					Effect	ct				Detec	aon	
FMEA ID	Name	Function Fai	ailure Mode / Possible ait / Constraint Causes	Local	Next Higher Mis	ission Umbra Violation	Severity Type o	f Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Detection Diagnosis (Local	(System)

	<u> </u>
Column Heading	Definition
FMEA ID	Unique ID for each failure mode
Name	HW or SW element name
Function	What function does the failed element perform?
Failure Mode/Limit/Constraint	Specific failure mode, i.e., sensor failure, SW error, electronic part failure
Possible Causes	Credible causes for failure, i.e., radiation upset on FPGA
Phase	See Table I in legend
Effects	What are the effects of the failures at various levels? List N/A if effect level does not apply
Local	Effect on the failed element
Next Higher	Effect of failed element on subsystem/instrument
Mission	Effect of failed element on mission
Umbra Violation	Is there an effect that can lead to umbra violation?
Severity	See Table II in legend
Type of FM	Active, Passive, None
Detection	
Observable	Yes/No
How Observed?	How is the fault observed (narrative) / Who observes the fault (HW, FSW, Autonomy, Ground)?
Tlm for diagnosis	Telemetry needed for diagnosis of fault
Tlm path for diagnosis	Where does the telemetry come from, who it is sent to/through
Time to Detect (Local)	Time detect locally (is this persistence)
Time to Detect (System)	Time to detect at system level (is this persistance?)
Response	
Response Level	Local, System, Instrument, or, None*
Desired local response	Narrative description of desired action taken locally at subsystem/instrument level
Allocation of local response	Who responds locally? HW, FSW, Autonomy, Ground
Time to Transmit Signal	How long does it take before local response begins?
Time to Fix Locally	Time to fix for local response
Desired SC response	Narrative description of desired action taken at system level
Allocation of SC response	Who responds locally? HW, FSW, Autonomy, Ground
Time to Transmit Signal	How long does it take before system response begins?
Time to Fix System	Time to fix for system response
Ground Response/Contingency	Ground response needed (narrative); ideas for steps in contingency plans
Quick Look Response	
System Side Switch	Binary indication that system side switch occurs
Processor Switch	Binary indication that processor switch occurs
Safe Mode	Binary indication that SC enters Safe Mode as response to fault

Notes:

Indicates column instrument teams need to fill in

* for instrument teams please list "instrument" if there is fault management internal to your instrument that will respond to fault condition, list "system" if you want the spacecraft to respond using one of the pre-determined rules

								Respon	se						Quick Look	
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Desired SC response	Allocation of System Response	Time to ix system	Time to Transmit Signal	Ground Response/ Contingency	System Side Switch	Processor Switch	Safe Mode

	i
Column Heading	Definition
FMEA ID	Unique ID for each failure mode
Name	HW or SW element name
Function	What function does the failed element perform?
Failure Mode/Limit/Constraint	Specific failure mode, i.e., sensor failure, SW error, electronic part failure
Possible Causes	Credible causes for failure, i.e., radiation upset on FPGA
Phase	See Table I in legend
Effects	What are the effects of the failures at various levels? List N/A if effect level does not apply
Local	Effect on the failed element
Next Higher	Effect of failed element on subsystem/instrument
Mission	Effect of failed element on mission
Umbra Violation	Is there an effect that can lead to umbra violation?
Severity	See Table II in legend
Type of FM	Active, Passive, None
Detection	
Observable	Yes/No
How Observed?	How is the fault observed (narrative) / Who observes the fault (HW, FSW, Autonomy, Ground)?
Tlm for diagnosis	Telemetry needed for diagnosis of fault
Tlm path for diagnosis	Where does the telemetry come from, who it is sent to/through
Time to Detect (Local)	Time detect locally (is this persistence)
Time to Detect (System)	Time to detect at system level (is this persistance?)
Response	
Response Level	Local, System, Instrument, or, None*
Desired local response	Narrative description of desired action taken locally at subsystem/instrument level
Allocation of local response	Who responds locally? HW, FSW, Autonomy, Ground
Time to Transmit Signal	How long does it take before local response begins?
Time to Fix Locally	Time to fix for local response
Desired SC response	Narrative description of desired action taken at system level
Allocation of SC response	Who responds locally? HW, FSW, Autonomy, Ground
Time to Transmit Signal	How long does it take before system response begins?
Time to Fix System	Time to fix for system response
Ground Response/Contingency	Ground response needed (narrative); ideas for steps in contingency plans
Quick Look Response	
System Side Switch	Binary indication that system side switch occurs
Processor Switch	Binary indication that processor switch occurs
Safe Mode	Binary indication that SC enters Safe Mode as response to fault

Notes:

Indicates column instrument teams need to fill in

* for instrument teams please list "instrument" if there is fault management internal to your instrument that will respond to fault condition, list "system" if you want the spacecraft to respond using one of the pre-determined rules

Operational Phase

- Launch Commision
- Encounter
- Cruise

Severity		
1		Failure modes that could result in serious injury, loss of life, or loss of spacecraft .
1R	Catastrophic	Failure modes of identical or equivalent redundant hardware or software elements that could result in Category 1 effects if all failed.
15		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.
2		Failure modes that could result in loss of three or more mission objectives
2R	Critical	Failure modes of identical or equivalent redundant hardware or software that could result in Category 2 effects if all failed.
2S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 2 consequences.
3	Significant	Failure modes that could cause loss to any mission objectives.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives

Subject Matter Expert(s):

Sam Sawada (PDU)

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FMEA information is only displayed in the first copy of the component.

	Sam Sawada (PDU)	in the first copy of the componen	t.			.	F#F-st			Ī		:		Datastian	0.0-4hd		
FMEA ID	Name	Function	Function Failure Mode / Limit Possible Causes Phase Local Next Higher Mission Umbra Violation Severity Type of FM Observable How Observable Observable How O		How Observed?	Detection Tlm for Diagnosis	Tlm Path for	Time to Detect	Time to Detect								
										Severity	,,,,,,				Diagnosis	(Local)	(System)
****	D. d d d. D M d. l.																
AV-1	Redundant Proc Module Avionics Redundancy															å	
AV-1.1	Controller																
AV-1.1.1	Processor A (Prime)																
									If switchover								
				1) failed power supply	į				doesn't happen within required				Hot spare would				
				2) software hangs		No way to recongnize failure,	Hot spare or ARC would recognize	Loss of redundancy for	amount of time,				see it via software,				
AV-1.1.1.a			No output	3) hardware failure (chips,	all	so it'd just keep going	issue and ARC demotes Prime,	causes 1 & 3	but system is	2R	Active	yes	ARC acknowledge				
				connectors, FPGA, etc.)	į		making Hot Spare Prime		designed to				timer on Prime would trigger				
									handle this				would trigger				
					ļ	i 			situation If switchover								
									doesn't happen				I				
				1) LVDS driver is flaky 2) SW issues		Might get feedback from	Hot spare would recognize issue		within required				Hot spare would see it via software,				
AV-1.1.1.b			Incorrect	3) Communications path		SpaceWire (either no data	(error detection on data transfer)	Loss of redundancy	amount of time,	2R	Active	yes	ARC watchdog				
			output/timing	connector/harness issue		return or bad data return).	and ARC demotes Prime, making Hot Spare Prime		but system is			ĺ	timer on Prime				
				(intermittent connection)	•	May self-demote	not spare Prime		designed to handle this				would trigger				
									situation								
									If switchover								
									doesn't happen								
			Loss of SPW		•	Donands on SW configuration	Autonomy would command a side		within required				Hot spare or Prime				
AV-1.1.1.c	(Input?)		Timecode	LVDS receiver fails		Prime would stay as Prime.	switch.	Loss of redundancy	amount of time, but system is	2R	Active	yes	would see it				
			Timecode			Time would stay as Time.			designed to				Would See It				
									handle this								
					ļ				situation								
				1) PWB crack	į				If switchover								
				PWB crack Connector disconnects	ļ		Hot spare would recognize issue		doesn't happen within required				Hot spare would				
				Converter card fails			and ARC demotes Prime, making		amount of time,				see it via software,				
AV-1.1.1.d			Hard failure	4) Component failing short (could		Processor dies	Hot Spare Prime. New Prime would eventually turn processor	Loss of redundancy	but system is	2R	Active	yes	ARC watchdog timer on Prime				
				look like an overcurrent, which			off.		designed to				would trigger				
				could cause an overtemp issue)					handle this								
AV-1.1.1.1	Watchdog Timer				ļ				situation								
	watendog inner			·					If switchover		Ě					<u> </u>	
									doesn't happen								
							Hot spare would recognize issue or	Loss of redundancy if	within required								
AV-1.1.1.a			Failure to timeout	1) FPGA or LEON fails	į	Lose software with no way	ARC watchdog timer would time	FSW branches to WDT	amount of time,	2S/R	Active	yes	Hot spare would				
			(when it should)			locally to recover	out and ARC would demote Prime, making Hot Spare Prime	again.	but system is designed to				see it or ARC WDT				
					į		making froe Spare Frime		handle this								
									situation								
									If switchover								
									doesn't happen within required	30 :fhala aasaasaa :							
			Timeout when it				Hot spare would recognize issue or ARC watchdog timer would time	1	amount of time,	2R if whole processor is lost			Hot spare would				
AV-1.1.1.1.b			shouldn't	1) FPGA fails		Reboot	out and ARC would demote Prime,	Loss of redundancy	but system is	3 if processor can keep	Active	yes	see it or ARC WDT				
							making Hot Spare Prime		designed to	working with no WDT							
									handle this								
				1	ļ	<u> </u>	Switch avionics sides, detected at		situation				-	ļ		ļ	
			SpW Router A (only			S/C internal communications	SpW link level by autonomy rule;										
Inputs			one router active at a given time)			fail, SpW timecode fails	Prime tells ARC to switch from	Loss of redundancy		2R			Autonomy rule				
							REM A to REM B									ļ	
		ļ	SpW Router B		<u></u>	<u>i</u>			-		ļ			ļ		ļ	
				(ongoing SSR trade to potentially				Loss of SSR redundancy,									
			SSR 1 (Prime only)	change to one SSR local to each		Couldn't access recorder	Lose playback ability	could switch to SSR 2	N/A		Active						
				processor, but connected to the other two SSRs)				without needing to switch REM									
		ļ		50.0. two 55.15 ₁	ļ			Santon Neivi			ļ						
			SSR 2 (Prime only)		 		<u>. </u>	_					<u>.</u>	ļ		ļ	
							No effect on spacecraft (loss of										
			ARC Mode Controller			Notes that Mode Controller 1 isn't providing data	redundancy), assuming that design can catch all of the possible failure			2R	Passive						
			1			ion r browning agra	modes										
			ADCIA L.C.														
			ARC Mode Controller														
			ARC Mode Controller														
			3						I		<u> </u>		1	<u> </u>		<u> </u>	
AV-1.1.2	Processor B (Hot)																
							ARC would recognize issue and		[1				
				1) failed power supply	1		demote Hot Spare, and promote										
AV-1.1.2.a			No output	2) software hangs	all		the Warm Spare or wrong data	Loss of redundancy for	None.	2R	Active	yes	ARC would see it				
v 1.1.2.0			140 output	3) hardware failure (chips,	ull	so it'd just keep going	would just be outvoted (via triple	causes 1 & 3	onc.	۷۱۸	vc	1-3	c would see It				
				connectors, FPGA, etc.)			voting). If demoted, processor										
					<u> </u>	<u> </u>	would be demoted to "failed."				<u> </u>	<u> </u>	<u> </u>	<u> </u>			

Subject Matter Expert(s): Geff Ottman (Avionics)

Richard Nichols (initial PDU) Sam Sawada (PDU)

Sam Sawada (PDU)

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FMEA information is only displayed in the first copy of the component.

AV-1.1 Avion Contr	Name	Function	Failure Mode / Limit	Response Level	Desired Local	Allocation of Local	Time to fix		ponse Desired System	Allocation of	Time to fiv	Time to Transmit	Ground Response /	System Side Switch	Quick Look	Cafa Manda	Remediation Helpful Autonomy Rule	. clas	
AV-1.1 Avion Contr			/ Constraint		Response	Response	locally	Signal	Response	System	system	Signal	Contingency	System side switch	Processor Switch	Safe Mode	Remediation Respiral Autonomy Rule	riag	Revisit Comments - KAF
AV-1.1 Avion Contr	lundant Proc Module									Response									
	onics Redundancy																		
AV-1.1.1 Proce	cessor A (Prime)			<u> </u>	<u> </u>			 	 			 			<u> </u>		<u> </u>		
	,																		
																	- Switch to 2nd set of		
AV-1.1.1.a			No output	Local	Processor switch	HW - ARC									X		- Cause 2 could		
																	possibly be fixed with		
																	reboot		
			Incorrect														Could try to reboot to		
AV-1.1.1.b			output/timing	Local	Processor switch	HW - ARC									X		fix software issue		
																	Loss of timecode - would		
AV-1.1.1.c (Inpu	out?)		Loss of SPW Timecode	Local	Side switch	HW - ARC								X			need to diagnose that it's not a SCIF failure, but the		
			rimeedae														LVDS receiver failing		
AV-1.1.1.d			Hard failure	Local	Processor switch	HW - ARC									X		Autonomy rule on hot spare to detect hard		
4V-1.1.1.u			riaiu iailuie	Local	Frocessor switch	TW - AIC									^		failure of Prime		
AV-1.1.1.1 Watc	tchdog Timer																		
	tendog miner		- 				ļ									•			<u></u>
AV-1.1.1.1.a			Failure to timeout	Local	Processor switch	HW - APC									X				x
			(when it should)	Local	Troccssor switch	AILC									Î .				^
			Timeout when it				Less than 10 ms												
AV-1.1.1.1.b			shouldn't	Local	Processor switch	HW - ARC	demote/promot	t							X				х
							e												
															<u> </u>			<u> </u>	
			SpW Router A (only																
nputs			one router active at a given time)																Х
			SpW Router B																
			SSR 1 (Prime only)	Local	Side switch	Autonomy								X					3 SSRs tied to each SBC, initial thought is that SBC sees error with
			,			,													SSR and requests demotion from ARC???
			SSR 2 (Prime only)														<u> </u>		
													No action by ARC, but						
			ARC Mode Controller	None									if ground identified the issue this processor						x
			1										could be marked						
			ARC Mode Controller	r									"failed"						
			2																
			ARC Mode Controller																
AV-1.1.2 Proce	cessor B (Hot)																		
					Hot spare												Cause 2 could possibly		
AV-1.1.2.a			No output	Local	demoted to "faield"	HW - ARC											be fixed with reboot		
<u> </u>			.i	<u>.</u>			İ		İ								.i		<u>.i</u>

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Tlm for Diagnosis	Method Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
AV-1.1.2.b			A)SpW->router B) commands to ARC C) SW issues	1) LVDS driver is flaky 2) SW issues 3) Communications path connector/harness issue (intermittent connection)		A) Might promote itself B) ARC acknowledge timer wouldn't get updated C) Depends on SW configuration	ARC would recognize issue and demote Hot Spare, and promote the Warm Spare. Processor would get demoted to "failed."	Loss of redundancy	None.	2R	Active	yes	ARC would see it				
AV-1.1.2.c AV-1.1.2.d			Loss of SPW Timecode ("1PPS")	LVDS receiver fails		Depends on SW configuration.	Hot spare could interpret this as a falsely failed Prime and request ARC demote Prime and promote the Hot Spare. The next Hot Spare would detect this as a failed Prime and the ARC would rotate everyone again or might switch side instead.	Loss of redundancy	None. When third processor is in "Cold" standby mode, we are far enough from the Sun that timing isn't critical and the s/c would be ok during the processor reboot.	2R	Active	yes	ARC (or next Hot Spare) may see it				
AV-1.1.2.e			Hard failure	1) PWB crack 2) Connector disconnects 3) Converter card fails		Processor dies	ARC would recognize issue and demote Hot Spare, and promote the Warm Spare	Loss of redundancy	None.	2R	Active	yes	ARC would see it				
AV-1.1.2.1	Watchdog Timer (This is the onboard WDT; the ARC hosts a second level WDT too)																
AV-1.1.2.1.a			Failure to timeout (when it should)	1) FPGA fails		Lose software with no way locally to recover	ARC would recognize issue and demote Hot Spare, and promote the Warm Spare	Loss of redundancy if FSW branches to WDT again.	None.	2S/R	Active	yes	ARC would see it				
AV-1.1.2.1.b			Timeout when it shouldn't	1) FPGA fails		Reboot	ARC would recognize issue and demote Hot Spare, and promote the Warm Spare	Loss of redundancy	None.	2R if whole processor is lost 3 if processor can keep working with no WDT	Active	yes	ARC would see it				
AV-1.13 AV-1.13.a	Processor C (Warm Spare)		No output	1) failed power supply 2) software hangs 3) hardware failure (chips, connectors, etc.)		No way to recongnize failure, so it'd just keep going	None.	Loss of redundancy for 1 &3, 2 could possibly be fixed with reboot	None.	2R	None	yes	Prime via SpW, if failure is known, ground could demote processor to "failed."				
AV-1.1.3.b			incorrect output/timing	1) LVDS driver is flaky 2) SW issues		Depends on SW configuration.	None.	Loss of redundancy	None.	2R	None	yes	Prime via SpW				
AV-1.1.3.c			Loss of SPW Timecode	LVDS receiver fails		Depends on SW configuration.	None.	Loss of redundancy	None.	2R	None	yes	Prime via SpW				
AV-1.1.3.d			Hard failure	1) PWB crack 2) Connector disconnects 3) Converter card fails		Processor dies	None.	Loss of redundancy	None.	2R	None	yes	Prime via SpW				
AV-1.13.1 AV-1.13.1.a	Watchdog Timer		Failure to timeout (when it should)	1) FPGA fails		Lose software with no way locally to recover	None.	Loss of redundancy if FSW branches to WDT again.	None.	25/R	None	yes	Prime via SpW				

							Re	sponse						Quick Look		1			
FMEA ID	Name Function	Failure Mode / Limit	Response Level				Time to Transmi	t Desired System		Time to fix		Ground Response /	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag Revisit	Comments - KAF
		/ Constraint		Response	Response	locally	Signal	Response	System Response	system	Signal	Contingency							
		Incorrect																	
AV-1.1.2.b		output/timing A)SpW->router	Local	Hot spare demoted to	HW - ARC											SW issue could	Prime could look for Hot		
AV-1.1.2.0		B) commands to ARC		"faield"	TIVV - AIRC											reboot	Prime could look for Hot Spare to be demoted		
		C) SW issues																	
AV-1.1.2.c		"Evil" hot spare															ý	Х	
		Loss of SPW															Loss of timecode - would need to diagnose that it's		
AV-1.1.2.d		Timecode ("1PPS")	Local	Side switch?	HW - ARC												not a SCIF failure, but the		
																	LVDS receiver failing		
AV-1.1.2.e		Hard failure	Local	Hot spare demoted to	HW - ARC												Prime could look for Hot		
				"faield"													Spare to be demoted		
	Watchdog Timer (This is the																		
AV-1.1.2.1	onboard WDT; the ARC hosts a second level WDT too)																		
	Second level WDT (DD)					Less than 10 ms													
۸۷ 1 1 2 1 -		Failure to timeout		Hot spare	LINAY ARIC	for													
AV-1.1.2.1.a		(when it should)	Local	demoted to "faield"	HW - ARC	demote/promot	i											Х	
						e													
		Timeout when it		Hot spare		Less than 10 ms for													
AV-1.1.2.1.b		shouldn't	Local	demoted to "faield"	HW - ARC	demote/promot	t											Х	
				Turcia		e													
AV-1.1.3	Processor C (Warm Spare)																		
						N/A. No fix possible other													
						than to demote						No action by ARC, but if ground identified the							
AV-1.1.3.a		No output	None			to cold spare.						issue this processor				Reboot might help a			
						ARC commanded to						could be marked				SW issue			
						not use this						"failed"							
						board.		ļ											
						N/A. No fix													
						possible other than to demote						No action by ARC, but							
AV-1.1.3.b		Incorrect	None			to cold spare.						if ground identified the issue this processor				Reboot might help a			
AV-1.1.5.0		output/timing	None			ARC commanded to						could be marked				SW issue			
						not use this						"failed"							
						board.													
						N/A. No fix													
						possible other						No action by ARC, but							
A)/ 4 4 2		Loss of SPW	Naca			than to demote to cold spare.						if ground identified the							
AV-1.1.3.c		Timecode	None			ARC						issue this processor could be marked							
						commanded to not use this						"failed"							
						board.													
						N/A. No fix					ļ								
						possible other						No action by ARC, but							
						than to demote to cold spare.						if ground identified the							
AV-1.1.3.d		Hard failure	None			to cold spare.						issue this processor					Loss of timecode		
						commanded to						could be marked "failed"							
						not use this board.													
AV-1.1.3.1	Watchdog Timer																		
						N/A. No fix													
						possible other													
		Failure to timeout				than to demote to cold spare.													
AV-1.1.3.1.a		(when it should)	None			ARC												Х	
						commanded to not use this													
						board.													
	ii		.4	k			i			i	.h	i	.X	.k	·		.X		J

							Effect							Detection I	Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed? Tin	n for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
			,							Sec,					2105110	(2000.)	(Gystem)
AV-1.1.3.1.b			Timeout when it shouldn't	1) FPGA fails		Reboot	None.	Loss of redundancy	None.	2R if whole processor is lost 3 if processor can keep working with no WDT	Active	yes	Prime via SpW				
AV-1.2	Avionics Redundancy Controller (ARC) - Mode Controller 1 only (other MCs would have same answers; the three MCs are triple voted at each processor).																
AV-1.2.a			No output	1) failed power supply 2) bad FPGA 3) hardware failure (chips, connectors, etc.)		Invalid output to all three processors and on-card voting circuits	None, due to two other MCs	None	None	2R	Active	Yes	Processor reports to autonomy/ ground a non- responsive MC				
AV-1.2.b			Incorrect output	Single LVDS driver fails		Invalid output to one processor or on-card voting circuit	None, due to two other MCs	None	None	2R	Active	Maybe	Processor reports to autonomy/ ground a non- responsive MC or other MCs report to processor non- majority vote				
AV-1.2.c			Hard failure	1) PWB crack 2) Connector disconnects 3) Converter fails 4) Overcurrent (required to include a current limiter)		1)Single failed MC; 1, 2, 3, and 4) Invalid output to all three processors (unique to individual MC) 4) MCs are individually fused in PDU for very large overcurrent, MC has built-in current limiting to mitigate internal fault		None	None	2R	Active	yes	Processor reports to autonomy/ ground a non- responsive MC				
Inputs			CCD Commands	Failed LVDS chip		None, due to triple voting	None	None	N/A	2R	Active	Yes	Processor reports to autonomy/ ground a non- responsive MC				
			SBC Prime or hot spare commands	Failed LVDS chip		None, due to triple voting	None	None	N/A	2R	Active	Yes	Processors report bad triple vote. Potential loss of ARC MC telemetry.				
			Power inputs (unswitched)	Blown fuse, bad connector, component failure		None, due to triple voting	None	None.	N/A	2R	Active	Yes	Processors report bad triple vote. Loss of ARC MC telemetry.				
AV-1.3	Avionics Redundancy Controller (ARC) - Mode Controller 2																
AV-1.4	Avionics Redundancy Controller (ARC) - Mode Controller 3 Redundant Elec Module																
AV-2.1	REM A																
AV-2.1.1 AV-2.1.1.a	TAC A		No output (hard failure)	1) failed power supply connector 2) hardware failure (chips, connectors, etc.) 3) Overcurrent		Loss of thruster and G&C control interfaces	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime, non- responsive SpW interface; G&C closed loop SW				
AV-2.1.1.b			Incorrect output	1) SpW failed 2) LVDS receiver fails		a) Loss of thruster and G&C	a & b) Prime tells ARC to initiate side switch, ARC switches sides of avionics. b only) Time to detect is much higher than a.	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime, non- responsive SpW interface; G&C closed loop SW				
AV-2.1.1.c			Incorrect timing	Bad board oscillator		Loss of thruster and G&C control interfaces	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime, non- responsive SpW interface; G&C closed loop SW				

							Res	sponse						Quick Look					
FMEA ID	Name F	unction Failure Mode / Limit / Constraint	t Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	t Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag Revisit	Comments - KAF
AV-1.1.3.1.b		Timeout when it shouldn't	Local	Processor reboot	HW - ARC	N/A. No fix possible other than to demote to cold spare. ARC commanded to not use this board.												х	
AV-1.2	Avionics Redundancy Controller (ARC) - Mode Controller 1 only (other MCs would have same answers; the three MCs are triple voted at each processor).																		
AV-1.2.a		No output	Local	Processor flags faulted MC for ground, but it will be out voted so no other action taken	HW - ARC	N/A. No fix, MC are on unswictched power services.													
AV-1.2.b		Incorrect output	Local	Processor flags faulted MC for ground, but it will be out voted so no other action taken	HW - ARC	N/A. No fix, MC are on unswictched power services.													
AV-1.2.c		Hard failure	Local	Processor flags faulted MC for ground, but it will be out voted so no other action taken	HW - ARC	N/A. No fix, MC are on unswictched power services.													
Inputs		CCD Commands	Local	Processor flags faulted MC for ground, but it will be out voted so no other action taken	HW - ARC														
		SBC Prime or hot spare commands	Local	Processor flags faulted MC for ground, but it will be out voted so no other action taken	HW - ARC														
		Power inputs (unswitched)	Local	Processor flags faulted MC for ground, but it will be out voted so no other action taken	HW - ARC														
AV-1.3	Avionics Redundancy Controller (ARC) - Mode Controller 2 Avionics Redundancy																		
AV-1.4 	Controller (ARC) - Mode Controller 3 Redundant Elec Module																		
	REM A TACA	No output (hard failure)	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Try power cycle during check-out or ground contact			
AV-2.1.1.b		Incorrect output	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Try power cycle during check-out or ground contact			
AV-2.1.1.c		Incorrect timing	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Try power cycle during check-out or ground contact			

FINEALD Name Function Failure Mode / Limit Possible Causes Phase Local Next Higher Mission Umbra Violation Severity Type of IM Observed	Vable How Observed? Tim for Diagnosis Tim Path for Diagnosis (Local) Time to Obtact (Local) Prime, non-responsive SpW interface; G&C closed loop SW Prime Non-responsive SpW interface; G&C closed loop SW Prime via SpW interface; G&C closed loop SW
Inputs SpaceWire Loss of thruster and G&C control interfaces SpaceWire Loss of thruster and G&C control interfaces SpaceWire Loss of thrusters Loss of thru	Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW
SpaceWire Control Interfaces with ARC witches sides of avoid. Propulsion bus Propulsion bus Loss of thrusters Prime tells ARC to initiate side witch, ARC witches sides of avoid. SRC component data SRC component data Loss of GRC control Interfaces witch, ARC witches sides of avoid. Loss of GRC control Interfaces witch, ARC witches sides of avoid. Loss of GRC control Interfaces witch, ARC witches sides of avoid. None Depends on side switch and switch and switch and switch and switch and switch and switch and switch and switch and reconfig time. AV-2.1.2 SSR A Locks up/resets Bad FPGA Loss of SSR data Prime tells, ARC to initiate side witch, ARC switches sides of avoid. None Depends on side switch and reconfig time. Prime tells, ARC to initiate side witch, ARC switches sides of avoid. None Depends on side switch and reconfig time. ARIVE Yes ALIVE Yes ALIVE Yes AV-2.1.2.1 SSR A Locks up/resets Bad FPGA Loss of SSR data Prime tells, ARC to initiate side witch, ARC switches sides of avoid. None Depends on side switch and reconfig time. ARIVE Yes ALIVE Yes ARIVE Yes ALIVE Yes ALIVE Yes ALIVE Yes ALIVE Yes ARIVE Yes	responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW interface; G&C closed loop SW
SpaceWire Control Interfaces with ARC witches sides of avoid. Propulsion bus Propulsion bus Loss of thrusters Prime tells ARC to initiate side witch, ARC witches sides of avoid. SRC component data SRC component data Loss of GRC control Interfaces witch, ARC witches sides of avoid. Loss of GRC control Interfaces witch, ARC witches sides of avoid. Loss of GRC control Interfaces witch, ARC witches sides of avoid. None Depends on side switch and switch and switch and switch and switch and switch and switch and switch and switch and reconfig time. AV-2.1.2 SSR A Locks up/resets Bad FPGA Loss of SSR data Prime tells, ARC to initiate side witch, ARC switches sides of avoid. None Depends on side switch and reconfig time. Prime tells, ARC to initiate side witch, ARC switches sides of avoid. None Depends on side switch and reconfig time. ARIVE Yes ALIVE Yes ALIVE Yes AV-2.1.2.1 SSR A Locks up/resets Bad FPGA Loss of SSR data Prime tells, ARC to initiate side witch, ARC switches sides of avoid. None Depends on side switch and reconfig time. ARIVE Yes ALIVE Yes ARIVE Yes ALIVE Yes ALIVE Yes ALIVE Yes ALIVE Yes ARIVE Yes	interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW interface; G&C closed loop SW
Propulsion bus Propulsion bus Loss of thrusters Prime tells ARC to initiate side switch, ARC with sides of avoinics which said experts and experiment to avoinics which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoinic which said experiment to avoin the said experiment to avoin th	closed loop SW Prime, non- responsive SpW Interface; G&C closed loop SW Prime, non- responsive SpW Interface; G&C closed loop SW Prime, non- responsive SpW Interface; G&C closed loop SW Prime, non- responsive SpW Interface; G&C closed loop SW
Propulsion bus loss of thrusters switch, ARC switches sides of avionics switch and reconfig time loss of SRC component data Cost of GRC component data Cost of SRC control interfaces switch, ARC switches sides of avionics Cost of thruster and GRC control interfaces switch, ARC switches sides of avionics Cost of thruster and GRC control interfaces Cost of thruster and GRC cost o	responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Interface; G&C closed loop SW
G&C component data G&C control interfaces None Gends G&C component data G&C component data G&C component data G&C control interfaces G&C co	interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW Orime, non- responsive SpW interface; G&C closed loop SW
G&C component data Loss of G&C control interfaces Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics	Prime, non- responsive SpW interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW
Loss of factive and G&C control interfaces switch, ARC switches sides of avionics Secondary power Loss of thruster and G&C control interfaces witch, ARC switches sides of avionics NV-2.1.2 SSR A Loss of thruster and G&C control interfaces witch, ARC switches sides of avionics None Depends and 2R Active Yes witch and reconfig time 2R Active Yes Active Yes	responsive SpW Interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW
AV-2.1.2.b data data Loss of SSR data Prime tells ARC to initiate side switch, ARC switches sides of avionics None Depends on side switch and reconfig time Prime tells ARC to initiate side switch, ARC switches sides of avionics None Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to initiate side switch, ARC switches sides of avionics Prime tells ARC to	interface; G&C closed loop SW Prime, non- responsive SpW interface; G&C closed loop SW
Secondary power Loss of thruster and G&C control interfaces Prime tells ARC to initiate side switch, ARC switches sides of avionics None Depends on side switch and reconfig time 2R Active Yes Active Yes Active Yes AV-2.1.2.a AV-2.1.2.a AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data 2 (ongoing trade) None. None Active Yes Active Yes	Prime, non- responsive SpW interface; G&C closed loop SW
Secondary power Control interfaces switch, ARC switch, ARC switch and reconfig time 2R Active Yes AV-2.1.2.a SSR A Locks up/resets Bad FPGA Loss of SSR data 7 (ongoing trade) None. None Active Yes AV-2.1.2.b Loss of SSR data 7 (ongoing trade) None. None Active Yes	responsive SpW interface; G&C closed loop SW
AV-2.1.2.b SSR A Locks up/resets Bad FPGA Loss of SSR data ? (ongoing trade) None. None Active Yes	closed loop SW
AV-2.1.2.a SSR A Locks up/resets Bad FPGA Loss of SSR data ? (ongoing trade) None. None Active Yes AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None None Active Yes	
AV-2.1.2.a Locks up/resets Bad FPGA Loss of SSR data ? (ongoing trade) None. None Active Yes AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	Prime via SpW
AV-2.1.2.b Hard failure 1) PWB crack 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	Prime via SpW
AV-2.1.2.b Hard failure 1) PWB crack 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	Prime via SpW
AV-2.1.2.b Hard failure 1) PWB crack 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	Prime via SpW
AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	
AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	
AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	
AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	
AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	
AV-2.1.2.b Hard failure 2) Connector disconnects Loss of SSR data ? (ongoing trade) None. None Active Yes	
	Prime via SpW
Inputs Loss of SSR data ? (ongoing trade) None. None Active Yes	Prime via SpW
secondary power Loss of SSR data ? (ongoing trade) None. None Active Yes	Prime via SpW
AV-2.12.1 Memory	
AV-2.1.2.1.a Memory IC failure Bad part Loss of some SSR data ? (ongoing trade) None. None Active Yes	File system on Prime would
	notice bad sector
AV-2.1.3	
AV-2.1.3 SpW Router A	
Consider reinitializatin of SCIF, but Donards on side	
AV-2.1.4.a No output Failed FPGA Loss of SpW connectivity initiate ride putter APC suitches None switch and 2R Active Yes	Prime via SpW
sides of avionics reconfig time	
Prime tells ARC to initiate side Depends on side	
AV-2.1.4.b Incorrect output Failed FPGA Bad data switch, ARC switches sides of None switch and 2R Active Yes avionics	Prime via SpW
avionics reconfig time	
Prime tells ARC to initiate side Depends on side	
AV-2.1.4.c Incorrect timing Failed FPGA Bad data switch, ARC switches sides of None switch and 2R Active Yes avionics reconfig time	Prime via SpW
Consider reinitialization of SCIE- but	
logists otherwise Prime tells ARC to None switch and 2P Active Ver	Prime via SpW
initiate side switch, ARC switches	crime via Spvv
States of advices of a control of SCIE but	
Bus voltage Uses of SnW connectivity otherwise Prime tells ARC to None switch and 2R Active Yes	Prime via SpW
initiate side switch, ARC switches sides of avionics	Control Spring
Sides of avonics Will detect incorrect input	
Incorrect input Router continues functioning elsewhere (depending on what the	
normally input was and where it was routed to	
Bad input	
AV-2.1.5 SCIFA	

Mail Mail	nts - KAF
Figure 1 Service Servi	
Property of the control of the con	
Specified Space We shall be sh	
AV 2.1.2.b AV 3.1.2.b AV 4.1.2.b AV 5.1.2.b AV 4.1.2.b AV 5.1.2.b AV 4.1.2.b AV 4.1	
Frequency of the secondary power of the secon	
GGC Component data GGC Component data GGC Component data AC cide switch over requests AC cide switch over requests and control state of the switch over requests denoted by the state of the switch over requests denoted by the switch over reques	
AV 2.1.2.b	
AV-2.12.b Mark failure Mark fail	
Secondary power Local Secondary power Local	
AV-2.1.2. SSR A AV-2.1.2.a Locks up/resets Local Av-2.1.2.b Locks up/resets Av-2.1.2.b Locks up/resets Av-2.1.2.b Locks up/resets Local Av-2.1.2.b Locks up/resets Av-2.1.2.b Locks up/resets Local Av-2.1.2.b Locks up/resets	
AV-2.1.2.a SSR A AV-2.1.2.a Locks up/resets Local locks up/resets Local locks up/resets Local locks up/resets local locks up/resets local locks up/resets local local locks up/resets local loc	
AV-2.1.2 a V-2.1.2 a V-2.1.2 b V-2.1	
AV-2.1.2.a Locks up/resets Local shart SSC sees error with SSR and requests demotion from ARC??? AV-2.1.2.b Hard failure Local shart SSC sees error with SSR and requests demotion from ARC??? SSR switchover; File system mount Try power cycle X SSR switchover; SSR swi	
AV-2.1.2.a Locks up/resets Local is that SBC sees error with SSR and requests demotion from ARC??? AV-2.1.2.b Hard failure Local is that SBC sees error with SSR and requests demotion from ARC??? SSR switchover; File system mount Try power cycle Try power cycle X Try power cycle X Try power cycle X	
AV-2.1.2.a Locks up/resets Local is that SBC sees error with SSR and requests demotion from ARC??? AV-2.1.2.b Hard failure Local is that SBC sees error with SSR and requests demotion from ARC??? SSR switchover; File system mount Try power cycle Try power cycle X Try power cycle X Try power cycle X	
AV-2.1.2.a Locks up/resets Local strat Successor are reported that Successor are reported to the report of the Successor are reported to the succe	
AV-2.1.2.b AV-2.1.2.b Av-2.1.2.b	
AV-2.1.2.b Hard failure Local SSRs tied to each SBC, initial thought is that SBC sees error with SSR and requests demotion	
AV-2.1.2.b Hard failure Local SBC, initial thought is that SBC sees error with SSR and requests demotion on the content of the	
AV-2.1.2.b Hard failure Local SBC, initial thought is that SBC sees error with SSR and requests demotion requests demotion	
AV-2.1.2.b Hard failure Local SBC, initial thought is that SBC sees error with SSR and requests demotion requests demotion	
AV-2.1.2.D Hard failure Local error with SSR and requests demotion requests demotion requests demotion	
requests demotion	
TOM AKL???	
3 SSRs tied to each SBC, initial thought	
Inputs SpaceWire Local is that SBC sees Processor File system STV power cycle Y	
error with SSR and requests demotion requests demotion	
from ARC???	
3 SSRs tied to each	
SBC, initial thought is that SBC sees SSR switchover;	
secondary power Local error with SSR and Processor File Structure Industrial Information I	
requests demotion from ARC???	
N/3131 Marian	
AV-2.1.2.1 Memory	
3 SSRs tied to each SSRc, initial thought	
is that SDC coor. Add to had	
AV-2.1.2.1.a Memory IC failure Local States Secretary with SSR and Frequests demotion Processor	
from ARC???	
AV-2.1.3 SSR B	
AV-2.1.4 SpW Router A	
Power cycle during prime requests pround contact &	
AV-2.1.4.a NO Output Cocal ARC side switch NV - ARC Side switch NV - ARC	
out Power cycle during	
Prime requests Prime request Prime requests Prime request Prime re	
AV-2.1.4.D Incorrect output Local ARC side switch ARC side swi	
Power cycle during Power cycle during	
AV-2.1.4.c Incorrect timing Local Prime requests ARC side switch Prime requests ARC side switchover Side switc	
Out Out Out	
Power cycle during Prime requests Prime requests your and State of the Prime requests your and state of the Prime requests	
inputs perform REM check perform REM check	
out Out Power cycle during	
Prime requests HW APC Side suits bours	
Post Voltage ARC side switch ARC side	
Incorrect input 7 7 7 7 X	
AV-2.1.5 SCIF A	

