administration

### Reliability Analysis of Complex NASA Systems with Model Based Engineering

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

Sponsored by NASA/HQ : John Evans and Anthony DiVenti

RAMS 2020 - PAPER ID 71 Model-based System Engineering for Reliability Analysis Jan 29<sup>th</sup> 2020 SESSION – 12





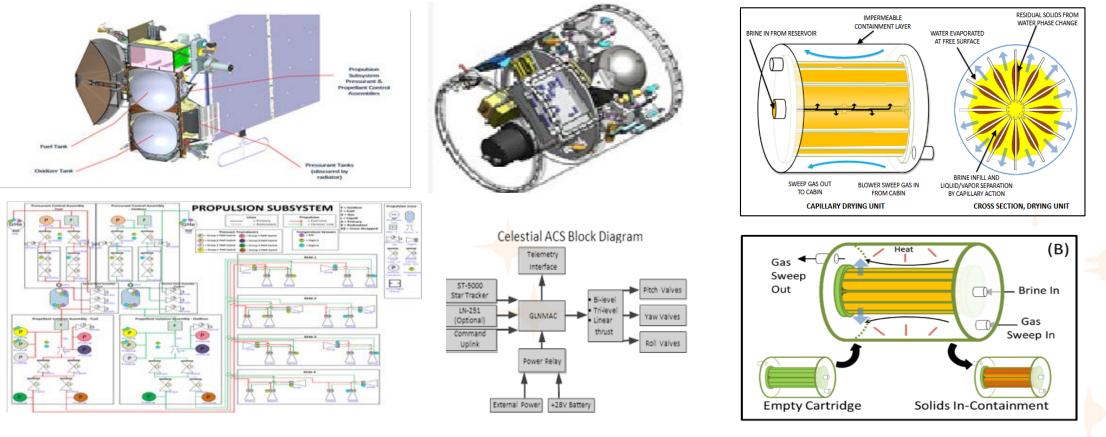
## **MBSMA Initiative Pathfinder Partner Project Objectives**

- 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 ?

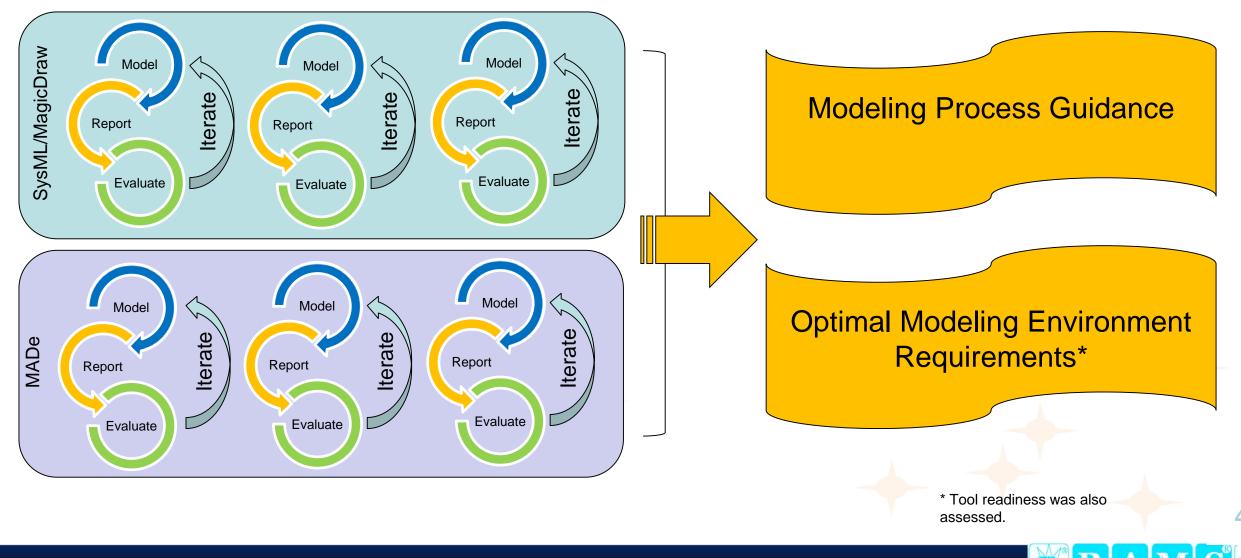
### **MBSMAI** Methodology

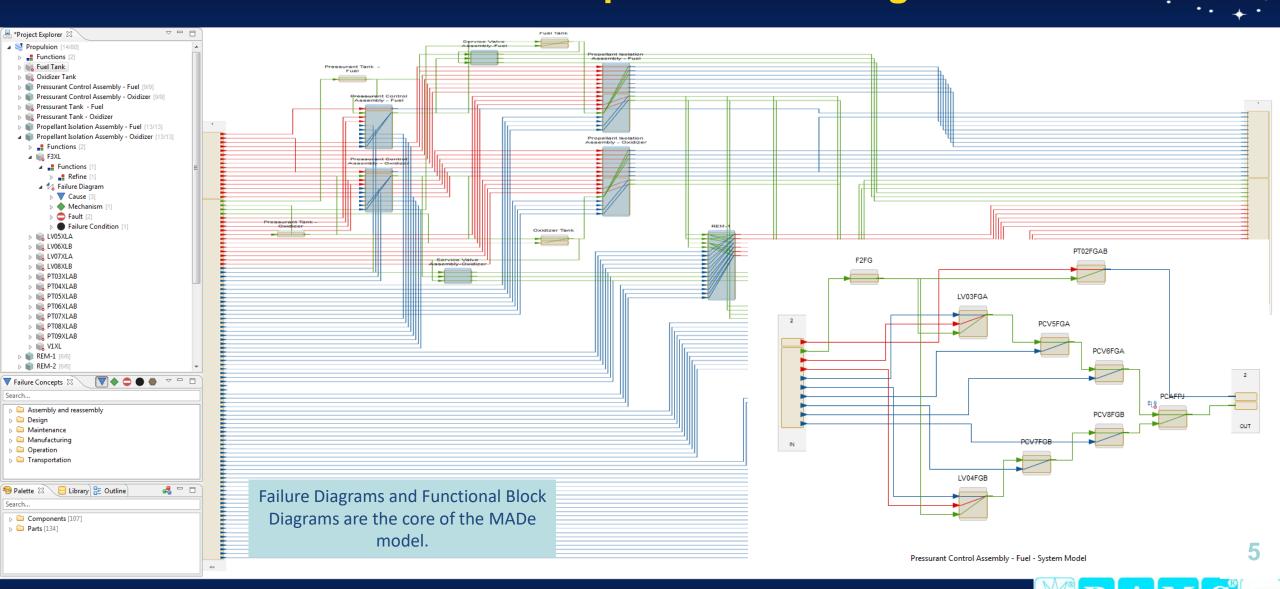
Use three mission test cases to evaluate the ability of Model-Based Engineering to support Reliability Analyses of Probability Analysis (PA)) Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), and Limited Life Analysis (LLA).

