

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 29th 2020 SESSION – 12





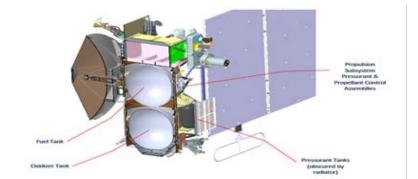
MBSMA Initiative Pathfinder Partner Project Objectives

- 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

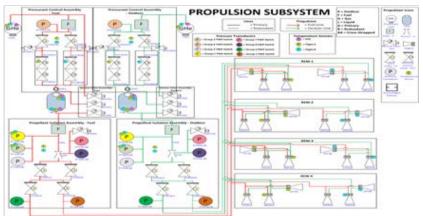
Is Model-Based Engineering valid and useable for Reliability Engineering for NASA mission Safety and Mission Assurance ?

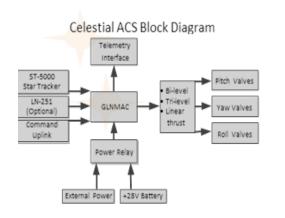
MBSMAI Methodology

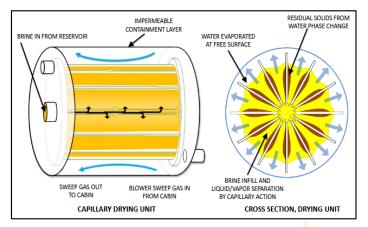
Use three mission test cases to evaluate the ability of Model-Based Engineering to support Reliability Analyses of Probability Analysis (PA)) Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), and Limited Life Analysis (LLA).