							Effect							Detection	Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
**************************************														,			
AV-2.1.5.a			Local failure	Bad IC or other component (failure isolated to a single			Prime tells ARC to initiate side switch, ARC switches sides of	None	Depends on side switch and	2R	Active	Yes	Prime via SpW				
				interface)		instrument	avionics		reconfig time								
AV-2.1.5.b			Hard failure	Cracked board; failed FPGA		Loss of interface with all S/C	Prime tells ARC to initiate side switch, ARC switches sides of	None	Depends on side switch and	2R	Active	Yes	Prime via SpW				
						components and instruments	avionics		reconfig time								
			Incorrect timing with				Prime tells ARC to initiate side		Depends on side								
AV-2.1.5.c			transponder clock interface	Failed FPGA		Bad data	switch, ARC switches sides of avionics	None	switch and reconfig time	2R	Active	Yes	Prime via SpW				
							Prime tells ARC to initiate side		Depends on side								
AV-2.1.5.d			Incorrect output	Failed FPGA		Bad data	switch, ARC switches sides of avionics	None	switch and reconfig time	2R	Active	Yes	Prime via SpW				
							Prime tells ARC to initiate side		Depends on side								
Inputs			SpaceWire			Loss of interface with all S/C components and instruments	switch, ARC switches sides of	None	switch and	2R	Active	Yes	Prime via SpW			İ	
							avionics		reconfig time								
			Secondary Power			Loss of interface with all S/C components and instruments	Prime tells ARC to initiate side switch, ARC switches sides of	None	Depends on side switch and	2R	Active	Yes	Prime via SpW				
						components and instruments	avionics		reconfig time								
										2 - if FIELDS is lost							
			Component/			Lose telemetry from	Depends on		Depends on side	2R - if a critical component is lost							
			Instrument telemetry			component or instrument	component/instrument lost - worst case would cause a side switch		switch and reconfig time	3 - if another instrument is lost	Active	Yes	Prime via SpW				
			,						Ĭ	4 - for other (non- critical) components							
										cinically components							
			EMXO - EMXO lives				May attempt to reconfigure first,										
			in XCVR now; Rich	1) Harness break			but may also try side switch of REM (won't work unless		Depends on side								
				Failure at source (see transponder)		Won't receive PPS or 50 Hz	transponders are switched too). Path taken would depend on first	None	switch and reconfig time		Active					İ	
			plan.				symptom seen.										
AV 2.1.5.1	CCD (TBD - probably going																
AV-2.1.5.1	away)												Ground				
AV-2.1.5.1.a			Hard failure	Failed FPGA		Loss of config commands	None	None	None	4		Yes	verification of CCD commands				
AV-2.2 AV-2.2.1	REM B TAC B																
AV-2.2.2	SSR B																
AV-2.2.2.1 AV-2.2.3	Memory SpW Router B																
AV-2.2.4 AV-2.2.4.1	SCIF B CCD																
AV-2.2.4.2 AV-4	EXMO RIUs													,			
	RIUs RIU-A RIU-A 1																
							For non-critical loads, no effect.										
	RIUs are cross-strapped - two			1) Broken wire			For critical loads, autonomy would detect missing or bad value and										
AV-3.1.01.a	eight-RIU strips which can be powered by REM A or REM B.			2) IC failure 3) Hard short on card		No temperature data from RIU.		None	None	4	Active	yes	FSW detects bad data			2-3 seconds (for critical data)	
	16 RIUs total			s, riara silor on cara			power causing the loss of the									İ	
							string.										
							For non-critical loads, no effect.						FOLIA I :			22	
AV-3.1.01.b			Incorrect output	Loose wire or noise		Bad temp data from sensor	For critical loads, autonomy would detect missing or bad value and	None	None	4	Active	yes	FSW detects bad data			2-3 seconds (for critical data)	
							switch to B string.										
							For non-critical loads, no effect. For critical loads, autonomy would						FSW detects bad			2-3 seconds (for	
AV-3.1.01.c			Incorrect timing	Loose wire or noise		Bad temp data from sensor	detect missing or bad value and	None	None	4	Active	yes	data			critical data)	
							switch to B string.										
Inputs			Secondary Power			No temperature data from	For non-critical loads, no effect. For critical loads, autonomy would	None	None	4	Active	ves	FSW detects bad			2-3 seconds (for	
put3			- somany i owei			RIU.	detect missing or bad value and switch to B string.			7		,	data			critical data)	
		h	Face	.a		6	6				·fr						

									snonso						Quick Look		ı				
FMEA ID	Name	Function	Failure Mode / Limit	t Response Level	Desired Local	Allocation of Loca	al Time to fix		sponse t Desired System	Allocation of	Time to fix	Time to Transmit	Ground Response /	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
			/ Constraint		Response	Response	locally	Signal	Response	System Response	system	Signal	Contingency								
										Kesponse							Power cycle during		·		
AV-2.1.5.a			Local failure	Local	Prime requests	HW - ARC	Side switchover							X			ground contact &				
AV 2.1.5.0			Local failure	Local	ARC side switch	TW ARC	Side Switchover							^			perform REM check out				
				<u> </u>		<u> </u>					-						Power cycle during		<u> </u>		
AV/ 2.4.5.b			Hard failure	Local	Prime requests	LINK ARC	Side switchover							X			ground contact &				
AV-2.1.5.b			naru ialiure	Local	ARC side switch	HW - ARC	Side Switchover							^			perform REM check				
				ļ	-				-	·							out Power cycle during		. .		
			Incorrect timing with		Prime requests												ground contact &				
AV-2.1.5.c			transponder clock interface	Local	ARC side switch	HW - ARC	Side switchover							X			perform REM check				
			interrace			ļ											out		ļ		
					Prime requests												Power cycle during ground contact &				
AV-2.1.5.d			Incorrect output	Local	ARC side switch	HW - ARC	Side switchover							X			perform REM check				
																	out		ļ		
					Drimo roquests												Power cycle during ground contact &				
Inputs			SpaceWire	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			perform REM check				
																	out]		
																	Power cycle during				
			Secondary Power	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			ground contact & perform REM check				
					Side Switten												out				
					Depends on																
					component																
			Component/		affected: 1)Prime	1) HW - ARC											Power cycle during				
			Instrument	Local	requests ARC side switch		Side switchover							X			ground contact & perform REM check			X	
			telemetry		2)Switch to	2) Autonomy											out				
					redundant																
					component																

			EMXO - EMXO lives		Prime requests																
			in XCVR now; Rich		ARC side switch																
			Conde is working on	Local		HW - ARC								X						Х	
			a fault mitigation		May reconfigure																
			plan.		EMXO first????																
	CCD (TBD - probably going																				
	away)																		.l		
AV-2.1.5.1.a			Hard failure				Side switchover														
						ļ													.		
AV-2.2 AV-2.2.1	REM B TAC B					ļ													.ļ		
AV-2.2.1																			·		
AV-2.2.2.1	Memory																		<u></u>		
AV-2.2.3																			ļ		
AV-2.2.4 AV-2.2.4.1	SCIF B			-		<u></u>													ļ		
AV-2.2.4.2				†	<u> </u>	<u> </u>			<u> </u>	†		-							<u>.</u>		
AV-4	RIUs																		·	,	
	RIU-A RIU-A 1			-	- 														ļ	_	
AV-3.1.U1	MO-A 1			†	<u> </u>	†		ļ	·		-								·	-	
					For critical loads,																
	RIUs are cross-strapped - two				switch to																
AV-3.1.01.a	eight-RIU strips which can be powered by REM A or REM B.		No output	Local	redundant unit if temp data above	Autonomy											Power cycle during ground contact.				
	16 RIUs total				threshold or												o. III. I contact.				
					missing/stale?																
				ļ		ļ				ļ									<u> </u>	-	
					For critical loads,																
					switch to redundant unit if												Power cycle during				
AV-3.1.01.b			Incorrect output	Local	temp data above	Autonomy											ground contact.				
					threshold or																
					missing/stale?																
					For critical loads,																
					switch to														•		
AV-3.1.01.c			Incorrect timing	Local	redundant unit if	Autonomy											Power cycle during				
5.1.01.0			cocot tilling		temp data above												ground contact.				
					threshold or missing/stale?																
						ļ													ļ		
					For critical loads,																
					switch to redundant unit if												Power cycle during				
Inputs			Secondary Power	Local	temp data above	Autonomy											Power cycle during ground contact.		•		
					threshold or																
					missing/stale?																
	i.																				

							Effect							Detection	Method		1
FMEA ID	Name	Function	Failure Mode / Limit	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation		Type of FM	Observable	How Observed?	Tlm for Diagnosis		Time to Detect	Time to Detect
			/ Constraint							Severity					Diagnosis	(Local)	(System)
			I2C bus			No temperature data from RIU.	For non-critical loads, no effect. For critical loads, autonomy would detect missing or bad value and switch to B string.	None	None	4	Active	yes	FSW detects bad data			2-3 seconds (for critical data)	
			Telemetry input (temp sensor, tell tales)			No data from specific component	For non-critical loads, no effect. For critical loads, autonomy would detect missing or bad value and switch to B string.	None	None	4	Active	yes	FSW detects bad data			2-3 seconds (for critical data)	
	RIU-A 2													ļ			
AV-3.1.03 AV-3.1.04	RIU-A 3 RIU-A 4																
AV-3.1.05	RIU-A 5																
AV-3.1.06	RIU-A 6													ļ			
AV-3.1.07 AV-3.1.08	RIU-A 7 RIU-A 8					i 					i 			i 			
AV-3.1.08	RIU-B																
AV-3.2.01	RIU-B 1																
AV-3.2.02 AV-3.2.03	RIU-B 2 RIU-B 3										ļ						
AV-3.2.04	RIU-B 4													<u> </u>			
AV-3.2.05	RIU-B 5)															
AV-3.2.06	RIU-B 6													ļ			
AV-3.2.07 AV-3.2.08	RIU-B 7 RIU-B 8													<u>.</u>			
	Power Distribution Unit					<u> </u>					l			<u> </u>	I		
AV-4.1	Side A																
		Provides C&DH command interface to PDU															
		2) Provides PDU telemetry interface															
AV-4.1.1	CMD TLM A	to C&DH															
,,,		3) Provides +5V to Relay/Cap and															[
		FET Switching slices 4) Provides internal bus signals															
		5) Provides separation interface									ĺ			ļ			
AV-4.1.1.a				1) SEU 2) SW failure	All	Unable to interface with REM and provide command/telemetry interface	Loads stay on. Switch sides of Avionics.	No effect	Should be within timeframe of loss of control loop.	4	Active	yes	No PRIO telemetry	PDU heartbeat	PDU to REM	n/a	
AV-4.1.1.b			Unexpected reset	1) SEU 2) SW failure		and provide	Loads all get switched off. Switch sides of Avionics. Reset sequence in PDU switches loads back on.		Should be within timeframe of loss of control loop.	4	Active	yes	Lots of components get switched off unexpectedly.	PDU heartbeat	PDU to REM		
AV-4.1.1.c			PDU Power and reset sequence doesn't run when expected			A whole list of things which should occur (HW getting switched on/off, etc.) doesn't.	Avionics side switch.	No effect	Should be within timeframe of loss of control loop.	4	Active	yes	Things which should occur during PDU reset don't.	PDU heartbeat	PDU to REM		
AV-4.1.1.d			Hard failure	1) Electronics failure 2) Connector/cable failure	All	Card unusable. No ability to interface with REM. Critical board function(s) are not working. No secondary power to other slices.	Switch to B side of avionics	No effect	Unless something needs to be commanded during switchover time period to PDU B, umbra violation shouldn't be possible	2R	Active	yes	Stale/anomalous telemetry	PDU heartbeat	PDU to REM		
Inputs			Command/ telemetry interfaces			Components would stop getting telemetry	Switch to B side of avionics	No effect		2R	Active	yes	Stale telemetry	PDU heartbeat	PDU to REM		

								Res	sponse					1	Quick Look		•			
FMEA ID	Name	Function	Failure Mode / Limit	Response Level	Desired Local	Allocation of Local	Time to fix		Desired System	Allocation of	Time to fix	Time to Transmit	Ground Response /	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag Revisit	Comments - KAF
			/ Constraint	·	Response	Response	locally	Signal	Response	System	system	Signal	Contingency							
										Response										
				•	For critical loads,															
					switch to redundant unit if												Power cycle during			
			I2C bus	Local	temp data above	Autonomy											ground contact.			
					threshold or															
					missing/stale?															
					For critical loads,					!·····				•	·					
					switch to															
			Telemetry input (temp sensor, tell	Local	redundant unit if	Autonomy											Power cycle during			
			tales)	Local	temp data above	Autonomy											ground contact.			
			,		threshold or															
					missing/stale?	ļ														
AV-3.1.02 AV-3.1.03	RIU-A 2 RIU-A 3					ļ														
AV-3.1.03 AV-3.1.04	RIU-A 4					}		ļ			·									
	RIU-A 5					1														
AV-3.1.06	RIU-A 6					ļ														
	RIU-A 7					ļ		ļ	ļ		ļ					<u> </u>				
	RIU-A 8 RIU-B					ļ			ļ		·									<u> </u>
	RIU-B 1								 	ļ	 									
AV-3.2.02	RIU-B 2																			
	RIU-B 3					ļ			ļ											
AV-3.2.04 AV-3.2.05	RIU-B 4 RIU-B 5					ļ			ļ											
	RIU-B 6																			
	RIU-B 7		·			ļ				ļ	·			·	·					
	RIU-B 8																			
	Power Distribution Unit					ļ					ļ				ļ					
AV-4.1	Side A	1) Provides C&DH command				ļ														
		interface to PDU																		
		2) Provides PDU telemetry interface	•																	
AV-4.1.1	CMD TLM A	to C&DH																		
		Provides +5V to Relay/Cap and FET Switching slices																		
		Provides internal bus signals																		
		5) Provides separation interface																		
					System side												Autonomy would see stale data or would			
			t and an	t and	switch; return to		- 1-	TBD - based on						,			set a flag indicating			
AV-4.1.1.a			Lock up	Local	previous load	Autonomy	n/a	autonomy rule						X			stale/non-responsive			
					configuration												PDU and switch to B			
																	side.			
					System side switch; return to															
AV-4.1.1.b			Unexpected reset	Local	previous load	Autonomy														
					configuration															
					C				!		<u> </u>			•		ā				
			PDU Power and reset	t	System side															
AV-4.1.1.c			sequence doesn't	Local	switch; return to previous load	Autonomy														
			run when expected		configuration															
					System side															
AV-4.1.1.d			Hard failure	Local	switch; return to previous load	Autonomy											Switch to side B			No PDU switch, this should be system side switch
					configuration															
					_															
					System side	ļ	<u> </u>		ļ		ļ									
			Command/	l a sal	switch; return to															No applies the late of the lat
Inputs			telemetry interfaces	rocai	previous load	Autonomy													Х	No PDU switch, this should be system side switch
				<u> </u>	configuration	<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>	<u> </u>			<u> </u>	<u> </u>		<u> </u>	<u> </u>	<u> </u>	<u> </u>

_				<u>.</u>		Effect				_			Detection			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
			2 Breakwires	Until separation from 3rd stage	If both breakwires on the active PDU broke prior to separation, would get a false indication of separation.	Switch to B side of avionics	No effect	N/A	4	Active			PDU heartbeat	PDU to REM		
			Power (switched in ARC)	All	Card unusable. No ability to interface with REM. Critical board function(s) are not working. No secondary power to other slices.	Switch to B side of avionics	No effect	Unless something needs to be commanded during switchover time period to PDU B, umbra violation shouldn't be possible	2R	Active		Stale/anomalous telemetry	PDU heartbeat	PDU to REM		
AV-4.1.2	Relay Cap A	1) Provides main bus voltage for critical and non-critical loads 2) Provides load current telemetry (total and individual loads and non-critical loads) 3) Provides safety bus voltages 4) Provides capacitance for main bus 5) Provides connection to single point ground 6) Provides power to unswitched services 7) Includes "common relays" (used for autonomy) 8) Connection to umbilical power 9) Misc. functions: 9a) Fuse monitoring 9b) Arming plug monitoring 9c) Temperature monitoring (for informational purposes only)														
AV-4.1.2.a			Fails to provide function #1 (main bus voltage for critical and non- critical loads)	1) Incoming power wire breaks/bad connection 2) Short to ground (double- insulated wires)	1) Multiple pairs (6) of incoming power wires (power & return) per RC slice. The loss of a single wire/pair would be within margin for s/c. The loss of more than one (multiple failures) would cause there to be too little power available to the s/c. 2) An unconstrained short would melt the wires and discharge the battery.	1) No effect (assuming a single	1) No effect (assuming a single failure) 2) LOM	N/A	1) 4 2) 2	Active			State of charge			
AV-4.1.2.b			Fails to provide function #2 (load current telemetry)		PSE also supplies total current telemetry. Non-critical failure.	Worst case, switch off a single load.	Worst case would switch off one of the instruments, degrading (but not failing) science.	N/A	2 - if FIELDS is lost 2R - if a critical component is lost 3 - if another instrument is lost 4 - for other (non-	Active						
AV-4.1.2.c			Fails to provide function #3 (safety bus voltages)		Redundant relay for each bus. Two safety buses. Would need four failures to fail to power a component on a safety bus from this PDU.	No effect.	No effect.	N/A	4	Passive - Redundancy						
AV-4.1.2.d			Fails to provide function #4 (capacitance for main bus)	Capacitor shorts	Fused to prevent power spike.	More noise to loads.	No effect.	N/A	4	None						
AV-4.1.2.e			Fails to provide function #5 (connection to single.		Should have redundant wires (Rich checking)	No effect.	No effect.	N/A	4 (with redundant wires)	Passive - Redundancy						

								Res	sponse						Quick Look		•			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally		Desired System Response	Allocation of System	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag Revisit	Comments - KAF
			2 Breakwires	Local	System side switch; return to previous load configuration	Autonomy				Response							Each PDU requires 2 of 2 to be broken to indicate separation. Veracity of false separation indication could be determined by switching on redundant PDU. Would need four separate failures for both PDUs to falsely indicate separation prior to it actually occurring.			No PDU switch, this should be system side switch
			Power (switched in ARC)	Local	System side switch; return to previous load configuration	Autonomy														No PDU switch, this should be system side switch
AV-4.1.2	Relay Cap A	1) Provides main bus voltage for critical and non-critical loads 2) Provides load current telemetry (total and individual loads and non-critical loads) 3) Provides safety bus voltages 4) Provides capacitance for main bus 5) Provides connection to single point ground 6) Provides power to unswitched services 7) Includes "common relays" (used for autonomy) 8) Connection to umbilical power 9) Misc. functions: 9a) Fuse monitoring 9b) Arming plug monitoring 9c) Temperature monitoring (for informational purposes only)																	X - When we know what loads are where	
AV-4.1.2.a			Fails to provide function #1 (main bus voltage for critical and non- critical loads)	System	LBSOC Safing	Autonomy											None			Relay Cap A & B on same card? So nothing we can do? Would look like unexpected battery discharge fault, but not fixable??
AV-4.1.2.b			Fails to provide function #2 (load current telemetry)	Local	For some loads, may want to re- enforce that one is always on?	Autonomy													x	
AV-4.1.2.c			Fails to provide function #3 (safety bus voltages)																	
AV-4.1.2.d			Fails to provide function #4 (capacitance for main bus) Fails to provide																	
AV-4.1.2.e			function #5											<u></u>					Х	

							Effect						Detection	Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed? Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
AV-4.1.2.f			Fails to provide function #6 (power to unswitched services)			theaters have series redundant thermostats to prevent "stuck on" load (need double- insulated wires). All unswitched loads allocated redundantly, so loss of a single one is ok.		No effect.	N/A	4	Passive - Redundancy					
AV-4.1.2.g			Fails to provide function #7 ("common relays")			Not currently planning to use this funcitonallity, although that may change later. In either case, this functionality would be useful for ground, but probably not used autonomously, and would not affect mission success if it failed.		No effect.	N/A	4	None					
AV-4.1.2.h			Fails to provide function #8 (connection to umbilical power)		Ground only	For ground-use only. Blocking diodes prevent current back- flow.		No effect.	N/A	4	None					
AV-4.1.2.i			Fails to provide function #9a (fuse monitoring)			For ground use primarily. Not fusing loads, fusing bus. Filter capacitors. Could lose at least one and be ok.	No offort	No effect.	N/A	4	None					
AV-4.1.2.j			Fails to provide function #9b (arming plug monitoring)			I&T ground function to see if arming plugs are in.	No effect.	No effect.	N/A	4	None					
AV-4.1.2.k			Fails to provide function #9c (temperature monitoring)			For informational purposes only.	No effect.	No effect.	N/A	4	None					
Inputs			EPS Power			no power to downstream components	Loss of power to multiple components. Switch sides of Avionics.	No effect.	N/A	4	Active	yes	Loads not powered			
			Umbilical power Separation (from upper stage) indicators			Redundant separation indicators on each PDU.	No effect. Verification of a false separation indication could be performed by switching on the redundant PDU. Four failures would be required before BOTH PDUs indicated separation prematurely.	No effect.	N/A	4	None Passive - Redundancy					
AV-4.1.2.1 AV-4.1.2.1.a	Fuse Module	1) Provides fusing to all loads	Failure to blow (assumes a failure in the load, causing it to draw a high current - six services to unswitched loads (no circuit breaker) which are switched in the ARC.)		E, M, C	Load draws extra current.	ARC limited to a certain number of mA to prevent fuse from blowing. If autonomy can detect load drawing extra current (possible except in the case of a short to chassis), it could switch off the affected load.	No effect.	NA	25 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	high current draw Load current	PDU to REM		
AV-4.1.2.1.b			Blows too soon	1) Design 2) Transient voltage 3) "Smart" short (high current setting that is not detected)	E, M, C	Lose power to a load.	Switch to side B	No effect.	N/A	2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	current telemetry would be zero. Would be indistinguishable from an ARC switch failure. Would probably have ground recommand, but wouldn't fix problem.	PDU to REM		

						Des							Quick Look		I			
FMEA ID Name Function	Failure Mode / Limi	t Response Level		Allocation of Local		Time to Transmit			Time to fix		Ground Response /	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag	Revisit Comments - KAF
	/ Constraint		Response	Response	locally	Signal	Response	System Response	system	Signal	Contingency							
	Fails to provide																	
AV-4.1.2.f	function #6 (power																	X (check for double-
AV TALE!	to unswitched services)																	insulated wires)
	services)																	
	Fails to provide																	
AV-4.1.2.g	function #7 ("common relays")																	
	Fails to provide												<u> </u>					
AV-4.1.2.h	function #8																	
	(connection to umbilical power)																	
														1			Ì	
AV-4.1.2.i	Fails to provide function #9a (fuse																	
	monitoring)																	
			<u> </u>														<u> </u>	
AV-4.1.2.j	Fails to provide function #9b (arming	g																
	plug monitoring)	ь																
	Fails to provide													<u> </u>				
AV-4.1.2.k	function #9c																	
	(temperature monitoring)																	
			System side															
Inputs	EPS Power	Local	switch; return to previous load	Autonomy								X						
			configuration										<u> </u>					
	Umbilical power																	
	Separation (from																	
	upper stage) indicators																	
	indicators																	
AV-4.1.2.1 Fuse Module 1) Provides fusing to all loads									ļ									
AV-4.1.2.1 It disentionale 1) Frovides rusing to an loads																		
			Consider having an over-current rule															
	Failure to blow		for each switched															
	(assumes a failure in the load, causing it	1	load with out a CB												Critical loads are			
	to draw a high		in order to protect the fuse? In some												redundant, so a single			
AV-4.1.2.1.a	current - six services to unswitched loads		cases this might be a complete system	Autonomy											fuse blowing would not cause a critical			х
	(no circuit breaker)		side switch or just												not cause a critical load to fail			
	which are switched		component switch															
	in the ARC.)		for those loads that are cross															
			strapped															
													: 					
			Consider having an															
			over-current rule															
			for each switched load with out a CB															
			in order to protect												Critical loads are			
AV-4.1.2.1.b	Blows too soon	Local	the fuse? In some cases this might be	Autonomy											redundant, so a single fuse blowing would			х
			a complete system												not cause a critical			
			side switch or just component switch												load to fail			
			for those loads															
			that are cross strapped															
			этарреи															
ii					!	<u></u>		.1					1		•			

	_		_				Effect				_			Detection	Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
AV-4.1.2.2	PRIO (2 PRIOs per RC slice, not redundant)	1) Provides main bus voltage telemetry for critical and non-critical loads 2) Provides load current telemetry (total and individual loads and non-critical loads) 3) Provides safety bus voltage monitor 4) Turns on safety bus relays (separate output for each safety bus) 5) controls autonomy relays															
AV-4.1.2.2.a			Hard failure (could take out one or both PRIOs - need both on a side)		L	If hard failure occurs prior to safety bus relay on, couldn't turn on safety bus.	Not able to power safety-inhibited loads.	гом	N/A	1	Passive - Redundancy??	yes	Safety buses wouldn't turn on				
AV-4.1.2.2.b			Hard failure (could take out one or both PRIOs - need both on a side)		E, M, C	Once safety bus is powered, these PRIOs are no longer mission critical. Loss of telemetry.	No telemetry for services affected.	No effect, unless lost telemetry is critical (revisit once telemetry is known)	N/A	4	None	yes	no telemetry from PRIO				
AV-4.1.2.2.c			configuration	1) Radiation 2) Bad command sent to prio and corrupted 3) SW failure	E, M, C	No telemetry, wouldn't respond to commands.	No telemetry for services affected.	No effect, unless lost telemetry is critical (revisit once telemetry is known)	Yes if prop loads (thrusters, cat bed heaters, latch valves) are affected??	4	Active	yes	no telemetry from PRIO	TBD			
AV-4.1.2.2.d			Lock-up/reset	Radiation	Е, М, С	No telemetry, wouldn't respond to commands.	No telemetry for services affected. Could switch to side B.	No effect, unless lost telemetry is critical (revisit once telemetry is known)	Yes if prop loads (thrusters, cat bed heaters, latch valves) are affected??	4	Active	yes	Stale telemetry	TBD			
AV-4.1.3	FET Slice 1	Provides power fusing and switching for all switched and pulsed loads Provides switched status for switched loads Provides current monitoring and circuit breaker function for overcurrent protection.															
AV-4.1.3.a			FET stuck on (normal service)	FET failure		Load stuck powered on.	Power budget hit.	No effect, depending on amount of current draw.	N/A	4	None	yes	load continues to be powered on after power off commanded				
AV-4.1.3.b			FET stuck on (high and low-side FETs)	FET failure			Switch off low-side FET to turn off power to pulsed load.	No effect.	N/A	4	Active		temperature increases coincident to pulsed load. Continued power drain after typical pulse duration.	Load current	PDU to REM		
AV-4.1.3.c			FET stuck off	FET failure		Load stuck powered off.	Switching sides of avionics would not fix problem (FET itself is common to both PDUs).	Loss of load.	N/A	2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active		Load continues to be powered off after power on command.	Load current	PDU to REM		
AV-4.1.3.d				1) Electronics failure 2) Connector/cable failure 3) Common electronics (redundant within FET slice)	Е, М, С	Some or all slice functions fail	Possible loss of power to any or all loads powered through FET slice 1. With redundancy of components and effective placement of loads on FET cards, the loss of a single FET card should not fail the mission.	Possibly degraded mission.	N/A	2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	Loss of power to load(s)	Load current	PDU to REM		
Inputs			Signals on interslice connectors			Redundant wires in interslice connectors, so loss of one would have no effect.	No effect.	No effect.	N/A	4	Passive - redundancy	no?					
		1) Provides over current and at	Primary power from RC Slice			Redundant power wires from RC Slice, so loss of one would have no effect.	No effect.	No effect.	N/A	4	Passive - redundancy	no?					
AV-4.1.3.1	Circuit Breaker	Provides over-current protection to fuse (set to short time period, high current)															

								Re	sponse						Quick Look		İ			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally		t. Desired System Response	Allocation of System	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag Revisit	Comments - KAF
	·		/ Constraint		Response	Response	locally	Sigilal	Response	Response	system	Signal	Contingency							
AV-4.1.2.2	PRIO (2 PRIOs per RC slice, no redundant)	telemetry for critical and non-critical loads 2) Provides load current telemetry (total and individual loads and non-critical loads) 3) Provides Safety bus voltage monitor 4) Turns on safety bus relays (separate output for each safety bus 5) controls autonomy relays																		
AV-4.1.2.2.a			Hard failure (could take out one or both PRIOs - need both on a side)																	
AV-4.1.2.2.b			Hard failure (could take out one or both PRIOs - need both on a side)																×	
AV-4.1.2.2.c			Incorrect PRIO configuration	Local	TBD	Autonomy											1) MOPs sends commands with PRIO reconfiguration scripts 2) MOPs sends command to RF CCD to off-pulse PDU		х	
AV-4.1.2.2.d			Lock-up/reset	Local	TBD	Autonomy											Switch to side B, and/or off-pulse		х	
AV-4.1.3	FET Slice 1	1) Provides power fusing and switching for all switched and pulsed loads 2) Provides switched status for switched loads 3) Provides current monitoring and circuit breaker function for overcurrent protection																		
AV-4.1.3.a			FET stuck on (normal service)																	
AV-4.1.3.b			FET stuck on (high and low-side FETs)	Local	TBD which loads, but monitor for continuous curren for TBD seconds and switch off low side FET; LVs are one known load	Autonomy													х	
AV-4.1.3.c			FET stuck off	Local	TBD which loads, but monitor for one of two always on?	Autonomy													х	
AV-4.1.3.d			Hard failure	Local	TBD which loads, but monitor for one of two always on?	Autonomy											1) MOPs tries to command load(s) on/off 2) Cycle power		x	
Inputs			Signals on interslice connectors																	
			Primary power from RC Slice																	
AV-4.1.3.1	Circuit Breaker	Provides over-current protection to fuse (set to short time period, high current)																		

							Effect							Detection	Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Carradian	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for	Time to Detect	Time to Detect
			/ Constraint							Severity					Diagnosis	(Local)	(System)
AV-4.1.3.1.a			Unable to reset	1) Part Failure		Assuming load has tripped circuit breaker, loss of switched load If load has not tripped circuit breaker, then no effect	Potential loss of a single instrument suite. Cycling power to load may reset circuit breaker. Ground would probably investigate problem at next ground contact.	depending on which		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 1 - if load is non-critical component	Active	yes	Load continues to be powered off after power on command.	Load current	PDU to REM		
										2 '61- 1'- 5151 00							
AV-4.1.3.1.b			Opens without stimuli	1) Part Failure	E, M, C	1) Loss of switched load		Degraded science or loss of redundancy if breaker continually trips for critical switched loads		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 1 - if load is non-critical component	Active	yes	Load switches off unexpectedly	Load current	PDU to REM		
AV-4.1.3.1.c			Trips too soon	1) Trip Value Set Too Low	Е, М, С	1) Load constantly trips circuit breaker	1) Ground command to disable or override the CB	1) None		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 1- if load is non-critical component	None	yes	Load switches off unexpectedly				
AV-4.1.3.1.d			Failure to trip (assumes load is drawing too high of a current)	1) Sense value incorrect (should be caught in testing)		Fuse would blow if current high enough.	Loss of load. Autonomy would turn off load permanently.	Degraded science or loss of redundancy, depending on load.		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 1 - if load is non-critical component	Active	yes	Power drain higher than expected. Load switches off when fuse blows.	Load current	PDU to REM		
Inputs		The Branches for income and House	Power from Fuse Module			Loss of load	Potential loss of entire instrument suite.	Degraded science or loss of redundancy, depending on load.		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 1 - if load is non-critical component	Active	yes	Load not powered.	Load current	PDU to REM		
AV-4.1.3.2	Fuse Module	1) Provides fusing to all loads															
AV-4.1.3.2.a			current	1) Design 2) Transient voltage 3) "Smart" short (high current setting that is not detected - multiple failures)	Е, М, С	Loss of load	Potential loss of entire instrument suite.	Degraded science or loss of redundancy, depending on load.		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 1 - if load is non-critical component	Active	yes	Load not powered.	Load current	PDU to REM		
AV-4.1.3.2.b			Failure to blow (assumes a failure in the load, causing it to draw a high current)	1) Design		Loss of load	Anything other than a short to chassis, autonomy would see and turn off load. Also will have circuit breakers for non-redundant loads like instruments and some other critical loads.	Degraded science or loss of redundancy, depending on load.		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 1 - if load is non-critical component	Active	yes	Not short to chassis: excess current draw by load. Short to chassis: difficult to diagnose. Eventually would load shed and side switch. Would probably see problem when switching loads back on one-byone.	Load current	PDU to REM		
AV-4.1.3.3	PRIO (8 loads per PRIO, but each FET has an A-side and a B-side, so two PRIOs control each load)	Provides load current telemetry for individual loads Provides switched status for switched loads Provides current monitoring and circuit breaker function for over- current protection															
AV-4.1.3.3.a		carent potection		1) Electronics failure 2) Connector/cable failure 3) SW failure	Е, М, С	Unable to control switched loads controlled by failed PRIO	No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.		4	Active ?	yes	Load not responding to commands.	Load current; power state vs commanded state	PDU to REM		

							Dog						1	Quick Look					
FMEA ID	Name Function	Failure Mode / Limit	t Response Level	Desired Local	Allocation of Local		Time to Transmit	Desired System		Time to fix	Time to Transmit	Ground Response /	System Side Switch		Safe Mode	Remediation	Helpful Autonomy Rule	Flag Revisit	Comments - KAF
		/ Constraint		Response	Response	locally	Signal	Response	System Response	system	Signal	Contingency							
AV-4.1.3.1.a		Unable to reset	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy				r copora							1) Send commands to turn load on 2) Send commands to turn load on and override CB 3) Cycle power		x	
AV-4.1.3.1.b		Opens without stimuli	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy											1) If CB continually trips, can override CB and rely solely on autonomy rule for over-current protection		x	
AV-4.1.3.1.c		Trips too soon														1) Turn load on 2) If CB continually trips, can override CB and rely solely on autonomy rule		х	
AV-4.1.3.1.d		Failure to trip (assumes load is drawing too high of a current)	Local	Consider having an over-current rule for each switched load with CB in order to protect the fuse?	Autonomy											1) Autonomy rules also protect against over-current 2) LVS protection if both CB and autonomy rule fail		x	
Inputs		Power from Fuse Module	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy													x	
AV-4.1.3.2 AV-4.1.3.2.a	Fuse Module 1) Provides fusing to all loads	Blows below rated current	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy											1) Circuit breakers are used to prevent fuses from blowing 2) Critical loads have redundant power paths, so a single fuse blowing would not cause a critical load to fail		x	
AV-4.1.3.2.b		Failure to blow (assumes a failure in the load, causing it to draw a high current)		Consider having an over-current rule for each switched load with CB in order to protect the fuse?	Autonomy											1) Circuit breakers are used to prevent fuses from blowing 2) Critical loads have redundant power paths, so a single fuse blowing would not cause a critical load to fail		x	
AV-4.1.3.3	PRIO (8 loads per PRIO, but each FET has an A-side and a B-side, so two PRIOs control each load) 1) Provides load current telemetry for individual loads 2) Provides switched status for switched loads 3) Provides current monitoring and circuit breaker function for overcurrent protection																		
AV-4.1.3.3.a		Hard failure	Local	TBD - if load stuck on when commanded off, consider rule for system side switch?	Autonomy											MOPs sends commands with PRIO reconfiguration scripts		х	