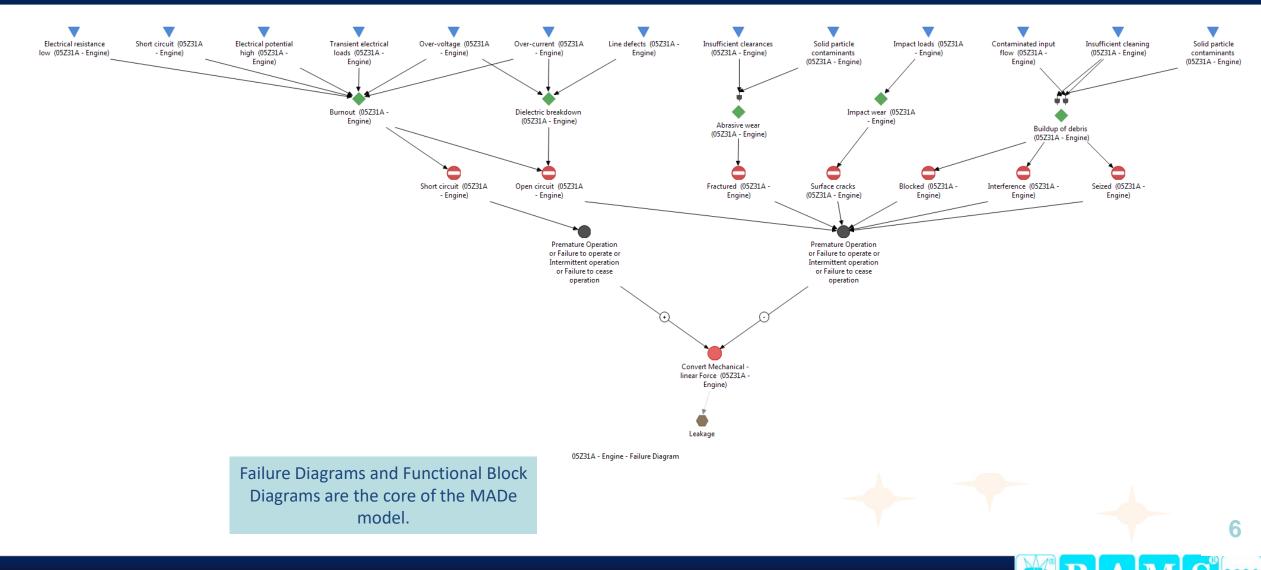


#### NASA MODEL BASED Safety and Mission Assurance

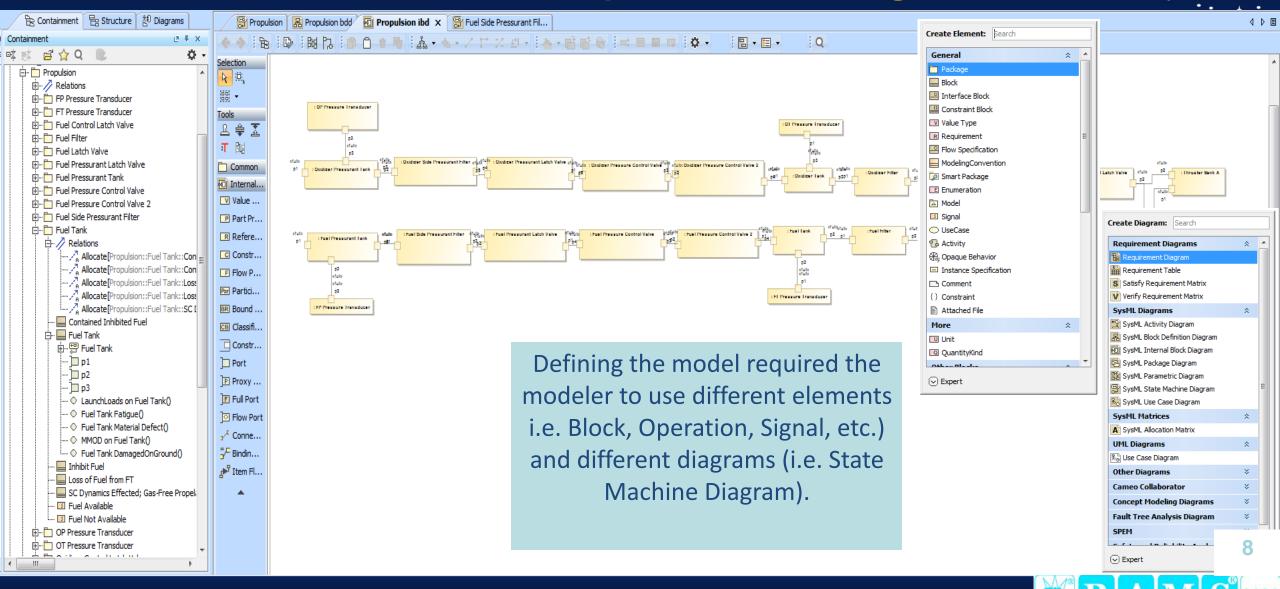
### **MBSMAI** Methodology



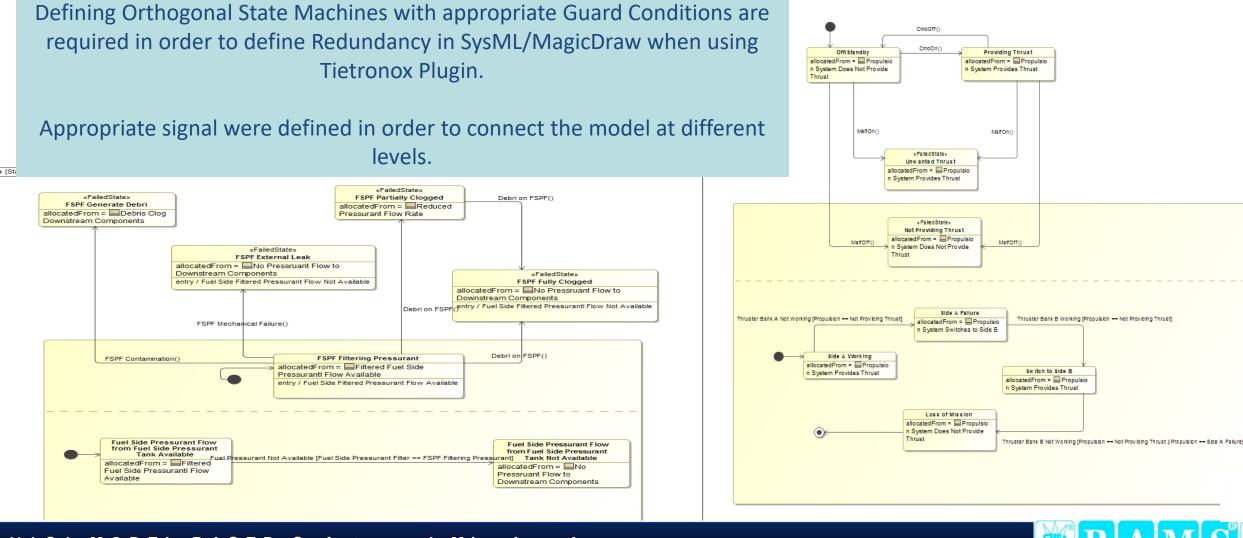


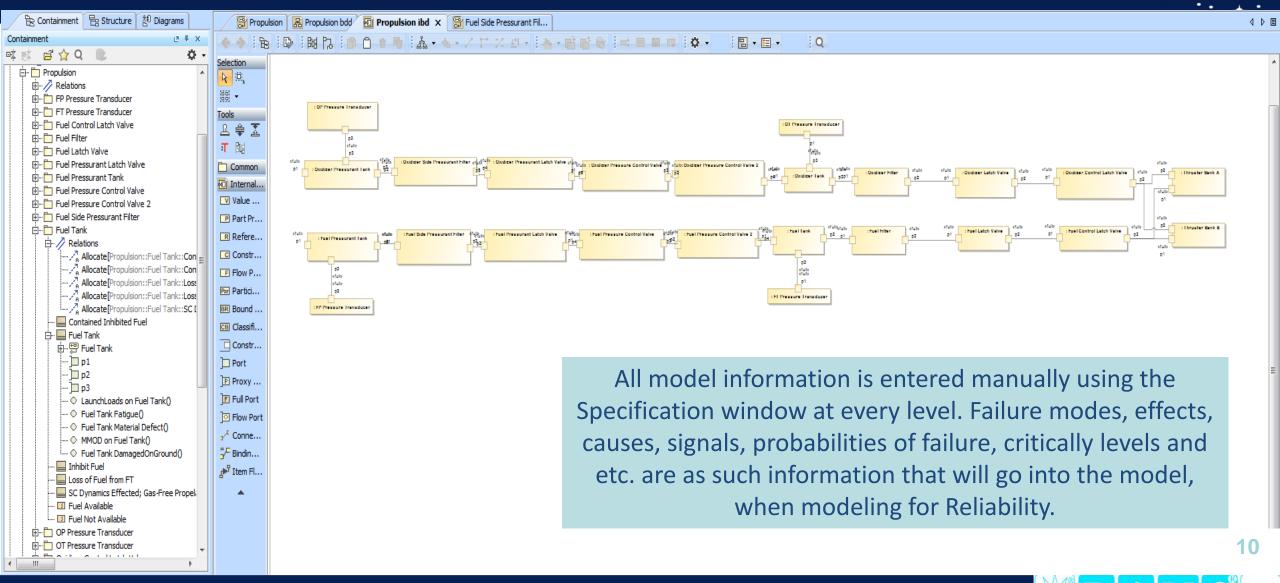


🖥 *Project	Explorer 🕱				Fuel Tank						
	Pusition [14/88] Functions [2] Fuel Tank Pressurant Control Assembly - Fuel [9/5 Pressurant Control Assembly - Oxidizer Pressurant Tank - Oxidizer Propellant Isolation Assembly - Fuel [113 Propellant Isolation Assembly - Oxidize ■ Functions [2] ■ FaxL ■ Functions [1] ■ J Functions [1] ■ V Failure Diagram ■ V Cause [3] ■ Mechanism [1] ■ Encitions [1]	[9/9] 3/13]	Pressurant Tank - Fuel	nt Gontrol		Propellant isolation Assembly - Fuel Propellant isolation Propellant isolation Assembly - Oxidicer					
	P Fault [2]     P Failure Condition [1]     LV05XLA     LV05XLB     LV07XLA		Oxidizer		e modeler c	of any discrep	ancy in	ADe was able to the design.		lr	
	Properties 🛛					<b>1</b>		\delta Problems 🛛		🍐 📣 🔅 🗸	
	瞩 Fuel Tank							Name		Model	*
	Bond	Duration of Operation (hr Mean Time To Repair (hr						A The 'PCV3XGB' failuation	ns) ure concept is disconnected ure concept is disconnected ol Gas (LV01XGA), contains flow propertie:	LV02XGB -> Surface cracks PCV3XGB -> Surface cracks	E
Þ	Functional Failures	Delay Time (hr	s): 0.0						ol Gas (LV02XGB), contains flow properties		
Failure	Reliability Exponential	Turn Around Time (hr	s): 0.0						ol Gas (LV03FGA), contains flow properties		
> 🗀 As:		Spares on Han	d: 0						ol Gas (PCV1XGA), contains flow propertie ol Gas (PCV2XGA), contains flow propertie		
▷ De	Monte Carlo	Failure Distribution Typ	e: Exponential				-	🏝 The In Flow, Contr	ol Gas (PCV3XGB), contains flow propertie	s that PCV3XGB -> Control (In Flows) ->	×
<ul> <li>▷ □ Ma</li> <li>▷ □ Op</li> <li>▷ □ Tra</li> <li>Palette</li> <li>Search</li> <li>▷ □ Co</li> <li>▷ □ Pa</li> </ul>								<ul> <li>The In Flow, Contr</li> </ul>	ol Gas (PCV4XGB), contains flow propertie ol Gas (PCV5FGA), contains flow propertie ol Gas (PCV6FGA), contains flow propertie ol Gas (PCV7FGB), contains flow propertie ol Gas (PCV8FGB), contains flow propertie ol Liquid (LV05XLA), contains flow propert ol Liquid (LV06XLB), contains flow propert	s that PCV5FGA -> Control (In Flows) -> s that PCV6FGA -> Control (In Flows) -> s that PCV7FGB -> Control (In Flows) -> s that PCV8FGB -> Control (In Flows) -> ies th LV05XLA -> Control (In Flows) ->	> > > G > G Li
		194						· · · · · · · · · · · · · · · · · · ·			7



• •• +•



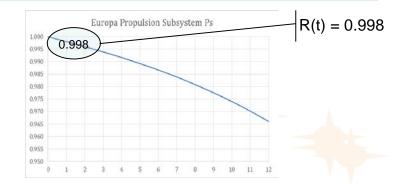


## **MBSMAI** Phase 1: EUROPA Model Probability Analysis Evaluation

SYSTEM HIERACHY	Propulsion > Series Group > Pressurant Con	trol Assembly - Fuel		
ITEM ID & NAME	Pressurant Control Assembly - Fuel		INDENTURE LEVEL	
RELIABILITY	0.997373	7 INHERENT AVAILABILITY	0.9999999 MTTF (HRS)	1
		Series Group	$\bigcirc$	2.1
		Paralel Group	2.2	
		Series Group	2.3	
		LV04FGB PCV7FGB	PCV8FGB	
	Series Group 2.	2 R(l)=0.9999982 R(l)=0.9999766	R(t)=0.9999766	oup 2.2
~	PT02FGAB F2FG	R(t)=0.9999514	PCAF	RJ
	R(t)=0.9998948 R(t)=0.9974786	Series Group	2.3 R(1)=0.99	199999
	R(t)=0.9973737	LV03FGA PCV5FGA	PCV6FGA R(t)=0.99	99999
		R(t)=0.9999982 R(t)=0.9999766	R(t)=0.9999766	
		R(t)=0.9999514		

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



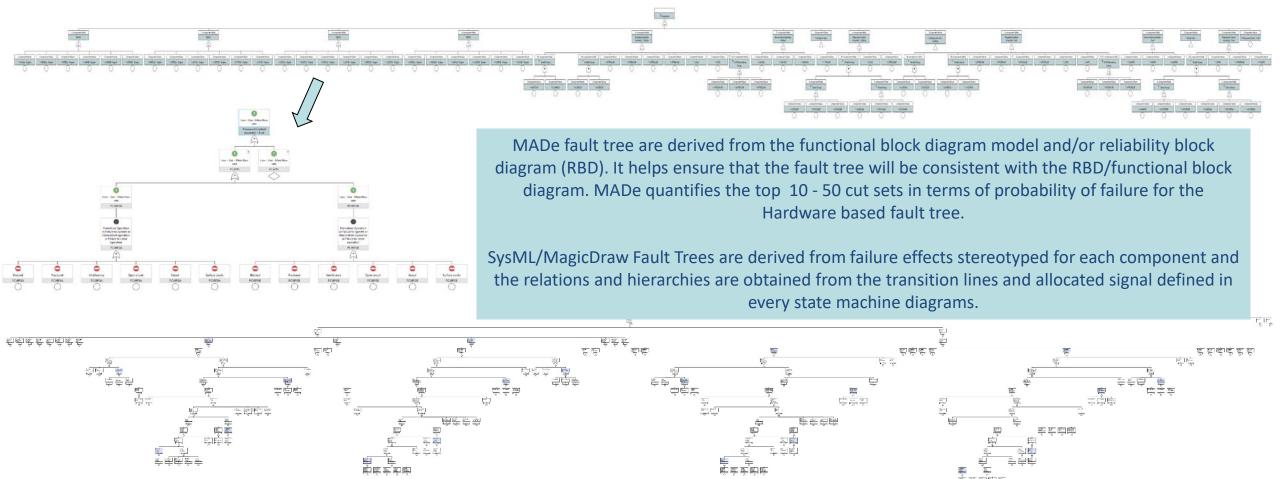
SysML/MagicDraw with Tietronix plugins does not currently support Probability Analysis. However, custom Plugins have been developed by individual enterprises.