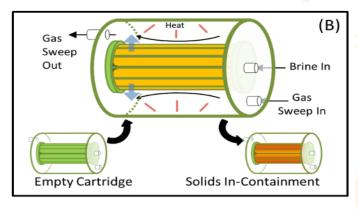




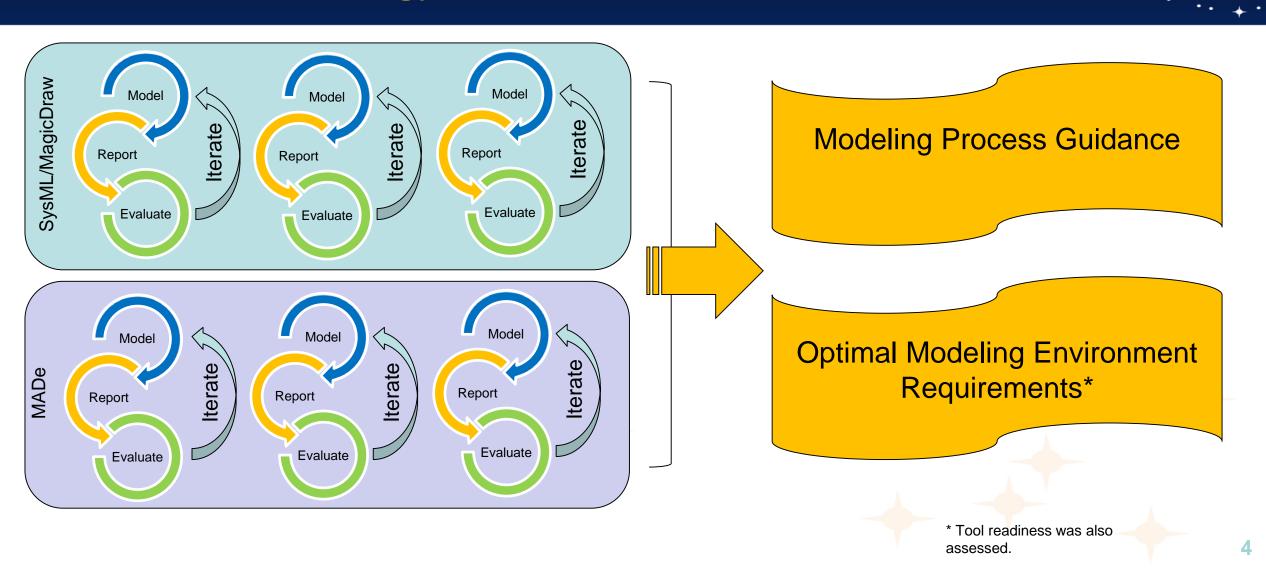


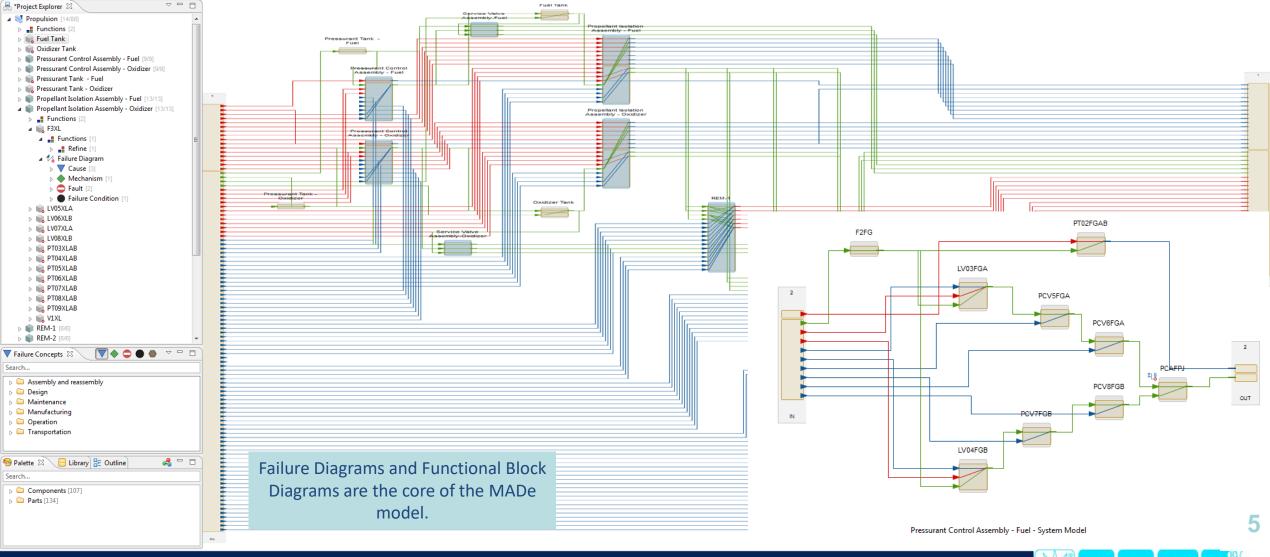


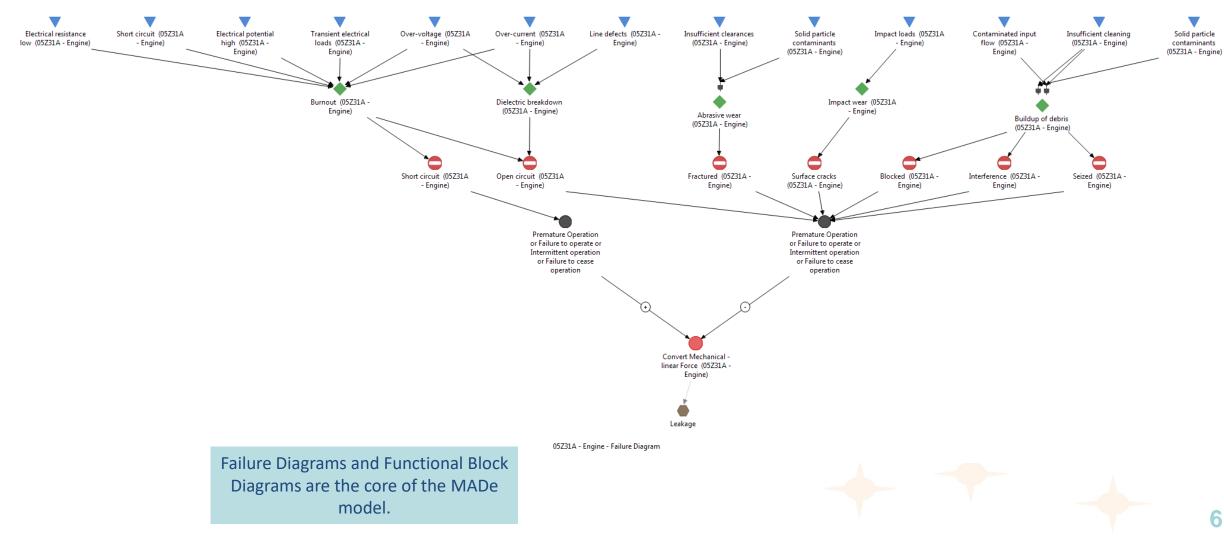


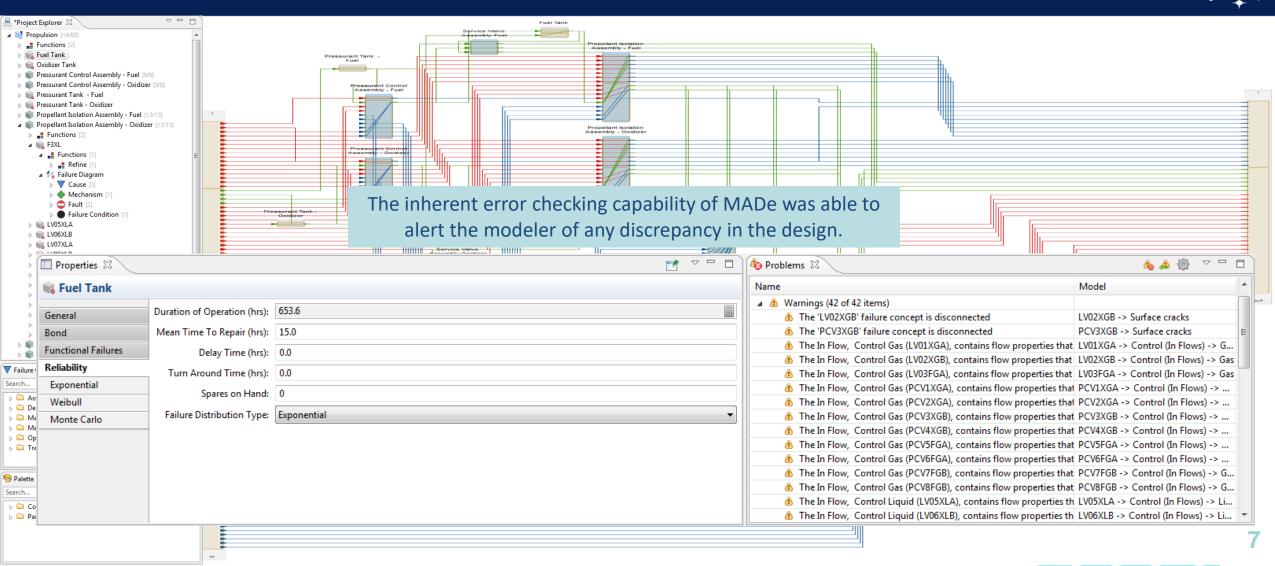


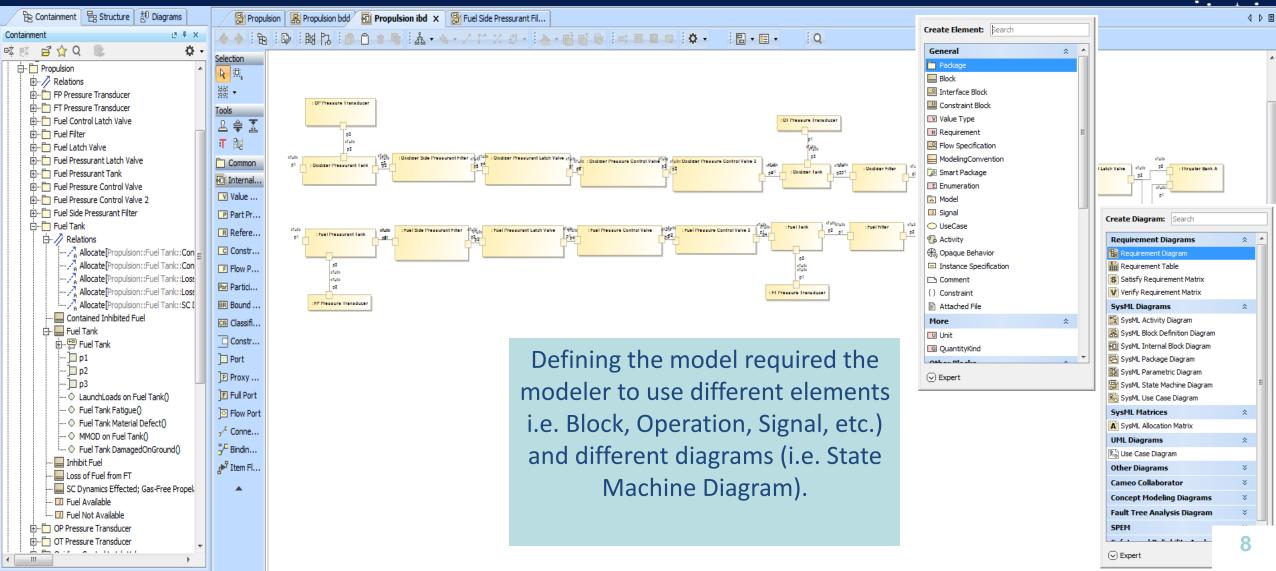
MBSMAI Methodology





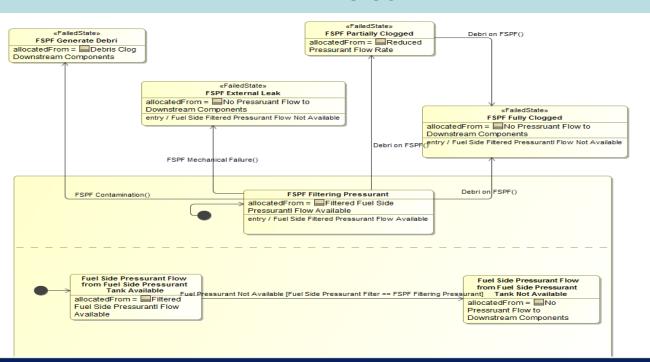


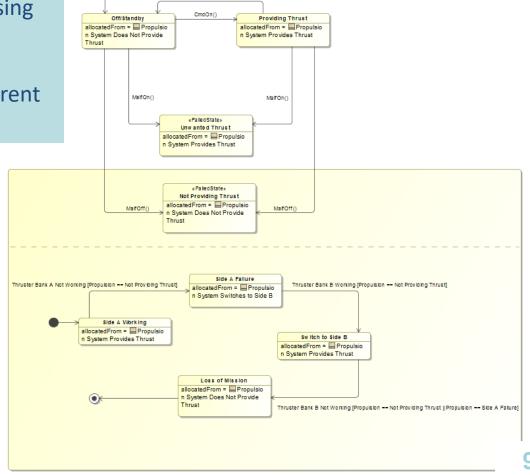




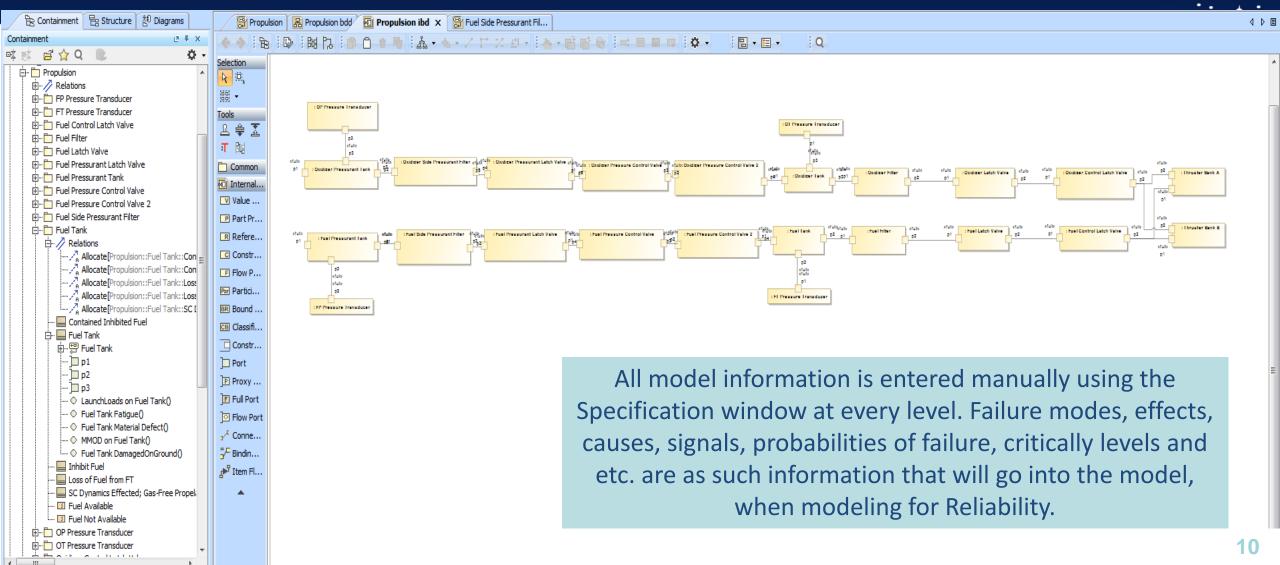
Defining Orthogonal State Machines with appropriate Guard Conditions are required in order to define Redundancy in SysML/MagicDraw when using Tietronox Plugin.

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

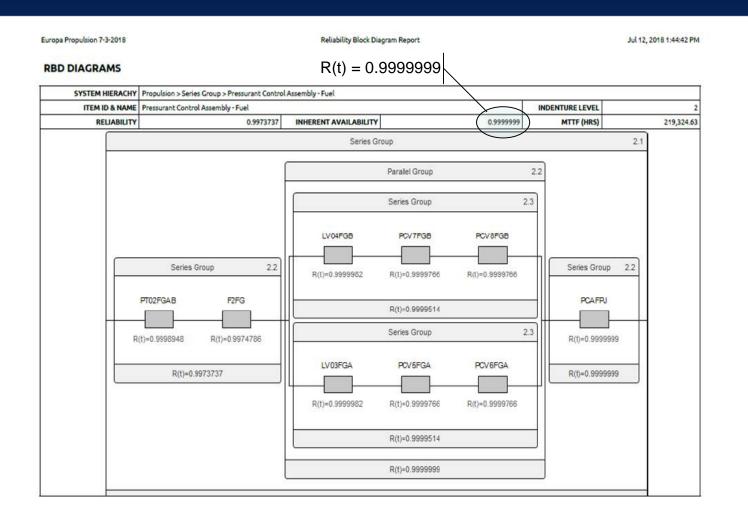




CmdOff()

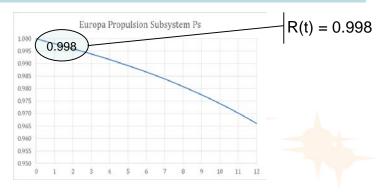


MBSMAI Phase 1: EUROPA Model Probability Analysis Evaluation



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

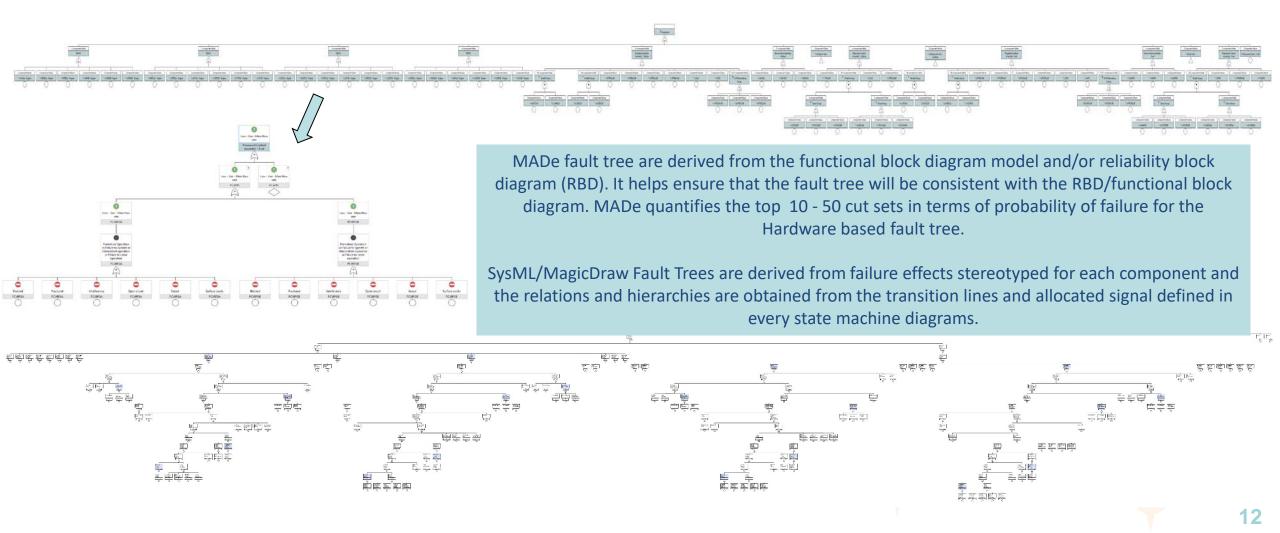


SysML/MagicDraw with Tietronix plugins does not currently support Probability Analysis. However, custom Plugins have been developed by individual enterprises.