						Effect			,	_		•	Detection			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
AV-4.1.3.3.b				1) Radiation 2) Bad command sent to prio and corrupted 3) SW failure	Any number of registers incorrectly configured	No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.		4	Active ?	yes	Load not responding to commands as expected. Autonomy should have a check in place to ensure that a pulse command isn't turned into a switch (prop LVs, etc.).	Load current; power state vs commanded state	PDU to REM		
AV-4.1.3.3.c			Lock-up/reset	Radiation E, M, C	No telemetry, wouldn't respond to commands. Connected loads turned off.	No telemetry for services affected. No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.	es if prop loads (thrusters, latch alves) are affected.	4	Active ?	yes	Stale telemetry. (Cat bed heater telemetry should be visible still - ensure current drawn is consistent with expected number of heaters in operation)	Load current; power state vs commanded state	PDU to REM		
Inputs			i2c bus - clock		No telemetry. Can't command loads.	No telemetry for services affected. No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.	ses if prop loads uthrusters, latch alves) are affected.	4	Active ?	yes	Stale telemetry. (Cat bed heater telemetry should be visible still ensure current drawn is consistent with expected number of heaters in operation)	Load current; power state vs commanded state	PDU to REM		
			i2c bus - serial data		No telemetry. Can't command loads.	No telemetry for services affected. No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.	es if prop loads (thrusters, latch salves) are affected.	4	Active ?	yes	Stale telemetry. (Cat bed heater telemetry should be visible still - ensure current drawn is consistent with expected number of heaters in operation)	Load current; power state vs commanded state	PDU to REM		
			12c bus - reset line		No telemetry, wouldn't respond to commands. Connected loads turned off.	No telemetry for services affected. No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.	es if prop loads thrusters, latch salves) are affected.	4	Active ?	yes	Stale telemetry. (Cat bed heater telemetry should be visible still - ensure current drawn is consistent with expected number of heaters in operation)	Load current; power state vs commanded state	PDU to REM		
			i2c bus - +5V		Unable to control switched loads controlled by failed PRIO	No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.		4	Active ?	yes	Load not responding to commands.	Load current; power state vs commanded state	PDU to REM		
			i2c bus - ground		Unable to control switched loads controlled by failed PRIO	No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.		4	Active ?	yes	Load not responding to commands.	Load current; power state vs commanded state	PDU to REM		
AV-4.14	FET Slice 2		12c bus - PRIO clock		No telemetry, wouldn't respond to commands. Connected loads turned off.	No telemetry for services affected. No side switch required in most cases due to cross-strapping of loads. For PSE or IMU, would need to switch sides of avionics either autonomously or through ground command.	No effect.	ces if prop loads (thrusters, latch salves) are affected.	4	Active ?	yes	Stale telemetry. (Cat bed heater telemetry should be visible still - ensure current drawn is consistent with expected number of heaters in operation)	Load current; power state vs commanded state	PDU to REM		

AV-4.1.3.3c Lock-up/reset Lock-up/reset Lock	utonomy Rule Flag	ag Revisit	Comments - KAF
AV-4.1.3.3.c Local incorrect PBO to disjust on when configuration local incorrect PBO to disjust on when commanded off, consider talk for when commanded off, consider talk for when commanded off, consider talk for when commanded off, consider talk for when commanded off, consider talk for when con		x	
AV-4.1.3.3.c lock-up/reset lock-up/reset lock lock-up/reset lock lock-up/reset lock lock-up/reset lock lock-up/reset lock-up/res		x	
AV-4.1.3.3.c Lock-up/reset Local comanded off, consider rule for system side switch? TBD - if load stuck on when com wh			
on when		х	
Inputs 12c bus - clock Local commanded off, consider rule for system side switch? Autonomy Commanded off, consider rule for system side switch? Autonomy Commanded off, consider rule for system side switch? Autonomy Commanded off, consider rule for system side switch?		х	
TBD - If load stuck on when commanded off, consider rule for system side switch? Autonomy Consider rule for system side switch?		х	
TBD - if load stuck on when commanded off, consider rule for system side switch? Autonomy		x	
I2c bus - +5V Local TBD - if load stuck on when commanded off, consider rule for system side switch? Autonomy System side switch?		х	
IZC bus - ground Local TBD - if load stuck on when commanded off, consider rule for system side switch? Autonomy		х	
IZC bus - PRIO clock Local TBD - if load stuck on when commanded off, consider rule for system side switch? AV-4.1.4 FET Slice 2		x	

-	_		_				Effect				_			Detection	vietnoa		
FMEA ID	Name	Function	Failure Mode / Limit	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation		Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for	Time to Detect	Time to Detect
			/ Constraint							Severity					Diagnosis	(Local)	(System)
AV-4.1.5	FET Slice 3																
AV-4.2	Side B																
AV-4.2.1	CMD TLM B																
AV-4.2.2	Relay Cap B																
AV-4.2.3	FET Slice 4																
AV-4.2.4	FET Slice 5																
AV-4.2.5	FET Slice 6																
												• • • • • • • • • • • • • • • • • • • •					

								Res	ponse						Quick Look			4.			
FMEA ID	Name	Function	Failure Mode / Limit	Response Level	Desired Local	Allocation of Local	Time to fix	Time to Transmit	Desired System	Allocation of	Time to fix	Time to Transmit	Ground Response /	System Side Switch	Processor Switch	Safe Mode	Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
			/ Constraint		Response	Response	locally	Signal	Response	System	system	Signal	Contingency								<u> </u>
										Response											:
AV-4.1.5	FET Slice 3																				:
AV-4.2	Side B																				
AV-4.2.1	CMD TLM B																				
AV-4.2.2	Relay Cap B																				
AV-4.2.3	FET Slice 4																				
AV-4.2.4	FET Slice 5				į									-						į	;
AV-4.2.5	FET Slice 6																				

Subject Matter Expert(s): Lew Roufberg

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and

Expert(s):		listed for comp	eleteness, but failure mode and			r#a-	•		İ				Detection M	a dha d		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection M TIm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
EP-1.1	Power System Electronics PSE-1 Bus Junction Slice															
EP-1.1.1.a	oos succion sice		Loss of telemetry (load current)	open circuit resistor short circuit	1) Scale of telemetry would change 2) Telemetry would read 0 Amps.	Would probably attempt an avionics side switch, but would not correct problem since resistors are used by both sides.	1) Long-term trending might reveal a way to adjust for change in scale No other effect. 2) Could verify that load current equals expected value by summing buck converter current, load current, and battery current (should equal 0). No other effect.		4	None	yes	Either 0 or out-of- scale reading in telemetry	?	PSE to CDH	n/a	N/A
EP-1.1.1.b			Loss of telemetry (battery current)		1) Scale of telemetry would change 2) Telemetry would read 0 Amps.	Would probably attempt an avionics side switch, but would not correct problem since resistors are used by both sides.	1) Long-term trending might reveal a way to adjust for change in scale No other effect. 2) Could verify that battery current equals expected value by summing buck converter current, load current, and battery current (should equal 0). No other effect.	N/a	4	None	yes	Either 0 or out-of- scale reading in telemetry	?	PSE to CDH	n/a	N/A
EP-1.1.1.c			Loss of telemetry (battery voltage)	1) open circuit resistor 2) short circuit	Lost bus voltage telemetry to controller	Controller would incorrectly cause Buck converters to limit current to bring voltage down. Autonomy would detect mismatch between battery and bus voltages and PDU would switch sides of PSE.	discharge if no side	N/a	4	Active	yes	See difference between battery voltage and bus voltage.	Battery and Bus Voltages	PSE to CDH to Autonomy	?	None
Inputs			Buck converter power		No effect to card.	S/c would receive 1/4 of the expected power, but system should have sufficient margin.	No effect		4	None	Yes	Reduced power to bus	Buck Converter Current	PSE to CDH	?	None
			Relay command (only changes when a fault occurs and it needs to change state)	Relay command when not necessary (no other fault)	Slice would tell one Buck Converter to go offline	S/C can handle loss of a single buck converter. No effect.	No effect	N/a	4	None	Yes	Could see Buck converter is offline.	Buck Converter Current	PSE to CDH	?	None
				No command when necessary (2nd failure)	No effect to card.	Buck converter would draw too much power. Battery would discharge.	Loss of mission		2	None	Yes.	With current sensors on buck converter slice	Buck Converter Current	PSE to CDH	?	None
EP-1.1.2	Solar Array Junction Board 1															
EP-1.1.2.a			Short (isolation diodes)	1) diode fails short	No effect without another short	No effect	No effect	N/a	4	None	No		None	None	None	None
EP-1.1.2.b			Open (isolation diodes)	1) diode fails open	lose power from a single solar array string	No effect (designed to work with loss of single string). Might need to extend wing further	No effect	N/a	4	None	Depends on the string (outboard 2 strings have current sensors)	Telemetry	SA current	SAJB to PSE to CDH	None	None
EP-1.1.2.c			Loss of telemetry (current)	1) open circuit resistor 2) short circuit	1) Scale of telemetry would change 2) Telemetry would read 0 Amps.	Would probably attempt an avionics side switch, but would not correct problem since resistors are used by both sides.	1) Long-term trending might reveal a way to adjust for change in scale No other effect. 2) Could verify that current equals expected value by summing buck converter current, load current, and battery current (should equal 0). No other effect.		4	None	yes	Either 0 or out-of- scale reading in telemetry			n/a	N/A
EP-1.1.2.d			Loss of telemetry (voltage)	1) open circuit resistor 2) short circuit	Stop sensing solar array voltag	Could cause buck converter to either over or under-current. Autonomy would see solar array current mis-match and would direct PDU to switch to other side of PSE.	No effect with side switch.	N/a	4	Active	Yes	Solar array current would not match expected	SA current, Buck converter current?	PSE to CDH	?	?

Subject Matter Lew Roufberg Expert(s):

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and

expert(s):		listed for comp	oleteness, but failure mode and							-								
FMEA ID	Name	Function	Failure Mode / Limit /	Response Level	Desired Local	Allocation of	Time to fix	Time to Transmit Signal	Time to Transmit Signal	Response Desired System Response	Allocation of System	Time to fix system	Time to Transmit Signal	Ground Response /	System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation
	· · · · · · · · · · · · · · · · · · ·		Constraint	nesponse zere.	Response	Local Response	locally	Time to Transmit orginal	Time to Transmit oignar	Desired System Response	Response	Time to the system		Contingency	System side surren	. rocessor ourieum	oute mode	nemealation
EP-1	Power System Electronics	<u> </u>																
EP-1.1 EP-1.1.1	PSE-1 Bus Junction Slice						<u> </u>											
EP-1.1.1	Bus Junction Since				-													
														Long to my tronding to				
								~1 sec (action depends on						Long-term trending to identify way to adjust for				
EP-1.1.1.a			Loss of telemetry (load current) Local	Contingnecy	Ground	?	persistence decided on by	?	None	None	None	None	change in scale; work-				Possibility of reprogramming something
					Procedure			fault protection)						around for verifying load				
														current				
														Long-term trending to				
			Loss of telemetry (battery		Contingnecy			~1 sec (action depends on						identify way to adjust for				
EP-1.1.1.b			current)	Local	Procedure	Ground	?	persistence decided on by	?	None	None	None	None	change in scale; work-				Possibility of reprogramming something
								fault protection)						around for verifying load current				
														Content				
							ļ		ļ									
EP-1.1.1.c			Loss of telemetry (battery	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	None				Side switch
			voltage)			, ,												
														If margin isn't sufficient,				
la se de			D. d	None	Name	Constant	_			Ness	Ness	Name	Mana	power cycle non-critical				
Inputs			Buck converter power	None	None	Ground	ľ	f	ľ	None	None	None	None	loads to reduce power				
														needed by system				
			Relay command (only changes											Ground contingency to				
			when a fault occurs and it	None	None	Ground	?	?	?	None	None	None	None	bring buck converters back				Wait until next ground contact, send
			needs to change state)											online (power cycle all?)				command to reset relay.
					-													
				None	None	Ground	?	?	?	None	None	None	None	None - loss of mission, but double fault				
		Ļ		Ļ			ļ							uouble lault				
EP-1.1.2	Solar Array Junction Board 1																	
					-													
EP-1.1.2.a			Short (isolation diodes)	None	None	None	None	None	None	None	None	None	None	None				
					-		i											
EP-1.1.2.b			Open (isolation diodes)	None	None	None	None	None	None	None	None	None	None	None				
								V1 con /ontion depends on						Long-term trending to identify way to adjust for				
EP-1.1.2.c			Loss of telemetry (current)	Local	Contingnecy	Ground	?	~1 sec (action depends on persistence decided on by	2	None	None	None	None	change in scale; work-				Possibility of reprogramming something
2. 1.1.2.0			2000 or telemetry (current)	2000	Procedure	Cround	ľ	fault protection)					Tone	around for verifying load				. ossibility of reprogramming sometiming
														current				
				***************************************	1		<u> </u>											
ED 1 4 2 -			loss of tolomote: (:-lt)	Local	DCE aldott-1	Autonor	2	2	2	None	None	None	None					
EP-1.1.2.d			Loss of telemetry (voltage)	Local	PSE side switch	Autonomy	'	•	ľ	None	None	None	None	·				
		<u> </u>					<u> </u>		.									

Subject Matter Expert(s): Lew Roufberg

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Revisit
EP-1	Power System Electronics			
EP-1.1	PSE-1	(· · · · · · · · · · · · · · · · · · ·
EP-1.1.1	Bus Junction Slice		Loss of telemetry (load current)	X (only one slice, can't "switch sides")
EP-1.1.1.b			Loss of telemetry (battery current)	X (only one slice, can't "switch sides")
EP-1.1.1.c			Loss of telemetry (battery voltage)	X (only one slice, can't "switch sides")
Inputs			Buck converter power	х
		:	Relay command (only changes when a fault occurs and it needs to change state)	
				х
EP-1.1.2	Solar Array Junction Board 1			
EP-1.1.2.a			Short (isolation diodes)	X (only one slice, can't "switch sides")
EP-1.1.2.b			Open (isolation diodes)	X (only one slice, can't "switch sides")
EP-1.1.2.c			Loss of telemetry (current)	X (only one slice, can't "switch sides")
EP-1.1.2.d			Loss of telemetry (voltage)	X (only one slice, can't "switch sides")

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)		

EPS - 30 of 317

March Marc	_			_			Effe	ot						Detection M	ethod		
Part Part	FMEA ID	Name	Function		Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity		Observable	How Observed?	Tlm for Diagnosis			
Second S				00.13.11.11											2.05.100.0	(2000.)	(Oyotem)
Management Man			***************************************														
Part Part	Inputs			Solar array power		Slice is ok.	S/c not receiving power.	Loss of mission.	N/a	2	None	Yes		Battery voltage	PSE to CDH	?	?
Concess Conc																	
Column C																	
Part Part	LF-1.1.4	Duck Converter Since 1 of 4				Converter slice will be off	No effect. Can lose a single				·			Ruck converter			
In the content of the	EP-1.1.4.a			No output	1) Open circuit output fuse			No effect.	N/a	4	None	Yes	Telemetry	1	PSE to CDH	?	?
Fig. 1. The control of the control o						Current will be too high or too	Controller will compensate for							Dueli servicator			<u></u>
Pill 1.4. See a second to reduce the control of the	EP-1.1.4.b			Incorrect current	1) reference voltage drift			No effect.	N/a	4	Passive	Yes	Telemetry		PSE to CDH	?	?
Partial de la caracte law lating from out propries de caracter production de la caracter product					<u> </u>	limited internally.	converter.				- 						
PALLS IN PRODUCT CARRIED STREETING PRODUCT CARRIED STREETING STREE							Potential EMC/EMI issue for										
State of the protection of the control of the contr	EP-1.1.4.c			Incorrect switching frequency			instruments; switch sides to	Worst case, lose data for one encounter	N/a	3	None	Not directly	wouldn't necessarily		?	?	?
Could clause book converter to great with the part of the count of the							clear problem										
and there could not control and from carbon or an under-carbon. The course again from carbon or any													. 52				
Implicit and a control agreed from controller government of the control and process of the control and																	
Service of contents of the con	Innuts						Autonomy would see solar		N/a	4	Active	Ves		SA current, Buck	PSE to CDH	2	2
In the second power state of PEL Pol 1	inputs			card		power or not enough		switch.	1470	-	Active	163		converter current?	TSE to CDIT	ľ	[
Solar array gover from ADD 1/100 year for a power of powe																	
Solar array power from SUN [1] Fitsy mode but converted and place of expression special will be a single but converted and power special place of converted and power from SUN [2] NUN failure and power special place of the power special p								No effect Is Is has									
Part Part				Calan announce from CAID	1) relay inside buck converter	No office the soul	Buck converter stops relaying		N/-			v	Battery discharging	Buck Converter	DSE to CDII		
P12.13 DOUT/MA IP 12.14 P12.15 DOUT/MA IP 12.15 DOUT/MA Hard failure Hard failure Adonomy would see his of telemetry or growth mixth telemetry or growth mixth telemetry or growth mixth telemetry or growth mixth telemetry or growth mixth telemetry or growth mixth telemetry or growth mixth telemetry or growth mixth to which to whole in constant policy or growth mixth to whole the original way to problem but it would be impossible to tell mental or problem but it would be impossible to tell mental or problem but it would be impossible to tell mental or problem but it would be impossible to tell mental or problem but it would be impossible to tell mental or problem but it would be impossible to tell mental or problem but it would be impossible to tell mental or problem but it would be impossible to tell mental or problem but mixture and the rot tell mental o				Solar array power from SAJB	2) SAJB failure	No effect to card	power		N/a	4	None	res	unexpectedly	Current	PSE TO CDH	f	None
P-1.2.1.a VolVilla A. Level failure Level grath Political fa								single buck converter)									
EP-1.2.1.a Part failure II power supply input opens in feed path 2 Fee																	
EP-1.2.1.a Hard failure																	
EP-1.2.1.a language l																	
EP-1.2.1.a land land land land land land land lan							telemetry and would comman	t									
EP-1.2.1.a Hard failure feed path output. Task, in telemetry output. PSE to LOH to a feed path output. The problem, problem, problem, put it would be impossible to tell the difference between this failure mode and the "no telemetry output "failure mode." Post output the problem,					1) power supply input opens in												
EP-1.2.1.b No telemetry output Discourage Discourag	EP-1.2.1.a			Hard failure				No effect.	N/A	2R	Active	Yes	Loss of telemetry			?	None
EP-1.2.1.b No telemetry output anomaliter not powered 2) open circuit September 1.5 September 2. September 2. September 3.					2) FPGA fails	output.								neartbeat	Autonomy		
EP-1.2.1.b No telemetry output 1) output transmitter not powered 2) open circuit Card would continue operating but no telemetry output. Voide B. EP-1.2.1.c Locks up/resets 1) SEU Card would continue operating Reset card. If necessary, switch to side B. N/a 4 Active yes Loss of telemetry PSE CMD/TLM heartheat Autonomy 7 None necessary. Switch no effect. N/A 4 Active yes Loss of telemetry Description PSE CMD/TLM PSE to CDH to neartheat PSE CMD/TLM PSE to CDH to reset, no telemetry output or reset.																	
EP-1.2.1.b No telemetry output in No telemetry output in No telemetry output in No telemetry output in No effect. No telemetry output in No telemetry output in No effect. N							mode and the "no telemetry										
EP-1.2.1.b No telemetry output powered 2) open circuit powered 2) open circuit powered 2) open circuit powered 2) open circuit powered but no telemetry output. To side B. Card requires a commanded reset, no telemetry output or reset.							output" failure mode.										
EP-1.2.1.b No telemetry output powered 2) open circuit powered 2) open circuit powered 2) open circuit powered 2) open circuit powered but no telemetry output. To side B. Card requires a commanded reset, no telemetry output or reset.																	
EP-1.2.1.b No telemetry output powered 2) open circuit powered 2) open circuit powered 2) open circuit powered 2) open circuit powered but no telemetry output. To side B. Card requires a commanded reset, no telemetry output or reset.																	
EP-1.2.1.b No telemetry output powered 2) open circuit powered 2) open circuit powered 2) open circuit powered 2) open circuit powered but no telemetry output. It is side B. Card requires a commanded reset, no telemetry output or reset.					1) output transmitter not												
EP-1.2.1.c Locks up/resets 1) SEU Card requires a commanded reset card. If necessary, switch no effect. N/A 4 Active yes Loss of telemetry PSE CMD/TLM PSE to CDH to Parther Autonomy 7 None	EP-1.2.1.b			No telemetry output	powered	Card would continue operating	Reset card. If necessary, switc	n No effect.	N/a	4	Active	yes	Loss of telemetry			?	None
EP-1.2.1.c Locks up/resets 1) SEU reset, no telemetry output or Reset and If necessary, switch No effect. N/A 4 Active yes Loss of telemetry PSE to Company					2) open circuit	but no telemetry output.	to side b.							neartbeat	Autonomy		
EP-1.2.1.c Locks up/resets 1) SEU reset, no telemetry output or Reset Card. If necessary, switch No effect. N/A 4 Active yes Loss of telemetry PSE to Compan																	
EP-1.2.1.c Locks up/resets 1) SEU reset, no telemetry output or Reset Card. If necessary, switch No effect. N/A 4 Active yes Loss of telemetry PSE to Compan											<u> </u>						
EP-1.2.1.c Locks up/resets 1) SEU reset, no telemetry output or Reset and If necessary, switch No effect. N/A 4 Active yes Loss of telemetry PSE to Company																	
EP-1.2.1.c Locks up/resets 1) SEU reset, no telemetry output or Reset Card. If necessary, switch No effect. N/A 4 Active yes Loss of telemetry PSE to Compan																	
EP-1.2.1.c Locks up/resets 1) SEU reset, no telemetry output or Reset Card. If necessary, switch No effect. N/A 4 Active yes Loss of telemetry PSE to Compan						Card requires a commanded	December of 16							DCE CMD /7:11	DOE to CDIII		
nung telemetry.	EP-1.2.1.c			Locks up/resets	1) SEU	reset, no telemetry output or	keset card. If necessary, switc to side B.	No effect.	N/A	4	Active	yes	Loss of telemetry			?	None
						nung telemetry.									•		
											<u> </u>						ļ
EP-1.2.1.d Loss of ability to command (or open circuit in path) Loss of telemetry Loss of telemetry Loss of telemetry Cocide R. N/A 4 Active yes Loss of telemetry Loss of tel							Reset card. If necessary switc	n						PSF CMD/TLM	PSE to CDH to		
EP-1.2.1.d Loss of ability to command (or open circuit in path) Loss of telemetry (or open circuit in path) Lo	EP-1.2.1.d			Loss of ability to command		Loss of telemetry	to side B.	No effect.	N/A	4	Active	yes	Loss of telemetry		:	?	None
14) IT ON Talls					L) II GA Idiis												
							; ; ;					į					<u> </u>

									Response						Quick Look		
FMEA ID Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local	Allocation of Local Response	Time to fix	Time to Transmit Signal	Time to Transmit Signal	Desired System Response	Allocation of System	Time to fix system	Time to Transmit Signal		System Side Switch	Processor Switch	Safe Mode	Remediation
		Constraint		Response	Local Response	locally				Response			Contingency				
						i		Ö									Solar arrays would extend to increase
Inputs		Solar array power	None	None	None	None	None	None	None	None	None	None	None				voltage
EP-1.1.3 Solar Array Junction Slice 2																	
EP-1.1.4 Buck Converter Slice 1 of 4																	Can lose any 1 buck converter
EP-1.1.4.a		No output	None	None	None	None	~1 sec	None	None	None	None	None	None				
				Limit current on													
EP-1.1.4.b		Incorrect current	Local	buck converter	HW	?	~1 sec	None	None	None	None	None	None				
													Trending of EMC/EMI in				Diamondo de Maria de Carlos de Carlo
EP-1.1.4.c		Incorrect switching frequency	Local	PSE side switch	Ground	?	?	?	None	None	None	None	instruments; ground would need to isolate where issue				Diagnose by turning each converter off individually to see if it fixes problem.
													is coming from, PSE side switch to clear problem				Leave off the bad one.
						<u> </u>							Smerred cical production				
Inputs		Control signal from controller card	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				Cycle power to controller card
		caru															
													If margin isn't sufficient, power cycle non-critical				
		Solar array power from SAJB	None	None	Ground	?	?	?	None	None	None	None	loads to reduce power				
50.4.0													needed by system				
EP-1.2 PSE-2 EP-1.2.1 CMD/TLM A																	
													Do we want tiered				
													autonomy response where we power cycle first and				
EP-1.2.1.a		Hard failure	Local	PSE reset	Autonomy	?	~1 sec	?	None	None	None	None	the PSE side switch?				
				PSE side switch	,								Or we can just side switch				
													and allow the ground to try to power cycle to "fix"				
													problem				
													Do we want tiered autonomy response where				
				205									we power cycle first and				
EP-1.2.1.b		No telemetry output	Local	PSE reset	Autonomy	?	~1 sec	?	None	None	None	None	the PSE side switch?				Reset card
				PSE side switch									Or we can just side switch and allow the ground to try	,			
													to power cycle to "fix"				
													problem				
													Do we want tiered autonomy response where				
				DCE wood+									we power cycle first and				
EP-1.2.1.c		Locks up/resets	Local	PSE reset	Autonomy	?	~1 sec	?	None	None	None	None	the PSE side switch?				Reset card
				PSE side switch									Or we can just side switch and allow the ground to try	,			
													to power cycle to "fix"				
													problem				
													Do we want tiered autonomy response where				
				DCE roast									we power cycle first and				
EP-1.2.1.d		Loss of ability to command	Local	PSE reset	Autonomy	?	~1 sec	?	None	None	None	None	the PSE side switch?				Reset card
				PSE side switch									Or we can just side switch and allow the ground to try	,			
													to power cycle to "fix"				
]			<u> </u>		<u>.</u>	<u>.</u>	<u> </u>					problem				

Inputs Solar array power EP-1.1.3 Solar Array Junction Slice 2 EP-1.1.4. EP-1.1.4.a Buck Converter Slice 1 of 4 EP-1.1.4.b Incorrect current Control signal from controller card Solar array power from SAJB EP-1.2 EP-1.2.1 CMD/TLM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output	FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Revisit
EP-1.1.3 Solar Array Junction Slice 2 EP-1.1.4 Bruck Converter Slice 1 of 4 EP-1.1.4.a No output EP-1.1.4.b Incorrect current EP-1.1.4.c Incorrect switching frequency Control signal from controller card Solar array power from SAJB EP-1.2 PSE-2 EP-1.2.1 CMD/TLM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output				Solar array power	
EP-1.14.a Buck Converter Slice 1 of 4 EP-1.14.b No output EP-1.14.c Incorrect current Inputs Control signal from controller card Solar array power from SAJB EP-1.2 PSE-2 EP-1.2.1 CMD/TLM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output	EP-1.1.3	Solar Array Junction Slice 2			<u> </u>
EP-1.1.4.b Incorrect current EP-1.1.4.c Incorrect switching frequency Inputs Control signal from controller card Solar array power from SAIB EP-1.2.1 CMD/TLM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output	EP-1.1.4	Buck Converter Slice 1 of 4	<u></u>		
EP-1.1.4.c Incorrect current EP-1.1.4.c Incorrect switching frequency Inputs Control signal from controller card Solar array power from SAJB EP-1.2.1 CMD/TLM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output					
Inputs Control signal from controller card Solar array power from SAJB EP-1.2 PSE-2 EP-1.2.1. CMD/TLM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output	EP-1.1.4.b			Incorrect current	
EP-1.2 PSE-2 EP-1.2.1 CMD/TIM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output	EP-1.1.4.c			Incorrect switching frequency	
EP-1.2.1 CMD/TLM A EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output	Inputs				
EP-1.2.1.a PSE-2 EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output					
EP-1.2.1.a Hard failure EP-1.2.1.b No telemetry output	EP-1.2	PSE-2			
	EP-1.2.1.a			Hard failure	
EP-1.2.1.c Locks up/resets	EP-1.2.1.b			No telemetry output	
	EP-1.2.1.c			Locks up/resets	
EP-1.2.1.d Loss of ability to command	EP-1.2.1.d			Loss of ability to command	

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

EPS - 33 of 317

Page Page	Detect Time to (Syste
Hands Interest to the property of the control of th	
AND CONTIAN AS IN SECURIOUS PROPERTY OF PROPERTY AND PROPERTY OF PROPERTY AND PROPERTY OF PROPERTY AND PROPER	None
And the service of the control of th	None
AND COMPAND AND AND COMPAND AND AND COMPAND AND AND COMPAND AND AND COMPAND AND AND COMPAN	None
AND CONTRACT MATERIAL PROCESSION AND SHORT MATERIAL PROCESSION AND	None
Part of the property of the pr	None
Figure 1 of the control of the contr	
FALS Controller A. Page Fatherer will be former under voltage offit property and states of the court of the	
P-1.2.1 Controller A. P-1.2.2.a Controller A. P-1.2.2.a In an in a failure 1] Power input could be conserved in the provided personal failure of personal failure	
Service A Committed A Committed A Committed A Committed Invest. Active Total Failure Committed I	
P-1.2.1 Controller A. P-1.2.2.a Controller A. P-1.2.2.a In an in a failure 1] Power input could be conserved in the provided personal failure of personal failure	
P-1.2.1 Controller A. P-1.2.2.a Controller A. P-1.2.2.a In an in a failure 1] Power input could be conserved in the provided personal failure of personal failure	
EP.1.2.2 Controller A Flare finiture I Power input could be perfect elementary from hos junction graph from SAU board Fig. 1.2.2 board in correct output I Segretary from hos junction graph from SAU board I Temestry from hos junction graph from SAU board I	
FP.1.2.2 Controller A Pland failure 1] Power input could be experiment will change but the signal output to block converters will stay at last commanded level. Attempt to registerments will change but the signal output to block converters will stay at last converters. Pl.1.2.2.b Incorrect output 1] Reference voltage drift 2] Still affects a register value 1] Reference voltage drift 2] Still affects a register value 2] Still	1
P-1.2.1 Controller A P-1.2.2 Controller A P-1.2.3 Controller A P-1.2.3 Controller A P-1.2.3 In a failure In a failure In Power input could be operated in large from the provided converters. In a failure In power input could be operated in large from the provided converters. In a failure In power input could be operated in large from the provided converters. In a failure In power input could be operated in large from the provided converters. In a failure In power input could be operated in large from the provided converters. In a failure In power input could be operated in large from the provided converter to under-obligate and would fail the power or under shapeing the battery of the provided converter to under-obligate and would fail the power or under-obligate and would	None
P-1.2.2.a land failure land land land land land land land land	
P-1.2.2.a large failure large failure large from the period of the period of the period power will not mark to period for power will change, but have the period power will not mark to period power will not mark to provide of power will not mark to provide power to power will not mark to provide power to power to power will not mark to provide power to power t	
P-1.2.2.a large failure large failure large from the period of the period of the period power will not mark to period for power will change, but have the period power will not mark to period power will not mark to provide of power will not mark to provide power to power will not mark to provide power to power to power will not mark to provide power to power t	
P-1.2.2.a large failure large failure large failure large for each failure large for under each failure large for	
2-1.2.2.a land failure 1) Power input could be open/short power will not mark to depending on exact failure. Prest statics. Eventually load requirements. Will change, but provided pr	
P-1.2.2.a lard failure oper/short 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 2) FGA fails register value 3) FGA fails register value 3) FGA fails register value 4. Active 4 FGA fails register value 4. Active 5 FGA telemetry recover under-thanging the battery over-turned residence from the span of the control	
Hard failure open/short 2) FPGA fails open/sho	
P-1.2.2.b Incorrect output 1) Reference voltage drift 2) SEU affects a register value See over/under charge in charging the battery of with sides of Avionics. No effect. N/A 4 Active Ves See battery over-current or under-current Sacurrent, Buck converter output 1) Reference voltage drift 2) SEU affects a register value Signal from card would be incorrect. Signal from card would be incorrect. N/A 4 Active Ves See battery See battery See to EDH 7 7 7 7 7 7 7 7 7	?
FP.1.2.2.b Incorrect output 1) Reference voltage dirft 2) SEU affects a register value 2 Signal from card would be incorrect. Signal from card would be incorrect. Signal from card would be incorrect. Lose FPGA telemetry (depending on exact failure). No effect. No ef	
P-1.2.2.b Incorrect output 1) Reference voltage drift 2) SEU affects a register value 2) SEU affects a register value 2) SEU affects a register value 3) Reference voltage drift 2) SEU affects a register value 3) See over/under charge in telemetry and reset slice. Autonomy will direct PDU to switch to side B 3. See battery over/under charge in telemetry and reset slice. Autonomy will direct PDU to switch to side B 3. See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry. Set to CDH 4. Active 3) See battery over/under charge in telemetry and sever the switch is side. Set to CDH 5. Active 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/under charge in telemetry and switch 3) See battery over/u	
P-1.2.2.b Incorrect output 1) Reference voltage drift 2) SEU affects a register value 1. Will either be over- or under-charging the battery charging the bat	
P-1.2.1.b Incorrect output 2) SEU affects a register value Charging the battery Autonomy will direct PDU to switch to side B Could cause buck converter to switch to side B Could cause buck converter to either over or under-current. Autonomy would see battery board Felemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board Felemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board Felemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board Felemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board Felemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ board Felemetry from bus for over-current interface, or signal from SAJ boar	
switch to side B Telemetry from bus junction slice and/or Cmd/Tim interface, or signal from SAI board LVPS LVPS Telemetry from bus junction slice and/or Cmd/Tim interface, or signal from SAI board LVPS Telemetry from bus junction slice and/or Cmd/Tim interface, or signal from SAI board LVPS LVPS Telemetry from bus junction slice and/or Cmd/Tim interface, or signal from SAI board LVPS LVPS Telemetry from bus junction slice and/or Cmd/Tim interface, or signal from SAI board LVPS LVPS LVPS Telemetry indicates 0 buck converter will go to 0 output. Attempt to reset slice. Autonomy will see 0 output from buck converters and direct PDU to switch to side B. addieved PDU	?
Felemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board LVPS Felemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board Signal from card would be incorrect. Signal from card would be incorrect. Signal from card would be incorrect. Autonomy would see battery over-current or under-voltage and would direct PDU to switch to other side of PSE. Buck converters will go to 0 output. Attempt to reset slice. No signal output to buck from buck converters and direct PDU to switch to side B. Na Active ves battery over-current back or under-voltage or under-voltage or under-voltage and would direct PDU to switch. SA current, Buck converter current? Autonomy will see of PSE to CDH to output. Attempt to reset slice. No effect. No signal from card would be interface, or signal from SAJ board or under-voltage and would direct PDU to switch to side B. No effect with side switch. No e	
Telemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board Lose FPGA telemetry (depending on exact failure). No signal output to busk converters and direct PDU to switch to side B. Lose FPGA telemetry (depending on exact failure). No signal output to busk converters and direct PDU to switch to side B. Lose FPGA telemetry (depending on exact failure). No signal output to busk converters and direct PDU to switch to side B.	
interface, or signal from SAJ board interface, or signal from SAJ board interface, or signal from SAJ board incorrect. over-current or under-voltage and would direct PDU to switch to other side of PSE. LVPS LVPS LVPS LVPS LVPS LVPS interface, or signal from SAJ board incorrect. over-current or under-voltage and would direct PDU to switch. to other side of PSE. Buck converters will go to 0 output. Attempt to reset slice. Autonomy will see 0 output from buck converters and direct PDU to switch to side B. No effect. No effect. N/A 4 Active ves or under-voltage converter or under-voltage and would great pour pour pour pour pour pour pour pour	
incorrect. over-current or under-voltage and would direct PDU to switch to other side of PSE. LVPS L	2
LVPS LVPS LVPS LVPS LVPS LVPS LVPS LVPS LVPS LVPS LOSE FPGA telemetry (depending on exact failure). No signal output to buck from buck converters and converters. Autonomy will see 0 output from buck converters and direct PDU to switch to side B. No effect.	
LVPS Buck converters will go to 0 output. Attempt to reset slice. (depending on exact failure). No signal output to buck converters and converters. No effect.	
LVPS LVPS LVPS LOSE FPGA telemetry (depending on exact failure). No signal output to buck from buck converters and converters. LOSE FPGA telemetry output. Attempt to reset slice. Autonomy will see 0 output from buck converters and converters and converters. No effect. No effe	
LVPS (depending on exact failure). No signal output to buck from buck converters and converters. direct PDU to switch to side B.	
No signal output to buck from buck converters and converters. No signal output to buck from buck converters and converters. direct PDU to switch to side B.	
converters. direct PDU to switch to side B.	?
Battery will discharge.	
P-123 IUFSA	
No telemetry; Autonomy	
would see no power to LVPS or	
P-1.2.3.a No output Open circuit FET Loss of power to controller and no telemetry or incorrect No effect. N/A 2R Active Yes Loss of telemetry VPS current or PSE to CDH to ?	?
command/telemetry voltage someplace and would direct PDU to switch to command/telemetry direct PDU to switch to co	
redundant side	
Telemetry indicates Reference voltage circuit Drift in voltage, erratic Drift in voltage, erratic Drift in voltage, erratic Drift in voltage, erratic	
P-1.2.3.b Incorrect output fereince voltage circuit point in voltage, erratic profit in voltage, errat	?
telemetry voltage?	
No telemetry; Autonomy	
would see no power to LVPS or Loss of power to controller and no telemetry or incorrect LVPS current or LVPS c	
Puputs Bus voltage from PDU command/telemetry voltage someplace and would some place and would command/telemetry voltage someplace and would some place and	2
direct PDU to switch to	ľ
redundant side redundant side	,
P-1.24 CMD/TLM B	ŕ
P-1.2.5 Controller B P-1.2.6 LVPS B	
P-1.Z.b iLVPS B P-2 Li-lon Battery	
20 parallel strings of 8 cells	
P-2.1 Cell 1 of n each, could lose any 1 string of a cells cells.	