**∲**made

PAGE 23 OF 33

### · · · · · · ·

### **MBSMAI** Phase 1: EUROPA Model Fault Tree Evaluation



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

SYSTEM	Propulsion > Presurant Co	ntroi Assenbly - Oxidaer :	FT01XCAB					DATE JU	25,2018 4 23 39 PM				
INDENTURE LEVEL	1							SHEET 15	OF	138			
REFERENCE DRAMING								COMPLED	IY todita				
NISSION	Regularioid							APPROVED BY					
DENTIFICATION	ITEM/		FAILURE MODES	NISSION PHASE /		FALURE EFFECTS		FALURE DETECTION	COMPENSATING	SEVER			
NUMBER	IDENTIFICATION (NOMENCLATURE)	FUNCTION	AND CAUSES	OPERATIONAL MODE	LOCAL EFFECTS	NEXT HIGHERLEVEL	END EFFECTS	MIANS	PROVISIONS	CLAS			
	PTIESSER Pressure Transducer	Convert Continueus Ampitude	High Continuous Amplitude due to Circuit beeling of the PTETRIAR as a next of delectric breakfown cuosed by line defects Degraded output or Palure to operate an intermittent operation or Loss of output	1: PastLaunch 100%	Canvert Continuous Analicude High	Signal Cantrivous Anplitude High (Pressumet Cantrol Assembly - Oxiduar)	Signal Cantinuous Amplitude (Sign (Propulsion)	Equipment Testing, Inspection, Ciperator Observation, Sensing Device	Change System Configuration, Modify Massion, Modify Sensor Sel, Override System				
			High Carotinuous Analitude due to Circuit beaking of Barritsticala ana nexit of delectric breaktoen caused by overvoltage Degraded output or Palure to operate or Intermittent operation or Loss of output		Carvert Continuous Anglicude High	Sigtal Canthudus Amplitude High (Fresurant Costrol Assembly- Oxidaer)	Signal Cantinuous Amplitude Higt (Propulsion)						
			High Carotinuous Analoude due to Circuit breaking of the PTEYICABL as a nexult of delectric breakdown caused by over-current Degraded output or Falure to operate or Intermittent operation or Loss of output		Canvert Continuous Anplitude High	Sigtel Canthuous Anglitude High (Presurant Costrol Assembly - Oxidae)	Sgrai Continuous Amplitude High (Propulsion)						
			High Continuous Amplitude due to Circuit brealing of the PTCHICAB as a result of barmult caused by overcoment. Degraded output or Falure to operate or intermittent operation or Loss of output		Convert Continuous Anplitude High	Signal Canthuous Anglitude High (Freeurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)						
			High Continuous Annolitude due to Circuit breaking of the PTVCXAB as a next of borroot caused by over-oitage Degraded output or Follume to operate or information operation or in output.		Convert Continuous Anplitude High	Signal Canthuous Anglibude High (Fressurant Control Accembly - Oxidizer)	Signel Cantinuous Amplitude High (Propulsion)						
			High Carolinuous Anaplitude due to Carolit beaking of the PTCNCAB as a result of borrout caused by electrical resistance low Degraded output or Fallure to operate or Intermittent operation or Loss of output		Convert Continuous Anglitude High	Signal Canthuous Anglitude High (Fressurant Control Assembly-Oxidzer)	Signal Continuous Amplitude High (Propulsion)						
			High Cartinuous Anpihude due to Corcult beating of the FTEXCAB are result of burnout caused by short croat Degraded output or Falure to operate or intermittent operation or Loss of output		Convert Continuous Amplitude High	Sgnal Canthuous Anpiltude High (Fresurant Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)						
			Low Continuous Amplitude due to Facturing of the P1013CAB as a result of advancement caused by insufficient dearancement solid particle contaminants		Convert Continuous Amplitude Low	Sgoal Cantinuous Amplitude Low (Presurant Control Assembly - Oxidizer)	Signel Continuous Amplitude Love (Propulsion)	Equipment Testing Impection, Operator Observation, Sensing Device	Charge System Configuration, Modify Masien, Modify Sensor Set, Override Swatem	1			

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

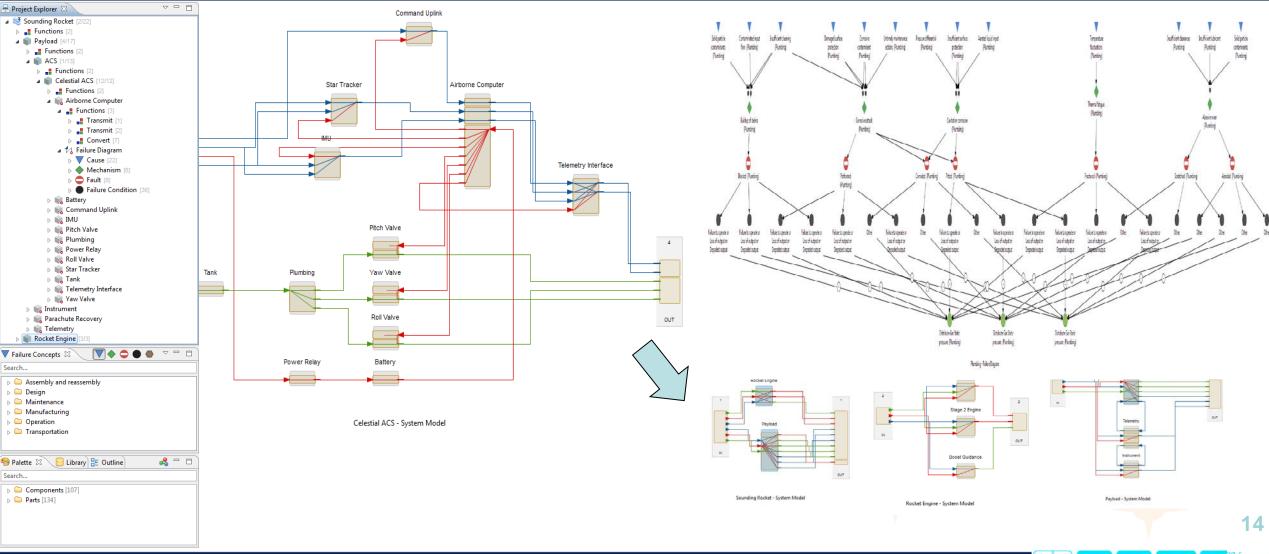
	5							
	4							
Likelihood of	3							
Occurrence	2							
	1							
	<1							
	Severity Category	4	3	3	2/2R	2	1R	1/1S
Criticality Risk Matrix	Severity Value	1	2		3		4	5
			Relative	e Severity	of Failure	Modes		