Made



MBSMAI Phase 1: EUROPA Model Fault Tree Evaluation



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



	ITEM/		FAILURE MODES			FALURE EFFECTS				
DENTIFICATION	FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	CAUSES	NISSION PHASE / OPERATIONAL MODE	LOCAL EFFECTS	NEXT HIGHERLEVEL	DIO EFFECTS	FALURE DETECTION MIANS	PROVISIONS	CLASS
	PTEXXEAS Presure Transducer	Convert Continuous Ampitude	High Continuous Amplitude due to Circuit breeiing of the PTENTICAE as a result of dielectric breeichount caused by line defects Degraded output or Fallure to operate or intermittent operation or Loss of output.	1: PostLaunch 100%	Carvert Continuous Anolicude High	Signal Centinuous Amplicude High (Pressurent Centrol Assembly - Oxidizer)	Signal Cantinuous Amplitude High (Propulsion)	Equipment Testing, Impection, Operator Observation, Sensing Device	Change System Configuration, Modify Mexico, Modify Sersor Set, Override System	
			High Cortinuous Amplitude due to Circuit beeking of the PTC NUCAU and music of dielectric breakdown caused by overvoltage Degraded output or Falure in operate or intermittent operation or Loss of output.		Convert Continuous Angilitude High	Signal Centinudus Amplitude High (Pressurant Central Assembly - Oxidizer)	Signal Continuous Amplitude High (Propublier)			
			High Cordinacia Angilitate due to Circuit- breeling of the PTE SICAB are must of defect in breakform caused by overcorrect. Degraded output or Failure to operate or intermittent operation or Loss of output		Convert Continuous Anglitude High	Signal Centricous Amplitude High (Pressurant Central Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			
			High Continuous Amplitude due to Cincult breeling of the PTCHCAB as a neutrol burrout is used by over-cornect. Degraded output or Failure to operate or intermittent operation or Loss of output.		Convert Continuous Amplitude High	Signal Continuous Amplitude High (Fresurant Costrol Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			
			High Continuous Amplitude due to Circuit bessing of the PTE-SCAB as a result of burnout caused by overwoltage. Degraded output or Failure to operate or intermittent operation or Loss of output.		Convert Continuous Anglitude High	Signal Continuous Amplitude High (Fressurent Control Assembly - Oxidizer)	Signal Continuous Amplitude High (Propulsion)			1
			High Continuous Amplitude due to Circuit beeling of the PTC SCEAR as a result of burnout caused by electrical resistance live Degraded output or Fallure to operate or intermittent operation or Loss of output.		Convert Continuous Amplitude High	Signal Canthucus Amplitude High (Pressurant Control Assembly - Oxidose)	Signal Continuous Amplitude High (Propulsion)			*
			High Cortinuous Angiltude due to Corcit breeling of the PTENCEAR as a result of burnout caused by short circuit. Degraded output or Fallure to operate or Intermittent operation or Loss of output.		Convert Continuous Amplitude High	Signal Carbituous Amplitude High (Pressurant Central Assembly - Oxidizer)	Signal Corbinuous Amplitude High (Propulsion)			
			Low Continuous Amplitude due to Fracturing of the PROSCAR as a result of abratises even caused by insufficient dearwaves and solid particle contaminants. Deprechel output or Fallure to operate or		Convert Continuous Amplitude Low	Signal Cantinuous Amplitude Low (Fressurant Control Assembly - Oxidizer)	Signal Continuous Anglitude Law (Propulsion)	Equipment Testing, Impedition, Operator Observation, Sensing Device	Change System Configuration, Modify Massien, Modify Sensor Set, Override System	

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

	Relative Severity of Failure Modes												
Criticality Risk Matrix	Severity Value	1	2		3		5						
	Severity Category	4	3	3	2/2R	2	1R	1/19					
	<1												
	1												
Occurrence	2												
Likelihood of	3												
	4												
	5												