															Quick Look		·
FMEA ID Name	Function	Failure Mode / Limit /	Response Level	Desired Local	Allocation of	Time to fix	Time to Transmit Signal	Time to Transmit Signal	Response Desired System Response	Allocation of System	Time to fix system	Time to Transmit Signal	Ground Response /	System Side Switch	Processor Switch	Safe Mode	Remediation
		Constraint		Response	Local Response	locally				Response			Contingency				
				ļ			·					·	·				
													Do we want tiered				
													autonomy response where we power cycle first and				
				PSE reset									the PSE side switch?				
Inputs		LVPS	Local		Autonomy	?	~1 sec	?	None	None	None	None					
				PSE side switch									Or we can just side switch and allow the ground to try	,			
													to power cycle to "fix"				
													problem				
													Do we want tiered				
													autonomy response where				
				DCE rocot									we power cycle first and the PSE side switch?				
		REM commands	Local	PSE reset	Autonomy	?	~1 sec	?	None	None	None	None	the PSE side Switch?				Reset card
				PSE side switch									Or we can just side switch				
													and allow the ground to try to power cycle to "fix"	1			
													problem				
EP-1.2.2 Controller A																	
							·										
				Reset Controller	\												
				slice?					Load shed / system side								Might combine some functions with
EP-1.2.2.a		Hard failure	Local / System	(Not sure how to	Autonomy	?	?	?	switch	Autonomy / HW?	?	?	?	X		x	CMD/TLM slice
				compare power v	S v												
				load requirement)												
EP-1.2.2.b		Incorrect output	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				
		Telemetry from bus junction															
Inputs		slice and/or Cmd/Tlm	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				CMD/TLM slice reset
pacs		interface, or signal from SAJ	2000.	i de side switeri	raconomy	•											on b, rem since resec
		board															
	-																
		<u> </u>															Might combine some functions with
		LVPS	Local	PSE side switch	Autonomy	?	,	<i>?</i>	None	None	None	None	?				CMD/TLM slice
50 4 2 2 UVDC 4																	
EP-1.2.3 LVPS A																	
FD 1330		No outout	Local	DCF aidait-d	Autonom	2	2		None	None	None	None	2				
EP-1.2.3.a		No output	Local	PSE side switch	Autonomy	r	r	r	None	None	None	None	f				
EP-1.2.3.b		Incorrect output	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				
			-		-												
Inputs		Rus voltage from DDII	Local	PSE side switch	Autonomy	2	7	2	None	None	None	None	2				
Inputs		Bus voltage from PDU	LUCAI	r at Side SWILLI	Autonomy	•	•	•	Notice	Note	None	None	<u>'</u>				
ED 1.2.4 CAAD/TIM D			ļ		ļ												
EP-1.2.4 CMD/TLM B EP-1.2.5 Controller B																	
EP-1.2.6 LVPS B																	
EP-2 Li-Ion Battery		30															
EP-2.1 Cell 1 of n		20 parallel strings of 8 cells each, could lose any 1 string of	F														
2. 2.1		cells.															
		<u> </u>				i	.i	ł					.t		il		

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Revisit
Inputs			LVPS	
			REM commands	
EP-1.2.2	Controller A			
EP-1.2.2.a			Hard failure	
EP-1.2.2.b			Incorrect output	
Inputs			Telemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board	
			LVPS	
EP-1.2.3	LVPS A	¢		
EP-1.2.3.a			No output	
EP-1.2.3.b			Incorrect output	
Inputs			Bus voltage from PDU	
EP-1.2.4	CMD/TLM B			
EP-1.2.5	CMD/TLM B Controller B LVPS B			
EP-1.2.6	LVPS B			
EP-2	Li-Ion Battery	<u> </u> 	20 parallal strings of 9 colls	
EP-2.1	Cell 1 of n		20 parallel strings of 8 cells each, could lose any 1 string of cells.	

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

EPS - 36 of 317

	·	=	:			Effec							Detection Me			
FMEA ID	Name Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
														_		
EP-2.1.a		Short	Separator short circuit		Slight reduction in battery capacity, temporary hot spot	Slight reduction in battery storage capacity	No effect.	N/A	4	None		Long-term battery trending	Battery voltage	PSE to CDH	?	?
EP-2.1.b		Open	Open interconnect			Slight reduction in battery storage capacity	No effect.	N/A	4	None		Long-term battery trending	Battery voltage	PSE to CDH	?	?
EP-2.1.c		High Impedance	Excessive degradation			Slight reduction in battery storage capacity	No effect.	N/A	4	None		Long-term battery trending	Battery voltage	PSE to CDH	?	?
Inputs		Current from bus junction slice			Battery would discharge and	Bus voltage would decrease	No effect	N/A	4	None		Battery current	Battery current and	PSE to CDH	?	?
EP-3	Color Associa				voltage would decrease					ļ		telemetry	voltage?			
	Solar Arrays Solar Array 1									ļ	<u>. </u>					
EP-3.1.1	Primary Array			ļ						ļ						
EP-3.1.1.1 EP-3.1.1.1.a	Strings	Short to ground	Insulator breakdown			Reduction in power margin; system is designed to accommodate this	No effect.	N/A	4	None	Yes	Telemetry will indicate lower output current	SA current	PSE to CDH	?	?
EP-3.1.1.1.b		Open	Cracked cell or open interconnect		Reduction in S/A output current	Reduction in power margin; system is designed to accommodate this	No effect.	N/A	4	None	Yes	Telemetry will indicate lower output current	SA current	PSE to CDH	?	?
:	Cells (with bypass diodes)			<u> </u>							Not likely; loss of					
EP-3.1.1.1.1.a		Short	Shorted diode	ļ	Small loss in power	Negliglble effect	No effect.	N/A	4	None	power is too small	N/A	None	None	None	None
EP-3.1.1.1.1.b		Open	Cracked cell		Bypass diode will conduct, leading to small loss in power	Negliglble effect	No effect.	N/A	4	None	Not likely; loss of power is too small	N/A	None	None	None	None
	Secondary Array			ļ						ļ						
EP-3.1.2.1 EP-3.1.2.1.a	Strings	Short to ground	Insulator breakdown		Reduction in S/A output current	First, reduction in power margin; then, extend wings farther to compensate if close to sun; system is designed to accommodate this. Could cause EMI effects by connecting current loop (no remediation).	No effect.	N/A	4	None	Yes	First, telemetry will indicate lower output current; then, lower S/A flap angle to compensate if close to sun	SA current	PSE to CDH	?	?
EP-3.1.2.1.b		Open	Cracked cell or open Interconnect		Reduction in S/A output current	First, reduction in power margin; then, extend wings farther to compensate if close to sun; system is designed to accommodate this	No effect.	N/A	4	None	Yes	First, telemetry will indicate lower output current; then, lower S/A flap angle to compensate if close to sun	SA current	PSE to CDH	?	?
	Cells (with bypass diodes)			ļ						ļ	Not likoly, less of					
EP-3.1.2.1.1.a		Short	Shorted diode	<u> </u>	Small loss in power	Negliglble effect	No effect.	N/A	4	None	Not likely; loss of power is too small	N/A	None	None	None	None

									Response						Quick Look		
FMEA ID Name	Function	Failure Mode / Limit /	Response Level			Time to fix	Time to Transmit Signal	Time to Transmit Signal	Desired System Response		Time to fix system	Time to Transmit Signal		System Side Switch	Processor Switch	Safe Mode	Remediation
		Constraint		Response	Local Response	locally				Response			Contingency				
EP-2.1.a		Short	None	None	None	?	Noticible with long-term (weeks) of battery trending	?	None	None	Nne	None	Ground performs long- term trending on battery; no response since this is not fixable Would any power cycling need to be done to conserve powering during				
													certain parts of orbit? Ground performs long-				
EP-2.1.b		Open	None	None	None	?	Noticible with long-term (weeks) of battery trending	?	None	None	Nne	None	term trending on battery; no response since this is not fixable Would any power cycling need to be done to conserve powering during certain parts of orbit?				
EP-2.1.c		High Impedance	None	None	None	}	Noticible with long-term (weeks) of battery trending	?	None	None	Nne	None	Ground performs long- term trending on battery; no response since this is not fixable Would any power cycling need to be done to conserve powering during certain parts of orbit?				
																	Depends on root cause; switching PSE
Inputs		Current from bus junction slice	e None	None	None	?		?	None	None	Nne	None					sides should resolve an issue internal to the EPS
EP-3 Solar Arrays																	
EP-3.1 Solar Array 1 EP-3.1.1 Primary Array	<u> </u>				i	<u> </u>											
EP-3.1.1.1 Strings																	
EP-3.1.1.1.a		Short to ground	None	None	None	?	If far from sun, could see reduction in current as fast as 1 sec; if close to sun, may have to wait until primary S/A receives sufficient illumination	?	None	None	Nne	None	Ground performs trending on SA power generation; no response since this is not fixable?	3			
EP-3.1.1.1.b EP-3.1.1.1.1 Cells (with bypass diodes)		Open	None	None	None	?	If far from sun, could see reduction in current as fast as 1 sec; if close to sun, may have to wait until primary S/A receives sufficient illumination	?	None	None	Nne	None	Ground performs trending on SA power generation; no response since this is not fixable?	3			
EP-3.1.1.1.1 (Cens (With Dypass Glodes)		Short	None	None	None	None	None	None	None	None	None	None	None				
EP-3.1.1.1.1.b EP-3.1.2 Secondary Array		Open	None	None	None	None	None	None	None	None	None	None	None				
EP-3.1.2.1 Strings						<u> </u>											
EP-3.1.2.1.a		Short to ground	None	None	None	?	1 sec to see reduction in S/A current; then, several minutes to see S/A flap angle decrease to compensate if close to sun.	?	None	None	Nne	None	Ground performs trending on SA power generation; no response since this is not fixable?				Type of insulation means this is very unlikely.
		0	Nana		None	?	2 sec to see reduction in S/A current; then, several minutes to see S/A flap	?	None	None	Nne	None	Ground performs trending on SA power generation; no response since this is	3			
EP-3.1.2.1.b		Open	None	None	None		angle decrease to compensate if close to sun.						not fixable?				
EP-3.1.2.1.1 Cells (with bypass diodes) EP-3.1.2.1.1 a		Short	None	None	None	None		None	None	None	None	None					

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Revisit
EP-2:1.a			Short	
EP-2.1.b			Open	
EP-2.1.c			High Impedance	
nputs			Current from bus junction slice	
P-3	Solar Arrays			
P-3.1	Solar Array 1			
EP-3.1.1 EP-3.1.1.1	Primary Array Strings			
EP-3.1.1.1.a	Strings		Short to ground	
EP-3.1.1.1.b			Open	
r-3.1.1.1.1	Cells (with bypass diodes)			
EP-3.1.1.1.1.a			Short	
EP-3.1.1.1.b	Secondary Array		Open	
P-3.1.2.1	Strings			
EP-3.1.2.1.a			Short to ground	
EP-3.1.2.1.b EP-3.1.2.1.1			Open	
	di			
EP-3.1.2.1.1.a			Short	

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

EPS - 39 of 317

							Effec	t						Detection N	ethod		
FMEA ID	Name	Function	Failure Mode / Limit /	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for	Time to Detect	
			Constraint								FM				Diagnosis	(Local)	(System)
EP-3.1.2.1.1.b			Open	Cracked cell		Bypass diode will conduct, leading to small loss in power; may be local hot spot	Negliglble effect	No effect.	N/A	4	None	Not likely; loss of power is too small	N/A	None	None	None	None
EP-3.1.2.2	Sensor Cell (8)																
EP-3.1.2.2.a			No output	Cracked cell or broken wire			Use redundant sensor cell (no side switching is required)	No effect.	N/A	4	Active	Yes	Telemetry	Sensor Cell Tlm	PSE to CDH to Autonomy	?	None
EP-3.1.2.2.b			Incorrect output	Cracked cell Excessive darkening (should affect all cells equally)		telemetry for one sensor cell (used for fault protection and calibration). Would likely only decrease output, not trip safing	autonomy parameters based	No effect.	N/A	4	Active	Yes	Telemetry	Sensor Cell Tlm	PSE to CDH to Autonomy	3	None
EP-3.1.2.2.c			Debond failure			Solar array temperature would increase		Question concerning number of sensors required, talking to Danielle.	N/A	4							
Inputs	Solar illumination		Reduction in illumination			Reduction in S/A output current	Battery will discharge. May need to change parameters (caught on ground by trending analysis). Could mean arrays are out further (impacts to time required to safe arrays)	No effect	N/A	4	Active	Yes	S/A current telemetry	SA current	PSE to CDH to Autonomy	?	?
EP-3.2	Solar Array 2			·													
EP-3.2.1 EP-3.2.1.1	Primary Array										ļ						
	Strings Cells			ļ							ļ						
EP-3.2.2	Secondary Array										1						
EP-3.2.2.1	Strings																
EP-3.2.2.1.1	Cells						lovalid stale or mission				ļ						
EP-4	Connect Relays						Invalid, stale, or missing battery telemetry would require controller switch.	None	N/A	4							
EP-5	Heaters										1						

										-								-
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Time to Transmit Signal	Response Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation
EP-3.1.2.1.1.b			Open	 None	None	None	None	None	None	None	None	None	None	None				
EP-3.1.2.2	Sensor Cell (8)																	
EP-3.1.2.2.a			No output	Local	Use redundant measurements only	Autonomy	?	~1 sec	?	None	None	Nne	None	None				
EP-3.1.2.2.b			Incorrect output	Local	Use redundant measurements only	Autonomy	?	~1 sec	?	None	None	Nne	None	None				
EP-3.1.2.2.c			Debond failure															
Inputs	Solar illumination		Reduction in illumination	System	None	None	None	?	?	Load shed, system side switch (LBSOC)	Autonomy / HW?	?	?	?	x	x	v	Depends on root cause; likely requires action to hardware beyond EPS (e.g., avionics processor to correct S/A pointing error)
EP-3.2.1 EP-3.2.1.1	Solar Array 2 Primary Array Strings																	
EP-3.2.2 EP-3.2.2.1	Cells Secondary Array Strings Cells																	
EP-4	Connect Relays																	
EP-5	Heaters			Ì			<u> </u>											

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Revisit
EP-3.1.2.1.1.b			Open	
EP-3.1.2.2	Sensor Cell (8)			
EP-3.1.2.2.a			No output	
EP-3.1.2.2.b			Incorrect output	
EP-3.1.2.2.c			Debond failure	
Inputs	Solar illumination		Reduction in illumination	
EP-3.2	Solar Array 2			
EP-3.2 EP-3.2.1	Primary Array			
FP-3.2.1.1	Strings			
	Cells			
EP-3.2.1.1.1				
EP-3.2.2	Secondary Array			
EP-3.2.2.1	Strings			
EP-3.2.2.1.1	Cells	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
EP-4	Connect Relays			х
EP-5	Heaters			Х

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

EPS - 42 of 317

Subject Matter Kenny Newsome Expert(s):

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FMEA information is only displayed in the first copy of the component.

ECU-1 ECU ECU-1.1 ECU Side A ECU-1.1.1 Control and S		Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
ECU-1.1 ECU Side A											:		Diagnosis		
			i	į											(System)
ECO-1.1.1 Control and 3	Status Sido A														
ECU-1.1.1.a	30033000		Circuitry Failure - FPGA, ASIC, etc	Complete Loss of Control and Status ability on ECU Side	switch to redundant ECU side	Switch to Redundant Side ECU Impact to Fault: Management: If Side A fails, we will no longer be able to handle position mis-match faults in same manner - where redundant side potentiometers are used as "third vote"	no effect	2R	Active	yes	Loss of Status Telemetry	ECU Aliveness	ECU to REM	?	?
ECU-1.1.1.b		Inability to execute control commands	1) Command UART Failure (receiver) 2) Command UART Fault (receiver) 3) Harness Fault	Unable to execute any ECU Control Commands: 1) Fails to step motor actuator when commanded (Flap, Feather, HGA) 2) Fails to return status telemetry 3) Fails to cancel step in progress when commanded 4) Fails to set cumulative step count (re-initialize) when	Autonomy should command switch to redundant ECU side and should set flag indicating ECU Fault/Failure.		Cause temporary loss of ECU side functionality for TBD seconds	2R	Active	yes	1) Observe commands not executed 2) Loss of Status Telemetry (Send Telemetry command not executed)	telemetry ; ECU step count telemetry; redundant ECU	ECU to REM	?	?
ECU-1.1.1.c		Inability to send status telemetry	1) Telemetry UART Failure (driver) 2) Telemetry UART Fault (driver) 3) Harness Fault	Unable to transmit any ECU status telemetry	Autonomy should command switch to redundant ECU side and should set flag indicating ECU Fault/Failure.	no effect	no effect	2R - if ECU is non recoverable 4 - if ECU can recover	Active	yes	Loss of Status Telemetry	ECU Aliveness	ECU to REM	?	?
ECU-1.1.1.d		Hung (repeating a command)		actuation.	Autonomy recognizes that actuator continues beyond expected value and switches sides of ECU.		If not caught quickly enough during encounter.	2R - if ECU is non recoverable 4 - if ECU can recover	Active	yes	Motion of actuator continues beyond expected value	Potentiometer telemetry; ECU step count telemetry; redundant ECU telemetry	ECU to REM	?	?
ECU-1.1.1.e		Hung/Locked up state (not commanding)	SEU	Command/Telemetry hung and unresponsive	Autonomy should command switch to redundant ECU side and should set flag indicating ECU Fault.	no effect	Cause temporary loss of ECU side functionality for TBD seconds	2R - if ECU is non recoverable 4 - if ECU can recover	Active	yes	2) Loss of Status	telemetry ; ECU step count telemetry; redundant ECU	ECU to REM	2	?

Subject Matter Expert(s): Kenny Newsome Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FMEA information is only displayed in the first copy of the component.

Marcin M			information is only displayed	in the first copy of the component.						Response						Quick Look			
No. No.	FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local	Allocation of Local	Time to fix			Allocation of System	Time to fix system	Time to Transmit	Ground Response /	System Side Switch		Safe Mode	Remediation	Revisit
		(¢						ļ				ç		, ,,				
							ļ	· •				ļ			ļ				
2014.1	ECU-1.1.1	CONTROL BIRD STREETS SIDE A		·	<u> </u>		ļ	· •	 			·			ļ		ļ	·	·
Column C																			
State Stat																			
Registration of the control of the c																			
Part Part																			
Part Part																			
Harmonic Registration of the control						otherwise system side													
Residual Residual	FCII 4 4 4 -			Used Salves	Laral			2	2	Mana	Name	Name	Nama	Ness				Control to an douglant ECU std.	
Californ Californ	ECU-1.1.1.a			Hard Fallure	Local		Autonomy	ľ	f	None	None	None	None	None				Switch to redundant ECO side	
Californ Californ						Mould this same													
Result R																			
Record R																			
Maria																			
Part Part								·				ļ			ļ				
Harding and the second																			
Hall have been been been been been been been be																			
Hard I all the second of the s																			
Col.																		Switch to redundant ECLI side (nower cycle will	
Author A	ECU-1.1.1.b			Inability to execute control commands	Local		Autonomy	?	?	None	None	None	None	None					
INCULLE CONTROL TO THE PROPERTY OF THE PROPERY OF THE PROPERTY OF THE PROPERTY OF THE PROPERTY OF THE PROPERTY						is correct power off	,												
CU-11.2																			
Figure from the control of the contr																			
FOLILIE FOLILIE FOR COLUMN TO SERVICE STAND ST																			
FOLILIE FOLILIE FOR COLUMN TO SERVICE STAND ST								<u> </u>	<u> </u>			<u> </u>	<u></u>		ļ				<u> </u>
EQUILITE Intelligence of the content of the conten						If potentiometer and													
ECULILE RECULLILE Recording Country and database believed by the recording a columns with the recording and columns with t																			
FEU 1.1.1.2 Parallel						mismatched, turn on													
Figure 1.1.1. Figure 1.1. Figu																			
SCUILLE FULL LIVE FU																			
Activities and the properties at the state televiery and the state televiery a																			
Autocomy 2 would be a work or several status telemetry and status teleme																		Switch to redundant ECU side (power cycle will	
Hunglicked up state (not commanding) Model this area by sould this area by sould this area by sould this not be sould this not be sould this not be sould this not be sould this not be sould this not be sould be involved to state (not command)	ECU-1.1.1.c			Inability to send status telemetry	Local	SWITCHTTT	Autonomy	?	?	None	None	None	None	None				clear fault). Next step would be avionics side	Х
resultant of the control of the cont																		switch.	
FCU-1.1.d In the properties of the control of the c																			
ECU-1.1.d Hung/Locked up state (not commanding) Full Plancy (repeating a command) Fu																			
Identify was alked an alwerses rule an alwerses rule an alwerses rule and alwerses r																			
Multiple freeding a command) ECU-1.1.1.d Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Hung (repeating a command) Local Hung (repeating a command) Local Hung (repeating a command) Hung (repeating a command) Local Hung (repeating a command) Hung (repeating																			
Hung (repeating a command) Local If potentiometer and step count are minimatched, furn on redundant ECU for primary ECU otherwise system side or minimatched, furn on minimatch						Might need an													
ECU-1.1.1.d Hung (repeating a command) Local step count are insmatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side sets (FU-1.1.1.e) FU-1.1.1.e Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local step count are insmatched, turn on redundant ECU side or switch sides of a vote; if third vote is correct power off primary ECU otherwise system side sets (FU-1.1.1.e) FU-1.1.1.e Hung/Locked up state (not commanding) Local step count are insmatched, turn on redundant ECU side (power cycle will a vote is correct power off primary ECU otherwise system side is correct power off						aliveness rule		<u>.</u>	<u> </u>			<u> </u>	<u></u>						<u> </u>
ECU-1.1.1.d land land land land land land land lan						If potentiometer and													
ECU-1.1.d Hung (repeating a command) Local striction of strict to the redundant ECU of strict your of primary ECU otherwise system side security (Part of primary ECU otherwi																			
Hung (repeating a command) Local and vote; if third vote is correct power off primary ECU otherwise system side is corre						mismatched, turn on													
FOUR LILE IN THE PRINCE CONTROL IN THE PRINCE CONTROL IN THE PRINCE IN T	FCIL1 1 1 d			Hung (repeating a command)	Local		Autonomy	2	2	None	None	None	None	None				Switch to redundant ECU side or switch sides of	v
ECU-1.1.e EU-1.1.e Fundable Local Primary EU otherwise system side is correct power off primary ECU otherwise system side	LCU-1.1.1.U			nang (repeating a collilliditu)	Local		Autonomy	ľ	ľ	IVOITE	IVOITE	IVOITE	HOHE	IVOITE					^
ECU-1.1.1e FEU-1.1.1e FEU-1.1.1e FEU-1.1.1e FEU-1.1.1e FINAL ART AND ART						primary ECU													
ECU-1.1.1.e Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Hung/Locked up state (not co																			
ECU-1.1.e Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Local Switch to redundant ECU side (power cycle will redundant ECU side (power cycle will sic correct power off primary ECU otherwise system side) Local Autonomy 7 7 None None None None None None None Non						switch???			ļ			<u> </u>							<u> </u>
ECU-1.1.e Hung/Locked up state (not commanding) Local Hung/Locked up state (not commanding) Local Switch to redundant ECU side (power cycle will redundant ECU side (power cycle will sic correct power off primary ECU otherwise system side) Local Autonomy 7 7 None None None None None None None Non						If potentiometer and													
Hung/Locked up state (not commanding) Hung/Locked up state (not commanding) Local redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side Redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side						step count are													
ECU-1.1.e Hung/Locked up state (not commanding) Local 3rd vote; If third vote is correct power off primary ECU otherwise system side 4utonomy 7 7 None No																			
is correct power off primary ECU otherwise system side	FCII-1 1 1 a			Hung/Locked up state (not commanding)	Local		Autonomy	2	?	None	None	None	None	None					y
primary ECU otherwise system side	LCO 1.1.1.C				Local		. atonomy				one	one						clear fault)	^
						primary ECU													
SWICD (**)																			
						switch???	<u> </u>		<u> </u>		<u> </u>	<u> </u>	<u></u>						

FMEA ID	Name	Function Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Effect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Tlm for Diagnosis	Tlm Path for	Time to Detect (Local)	
Inputs		REM generated commands for control and status - cross-strapped (REM A and REM B)		Complete Loss of Control and Status ability on ECU Side	switch to redundant ECU side	Switch to Redundant Side ECU Impact to Fault Management: If Side A fails, we will no longer be able to handle position mis-match faults in same manner - where redundant side potentiometers are used as "third vote"	no effect	4	Active	yes	Loss of Status Telemetry	Potentiometer telemetry ; ECU step count telemetry; redundant ECU telemetry ECU Aliveness	Diagnosis ECU to REM	77	(System)
		Bus Voltage - ECU Side A Power		Complete Loss of Control and Status ability on ECU Side	switch to redundant ECU side	Switch to Redundant Side ECU impact to Fault Management: If Side A fails, we will no longer be able to handle position mis-match faults in same manner - where redundant side potentiometers are used as "third vote"	no effect	4	Active	yes	Loss of Status Telemetry	Potentiometer telemetry; ECU step count telemetry; redundant ECU telemetry ECU Aliveness	ECU to REM		,
ECU-1.1.2 ECU-1.1.2.a	Power Side A	No Power	Open Circuit	Complete Loss of power to ECI Side	Autonomy should notice no Jopwer to ECU side, as well as lack of status telemetry and command switch to redundant ECU side.	Switch to Redundant Side ECU Impact to Fault Management: If Side A fails, we will no longer be able to handle position mis-match faults in same manner - where redundant side potentiometers are used as "third vote"	no effect	2R	Active	yes	Loss of Status Telemetry	ECU Aliveness; EC U Power State	ECU to REM PDU to REM	77	,
ECU-1.1.2.b		Incorrect Power Regulation	Voltage Regulation Failure	Unstable/Unpredictable operation.	Autonomy should notice incorrect power to ECU side and command switch to redundant ECU side.	Switch to Redundant Side ECU Impact to Fault Management: If Side A fails, we will no longer be able to handle position mis-match faults in same manner - where redundant side potentiometers are used as "third vote"	no effect	2R	Active	yes	1) Telemetry should indicate incorrect voltage 2) Loss of Status Telemetry?	ECU current / voltage	PDU to REM	?	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local	Allocation of Local	Time to fix	Time to Transmit	esponse						Quick Look		_	
			•				locally	Signal			Time to fix system	Time to Transmit Signal		System Side Switch	Processor Side	Safe Mode	Remediation	Revisit
					Response	Response	locally	Signai	Response	Response		Signai	Contingency					
					If potentiometer and step count are													
					mismatched, turn on redundant ECU for													
					3rd vote; If third vote													
					is correct power off primary ECU													
					otherwise system side													
Inputs			REM generated commands for control and status - cross-strapped (REM A and REM B)	Local	switch???	Autonomy	?	?	None	None	None	None	None				Switch to redundant ECU side	
			status - cross-strappeu (Keivi A anu Keivi B)															
					Would this same premise work or													
					would this not be													
					evaluated if ECU telemetry was stale?													
					Might need an													
					aliveness rule													
					If potentiometer and													
					step count are mismatched, turn on													
					redundant ECU for													
					3rd vote; If third vote is correct power off													
					primary ECU												Switch to redundant ECU side. PDU switch could allow a single FET to power ECU, but that ECU would	ld
					otherwise system side switch???												only work from then on with that PDU.	J.
			Bus Voltage - ECU Side A Power	Local	SWITCHTTT	Autonomy	?	?	None	None	None	None	None				Potentiometers would match each other (and actual location value), but step count would match what	
					Would this same												had been commanded (with commands that didn't	
					premise work or												get through).	
					would this not be													
					evaluated if ECU telemetry was stale?													
					Might need an aliveness rule													
ECU-1.1.2 Pow	wor Sido A				anveness rule													
			6		If potentiometer and	i						6 !			6			
					step count are													
					mismatched, turn on redundant ECU for													
					3rd vote; If third vote													
					is correct power off primary ECU													
					otherwise system side													
ECU-1.1.2.a			No Power	Local	switch???	Autonomy	?	?	None	None	None	None	None				Switch to redundant ECU side	
					Would this same premise work or													
					would this not be													
					evaluated if ECU telemetry was stale?													
					Might need an													
					aliveness rule													
					If potentiometer and													
					step count are mismatched, turn on													
					redundant ECU for													
					3rd vote; If third vote is correct power off													
					primary ECU													
					otherwise system side switch???													
ECU-1.1.2.b			Incorrect Power Regulation	Local		Autonomy	?	?	None	None	None	None	None				Switch to redundant ECU side	
					Would this same													
					premise work or													
					would this not be evaluated if ECU													
					telemetry was stale?													
	į				Might need an aliveness rule													
	•																	

FMIA ID Name Function Failure Mode / Limit / Constraint Possible Causes Phase Local Next Higher Mission Umbra Violation Severity Type of FM Observable Now Observable Now Observable Now Observable Now Observable Now Observable Now Observable Now Observable Now Observable Now Observable Observable (System) **Switch to Redundant 55de ECU Imputs** **Description of Failure Mode / Limit / Constraint Possible Causes Phase Local Next Higher Mission Umbra Violation Severity Type of FM Observable Now Obs									Effect						Detection	Method		
Inputs Bus Voltage - ECU Side A Power Bus Voltage - ECU Side A Power Bus Voltage - ECU Side A Power Bus Voltage - ECU Side A Power Bus Voltage - ECU Side A Power Complete Loss of Control and Status ability on ECU Side status telemetry) and command switch to redundant ECU side switch). Autonomy should notice problem (ex. lack of status telemetry) and command switch to redundant ECU side switch). Bus Voltage - ECU Side A Power Bus Voltage - ECU Side A Power Bus Voltage - ECU Side A Power Complete Loss of Control and Status ability on ECU Side status telemetry and command switch to redundant ECU side switch). Bus Voltage - ECU Side A Power Complete Loss of Control and Status ability on ECU Side status telemetry and command switch to redundant ECU side switch). Bus Voltage - ECU Side A Power Complete Loss of Control and Status ability on ECU Side status telemetry and command switch to redundant ECU side switch). Bus Voltage - ECU Side A Power Complete Loss of Control and Status ability on ECU Side status telemetry and command switch to redundant ECU side switch). Bus Voltage - ECU Side A Power Complete Loss of Control and Status ability on ECU Side switch or serious telemetry and command switch to redundant ECU side switch). Complete Loss of Status and selection mismatch faults in came manner—where redundant ECU side switch). Complete Loss of Status and selection mismatch faults in came manner—where redundant ECU side switch). Complete Loss of Status and selection mismatch faults in came manner—where redundant ECU side switch). Complete Loss of Status and selection mismatch faults in came manner—where redundant ECU side switch). Complete Loss of Status and selection mismatch faults in came manner—where redundant ECU side switch). Complete Loss of Status and selection mismatch faults in came manner—where redundant Side of the complete Loss of Status and selection mismatch faults in came manner—where redundant Side of the complete Loss of Status and selection mismatch faults in came manner—wh	FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes Ph	hase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis		Time to Detect (Local)	
		CLEAR		Bus Voltage - ECU Side A Power			Complete Loss of Control and Status ability on ECU Side	Autonomy should notice problem (ex. lack of status telemetry) and command switch to redundant ECU side (does not require avionics side	Impact to Fault Management: If Side A fails, we will no longer be able to handle position mis-match faults in same manner - where redundant side potentiometers are used as "third		4	Active	yes	Loss of Status	? ECU Power State		?	?
£CU-1.2.1 ;CONTOLAND STATUS SIDE B			<u> </u>								ļ	-						
ECU-1.2.2 Power Side B							ļ		-	ķ	ļ							