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

Don Her	tion	Potential Failure Mode	Immediate Failure Effect	End Effect			Potential Cause(s)	Fault Propagation Path (Explicit)
Propulsion		Linwanted Thrust	Propulsion System Provides Thrust	Propulsion System Provides Thrust	14		MalfOn	
Propulsion		Not Providing Thrust		Propulsion System Does Not Provide Thrust	i.		MaROFF	
	Fuel Latch Valve	Internal Leak	No Effect from Fuel Latch Valve	No Effect from Fuel Latch Valve	i	++-	FLV Contamination	
	Fuel Latch Valve	Back-Relef Falure	No Effect from Fuel Latch Valve	No Effect from Fuel Latch Valve	i.		PLV Mechanical Failure	
	Fuel Latch Valve	External Leak	Loss of Ruel from Ruel Latch Valve	Loss of Fuel from Fuel Latch Valve	i		FLV Workmanship Issue	
	Fuel Latch Valve	External Leak	Loss of Puel from Puel Latch Valve	Loss of Fuel from Fuel Latch Valve			FLV Waterhammered	
	. Fuel Latch Valve	Faled Close	Puel Latch Valve Does Not Provide Puel	Fuel Control Latch Valve Does Not Provide Fuel	-		PLV Col Pakze	Fuel Latch Valve Failed Close >> Signal: Fuel Latch Valve is Not Providing Fuel && Fuel Co
	Fuel Latch Valve	Faied Open	Fuel Latch Valve Provides Fuel	Fuel Control Latch Valve Provides Fuel	5	1771	R.V.Col Falure	Fuel Latch Valve, Failed Open>> Signal: Fuel Latch Valve is Providing Fuel && Fuel Control
	. Fuel Control La	Internal Leak		No Effect from Fuel Control Latch Valve	1		FCLV Contamination	Factory rates and open 2 agrain and used rates are a remaining rate autor const
	Fuel Control La	Back Relef Falure	No Effect from Fuel Control Latch Valve		1		FCLV Mechanical Falure	
	Fuel Control La	External Leak		Loss of Fuel From Fuel Control Latch Valve	-		PCLV Workmanship Issue	
	Fuel Control La.	External Leak		Loss of Fuel From Fuel Control Latch Valve	-		PQ.V Waterhammered	
	Fuel Control La	Ealed Close	Fuel Control Latch Valve Does Not Prov.		2		FO.V Col Falure	Fuel Control Latch Valve, Failed Close >> Sgnai: FCLV Does Not Provide Fuel Flow >> Thr
	Fuel Control La	Faled Close	Fuel Control Latch Valve Does Not Prov.		-		FCLV Col Falure	Fuel Control Latch Valve, Failed Close >> Signal: PCLY Does Not Provide Fuel Flow >> Thr
	Fuel Control La.	Faled Open	Fuel Control Latch Valve Provides Fuel	Thruster Bank 8 Provides Thrust			FCLV Col Falure	Fuel Control Latch Valve, Failed Open>> Signal: FCLV Provides Fuel Flow>> Thruster Ban
	Fuel Control La	Faled Open	Fuel Control Latch Valve Provides Fuel	Thruster Bank A Provides Thrust	÷		FO.V.Col Fakre	Puel Control Latch Valve Failed Open > > Sonal: PCLV Provides Fuel Plov >> Thruster Ban
Propulsion		External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	÷		MMOD on Fuel Tank	Fuel Tark, External Leak>> Sonal: Fuel Not Available>> Fuel Filter, Fuel Flow from Fuel T
Propulsion		External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components			Fuel Tank Fatigue	Puel Tark External Leak>> Signal: Puel Not Available>> Puel Piter Puel Pow from Puel T
Propulsion		External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	1		Launch ands on Fuel Tank	Fuel Tank External Leak>> Signal: Fuel Not Available >> Fuel Fifter /Fuel Flow from Fuel T
Propulsion		External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	1		Fuel Tark Material Defect	Fuel Tark External Leak >> Signal: Fuel Not Available >> Fuel Filter Fuel Flow from Fuel 1 Fuel Tark External Leak >> Signal: Fuel Not Available >> Fuel Filter Fuel Flow from Fuel 1
Propulsion		PMD Fractured Structure		SC Dynamics Effected: Gas-Free Propelant f			Laund Loads on Fuel Tark	Fuel tank colema Leak >> signal: rue hisk available >> rue hise zrue how now rue i
Propulsion		PMD Fractured Structure		SC Dynamics Effected; Gas-Pree Propelant F			Puel Tank DamagedOnGround	
Propulsion		PMD Fractured Structure		SC Dynamics Effected; Gas-Free Propelant f			Fuel Tank Material Defect	Thruster Bank 8-Orthogonal Thruster B1 Failure >> Signal: Thruster Bank 8 Not Working I
	. Thruster Bank B	Thruster 81 Falure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B1 Valve Col Falure	
	. Thruster Bank B	Thruster Valves 81 Failed Open	No Effect from Thruster Bank 8 Falure	Propulsion System Provides Thrust	14	***	Nechanical Falure of Thruster81	Thruster Bank B-Orthogonal. Thruster Valves B1 Failed Open>> Signal: Thruster Bank B 1
	. Thruster Bank B	Thruster Valves B1 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2	941	Excessive Heat Soakback from ThrusterB1	Thruster Bank 8-Orthogonal Thruster Valves 61 Failed Open>> Signal: Thruster Bank 8 II
	. Thruster Bank B	Thruster Valves B2 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2	444	Mechanical Falure of Thruster82	Thruster Bank 8-Orthogonal. Thruster Valves 82 Failed Open >> Signal: Thruster Bank 8 1
	. Thruster Bank B	Thruster Valves B2 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from ThrusterB2	Thruster Bank 5-Orthogonal. Thruster Valves 82 Pailed Open>> Signal: Thruster Bank 8 ii
	Thruster Bank B	Thruster Valves B3 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Excessive Heat Soekback from ThrusterB3	Thruster Bank B-Orthogonal, Thruster Valves B3 Failed Open>> Signal: Thruster Bank B V
	. Thruster Bank B	Thruster Valves ICJ Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Mechanical Falure of Thrusterli 3	Thruster Bank B-Orthogonal. Thruster Valves BJ Failed Open>> Signal: Thruster Bank B II
	. Thruster Bank B	Thruster Valves 84 Failed Open	No Effect from Thruster Bank 8 Falure	Propulsion System Provides Thrust	2		Mechanical Failure of Thruster84	Thruster Bank 8-Orthogonal. Thruster Valves 84 Failed Open>> Signal: Thruster Bank 8 I
	. Thruster Bank B	Thruster Valves 84 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2	+++	Excessive Heat Soakback from ThrusterB4	Thruster Bank 8-Orthogonal. Thruster Valves 84 Failed Open>> Signal: Thruster Bank 8 II
	. Thruster Bank B	Thruster Valves B5 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from ThrusterB5	Thruster Bank 8-Orthogonal, Thruster Valves 85 Failed Open >> Signal: Thruster Bank 8 I
	. Thruster Bank B	Thruster Valves B5 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Mechanical Falure of Thruster85	Thruster Bank B-Orthogonal. Thruster Valves B5 Failed Open >> Signal: Thruster Bank B II
	. Thruster Bank B	Thruster Valves B6 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Nechanical Falure of Thruster86	Thruster Bank 8-Orthogonal. Thruster Valves 86 Failed Open>> Signal: Thruster Bank 8 ii
	. Thruster Bank B	Thruster Valves B6 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	8		Excessive Heat Soakback from ThrusterB6	Thruster Bank B-Orthogonal. Thruster Valves B6 Failed Open>> Signal: Thruster Bank B 1
	. Thruster Bank B	Thruster Valves 87 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2	44.4	Excessive Heat Solkback from ThrusterB7	Thruster Bank 5-Orthogonal. Thruster Valves 37 Failed Open>> Signal: Thruster Sank 5 I
	. Thruster Bank B	Thruster Valves B7 Failed Open	No Effect from Thruster Sank 8 Failure	Propulsion System Provides Thrust	2		Mechanical Failure of Thruster67	Thruster Bank B-Orthogonal.Thruster Valves B7 Failed Open>> Signal: Thruster Bank B I
	. Thruster Sank B	Thruster Valves B3 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Mechanical Failure of Thruster88	Thruster Bank B-Orthogonal Thruster Valves B8 Failed Open >> Signal: Thruster Bank B ii
	Thruster Bank B	Thruster Valves B8 Failed Open	No Effect from Thruster Bank D Failure	Propulsion System Provides Thrust	2	***	Excessive Heat Sockback from ThrusterB8	Thruster Bank B-Orthogonal, Thruster Valves BB Faled Open>> Signal; Thruster Bank B V
	. Thruster Bank B	Thruster Valves 810 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Mechanical Failure of Thruster® 30	Thruster Bank 8-Orthogonal. Thruster Valves 8:10 Failed Open>> Signal: Thruster Bank 8
	. Thruster Bank B		No Effect from Thruster Bank 8 Failure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from ThrusterB10	
	. Thruster Bank B		No Effect from Thruster Bank B Fakure	Propulsion System Provides Thrust	2	14.0	Mechanical Failure of Thruster 511	Thruster Bank B-Orthogonal. Thruster Valves B11 Failed. Open>> Signal: Thruster Bank B
	. Thruster Bank B		No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2	i.e.	Excessive Heat Soakback from ThrusterB11	
	. Thruster Bank B	Thruster Valves B9 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from Thruster89	Thruster Bank 8-Orthogonal Thruster Valves 89 Failed Open>> Signal: Thruster Bank 81
	. Thruster Bank B	Thruster Valves D9 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2	***	Mechanical Falure of Thruster89	Thruster Bank B-Orthogonal Thruster Valves B9 Failed Open>> Signal: Thruster Bank B
	. Thruster Bank B		No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Mechanical Failure of Thruster812	Thruster Bank B-Orthogonal. Thruster Valves B12 Failed. Open>> Signal: Thruster Bank B
	. Thruster Bank B	Thruster Valves 812 Failed Open	No Effect from Thruster Bank B Palure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from ThrusterB12	
	. Thruster Bank B	Thruster 82 Falure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B2 Valve Coll Falure	Thruster Bank B-Orthogonal. Thruster 52 Failure >> Signal: Thruster Bank B Not Working I
Propulsion	. Thruster Sank B	Thruster 83 Fakure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2	144	Thruster 83 Valve Coll Failure	Thruster Bank B-Orthogonal. Thruster B3 Failure >> Signal: Thruster Bank B Not Working a
	. Thruster Bank B	Thruster 84 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster D4 Valve Coll Failure	Thruster Bank 8-Orthogonal. Thruster 84 Failure>> Signal: Thruster Bank 8 Not Working I
Propulsion	. Thruster Bank B	Thruster 85 Falure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster BS Valve Col Falure	Thruster Bank B-Orthogonal. Thruster B5 Failure >> Signal: Thruster Bank B Not Working I
nopulsion	. Thruster Bank B	Thruster 86 Falure	Thruster Bank II Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B6 Valve Col Falure	Thruster Bank B-Orthogonal. Thruster B6 Failure>>> Signal: Thruster Bank B Not Worlong I
hopulsion	. Thruster Sank B	Thruster 87 Failure	Thruster Bank 8 Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster 87 Valve Col Falure	Thruster Bank 8-Orthogonal. Thruster 87 Falure >> Signal: Thruster Bank 8 Not Working I
hopulsion	. Thruster Bank B	Thruster 58 Falure	Thruster Bank 8 Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B8 Valve Coll Falure	Thruster Bank B-Orthogonal. Thruster 68 Failure >> Signal: Thruster Bank B Not Working I
Propulsion	Thruster Bank B	Thruster 89 Falure	Thruster Bank 8 Loss of Thrust	Propulsion System Does Not Provide Thrust	2	1.4.5	Thruster B9 Valve Coll Falure	Thruster Bank 8-Orthogonal. Thruster 89 Failure >> Signal: Thruster Bank 8 Not Working J
Propulsion	Thruster Bank B	Thruster 810 Failure	Thruster Bank 8 Loss of Thrust	Propulsion System Does Not Provide Thrust	2	1	Thruster 810 Valve Coll Failure	Thruster Bank B-Orthogonal, Thruster B10 Failure >> Signal: Thruster Bank B Not Working
	Thruster Bank B	Thruster 811 Fakure	Thruster Bank 8 Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B11 Valve Coll Failure	Thruster Bank 8-Orthogonal Thruster B11 Falure>>> Signal: Thruster Bank 8 Not Working
Propulsion		Thruster #12 Failure	Thruster Bank 8 Loss of Thrust	Propulsion System Does Not Provide Thrust	5	1	Thruster B12 Valve Col Falure	Thruster Bank B-Orthogonal Thruster 812 Failure>>> Signal: Thruster Bank B Not Working
	Oxdzer Tark	External Leak	Loss of Oxidaer	No Oxidizer Flow to Downstream Components	1	-	LaunchLoads on Oxidizer Tank	Oxdaar Tank,External Loak>> Signal: Oxdaar Not Available>> Oxdaar Filter.Oxdaar F
	Oxidzer Tark	External Look	Loss of Oxidaer	No Oxidizer Flow to Downstream Components			MMOD on Oxidizer Tank	Ovidizer Tank External Leak>> Signal: Ovidizer Not Available>> Ovidizer Filter Ovidizer F

1	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
1	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?	1	2		147
1	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	(		SPF	148
1	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