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

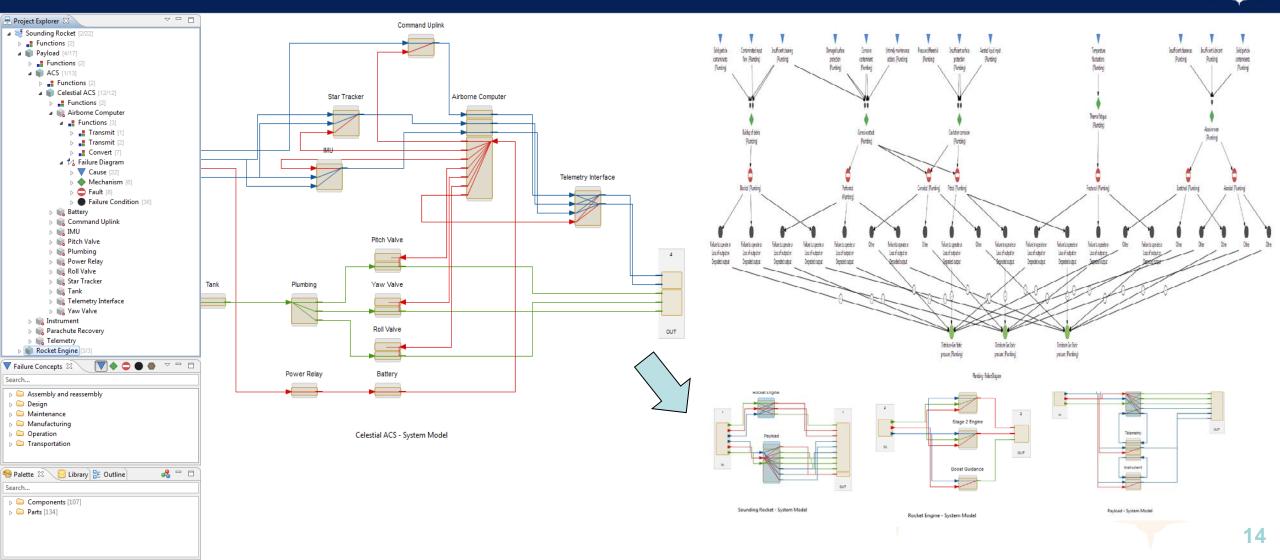
Stem Hier	Item .	Potental Failure Mode	Immediate Failure Effect	End Effect	land.	***	Potental Cause(s)	Fault Propagation Path (Explicit)
ropulsion	Propulsion	Unwanted Thrust	Propulsion System Provides Thrust	Propulsion System Provides Thrust	15		MafOn	
ropulsion		Not Providing Thrust	Propulson System Does Not Provide Thr	Propulsion System Does Not Provide Thrust	1	-	MaROFF	
	Fuel Latch Valve	Internal Leak	No Effect from Fuel Latch Valve	No Effect from Fuel Latch Valve	1	-	FLV Contamination	
	Fuel Latch Valve	Back-Relef Falure	No Effect from Fuel Latch Valve	No Effect from Fuel Letch Valve	1		PLV Mechanical Failure	
	Fuel Latch Valve	External Leak	Loss of Fuel from Fuel Latch Valve	Loss of Fuel from Fuel Latch Valve	1	+	FLV Workmanship Issue	
	Fuel Latch Valve	External Leak	Loss of Fuel from Fuel Latch Valve	Loss of Fuel from Fuel Latch Valve	1	+	FLY Waterhammered	
	Fuel Latch Valve	Faled Close	Puel Latch Valve Does Not Provide Fuel	Fuel Control Latch Valve Does Not Provide Fue	12		PLV Col Palure	Fuel Latch Valve Failed Close>>> Signal: Fuel Latch Valve is Not Providing Fuel && Fuel Control Li
ropulson	Fuel Latch Valve	Faled Open	Fuel Latch Valve Provides Fuel	Fuel Control Latch Valve Provides Fuel	2		PLV Col Falure	Fuel Latch Valve, Failed Open>> Signal: Fuel Latch Valve is Providing Fuel && Fuel Control Latch
ropulsion	Fuel Control La	Internal Leak	No Effect from Fuel Control Latch Valve	No Effect from Fuel Control Latch Valve	1		FCLV Contamination	
ropulsion	Fuel Control La.	Back Relef Falure	No Effect from Fuel Control Latch Valve	No Effect from Fuel Control Latch Valve	1		FCLV Mechanical Failure	
ropulsion	Fuel Control La	External Leak	Loss of Fuel From Fuel Control Latch Valve	Loss of Fuel From Fuel Control Latch Valve	1	т	FCLV Workmanship Issue	
ropulsion	Fuel Control La	External Leak	Loss of Fuel From Fuel Control Latch Valve	Loss of Fuel From Fuel Control Latch Valve	1		PGLY Waterhammered	
Propulsion	Fuel Control La	Faled Close	Fuel Control Latch Valve Does Not Provi	Thruster Bank B Loss of Thrust	1		FCLV Col Falure	Fuel Control Latch Valve-Failed Close>> Signal: FCLV Does Not Provide Fuel Flow>> Thruster Bit
ropulsion	Fuel Control La	Faled Close	Fuel Control Latch Valve Does Not Provi	Thruster Bank A Loss of Thrust	1		FCLY Col Falure	Fuel Control Latch Valve Failed Close>> Signal: FCLV Does Not Provide Fuel Flow>> Thruster &
Propulsion	Fuel Control La	Faled Open	Fuel Control Latch Valve Provides Fuel	Thruster Bank & Provides Thrust	1		FCLV Col Falure	Fuel Control Latch Valve Failed Open>> Signal: FCLV Provides Fuel Flow>> Thruster Bank 8-On
ropulsion	Fuel Control La	Falled Open	Puel Control Latch Valve Provides Puel	Thruster Bank A Provides Thrust	1		FCLV Col Falure	Fuel Control Latch Valve, Failed Open >> Signal: PCLV Provides Fuel Flow >> Thruster Bank A-Or
ropulsion	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	1		MMOD on Fuel Tank	Fuel Tank External Leak>> Signal: Fuel Not Available>> Fuel Filter Fuel Flow from Fuel Tank No
ropulsion	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	1		Fuel Tank Fatigue	Fuel Tank External Leak>> Signal: Fuel Not Available>> Fuel Filter Fuel Flow from Fuel Tank N
ropulsion	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	1		LaunchLoads on Fuel Tank	Fuel Tank External Leak>> Signal: Fuel Not Available>> Fuel Fifter Fuel Flow from Fuel Tank N
ropulsion	Fuel Tank	External Leak	Loss of Fuel from FT	No Fuel Flow to Downstream Components	1		Fuel Tank Material Defect	Fuel Tank External Leak >> Signal: Fuel Not Available >> Fuel Filter Fuel Flow from Fuel Tank No
ropulsion	Fuel Tank	F940 Fractured Structure	SC Dynamics Effected; Gas Free Propel	SC Dynamics Effected; Gas-Free Propelant f	1		LaunchLoads on Fuel Tank	
ropulsion	Fuel Tank	PMD Fractured Structure	SC Dynamics Effected; Gas Free Propel	SC Dynamics Effected; Gas Free Propelant f	1	П	Fuel Tank DamagedOnGround	
ropulsion	Fuel Tank	PMD Fractured Structure	SC Dynamics Effected; Gas-Free Propel	SC Dynamics Effected; Gas-Free Propelant f	1		Puel Tank Material Defect	
ropulsion	Thruster Bank B	Thruster 81 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster Bit Valve Coll Failure	Thruster Bank 8-Orthogonal Thruster 8: Failure>> Signal: Thruster Bank 8 Not Working && Pro
ropulsion	Thruster Bank B	Thruster traives 81 Failed Open.	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Mechanical Falure of Thruster81.	Thruster Bank B-Orthogonal, Thruster Valves 81 Failed Open>> Signal: Thruster Bank B Workin
ropulsion	Thruster Bank B	Thruster Valves 81 Failed Open	No Effect from Thruster Bank 8 Failure	Propulsion System Provides Thrust	2	-+1	Excessive Heat Soakback from Thruster81	Thruster Bank 8-Orthogonal Thruster Valves 61 Failed Open>> Signal: Thruster Bank 8 Workin
ropulsion	Thruster Bank B	Thruster Valves B2 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Mechanical Falure of Thruster82	Thruster Bank B-Orthogonal, Thruster Valves B2 Failed Open>> Signal: Thruster Bank B Working
ropulsion	Thruster Sank B	Thruster Valves 82 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from Thruster82	Thruster Bank 5-Orthogonal. Thruster Valves 82 Failed Open>> Signal: Thruster Bank 5 Working
repulsion	Thruster Bank B	Thruster Valves B3 Falled Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Excessive Heat Sookback from Thruster83	Thruster Bank B-Orthogonal. Thruster Valves B3 Failed Open>> Signal: Thruster Bank B Working
ropulsion		Thruster Valves 83 Failed Open	No Effect from Thruster Bank B Falure	Propulsion System Provides Thrust	2		Mechanical Falure of Thruster®3	Thruster Bank B-Orthogonal. Thruster Valves B3 Failed Open>> Signal: Thruster Bank B Working
	Thruster Bank B	Thruster Valves 84 Failed Open	No Effect from Thruster Bank 6 Failure	Propulsion System Provides Thrust	2	111	Mechanical Failure of Thruster84	Thruster Bank B-Orthogonal, Thruster Valves B4 Failed Open>> Signal: Thruster Bank B Working
ropulsion	Thruster Bank B	Thruster Valves 84 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust.	2 .	100	Excessive Heat Soakback from Thruster84	Thruster Bank 8-Orthogonal. Thruster Valves 84 Failed Open>> Signal: Thruster Bank 8 Working
ropulsion	Thruster Sank B	Thruster Valves BS Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from ThrusterB5	Thruster Bank 8-Orthogonal, Thruster Valves 85 Failed Open>> Signal: Thruster Bank 8 Working
ropulsion	Thruster Sank B	Thruster Valves B5 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Mechanical Falure of Thruster85	Thruster Bank 8-Orthogonal. Thruster Valves 85 Failed Open>> Signal: Thruster Bank 8 Workin
ropulsion	Thruster Bank B	Thruster Valves B6 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	5		Mechanical Falure of Thruster86	Thruster Bank B-Orthogonal. Thruster Valves B6 Failed Open>> Signal: Thruster Bank B Working
ropulsion		Thruster Valves B6 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2	***	Excessive Heat Soakback from Thruster(16	Thruster Bank B-Orthogonal. Thruster Valves B6 Failed Open>> Signal: Thruster Bank B Working
	Thruster Sank B	Thruster Valves 67 Failed Open	No Effect from Thruster Bank 8 Failure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from Thruster87	Thruster Bank 5-Orthogonal Thruster Valves 57 Failed Open>> Signal: Thruster Bank 5 Working
ropulsion	Thruster Bank B	Thruster Valves 87 Falled Open	No Effect from Thruster Sank 8 Failure	Propulsion System Provides Thrust	2		Mechanical Failure of Thruster87	Thruster Bank B-Orthogonal, Thruster Valves B7 Falled Open>> Signal: Thruster Bank B Working
ropulsion	Thruster Bank B	Thruster Valves B8 Falled Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2	141	Mechanical Failure of Thruster88	Thruster Bank B-Orthogonal. Thruster Valves B8 Falled Open >> Signal: Thruster Bank B Working
	Thruster Bank B	Thruster Valves B8 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2	***	Excessive Heat Soakback from ThrusterB8	Thruster Bank 8-Orthogonal Thruster Valves 86 Falled Open>> Signal: Thruster Bank 8 Working
ropulsion	Thruster Bank B	Thruster Valves 810 Falled Open		Propulsion System Provides Thrust	2		Mechanical Failure of ThrusterB 10	Thruster Bank 6-Orthogonal. Thruster Valves 8:10 Failed Open>> Signal: Thruster Bank 8 Work
ropulsion	Thruster Bank B	Thruster Valves 810 Falled Open		Propulsion System Provides Thrust	12		Excessive Heat Soakback from Thruster810	
ropulsion		Thruster Valves 811 Failed Open		Propulsion System Provides Thrust	2	144	Mechanical Falure of Thruster511	Thruster Bank 8-Orthogonal Thruster Yalves 811 Failed Open>> Signal: Thruster Bank 8 Work
ropulsion	Thruster Bank B	Thruster Valves B11 Failed Open		Propulsion System Provides Thrust	2			Thruster Bank B-Orthogonal, Thruster Valves B11 Failed Open>> Signal: Thruster Bank B Work
opulsion	Thruster Sank B	Thruster Valves B9 Falled Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2		Excessive Heat Soakback from Thruster89	Thruster Bank 8-Orthogonal. Thruster Valves 69 Failed Open>> Signal: Thruster Bank 8 Workin
ropulsion		Thruster Valves 89 Failed Open	No Effect from Thruster Bank B Failure	Propulsion System Provides Thrust	2	111	Mechanical Failure of Thruster89	Thruster Bank B-Orthogonal, Thruster Valves 89 Failed Open>> Signal: Thruster Bank 8 Works
ropulsion		Thruster Valves 812 Falled Open		Propulsion System Provides Thrust	2		Mechanical Failure of ThrusterS12	Thruster Bank B-Orthogonal. Thruster Valves B12 Falled Open>> Signal: Thruster Bank B Work
opulsion	Thruster Bank B		No Effect from Thruster Sank B Failure	Propulsion System Provides Thrust	2	111	Excessive Heat Soakback from ThrusterB12	
	Thruster Bank B	Thruster 62 Falure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B2 Valve Coll Failure	Thruster Bank 8-Orthogonal. Thruster 82 Failure >> Signal: Thruster Bank 8 Not Working && Pro
opulsion	Thruster Sank B	Thruster B3 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B3 Valve Coil Failure	Thruster Bank B-Orthogonal, Thruster 83 Failure >> Signal: Thruster Bank B Not Working && Pro
opulsion	Thruster Bank B	Thruster 84 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B4 Valve Col Failure	Thruster Bank 8-Orthogonal. Thruster 84 Failure>> Signal; Thruster Bank 8 Not Working && Pro
opulsion	Thruster Bank B	Thruster 85 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	5		Thruster BS Valve Coll Failure	Thruster Bank 8-Orthogonal. Thruster 85 Failure>> Signal: Thruster Bank 8 Not Working && Pro
opulsion		Thruster 86 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B6 Valve Col Failure	Thruster Bank B-Orthogonal. Thruster (66 Failure>> Signal: Thruster Bank (8 Not Working && Pro
opulsion	Thruster Sank B	Thruster 87 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2	***	Thruster B7 Valve Col Falure	Thruster Bank 8-Orthogonal Thruster 87 Failure >> Signal: Thruster Bank 8 Not Working && Pr
opulsion		Thruster 88 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2	***	Thruster 88 Valve Coil Falure	Thruster Bank B-Orthogonal. Thruster 88 Failure>> Signal: Thruster Bank B Not Working && Pr
opulsion		Thruster 89 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2	441	Thruster B9 Valve Coll Failure	Thruster Bank 8-Orthogonal. Thruster 89 Failure >> Signal: Thruster Bank 8 Not Working && Po
	Thruster Bank B	Thruster 810 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2	141	Thruster 810 Valve Coll Failure	Thruster Bank 6-Orthogonal Thruster 610 Failure>> Signal: Thruster Bank 6 Not Working && P
opulsion	Thruster Bank B	Thruster 811 Falure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	5		Thruster 811 Valve Coll Failure	Thruster Bank 8-Orthogonal. Thruster 811 Falure>> Signal: Thruster Bank 8 Not Working && P
	Thruster Bank B	Thruster 812 Failure	Thruster Bank B Loss of Thrust	Propulsion System Does Not Provide Thrust	2		Thruster B12 Valve Coll Failure	Thruster Bank 8-Orthogonal. Thruster 812 Failure>> Signal: Thruster Bank 8 Not Working && P
non-Reinan	Oxdzer Tark	External Leak	Loss of Oxedoer	No Oxidizer Flow to Downstream Components			LaunchLoads on Oxdizer Tank	Oxidizer Tank, External Leak>> Signal: Oxidizer Not Available>> Oxidizer Filter, Oxidizer Flow

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		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 effec <mark>tive</mark> mitigation	5	SPF	149