								F	Response						Quick Look			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local	Allocation of Local	Time to fix	Time to Transmit	Desired System	- Allocation of System	Time to fix system	Time to Transmit	Ground Response /	System Side Switch	Processor Side	Safe Mode	Remediation	Revisit
					Response	Response	locally	Signal	Response	Response		Signal	Contingency					
Inputs			Bus Voltage - ECU Side A Power	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch??? Would this same premise work or would this not be evaluated if ECU telemetry was stale? Might need an aliveness rule	Autonomy	?	,	None	None	None	None	None				Switch to redundant ECU side. PDU switch could allow a single FET to power ECU, but that ECU would only work from then on with that PDU. Potentiometers would match each other (and actual location value), but step count would match what had been commanded (with commands that didn't get through).	
ECU-1.2 ECU Si				ļ	ļ	i 			i \$		ļ							i \$
	ol and Status Side B										ļ							į
ECU-1.2.2 Power	r Side B	. <u></u>			<u>i</u>	İ		.	<u>;</u>		<u> </u>						<u>i</u>	İ

bject Matter
Robin Vaughan
Robin Vaughan
Robin Vaughan
Robin Vaughan

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	TIm for Diagnosis	TIm Path for Diagnosis	Time to Detec	t Time to De (System
4	Star Trackers Star Tracker A														<u> </u>	-	ļ
111a			correctly process these commands, it can fail to reach the pormal	1) Faulty connector or harness/wiring inside unit 2) localized electronics fault that affects command processing logic; localized electronics fault that prevents configuration change inside unit 3) Error in tracker processor internal software/firmware	as	Tracker does not reach normal operating mode, either degraded attitude solutions are generated or no attitude solutions are generated.	attitude solution saved from previous processor on shut down if processor reset or	could be deemed unusable for the rest of the mission. May not meet WISPR attitude knowledge accuracy requirements around perihelia with only one tracker. Still meet full mission science requirements.	Unlikely that a localized change in attitude large enough to cause are enough to cause are enough to cause are enough to the enough to cause the tracker. A slowly drifting attitude solution might be harder to detect and could sentually result in an unbraviolation if undetected. Smilarly, propagation using entity and enough	3		Probably	If tracker is able to output telementy, it should indicate the control of the con			Probably 10-20 seconds to decide that a problem is awarants taking action	
C-1.1.b			Injust message not received or processed. (The trackers typically insed some information from the avioricat/FSW to generate correct stitude solutions. Examples are 62 velocity wit 5 un for absertation corrections, timing public to get the equivalent of 107 for star position calculation. A fault on the 9/c side or inside the tracker that facinate this information to not be available will cause problems for the tracker in that the attitude solutions coming out will be regnaded.)	Cocalead electronics faul that affects message processing logic Tirror in tracker processor internal software/firmware	All	Tracker uses old or incorrect information to generate attitude solution; solution accuracy is degraded	solutions. G&C software may	the rest of the mission. May	violation would be accepted by the G&C software even if it were generated by the tracker. A slowly drifting attitude solution might be	3		Maybe	Some trackers have status telemetry that will indicate if it is receiving the timing putse or other input data. G&C software will be monitoring some of these health & status flags. Telemetry will also be downlinked occasionally as part of ground monitoring of G&C component performance.			Probably 10-20 seconds to decide that a problem is persistent and warrants taking action	
5114			Failure to output requested telemetry; output messages not generated. (Tracker does not output any attitude solutions.)	11 Aemous/venezur van aber to roden in measurements 12 Permanent famige to detector elements (ballen, optics, APS detector, etc.): - Permanent radiation damage to detector elements (ballen, optics, APS detector, etc.): - Permanent radiation damage to detector - Surface damage to bolffer or design error allows too much stray light into tracker optical path - Cracks, p.ost, or material deposits (contamination) on tenses make images unusuable - Adultion expouse detainen glass so than one enough light gets to detector to detect - Permanent of the enough of the end of the enough of the end of the enough of the end of the enough of the en		Tracker may transition to a mode where it doesn't try to generate attituc sloutions. If it doesn't succeed in gettin a solution for some predefined time period (reaction depends on which tracker we choose to fly)	GEC software will either continue to use tracker continues to the tracker conductions for the other tracker artitude using give rate data from last valid star tracker attitude solution	If not corrected, the tracker could be deemed unusable for the rest of the mission. May not meet WISPR attitude knowledge accuracy requirements around perihelia with only one tracker.	Propagated attitude will slowly drift from true attitude and could eventually result in an	3		Maybe	Some trackers have status telementy that will indicate that they can no longer generate attitude solutions. GRG coffurer will be monitoring some of these health & status Rigs. GRG artitude estimation software will fing a problem for from the same tracker are missing. Telementy will also be downlinked occasionally as part of ground monitoring of GRG. Component performance. Most \$73 provide telementy on background level. Long-term trending could reveal a problem.			Probably 10-20 seconds to decide that a problem is persistent and warrants taking action	
:-1.1.d			Output telemetry contains insufficient measurements, [Tracker alone not output the expected number/quantity of attitude solutions or does not generate telemetry messages at expected rate for read out of rail complement of measurements not generated for single data message.)	1) Seman's detector sponsitionally vasible to collect star fined images a) Enamps do detector elements (Dalling outs), APS, detector, etc.) Temporary radiation damage to detector Collectification from other parts of the 's', temporarily gets into tracker optical path as stray light (could be dependent on attitude relative to Saul). Discovering the relative to Saul's could be dependent on attitude relative to Saul's Date of the catalistic own temporarily causing too much noise in star images. Pume particles from thruster firing passing through tracker FOV "light or low temporarily catalistic processor starting and conference of the starting		Tracker may transition to a mode where it doesn't try to generate attituc solutions if if doesn't success in getting a solution for some predefined time period (reaction depends on which tracker we choose to fly)	G&C software will either continue to use tracker solutions for the other tracker or attempt to propagets y/c stitude using gyro rate data tracker attitude solutions	knowledge accuracy	Propagated attitude will slowly distiff from true attitude and could eventually result in an unbera violation of time between measurements is very long; less likely in this case since we are assuming we are getting some attitude solutions - just not the total amount we should be getting	3		Maybe	Some trackers have status telementy. G&C software will be monitoring some of these health & status flags. G&C statude estimation software will flag a problem if soo many consecutive attitude solutions from the same tracker are consecutive attitude solutions from the same tracker are downlinked occasionally as part of ground monitoring of G&C component performance.			Probably 10-20 seconds to decide that a problem is persistent and warrants taking action	
:-1.1.e			Output telemetry contains degraded measurements. (Tracker outputs attribute solutions whose quality is less than expected (not meeting spect)	In Journal of the control of the con		Fraders usually output some quality, flags along with the attitude solution. When the solution where they no longe generate attitude solutions if low-quality solutions persis for some predefined time period.	continue using solutions from the other tracker if available	the rest of the mission. May not meet WISPR attitude knowledge accuracy	between measurements is very long; less likely in this	3		Maybe	Some trackers have status telemetry, G&C coftware will be monitoring onne of these health & status flags. G&C stitude estimation software will flag a problem if too many consecutive attribute solutions from the same tracker are respected. Telemetry will also be downished occasionally as to downished occasionally as for the companies of performance.			Probably 10-20 seconds to decide that a problem is persistent and warrants taking action	
Mil			Output telemetry contains incorrect measurements which are flagged valid. (Tracker outputs attitude solutions whose time or sittlitude is wrong but without indicating any problems with the solutions in its own quality flags.)	1) Temporary environmental/viewing conditions degrading star images (not enough bright stars found in images): 10 lott for other radiation event temporarily causing too much noise in star images of other radiation event temporarily causing too much noise in star images of other radiation event temporarily causing too much noise in star images of other particular content of the compensated by internal cooler (thermal rotate) and extended of the content of the compensated by internal cooler (thermal rotate) of the content of th		None - tracker thinks everything is ok	associated with these checks and some bad measurements may be used in the attitude estimation if they are just "slightly off" instead of obviously out of family.	tracker could be deemed	Possible, but not likely. The attitude solutions could be off just enough to cause the spacecraft to "till" relative to the Sun or slowly drift off from the desired TPS to Sun pointing.	3		Maybe	G&C attitude estimation software will flag a problem if too many consecutive attitude solutions from the same tracker are rejected. Telemetry will also be downlinked occasionally as part of ground monitoring of G&C component performance.			Probably 10-20 seconds to decide that a problem is persistent and warrants taking action	:
puts			Power			ST not powered	Can't meet WISPR pointing requirements during encounter. Switch to other ST	No effect.	N/A	3							
			Time code			ST will keep working	If not already active. Accuracy of ST output will drift and might send flags to autonomy. Ground will notice drift in long-term trending an will command s/t o resetST and/or switch to other ST, if it's not already active. With loss of a ST, can't meet WISPR aointing requirements.	No effect.	Drift may cause s/c to get into undesired position, but SLSes should alert autonomy to any potential umbra violations.	3							
			5/c velocity from FSW			ST will keep working, but will report th it's not getting this information.	Accuracy of ST output will drift and might send flags to autonomy. Ground will notice drift in long-term trending and will command s/c to reset ST and/or switch to other ST, if it's not already active. With loss of a ST, can't meet WISPR pointing requirements.	No effect.	Drift may cause s/c to get into undesired position, but SLSes should alert autonomy to any potential umbra violations.	3							
			Multiplexer			If set to wrong side of avionics, looks like ST is off.	Switch sides of avionics and/o command muliplexer to correct setting. Can't meet WISPR pointing requirements during encounter with a single ST.	No effect.	N/A	3							

Subject Matter Expert(s):	Robin Vaughan	occur until 2014. Yellow hig	dent on the exact sensors selected. Selection will probably not hlighted blocks are redundant components. Components are listed					Personre				Quick Response		•	
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Leve	Desired Local Response	Allocation of Local Response	Time to fix Transr locally Signs		Allocation of Time to fix System system	Time to Transmit Signal	Ground Response / Contingency	essor itch	Safe Mode	Remediation	R
GC-1 GC-1.1	Star Trackers Star Tracker A											 			
GC-1.1.a			nput command not received or acted on. (When turned on, rrackers typically need to be sent a series of commands that bring them up to full operational mode. If the tracker is unable to correctly process bese commands, it on fail to reach the normal tracking mode where it would start generating attitude solutions.)		GEC attitude estimation softwar will flag a problem if too many consecutive attitude solutions from the same tracter are mission are rejected fight to pass the saint properties of the solution of the solution of the consecutive of the solution of the solution of the solutions).			If G&C software flags a problem either from the health & status telemetry or with the attitude solutions, it will request action errorn fault protection. Usually this is by susputting flag that are used in the premise of various autonomy rules.						Software roboot, tracker reset, or tracker power cycle may fix some problems with electronic or software. Switching to redundant unit may not alleviate problems if the error lies in common software.	
GC-1.1.b			Input message not received or processed. (The trackers typically inced some information from the avionicx/SSW to generate correct attitude solutions. Examples are six evelocity wit Son for deservation position calculation. A fault on the xX dies or inside the tracker that causes this information to not be available will cause problems for the tracker in that the attitude solutions coming out will be fegraded.)		G&C attitude estimation softwar will flag a problem if too many consecutive attitude solutions from the same tracker are rejected (fall to pass the sanity checks - mostly consistency checks on the time sequence of solutions)	e		of G&C software flags a problem either from the health & status telemetry or with from flag protection. Usually this is by corporating flags that are used in the premise of various autonomy rules.						inernal reset (no ground or autonomy action required), software reboot, tracker reset, or such electronic or software. Switching such electronic or software. Switching redundant unit may not alleviate problems it the error lies in common software.	
GC-1.1.c			Failure to output requested telemetry, output messages not generated. (Tracker does not output any attitude solutions.)					If G&C software flags a problem either from the health & status telemetry or with the attitude solutions, it will request action from fault protection. Usually this is by coupturiting flags that are used in the premise of various autonomy rules.			Might be able to boil off constannation material (parti-om \$T from \$\cdot\) constant in the constant in the constant coders that could be turned of it to all of this process, low-of-a round parts of the image field that have paged in the process, the constant in the paged in the constant in the paged in the constant in the paged in the constant in the paged in the constant in the loop to diagnose the problem and decide on what fix to try.			Software reboot, tracker reset, or tracker power cycle may fix some problems with electronic or software. Switching to redundant unit may not alleviate problems it the error lies in common software.	
GC-1.1.d			Output telemetry contains insufficient measurements, [Tracker dose not output the expected number/guantity of attitude solutions or dose not generate telementy messages at expected pate for read out or full complement of measurements not generated for single data message.)					F G&C software flags a problem either ron the health. B. statu telemetry or with the attitude solution, it will request action from fault protection. Usually this by soutputting flags that are used in the premise of various autonomy rules.			Might be able to boil off contamination material (anti-ram ST only-some ST have interested in coders that could be turned off to did in this process), what around an other process of the state of suspect image content, change statuder estable to class of suspect image content, change statuder estable to class of suspect image content, change statuder estable to diddressed with a fault protection response on the spacecraft. We'd when to get the ground in the loop to classification of such that the subsection of such that such as such		Software reboot, tracker reset, or tracker power cycle may fix some problems with electronic or software. Switching to redundant unit may not alleviate problems if the error less in common software.	÷	
GC-1.1.e			Output telemetry contains degraded measurements. (Tracker outputs attitude solutions whose quality is less than expected (not eneeding spect.)					of GAC software flags a problem either from the health & status telementy or with the attitude solutions, it will request action from fault protection. Usually this is by soutputting flags that are used in the premise of various autonomy rules.						Software reboot, tracker reset, or tracker power cycle may fix some problems with electronic or software. Switching to redundant unit may not alleviate problems if the error less in comman software.	**************************************
GC-1.1.f			Output telemetry contains incorrect measurements which are flagged valid. (Tracker outputs attitude solutions whose time or attitude is wrong but without indicating any problems with the solutions in its own quality flags.)					If G&C software flags a problem either from the health & status telemetry or with the attitude solutions, it will request action from fault protection. Usually this is by coupturiting flags that are used in in the premise of various autonomy rules.						Software reboot, tracker reset, or tracker power cycle may fis some problems with electronics or activate. Switching to recluded not many man alleviate problems if the error lies in common software.	
Inputs			Power												[
			Time code												
			S/c velocity from FSW												***************************************
			Multiplexer												
GC-1.2	Star Tracker B	<u> </u>	İ	İ	1	1				1				İ	İ

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation	Severity 1	ype of FM	Observable	How Observed?	Detection Meth TIm for Diagnosis	od TIm Path for Diagnosis	Time to Detect Time to Detect (Local) (System)
	Solar Limb Sensors	on the current design, there is ofter ally redundant. This two terminally redundant. This two experiences of the mass of the reduction of the mass of			At default attitude when <0.8 AU from Sun				Note on umbra violation for SLS. When any of the SLS heads see the Sun, then safe and see the Sun, the safe and see the Sun, the safe and see the Sun, the safe and see the Sun the safe and see the Sun before the safe and see the Sun before the SLS heads will be suffered to the SLS heads will be suffered to the SLS head see the Sun before the SLS heads will be suffered to suffer suffered to suffere suffered to suffere suffered to suffere suffered to suffere suffered to suffere suffered to suffere suffered to suffere suffered to suffere suffered to suffere suffered to suffered							
GC-2.1.a			signor message not a reached or processed. (The solar limb sensors may reed some information from the avionics/SSW to set gains or awareners that are used in comparing som offset angle from cell intensity readings. A salar on the s/s dee from cell intensity readings. A salar on the s/s dee from time the solar intensity readings. A salar on the system of the available will cause problems for the solar limb sensor that the angle solutions coming out will be degraded. (cases where angle solutions are grossly incorrect are included in another section below))	Faulty connector or harness/wiring inside unit Localized electronics fault that affects message processing logic First in solar limb sensor internal firmware (PPGA)		Sun geometry when first detected is iunchanged so time of detection is unaffected; sold imbo bearon used of or incorrect information to generate Son offerst englis angle accuracy to some offerst englis and sold sold sold incorrect information to output may be delayed.	Control correction will be wrong because offset angle is Will not meet WISPR pointing requirements with meet wisPR pointing requirements willing based on S.S. data. S.C may think it's seeing the Son earlier than a tactually is, for may "see" it too late.	SLS. If we avoid umbra violation, we may be able to correct the parameter values before we have another attitude anomaly where SLS would see the Sun.(With luck	Possible. Spacecraft could drift into s/c packaging umbra while trying to correct attitude using SLS angle data if control action is not "strong" enough or not taken soon enough.		None Active P Active	robably not	Don't think there is a way to detect this. If we are using the wrong parameters in the SLS signal processing, we won't have any way to conclude that we are getting wrong answers. (This assumes that target attitude is *271PS to Sun.)	1) None 2) SLS heartbeat?	2) None 2) SLS to CDH to Autonomy II SLS to CDH to Autonomy	31 Nane 23 7 None 31 7
GC-21b			Case 1: Failure to output requested telemetry; output messages and generated. (One solar limb sensor head does not output any Sun presence or offset angle data (presumes that we get to an intribute where the new output set was to so that it should be instructed and the solar output set of the solar presence flags and offset angle values).)	Sensor/detector not able to collect measurements, damage to detector elements (Sheled, Ozore glass, solar cells, etc.) — Permanent radiation damage to detector element — Failure in detector solar cells for output current — Craks, pits, or material deposits (contemantation) on cover glass blocks or alters path of Sun (glit reaching detector cells — Sing light reaching detector cells — Sing light reaching detector cells — The contemporary of the cells of the cells of the cells — Admitted the cells of the cells of the cells — Reaching of the cells of the cells — Reaching of the		none -SLS is trying to communicate and int't able to or cannot detect the Sun when it is exposed to it	None if failure confined to single side of detector head or one side of redundant electronics (the loss of a single sensor is oil.). The other side of the head would detect the Sur and alter G&C software to the volation. Or data available from other side of electronics. (Presumes we mu with both sides on at all times)	Potential loss of mission if SLS data not available from	No if data still available from other side of detector head or detectories, each of side its common to both electronics or both sides of a single sensor head	2R	one F	robably not	There may not be a way to detect this since the normal condition for the SLS is to not have any data to output because the heads are not seeing the Sun if we run with both sides on, we might be able to see that one side of a head is outputting data and the other one in it assuming that head is seeing the Sun if assuming that head is seeing the Sun	SL5 output	SLS to CDH	y None
6€-2.1.¢			Case 2: Failure to output requested telemetry; output messages and generated. (One side of SLS electronics does not output any Sun presence or offset angle data (presumes that we get to an stitute where one more heads voud set be Sun so that it should be outputting Sun presence flags and offset angle values).)	- Hardware damage or fault in internal electronics boards or harnessing that prevents detector data processing Hardware damage or fault in internal electronics boards or harnessing or connectors		none - SLS is trying to communicate and int's able to or cannot detect the Sun when it is exposed to it	None if failure confined to single side of detector head or one side of redundant electronics (the loss of a single sensor is ok). The other side of the head would detect the Sur and alert G&s oftware to the violation. Or data available from other side of electronics. (Presumes we run with both sides on at all times)	Potential loss of mission if SLS data not available from	common to both electronics	2R N	one h		We may be able to detect that the electronics never puts data on the interface to the SCIF card. We won't be able to detect that the electronics outputs a message that says "Sun not present" when a head really is seeing the Sun.		SLS to CDH	7 None
GC-2.1.d			are flagged valid. (solar limb sensor outputs Sun presence flags or	1) Environmental/viewing conditions cause failse Sun detection 3) Glint reflected off other spacecard components illuminates the detector head enough to cause it to think it see the Sun cause it is think it see the Sun cause it is think it see the Sun cause it is think it see the Sun cause it is think it see the Sun cause it is think it see the Sun cause it is think it see the Sun cause it is the Sun of Sun of Sun of Sun of Sun of Sun of Sun of Sun cause it is sun of Sun of		None - solar limb sensor thinks everything is ok	Depends how we program the G&C software when looking at SL data. If we decide to respond to any single detection by one of side of the control action when it isn't necessary. If we are always getting information from both discleded to the control of the side to each head, we may be side to detect that just one side thinks it's sening the sun and the other side doesn't. But then it's not clear which side we should believe.	try to change the attitude when it's at the correct attitude and end up moving		2R A	tive A	Maybe	G&C software may be able to isolate the false reading if data wailable from both sides the head (and fault is not common to both sides). May be difficult to detail with side is sending the "urong" data.	Error flag?	G&C to CDH to Autonomy	7 None
GC-21e			Core 2-Output belienetry contains incorrect measurements while we flagged walfs. (solar limb series outputs Sun presence flags or other supeled staff are aroung but without inclinating any problems with the solutions in its own status flags (if there are any Care 2 Gross) incorrect Sun offset angle data - not tracking true Sun-relative geometry.)	component in processing chain course signals to be combined incorrectly when		None - solar limb sensor thinks everything is ok	Depends how we program the G&C software when looking at SL data. If we decide to respond to any side of the SL heads, then we may take control action when it isn't necessary. If we are always getting information from both difference between what the way that the two sides are outputting. But then it's not clear with side we should believe.	when it's at the correct attitude or make the wrong change to an off-Sun attitude Either way we end up moving	. isolated false readings.	2R	htive h		GSC software may be able to isolate the false reading if data wailable from both iden of the head (and fault is not common to both iden). Seriously bad readings—like being 40 deg off Sum near periapse—can probably be rejected since the syl would not survive this condition. Smaller offsets that are incorrect would be harder to detect. No good way to determine which sensor is sending the "wrong" data.	Error flag?	G&C to CDH to Autonomy	y None
60-2-1.1			are flagged valid. (solar limb sensor outputs Sun presence flags or offset angle data that are wrong but without indicating any problems with the solutions in its own status flags (if there are any Case 3 Incorrect timing of Sun presence or angle data - indications	Error in electronics interface with s/c A) Mismatch in timing between output of messages by SLS and readout of interface by		None - solar limb sensor keeps working as if everything is ok	Depends on the size of the delay and how erratically the data are delivered to the G&C accidence of the G&C accide	unable to respond soon	Possible if failure is common to both sides of head or determine. If delay is too long between SLS head first seeing between SLS head first seeing he sum and reporting it to GAC. (if may have driffed sides, may be not be under a boundary. Or GAC may pause sides, manghe to the umbra boundary. Or GAC may pause that saking action if there are long time gaps in the SLS data. If delay is siolated to one side, the differences in readings some to deal with save to be deal with a save to be deal with contracted about horse is not confused about how much correction is needed.	2R	h tive	faybe	G&C software may be able to deal with differences between disea and use data from the "earliest" side to correct attitude.	Error flag?	GEC to CDH to Autonomy	7 None
Inputs GC-2.2	Solar Limb Sensor ^p		Power			No effect if power is only lost to one side of electronics,	No effect.	No effect.	N/A	4						
QC-2.2	Judi Liniu Sensor B	<u>.</u>	A		.1	.t	A	A					<i>,</i>		<i></i>	·ii

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response		Time to Transmit	Response Desired System Response	Allocation of System	Time to fix system	Time to Transmit	Ground Response / Contingency	System Side Switch	Quick Processor Switch	Response Safe Mode	Remediation	Revisit
GC-2	Solar Limb Sensons	the three current desires, there is, one electronics box which is correctly reduced. The two victorials yield-united his two series of heads and to the spacecraft (two destination of the control of the control of the control of the control heads, such is series of heads, such is series of heads, such is series of heads, such is series of heads, such is series of heads, and the control heads, such is series of heads of the electronics. There is a connected to a different side of the electronics. There is a connected to a different side of the electronics. There is a connected to a different side of the electronics. There is a connected to a different side of the electronics of the electron						Signal		Response		Signal						
GC-2.1.a	sider Limb Semont A		Input message not received or processed. (The solar limb sensors may need some information from the avoincit/SW to set gains or againstens that are used in computing some offers angle from cell intensity readings. A faut on the ty clade or inside the solar limb avoincition of	I) None 2) Local 3) Local	IJ None 2J Power cycle SLS IJ Power cycle SLS	I) None 2) Autonomy 3) Autonomy	None	1) None 2) 7 3) 7	None	None	None	None	None				Redundant heads may not help because the parameters are probably the same for both might help if the other side of the neight help if the other side of the electronics doesn't have the internal problem that causes it to miss getting inplated parameters. But then we have to figure out have to give the "right" data from the two readings from each side. Might be able to it on Fight callbration at larger solar distances, but unlikely since will be at the saturation limit for low intervally insoit of the time where we could attempt scalabration. Triging to calibrate at ornal solar scalabration. Triging to calibrate at ornal solar scalabration. Triging to calibrate at ornal solar far enough off Sun for the SLS head to see the Sun and generate angle data – assuming that the star tracker and ephemeris would hold us at an attitude that was still outside the si/c packaging unbra and using the attitude and pehemeris indice to get the star scalabration. Triging the attitude and ephemeris find to get the star scalabration and the star scalabration and scalabration. The scalabration is a star scalabration scalabration. The scalabration is scalabration. The scalabration is scalabration scalabration scalabration scalabration scalabration. The scalabration s	
GC-2.1.b			Case 1: Failure to output requested telemetry, output messages ned generated. (One solar limb sensor head does not output any sun presence or offset angle data (presumes that we get to an attitude where the head would see the sun to that 2 should be outputting Sun presence flags and offset angle values).)	Local / Ground	None	Ground	None	None	None	None	None	None	Ground contingency - turn on both 51s to used from fails to output data; journally try to power cycle?				like redundant harborer - redundant i succions of single electronics unit and redundant sections of detector heads. (Issuaming the fallure is not common to both sides of a head or the electronics.) If common to both lides of a head, we've lost data from one of the 4 heads. Depending no here the Sun is actually drifting off from *2, we may not detect the drift and get to an unbrav violation. Any contamination or alignment shifts will skey affect both ties of a single head shey affect both ties of a single head head (but not impossible) slight be able to both off contamination material - assuming we ever realized it was three in the first place.	n n
GC-21.c			Case 2. Failure to output requested telemetry, output messages not generated. (One side of 3.5 electronics does not output any Sun presence or offset angle data (presumes that we get to an situate where one or more heads would see the Suns to that 4 should be outputting Sun presence flags and offset angle values).)	Local / Ground	None	Ground	None	None	None	None	None	None	Ground contingency - turn on both SLS to see if one fails to output data; possibly try to power cycle?				Use redundant side of electronics. Solar limb sensor power cycle might clear the fault in the electronic. Or there may not be any way to fix this problem if hardware inside the solar limb sensor is broken or if it is a common problem due to common fermware.	1
GC-2.1.d			Case 1: Output telementry contains incorrect measurements which are flagged valid. (colar limb sensor outputs Sun presence flags or officet angle data that are wrone plan without indicating any problems with the solutions in its own stath flags (if there are and Case 1 False Sun detection - indicating Sun presence when head is not seeing the Sun.)		7	Autonomy	7	7	None	None	None	None	None				Use redundant hardware - either separate redundant units, or redundant sections of single electronics unit and redundant optical heads. The real question here is how likely is a false detection. There are not many good ways to detect this assuming that the SLS is on detect this assuming that the SLS is on detect this assuming that the SLS is ont defense against attitude drifting off Sun. Use of redundant sensor or electronics may not solve problems due to common or similar equipment. SLS feet or poener cycle may clear an electronics or SW/FW fasit, but may not. Association in the support cycle the SLS while in view of the Sun.	al e o
GC-21.e			Case 2. Output telemetry contains incorrect measurements which are flagged vaid. (colar limb sensor outputs Sup presence flags or offerst angle data hat are wong but without indicating any grorbelms with the solutions in its own status flags (if there are any Case 2 Grossy) incores Sun offset angle data – not tracking true Sun-relative geometry.)	Local	7	Autonomy	7	?	None	None	None	None					Use redundant hardware - either separate redundant units, or redundant section of single electronics until and redundant optical single electronics until and redundant optical. The red question here is how likely getting really bids angle views is - there are not many (if any) ways to detect this by independent means. Use of redundant hardware may not alleviate the problem if the failure is in a common or similar component. Power cycling may fix an electronics or SW/FW error, but would have no effect on a jewt faul.	1
6C-2.1.f			Case 3: Output telemetry contains incorrect measurements which are flagged valid. (Josa limb senor outputs Sun presence flags or officet angle data that are wong Dut without indicating any problems with the solutions in its own status flags (if there are any case a liscorrect timing of Sun presence range data - Indications come too late relative to the true Sun-relative geometry.)	Local	,	Autonomy	7	2	None	None	None	None					Use redundant hardware - silter separate redundant units, or redundant section of redundant section of heads. The real question here is how likely is getting into gitting time delays or erratic behavior on the data interface.	ng.
Inputs GC-2.2	Solar Limb Sensor B		Power															х

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	TIm for Diagnosis	TIm Path for Diagnosis	Time to Detect Time to E
ı	inertial Measurement Unit	loop mode. If two fail, a TCM couldn't be performed. A single failure at any point in time in the mission would be ok. The FMEA results are the same as what is listed (for the	Note that the current design has redundancy in both the number of individual gross and in the electronic/jower supplies. Minimum requirement for controllability is juyers covering 3 orthogonal directions. Liber we will have one unit with it gives and 2 electronic/jower supplies (more likely) or just that each have 3 gross and 1 electronic/jower supply (less likely). In the latter case, we would have for un with both units on lay probably month them in different orientations) to ensure we'd have 3 good gross at all times.													
	IMU Side A								ļ						å	
3.1.a			liput command not received or acted on (When turned on, some IMM), need to be sent a series of commands that configure them to the correct operational mode. If the IMM is unable to correctly process these commands, it on fall to reach, it on fall to reach the normal operating mode where it would start outputting given rate data.)		All		if some gyro data are available, G&C software may generate less accurate spouccarfla stitule. & rate solutions, if no gyro data is evaluable, G&C software may be unable to generate authorid/rise solutioner/of the solutioner/of the spacecraft. G&C software will yet oue rate informer of the spacecraft. G&C software will yet oue rate informer of the spacecraft is gyro data are available.	the rest of the mission. This would be a loss of mission if redundant IMU/gyros are not	eventually result in an umbra	2R	Active	Probably	If MU is able to output believely. It should indicate in current operating mode. GBC software will be monitoring isome of these health & status flags. Telemetry will also be downlinked octasionally as part of ground monitoring of GBC component.	IMU Operating Mode G&C IMU error flag	CDH to Autonomy	3 Mone
3.1.b			Imput message not received or processed [The IMU typically needs some timing information from the avionics/TSW to generate correct time tags on the gyro rate data solutions. A fluid on the s/c swallbel will called problems for the Mill in that the rate measurements coming out will be misleading or dropped due to the incorrect time tags.)	Faulty connector or harness/wiring inside unit Coolined electronics fault that affects message processing logic Forer in MU processor internal software/firmware	All	MILLUS SE INTO SOUL TIME IN THE SECOND TO	gyro measurements if their time tags are inconsistent with	rate data is available, this	enough to cause an umbra violation would be accepted by the G&C software even if it were generated by the IMU. A slowly drifting attitude solution might be harder to	2R	Active	Maybe	Most IMUs have status telemetry that will indicate if it is receiving the timing pulse or bother input data. Good software will be monitoring of the control of lags. Telemetry will also be downlinked occasionally as part of ground monitoring of G&C component performance.		MU to GNC/CDH to Autonomy	? None
3.1.c			generated (into dues not output any gyro rate measurements)	1) Sensor/detector nor able to collect measurements 2) Damage for detector elements internal to the gyrol (strange mechanisms are specific 2) Damage for detector elements internal to the gyrol (strange), for itilis or earticle respective for the strange for the control of the strange for the control of the strange for the control of the strange for the control of the strange for the control of the strange for the control of the strange for the control of the strange for the control of the strange for the		Gyros may fransision to a mode where they don't try to generate rate data or data may be flagged invalid from one or more gyros	Since insufficient gyro data is available, G&C software will either use rate information from the star ratempt to propagate s/c attitude through continuing star ratcker attitude solutions. Ratt knowledge will be degraded - knowledge or continuing requirements may not be met.	can't be obtained, the IMU could be deemed unusable for the rest of the mission. Probably will not meet attitude knowledge or control accuracy requirements	missing or degraded rate data will slowly drift from true	2R	Active	Maybe	Some IMUs have status telemetry that will indicate that they can no longer generate grow data. G&C software will be monitoring some of these health & status flags. G&C stitude estimation software will liga problem if too many consecutive measurements from the same BMU are missing. Felemetry will also be downishly as part of ground monitoring of G&C component performance.	IMU health and status flags	IMU to GNC/CDH to Autonomy	Probably 5-10 seconds to secide that a problem is persistent and we second to the second section
8.1.d			not output the expected number/quantity of gyro rate measurements of does not generate telementry messages at expected rate for read out or full complement of measurements not generated for single data message)	1) Sensor/detector sporadically unable to collect gyro rate data 2) Damage to gyros (damage mechanisms are specific to the tupe of gyro selected (FOG, EMG, MBGM, MSG), examples for rifical are particle trapped inside or misalighment of resonator pieces causes friction or disturbs the normal resonance) of informational privings conditions degrading gyro measurements (sensitivity to of informational privings conditions degrading gyro measurements (sensitivity to of information (and the privings of the privi		Gyros may transition to a mode where they don't try to generate rate data or data may be Hagged invalid from one or more gyros	Since insufficient gyro data are wallable, G&C ioftware will form the star tracker measurements or attempt to propagate s/6 attitude through continuing star tracker attitude solutions. Bate innowledge will be degraded - knowledge or control requirements may not be met.	If sufficient gyro rate data can't be obtained, the IMU could be deemed unusable for the rest of the mission. Probably will not meet attitude knowledge or control	Propagated attitude with missing or degraded rate data will slowly drift from true stituted and could eventually result in an umbra violation.	2R	Active	Maybe	some IMU have status telemetry that will indicate that they can no longer generate grow date. Giving some of these health. Giving some of these health. & status, 1849. Get a status of these health. & status large, G&C status de estimation software will flag a problem if so many consecutive invesurements from the same date of the status	MU health and status flags	MAU to GNC/CDH to Autonomy	Probably 5-10 econds to decide that a groblem is prosiblem is persistent and warrants taking action
lie			Output telemetry contains degraded measurements (IMU outputs) or gyror are data whose quality is less than expected or not meeting spec)	1) Environmental conditions degrading gyro data 3) CMG or other radiation event temporarly causing too much noise in rate data 3) Local source of IMU stimulation (e.g. vibration) causing "noise" in rate data 3) Local source of IMU stimulation (e.g. vibration) causing "noise" in rate data 1-litips of noise temporate that can be compensated by internal temperature control inechanisms. 2) Elizar or in software or related memory degrades processing of gyro rate measurements 3) Gyror read out of data processing algorithms are iscerred. 3) Time stamp associated with gyro rate data is blaced from correct time		Data may be flagged invalid or quality indicators may be changed ot indicate the problem with data from one or more gyros	G&C software may reject some of the rate data if it does not pass consistency checks. Software should continue to be able to generate attitude solutions, but hey will not be as accurate. Rate knowledge or control requirements may not be met.	could be deemed unusable for the rest of the mission. Probably will not meet attitude knowledge or control accuracy requirements	Propagated attitude with missing or degraded rate data will slowly drift from true attitude and could eventually result in an umbra violation.	2R	Active	Maybe	Some fMU have slatus telemetry that will indicate that they can no longer generate gro data. G.G. controlled the controlling specification of the controlling specificatio	IMU health and status flags	aMU to GNC/CDH to Autonomy	Probably 5-10 seconds to decide that a problem is persistent and warrants taking action
3.1.f			quality flags)	1) Environmental/viewing conditions degrading gyro rate data 3) CMI or other radiation event temporarily causing too much noise in rate data 3) CMI or other radiation event temporarily causing too much noise in rate data 5) Local source of MIS instituation (e.g. vibration) classing "noise" in rate data 6) leigh or low temperature that can't be compensated by internal temperature control mechanisms. 2) Error in some or radiated memory company processing of your can ensurements 2) Error in synthesis that package rave gror exadout for one message temperature 3) Error in hardware chain for gyror readout causes incorrect data to be used by processing software - raw readings are corrupted and don't reflect actual gyro output		None - IMU thinks everything is ok MAU structs down	G&C software will reject a measurement if it's not consistent with recent past history of s/c attitude & rate history of s/c attitude & rate But there will be bounds associated with these checks and some bad measurements may be used in the attitude estimation if they are just "slightly off" instead of obviously out of family. Switch sides of IMU	unusable for the rest of the mission. Probably will not meet attitude knowledge or control accuracy requirement: without gyro rate data. May be loss of mission. No effect.	rate measurements could be off just enough to cause the spacecraft to "tilt" relative to the Sun or slowly drift off from the desired TPS to Sun	2R 2R	Active	Maybe	G&C attitude estimation software will flag a problem if too many consecutive gyro rate measurements from the same gyro are rejected. Telemetry will also be downlinked occasionally as part of ground monitoring of G&C component performance.	IMU health and status flags	IMU to GNC/CDH to Autonomy	Probably 5-10 seconds to decide that a problem is persistent and warrants taking action
			Relay commands				No effect until the IMU configuration needs to be changed.	Should always be able to have 3 gyros and one data interface board working. Might not be able to access all the accelerometers, which means that TCMs could not be performed in closed-loop mode.	N/A	3						
			Data (commands from the SCIF)			Some IMU data is lost	Since insufficient gyro data is available, G&C software will either use rate information from the star tracker measurements or attempt to propagate s/C attitude through continuing star tracker attitude solutions. Rat knowledge will be degraded-knowledge or control requirements may not be met.	can't be obtained, the IMU could be deemed unusable for the rest of the mission. Probably will not meet attitude knowledge or control accuracy requirements	missing or degraded rate data will slowly drift from true	2R						