### **MBSMAI** Phase 1: Sounding Rocket Modeling

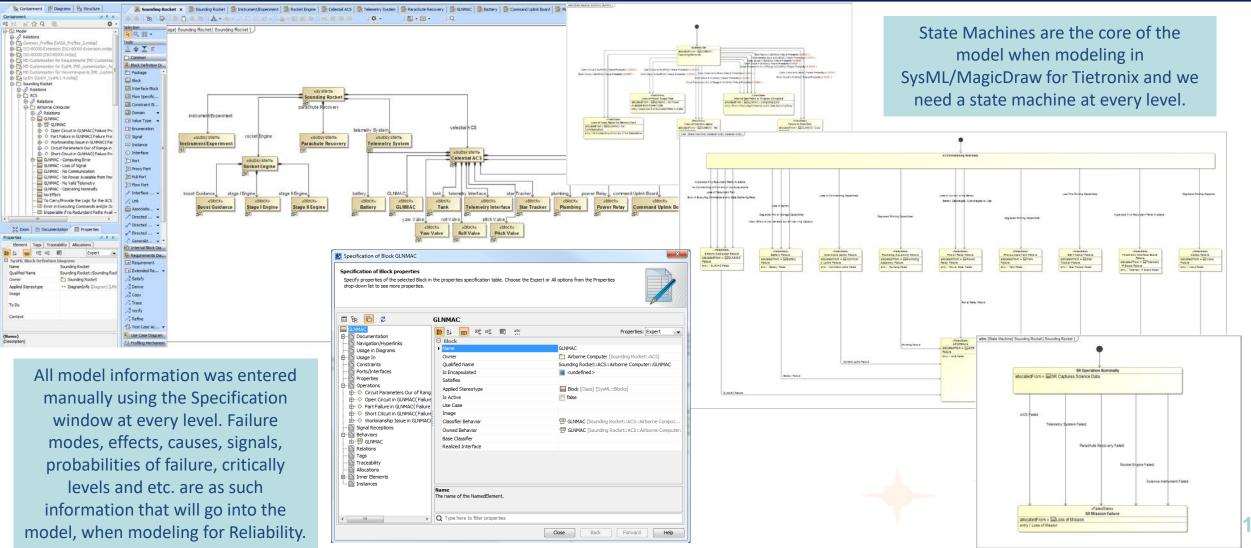
.+

🖁 Project Explorer 🛛	Command Uplink		
▲ Sounding Rocket [2/22] ▶	Compensating Provisions - Perforating of the Plumbing		
a 📦 Payload [4/17]	Compensating Provisions - Perforating of the Plumbing		Selpeta Contributiva Indiational India India Contri Indiatana Anaziliati Indiatana kateliativat Indiatana Indiat
Functions [2] ACS [1/13]	Compensating Provisions		Rotry / Potry Potry Potry Potry
Functions [2] Celestial ACS [12/12]	Assign one or more Compensating Provisions for Perforating of the Plumbing.	444	When modeling in MADe, the modeler can add
Functions [2]			$\mathbb{Y}$ when modeling in MADE, the modeler can add
Airborne Computer     Airborne Computer	Compensating Provisions Detection Methods		criticality and severity parameters using the
Transmit [1]	Name Definition	A	Like Face Approx
Transmit [2] Convert [7]	Visite         Definition           V         Abort Mission         Aborting or canceling the mission in response	so to the failure	Criticality Editor feature. Failure detection and
a ঝ Failure Diagram			compensation factors can be added to the
Cause [22] Mechanism [6]	Change System Configuration     Condition-based Maintenance     Condition-based Maintenance     Repairing or replacing the item in a condition		
Fault [8] Fault [8]			model on every failure diagram.
Failure Condition			
<ul> <li>Command Uplink</li> <li>IMU</li> </ul>	Modify Sensor Set Adding or modifying a sensor/alarm to the		
Nico Valve	Override System A manual or automatic override of an item	··· · 문 Celestial ACS ( F Sounding Rocket 중 Sounding Rocket	1/4 Airborne Comput 🔀 Command Uplink 1/4 Command Uplink 1/4 Battery 1/4 IMU 1/4 Pitch Valve 1/4 Plumbing 🗊 Plumbing 🚯 R/C Properties 🖄 🎽 🗉 🕼
Plumbing Power Relay	• III	ty Criticality & Reliability Editor	
Roll Valve	Narrative		
⊳ 🖏 Star Tracker ⊳ 🙀 Tank	Reuired Narrative in case the options are not explanetory enough.	Item / Failure Selection Criticality 👻	Very Low
Fight Strengthered Strengthe	Redired Narrative in case the options are not explanetory enough.	▲ Sounding Rocket	
Vaw Valve Instrument		A 📲 Convert	1 2 3 4 5 6 7 8 9 10
Sarachute Recovery		<ul> <li>Gas - Mass flow rate</li> <li>Pneumatic - Mass flow rate</li> </ul>	High
Kocket Engine [3/3]		Preumatic - Mass flow rate	Probability/Occurrence 2.0
▼ Failure Concepts 🖄 🔽 ♦ 🗘 ●		Discrete - Data	
Search	L	OK Discrete - Data Discrete - Data	Extremely/mprobable
Assembly and reassembly		Gas - Mass flow rate	
Design		<ul> <li>Gas - Mass flow rate</li> <li>Gas - Mass flow rate</li> </ul>	
<ul> <li>Maintenance</li> <li>Manufacturing</li> </ul>		🔺 📲 Inhibit	Severity 7.0
Operation	Celestial ACS - System Model	<ul> <li>Mechanical - linear - Linear velocity</li> <li>Payload</li> </ul>	Severe Major
Transportation		<ul> <li>Rocket Engine</li> </ul>	
🤧 Palette 🛛 🧧 Library 📴 Outline			Low
Search  Components [107]			Probability/Occurrence 4.0
<ul> <li>Components [107]</li> <li>Parts [134]</li> </ul>			Extremely Remote
			1 2 3 4 5 6 7 8 9 10 15
			• "

· · · + ·

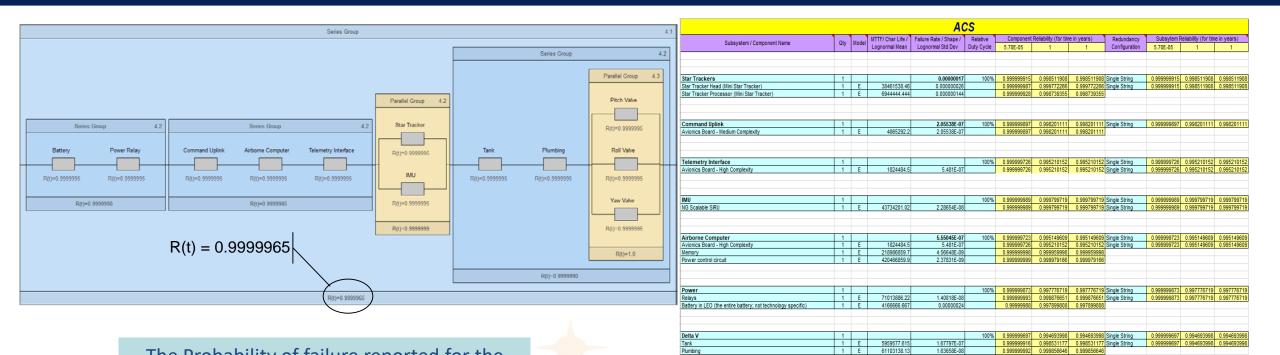
 $\mathbf{R} \mathbf{A} \mathbf{M} \mathbf{S}$ 

## **MBSMAI Phase 1: Sounding Rocket Modeling**



#### NASA MODEL BASED Safety and Mission Assurance

### **MBSMAI** Phase 1: Sounding Rocket Probability Analysis Evaluation



Thruster Valve

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.

3 | F

1 41053E

0.9963

R(t) = 0.999998923

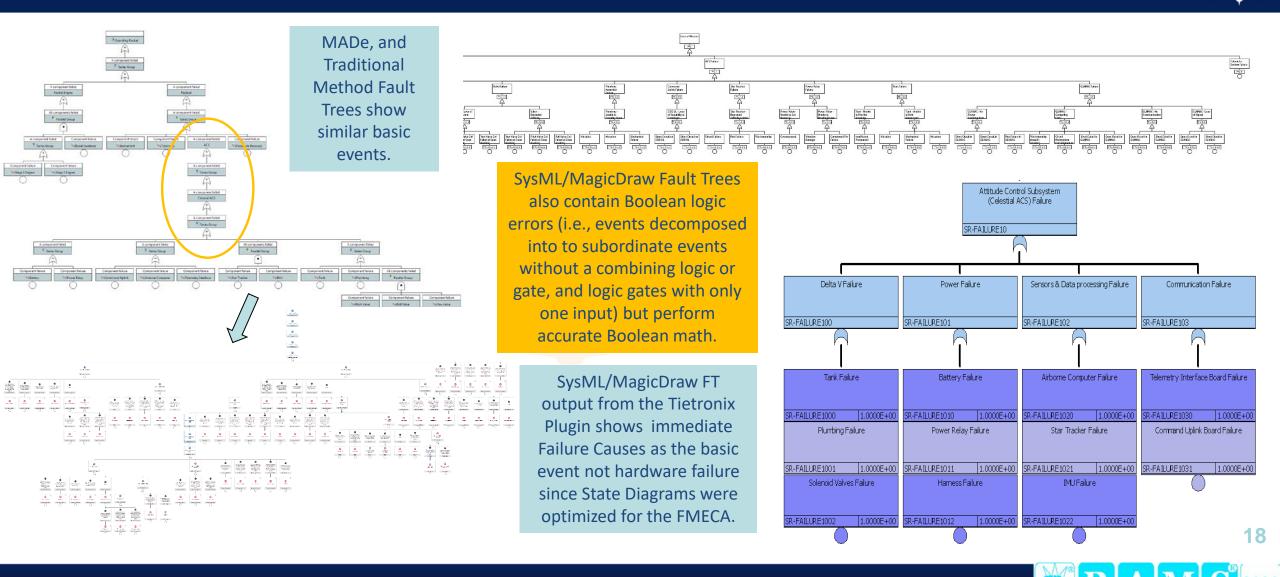
#### NASA MODEL BASED Safety and Mission Assurance