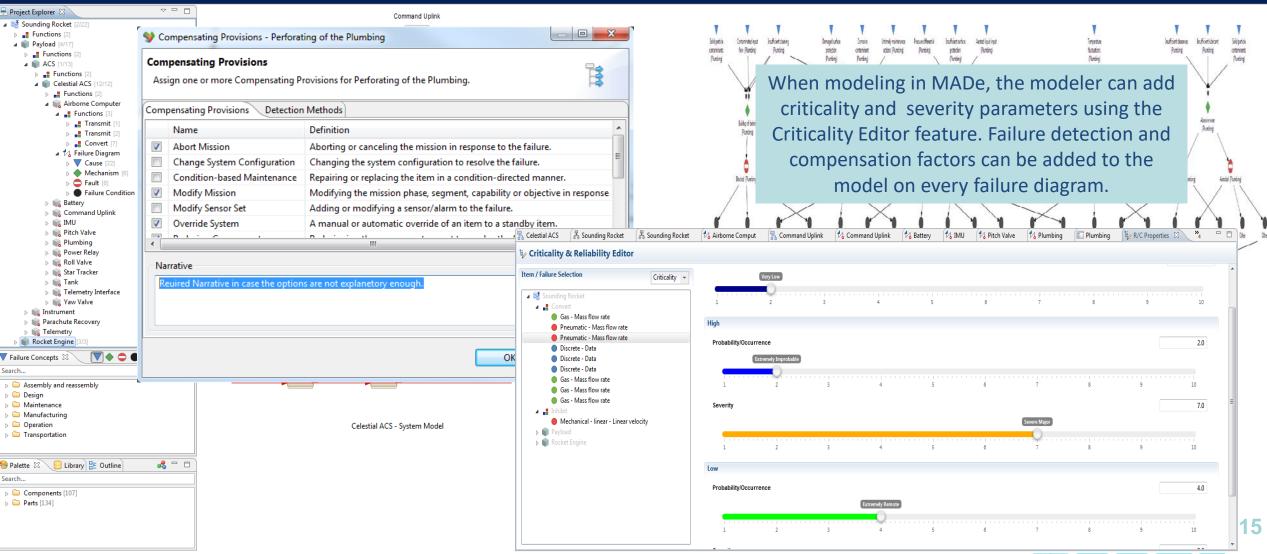


13

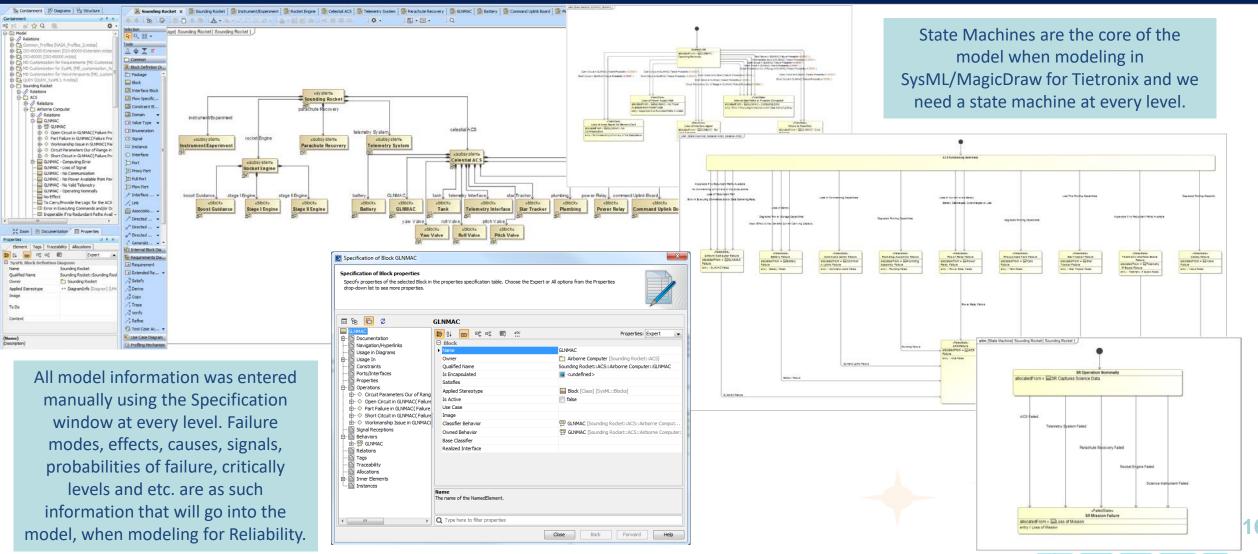
MBSMAI Phase 1: Sounding Rocket Modeling



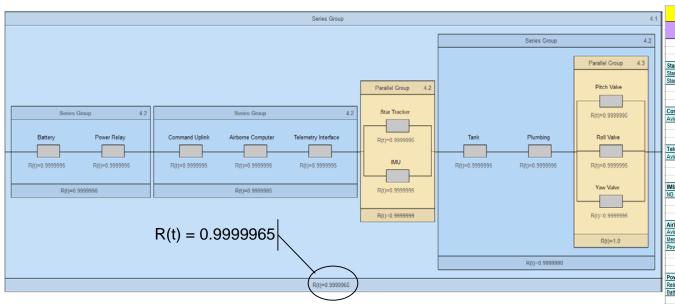
MBSMAI Phase 1: Sounding Rocket Modeling



MBSMAI Phase 1: Sounding Rocket Modeling



MBSMAI Phase 1: Sounding Rocket Probability Analysis Evaluation

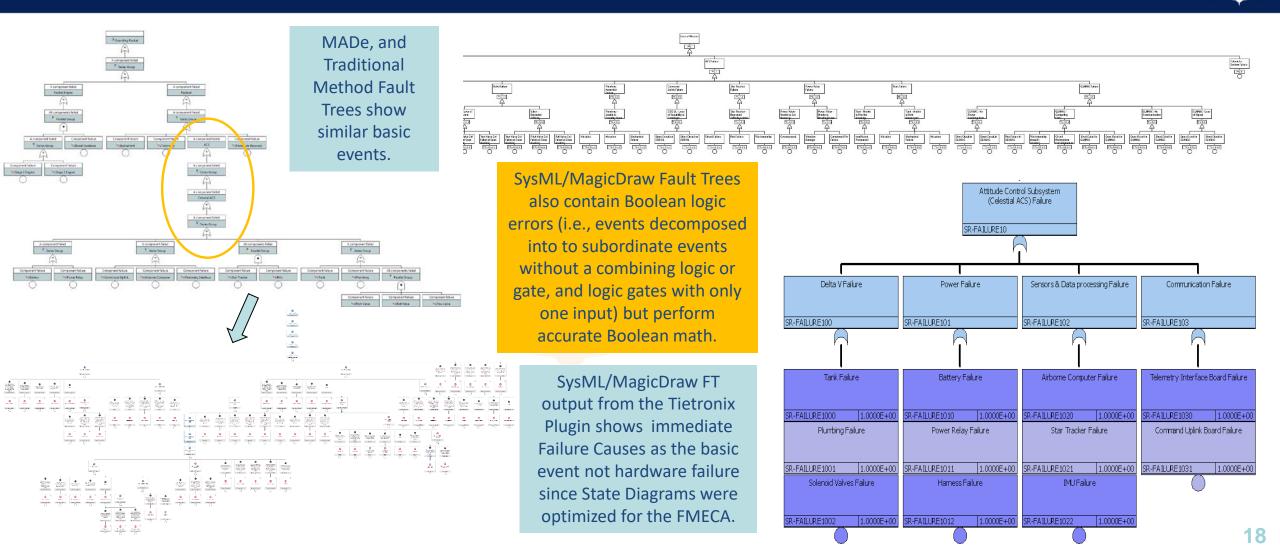


MTTF/ Char Life / Failure Rate / Shape / 1908 Single String Star Tracker Head (Mini Star Tracker) Telemetry Interface NG Scalable SIRU Airborne Compute Avionics Board - High Comp 218986859 4.56648E-0 0.999999873 0.997776719 0.997776719 Single String 0.999999873 0.997776719 5959577.61 1.67797E-07 61103138.1 1.63658E-08 Plumbing R(t) = 0.999998923ACS Total