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit	Response Desired System Response	Allocation of System	Time to fix system	Time to Transmit	Ground Response / Contingency	System Side Switch	Quick Processor Switch	Response Safe Mode	Remediation	Revisit
C-3	inertial Measurement Unit	couldn't be performed. A single failure at any point in time in the mission would be ok. The FMEA results are the same as what is listed (for the	Note that the current design has redundancy in both the number of individual gross and in the electronic/gover supplies. Minimum requirement for controllability is a grow covering 3 orthogonal directions. Either we will have one unit with 4 gross and 2 exterioric/gover supplies (more likely) of cults that each have 3 gross and 1 electronic/gover supply (less likely). In the latter case, we would have for in with bloot units on lay probably month them in different orientations) to ensure we'd have 3 good gross at at times.					Signal		Response		Signal						
iC-3.1	IMU Side A										ļ	ļ					Use star tracker rate data if redundant gyro	 !
GC-3.1.a			Input command not received or acted on (When hursed on, some and the configure them to the correct operational mode. If the MUI is unable to correctly process these commands, it can full to reach the normal operation, and on the correctly process these commands, it can full to reach the normal operating mode where it would start outputting give rate 66s.)	Local	astU switch	Autonomy	7	2	None	None	None	None					hardware is not available. Software reset or IMMJ power cycle may cornect a software or electronic problem. Switching to the redundant IMMJ may not fiss a problem that lite is normann electronic software. If a software is normann electronic software is not remediated in increasany if 3-2 gyros continue to operate normally. If 3 gyros continue to operate normally, If 4 3 gyros are providing data, then the full attitude state is not observable and G&C coftware provided patch, then the full attitude state is not observable and G&C coftware removaled have to supplement the gyros data with another source of rate data (se star tracker measurements) if available. In other words, we are tolerant to loss of some gyros tracker measurements) if available in other sources, we are tolerant to loss of some gyros.	
GC-3.1.b			thout message not received or processed (The IMU typically needs come timing information from the eviolocit/SW to generate correct time tage on the pror rate data solutions. A fault on the s/c side or inside the IMU that causes this information to not the side or inside the IMU that causes this information to not available will cause probleme for the IMU in that the rate measurements coming out will be misleading or dropped due to the incorrect time tags.)	Local	MU switch	Autonomy	7	2	None	None	None	None	None				Use star tracker net data if redundant gyro nardware in not available. If the error in the time tags for the IMU data could be characterized on the ground, the GGG FSW could be modified to correct the time tags on-board. If the star tracker kept working, we should have time to detend correct this with ground analysis. This is not something that on-board fault protection could handle. Soft reboot or power cycle may correct an electronics or software/firmware bissue. Any faults due to common components or software would not be corrected with an iMU switch.	
GC-3-1.c			Failure to output requested telemitry, output messages not igenerated (IMU does not output any gyro rate measurements)	Local	and I switch of GGC software flags a problem either from the health & status eithenty or with the giro measurements, it will request ston from fault protections. Shoully this to by outputting flags and are used in the premise of earthcase authorizing value either flags.	Autonomy	7	2	None	None	None	None	None				Use star tracker rate data if redundant gyro hardware is not available. Software reset or IMU power cycle may correct a software or electronic problem. Switching to the redundant IMU may not fix a problem that fies in common electronics or software.	
GC-3.1.d			Output telemetry contains insufficient measurements (MMU does not output the expected number/quantity of gro rate measurements or does not generate telemetry messages are specied cate for rood of rolf complement of measurements and generated for single data message)	Local	MU switch of GGC software flags a problem where from the health & status elementery or with the gyro measurements, it will request section from fault protection. Justilly this is by outputting flags are are used in the premise of serious autonomy rules;	Autonomy	7	2	None	:None	None	None	None				Use star tracker rate data if redundant gyro hardware is not available. Software restor full power cycle may correct a software or electronics problem. Switching to the deundant IRUI may not fix a problem that lies in common electronics or software.	
GC-3.1.e			Output telemetry contains degraded measurements (IMU outputs gyro rate data whose quality is less than expected or not meeting spec)	Local	MU switch If GGC software flags a problem where from the health & status sheenedry or with the gyro measurements, it will request scion from fault protection. I health with is by outputting flags that are used in the premise of serious autonomy rules.	Autonomy	7	7	None	None	None	None	None				Use star tracker rate data if redundant gyro hardware is not available. Software reset or MIM Jower cycle may correct a software or electronics problem. which may be redundant IMU may not fix a problem that lies in common electronics or software.	
GC-3.1.f			Output telementry contains incorrect measurements which are flagged valid (IML) outputs gyro rate data whose time or rate is wrong but without indicating any problems with the data into own quality flags)	Local	MU switch If G&C software flags a problem other from the health & status telemetry or with the gyro rates, it will request action from fault protection. Usually this is by sortputting flags that are used in the premise of various autonomy rules.	Autonomy	7	?	None	None	None	None	None				Use star tracker rate data if redundant gyro hardware in not available. Software reset of MIJ power cycle may correct a software or electronics problem. Switching to the redundant IMU may not fix a problem that lies in common electronics or software.	
Inputs			Relay commands															х
			Data (commands from the SCIF)															х
GC-4	IMU Side B Reaction Wheels Rx Wh 1																	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Method	od TIm Path for Diagnosis	Time to Detect (Local) (System)
GC-4.1.a			brable to eart force/forque on spacecraft (flywheel is not being consistent on to existing the change its spin; flywheel anturally spins shown due to losses in the system (friction); flywheel is unable to rotate)		All except launch (of less concern when thrusters as concern when thrusters are control, but of all will always some effect since we continue to command the wheels during TCMs and momentum dumps)	reach a low or zero speed equilibrium but could be kicked up again by externa	pick up the slack and maintain desired attitude, just not as accurately. Probably will not meet jitter requirements and may not meet science pointing accuracy requirements as wheel is spinning down.	remaining 3 wheels, but momentum dumps will be	Unlikely since the other 3 wheels should maintain attitude, although they may b running at higher	2R		r'es	compare wheel speed/torque to commanded wheel speed/torque to commanded wheel speed/torque from the speed to commanded wheel speed to commanded wheel speeds and other health status torque and other health status the monit			TIIO - probably ** which for a ** control opics to opics an heel unvesponsive
GC-4.1.b			Case 1: Incorrect force/forque exerted on spacecraft	Frozen torque command - direction and magnitude stay at some fixed value; include both max and below max magnitude values.		The "stuck" or "run away" wheel will eventually reach saturation (man speed with how long that takes depending on the speed magnitude when command first froze.	and once 2 of them are saturated, we lose	case - even if solar limb sensors detect the umbra violation it may not be correctable in the time available depending on how we design the auto dump logi	Possible if failed wheel is still considered available, but despends on more members sate despends on the members as a second of the second of the occurs and timing of momentum dump logic and wheel fault logic (to turn off misbehaving wheel)	2		res	compare wheel speed/forque to commanded wheel speed/forque for the speed/forque for the speed forque for the speed forque for the speed forque			TIIO - probably "In was the for a " "In control of the control of
GC-4.1.c			Case 2: Incorrect force/torque exerted on spacecraft	Direction stack at + or , magnitude correct responding only to magnitude part of command.		The "stuck" wheel will eventually reach isturation (max speed) with how long that takes depending on the speed magnitude when direction first got stuck.	The controller will mistakenly keep sending commands to all the wheels. The one that's only responding to to torque magnitude will eventually saturate at mas speed. The momentum will be higher, but may or may not be at the dump limit when the wheel may limit when the wheel may limit when the wheel may limit when the wheel and none 2 of them are saturated, we lose controllability. If the system can do a momentum dump before 2 of the wheels reach saturation, we may survive longer but dumps will be done more frequently (if allowed) is used to be a start of the	Loss of mission in the worst case - even if solar limb sensors detect the umbra violation it may not be	Possible if too many wheels reach saturation before a momentum dump can be performed.	2						
GC-4.1.d			Case 3: incorrect force/torque exerted on spacecraft	Direction reversed, magnitude correct - error in wheel interface electronics; most wheels have separate inputs for the direction and magnitude of the commanded torque that are probably processed separately in the wheel electronics.		Wheel will spin in opposite direction from commanded direction and exert a lorque that fights against the desired control. Worn treessarily reach saturation (mas speed) since direction agar can still change with time.	when this occurs. There	Loss of mission in the worst case - even if solar limb sensors detect the umbra violation it may not be	Probably not in this case.	2						
GC-4-1.e			Case 4: Incorrect force/torque exerted on spacecraft	Magnitude studs, direction correct; responding only to direction part of command, but non-zero magnitude; include both max and below max magnitude values.		Wheel will spin in correct direction from commanded direction but torque magnitude will be larger or smaller that commanded. Worn necessarily reach saturation (max speed) since direction sign can still change with time. It sessentially adding in some disturbance torque that can work with the system o against it.	oscillate between + and - values. If magnitude is high, this might just drive one of the other wheels to saturation and if a momentum dump isn't	correctable in the time available depending on how	Possible, but less likely if torque magnitude is lower.	2						
6041.1			Case 5: Incorrect force/torque exerted on spacecraft	Wheel responding significantly out-of-spec - magnitude and direction of torque icommand are correct, but torque output to spacecraft deviates from it all cucalized increase in infiction is part of lymbeller ottoining registral increase in infiction passing shall be a facility of the completely stop in from moving, of learning the completely stop in from moving. Of learning noting the completely stop in from moving of learning the complete stop in from moving of learning the complete stop in from moving of learning the complete stop in the complete s		a) If wheel is sluggish, it puts out less torque than commanded and may consume more power as the motor works to overcome bigger foss effects. b) If wheel is "energetic", it puts out more torque than commanded, unlikely usually it she tisses that are bigger than expected, if I puts out of the pu	 b) Turns may complete faster. c) Hard to predict without guessing at the nature of the erratic behavior. But if it's intermittent even at max torque, the other 3 wheels 	sensors detect the umbra violation it may not be correctable in the time	a) Possible if failed wheel is still considered available, but sidepends on monetum state of system when wheel failure occurs and timing of momentum dump logic and wheel is still considered available, but is still considered available, but sidepends on monetum state of system when wheel fault logic and wheel is still considered available, but depends on monetum state of system when wheel fault logic for momentum dump logic and wheel sall logic (to turn off misbehaving wheel) c) Unlikely in this case	2						
GC-41.g			Degraded force/torque exerted on spacecraft	1) Slight deviation in magnitude of torque, direction correct; leading to a sluggish system but not likely leading to any gross failure 2) When responding slightly not of-spec; 3) When friction than expected 3) Inhablance causing irregular rotation of flywhed; 3) Inhablance causing irregular rotation of flywhed; 6) Electric motor causing motor control actions to be just slightly off what is needed to get wheel to desired torque		Wheel takes longer to get to desired speed/forque; might consume more power in trying to get to commanded state	pointing accuracy	Science measurements possibly degraded (WISPR) if Inter requirements are violated. If offending wheel is disabled, will need momentur dumps more often, using more fuel	Probably not	2R		ground analysis, not on-board	May be able to detect something like this by long- term trending of wheel speed and torque assuming we get enough telemetry to the ground			

FMEA ID Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix	Time to Transmit	Response Desired System Response	Allocation of System	Time to fix system	Time to Transmit	Ground Response / Contingency	Quict System Side Processor Switch Switch	k Response Safe Mode	Remediation	Revisit
6C-4.1.a		Unable to exert force/forque on spacecraft (flywheel is not being scred on to maintain or change its spin; flywheel naturally spins sidown due to losses in the system (friction); flywheel is unable to rotate)					Signal		Proposes		Signal	Ground might attempt a power switch.			First action would be to switch sides (REM) for commanding of the wheels for just this wheel if we can do it on a per wheel basis) - sessing the falliers is in the commanders of the commanders	
6C41b		Case 1: incorrect force/torque exerted on spacecraft													For this case, we are assuming that the failed swheel is still actively rotating and not in the way the controlled commanded it to. The way the controlled commanded it to. The way the controlled commanded it to. The same of the control of the con	
6C-4.1.c		Case 2: Incorrect force/torque exerted on spacecraft														
GC41.d		Case 3: Incorrect force/forque exerted on spacecraft													Will do polarity tests pre-launch that should detect in-wiring or miscommunication in the second of	
GC41e		clase 4: Incorrect force/forque exerted on spacecraft														
GC-41.f		Case 5: Incorrect force/torque exerted on spacecraft														
GC-41g		Degraded force/torque exerted on spacecraft													Stop using the one wheel that's misbehaving assuming the other 3 wheels are still performing in spec. Will have to adjust control parameters to tune to the 3 wheels that are left.	

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

				à.			Effect							Detection Metho	d		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	TIm for Diagnosis	TIm Path for Diagnosis	Time to Detect ' (Local)	Time to Detect (System)
GC-4.1.h			Failure to output requested telemetry; output messages not generated	1) Permanent loss of tachometer data - cause depends on mechanism that wheel uses to irriday speed data. Calculation of wheel speed can be done in wheel isted or in light incharacter or similar data output by wheel salcometer. 2) loss of feetbask of songer or other health 8. status televiety - may only be loss of electronics - can't read data from internal source, can't correctly generate telemetry inessage, etc.			I) Incorrect estimate of wheel and system momentum. Might wait longer than we should to initiate a momentum dump. If the other 3 wheels still have sould speed estimates and we have valid angular rate estimate, we should be ok. 2) G&S coftware loses ability to detect some problems with the wheel.	No effect. G&C will have less data for long-term trending of wheel performance.		4		Yes	No wheel speed messages for some long period of time. No wheel telementy messages received for some long period of time.				
GC-4.1.i			Output telemetry contains insufficient measurements	3) Temporary loss of tachometer counts or wheel speed data - intermitten skips or repeats, born periods of no data - intermitten skips or 25 kips and apps in dechadax of torque or other health & status telemetry - may only be loss of monitor data, these data are not directly used in the control loop			the computation. Might initiate a dump when not needed or wait too long to initiate a dump if skipped counts cause wheel to appear to be rotating much faster or	Might do more momentum dumps than needed if errors in wheel speed estimate are not detected. More momentum dumps decreased science time and increase propellant usage (should have sufficient margin). J G&C will have less data for long-term trending of wheel	Unlikely - if too much time lapses between momentum dumps, the SLSes will see the Sun prior to umbra violation and safe the s/c.	4		Probably - depends on how the data loss manifests itself	GBC software will have checks on changes in wheel speed estimates, compared with previous speed and commanded torque. Gross jumps should be detected and flagged as errors.				
GC-4.1.j			Output telemetry contains incorrect measurements which are flagged valid	Tachometer outputs wrong signals/counts or incorrect wheel speed is output		None - wheel continues to respond to commands, it just deser't talk back every time it's expected to.	incorrect estimate of wheel and system momentum. Might initiate a dump when on needed or wait too long it initiate a dump if wheel appears to be rotating much faster or slower than it actually is	dumps than needed if errors in wheel speed estimate are not detected. More momentum dumps decreased		4							
GC-4.1.k			Higher friction in a wheel happens in combination with a side switch (for other reasons)			Wheel spins down due to side switch. Only a single wheel is affected by the friction, but all wheels are affected by the side switch.	Spacecraft turns (direction and speed depends on conditions at time of side switch).	Possibly mission-ending.	Possible, depending on where in orbit, how fast, and which direction it's turning.	1		No					
Inputs			Power			Wheel spins down.	OK due to margin with other three.	No effect.	N/A	4		Yes	- PDU current goes to 0 - Expect otuput data and acknowledge commands that aren't sent of SW should flag it and tell FSW.				
GC-4.3	Rx Wh 2 Rx Wh 3		Commands from TAC			Wheel would spin down if not commanded.	Controller will see attitude and rate errors and will try to get them to 0. FSW will re- command. Could switch to other TAC.	No effect.	N/A	4		Yes	Stop acknowledging commands.				
GC-4.4	Rx Wh 4		<u> </u>	.i	L	.l	i	i	i		i	İ			L	i.	

								Response Desired System Response						Quick	Response		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Continge	ency System Side Switch	Processor Switch	Safe Mode	Remediation	Revisit
GC-4.1.h			failure to output requested telemetry; output messages not generated													Switch to other side for wheel telementy interface to seel It elementy is restored. Power cycling the wheel could clear an electronics problem. May not help if the problem is internal to the wheel. Would not recommend anything other than side switd for no-board automore, change to propagate wheel speed from last valid estimate and torque commands. Might try turning off wheel, depending on lost telementy.	
GC-4.1.i			Output telemetry contains insufficient measurements													Switch to other side for wheel telemetry interface to see if telemetry is restored. Power cycling the wide could clear an electronic problem. May not help if the problem is internal to the wheel. Would not recommend anything other than side switch do not bear all actions. If error persists, might take wheel off-line.	
GC-4.1.j			Output telemetry contains incorrect measurements which are flugged valid													Power cycling the wheel could clear an electronics problem. May not help if the problem is internal to the wheel. Might try flight software charge to propagate wheel speed using forage commands: gingore remoneus telementy. Or might be possible to correct telementy if we can back out correct wheel speeds from ground analysis of telementry over long time periods. If error persists, might take wheel off-line.	
GC-4.1.k			Higher friction in a wheel happens in combination with a side switch (for other reasons)														
Inputs			Power														
			Commands from TAC														
GC-4.3	Rx Wh 2 Rx Wh 3 Rx Wh 4					ļ								<u> </u>			

Subject Matter Jack Ercol Notes: Initially filled out by Jack Ercol, but basically redone by HSSSS. Clay is talking to Expert(s): HSSSS contact HSSSS for updates/verification.

Expert(s):	HSSSS contact	HSSSS for updates/verification.					Effec	•		I	1		Detection Method		
FMEA ID	Name	Function	Failure Mode / Limit /	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable How Observed?	Tim for Diagnosis Tim Path for Diagn	osis Time to Detect (Local)	Time to Detect
TCS-ACCU-1	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed P2 gas charge that is applied between the bellows and the tank shell. Holds T3D in 3 min. of coolant; T3D p3g MDP; Bellows neutral position is T3D.	Constraint Cross-bellows Internal Leakage	1) Over stress (ext induced); 2) Contaminants induced; 3) Corrosion; 4) Fatigue; 5) Material/process (weld) flaw.	All	The bellows will extend to its neutral no-load position; interchanging and mixing of fluids between N2 and coolant cavities due to temperature excursions.	N2 bubbles getting into the coolant loop could cause cavitation of the active pump (items PM1/PM2). Decrease or loss of flow would lead to rise in loop temperatures and potential inability to meet solar array cooling needs.	would lead to loss ICS and	N/A	2		1) Pump delta-p sensor and/c current and temp sensors detect cavitation; 2) Loop temp sensors detect degraded cooling			(System)
TCS-ACCU-2	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and that has shell. Holds 3piled between the bellows and the tank shell. Holds 1D in 3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Coolant Leakage	1) Over stress (ext induced); 2) Corrosion; 3) Fatigue; 4) Material/process (weld) flaw.	All	Coolant leaks to external from the accumulator.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and mission.	N/A	2		1) Tank pressure and temperature sensors detect loss of coolant; 2) Pump delta-p sensor and/c current and temp sensors detect cavitation; 3) P2 detects loss of main loo pressure. 4) Loop temp sensors detect loss of cooling			
TCS-ACCU-3	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. Notice TBD in 3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Gas Leakage	(1) Over stress (ext induced); 2) Corrosion; 3) Fatigue; 4) Material/process (weld) flaw.	All	Gas leaks to external from the	Unable to maintain a net positive pump input pressure resulting in pump cavitation. Inability to provide thermal for expansion could result in bellows rupture.	loss of coolant due to rupture		2		1) Tank pressure sensor detects loss of pressurization 2) Pump delta-p sensor and/c current and temp sensors detect cavitation; 3) P2 detects loss of main loo pressurization; 4) Loop temp sensors detect loss of cooling			
TCS-ACCU-4	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed M2 gas charge that is applied between the bellows and the tank shell. Holds TBD In 3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	Fails to Expand/Contract	Jammed bellows (Interference of moving parts); Contamination.	All	inability to expand during high temp operation could cause bellows over pressure and potential rupture. inability to contract during low temp operation could cause pump cavitation.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavidation common cause or loss of coolant due to rupture would lead to loss TCS and mission.	N/A	2		1) Tank pressure and temperature sensors may detect pressure fluctuations due to temperature excursions; 2) Pump delta-p sensor and/current and temp sensors detect cavitation; 3) Loop temp sensors detect loss of cooling			
TCS-LV1-1	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Fails open	1) Contamination; 2) Seal failure; 3) FSW Failure; 4) Electrical/ Electronics failure; 5) Autonomy failure; 6) Failed sequence		Coolant would be allowed into the main loop before it is desired.	Coolant would freeze, potentially leading to rupture.	Rupture due to freezing results in loss of TCS and mission.	N/A	2		1) Tank pressure and temperature sensors may detect loss of coolant into the main loop; 2) Pump delta-p sensor and system pressure and temp sensors will all detect rupture resulting in loss of TCs.			
TCS-LV1-2	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	internal leakage (large leak)	1) Contamination; 2) Seal fallure	All		Sufficient coolant leaks into system to cause a blockage when it freezes, potentially leading to rupture.		N/A	2		1) Tank pressure and temperature sensors may detect loss of coolant into the main loop; 2) Pump delta-p sensor and system pressure and temp sensors will all detect rupture resulting in loss of TCs.			
TCS-LV1-3	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Internal leakage (small leak)	1) Contamination; 2) Seal failure	All	Coolant would be allowed into the main loop before it is desired.	Coolant leak is insufficient to block pipe when frozen. Frozen coolant would eventually melt with no damage to the system.	No effect.	N/A	4		Tank pressure and temperature sensors may detect loss of coolant into the main loop.			
TCS-LV1-4	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens	Valve stays closed when commanded to open	1) Contamination; 2) Jamming; 3) Binding; 4) Seal failure; 5) FSW Failure; 6) Electrical/ Electronics failure; 7) Autonomy failure; 8) Failed sequence	All	Valve stays closed.	Re-send command to open valve, but if failure persists, no coolant is available to the TCS.		N/A	2		1) Pump delta-p sensor detects loss of flow; 2) Loop temp sensors detect loss of cooling			
TCS-LV1-5	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Valve closes when not commanded to close	Mechanical failure (cannot be commanded to close after ground testing is completed)	All	Valve closes.	The system loses access to the accumulator, resulting in potential rupture or pump cavitation as a result of high/low temperature excursions, respectively.	Rupture due to high temperatures leads to loss of coolant, loss of TCS, and loss of mission. Pump cavitation due to low temperatures leads to pump failures, loss of TCS, and loss of mission.	N/A	2		1) Tank pressure and temperature sensors detect loss of cooland due to rupture 2) Pump delta-p sensor detects loss of flow; 3) Loop temp sensors detect loss of cooling			
TCS-LV1-6	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure		Coolant leaks to space.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2		1) Tank pressure and temperature sensors detect loss of coolant; 2) Pump delta-p sensor and/current and temp sensors detect cavitation; 3) P2 detects loss of main loo pressure; 4) Loop temp sensors detect loss of cooling			
TCS-LV1-7	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Position indicator indicates "closed" when valve is actually open	Sensor malfunction	All		Re-send open command (does not affect state of valve). Will see reduction in pressure in accumulator from fully-loaded position, and will see cooling to the solar arrays. Eventually will assume PI sensor failure.	No effect.	N/A	4		Accumulator pressure sensor sees drop in accumulator pressure The pressure 2) Temperature telemetry with show that system is operating.			
TCS-LV1-8	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Position indicator indicates "open" when valve is actually closed	Sensor malfunction	Launch through cooling system activation	Valve is closed, as	Will see no pressure drop at accumulator (expected if valve is open). Eventually will assume PI sensor failure.	No effect.	N/A	4		Accumulator pressure sensor does not detect drop in accumulator pressure.			
TCS-LV2-1	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on	Fails open	1) Contamination; 2) Seal failure; 3) FSW Failure; 4) Electrical/ Electronics failure; 5) Autonomy failure; 6) Failed sequence	From initial cooling system activation (radiators 1 & 4) through final cooling system activation (radiators 2 & 3)	Coolant would be allowed into the loop containing Radiators 2&3 before it is desired.		Rupture due to freezing results in loss of TCS and vehicle	N/A	2		Pump delta-p sensor and system pressure and temp sensors will all detect rupture resulting in loss of TCs.			

Subject Matter Jack Ercol Expert(s): HSSSS contact

Notes: Initially filled out by Jack Ercol, but basically redone by HSSSS. Clay is talking to HSSSS for updates/verification.

	HSSSS contact	HSSSS for updates/verification.							Response						Quick Response			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signa		Allocation of System Respons	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Processor Switch	Safe Mode	Remediation	Revisit
TCS-ACCU-1	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed P2 gas charge that is applied between the bellows and the tank shell. Holds T8D In alm. of coolant; T8D psig MDP; Bellows neutral position is TBD.	Cross-bellows Internal Leakage	Seconds/minutes					N/A	None							Historically this has been an accepted risk in similar spaceflight applications, based on it's a highly reliable all welded pressure barrier metal beliow assembly design, rigourous design stress analyses, manufacturing process controls, mandatory hardware inspection points, and qual/accept tests.	
TCS-ACCU-2	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. Holds TBD In3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Coolant Leakage	Seconds/minutes					N/A	None								
TCS-ACCU-3	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. Holds TBD In3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Gas Leakage	Seconds/minutes					N/A	None								
TCS-ACCU-4	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. Holds TBD In a min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	Fails to Expand/Contract	Seconds/minutes					N/A	None								
TCS-LV1-1	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following bunch to allow coolant into radiators 1 and 4 and solar arrays.	Fails open	Minutes					N/A	None								
TCS-LV1-2	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Internal leakage (large leak)	Minutes					N/A	None								
TCS-LV1-3	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Internal leakage (small leak)	Minutes (depends on severity of leak)					N/A	None								
TCS-LV1-4	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Valve stays closed when commanded to open	Minutes					N/A	None							Redundant, independent opening electronics. This would require two failures.	
TCS-LV1-5	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following bunch to allow coolant into radiators 1 and 4 and solar arrays.	Valve closes when not commanded to close	Minutes					N/A	None								
TCS-LV1-6	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	External leakage	Seconds/minutes					N/A	None								
TCS-LV1-7	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Position indicator indicates "closed" when valve is actually open															
TCS-LV1-8	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Position indicator indicates "open" when valve is actually closed															
TCS-LV2-1	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails open	Minutes					N/A	None							Can adjust vehicle orientation to prevent freezing	

FMEA ID	Name	Function	Failure Mode / Limit /	Possible Causes	Phase	Local	Effer Next Higher	ct Mission	Umbra Violation	Severity	Type of FM	Observable How Observed		ion Method TIm Path for Diagnosis	Time to Detect (Local)	Time to Detect
	Name	runcuon	Constraint	rossible causes	Filase	Local	Next Higher	Wilsou	Ollibra violation	Severity	Type of Five	1) Tank pressure and	Till for Diagnosis	illi Fatti toi Diagnosis	Time to Detect (Local)	(System)
TCS-LV2-2	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	internal leakage (large leak)	1) Contamination; 2) Seal failure	From initial cooling system activation (radiators 1 & 4) through final cooling system activation (radiators 2 & 3)	the loop containing Radiators	Sufficient coolant leaks into system to cause a blockage when it freezes, potentially leading to rupture.		N/A	2		temperature sensors of temperature sensors re detect loss of coolant main loop; 2) Pump detta-p senso system pressure and t sensors will all detect resulting in loss of TCS	nto the and mp upture			
TCS-LV2-3	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	internal leakage (small leak)	1) Contamination; 2) Seal failure	From initial cooling system activation (radiators 1 & 4) through final cooling system activation (radiators 2 & 3)	Coolant would be allowed into the loop containing Radiators 2&3 before it is desired.		No effect.	N/A	4		Tank pressure and temperature sensors r detect loss of coolant main loop.				
TCS-LV2-4	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Valve stays closed when commanded to open	1) Contamination; 2) Jamming, 3) Binding; 4) Seal failure; 5) FSW Failure; 6) Electrical/ Electronics failure; 7) Autonomy failure; 8) Failed sequence	From final cooling system activation (radiators 2 & 3) on.	Valve stays closed.	Re-send command to open valve, but if failure persists, no coolant is available to radiators 2 & 3.	Loss of TCS. Loss of mission.	N/A	2		1) Pump delta-p senso detects loss of flow; 2) Loop temp sensors loss of cooling 3) Position indicator o indicates closed state	letect			
TCS-LV2-5	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Valve closes when not commanded to close	Mechanical failure (cannot be commanded to close after ground testing is completed)		Valve closes.	The system loses access to Radiator 2 & 3.	S Loss of TCS. Loss of mission.	N/A	2		1) Pump delta-p senso detects loss of flow; 2) Loop temp sensors loss of cooling 3) Position indicator o indicates closed state	letect			
TCS-LV2-6	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	From initial cooling system activation (radiators 1 & 4) on.	Coolant leaks to space.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	1	2		1) Tank pressure and temperature sensors closs of coolant; 2) Pump delta-p sensor current and temp sens detect exhatation; 3) PZ detects loss of m pressure; 4) Loop temp sensors loss of cooling.	and/or ors ain loop			
TCS-LV2-7	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Position indicator indicates "closed" when valve is actually open	Sensor malfunction	From final cooling system activation (radiators 2 & 3) on.	Valve is open, as commanded	Re-send open command (does not affect state of valve). Will see reduction in pressure in accumulator, and will see additional cooling to solar arrays. Eventually will assume a PI sensor failure.	No effect.	N/A	4		Accumulator pressus sensor sees drop in accumulator pressure Temperature telem show that system is of	try will			
TCS-LV2-8	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Position indicator indicates "open" when valve is actually closed	Sensor malfunction	Launch through final cooling system activation (radiators 2 & 3)	Valve is closed, as commanded.	No effect until initial cooling system activation (Radiators 1 & 4). At initi cooling system activation, will see that the temperatures surrounding Radiators 2 & 3 do not change. Will eventually assuming a PI sensor failure.	al No effect.	N/A	4		Accumulator pressure does not detect drop i accumulator pressure.				
TCS-LV3-1	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails open/Internal leakage	1) Contamination; 2) Seal failure; 3) Software Failure; 4) Electrical/ Electronics failure	All	Coolant may be allowed into the radiator 2/3 segment of the cooling loop before it is desired.	Potential coolant freezing, potentially leading to rupture and subsequent leakage.	Rupture due to freezing results in loss of TCS and vehicle	N/A	2		P3 detects pressure ris coolant leaks in	e as			
TCS-LV3-2	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails closed	1) Contamination; 2) Jamming; 3) Binding; 4) Seal failure; 5) Software Failure; 6) Electrical/ Electronics failure	All	Valve doesn't open when commanded, or valve closes inadvertently.	Loss of flow to radiators 2 and 3.	Inability to supply coolant to radiators 2 and 3 results in inability to handle nominal heat loads, which eventually leads to loss of vehicle when the TCS can no longer keep		2		Loop temp sensors de failure to supply flow t radiators 2 and 3.				
TCS-LV3-3	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage, upstream side	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	All	Coolant leaks to external from the downstream side of the valve beginning when LV2 and LV3 are opened.		Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	•	2		1) Tank pressure and temperature sensors colors of colonal rafer I/ been opened; 2) Pump deta-p senso current and temp sens detect cavitation; 3) PZ detects loss of m pressure. 4) Loop temp sensors loss of cooling	2 has r and/or ors ain loop			
TCS-LV3-4	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 or the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage, downstream side	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	!		Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2		1) Tank pressure and temperature senors costs of coolant after LV been opened; 2) Pump delta-p senso current and temp sendetect cavitation; 3) P2 detects loss of m pressure. [4) Loop temp sensors	1 has and/or ors ain loop			
TCS-CV1-1	Pump check valve	Check valve prevents back flow through the inactive pump leg	internal Leakage	1) Ball/seat deformation; 2) Contamination	All	Some coolant recirculation flow is allowed through the check valve.	Degraded flow performance through the solar arrays and radiators.	If the leakage is severe enough, then inability to h handle nominal heat loads is possible, leading to loss of vehicle when the TCS can no longer keep up.	N/A	2		loss of cooling 1) Pump delta-p senso detects flow degradat 2) Loop temperature s detect degraded cooli performance	on; ensors			
TCS-CV1-2	Pump check valve	Check valve prevents back flow through the inactive pump leg	Fails in PM1 flow position	1) Ball/seat deformation; 2) Contamination	All	Check valve is stuck blocking flow through the PM2 leg	Running PM2 results in a dead head condition. Unable to use PM2 to provide flow.		N/A	2R		1) Pump delta-p senso detects loss of flow wh is running; 2) PM2 current and sp sensors detect dead h condition; 3) Loop temperature s detect loss of cooling; PM2 is active.	eed ad ensors			
TCS-CV1-3	Pump check valve	Check valve prevents back flow through the inactive pump leg	Fails in PM2 flow position	1) Ball/seat deformation; 2) Contamination	All	Check valve is stuck blocking flow through the PM1 leg	Running PM1 results in a dead head condition. Unable to use PM1 to provide flow.	Loss of pump redundancy. If next failure is PM2, then loss of TCS and vehicle.	N/A	2R		1) Pump delta-p senso detects loss of flow wh is running; 2) PMI current and sp sensors detect dead h condition; 3) Loop temperature s detect loss of cooling if PMI is active.	eed ad ensors			

								Response						Quick Response			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	ocation of Local Response	Time to fix locally	Time to Transmit Signal		Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Processor Switch	Safe Mode	Remediation	Revisit
TCS-LV2-2	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Internal leakage (large leak)	Minutes				N/A	None							Can adjust vehicle orientation to prevent freezing	
TCS-LV2-3	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Internal leakage (small leak)	Minutes				N/A	None							Can adjust vehicle orientation to prevent freezing	
TCS-LV2-4	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Valve stays closed when commanded to open	Minutes													
TCS-LV2-5	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Valve closes when not commanded to close	Minutes													
TCS-LV2-6	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage	Seconds/minutes													
TCS-LV2-7	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Position indicator indicates "closed" when valve is actually open														
TCS-LV2-8	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Position indicator indicates "open" when valve is actually closed					N/A	None								
TCS-LV3-1	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails open/Internal leakage	Minutes				N/A	None							Can adjust vehicle orientation to prevent freezing	
TCS-LV3-2	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails closed	Minutes				N/A	None								
TCS-LV3-3	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage, upstream side	Seconds/minutes				n/A	None								
TCS-LV3-4	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage, downstream side	Seconds/minutes				n/A	None								
TCS-CV1-1	Pump check valve	Check valve prevents back flow through the inactive pump leg	internal Leakage	Minutes				N/A	None								
TCS-CV1-2	Pump check valve	Check valve prevents back flow through the inactive pump leg	Fails in PM1 flow position	Seconds (after PM2 is commanded)				n/A	None								
TCS-CV1-3	Pump check valve	Check valve prevents back flow through the inactive pump leg	Fails in PM2 flow position	Seconds (after PM1 is commanded)				n/A	None								

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effec Next Higher	ct	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection TIm for Diagnosis	Method Tim Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
TCS-CV1-4	Pump check valve	Check valve prevents back flow through the inactive pump leg	External Leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	All	Coolant leaks to external beginning when LV1 is opened post launch.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.		2			1) Tank pressure and temperature sensors detect loss of coolant after LV1 has been opened; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) PZ detects loss of main loop pressure. 4) Loop temp sensors detect				(Opening)
TCS-PM1-1	Pump 1	Provides coolant flow through the solar arrays and radiators	Overspeed/Excessive flow	1) Motor Controller Electronics failure; 2) Software Failure	All		Waste of vehicle power, potential cooling performance degradation	If the degradation is severe enough, then inability to handle nominal heat loads is possible, leading to loss of vehicle when the TCS can no longer keep up. Can switch to the redundant pump to avoid this.	0	2R			lioss of cooling 1) Pump delta-p sensor detects excessive flow; 2) Pump current sensor detects excessive current draw; 3) Loop temperature sensors detect degraded cooling performance				
TCS-PM1-2	Pump 1	Provides coolant flow through the solar arrays and radiators	Underspeed/insufficient flow delta-p	1) Motor controller electronics failure; 2) Software failure; 3) Bearing failure; 4) Excessive internal leakage; 5) Loose impeller; 6) Entrapped contaminants	All		Degraded flow performance through the solar arrays and radiators	if the degradation is severe enough, then inability to handle nominal heat loads is possible, leading to loss of vehicle when the TCS can no longer keep up. Can switch to the redundant pump to avoid this.	0	2R			1) Pump delta-p sensor detects flow degradation; 2) Loop temperature sensors detect degraded cooling performance				
TCS-PM1-3	Pump 1	Provides coolant flow through the solar arrays and radiators	Locked rotor	Excessive bearing wear or contamination resulting in increased bearing drag or seizure; 2) Binding	All	Loss of coolant flow. Pump should be safe with regard to current indefinitely (TBC)	No coolant flow through the solar arrays and radiators	Must switch to the redundant pump to resume cooling. If the redundant pump also fails then loss of TCS and vehicle.	•	2R			1) Pump delta-p sensor detects loss of flow; 2) Pump current sensor detects current draw characteristic of a locked rotor event; 3) Loop temperature sensors detect degraded cooling				
TCS-PM1-4	Pump 1	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	Pump cavitations; 2) Flow blockage; 3) High heat load/environment; 4) High coolant temp; 5) Bearing degradation	All	Potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment		??	2			performance Loop temp sensors may provide an indirect indication that the pump is overheating				
TCS-PM1-5	Pump 1	Provides coolant flow through the solar arrays and radiators	Overcurrent	1) Electronics failure; 2) Bearing drag	All	Local heating, potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment	Potential loss of TCS and vehicle	??	2			Pump current sensor and vehicle level overcurrent protection features (TBD) will catch many overcurrent scenarios in time to allow for pump shutdown				
TCS-PM1-6	Pump 1	Provides coolant flow through the solar arrays and radiators	Fails on	1) Motor Controller Electronics failure; 2) Software Failure	All	Pump is on when not expected to be on	Waste of vehicle power, potential cooling performance degradation	If the degradation is severe enough, then inability to handle nominal heat loads is possible, leading to loss of vehicle when the TCS can no longer keep up. Can switch off the redundant pump to restore normal flow.	N/A	2R			1) Pump delta-p sensor detects irregular flow; 2) Pump current sensor detects current from inactive pump; 3) Loop temperature sensors detect degraded cooling performance				
TCS-PM1-7	Pump 1	Provides coolant flow through the solar arrays and radiators	Fails off	1) Motor Controller Electronics failure; 2) Software Failure	All	Loss of coolant flow	No coolant flow through the solar arrays and radiators	Must switch to the redundant pump to resume cooling. If the redundant pump also fails then loss of TCS and vehicle.		2R			1) Pump delta-p sensor detects loss of flow; 2) Pump current sensor detects no current draw; 3) Loop temperature sensors detect loss of cooling				
TCS-PM1-8	Pump 1	Provides coolant flow through the solar arrays and radiators	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	All	Coolant leaks to external from the pump beginning when LV1 is opened post launch.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	4	2			Tank pressure and temperature sensors detect loss of coolant after LV1 has been opened; Pump delta-p sensor and/or current and temp sensors detect cavitation; P2 detects loss of main loop pressure. Lloop temp sensors detect loss of cooling				
TCS-PM2-1	Pump 2	Provides coolant flow through the solar arrays and radiators	Overspeed/Excessive flow	1) Motor Controller Electronics failure; 2) Software Failure	All	Pump outputs excessive flow and draws excessive current	Waste of vehicle power, potential cooling performance degradation	If the degradation is severe enough, then inability to handle nominal heat loads is possible, leading to loss of vehicle when the TCS can no longer keep up. Can switch to the redundant pump to avoid this.	0	2R			1) Pump delta-p sensor detects excessive flow; 2) Pump current sensor detects excessive current draw; 3) Loop temperature sensors detect degraded cooling performance				
TCS-PM2-2	Pump 2	Provides coolant flow through the solar arrays and radiators	Underspeed/insufficient flow delta-p	1) Motor controller electronics failure; 2) Software failure; 3) Bearing failure; 4) Excessive internal leakage; 5) Loose impeller; 6) Entrapped contaminants	All	Pump outputs insufficent flow delta-p	Degraded flow performance through the solar arrays and radiators	If the degradation is severe enough, then inability to handle nominal heat loads is possible, leading to loss of vehicle when the TCS can no longer keep up. Can switch to the redundant pump to avoid this.	0	2R			Pump delta-p sensor detects flow degradation; Loop temperature sensors detect degraded cooling performance				
TCS-PM2-3	Pump 2	Provides coolant flow through the solar arrays and radiators	Locked rotor	Excessive bearing wear or contamination resulting in increased bearing drag or seizure; 2) Binding	All	Loss of coolant flow. Pump should be safe with regard to current indefinitely (TBC)	No coolant flow through the solar arrays and radiators	Must switch to the redundant pump to resume cooling. If the redundant pump also fails then loss of TCS and vehicle.	1	2R			Pump delta-p sensor detects loss of flow; Pump current sensor detects current draw characteristic of a locked rotor event; J toop temperature sensors detect degraded cooling				
TCS-PM2-4	Pump 2	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	1) Pump cavitations; 2) Flow blockage; 3) High heat load/environment; 4) High coolant temp; 5) Bearing degradation	All	Potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment		??	2			performance Loop temp sensors may provide an indirect indication that the pump is overheating				
TCS-PM2-5	Pump 2	Provides coolant flow through the solar arrays and radiators	Overcurrent	1) Electronics failure; 2) Bearing drag	All	Local heating, potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment		??	2			Pump current sensor and vehicle level overcurrent protection features (TBD) will catch many overcurrent scenarios in time to allow for pump shutdown				