17

ACS Total

### + + +

### **MBSMAI** Phase 1: Sounding Rocket Fault Tree Evaluation



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

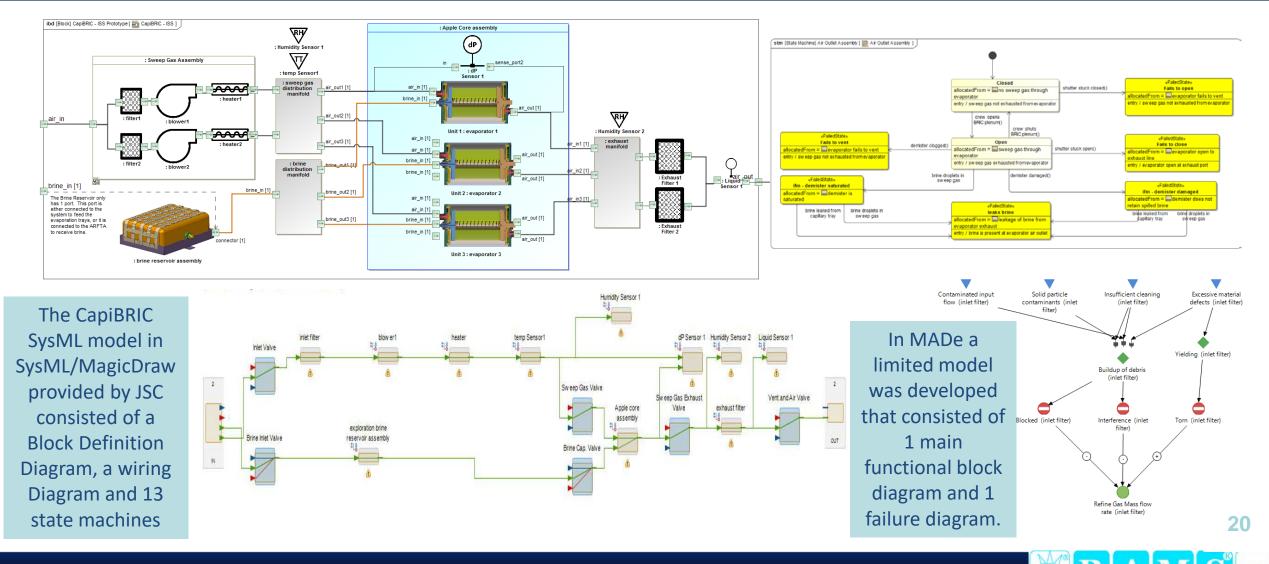
81 rows F	ailure Level: .	ALL Criticality Level: AL	LL End Effect: ALL											Base Model 6-8-2018					FM	ECA (RPN, PHMT)						Aug 8, 2018	18 1:07:20 PM
, System	Subsyst		Potential Falure M	. Inmediate Failure Eff	fect End Effect	Potential Cause(s)	Fault Propagation Path (Explicit)																				
Soundin		Sounding Sounding	SR Mission Failure	Loss of Mission	Loss of Mission 1	ACS Faled				TTT	TIT		-	SYSTE	EM Sounding Rocket :	> Payload > ACS > Celestia	al ACS > Battery							DATE Aug 8, 201	8 1:07:20 PM		
Soundin		Sounding Sounding	SR Mission Failure	Loss of Mission	Loss of Mission 1 Loss of Mission 1	Telenetry System Faled Parachute Recovery Faled								INDENTURE LEVI	FLS									SHEET 35	0	F 111	
Soundin		Sounding Sounding	SR Mission Failure	Loss of Mission	Loss of Mission 1	Rocket Engine Failed																					
Soundin		Sounding Sounding	SR Mission Falure	Loss of Mission	Loss of Mission 1	Science Instrument Palled								REFERENCE DRAWIN	NG									COMPILED BY	Youngjo Lim		
Soundin	Celestial	Sounding Celestal	Arborn Computer F.	. GLNMAC Falure	Loss of Mission 3	Error in Executing Commands and/or D.	Celestial ACS Arborn Computer Failure>> Signal: GUMAC Failure>> Celestial ACS.							MISSIC	ON Test Mission									APPROVED BY			
Soundin	Celestal	Sounding Celestial Sounding Celestial	Airborn Computer F. Airborn Computer F.	. GLNMAC Falure 	Loss of Mission 3 Loss of Mission 3	Droperable if no Redundant Paths Aval	Celestal ACS Arborn Computer Falure>> Signal: GUMIAC Falure>> Celestal ACS. Celestal ACS. Arborn Computer Falure>> Signal: GUMIAC Falure>> Celestal ACS.																				
Soundin	Celestal	Sounding Celestal	Arborn Computer F.	GLNMAC Falure	Loss of Mission 3	No Commanding to from and of the Su	Celestial ACS. Arborn Computer Falure >> Signal: GLNMAC Falure >> Celestial ACS.						- I I					EMODE	CAURTE	OF FAILURE	FAULT	E EFFECTS	1	1	-	RITICALITY	
Soundin	Celestial	Sounding Celestial	Battery Falure	Battery Failure	Loss of Mission 3	Loss of Battery	Celestial ACS.Battery Falure>> Signal: Battery Falure>> Celestial ACS.ACS Falure	>> Signal: ACS Faled>> Sour	nding Rocket, SR Mission Failure	>> Signal				ITEM NO.	ITEM/PHYSICAL	FUNCTION/		IE MODE	CAUSES	FFAILURE	FAILUR	ie errecis	DETECTION	COMPENSATING		RITCALITY	
Soundin	Celestal	Sounding, Celestal	Battery Falure	Battery Falure	Loss of Mesion 3	Degraded Power Storage Capabilities	Celestial ACS Battery Failure>> Signal: Battery Failure>> Celestial ACS ACS Failure							TIEM NO.	DESCRIPTION	NARRATIVE	FUNCTIONAL	FAULT	MECHANISM	CAUSE	NEXT HIGHER LEVEL	L END EFFECTS	METHODS	PROVISIONS	o s	D	RPN
Soundin	Celestal	Sounding Celestial	Battery Falure Compared Unlerk Fail	Battery Fakure Command Univie Pails	Loss of Mission 3	Major Effect to Nax Derated Current	Celestial ACS. Battery Falure >> Signal: Battery Falure >> Celestial ACS. ACS Falure						-				FAILURE									-	
Soundin	Celectral	Sounding Celestial Sounding Celestial	Plumbing Assembly F	Plumbing Assembly Fa		Loss of Cormanding Capabilities Degraded Pointing Capabilities	Celestial ACS.Command Uplink Falure >> Signal: Comand Uplink Falure >> Celestial Celestial ACS.Plumbing Assembly Falure >> Signal: Plumbing Falure >> Celestial ACS								Battery	Supply Electrical Voltag	ge Supply Electrical	Short circuit	Dielectric breakdown		Transmit Discrete	Convert Discrete	Operator	Abort Mission,	10.0 8.0	10.0	800
Soundin	Celestial	Sounding Celestal	Power Relay Falure	Power Relay Failure	Loss of Mission 2	Loss of Current to the Battery	Celestial ACS.Power Relay Falure >> Signal: Power Relay Falure >> Celestial ACS.A				+++++	+++++			An electrical battery	Modelled as an	Voltage Low			exceeded	Data Low (Celestial ACS) AND Convert	Data Low (Sounding Rocket)	Observation, Sensing Device				
Soundin	Celectial	Sounding Celestal	Power Relay Falure	Power Relay Failure	Loss of Mission 3	Battery Discharged, Overcharged or Los	Celestial ACS Power Relay Falure>> Signal: Power Relay Falure>> Celestial ACS A	CS Falure>> Signal: ACS Fale	ed>> Sounding Rocket.SR Missi	ion Falure					is a combination of	electrical storage device					Gas Mass flow rate			Quality Control and Robust Reliability			
Soundin	Celestial	Sounding Celestial	Pressurized Tank Fai		Loss of Mission 3	Degraded Pointing Capabilities	Celestial ACS Pressuraed Tark Falure >> Signal: Tark Falure >> Celestial ACS ACS								one or more electrochemical	which converts stored chemical energy into	in failed string No connection of				Low (Celestial ACS) AND Convert Gas		No current fluctuation detected				
Soundin	Celestal	Sounding Celestal Sounding Celestal	Star Tracker Falure	Star Tracker Failure	Loss of Mission 3 al Loss of Mission 3	Lost Fine Pointing Capabilities Enoperable if no Redundant Paths Aval	Celestal ACS.Star Tracker Falure>> Signal: Star Tracker Falure>> Celestal ACS.A Celestal ACS.Telemetry Interface Board Falure>> Signal: Telemetry IF Board Falure								cells used to	electrical energy.	battery power line				Mass flow rate Low		at different points				.
Soundin	Celestial	Sounding Celestal	Valves Falure	Valve Failure	Loss of Mission 3	Degraded Pointing Capability	Celestal ACS. Rememy Interace board Palure >> signal: Telenery In Board Palure >> Celestal ACS. Valves Falure >> Signal: Valve Falure >> Celestal ACS.ACS Falure >>								convert stored chemical energy		Short across battery connections				(Celestial ACS) AND Transmit Continuous						
Soundin	Celestial	Sounding Celestal	ACS Palure	ACS Falure	Less of Mission 2	Battery Falure	Celestial ACS ACS Falure>> Signal: ACS Faled>> Sounding Rocket SR Hission Falu	re>> Signal: Loss of Mission			1111	1111			into electrical		Failure to rease				Data Low (Celestial	1	1	1			
Soundin	Celestial	Sounding Celestial	ACS Falure	ACS Falure	Loss of Mission 2	Comand Uplink Failure	Celestial ACS.ACS Falure>> Signal: ACS Faled>> Sounding Rocket.SR Mission Falu								energy.		Pailure to cease operation or Pailure				ACS) AND Convert						
Soundin	Celestal	Sounding Celestial	ACS Falure	ACS Falure	Loss of Mission 2	Plumbing Failure	Celesital ACS. ACS Falure >> Signal: ACS Faled >> Sounding Rocket SR Mission Falu										to operate or				Gas Mass flow rate Low (Celestial ACS)	1					. [
Soundin	Celestial	Sounding Celestial Sounding Celestial	ACS Falure ACS Falure	ACS Failure ACS Failure	Loss of Mission 2 Loss of Mission 2	Power Relay Failure Tank Failure	Celestial ACS.ACS Failure>> Signal: ACS Failed>> Sounding Rocket.SR Mosion Failure>> Signal: ACS Failed>> Sounding Rocket.SR Mission Failure>> Signal: ACS Failed>> Sounding Rocket.SR Mission Failure>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>> Signal: ACS Failed>>> Sounding Rocket.SR Mission Failure>>>>>>>>>>>>>>>>>>>>> Signal: ACS Failed>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>			2.00			-1				Intermittent operation or Loss of				con (consult ACS)						
Soundin	Celestal	Sounding Celestial	ACS Falure	ACS Palure	Loss of Mission 2	Star Tracker Falure	Celestial ACS.ACS Falure>> Signal: ACS Faled>> Sounding Rocket.SR Mission Falu	re>> Signal: Loss of Merico		jere -							output	L			Transmit Discrete	Convert Gas Mass	Operator	Abort Mission,	10.0 9.0	10.0	900
Soundin	Celectial	Sounding (celestal	ACS Falure	ACS Falure	Loss of Mission 2	Telemetry D <sup>I</sup> Board Falure	Celestial ACS ACS Falure>> Signal: ACS Faled>> Sounding Rocket SR Mission Falu	re>> Signal: Loss of N Item	Component Fu	unction Fa	silure Mode	Failure	Local	Subsystem End E	iffect(s) Detectio	on Compensation	Criticalit Connents	SP			Data Low (Celestial ACS) AND Convert	flow rate Low (Sounding Rocket)	Observation, Sensing Device	Redesign Component			
Soundin	Celestial	Sounding Celestal	ACS Falure	ACS Failure	Loss of Mission 2	Valve Falure	Celestial ACS.ACS Falure>> Signal: ACS Faled>> Sounding Rocket.SR Mission Falu	re>> Signal: Loss of N		N-MAC can be Fai	Anna ba anna 🛛 🔿		Effect(s)	Enecdal	mission # No data sign		,	<u>,</u>			Gas Mass flow rate	(Sounding Rockec)		Quality Control and			
Soundin	Celes6al	Sounding Celestial	ACS Falure	ACS Falure	Loss of Mission 2	GLNMAC Failure	Celesitial ACS. ACS Failure >> Signal: ACS Failed >> Sounding Rocket SR Mission Failure			o provide a full da	ita ci	ircuit	Loss a signal	redundant path remainin		an Headingan padi					Low (Celestial ACS)		No current fluctuation detected	Robust Reliability Analysis			.
Soundin	Ceesoa	Sounding Bettery Sounding Bettery	Power Harness Fale. Power Harness Fale.	Battery - Short Across Battery - Short Across	s Loss of Mission 4 s Loss of Mission 4	Component,Pin Failure in Battery Vibration Damage to Battery	Battery Power Harness Failed Short>> Signal: Loss of Battery>> Celestial ACS.Batt Battery Power Harness Failed Short>> Signal: Loss of Battery>> Celestial ACS.Batt			stion polution				fails.							AND Convert Gas Mass flow rate Low		at different points	Analysis			
Soundin	Celettal	Sounding Battery	Power Harness Fale	Battery - No Cornect		Component,Pin Failure in Battery	Eattery Power Harness Faled Open>> Sanal: Loss of Eattery>> Celestial ACS Batt			ding position, Co s. sttitude, and int		Part Failure, P Stouit Failure	Computing	Errors in Loss of j executing poience		hal Redundant path					(Celestial ACS) AND						
Soundin	Celestial	Sounding Battery	Power Harness Fale.	Battery - No Connects	o Loss of Mission 4	Vibration Damage to Battery	Battery Power Harness Pailed Open >> Signal: Loss of Battery >> Celestial ACS.Batt	tery Falure>> Signal: 8		stes to control pai		e Workmanshin	errora	contrands mission	, Loop or						Transmit Continuous Data Low (Celestial						.
Soundin	Celestial	Sounding Battery	Wire Breakage	Battery - Reduction of	f Loss of Mission 4	Wbration Damage to Battery	Battery. Wre Breakage >> Signal: Major Effect to Max Denated Current Carrying Cap		systems f	for opinning and pro				and/or data							ACS) AND Convert						
Soundin	Celestal	Sounding Battery	Loss of One String	Battery - Cannot Stor	e Loss of Mission 4	Joint Failure (Nickle Tab, Spot Weld, 5	Battery Loss of One String >> Signal: Degraded Power Storage Capabilities >> Celes		non-spi	inning rockets.				gathering and							Gas Mass flow rate						
Soundin	Celestial	Sounding Bettery Sounding Power Relay	Loss of One String Faled Short	Battery - Cannot Stor Power Relay - Unable		Cell Short/Open Crouit in Battery Overstressed	Battery Loss of One String>> Signal: Degraded Power Storage Capabilities>> Celes Power Relay, Failed Short>> Signal: Battery Discharged, Overcharged or Lost>> Ce			Lo	ss of interface. C	ircuit Failure -	No valid	Minoreffect No effect	ct Faulty	Software Quality					Low (Celestial ACS)						
Soundin	Criedal	Sounding Power Relay	Faled Open	Power Relay - Unable		Woration Damage	Power Relay, Failed Open>> Signal: Loss of Current to the Battery>> Celestial ACS.			sig	anal O	pen/Shorl/Out	telemetry		Telemetry	control					Transmit Discrete	Convert Gas Mass	Operator	Abort Mission.	10.0 9.0	10.0	900
Soundin	Celestal	Sounding Power Relay	Faled Open	Power Relay - Unable		Component/Pin Failure	Power Relay, Failed Open >> Signal: Loss of Current to the Battery >> Celestial ACS	Power Relay Failure>1				f Range									Data Low (Celestial	flow rate Low	Observation, Sensing		1000 500		
Soundin	Celestial	Sounding Command	Loss of Signal	CMD UL - Loss of Cap		Open Circuit on CMD UL	Command Uplink Board.Loss of Signal >> Signal: Loss of Commanding Capabilities >>				ss of power C pply path O	ircuit Failure - 1 Ioan/Short	No power remitable from	Inoperable # no Loss of a redundant remainin		y Redundant path					ACS) AND Convert Gas Mass flow rate	(Sounding Rocket)	Device	Quality Control and			
Soundin	Celestal	Sounding Command	Loss of Signal	CMD UL + Loss of Cap	a Loss of Mission 4	Short Circuit on CMD UL Circuit Palure	Command Uplink Board Loss of Signal >> Signal: Loss of Commanding Capabilities >>			14	pp-y pain a	aprill oner	power node	paths. fails.							Low (Celestial ACS)		No current	Robust Reliability			
Soundin	Celestal	Sounding Star Tracker Sounding Star Tracker	Inoperable	Star Tracker - Degrad Star Tracker - Degrad		Orost Palure Part Falure	Star Tracker Jnoperable>> Signal: Lost Fine Pointing Capabilities>> Celestial ACS.5 Star Tracker Jnoperable>> Signal: Lost Fine Pointing Capabilities>> Celestial ACS.5					ircuit Failure -	No	No commanding Loss of							AND Convert Gas		fluctuation detected at different points	Analysis			
Soundin	Celestal	Sounding Star Tracker	Inoperable	Star Tracker - Degrad		Workmanship	Star Tracker Inoperable >> Signal: Lost Fine Pointing Capabilities >> Celestial ACS-S				analfor O emory card	)pen/Short	communication	tofrom any of the remaining cubavatence fails.	ng path signal toffrom	n					Mass flow rate Low (Celestial ACS) AND		ac university points				
Soundin	Celestial	Sounding Yaw Valve	Faled Cose	Valve - Degraded Atti		Yaw Valve Coll Failed at Close Position	Yaw Valve, Failed Close >> Signal: Degraded Pointing Capability >> Celestial ACS.Val	ves Failure>> Signal: 1			alory curu			paragoteno rans.	and the second second						Transmit Continuous						.
Soundin	Celestial	Sounding Yaw Valve	Faled Open	Valve - Loss of Pressu		Yaw Valve Coll Failed at Open Position	Yaw Valve.Failed Open>> Signal: Degraded Pointing Capability>> Celestial ACS. Val			rical battery is a Lo			Cannot store	Degraded power Loss of I		ding Redundant strings 8	5				Data Low (Celestial ACS) AND Convert						
Soundin	Celestial	Sounding Pitch Valve Sounding Pitch Valve	Faled Cose Faled Open	Valve - Degraded Atti		Pitch Valve Coll Failed at Close Position	Pitch Valve Faled Close >> Signal: Degraded Pointing Capability >> Celestal ACS.Va			vation of one or bai			power in failed	storage comphiltes Loss	drop at differ	rent					Gas Mass flow rate						
Soundin	Celestal	Sounding Pitch Valve	Faled Open Faled Close	Valve - Loss of Pressu Valve - Depreded Attr		Pitch Valve Col Failed at Open Position Bol Valve Col Failed at Close Position	Pitch Valve /Faled Open>> Signal: Degraded Pointing Capability>> Celestial ACS Va Roll Valve Faled Close >> Signal: Degraded Pointing Capability>> Celestial ACS Valve			sed to convert		ickel tab, spot	otring	of a battery	points						Low (Celestial ACS)						
Soundin	Celestal	Sounding Roll Valve	Faled Open	Valve - Loss of Pressu		Roll Valve Coll Falled at Colle Position	Roll Valve Falled Cole >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Celestial ACS, Valve Falled Open >> Signal: Degraded Pointing Capability >> Cele		stored c	chemical energy	w	reld, or solder		string.				1			Transmit Discrete		Operator	Abort Mission	10.0 9.0	1 40.0	900
Soundin	Celestial	Sounding Plumbing	Fractured	Plumbing - Unable to 1	Tr Loss of Mission  4	Mechanical Failure	Plumbing. Practured >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Plumb		into ele-	ectrical energy.		oint failure libration	Reduction of	Misior effect to Loss of I	Martin Committee	ding Redundant lines to	-	_			Data Low (Celestial	Convert Gas Mass flow rate Low	Observation, Sensing		10.0 9.0	10.0	900
Soundin	Celestial	Sounding Plumbing	Gradked	Plumbing - Unable to 1		Vbration	Plumbing Cracked >> Signal: Degraded Pointing Capabilities >> Celestial ACS Plumbr			Bei				Major effect to Loss of I max denated		ang Hedundant lines to t rent maintain derating	°				ACS) AND Convert	(Sounding Rocket)	Device	Quality Control and			
Soundin	Celestial	Sounding Plumbing Sounding Tank	Corroded	Plumbing - Unable to 1 Tank - Unable to Hold		Abrasion Mechanical Fabure	Plumbing. Corroded >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Plumb				ľ			g current carrying	points	requirements.		1			Gas Mass flow rate Low (Celestial ACS)	1	No current	Robust Reliability			
Soundin	Celestal	Sounding Tank Sounding Tank	Oracked		P Loss of Mission 4	Mechanical Palure Woration	Tark Fractured>> Signal: Degraded Pointing Capabilities>> Celestial ACS Pressuria Tark Cracked>> Signal: Degraded Pointing Capabilities>> Celestial ACS.Pressuriae			_			capacity	capacity			_	_			AND Convert Gas	1	fluctuation detected				. [
Soundin	Celestial	Sounding Tank	Corroded	Tank - Unable to Hold		Abrasion	Tank.Corroded >> Signal: Degraded Pointing Capabilities >> Celestial ACS Pressuriar	ed Tank Falure >> Sign		Po	werharness C Isopen fa		No connection of battery power	Loss of battery Loss of I	Mission No current dotected at	Redundant lines to 8 maintain derating	5				Mass flow rate Low		at different points				
Sound	to an and	Providen Prot	Para 48 Para	Tank I kashin in Par		C. 20		"ressurized Tank Fail		191		libration I	line	·	different poir			1			(Celestial ACS) AND Transmit Continuous		1				
Sound								edundant Path>>1			d	lanage						_			Data Low (Celestial						.
Sound	C	N A I / N A	lagia	2000	Course		المعادية والمعالية والمعالية والمعال	edundant Path>>1 2.4		Po	wer harness C		Short across battere	Discharge of Loss of I battery, Loss of	Mission No current o fluctuation	or Quality control and 5 robust reliability	5				ACS) AND Convert Gas Mass flow rate						
Sound Sound Sound	SVG		IJIGPICI	Jraw	Sever	IIV and II	kelihood values	ible>> Celestal AC ible>> Celestal AC		fail			connections	Battery, Loss of	fluctuation detected at			1			Low (Celestial ACS)	1	1	1			
psond	_y	////	~ 0.01		0000	ity and El		MEAN CORSON AL			a	lanage		,-	different poir	nta			<b>↓</b>								
								3.1	Command Uplink Recieves			open or short		No commanding Mission	failure Verification							1.111.1				1.1	
	-	ro onto	arad	man	ually a	and can ac	orrelate to the			dafor Inhibit ding a also	•	n any of signals	commanding to computer	of computer without computer						arrati	IVA 20	Ditibr	ns w	ere u	haz	to	
	d	re ente	ered	IIIdill	udiiv c					he Uplink to the				connor					IN	unati		Junit			JCU	U	
					•				computer	м								-									
					_			5.1		ction of pipes Fra branch a edi	actured/crack M /corroded fa	fechanical I silure/sibration/	Degraded	Degraded Short II pointing miction	le of Degraded Loss of telemetre	Inspection. Guality 4 control.	4			:C					1 a 1		
	GC	FC Rick	/ dofi	initio	nc To	have a co	mplete FMECA			branch s edi ticflowinto			adjustment	capabality. Mission.		Control			CL	arity	IVIAD)	e FIVI	F(A)	outpu	TS r		
	03		v uell		115.10	nave a CC	INDIELE FIVIELA		nultiple f	flowe.	-		capabilities		cencor.			_	CI	arry			LONG	Jucha	C3 L	, ut	
								6.1		uit breaker is an Po				Loss of current Loss of I	Mission No current	Redundant lines to	5	1		_				-			
		11 A 1 A 1		1.1.1						tically operated op trical switch		silure or ·	of battery power line	r to the battery	detected at					+00	Ima	difica	tions		ha		
	2	ll think	ing a	nd d	ata en	stry for to	calculate RPN		designe	ed to protect an	a la	lanage			and the point							unica	LIONS	may	De		
	a			nu u		itiy iti tu		6.2		cal circuit from Po		Overstressed 3	Short across	Discharge of Loss of I			5	1									
			0						damaga	e caused by an she	ort	1	fuse	battery. Battery	fluctuation	robust reliability		1									