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



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

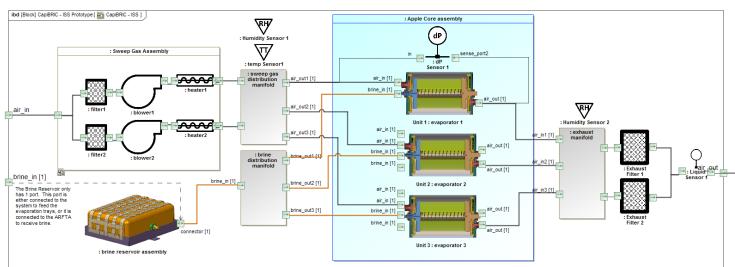
B1 rows	Failure Level:	ALL Criticality Leve	l: ALL End Effect: Al	ı								Base Model 6-8-	2018					FM	ECA (RPN, PHMT)					At	ug 8, 2018 1:07:20 PM
System	Subsyst	Item #6 Item	Potental Falure N	1 Immediate Failure Effi	fect End Effect	Potential Cause(s)	Fault Propagation Path (Explicit)																		, -,
Soundin		Sounding Sounding	SR Mission Failure	Loss of Mission	Loss of Mission 1	ACS Faled							SYSTEM S	ounding Rocket > P	ayload > ACS > Celestial A	ACS > Battery							DATE Aug 8, 2018 1	1:07:20 PM	
Soundin		Sounding Sounding Sounding Sounding	SR Mission Failure SD Mission Failure	Lose of Mission	Loss of Mission 1 Loss of Mission 1	Telemetry System Falled Parachute Recovery Falled						INDEN	TURE LEVEL 5										SHEET 35	OF 1	111
Soundin		Sounding Sounding	SR Mission Failure	Loss of Mission	Loss of Mission 1	Rocket Engine Failed																			
Soundin		Sounding Sounding	SR Mission Failure	Loss of Mission	Loss of Mission 1	Science Instrument Palled						REFERENC	CE DRAWING										COMPILED BY You	ngjo Lim	
Soundin	Celestal	Sounding Celestal	. Arborn Computer		Loss of Mesian 3	Error in Executing Commands and/or D.	Celestal ACS Arborn Computer Failure>> Signal: GL7MAC Failure>> Celestal ACS ACS Failure>> Signal						MISSION TO	est Mission									APPROVED BY		
Soundin	Celestal	Sounding Celestial	Airborn Computer Airborn Computer		Loss of Mission 3	Loss of Redundant Path	Celestial ACS. Arborn Computer Failure>> Signal: GUMMAC Failure>> Celestial ACS. ACS Failure>> Signal: GUMMAC Failure>>						_												
Soundn	Celestial	Sounding Celestial .	Airborn Computer		Loss of Mission 3		. Celestial ACS. Airborn Computer Failure>> Signal: GLNMAC Failure>> Celestial ACS. ACS Failure>> Signal									FAILURE	MODE	CAUSES	OF FAILURE	FAILURE	EEEECTS			CRITIC	CALITY
Soundn	Celestial	Sounding Celestial	Battery Failure	Battery Failure	Loss of Mission 3	Loss of Battery	Celestial ACS Battery Falure>> Signal: Battery Falure>> Celestial ACS.ACS Falure>> Signal: ACS Falure					ITEM N	ю. ПТЕ	EM/PHYSICAL	FUNCTION/ FUNCTIONAL			CHUSES	T TAILUILE	TALEUNE		DETECTION	COMPENSATING		
Soundin	Celestal	Sounding Celestial	Battery Failure Battery Failure	Battery Falure Battery Falure	Loss of Mission 3	Degraded Power Storage Capabilities Major Effect to Max Denated Current	Celestial ACS Battery Failure>> Signal: Battery Failure>> Celestial ACS.ACS Failure>> Signal: ACS Failure>> Celestial ACS.ACS Failure>> Signal: ACS Failure>> Celestial ACS.ACS Failure>> Signal: ACS Failure>>						- D	ESCRIPTION	NARRATIVE	FUNCTIONAL FAILURE	FAULT	MECHANISM	CAUSE	NEXT HIGHER LEVEL	END EFFECTS	METHODS	PROVISIONS	0 S	D RPN
Soundin	Celestral	Sounding Celestial Sounding Celestial	Command Uplink R			Loss of Commanding Capabilities	Celestial ACS.Command Uplink Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: ACS.ACS Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Comand Uplink Failure >> Celestial ACS.ACS Failure >> Signal: Celestial ACS.ACS Failure >> Celestial ACS.ACS Failure >> Signal: Celestial ACS.ACS Failure >> Signal: Celestial ACS.ACS Failure >> Celestial ACS.ACS Failure >																	\rightarrow	$\overline{}$
Soundin	Celestal	Sounding Celestial	Plumbing Assembly			Degraded Pointing Capabilities	Celestial ACS Plumbing Assembly Failure >> Signal: Plumbing Failure >> Celestial ACS.ACS Failure >> Signal						Batte	ery S	Supply Electrical Voltage	Supply Electrical Voltage Low	Short circuit	Dielectric breakdown	Item life-span exceeded	Transmit Discrete Data Low (Celestial	Convert Discrete Data Low (Sounding	Operator Observation, Sensing	Abort Mission, 1 Redesign Component	10.0 8.0	10.0 800
Soundin	Celestial	Sounding Celestial	Power Relay Failur		Loss of Mission 3	Loss of Current to the Battery	Celestial ACS.Power Relay Failure>> Signal: Power Relay Failure>> Celestial ACS.ACS Failure>> Signal:								Modelled as an	1 -			exceeded	ACS) AND Convert	Rocket)	Device			
Soundn	Celectial	Sounding Celestial	Power Relay Failur Pressurized Tank F		Loss of Mission 3		st Celestal ACS Power Relay Failure>> Signal: Power Relay Failure>> Celestal ACS ACS Failure>> Signal:							combination of e	electrical storage device which converts stored	Cannot store power in failed string				Gas Mass flow rate Low (Celestial ACS)		No current	Quality Control and Robust Reliability		
Soundin	Celestal	Sounding Celestal	Star Tracker Falur		Loss of Mission 3	Degraded Pointing Capabilities Lost Fine Pointing Capabilities	Celestial ACS Pressurized Tank Fallure>> Signal: Tank Fallure>> Celestial ACS, ACS Fallure>> Signal: AC Celestial ACS, Star Tracker Fallure>> Signal: Star Tracker Fallure>> Celestial ACS, ACS Fallure>> Signal:							trochemical c	chemical energy into	No connection of				AND Convert Gas		fluctuation detected	Analysis		
Soundin	Celestal	Sounding Celestial	Telemetry Interfac		N Loss of Mission 3	Inoperable if no Redundant Paths Avai.	Celestial ACS. Telemetry Interface Board Failure >> Signal: Telemetry IF Board Failure >> Celestial ACS. Al							used to ent stored	electrical energy.	battery power line Short across battery				Mass flow rate Low (Celestial ACS) AND		at different points			
Soundin	Celestial	Sounding Celestial	Valves Failure	Valve Failure	Loss of Mission 3	Degraded Pointing Capability	Celestial ACS. Valves Falure>> Signal: Valve Falure>> Celestial ACS. ACS Falure>> Signal: ACS Faled>:		e>> Signal: L				chem	nical energy		connections				Transmit Continuous					
Soundin	Celestial	Sounding Celestial	ACS Falure	ACS Falure	Loss of Mission 2	Battery Falure	Celestial ACS-ACS Falure>> Signal: ACS Falled>> Sounding Rocket-SR Mission Falure>> Signal: Loss of		-				into ener	electrical		Failure to cease				Data Low (Celestial					
Soundin	Celestial	Sounding Celestial	ACS Pature ACS Fature	ACS Pature ACS Fature	Loss of Mission 2 Loss of Mission 2	Comand Uplink Failure Mumbing Failure	Celestal ACS.ACS Failure>> Signal: ACS Failed>> Sounding Rocket.SR Mission Failure>> Signal: Loss of Celestal ACS.ACS Failure>> Signal: ACS Failed>> Sounding Rocket.SR Mission Failure>> Signal: Loss of						enen	gy.		operation or Failure				ACS) AND Convert Gas Mass flow rate					
Soundin	Celestial	Sounding Celestial	ACS Falure	ACS Failure	Loss of Mission 2	Power Relay Falure	Celestial ACS, ACS Failure>> Sonal: ACS Failed>> Sounding Rocket, SR Mission Failure>> Sonal: Loss of									to operate or Intermittent				Low (Celestial ACS)					
Soundin	Celestial	Sounding Celestial	. ACS Falure	ACS Palure	Loss of Mission 2	Tank Failure	Celestial ACS.ACS Falure>> Signal: ACS Faled>> Sounding Rocket.SR Mission Falure>> Signal: Loss of	Mission								operation or Loss of								\rightarrow	\rightarrow
Soundn	Celestial	Sounding Celestial	ACS Falure	ACS Falure	Loss of Mission 2	Star Tracker Failure	Celestial ACS.ACS Failure>> Signal: ACS Failed>> Sounding Rocket.SR Mission Failure>> Signal: Loss of		- 11		Failure	Local Subsystem			Cr.	output iticalit SI	1			Transmit Discrete Data Low (Celestial	Convert Gas Mass flow rate Low	Operator Observation, Sensing	Abort Mission, 1 Redesign Component	10.0 9.0	10.0 900
Soundn	Celestial	Sounding Celestial	ACS Falure	ACS Failure	Loss of Mission 2	Telemetry IF Board Failure Valve Failure	Celestial ACS, ACS Failure>> Signal: ACS Failed>> Sounding Rocket SR Mission Failure>> Signal: Loss of Celestial ACS, ACS Failure>> Signal: ACS Failed>> Sounding Rocket, SR Mission Failure>> Signal: Loss of		Function I	ailure Mode	Cause	Effect(s) Effect(s)	End Effect	(s) Detection	Compensation	iticalit Connents F				ACS) AND Convert	(Sounding Rocket)	Device			
Soundin	Celestal	Sounding Celestial	ACS Falure ACS Falure	ACS Failure ACS Failure	Loss of Mission 2	GLIMAC Failure	Celestial ACS.ACS Palure>> Signal: ACS Paled>> Sounding Rocket.SR Mission Falure>> Signal: Loss of Celestial ACS.ACS Falure>> Signal: ACS Faled>> Sounding Rocket.SR Mission Falure>> Signal: Loss of	1.1 Airborne Computer The						n if No data signal	Redundant path		1			Gas Mass flow rate Low (Celestial ACS)		No current	Quality Control and Robust Reliability		
Soundin	Celestial	Sounding Bettery	Power Harness Fa	le Battery - Short Across		Component, Pin Failure in Battery	Battery, Power Harness Failed Short>> Signal: Loss of Battery>> Celestial ACS, Battery Failure>> Signal:	use	ed to provide a full of svigstion colution	lata ci	ircuit	redundant pat	th remaining pati	h						AND Convert Gas		fluctuation detected	Analysis		
Soundin	Celestial	Sounding Battery	Power Harness Fa			Vibration Damage to Battery	Battery, Power Harness Failed Short>> Signal: Loss of Battery>> Celestial ACS. Battery Failure>> Signal:	12 in		orrupted P	art Failure. Cor	eputing Errors in	Loss of primary	v No data signal	Redundant path					Mass flow rate Low		at different points			
Soundin	Celestal	Sounding Battery	Power Harness Fa	The second second		Component,Pin Failure in Battery	Battery.Power Harness Failed Open>> Signal: Loss of Battery>> Celestial ACS-Battery Failure>> Signal:	Velo	ocity, sttitude, and i		ircuit Failure, erre		science, Loss	of						(Celestial ACS) AND Transmit Continuous					
Soundin	Celestal	Sounding Battery Sounding Battery	Power Harness Fa	le Battery - No Connecto Battery - Reduction of		Woration Damage to Battery Woration Damage to Battery	Battery Power Harness Falled Coem >> Signal: Loss of Battery >> Celestial ACS.Sattery Fallure >> Signal: Battery : We Breakage >> Signal: Major Effect to Max Denated Current Carrying Capacity >> Celestial ACS		dy rates to control p		r Workmanship.	commands and/or data	mission.							Data Low (Celestial					
Saundin	Celestial	Sounding Battery	Loss of One String			Joint Falure (Nidde Tab., Spot Weld., 5	Battery Loss of One String >> Signal: Degraded Power Storage Capabilities >> Celestial ACS Battery Fall.		ems for spinning and p n-spinning rockets.	rogram		anthering and								ACS) AND Convert Gas Mass flow rate					
Soundn	Celestial	Sounding Bettery	Loss of One String	Battery - Cannot Store		Cell Short/Open Crout in Battery	Battery Loss of One String>> Signal: Degraded Power Storage Capabilities>> Celestial ACS.Battery Fall.	in				relay								Low (Celestial ACS)					
Soundn	Celestial	Sounding Power Re		Power Relay - Unable t		Overstressed	Power Relay, Failed Short>> Signal: Battery Discharged, Overcharged or Lost>> Celestial ACS Power Re				ircuit Failure - No Ipen/Shor/Out teld		No effect	Faulty	Software Guality									$-\!\!+\!\!-\!\!\!+$	-
Soundin	Celestial	Sounding Power Re Sounding Power Re		Power Relay - Unable t Power Relay - Unable t		Woration Damage Component/frin Failure	Power Relay, Failed Open>> Signal: Loss of Current to the Battery>> Celestial ACS Power Relay Failure: Power Relay, Failed Open>> Signal: Loss of Current to the Battery>> Celestial ACS Power Relay Failure:				FRance	metry		leiemetry	Control					Transmit Discrete Data Low (Celestial	Convert Gas Mass flow rate Low	Operator	Abort Mission, 1 Redesign Component	10.0 9.0	10.0 900
Soundin	Celestial	Sounding Command	Loss of Signal	CMD UL - Loss of Capa		Open Crouit on CMD UL	Command Uplink Board, Loss of Signal >> Signal Loss of Commanding Capabilities >> Celestial ACS, Commit				ircuit Failure - No		o Loss of mission	n # No telemetry	Redundant path					ACS) AND Convert	(Sounding Rocket)	Device	1 - 1		
Soundin	Celestal	Sounding Command	Loss of Signal	CMD UL + Loss of Capa		Short Circuit on CMD UL	Command Uplink Board Loss of Signal >> Signal: Loss of Commanding Capabilities >> Celestial ACS. Commo		•	upply path O	lpen/Short ava	ilable from redundant	remaining pati	h						Gas Mass flow rate Low (Celestial ACS)		No current	Quality Control and Robust Reliability		
Soundn	Celestal	Sounding Star Trad		Star Tracker - Degrade		Circuit Falure	Star Tracker Inoperable >> Signal: Lost Fine Pointing Capabilities>> Celestial ACS. Star Tracker Failure >>	1.5	ı	oss of input Ci	ircuit Failure - No	No commandir	ng Loss of mission	n if No telemetry	Redundant path					AND Convert Gas		fluctuation detected	Analysis		
Soundn	Celestial	Sounding Star Trad		Star Tracker - Degrade		Part Falure	Star Tracker Inoperable >> Signal: Lost Pine Pointing Capublities >> Celestal ACS. Star Tracker Failure >> Star Tracker Inoperable >> Signal: Lost Pine Pointing Capublities >> Celestal ACS. Star Tracker Failure >>	*1			lpen/Short cor	munication tofrom any of t								Mass flow rate Low		at different points			
Soundin	Celestial	Sounding Star Trad Sounding Yaw Valve	r Inoperable Falled Close	Star Tracker - Degrade Valve - Degraded Attiti		Workmanship Yany Value Coil Failed at Close Boston	Yaw Valve, Failed Close >> Signal: Degraded Pointing Capability >> Celestial ACS, Valves Failure >> Signal:	5	,	emory card		oubayatema	fails.	subsystems						(Celestial ACS) AND Transmit Continuous					
Soundin	Celestial	Sounding Yan Valv	Falled Open	Valve - Loss of Pressur	rant Loss of Mission 4	Yaw Valve Coll Falled at Open Position	Yaw Valve Failed Open>> Signal: Degraded Pointing Capability>> Celestial ACS Valves Failure>> Signal:	2.1 Battery An el	lectrical battery is a L	oss of one SI	hort/open Car	not store Degraded pos	ver Loss of Mission	n Current reading	Redundant strings 5		1			Data Low (Celestial					
Soundin	Celestial	Sounding Pitch Valv		Valve - Degraded Attit		Pitch Valve Coil Failed at Close Position	Pitch Valve Falled Close>> Signal: Degraded Pointing Capability>> Celestial ACS, Valves Fallure>> Signal	ti com	mbination of one or b	attery string ci		rer in failed storage		drop at different						ACS) AND Convert Gas Mass flow rate					
Soundn	Celestal	Sounding Pitch Valv	Faled Open	Valve - Loss of Pressur		Pitch Valve Coll Failed at Open Position	Pitch Valve Failed Open>> Signal: Degraded Pointing Capability>> Celestial ACS. Valves Failure>> Signal		re electrochemical Ils used to convert		attery cell, stri ickel tab, spot	ng capabilites Lo of a battery	010	points						Low (Celestial ACS)					
Soundin	Celestial	Sounding Roll Yalve Sounding Roll Yalve	Faled Close Faled Open	Valve - Degraded Attit Valve - Loss of Pressur			Roll Valve Failed Close>> Signal: Degraded Pointing Capability>> Celestial ACS. Valves Failure>> Signal: Roll Valve, Failed Open>> Signal: Degraded Pointing Capability>> Celestial ACS. Valves Failure>> Signal:		ed chemical energy		eld, or solder	or a pattery string.												\rightarrow	-
Soundin	Celestal	Sounding Plumbing	Practured Practured	Plumbing - Unable to Tr		Mechanical Failure	Plumbing, Fractured >> Signal: Degraded Pointing Capabilities >> Celestial ACS, Plumbing Assembly Palure.		electrical energy.	io	int failure									Transmit Discrete Data Low (Celestial	Convert Gas Mass flow rate Low	Operator Observation Sensing	Abort Mission, 1 Redesign Component	10.0 9.0	10.0 900
Soundn	Celestial	Sounding Plumbing	Cracked	Plumbing - Unable to Ti	Fr Loss of Mission 4	Vibration	Plumbing Cracked>> Signal: Degraded Pointing Capabilities>> Celestial ACS Plumbing Assembly Failure>		Į.			luction of Major effect to derated may derated	Loss of Mission		Redundant lines to 5					ACS) AND Convert	(Sounding Rocket)	Device			
Soundn	Celestial	Sounding Plumbing	Corroded	Plumbing - Unable to Tr		Abrasion	Plumbing, Corroded >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Plumbing Assembly Failure:	>:	,			rent carrying current carryin	ng	points	requirements.					Gas Mass flow rate Low (Celestial ACS)		No current	Quality Control and Robust Reliability		
Soundin	Celestal	Sounding Tank	Fractured Cracked	Tank - Unable to Hold I Tank - Unable to Hold I		Mechanical Failure Woration	Tark Practured >> Signal: Degraded Pointing Capabilities >> Celestial ACS Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark Failure >> Signal: Degraded Pointing Capabilities >> Celestial ACS. Pressurated Tark	9			cop	acity capacity	-							AND Convert Gas		fluctuation detected	Analysis		
Soundin	Celestal	Sounding Tank Sounding Tank	Corroded	Tank - Unable to Hold 9		Abrasion	Tank, Corroded > > Signal: Degraded Pointing Capabilities > > Celestial ACS Pressurged Tank Falure > > Sig	2.3		lower harness Co sils open fa		connection Loss of battery attern power	y Loss of Mission		Redundant lines to 5 maintain densting					Mass flow rate Low		at different points			
Sound	I brown		T ## P	an Frank Charles as Para A		Para different Parameter	Tool for Marine Process Country Countr	ni)	ľ		ibration line	acces posice		different points						(Celestial ACS) AND Transmit Continuous					
Sound							edundant Path>>	-1		di	anage									Data Low (Celestial					
Sound	C	- N / I / N	10000	Drown	Carroni	+,, and 1;	kalihaad valuas edundert Reth>>	2.4			omponent/pin Shi				Guality control and 5 robust reliability					ACS) AND Convert Gas Mass flow rate					
Sound Sound Sound	DV:	SIVIL/I	งเสยเต	DIAW	Seven	tv and ti	kelihood values	ic	ľ			nections Battery.	*		analysis					Low (Celestial ACS)					
2,000	- 7 '					-, -::				dı	amage			different points				_							
								3.1 Command Uplink Recid	ieves Uplink L mandsfor Inhihit		pen or short Los	s of No commandir manding to of computer	ng Missionfailure	 Verification of commanding 			1	B.I.			Later tal		ara iic	I I	
	_						arralata ta tha	Conn		00	y or original COI		www	community			1	1/1	つととつもに	1/0 20	MITIO	DC MI		OO T	