								Response						Quick Response			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response Allocation of Local Response	Time to fix locally	Time to Transmit Signa		Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Processor Switch	Safe Mode	Remediation	Revisit
TCS-CV1-4	Pump check valve	Check valve prevents back flow through the inactive nump leg	External Leakage	Seconds/minutes				N/A	None								
TCS-PM1-1	Pump 1	Provides coolant flow through the solar arrays and radiators	Overspeed/Excessive flow	Minutes				N/A	None								
TCS-PM1-2	Pump 1	Provides coolant flow through the solar arrays and radiators	Underspeed/insufficient flow delta-p	Minutes				N/A	None								
TCS-PM1-3	Pump 1	Provides coolant flow through the solar arrays and radiators	Locked rotor	Seconds				N/A	None								
TCS-PM1-4	Pump 1	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	Minutes				N/A	None								х
TCS-PM1-5	Pump 1	Provides coolant flow through the solar arrays and radiators	Overcurrent	Seconds				N/A	None								х
TCS-PM1-6	Pump 1	Provides coolant flow through the solar arrays and radiators	Fails on	Seconds				N/A	None								
TCS-PM1-7	Pump 1	Provides coolant flow through the solar arrays and radiators	Fails off	Seconds				N/A	None								
TCS-PM1-8	Pump 1	Provides coolant flow through the solar arrays and fradiators	External leakage	Seconds/minutes				N/A	None								
TCS-PM2-1	Pump 2	Provides coolant flow through the solar arrays and radiators	Overspeed/Excessive flow	Minutes				N/A	None								
TCS-PM2-2	Pump 2	Provides coolant flow through the solar arrays and radiators	Underspeed/Insufficient flow delta-p	Minutes				N/A	None								
TCS-PM2-3	Pump 2	Provides coolant flow through the solar arrays and radiators	Locked rotor	Seconds				N/A	None								
TCS-PM2-4	Pump 2	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	Minutes				N/A	None								х
TCS-PM2-5	Pump 2	Provides coolant flow through the solar arrays and radiators	Overcurrent	Seconds				N/A	None								х
													i				

							Effec	t						Detection	Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	TIm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
TCS-PM2-6	Pump 2	Provides coolant flow through the solar arrays and radiators	Fails on	1) Motor Controller Electronics failure; 2) Software: All Failure		Pump is on when not expected to be on	Waste of vehicle power, potential cooling performance degradation	If the degradation is severe enough, then inability to handle nominal heat loads is noossible, leading to loss of vehicle when the TCS can no longer keep up. Can switch off the redundant pump to restore normal flow.	N/A	2R			Pump delta-p sensor detects irregular flow; Pump current sensor detects current draw from inactive pump; Jupp temperature sensors detect degraded cooling performance				
TCS-PM2-7	Pump 2	Provides coolant flow through the solar arrays and radiators	Fails off	1) Motor Controller Electronics failure; 2) Software All Failure		Loss of coolant flow	No coolant flow through the solar arrays and radiators	Must switch to the redundant pump to resume cooling. If the redundant pump also fails, then loss of TCS and vehicle.	N/A	2R			1) Pump delta-p sensor detects loss of flow; 2) Pump current sensor detects no current draw; 3) Loop temperature sensors detect loss of cooling				
TCS-PM2-8	Pump 2	Provides coolant flow through the solar arrays and radiators	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure		Coolant leaks to external from the pump beginning when LV: is opened post launch.		Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant after IV1 has been opened; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				
TCS-MV-1	Manual fill valve	Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant leakage to exterior.	Fails open/Internal leakage	1) Contamination; 2) Seal failure; 3) Software Failure; 4) All Electrical/ Electronics failure		Coolant leaks through the manual valve	No effect while the line is capped	No effect. If the cap also fails, then loss of coolant leading to loss of TCS and vehicle	N/A	2R			First failure undetectable while line is capped. If the cap also fails, then: 1) Tank pressure and temperature sensors detect loss of coolant; 2) Pump delta-p sensor and/or current and temp sensors detect cathodistion; 3) P2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				
TCS-MV-2	Manual fill valve	Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant leakage to exterior.	Fails closed	1) Contamination; 2) Jamming; 3) Binding; 4) Seal failure; 5) Software Failure; 6) Electrical/ Electronics failure		Unable to fill through the manual valve	Can't fill the accumulator pre-launch	Mission delay	N/A	4			N/A				
TCS-MV-3	Manual fill valve	Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant leakage to exterior.	External leakage, tank side	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure		Coolant leaks to external from the manual valve	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of colant would lead to loss TCS and vehicle.	N/A	2			Tank pressure and temperature sensors detect loss of coolant; Pump delta-p sensor and/or current and temp sensors detect cavitation; To 2 detects loss of main loop pressure. To 2 detects loss of sensors detect loss of cooling				

									Response						Quick Response		1	
FMEA ID	Name	Function	Failure Mode / Limit /	Response Level	Desired Local Response	Allocation of Local	Time to fix locally	Time to Transmit Signal	Desired System	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response /	System Side Switch	Processor Switch	Safe Mode	Remediation	Revisit
TCS-PM2-6	Pump 2	Provides coolant flow through the solar arrays and radiators	Constraint Fails on	Seconds		Response			Response N/A	None			Contingency					
TCS-PM2-7	Ритр 2	Provides coolant flow through the solar arrays and radiaturs	Fails off	Seconds					N/A	None								
TCS-PM2-8	Pump 2	Provides coolant flow through the solar arrays and radiators	External leakage	Seconds/minutes					N/A	None								
TCS-MV-1	Manual fill valve	Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant leakage to exterior.	Fails open/internal leakage	Minutes					N/A	None								
TCS-MV-2	Manual fill valve	Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant leakage to exterior.	Fails closed	Seconds					N/A	None								
TCS-MV-3		Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant leakage to exterior.		Seconds/minutes					N/A	None								

Subject Matter Dave Copeland Expert(s): (Telecomm) Components are listed for completeness, but failure mode chris Haskins (FR) and FMEA information is only displayed in the first copy of

	Chris Haskins (FR)	and three information is only	displayed in the first copy of				Eff	ect						Detection Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis Tlm Pa Diagr		ect Time to Detect (System)
TM-1 TM-1.1	Transponder			ļ											((C)CICINI)
TM-1.1 TM-1.1.1	FR A Power Converter															
TM-1.1.1.a			Overcurrent (in power converter or one of its loads)	1). SEU 2) Hard circuit failure 3) Both exciters on		Depends on the severity of the overcurrent. Ranges from no effect to unrecoverable failure of FR A.		No effect.	N/A	2R	Active	Yes	FR A would go down. Loss of telemetry, timing, etc. Loss of comm if in contact with ground. PDU would detect overcurrent condition.	PDU tim for FR A current	N/A	?
TM-1.1.1.b			Hard failure	1) Component failure 2) Overcurrent		Transponder A shuts down.	Might blow fuse to FR A. Switch to B-side of telecomm. No other effect.	No effect.	N/A	2R	Active	Yes	FR A would go down. Loss of telemetry, timing, etc. Loss of comm if in contact with	Heartbeat from FR 7	n/a	?
			Out of regulation secondary	1) Overcurrent		Ranges from negligible to hard	worst case: switch to RF side B						ground. Analyze downlink telemetry	Trending by RF		
TM-1.1.1.c		<u> </u>	voltage	Circuit-level failure anywhere in radio		failure of radio.	(would lose heart beat)	No effect.	N/A	2R	None	Yes, with human-in-the-loop	(long-term trending)	team	N/A	N/A
Inputs			28V and return (applies to whole radio)			Radio down	Switch to RF side B			4						
TM-1.1.2	Spacecraft Interfaces (except power)															
TM-1.1.2.1		Spacewire														
TM-1.1.2.1.a			No/out-of-tolerance output	Hardware failure (broken harness, pin, or circuit failure)		Radio could not be configured for different modes of operation. Couldn't send downlink telemetry. Uplink data stream would be lost on non-critical virtual channels.	S/C wouldn't receive uplink data stream, request for downlink data, configuration data, status data. Would do RF side switch first to see if it corrects the problem, followed by an avionics side switch.	No effect.	N/A	4	None	yes	Ground might notice an issue with the frames repeating or being empty, indicates that radio works, but no data is coming down - router status, error message, bad command counts. Autonomy could checi run state to see if FSW, etc. is responding (command loss timer, etc.)			
TM-1.1.2.1.b			Corrupt data (both to and fron the radio)	FPGA, logic or clock failure		Radio could not be configured for different modes of operation. Couldn't send downlink telemetry. Uplink data stream would be lost on non-critical virtual channels.	downlink data, configuration data, status data. Could clog up SpaceWire at s/c level.	No effect.	N/A	4	None	yes	Ground might notice an issue with the frames repeating or being empty, indicates that radio works, but no data is coming down - bad command counts, CRC error			
TM-1.1.2.2.a		JART (output)	No/out-of-tolerance output	Hardware failure (broken harness, pin, or circuit failure)		No critical commands	Would likely follow common response to CLT timeout - soft reset of radio, power cycle to radio, side switch of RF, then sideswitch of avionics.	No effect.	N/A	4	Active	yes	CLT will expire. CCD commands are only sent durin ground contact (failure of commands will be seen in trending). No autonomous reaction.	Ground - loss of signal/lock CLT not tickled	?	N/A
TM-1.1.2.2.b			Corrupt data	FPGA, logic or clock failure		No critical commands	Would likely follow common response to CLT timeout - soft reset of radio, power cycle to radio, side switch of RF, then sideswitch of avionics.	No effect.	N/A	4	Active	yes	CLT will expire. CCD commands are only sent durin ground contact (failure of commands will be seen in trending). No autonomous reaction.	Ground - loss of signal/lock CLT not tickled	?	N/A
TM-1.1.2.3		Clock (output)		Hardware failure (broken		Avionics would detect the				-			Lack of clock from transponder			
TM-1.1.2.3.a			No/out-of-tolerance output	harness, pin, or circuit failure)		failure of the clock output.	Switch to side B of RF.	No effect.	N/A	2R	Active	yes	Would not affect RF.	Clock output RF to REM	?	N/A
TM-1.1.2.3.b			Corrupt data	FPGA, logic or clock failure		Avionics would detect the failure of the clock output.	Switch to side B of RF.	No effect.	N/A	2R	Active	yes	Lack of clock from transponder Would not affect RF.	Clock output RF to REM	?	N/A
TM-1.1.2.4		Baseband		<u> </u>		ļ			ļ					‡		
TM-1.1.2.4.a			No/out-of-tolerance output	Hardware failure (broken harness, pin, or circuit failure)		Not used in flight.	If baseband enable receiving failed (so s/c is expecting commanding via baseband instead of RF), at CLT timeout, could force s/c to ignore baseband and use RF command path instead.	No effect,	N/A	4	Active	yes	CLT expires, no commands coming through RF.	Ground - loss of signal/lock CLT not tickled	?	N/A
TM-1.1.2.4.b			Corrupt data	FPGA, logic or clock failure		Not used in flight.	If baseband enable receiving failed (so s/c is expecting commanding via baseband instead of RP), at CLT timeout, could force s/c to ignore baseband and use RF command path instead.	No effect,	N/A	4	Active	yes	CLT expires, no commands coming through RF.	Ground - loss of signal/lock CLT not tickled	?	N/A
TM-1.1.2.4		MET Synch												-		
TM-1.1.2.4.a			No/out-of-tolerance output	Hardware failure (broken harness, pin, or circuit failure)		Ground use only	No effect.	No effect.	N/A	4	None	N/A				
TM-1.1.2.4.b	X-Band Rx (function -		Corrupt data	FPGA, logic or clock failure		Ground use only	No effect.	No effect.	N/A	4	None	N/A		-		
TM-1.1.3	includes at least two	1	1	1												

Subject Matter Dave Copeland Expert(s): (Telecomm) Components are listed for completeness, but failure mode chris Haskins (FR) and FMEA information is only displayed in the first copy of

FMEA ID	Name	Function	Failure Mode / Limit /	Response Level	Desired Local Response	Allocation of Local	Time to fix locally	Time to Transmit	Desired System		Time to fix system			System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation
<i>N</i> -1	Transponder	1	Constraint			Response		Signal	Response	System Response		Signal	Contingency				
Л-1 Л-1.1	FR A			<u> </u>				<u> </u>			<u> </u>				i i		<u> </u>
l-1.1.1	Power Converter	<u> </u>		<u>. </u>		<u> </u>	<u> </u>	<u> </u>			. 	ļ		İ	ļļ		
M-1.1.1.a			Overcurrent (in power	Local	Power cycle radio and if condition still exists power down radio and re-enforce other side? Question on how to implementlimit power cycle rule fire count and use longer persistence for side switch rule?	Autonomy	N/A	~1 sec (next telemetry status	None	None	None	None	,				ARC cycles power to converter, avionics would need to redirect signal through switching matrix to switch to side B.
V-2.2.2.0			converter or one of its loads)		If the radio is overcurrent, I would think we would do an RF side switch rather than power cycling? Does radio have CB and fuse?			packet from radio)									Switching is done through the ARC, but autonomy would detect a fault and then tell ARC to power cycle or power off
И-1.1.1.b			Hard failure	Local	RF Side Switch	Autonomy	N/A	~1 sec (next telemetry status packet from radio)	None	None	None	None	?				
M-1.1.1.c			Out of regulation secondary voltage	Local?	None	None/Ground?	?		None	None	None	?	Contingency proc needed?				Reduce operating temperature range, optimize bus voltage.
Inputs	<u> </u>		28V and return (applies to	<u></u>				<u> </u>									
	Spacecraft Interfaces		whole radio)	<u> </u>													
TM-1.1.2	(except power)														j j		
TM-1.1.2.1		Spacewire											RF side switch, then avionics				
TM-1.1.2.1.a			No/out-of-tolerance output	None	None	Ground?							side switch (is avionics side switch different from system side switch?)				Power cycle, switch to side B
M-1.1.2.1.b			Corrupt data (both to and from the radio)	¹ None	None	Ground?							RF side switch, then avionics side switch (is avionics side switch different from system side switch?)				Power cycle, soft reset
TM-1.1.2.2		UART (output)											Ground contingency to				
ГМ-1.1.2.2.а			No/out-of-tolerance output	Local/System	Power cycle FR, RF side switch? Possible system side switch? Could use 2 CLTs, first to power cycle	Autonomy			Depending on how CLT implemented 2nd CLT might be used for system side switch	Autonomy	?	?	reacquire SC Need to talk through all the combinations within RF system that ground should try when attempting to reacquire	Maybe?			
M-1.1.2.2.b			Corrupt data	Local/System	Power cycle FR, RF side switch? Possible system side switch? Could use 2 CLTs, first to power	Autonomy			Depending on how CLT implemented 2nd CLT might be used for system	Autonomy	?	?	Ground contingency to reacquire SC Need to talk through all the combinations within RF system	Maybe?			
					cycle				side switch				that ground should try when attempting to reacquire				
M-1.1.2.3 M-1.1.2.3.a		Clock (output)	No/out-of-tolerance output	Local	RF side switch	Autonomy	?	?	None	None	None	None	None				
M-1.1.2.3.b			Corrupt data	Local	RF side switch	Autonomy	?	?	None	None	None	None	None		ļ		
M-1.1.2.4		Baseband												<u> </u>			
					Power cycle FR, RF side switch? Possible system side switch?				Depending on how CLT implemented				Ground contingency to reacquire SC				
M-1.1.2.4.a			No/out-of-tolerance output	Local/System	Part of CLT response should include re-enforcing RF Could use 2 CLTs, first to power cycle	Autonomy			2nd CLT might be used for system side switch	Autonomy	?	?	Need to talk through all the combinations within RF system that ground should try when attempting to reacquire	Maybe?			
					Power cycle FR, RF side switch? Possible system side switch?				Depending on how CLT implemented				Ground contingency to reacquire SC				
ΓM-1.1.2.4.b			Corrupt data	Local/System	Part of CLT response should include re-enforcing RF Could use 2 CLTs, first to power	Autonomy			2nd CLT might be used for system side switch	Autonomy	?	?	Need to talk through all the combinations within RF system that ground should try when attempting to reacquire	Maybe?			
		MET Synch			cycle								. • • • • • • • • • • • • • • • • • • •				
TM-1.1.2.4						<	. (·		·····	. A						
			No/out-of-tolerance output														
TM-1.1.2.4 FM-1.1.2.4.a FM-1.1.2.4.b			No/out-of-tolerance output Corrupt data														

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	fect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Method	Tim Path for	Time to Detect	Time to Detect
TM-1.1.3.a			Locks up/resets (probably wouldn't happen at the card level)	1) SEU 2) Component failure		No critical commands	Switch to side B of RF.	No effect.	N/A	2R	FM	yes	CLT will expire. CCD commands are only sent durir ground contact (failure of commands will be seen in trending). No autonomous reaction.	B Heartbeat from FR; FR reset type	Diagnosis	(Local)	(System)
TM-1.1.3.b			Hard failure	1) Component failure		Transponder A shuts down.	Switch to B-side of telecomm. No other effect.	No effect.	N/A	2R	Active	Yes	FR A would go down. Loss of telemetry, timing, etc. Loss of comm if in contact with ground.	Heartbeat from FR		N/A	N/A
TM-1.1.3.c			Failure to acquire	1) Component failure 2) Radiation effects		Status telemetry would indicate loss of signal/lock	Ground would try to reacquire s/c. Eventually CLT would timeout. Would switch to side for telecomm. Would likely follow common response to CLT timeout - soft reset of radio, power cycle to radio, is deswitch of RF, then sideswitch of avionics. Decision-maker would depend on phase of mission. C&DH does the actual switching. Might need to retransmit any upload in progress.	None.	if ground is unable to uplink to s/c, a stale ephemeris could lead to UV. CLT should timeout prior to this happening and s/c should "safe."	t 3	Active	Yes	S/c would know that it didn't acquire an uplink signal. If in contact with ground, FCs wou notice failure to acquire.	Ground - loss of signal/lock d CLT not tickled		?	w/A
TM-1.1.3.d			Failure to detect commands	1) Component failure 2) Radiation effects 3) Failure to acquire		No critical commands, althoug there would be signal lock with ground.	Ground would try to reaquire s/c. Eventually CLT would itmeout. Would likely follow common response to CLT itmeout - soft reset of radio, abover cycle to radio, side switch of RF, then sideswitch of avionics. Decision-maker would depend on phase of mission. C&DH does the actual switching. Might need to retransmit any upload in progress.		if ground is unable to uplink to is/c, a stale ephemeris could lead to UV. CLT should timeout prior to this happening and s/c should "safe."	t 3		yes	CLT will expire. CCD commands are only sent durir ground contact (failure of commands will be seen in trending). No autonomous reaction.	Ground - loss of g signal/lock CLT not tickled		?	√/A
TM-1.1.3.e			Reduced performance	1) Component failure 2) Radiation effects		See loss of signal/lock. Ground could see dropped commands. Performance reduction may be minor and it's likely that the ground would react, not the s/c.	timeout - soit reset of radio,		if ground is unable to uplink to is/c, a stale ephemeris could lead to UV. CLT should timeout prior to this happening and s/c should "safe."	t 3	Active	Yes	Non-incrementing command counters, incrementing bad command counters, bad s/c II BCH errors. Margin might hid problems, would need to look at data trending.	signal/lock , CLT not tickled		?	√/A
Inputs			RF Signal from ground	No signal corrupted signal incorrect data rate or corrupted data (miscorrected data (misconfiguration of ground station)		lock and AGC would report no signal 2) Could be reporting lock and valid AGC, but still have corrupted data 3) Possible intermittent lock,	switch sides of radio, check switch assembly, no data from ground. S/c unaffected 3) bad frame counts would	Should be able to fix problem on ground. No effect to mission	If ground is unable to uplink to s/c, a stale ephemeris could lead to UV. CIT should timeout prior to this happening and s/c should "safe."	t 3	Active	Yes	1) Would show loss of lock, unexpected AGC voltage 2) Could show lock, but bad frame counter would increment or command to counter would not increment 3) Varying AGC levels, lower than expected AGC level, increased error count. 4) Ground would notice failun to acquire	Ground - loss of signal/lock CLT not tickled			N/A
			Configuration commands from C&DH			Could be reporting lock and vaild AGC, but still have corrupted data. Would see a loss of lock or reduced signal strength	5/c wouldn't receive commands. S/c could re-issue correct configuration or possibly check the mode of the s/c. Would likely follow common response to CLT timeout - soft reset of radio, power cycle to radio, side switch of Rr, then sideswitch of avionics.	critical commands, mission should be unaffected.	if ground is unable to uplink to s/c, a stale ephemeris could lead to UV. CLT should timeout prior to this happening and s/c should "safe."	t 3	Active	Yes	Reported status telemetry	Ground - loss of signal/lock CLT not tickled		?	N/A
TM-1.1.4 TM-1.1.4.a	X-Band Tx		Locks up/resets	1) SEU		Transponder A would come back on in the "off" state.	Next ground contact would see no response from s/c. Would likely follow common response to CLT timeout - soft reset of radio, power cycle to radio, side switch of RF, then sideswitch of avionics.		N/A	4	Active	Yes	Ground would see issue	Heartbeat from FR; FR rest type		N/A	N/A
TM-1.1.4.b			Hard failure	1) Component failure		Transponder A doesn't work.	Overcurrent might cause FR to be shut down by s/c Undercurrent could heat up TWTA which might cause damage to radio. (critical temperature point, needs a thermostat)	No effect.	N/A	2R	Active	Yes	S/C might not be able to deter failure, but ground would see loss of comm			N/A	N/A
TM-1.1.4.c			Reduced performance	Radiation effects Component degradation		Radio wouldn't notice any problem.	S/C wouldn't notice any problem. Ground will detect and will switch sides of the Radio	No effect.	N/A	4	None	Yes	Ground would see issue	TIm for reducecd performance defined by RF team		None	None

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Respor Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation	Revisit
TM-1.1.3.a			Locks up/resets (probably wouldn't happen at the card level)	Local	Power cycle FR	Autonomy	N/A	~1 sec (next telemetry status packet from radio)	None .	None	None .	None	None					
TM-1.1.3.b			Hard failure	Local	Power cycle FR; when rule fire count met, the RF side switch?	Autonomy	N/A	~1 sec (next telemetry status packet from radio)	None	None	None	None	None					
TM-1.1.3.c			Failure to acquire	Local/System	Power cycle FR, RF side switch? Possible system side switch? Could use 2 CLTs, first to power cycle	Autonomy			Depending on how CLT implemented 2nd CLT might be used for system side switch	Autonomy	7	7	Ground contingency to reacquire SC Need to talk through all the combinations within RF system that ground should try when attempting to reacquire	Maybe?			Cycle power to radio or issue firmware reset or reconfiguration cmd.	
TM-1.1.3.d			Failure to detect commands	Local/System	Power cycle FR, RF side switch? Possible system side switch? Could use 2 CLTs, first to power cycle	Autonomy			Depending on how CLT implemented 2nd CLT might be used for system side switch	Autonomy	7	2	Ground contingency to reacquire SC Need to talk through all the combinations within RF system that ground should try when attempting to reacquire	Maybe?			Power cycle, firmware reset, reconfigure	
TM-1.1.3.e			Reduced performance	Local/System	Power cycle FR, RF side switch? Possible system side switch? Could use 2 CLTs, first to power cycle	Autonomy			Depending on how CLT implemented 2nd CLT might be used for system side switch	Autonomy	2	?	Ground contingency to reacquire SC Need to talk through all the combinations within RF system that ground should try when attempting to reacquire	Maybe?			Power cycle, reoptimize ground station links (pick stations with most margin), operate with shorter passes (reduce elevation angle range)	
Inputs			RF Signal from ground	Local/System	Power cycle FR, RF side switch? Possible system side switch? Could use 2 CLTs, first to power cycle Ground may be able to fix	Autonomy / Ground			Depending on how CLT implemented 2nd CLT might be used for system side switch	Autonomy	7	7	Ground contingency to reacquire SC Need to talk through all the combinations within RF system that ground should try when attempting to reacquire				Ground would fix their problem	
TM-1.1.4	X-Band Tx		Configuration commands from C&DH	Local/System	Power cycle FR, RF side switch? Possible system side switch? Could use 2 CLTs, first to power cycle Ground may be able to fix	Autonomy / Ground			Depending on how CLT implemented 2nd CLT might be used for system side switch	Autonomy	?	?	Ground contingency to reacquire SC Need to talk through all the combinations within RF system that ground should try when attempting to reacquire				issue correct configuration commands	
TM-1.1.4.a	ps some IA		Locks up/resets	Local	Power cycle FR; when rule fire count met, the RF side switch?	Autonomy	N/A		None	None	None	None	None					
TM-1.1.4.b			Hard failure	<u>Local</u>	Power cycle FR; when rule fire count met, the RF side switch?	Autonomy	N/A	OWLT	None	None	None	None	None					
TM-1.1.4.c			Reduced performance	None/Local?	RF side switch	Ground			None	None	None	None	Ground to monitor performance; contingency for RF side switch				Power cycle, firmware reset, switch sides, reconfigure	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	fect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?		Im Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
Inputs			Configuration commands from C&DH				Ground would see problem with data or would see no lock and would take steps to reacquire lock.		N/A	4		Yes	Reported status telemetry	TIm for reducecd performance defined by RF team		None	None
TM-1.1.5 TM-1.1.5.a	Ka-Band Tx		Locks up/resets	1) SEU		Transponder A would come back on in the "off" state.	Next ground contact would see no response from s/C. Would likely follow common response to CLT timeout - soft reset of radio, power cycle to radio, side switch of RF, then sideswitch of avionics.		N/A	4	Active	Yes	Ground would see issue	Heartbeat from FR; FR reset type		N/A	N/A
TM-1.1.5.b			Hard failure	1) Component failure		Transponder A doesn't work.	Overcurrent might cause FR to be shut down by s/c Undercurrent could heat up TWTA which might cause damage to radio. (critical temperature point, needs a thermostat)	No effect.	N/A	2R	Active	Yes	S/C might not be able to detec failure, but ground would see loss of comm			N/A	N/A
TM-1.1.5.c			Reduced performance	Radiation effects Component degradation		Radio wouldn't notice any problem.	S/C wouldn't notice any problem. Ground will detect and will switch sides of the Radio	No effect.	N/A	4	None	Yes	Ground would see issue	TIm for reducecd performance defined by RF team		None	None
Inputs			Configuration commands from C&DH				Ground would see problem with data or would see no lock and would take steps to re- acquire lock.	Will need to reschedule interrupted data download.	N/A	4	None	Yes	Reported status telemetry	TIm for reducecd performance defined by RF team		None	None
TM-1.2 TM-1.2.1 TM-1.2.2	FR B Power Converter Spacecraft Interfaces (except power)																
TM-1.2.2.1 TM-1.2.2.2 TM-1.2.2.3 TM-1.2.2.4 TM-1.2.2.4 TM-1.2.3 TM-1.2.4	X-Band Rx X-Band Tx	Spacewire UART Clock Baseband MET Synch															
TM-1.2.5 TM-2 TM-2.1	Ka-Band Tx TWTA IX TWTA A/EPC												Current and voltage would be out-of-spec, ground would lose downlink.				
TM-2.1.a			No RF output	1) hard failure in TWTA		Fails TWTA and EPC	Downlink lost. PDU would switch the TWTA and FR to side B. No other effect.	No effect.	N/A	2R	Active	Yes	If anode voltage too low, would signal EPC failure - response would be to cycle jower to EPC. If anode voltage looks fine, but RF output power drops - response would be MOps contingency procedure if TWTA turns off and on repeatedly, might need an avoincis side switch.	EPC anode voltage How to catch TWTA ⁷ on/off?		?	?
TM-2.1.b			Fault reported in TWTA tlm lines / No RF output	High helix current Overcurrent High temperature Failure in EPC		Might cycle power	If monitored parameters affected, PDU would switch to B string. No other effect.	No effect.	N/A	4	Active	yes	High voltage monitored by the s/c Only ground would notice variation in received power	EPC aliveness; TWTA current		?	?
Inputs			+28V			TWTA doesn't work	Downlink lost. PDU would switch the TWTA and FR to side B. No other effect.	No effect.	N/A	4	Active	Yes	TWTA doesn't come on when commanded to. Symptoms would initially imflict those of "No RF output," specifically: If anode voltage too low, would signal EPC failure - response would be to cycle power to EPC if anode voltage looks fine, but RF output power drops - response would be MOps contingency procedure if TWTA turns off and on repeatedly, might need an avionics side switch.	TWTA aliveness ?		7	None
TM-2.2 TM-2.3	X TWTA B/EPC Ka TWTA A/EPC		RF input from radio			No RF output (but EPC comes on and TWTA is receiving power)	Downlink lost. PDU would switch the TWTA and FR to RF side B. No other effect.	No effect.	N/A	4	Active	yes	Ground wouldn't see output. The CLT might expire.	TWTA/EPCc health tlm? ?		?	?
TM-2.3.a	TO THE PARTY OF TH		No RF output	1) hard failure in TWTA		Fails TWTA and EPC	Downlink lost. S/C would switch the TWTA and FR to RF side B. No other effect.	No effect.	N/A	2R	Active	Yes	Current and voltage would be out-of-spec, ground would lost downlink. If anode voltage too low, would signal EPC failure - response would be to cycle power to EPC If anode voltage looks fine, but RF output power drops - response would be MOps contingency procedure if TWTA turns off and on repeatedly, might need an avionics side switch.	TWTA power state PDU t	o Autonomy	?	7

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Respon Time to Transmit Signal	se Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation	Revisit
Inputs			Configuration commands from C&DH	None/Local?	RF side switch or re-issue correct configuration	Ground			None	None	None	None	Ground to monitor performance; contingency for RF side switch and/or re-issue correct configuration				issue correct configuration commands	
TM-1.1.5	Ka-Band Tx																	
TM-1.1.5.a			Locks up/resets	Local	Power cycle FR	Autonomy	N/A		None	None	None	None	None					
TM-1.1.5.b			Hard failure	Local	Power cycle FR; when rule fire count met, the RF side switch?	Autonomy	N/A	OWLT										
TM-1.1.5.c			Reduced performance	None/Local?	RF side switch or re-issue correct configuration	Ground			None	None	None	None	Ground to monitor performance; contingency for RF side switch and/or re-issue correct configuration				Power cycle, firmware reset, switch sides, reconfigure	
Inputs			Configuration commands from C&DH	None/Local?	RF side switch or re-issue correc configuration	Ground			None	. <mark>None</mark>	None	None	Ground to monitor performance; contingency for RF side switch and/or re-issue correct configuration				lssue correct configuration commands	
TM-1.2 TM-1.2.1	FR B Power Converter Spacecraft Interfaces																	
TM-1.2.2 TM-1.2.2.1	(except power)	Spacewire																
TM-1.2.2.2 TM-1.2.2.3 TM-1.2.2.4		UART Clock Baseband																
TM-1.2.2.4 TM-1.2.3 TM-1.2.4	X-Band Rx X-Band Tx	MET Synch																
TM-1.2.5 TM-2	Ka-Band Tx TWTA																	ļ
TM-2.1	X TWTA A/EPC																	
TM-2.1.a			No RF output	Local/System	Power cycle EPC	Autonomy	?	? Depends on how often those values are sampled. Probably 1Hz tick.	Possible system side switch?	Autonomy	3	?	?					
TM-2.1.b			Fault reported in TWTA tlm lines / No RF output	Local	Power cycle EPC, TWTA Possible RF side switch	Autonomy	?	? Depends on how often those values are sampled. Probably 1Hz tick.	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
Inputs			+28V	Local	RF side switch	Autonomy	?	?	None	None	N one	None	?					
			RF input from radio	Locacl	RF side switch	Autonomy	?	?	None	None	None	None	?					
TM-2.2 TM-2.3	X TWTA B/EPC Ka TWTA A/EPC																	
TM-2.3.a			No RF output	Local	RF side switch	Autonomy	?	? Depends on how often those values are sampled. Probably 1Hz tick.	None	None	None	None	SC reacquire contingency - no downlink				Ka TWTA can switch radios independently of RF side. Ground could also switch antenna plarization. S/C would not do any of this autonomously.	
				<u></u>														<u> </u>

FMEA ID	Name	Function	Failure Mode / Limit /	Possible Causes	Phase	Local	Eff Next Higher	ect Mission	Umbra Violation	Severity	Type of	Observable	How Observed?	Detection Me		Time to Detect	Time to Detect
			Constraint							,	FM				Diagnosis	(Local)	(System)
TM-2.3.b			Fault reported in TWTA tlm lines / No RF output	High helix current Overcurrent High temperature Failure in EPC		TWTA would continue working but would output incorrect voltage	If monitored parameters affected, S/C would switch to B string. No other effect.	No effect.	N/A	4	Active	Yes	High voltage monitored by the s/c Only ground would notice variation in received power	PDU TWTA currer	PDU to CDH/Autonomy	?	?
Inputs			÷28V			TWTA doesn't work	Downlink lost. S/C would switch the TWTA and FR to RF side B. No other effect.			4	Active	Yes	TWTA doesn't come on when commanded to. Symptoms would initially mimic those of "No RF output," specifically: If anode voltage too low, would signal EPC failure response would be to cycle power to EPC III anode voltage looks fine, but RF output power drops-response would be MOps contingency procedure IT TWTA turns off and on repeatedly, might need an avionics side switch.		t CDH/Autonomy	2	?
			RF input from radio			No RF output	Downlink lost. S/C would switch the FR to RF side B. No other effect.			4	Active	Yes	Ground wouldn't see output. The CLT might expire.	No RF output on ground CLT expiration	?	?	?
	Ka TWTA B/EPC Low Noise Amplifier																
	LNA A		No output	1) component failure		No uplink signal to radio	Command loss timer limit violation will cause (autonomy?) switch to RF side B and adjust switches to point to the other antenna. No other	No effect.	N/A	2R	Active	Yes	S/C would see absence of commands from ground. CLT not tickled.	None No RF output on ground	?	?	?
TM-3.1.b			incorrect output	1) Degraded performance (gain, noise figure)		Degraded link performance for that uplink.	effect. S/c would only notice if degradation was sufficient to cause errors in uplink datastream. Not noticable with sufficient link margin. Radio's input power would not match the expected value [probably noticed on ground, not on board s/c). (Ground command to) S/c would switch to side B.		N/A	4	None		S/c would only notice if degradation was sufficient to cause errors in uplink datastream. Not noticable with sufficient link margin. Radio's input power would not match the expected value (probably noticed on ground, not on board s/c). Ground would perform any switches.	CLT expiration None - degraded performance	None	None	None
Inputs			Secondary voltage from Radio			No uplink signal to radio	Command loss timer limit violation will cause	No effect.	N/A	4	Active	Yes	S/C would see absence of commands from ground. CLT not tickled.	None No RF output on ground CLT expiration	?	?	?
			RF input from filter			No uplink signal to radio	Command timer limit violation will cause (autonomy?) switch to side B. No other effect.	No effect.	N/A	4	Active	Yes	S/C would see absence of commands from ground.	No RF output on ground CLT expiration	?	?	?
	LNA B Hybrid													CET EXPIRATION		ļ	
	HYDrio Ka-Band HYB-2		No output / incorrect output	1) Mechanical failure in device 2) Failure at waveguide flange		No output to expected device from Hybrid.	No RF or degraded RF signal. Ground would notice lack or degradation of signal and command RF to switch sides and/or switch Ka-band TWTAs, but degraded signal would remain even after switch.	Eventually overwhelm SSRs du to only having fanbeam downlink.	N/A	2	None		Ground detects data errors, incorrect power, or loses downlink. Autonomy would not react.	None - degraded performance	None	None	None
Inputs			RF output from FRs			No effect on hybrid.	Ground would detect data errors, incorrect transmit power, or lost downlink and would command RF to switch sides.	No effect.	N/A	4	None		Ground detects data errors, incorrect power, or loses downlink. Autonomy would not react.	None - degraded performance	None	None	None
TM-5.1	Filter Filter A (component may be removed from design)												S/C would see absence of				
TM-5.1.a			No output	1) component failure		No uplink signal to radio	Command timer limit violation will cause (autonomy?) switch to side B. No other effect.	No effect.	N/A	2R	Active	Yes	S/C would see absence of commands from ground. CLT not tickled. This is a completely passive component so ground might assume failun is in the LNA.		?	?	?
TM-5.1.b			Degraded output	1) component failure		Degraded link performance for that uplink.	S/c would only notice if degradation was sufficient to cause errors in uplink datastream. Not noticable with sufficient his margin. Radio's input power would not match the expected value [probably noticed on ground, not on board s/c). (Ground command to) S/c would switch to side B.		N/A	4	None		S/c would only notice if degradation was sufficient to cause errors in uplink datastream. Not noticable with sufficient link margin. Radio's input power would not match the expected value (probably noticed on ground, not on board s/c). Ground would perform any switches. This is a completely passive component, so ground might assume failure is in the LNA.	None - degraded performance	None	None	None
Inputs	Filter B		Uplink signal from diplexer			No uplink signal to radio	Command timer limit violation will cause (autonomy?) switch to RF side B. No other effect.	No effect.	N/A	4	Active	Yes	S/C would see absence of commands from ground. CLT not tickled. This is a completely passive component so ground might assume failur is in the LNA.	None CLT expiration	?	7	?