would be done at manually at the modeling stage and the plugin will extract the data and tabulate it for the user.

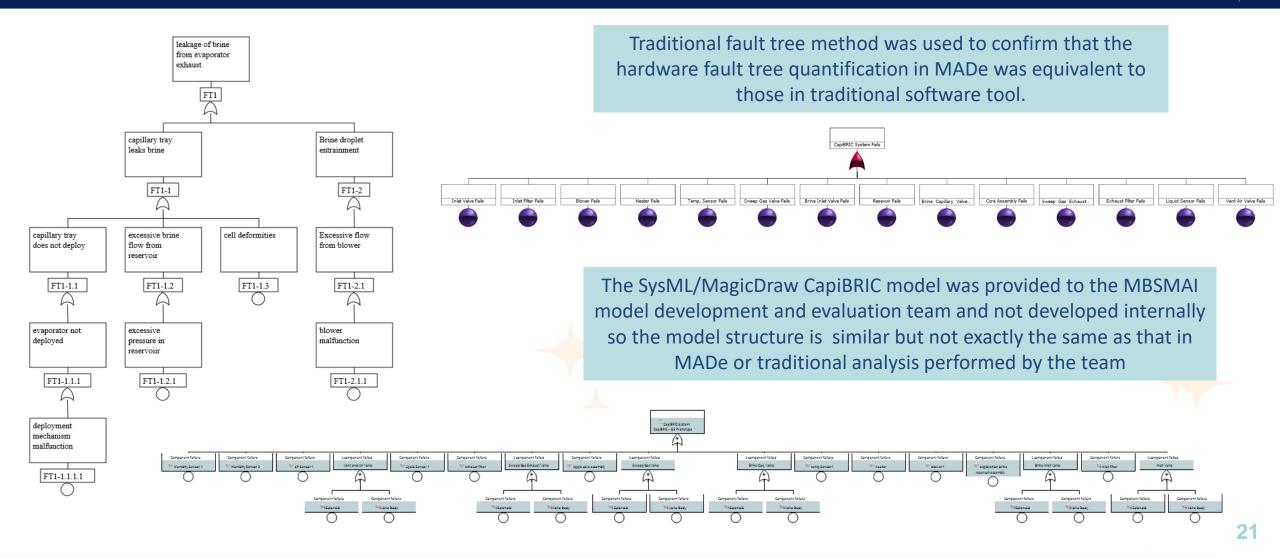


required to synthesize/input mission consequences more autonomously.