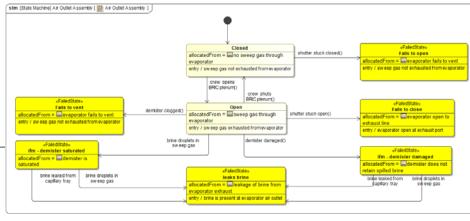
SysML/MagicDraw Severity and Likelihood values are entered manually and can correlate to the GSFC Risk definitions. To have a complete FMECA all thinking and data entry for to calculate RPN would be done at manually at the modeling stage and the plugin will extract the data and tabulate it for the user.

| Vibration damage | Vibration d

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



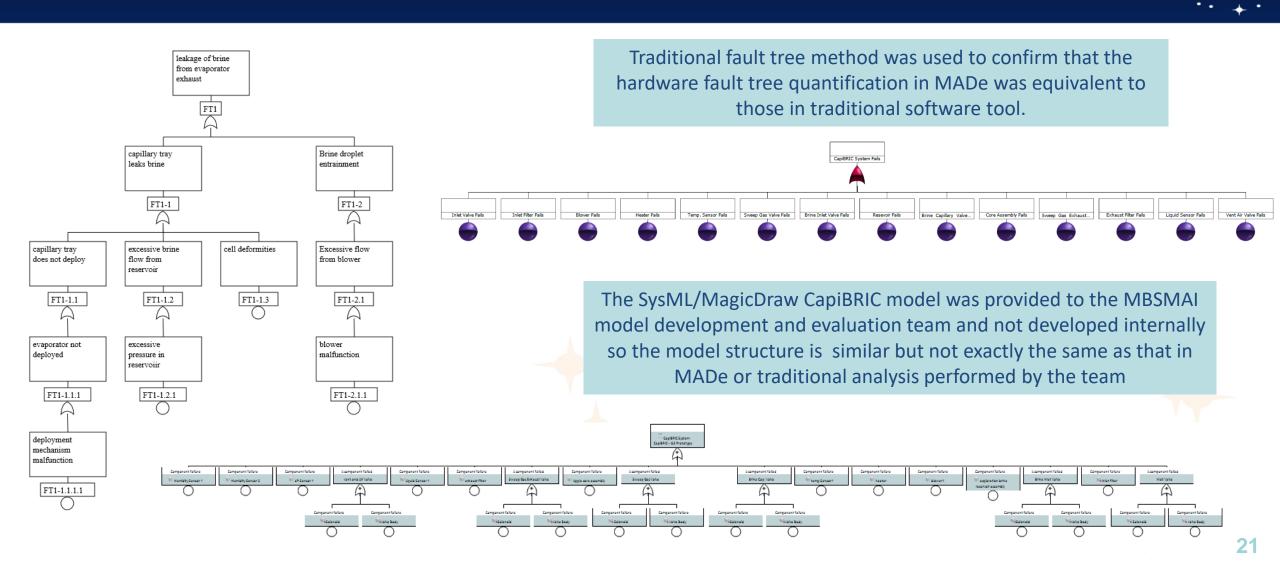


The CapiBRIC
SysML model in
SysML/MagicDraw
provided by JSC
consisted of a
Block Definition
Diagram, a wiring
Diagram and 13
state machines

Inlet Valve inlet filter blow err temp Sensor1 Humidity Sensor 2 Liquid Sensor 1 Humidity Sensor 2 Liquid Se

Contaminated input Insufficient cleaning contaminants (inlet In MADe a Yielding (inlet filter) limited model Buildup of debris was developed that consisted of Interference (inlet 1 main functional block diagram and 1 Refine Gas Mass flow rate (inlet filter) failure diagram.

MBSMAI Phase 1: CapiBRIC Model Fault Tree Evaluation



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

Item Herarchy	Item		Potental Falure Mode	Immediate Failure Effect	End Effect		CRIT LEVEL	Potential 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	12 1	4	capitary flow pap	brine reservoir. No flow from reservoir >> Signal: brine from reservoir not pro-
CapBRSC - Baseline > > exploration brine reserv		н	No flow from reservoir	insufficient flow from reservoir	insufficient flow through feed so valve	2		capillary flow gap	brine reservoir. No flow from reservoir >> Signal: brine from reservoir not pro-
CapBRIC Context>>CapBRIC - ISS Prototype		н	Excessive flow from reservoir	excessive brine flow from reservoir	evaporator does not receive brine		0.14	excessive pressure in reservoir	brine reservoir. Excessive flow from reservoir >> Signal: excessive brine flow
CapBRSC Context>>CapBRSC - ISS Prototype	brine reservoir	$^{+}$	Excessive flow from reservoir	excessive brine flow from reservoir	Personnel intury due contact with brine	5	2	excessive pressure in reservoir	brine reservor. Excessive flow from reservor >> Signal: excessive brine flow
CapBRIC - Baseline >> exploration brine reserv		н	Excessive flow from reservoir	excessive brine flow from reservoir	evaporator does not receive brine		5.4	excessive pressure in reservoir	brine reservoir. Excessive flow from reservoir >> Signal: excessive brine flow.
CapiBRIC - Baseline > > exploration brine reserv	brine reservoir	т	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
CapiBRIC Context>>CapiBRIC - ISS Prototype		н	leaks brine	reservor leaks brine	reservor leaks brine		1	reservor damaged	
CapiBRUC Context > > CapiBRUC - 155 Prototype		н	leaks brine	reservor leaks brine	reservor leaks brine	1		reservor seal malfunction	
CapiBRUC - Baseline > > exploration brine reserv		$^{+}$	leaks brine	reservor leaks brine	reservor leaks brine	1		reservoir danaged	
CapiBRIC - Baseline > > exploration brine reserv		$^{+}$	leaks brine	reservor leaks brine	reservor leaks brine	1		reservoir seal malfunction	
CapiBRIC Context >> CapBRIC + ISS Prototype	feed ine solati		Faled Open	evaporator not isolated	evaporator not isolated	1	4	valve malfunction	
CapifRIC - Baseline >> exploration brine reserv		Tä)	Faled Open	evaporator not isolated	evaporator not isolated	î	4	valve malfunction	
CapilRIC Context>>CapilRIC - ISS Prototype	feed line isolati		Faled Closed	evaporator isolated from reservoir	evaporator isolated from reservoir	1	4	valve malfunction	
CapilRIC - Baselne > >exploration brine reserv		til	Faled Closed	evaporator isolated from reservoir	evaporator isolated from reservoir	1	4	valve malfunction	
CapilRIC Context>>CapilRIC - ISS Prototype	feed line isolati	Lil.	Low flow	insufficient flow through feed iso v	insufficient flow through feed iso valve	1	4	contamination	
CapilRIC Context>>CapilRIC - ISS Prototype		E	Low flow		insufficient flow through feed iso valve	1	4	brine from reservoir not provided	
CapifRIC - Baseline > >exploration brine reserv		f#	Low flow		insufficient flow through feed iso valve	1	4	contamination	
CapiBRIC - Baseline > >exploration brine reserv		C	Low flow		insufficient flow through feed so valve	î	14	brine from reservoir not provided	
CapiBRIC - RuBRICs Cube > >blower	blower	f"	Faled off	No flow from blower	No flow from blower	1	4	blower malfunction	
CapiBRIC - Iffi Apple Core >>blower	blower	+	Faled off	No flow from blower	No flow from blower	î	4	blower malfunction	
CapiBRIC - RuBRICs Cube > >blower	blower	+	Falled high	Excessive flow from blower	demister is seturated	3	4	blower malfunction	blower Failed high>> Signal: excessive flow from blower>> Capillary Tray Br
CapERIC + 1fil Apple Core >>blower	blower	+	Faled high	Excessive flow from blower	demister is seturated	3	4	blower mathunction	blower Failed high>> Signal: excessive flow from blower>> Capillary Tray.Br
CapiBRIC - RuBRICs Cube >>blower	blower	++	Falled low	Insufficient flow from blower	capillary tray contains brine		4	blower malfunction	blower.Failed low>> Signal: insufficient flow from blower>> heater./lio or Lo
Capific - Ruffics Cube > >blower	blower	++	Falled low	Insufficient flow from blower	Water is not recovered		3	blower malfunction	blower.Failed low>> Signal: insufficient flow from blower>> heater./lio or Lo
CapiBRIC - RuBRICs Cube > >blower	blower	++	Falled low	Insufficient flow from blower	capillary tray contains brine		4	insufficient flow to blower	blower Failed low>> Signal; insufficient flow from blower>> heater //io or Lo
CanBRIC - RuBRICs Cube > >blower	blower	++	Failed low	Insufficient flow from blower	Water is not recovered	5		insufficient flow to blower	blower Failed low > > Signal: Insufficient flow from blower > > heater No or Lo
CapiBRIC - Iffl Apple Core > >blower	blower	+	Falled low	Insufficient flow from blower	capillary tray contains brine	3		blower malfunction	blower Failed low >> Signal: insufficient flow from blower >> heater No or Lo
CapBRIC - 16I Apple Core > Hower	blower	++	Failed low	Insufficient flow from blower	Water is not recovered	5		blower malfunction	blower Falled low >> Signal: insufficient flow from blower >> heater No or Lo
CapiBRIC - Iffi Apple Core >>blower		₩	Faled low	Insufficient flow from blower	capillary tray contains brine	3		Insufficient flow to blower	blower.Falled low>> Signal: insufficient flow from blower>> heater.No or Lo.
CapiBRIC - 1fil Apple Core > Hower CapiBRIC - 1fil Apple Core > Hower	blower	-	Faled low	Insufficient flow from blower	Water is not recovered		3	Insufficient flow to blower	blower.Falled low>> Signal: insufficient flow from blower>> heater.No or Lo. blower.Falled low>> Signal: insufficient flow from blower>> heater.No or Lo.
CapBRIC - 1fil Apple Core > >blower CapBRIC - Baseline > >nlet filter		+							blower.halled low>> Signal: insufficient flow from blower>> heater.flo or Lo.
Capititic - Baseine > > riset riter Capititic - RuBRICs Cube > > rislet filter	inlet filter	100	Falls to prevent contamination	contamination in feed line	contamination in feed line	1	4	filter damaged	
	inlet filter	100	Fails to prevent contamination	contamination in feed line	contamination in feed line	1		filter damaged	
CopERIC - Ifil Apple Core>>inlet filter CopERIC - Baseline>>inlet filter	inlet filter	-00	Fals to prevent contamination	contamination in feed line filter allows insufficient flow	contamination in feed line capillary tray contains brine		4	fiter damaged	injet filter Low flow>> Signal: insufficient flow to blower>> blower Failed low
CapBRIC - Baseine > > niet filter CapBRIC - Baseine > > niet filter	inset filter		Low flow	filter allows insufficient flow			4	filter clogged	
		100			Water is not recovered		3	fiter dogged	rriet filter Low flow >> Signal: insufficient flow to blower >> blower Falled low
CapiBRIC - RuBRICs Cube > smlet filter CapiBRIC - RuBRICs Cube > smlet filter	inlet filter inlet filter		Low flow	fiter allows insufficient flow fiter allows insufficient flow	capillary tray contains brine			filter clogged	rriet filter.com flow>> Signal: insufficient flow to blower>> blower.Failed low
		-			Water is not recovered	6	3	filter clogged	niet filter Low flow>> Signal: insufficient flow to blower>> blower Faled low
CapiBRIC - Iffl Apple Core>>inlet filter	inlet filter	-	Low flow	fiter allows insufficient flow	capillary tray contains brine	-100	4	filter clogged	riet filter.Low flow>> Signal: insufficient flow to blower>> blower.Failed low
CapiERIC - 1fil Apple Core>>inlet filter	inlet filter	10	Low flow	fiber allows insufficient flow	Water is not recovered	6	3	filter dogged	niet filter Low flow>> Signal: insufficient flow to blower>> blower Failed low
CapiBRIC - Baseline > > heater	heater	ш	Temperature High	Overtemp causes damage to Capil		1		heater not controlled	
CapilRIC - RullRICs Cube >>heater	heater	ш	Temperature High	Overtemp causes damage to Capil		1		heater not controlled	
CapiBRIC - Iffi Apple Core>>heater	heater	ш	Temperature High	Overtemp causes damage to Capil		1		heater not controlled	
CapiBRIC - Baseline > > heater	heater	ш	Temperature Low	Insufficient heat	Insufficient heat	1	4	heater malfunction	
CapiBRIC - Baseline > > heater	heater	ш	Temperature Low	Insufficient heat	Insufficient heat	1	4	no power to heater	
CapiBRIC - RuBRICs Cube > >heater	heater	ш	Temperature Low	Insufficient heat	Insufficient heat	1	4	heater malfunction	
CapiBRIC - RuBRICs Cube >>heater	heater	ш	Temperature Low	Insufficient heat	Insufficient heat	1	4	no power to heater	
CapiERSC - Iffl Apple Core>>heater	heater	ш	Temperature Low	Insufficient heat	Insufficient heat	1	4	heater malfunction	
CapiERIC + Iffi Apple Core >>heater	heater	ш	Temperature Low	Insufficient heat	Insufficient heat	1	4	no power to heater	
CapiERSC - Baseline > > heater	heater	ш	No or Low Flow	No flow through heater	capillary tray contains brine		4	insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>>
CapiERDC - Baseline > >heater	heater	П	No or Law Flaw	No flow through heater	Water is not recovered		3	insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>>
CapBRIC - RuBRICs Cube > >heater	heater	П	No or Law 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 Law Flaw	No flow through heater	Water is not recovered	4		insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>>
CapBR3C - 1fili Apple Core > >heater	heater	П	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>>
CapiBRSC - 1fili Apple Core >> heater	heater		No or Law Flaw	No flow through heater	Water is not recovered		3	insufficient flow from blower	heater.No or Low Flow>> Signal: sweep gas not provided to evaporator>>
CapBRIC - Baseline > > heater	heater	П	Temperature Exceeds Flamma	Personnel injury or vehicle damage	Personnel injury or vehicle damage to du	- 1	1	heater power direuit not out	
CapBRIC - RuBRICs Cube >>heater	heater	П	Temperature Exceeds Flamma	Personnel injury or vehicle damage	Personnel injury or vehicle damage to du	. 1	1	heater power drouit not out	
CopeRUC - Iffi Apple Core > >heater	heater	П			Personnel injury or vehicle damage to du			heater power grout not out	
CapiBRIC - Baseline >> Controls Assembly	Controls Assembly		Fals Off			1		power crout malfunction	
CasiBRIC - RuBRICs Cube > > Controls Assembly	Controls Assembly		Fals Off			\Box		power crout malfunction	
CapiBRIC - Iffi Apple Core > > Controls Assembly	Controls Assembly		Fals Off			+		power circuit malfunction	
CapiBRIC - Baseline > > Controls Assembly	Controls Assembly		Fals to solate feed line			-		feed line outoff crout maifunction	

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 C	OF FAILURE	FAILURE	EFFECTS	DETECTION	COMPENSATING		CRIT	ICALITY	
DESCRIPTION	FUNCTIONAL NARRATIVE	FUNCTIONAL FAILURE	FAULT	MECHANISM	CAUSE	NEXT HIGHER LEVEL	END EFFECTS	METHODS	PROVISIONS	0	5	D	RPN
inlet filter	Refine Gas Mass flow rate	Refine Gas Mass flow rate High	Tom	Yielding	Excessive material defects	Convert air_out Temperature High (CapiBRIC System: CapiBRIC - ISS Prototype) AMD 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) AMD 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 System: CapiBRIC System:	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 - 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.

R

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.

26

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.