### **MBSMAI** Phase 1: HUMAN SYSTEM – CapiBRIC Modeling



### **MBSMAI** Phase 1: CapiBRIC Model Fault Tree Evaluation



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

ure	Level: ALL	Criticality Level: ALL End Effect: ALL	

Iten Herarchy	ttem	Potential Failure Mode	Immediate Failure Effect	End Effect	CRITLEVEL	Potental Cause(s)	Fault Propagation Path (Explicit)
CapIBRUC Context>>CapIBRUC - ISS Prototype	brine reservoir	No flow from reservoir	insufficient flow from reservoir	Insufficient flow through feed iso valve	2	capillary flow gap	brine reservoir.No flow from reservoir >> Signal: brine from reservoir not pro.
Cap8RSC - Baseline >> exploration brine reserv	brine reservoir	No flow from reservoir	insufficient flow from reservoir	insufficient flow through feed iso valve	2 4	capilary flow gap	brine reservoir.No flow from reservoir >> Signal: brine from reservoir not pro
CapBRUC Context>>CapBRUC - 155 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 .
CapBRIC - 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 reservor	excessive brine flow from reservoir	Personnel injury due contact with brine	5 2	excessive pressure in reservoir	brine reservor. Excessive flow from reservor >> Signal: excessive brine flow .
Cap6RIC Context>>Cap6RIC - 155 Prototype	brine reservor	leaks brine	reservor leaks brine	reservor leaks brine	1 1	reservor damaged	
CapiBRUC Context>>CapiBRUC - 155 Prototype	brine reservor	Jeaks brine	reservoir leaks brine	reservoir leaks brine	1 1	reservor seal malfunction	
CapBRUC - Baseline >> exploration brine reserv	brine reservoir	leaks brine	reservor leaks brine	reservor leaks brine	1 1	reservor damaged	
CapiBRIC - Baseline >> exploration brine reserv	brine reservoir	Jeaks brine	reservor leaks brine	reservoir leaks brine	1 1	reservoir seal malfunction	
CapERIC Context>>CapERIC - ISS Prototype	feed ine solat	Failed Open	evaporator not isolated	evaporator not isolated	1 4	valve malfunction	
CapiBRIC - Baseline>>exploration brine reserv	feed ine isolat	Faled Open	evaporator not isolated	evaporator not isolated	1 4	valve malfunction	
CapIERIC Context>>CapIERIC - ISS Prototype	feed ine isolat	Faled Closed	evaporator isolated from reservoir	evaporator isolated from reservoir	1 4	valve malfunction	
CapiORIC - Baseline >> exploration brine reserv	feed ine isolat	Faled Cosed	evaporator isolated from reservoir	evaporator isolated from reservoir	1 4	valve malfunction	
CapIERIC Context>>CapIERIC - ISS Prototype	feed ine isolat	Low flow	insufficient flow through feed iso v	insufficient flow through feed iso valve	1 4	contamination	
CapERIC Context>>CapERIC - ISS Prototype	feed ine isolati	Low flow	insufficient flow through feed iso v	insufficient flow through feed iso valve	1 4	brine from reservoir not provided	
CapiTRIC - 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 isolat	Low flow	insufficient flow through feed iso v	insufficient flow through feed iso valve	1 4	brine from reservoir not provided	
CapIERIC - RuERICs Cube > >blower	blower	Faled off	No flow from blower	No flow from blower	1 4	blower malfunction	
CapiERIC - 1fil Apple Core >>blower	blower	Faled off	No flow from blower	No flow from blower	1 4	blower malfunction	
CapifiRIC - RufiRICs Cube > shiower	blower	Faled high	Excessive flow from blower	demister is saturated	3 4	blower malfunction	blower Faled high>> Signal: excessive flow from blower>> Capillary Trav.Br.
CapERIC + 1fil Apple Core > >blower	blower	Faled high	Excessive flow from blower	demister is saturated	3	blower malfunction	blower Falled high >> Signal: excessive flow from blower >> Capillary Tray Br.
CapERIC - RuERICs Cube > >blower	blower	Faled low	Insufficient flow from blower	capillary tray contains brine	3	blower malfunction	blower Faled low>> Signal: insufficient flow from blower>> heater.No or Lo.,
CapERIC + RuBRICs Cube > >blower	blower	Faled low	Insufficient flow from blower	Water is not recovered	5 3	blower malfunction	blower.Faled low >> Signal: insufficient flow from blower >> heater.No or Lo
CapiERIC - RuBRICs Cube > >blower	blower	Faled low	Insufficient flow from blower	capillary tray contains brine	3 4	insufficient flow to blower	blower Faled low>> Signal: insufficient flow from blower>> heater.No or Lo.
CapiERIC - RuBRICs Cube > >blower	blower	Falled low	Insufficient flow from blower	Water is not recovered	5 3	insufficient flow to blower	blower Faled low >> Signal: insufficient flow from blower >> heater No or Lo.
CapERDC - 1fil Apple Core > >blower	blower	Faled low	Insufficient flow from blower	capillary tray contains brine	3	blower mailunction	blower Faled low>> Signal: insufficient flow from blower>> heater.No or Lo.
CapERIC + 16 Apple Core > >blower	blower	Faled low	Insufficient flow from blower	Water is not recovered	5 3	blower malfunction	blower Faled low>> Signal: insufficient flow from blower>> heater.No or Lo.
CapiBRIC - 1fil Apple Core>>blower	blower	Faled low	Insufficient flow from blower	capillary tray contains brine	3 4	insufficient flow to blower	blower.Faled low>> Signal: insufficient flow from blower>> heater.No or Lo
CapiBRIC - 1fil Apple Core>>blower	blower	Faled low	Insufficient flow from blower	Water is not recovered	5 3	insufficient flow to blower	blower Faled low>> Signal: insufficient flow from blower>> heater No or Lo
CapBRJC - Baseline >>nlet filter	inlet filter	Fails to prevent contamination	contamination in feed line	contamination in feed line	1 4	filter damaged	
CADERIC - RuBRICs Cube > >inlet filter	inlet filter	Fails to prevent contamination	contamination in feed line	contamination in feed line	1 4	fiter damaged	
CopERIC - 1fil Apple Core > >inlet filter	inlet filter	Fails to prevent contamination	contamination in feed line	contamination in feed line	1 4	fiter damaged	
CapBRIC - Baseline > > inlet filter	inlet filter	Low flow	fiter alows reufficient flow	capilary tray contains brine	4	fiter clopped	injet filter Low flow >> Signal: insufficient flow to blower >> blower.Failed low.
CopERIC - Baseline > >niet filter	whet filter	Low flow	fiter alows insufficient flow	Water is not recovered	63	fiter clooged	niet filter Low flow >> Signal: insufficient flow to blower >> blower Faled low.
CANERIC - RuBRICS Cube > Sinlet filter	inlet filter	Low flow	fiter alows insufficient flow	capilary tray contains brine	4 4	fiter clogged	niet filter.Low flow >> Signal: insufficient flow to blower >> blower.Failed low.
CanifiRIC - RufiRICs Cube > snlet filter	inlet filter	Low for	fiter alows insufficient flow	Water is not recovered	63	fiter clopped	miet filter Low flow >> Signal: insufficient flow to blower >> blower Faled low.
CapitRIC - 1fil Apple Core>pinlet filter	iniet filter	Low flow	fiber alows insufficient flow	capilary tray contains brine	4 4	filter clogged	niet fiter Low flow>> Signal: insufficient flow to blower>> blower Failed low.
CapilRIC - 1fil Apple Core > solet filter	inlet filter		fiber alows insufficient flow	Water is not recovered	6	filter dogged	niet filter Low flow>> Signal: insufficient flow to blower>> blower / alled low.
CapilRIC - Baselne > sheater	beater	Temperature High	Overtemp causes damage to Capill		1	beater not controlled	
CapIRIC - RuliRICs Cube > >heater	heater	Temperature High	Overtemp causes damage to Capil		1	heater not controlled	
CapiERUC - 1fil Apple Core>>heater	heater	Temperature High	Overtemp causes damage to Capil		1	heater not controlled	
CapitRIC - Baseline >>heater	heater	Temperature Low	Insufficient heat	Insufficient heat	1 4	heater malfunction	
CapIDRIC - Baseline >>heater	heater	Temperature Low	Insufficient heat	Insufficient heat	1 4	no power to heater	
CapERIC - RuBRICs Cube >>heater	heater	Temperature Low	Insufficient heat	Insufficient heat	1 4	heater malfunction	
CapIDRIC - RuBRICs Cube >>heater	heater	Temperature Low	Insufficient heat	Insufficient heat	1 4	no power to heater	
CapERIC - 1fil Apple Core >>heater	heater	Temperature Low	Insufficient heat	Insufficient heat	1 4	heater malfunction	
CapiERIC + 1fil Apple Core >>heater	heater	Temperature Low	Insufficient heat	Insufficient heat	1 4	no power to heater	
CapERIC + Baseline > >heater	heater	No or Low Flow	No flow through heater	capilary tray contains brine	2 4	insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>>
CasiERUC - 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	capilary tray contains brine	2 4	insufficient flow from blower	heater.No or Low Flow >> Signal: sweep gas not provided to evaporator >>
CapiERIC - 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>>
CapERIC + 1fil Apple Core > >heater	heater	No or Low Flow	No flow through heater	capilary tray contains brine	24	insufficient fow 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 Row>> Signal: sweep gas not provided to evaporator>>
CapiBRUC - Baseline >>heater	heater		. Personnel injury or vehicle damage		.1 1	heater power dircuit not out	
CapERIC - RuBRICs Cube >>heater	heater			Personnel injury or vehicle damage to du		heater power drout not out	
CapiBRJC - 1fil Apple Core >>heater	heater			Personnel injury or vehicle damage to du		heater power grout not out	
CapeRic - Baseline >>Controls Assembly	Controls Assembly	Fais Off	The second	the second state of the second s		power grout malfunction	
	Controls Assembly	Fails Off				power crcuit malfunction	
CapERUC - 151 Apple Core >>Controls Assembly		Fals Off				power crcuit malfunction	
						feed line cutoff croat exifunction	

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	FUNCTION/	FAILUR	E MODE	CAUSES 0	FFAILURE	FAILURE	EFFECTS	DETECTION	COMPENSATING		CRIT	ICALITY	
DESCRIPTION	FUNCTIONAL	FUNCTIONAL	FAULT	MECHANISM	CAUSE	NEXT HIGHER LEVEL	END EFFECTS	METHODS	PROVISIONS	0	5	D	RPN
nlet filter	Refine Gas Mass flow rate	Refine Gas Mass flow rate High	Tom	Yielding	Excessive material defects	Convert air_out Temperature High (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 (CapiURIC 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 - ISS Prototype) AND Convert air_out Mass flow rate Low (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. 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 nonmodelers 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.

## <sup>+</sup> Conclusion and Path Forward

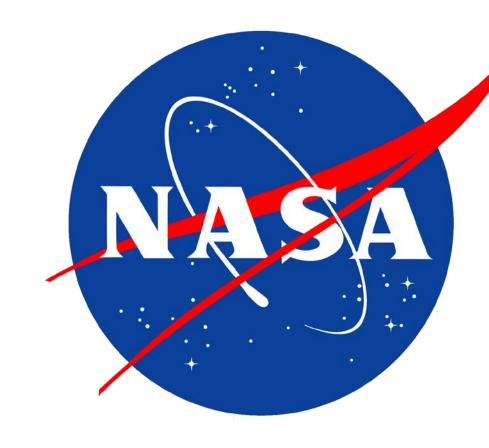
### Conclusions

- 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 MODEL BASED Safety and Mission Assurance

21

**RAMS**<sup>°</sup>2020

RA