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Respon Time to Transmit Signal	se Desired System Response	Allocation of System Response	Time to fix system		t Ground Response /	System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation	Revisit
TM-2.3.b			Fault reported in TWTA tlm lines / No RF output	Local	RF side switch	Autonomy	?	? Depends on how often those values are sampled. Probably 1Hz tick.	None Kesponse	None	None	Signal None	Ground to monitor performance; contingency for RF side switch				Ka TWTA can switch radios independently of RF side. Ground could also switch antenna plarization. S/C would not do any of this autonomously.	
Inputs			+28V	Local	RF side switch	Autonomy	?		None	None	None	None	SC reacquire contingency - no downlink					x
TM-2.4	Ka TWYA B/FPC		RF input from radio	Local	RF side switch	Autonomy	?	?	None	None	None	None	SC reacquire contingency - no downlink					х
TM-3 TM-3.1	Low Noise Amplifier LNA A																	<u> </u>
TM-3.1.a			No output	Local	RF side switch	Autonomy	?	~1 sec	None	None	None	None	SC reacquire contingency - no downlink				if s/c is positioned appropriately, the other FR could be in view of Earth and still receive commands. Would give a positive indication of failure - carrier lock on wrong radio.	
TM-3.1.b			ncorrect output	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
Inputs			Secondary voltage from Radio	Local	RF side switch	Autonomy	?	?	None	None	None	None	Ground to reacquire SC					
			RF input from filter	Local	RF side switch	Autonomy	?	?	None	None	None	None	Ground to reacquire SC					
TM-3.2 TM-4	LNA B Hybrid																	<u> </u>
TM-4.1.a	Ka-Band HYB-2		No output / incorrect output	Local / Ground	RF side switch	Ground	2	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
Inputs			RF output from FRs	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
TM-5.1	Filter Filter A (component may be removed from																	
TM-5.1.a	design)		No output	Local	RF side switch	Autonomy	7	,	None	None	None	None	Ground to reacquire SC				If s/c is positioned appropriately, the other FR could be in view of Earth and still receive commands. Would give a positive indication of failure - carrier lock on wrong radio.	
TM-5.1.b			Degraded output	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
Inputs	Filter B		Uplink signal from diplexer	Local	RF side switch	Autonomy	?	?	None	None	None	None	Ground to reacquire SC					

FMEA ID	Name	Function	Failure Mode / Limit / Possible Cause Constraint	s Phase	Local	Ef Next Higher	ect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Meth Tlm for Diagnosis	od TIm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
	Diplexer DPA		No output (uplink or downlink) 1) component failure		Loss of uplink or downlink signal	With severe enough degradation, (uplink - autonomy CLT timeout, downlink - ground would notice and send command) S/C would switch to RF side B. No other effect.	No effect.	N/A	2R	Active	Yes	Loss of uplink would look like degraded LNA (s/c would see an absence of commands from ground, CLT wouldn't be tickled). Loss of downlink would cause a reduction in receive power on ground.	None CLT expiration	?	?	?
TM-6.1.b			Degraded output (uplink or downlink) 1) component failure		Degradation of uplink or downlink signal	S/c or ground would detect issue (Ground-sent command to switch sides) and switch to RF side B	No effect.	N/A	4	None		S/C would not be able to isolate problem to diplexer. If uplink path failed, s/c would see loss of uplink. If downlink path failed, ground would see loss of downlink. Notice through trending. No autonomous reaction.		None	None	None
Inputs			Uplink signal from switch assembly		Loss of both uplink and downlink signal	S/c or ground would detect issue (Ground-sent command to switch sides) and switch to RF side B	No effect.	N/A	4	None		S/C would not be able to isolate problem to diplexer. If uplink path failed, s/C would see loss of uplink. If downlink path failed, ground would see loss of downlink. Notice through trending. No autonomous reaction.		None	None	None
			Downlink signal in from X-band TWTAs		Loss of downlink signal	S/c or ground would detect issue (Ground-sent command to switch sides) and switch to RF side B (could still uplink, if necessary)	No effect.	N/A	4	None		S/C would not be able to solate problem to diplexer. If uplink path failed, s/c would see loss of uplink. If downlink path failed, ground would see loss of downlink. Notice through trending. No autonomous reaction.		None	None	None
	DP B RF Switch															
	5W1		Switch stuck in a single position Component failure		Switch stuck in single configuration	Could still access all antennas by switching FRs or TWTAs. No effect on S/C.	No effect.	N/A	2R	None	Yes	Tell-tales Would not be able to communicate through commanded path if switch didn't flip.	Switch Telltales	?	?	None
TM-7.1.b			Telltales fail Component failure		No sensing on switch.	No effect. Ground will need to infer position based on received power.	No effect.	N/A	4	None	Yes	Communications would work through a pathway configuration that the tell-tale status says the s/c is not in.	Switch Telltales and power status	?	?	None
TM-7.1.c			Switch not in any position Redundant coils burnt (electrical fault) failures)	out (two	Switch not connected to any antenna	FR A can no longer transmit or receive from any X-band antenna.	No effect.	N/A	2R	None	Yes	Ground would see loss of X- band downlink.	Loss of downlink signal	?	?	None
TM-7.1.d			Switch not in any position not a credible failure (mechanical fault)		Not a credible failure	No effect.	No effect.	N/A	4	None		None	None	None	None	None
Inputs			RF signal from previous switch, idplexer, or antenna		Switch can't send RF signal on to proper device	Worst case could lose an antenna	Lost RF coverage to some portion of s/c (x-band only). Worst case - lose abilty for nominal operations through 34M DSN. Lose x-band downlink capability until s/c has moved enough to see another antenna. Could rotat s/c for partial mitigation to achieve degraded link performance.	N/A	4	Active		Ground would see loss of antenna. S/c could see loss of uplink, CLT time-out would cause autonomy to switch sides, but would eventually need to go looking for Earth with a different antenna.	CLT countdown Ground - loss of antenna coverage	CLT countdown in Autonomy	7	?
TM-7.2	SW2															
тм-7.2.а			Switch stuck in a single position Component failure		Switch stuck in single configuration	Could still access all antennas by switching FRs or TWTAs. No effect on S/C.	No effect.	N/A	2R	None	Yes	Tell-tales Would not be able to communicate through commanded path if switch didn't flip.	Switch Telltales	?	?	None
TM-7.2.b			Telltales fail Component failure		No sensing on switch.	No effect. Ground will need to infer position based on received power.	No effect.	N/A	4	None	Yes	Communications would work through a pathway configuration that the tell-tale status says the s/c is not in.	Switch Telltales and power status	?	?	None
TM-7.2.c			Switch not in any position Redundant coils burnt lelectrical fault) failures)	out (two	Switch not connected to any antenna	FR B can no longer transmit or receive from any X-band antenna.	No effect.	N/A	2R	None	Yes	Ground would see loss of X- band downlink.	Loss of downlink signal	?	?	None
TM-7.2.d			Switch not in any position not a credible failure (mechanical fault)		Not a credible failure	No effect.	No effect.	N/A	4	None			None	None	None	None
Inputs			RF signal from previous switch, diplexer, or antenna		Switch can't send RF signal on to proper device	Worst case could lose an antenna	Lost RF coverage to some Lost RF coverage to some Dortion of s/c (x-band only). Worst case - lose ability for nominal operations through 34M DSN. Lose x-band downlink capability until s/c has moved enough to see another antenna. Could rotat s/c for partial mitigation to achieve degraded link performance.	N/A	4	Active		Ground would see loss of uplink, CLT time-out would cause autonomy to switch sides, but would eventually need to go looking for Earth with a different antenna.	CLT countdown Ground - loss of antenna coverage	CLT countdown in Autonomy	7	?

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Respor Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transm Signal	it Ground Response / Contingency	System Side Switch	Quick Look Processor Switch	Safe Mode	Rem	nediation	Revisit
	Diplexer DP A																		
IIW-0.1	DF A																		†
TM-6.1.a			No output (uplink or downlink)	Local	RF side switch	Autonomy	?	?	None	None	None	None	Ground to reacquire SC						
				ļ							ļ								
			2										Ground to monitor						
TM-6.1.b			Degraded output (uplink or downlink)	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	performance; contingency for RF side switch						
													N side switch						
Inputs			Uplink signal from switch assembly	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for						
			assembly										RF side switch						
			Downlink signal in from X-band TWTAs					_					Ground to monitor						
			TWTAs	Local / Ground	RF side switch	Ground	'	,	None	None	None	None	performance; contingency for RF side switch						
TM-6.2	DP B			<u> </u>	ļ			ļ			ļ	ļ							
TM-7	RF Switch			ļ	<u></u>			<u></u>			<u></u>	<u> </u>		i 					
TM-7.1	SW1																		
TM 7.1 -			C	Laurel / Consumed	Name	Constant	News	Name	Name	N	Name	Al	Need to talk through all the combinations within RF system						
TM-7.1.a			Switch stuck in a single position	Local / Ground	None	Ground	None	None	None	None	None	None	that ground should try when attempting to reacquire			•			
												ļ							
			T. W. L. C. I										Need to talk through all the combinations within RF system						
TM-7.1.b			Telltales fail	Local / Ground	None	Ground	None	None	None	None	None	None	that ground should try when attempting to reacquire			•			
													Need to talk through all the combinations within RF system						
TM-7.1.c			Switch not in any position (electrical fault)	Local / Ground	None	Ground	None	None	None	None	None	None	that ground should try when attempting to reacquire; this						
			(electrical fault)										fault would result in RF side						
			Switch not in any position				ļ	ļ		ļ	ļ	ļ	switch?	<u> </u>	 	<u> </u>			
TM-7.1.d			(mechanical fault)	None	None	None	None	None	None	None	None	None	None						
Inputs			RF signal from previous switch,	Local	CLT expires and performs RF side	Autonomy	?	?	CLT 2 expires and performs system	Autonomy	?	?	?						
·			diplexer, or antenna		switch				side switch	ĺ									
TM-7.2	SW2						ļ	ļ			ļ	ļ			ļ	<u> </u>			
1.6171.2	J					<u> </u>	<u></u>		İ	<u> </u>	<u> </u>	İ	Need to talk through all the	<u></u>					-
TM-7.2.a			Switch stuck in a single position	Local / Ground	None	Ground	None	None	None	None	None	None	combinations within RF system			ļ			
													that ground should try when attempting to reacquire						
				 			<u></u>		ļ		<u></u>	ļ	Need to talk through all the				ļ		-
TM-7.2.b			Telltales fail	Local / Ground	None	Ground	None	None	None	None	None	None	combinations within RF system						
													that ground should try when attempting to reacquire						
						<u> </u>	<u></u>		İ	<u> </u>	<u> </u>	İ	Need to talk through all the	<u></u>					-
			Switch not in any position										combinations within RF system						
TM-7.2.c			Switch not in any position (electrical fault)	Local / Ground	None	Ground	None	None	None	None	None	None	that ground should try when attempting to reacquire; this						
													fault would result in RF side switch?						
TM 7.2 -			Switch not in any position	None	None	None	None	None	None	None	None	None		ļ					
TM-7.2.d			(mechanical fault)	None	None	None	None	None	None	None	None	None	None	ļ		<u> </u>			.
									CIT 2 avaises and										
Inputs			RF signal from previous switch, diplexer, or antenna	Local	CLT expires and performs RF side switch	Autonomy	?	?	CLT 2 expires and performs system	Autonomy	?	?	?						
			preser, or antennia						side switch										
		1	1	1	1	1	1	<u> </u>	1	<u> </u>	<u></u>	į	1	<u> </u>	į	<u>.</u>	į		
TM-7.3	SW3		······································	1			•	1						1		1			

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Eff Next Higher	ect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Meth Tlm for Diagnosis	od Tlm Path for Diagnosis	Time to Detect	Time to Detect (System)
TM-7.3.a			Switch stuck in a single position	Component failure		Switch stuck in single configuration	Could still access all antennas by switching FRs or TWTAs. No effect on S/C.	No effect.	N/A	2R	None	Yes	Tell-tales Would not be able to communicate through commanded path if switch didn't flip.	Switch Telltales	?	?	None
TM-7.3.b			Telltales fail	Component failure		No sensing on switch.	No effect. Ground will need to infer position based on received power.	No effect.	N/A	4	None	Yes	Communications would work through a pathway configuration that the tell-tale status says the s/c is not in.	Switch Telltales and power status	?	?	None
TM-7.3.c			Switch not in any position (electrical fault)	Redundant coils burnt out (two failures)		Switch not connected to any antenna	S/c can no longer transmit or receive from any LGA.	No effect.	N/A	2R	None	Yes	Ground would see loss of X- band downlink.	Loss of downlink signal	?	?	None
TM-7.3.d			Switch not in any position (mechanical fault)	not a credible failure		Not a credible failure	No effect.	No effect.	N/A	4	None			None	None	None	None
Inputs			RF signal from previous switch, diplexer, or antenna			Switch can't send RF signal on to proper device	Worst case could lose an antenna	Lost RF coverage to some portion of s/c (x-band only). Worst case - lose ability for nominal operations through 34M DSN. Lose x-band downlink capability until s/c has moved enough to see another antenna. Could rotate s/c for partial mitigation to achieve degraded link performance.	N/A	4	Active		Ground would see loss of antenna. S/c could see loss of uplink, CLT time-out would cause autonomy to switch sides, but would eventually need to go looking for Earth with a different antenna.	CLT countdown Ground - loss of antenna coverage	CLT countdown in Autonomy	2	2
TM-7.4 TM-7.4.a	5W4		Switch stuck in a single position	Component failure		Switch stuck in single configuration	Could still access all antennas by switching FRs or TWTAs. No effect on S/C.	No effect.	N/A	2R	None	Yes	Tell-tales Would not be able to communicate through commanded path if switch didn't flip.	Switch Telltales	?	?	None
TM-7.4.b			Telltales fail	Component failure		No sensing on switch.	No effect. Ground will need to infer position based on received power.	No effect.	N/A	4	None	Yes	Communications would work through a pathway configuration that the tell-tale status says the s/c is not in.	Switch Telltales and power status	?	?	None
TM-7.4.c			Switch not in any position (electrical fault)	Redundant coils burnt out (two failures)		Switch not connected to any antenna	S/c can no longer transmit or receive from any fan beam antenna.	No effect.	N/A	2R	None	Yes	Ground would see loss of X- band downlink.	Loss of downlink signal	?	?	None
TM-7.4.d			Switch not in any position (mechanical fault)	not a credible failure		Not a credible failure	No effect.	No effect.	N/A	4	None			None	None	None	None
Inputs			RF signal from previous switch, diplexer, or antenna			Switch can't send RF signal on to proper device	Worst case could lose an antenna	Lost RF coverage to some portion of s/c (k-band only). Worst case - lose abilty for nominal operations through 34M DSN. Lose x-band downlink capability until s/c has moved enough to see another antenna. Could rotate s/c for partial mitigation to active vegerate of the performance.	N/A	4	Active		Ground would see loss of antenna. S/c could see loss of uplink, CLT time-out would cause autonomy to switch sides, but would eventually need to go looking for Earth with a different antenna.	CLT countdown Ground - loss of antenna coverage	CLT countdown in Autonomy	7	?
	Flex Waveguide FW A																
TM-8.1.a			Crack	1) Material defect 2) Dust strike		Degraded wave propagation to/from antenna	Degraded antenna performance. Ground command Switch to other side.	No effect.	N/A	4	None	Yes. (After process of elimination)	Gournd would see reduced downlink power. Autonomy would not act.	None	None	None	None
Inputs			RF output from Ka-band TWTAs			Degraded wave propagation to/from antenna	Degraded antenna performance. Ground command Switch to other side.	No effect.	N/A	4		Yes. (After process of elimination)	Gournd would see reduced downlink power. Autonomy would not act.	None	None	None	None
TM-9	FW B Antennae																
TM-9.1 TM-9.1.a	HGA		Mechanical failure	1) Material defect 2) Dust strike		Antenna fails to send/receive communications.	S/C unable to return data in a timely fashion. Ground would attempt to switch antenna polarization, but would not correct problem.	Mission success severely impacted by data rate loss.	N/A	2 - if data return is too low 3 - if science requirements can still be met	None	Yes. (After process of elimination)	No more comm to/from HGA.	None Loss of comm with HGA	None	None	None
TM-9.1.b			Degraded performance			Poor perfomance (either less power or corrupted signal)	Run at lower data rates. Ground would switch antenna polarization.	Mission success severely impacted by data rate loss.	N/A	2 - if data return is too low 3 - if science requirements can still be met	None	Yes. (After process of elimination)	Ground would see lower powe or corrupted signal	None r Loss of comm with HGA	None	None	None
TM-9.2.a	IGA1		Mechanical failure	1) Material defect 2) Oust strike		Antenna falls to send/receive communications.	No problem as long as s/c can orient itself such that working antenna is pointing to Earth. May not be possible at all points in mission. Only used during TCMs, may lose comm due to s/c pointing requirements for TCM. Ground would command s/c to switch antennae.	loss of LGA	N/A	3		Yes. (After process of elimination)	No more comm to/from LGA.	None Loss of comm with LGA	None	None	None
TM-9.3 TM-9.4	FB 1		<u> </u>							<u> </u>	<u></u>			<u> </u>			

FMEA ID	Name	Function	Failure Mode / Limit /	Response Level	Desired Local Response	Allocation of Local	Time to fix locally		Desired System	Allocation of	Time to fix system			System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation	Revisit
			Constraint			Response		Signal	Response	System Response		Signal	Contingency Need to talk through all the					
M-7.3.a			Switch stuck in a single position	n Local / Ground	None	Ground	None	None	None	None	None	None	combinations within RF system that ground should try when					
													attempting to reacquire					
M-7.3.b			Telltales fail	Local / Ground	None	Ground	None	None	None	None	None	None	Need to talk through all the combinations within RF system					
				,									that ground should try when attempting to reacquire					
													Need to talk through all the combinations within RF system					
M-7.3.c			Switch not in any position (electrical fault)	Local / Ground	None	Ground	None	None	None	None	None	None	that ground should try when attempting to reacquire; this					
			Ciccincal laury										fault would result in RF side switch?					
и-7.3.d			Switch not in any position	None	None	None	None	None	None	None	None	None	None					
			(mechanical fault)															
									CLT 2 expires and									
puts			RF signal from previous switch, diplexer, or antenna	' Local	CLT expires and performs RF side switch	Autonomy	?	?	performs system side switch	Autonomy	?	?	?					
1-7.4	SW4																	
и-7.4.a			Switch stuck in a single position	n Local / Ground	None	Ground	None	None	None	None	None	None	Need to talk through all the combinations within RF system					
л-7.4.a			Switch stuck in a single position	in Eucar / Ground	None	Ground	None	None	None	None	None	None	that ground should try when attempting to reacquire					
													Need to talk through all the					
M-7.4.b			Telltales fail	Local / Ground	None	Ground	None	None	None	None	None	None	combinations within RF system that ground should try when					
													attempting to reacquire					
			Switch not in any position										Need to talk through all the combinations within RF system that ground should try when					
И-7.4.с			(electrical fault)	Local / Ground	None	Ground	None	None	None	None	None	None	attempting to reacquire; this fault would result in RF side					
													switch?					
1-7.4.d			Switch not in any position (mechanical fault)	None	None	None	None	None	None	None	None	None	None					
uts			RF signal from previous switch,	' Local	CLT expires and performs RF side	Autonomy	7	?	CLT 2 expires and performs system	Autonomy	7	7	2					
			diplexer, or antenna		switch	,			side switch	,								
-8 -8.1	Flex Waveguide FW A																	
													Need to talk through all the combinations within RF system					
N-8.1.a			Crack	Local / Groound	Contingency Procedure	Ground	?	?	None	None	None	None	that ground should try when attempting to reacquire; this					
													fault would result in RF side switch?					
												{	Need to talk through all the					
outs			RF output from Ka-band TWTA	s Local / Groound	Contingency Procedure	Ground	?	?	None	None	None	None	combinations within RF system that ground should try when					
													attempting to reacquire; this fault would result in RF side switch?					
л-8.2 л-9	FW B												SWILLIE					
И-9 И-9.1	Antennae HGA																	
													Need to talk through all the					
И-9.1.a			Mechanical failure	Local / Ground	Contingency Procedure	Ground	?	?	None	None	None	None	combinations within RF system that ground should try when attempting to reacquire					
И-9.1.b			Degraded performance	Local / Ground	Contingency Procedure	Ground	?	?	None	None	None	None	Need to talk through all the combinations within RF system					
													that ground should try when attempting to reacquire					
-9.2	LGA 1																	
													Need to talk through all the combinations within RF system					
И-9.2.a			Mechanical failure	Local / Ground	Contingency Procedure	Ground	(ľ	None	None	None	None	that ground should try when attempting to reacquire					
			1	1	1	1												
и-9.3	LGA 2				- -	ļ	· •	· ·	<u> </u>		ļ	ļ	- 		ļ			

							Ef	fect						Detection Metho	d		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
TM-9.4.a			Mechanical failure	1) Material defect 2) Dust strike		Antenna fails to send/receive communications.	No problem as long as s/c can orient itself such that working antenna is pointing to Earth. May not be possible at all points in mission. Would rotate around 2 to get to an LGA, during periods of Ka-band contact, would have reduced uplink capability through LGA. Ground would command s/c to switch antennae.		N/A	3	None	Yes. (After process of elimination)	No more comm to/from FB.	None Loss of comm with	Juagnoss	None	None
TM-9.5 TM-10	FB 2 RFDU						Could probably still use that										
TM-10.a			Loss of single diode/resistor in cross-strapping section			Loss of cross-strapping capability to one side	side, but would probably switch to side B		N/A	2R		?	?				
TM-10.b			Loss of soft-start circuitry for TWTs			TWT no longer available	Switch to B side			2R							
Inputs			Tell tale signal from switch assembly			No sensing on switch.	received power.	No effect.	N/A	4		Yes	Communications would work through a pathway configuration that the tell-tale status says the s/c is not in.				
			DC power to TWTs			Fails TWTA	Downlink lost. PDU would switch the TWTA and FR to side B. No other effect.	No effect.	N/A	4		Yes	Current and voltage would be out-of-spec, ground would los downlink.				
			Control lines from avionics to switch assembly				Could still access all antennas by switching FRs or TWTAs. No effect on S/C.	No effect.	N/A	4		Yes	Tell-tales Would not be able to communicate through commanded path if switch didn't flip.				

								Respor							Quick Look			
FMEA ID	Name	Function	Failure Mode / Limit /	Response Level	Desired Local Response		Time to fix locally				Time to fix system		Ground Response /	System Side Switch	Processor Switch	Safe Mode	Remediation	Revisit
			Constraint			Response		Signal	Response	System Response		Signal	Contingency					
				ļ														
													Need to talk through all the					1
							1						combinations within RF systen					
TM-9.4.a			Mechanical failure	Local / Ground	Contingency Procedure	Ground	?	?	None	None	None	None	that ground should try when					
													attempting to reacquire					
																		İ
																		1
TM-9.5	FB 2			ļ			·	ļ	·	ļ	· ·			·				
TM-10	RFDU	······································	· · · ·				·		·	·	· •							·
			Loss of single diode/resistor in															
TM-10.a			cross-strapping section	Local	RF side switch													Х
	· •		Loss of soft-start circuitry for	ļ			·	ļ	·	ļ	· ·			·				
TM-10.b			TWTs	Local	RF side switch													Х
1			Tell tale signal from switch	Local	RF side switch													
Inputs			assembly	LOCAI	RF Side SWILCH													
	İ			İ			İ		İ		İ	İ		i i				İ
								? Depends on how										
			DC power to TWTs		05.11 2.1			often those values										
			DC power to I W Is	Local	RF side switch			are sampled.			1							1
							•	Probably 1Hz tick.										
											· • · · · · · · · · · · · · · · · · · ·							
			Control lines from avionics to															
			switch assembly	Local	RF side switch													
		.á		<i>i</i>	á			. 			. 4		······································	. ن	i			

Subject Matter Tim Cole Expert(s): Weilun Cheng Notes: Yellow highlighted blocks are redundant components.

Components are listed for completeness, but failure mode and FMEA information is only displayed in the first copy of the component.

	information is only displayed i	in the first copy of the component.			F	ffect						Detection Method		
FMEA ID Name	Function	Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tim for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)
ME-1 Gimbals ME-1.1 Solar Array														
ME-1.1 Solar Array #1														
ME-1.1.1.1 Flap Actuator							Ì							
ME-1.1.1.1.a		Fails to actuate when commanded	1) bad/bound bearing/mechanical failure 2) stepper motor failure 3) loose/separated connector	Solar array stuck in position	if SA needs to move out, generates insufficient power if SA needs to move in, generates too much power, potential overheating of wing (cells burned)	1) eventually drain battery, may be able to slew s/c to retain partial power for a time 2) lose mission	If in encounter, and SAs stuck out too far	2	Active		Potentiometer telemetry. Turn on redundant ECU for 3rd vote.		ECU to REM	?
ME-1.1.1.1.b		Incorrect actuation when commanded	1) incorrect potentiometer reading 2) residual torque (should have sufficient margin) 3) Motor coil or winding is open	Solar array in incorrect positio	1) if SA needs to move out, generates insufficient power (different than required). 2) if SA needs to move in, generates too much power (different than expected), potential overheating of wing (cells burned)	1) eventually drain battery, may be able to slew s/c to retain partial power for a time 2) lose mission	If in encounter, and SAs stuck out too far	2	Active	Yes	Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	?
ME-1.1.1.1.c		Actuates when not commanded	Holding torque exceeded (need to have sufficient E, C margin)	Solar array in incorrect positio	1) if SA needs to move out, generates insufficient power (different than required) 2) if SA needs to move in, generates too much power (different than expected), potential overheating of wing (cells burned)	1) eventually drain battery, may be able to slew s/c to retain partial power for a time 2) lose mission	If in encounter, and SAs stuck out too far	2	Active	Yes	Power level	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	3
ME-1,1,1,1,d		Launch locks fail to release	1) Frangibolt fails to release completely (electrically redundant, so more concerned with a mechanical fault) 2) Separation interfaces fail to crelease completely (mechanical Cearance issues/unexpected interferences) (probably adding a push-off spring to ensure deployment)	Solar arrays are stuck stowed	No/limited power to s/c	Lost mission (insufficient power/heat generated at 1 AU with only one solar array)	N/A	2	Active	Yes	Potentiometer telemetry, battery fails to charge. Turn on redundant ECU for 3rd vote.	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge	ECU to REM	?
ME-1.1.1.1.e		Launch lock premature release (two tie downs)	1) Temperature exceeds ~65C and frangibolt releases 2) inadvertent command (no power to safety bus until after s/c separation from 3rd stage) L 3) Incorrect notch on frangibolt (controlled by 100% inspection of notch by vendor, will add a double-check to notch in I&T)	Array will not deploy, but will "chatter"	May damage cells and/or cooling system	With sufficient losses in Solar Arrays and cooling system, would lose mission	N/A	2	None	No	N/A	None	None	N/A
Inputs		ECU commands ("commands" really are pulses of power to the motor)		Solar array in incorrect positio or not moving at expected rate (too fast or twoo slow)	1) if SA needs to move out, generates insufficient power (different than required). Switch to redundant ECU. 2) if SA needs to move in, generates too much power (different than expected), potential overheating of wing (cells burned). Switch to redundant ECU. 3) wrong rate generates varying effects, depending on direction of motion and whether wing is safing or not.		If in encounter, and SAs stuck out too far	4	Active	Yes	Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge	ECU to REM	?

Subject Matter Tim Cole Expert(s): Weilun Cheng

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FMEA information is only displayed in the first copy of the component.

		illiorillation is only displayed if	the first copy of the component.	
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Time to Detect (System)
ME-1	Gimbals			
ME-1.1	Solar Array			
ME-1.1.1	Solar Array #1		·	<u> </u>
ME-1.1.1.1	Flap Actuator			!
IVIL-1.1.1.1	i lap Actuatoi			ļ
ME-1.1.1.1.a			Fails to actuate when commanded	?
ME-1.1.1.1.b			Incorrect actuation when commanded	?
ME-1.1.1.1.c			Actuates when not commanded	?
ME-1.1.1.1.d			Launch locks fail to release	?
ME-1.1.1.1.e			Launch lock premature release (two tie downs)	N/A
Inputs			ECU commands ("commands" really are pulses of power to the motor)	?

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)		

Mech - 82 of 317

Subject Matter Tim Cole Expert(s): Weilun Cheng Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FME

Expert(s):		Components are listed for com	cks are redundant components. In the first copy of the component.																	
			•					Resp		Allocation of				System Side	Quick Look Processor	Safe Mode		•		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Desired System Response	System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	Switch	Switch		Remediation/ notes	Autonomy?	Comments	Revisit
ME-1	Gimbals									пеоропос										
ME-1.1 ME-1.1.1	Solar Array Solar Array #1																			
ME-1.1.1.1	Flap Actuator																Power other ECU to		(·····	
ME-1.1.1.1.a			Fails to actuate when commanded	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	7		If problem persists, umbra violation or LBSOC	Autonomy	?	?	None				compare potentiometer readings. If necessary, switch ECUs. re-command, slew, coolant system	During encounter: if tip current sensors detect current, autonomously bring in solar arrays	Discuss with FSW about making on ECU "active"	
ME-1.1.1.b			incorrect actuation when commanded	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	Autonomy	· · · · · · · · · · · · · · · · · · ·	7	If problem persists, umbra violation or LBSOC	Autonomy	7	?	None				change Power other ECU to compare potentiometer readings. If necessary, switch ECUs. re-command, slew, coolant system change, go back to "home position" then re-count/recalibrate	During encounter: if tip current sensors detect current, autonomously bring in solar arrays		
ME-1.1.1.1.c			Actuates when not commanded	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy		2	If problem persists, umbra violation or LBSOC	Autonomy		,	None				Power other ECU to compare potentiometer readings. If necessary, switch ECUs. re-command, slew, coolant system change, go back to "home position" then re-count/recalibrate	During encounter: if tip current sensors detect current, autonomously bring in solar arrays	This is designed to be non-credible	
ME-1.1.1.1.d			Launch locks fail to release	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None				slew to Sun, oversized motor can bust through, recommand frangibolt		Could be mitigated by design if push springs were added - Weilun to consider	
ME-1.1.1.1.e			Launch lock premature release (two tie downs)	None	N/A	N/A	N/A		None	N/A	N/A	N/A	N/A							
Inputs			ECU commands ("commands" really are pulses of power to the motor)	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy		7	If problem persists, umbra violation or LBSOC	Autonomy	?	7-7-7-1	None				Switch ECUs re-command, slew, coolant system change, go back to "home position" then re- count/recalibrate	During encounter: if tip current sensors detect current, autonomously bring in solar arrays		

					L1	fect						Detection Method		
FMEA ID Name	Function	Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	TIm Path for Diagnosis	Time to Detect (Local)
	ŀ	Harness too cold		increases required torque (above ability of motor)	Solar array unable to move.	Nearby heaters may be able to alleviate the issue (which is localized to the flexible portion of the harness connecting to the actuator).	N/A	3	Active	Yes	Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge	ECU to REM	?
ME-1.1.1.2 Feather Actuator ME-1.1.1.2.a	F	Fails to actuate when commanded	1) bad/bound bearing/mechanical failure 2) stepper motor failure 3) loose/separated connector	Solar array stuck in position	generates insufficient power generates too much power so feathering makes it impossible for array to retract sufficiently for encounter	retain partial power for a time; cooling system might get too	3) excessive feathering prevents array from retracting sufficiently for encounter	2	Active		Potentiometer telemetry. Turn on redundant ECU for 3rd vote.		ECU to REM	?
ME-1.1.1.2.b	l	ncorrect actuation when commanded	1) incorrect potentiometer reading 2) residual torque (should have sufficient margin) 3) Motor coil or winding is open	Solar array in incorrect position		retain partial power for a time; cooling system might get too	3) excessive feathering prevents array from retracting sufficiently for encounter	2	Active		Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	?
ME-1,1.1.2.c	F	Actuates when not commanded	Holding torque exceeded (need to have sufficient C margin)	Solar array in incorrect position		retain partial power for a time; cooling system might get too	3) excessive feathering prevents array from retracting sufficiently for encounter	2	Active	Yes	Power level	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	?
Inputs		ECU commands ("commands" really are pulses of power to the motor)		Solar array in incorrect position	1) if SA needs to move out, generates insufficient power (different than required) 2) if SA needs to move in, generates too much power (different than expected), potential overheating of wing (cells burned)	1) eventually drain battery, may be able to slew s/c to retain partial power for a time 2) lose mission	If in encounter, and SAs stuck out too far	2	Active		Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge	ECU to REM	?
	ŀ	Harness too cold		Increases required torque (above ability of motor)	Solar array unable to feather.	Nearby heaters may be able to alleviate the issue (which is localized to the flexible portion of the harness connecting to the actuator).	N/A	3	Active		Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry ; redundant ECU telemetry Battery state of charge	ECU to REM	?
ME-1.1.2 Solar Array #2 ME-1.2 HGA														
ME-1.2.1 HGA Gimbal												Autonomyould		
ME-1.2.1.a		Fails to actuate when commanded mechanical failure)	bad/bound bearing/mechanical failure 2) Exceeded life limit of bearing 3) stepper motor failure 4) loose/separated connector	HGA stuck in position	In some cases, may be able to slew spacecraft to point HGA to Earth.	Would have difficulty meeting minimum mission science return requirements. Worst case, loss of science.	If stuck at large enough angle, could be an umbra violation	2 - if data return is too low 3 - if science requirements can still be met	Active	Yes	Potentiometer telemetry, step count	Autonomy could power up the other ECU to check redundant potentiometer telemetry against primary potentiometer telemetry and motor step count (3rd vote)	ECU to REM	?
ME-1.2.1.b			Short in redundant windings within actuator (two failures)	HGA stuck in position	In some cases, may be able to slew spacecraft to point HGA to Earth.	Would have difficulty meeting minimum mission science return requirements. Worst case, loss of science.	If stuck at large enough angle, could be an umbra violation	2 - if data return is too low 3 - if science requirements can still be met		Yes	Potentiometer telemetry, step count	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-1.2.1.c	I	ncorrect actuation when commanded	1) incorrect potentiometer reading 2) residual torque (should have sufficient margin)	HGA is in wrong position	Turn on back-up ECU to verify potentiometer readings. Switch to redundant ECU. Recommand to proper position.	None	N/A	4	Active	Yes	Potentiometer telemetry, step count	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Time to Detect (System)
			Harness too cold	?
ME-1.1.1.2	Feather Actuator			
ME-1.1.1.2.a			Fails to actuate when commanded	?
ME-1.1.1.2.b			Incorrect actuation when commanded	?
ME-1.1.1.2.c			Actuates when not commanded	?
Inputs			ECU commands ("commands" really are pulses of power to the motor)	?
			Harness too cold	?
ME-1.1.2 ME-1.2	Solar Array #2			
ME-1.2 ME-1.2.1	HGA HGA Gimbal			
ME-1.2.1.a			Fails to actuate when commanded (mechanical failure)	?
ME-1.2.1.b			Fails to actuate when commanded (electrical failure)	?
ME-1.2.1.c			Incorrect actuation when commanded	?

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

Mech - 85 of 317

								Resp	onse						Quick Look					
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Desired System Response	Allocation of System	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Processor Switch	Safe Mode	Remediation/ notes	Autonomy?	Comments	Revisit
					If potentiometer and step					Response										
			Harness too cold	Local	count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None							
ME-1.1.1.2	Feather Actuator																			
ME-1.1.1.2.a			Fails to actuate when commanded	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	7	?	None				re-command, slew, cur coolant system cur change brir	ring encounter: if tip rent sensors detect rent, autonomously ng in solar arrays; go to fe" feathering position		
ME-1.1.1.2.b			Incorrect actuation when commanded	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	3	?	None				change, go back to cur "home position" cur	ring encounter: if tip rent sensors detect rent, autonomously ng in solar arrays		
ME-1.1.1.2.c			Actuates when not commanded	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None				change, go back to cur "home position" cur	ring encounter: if tip rent sensors detect rent, autonomously ng in solar arrays		
Inputs			ECU commands ("commands" really are pulses of power to the motor)		If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None				change, go back to cur "home position" cur	ring encounter: if tip rent sensors detect rent, autonomously ng in solar arrays		
			Harness too cold		If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None							
ME-1.1.2 ME-1.2	Solar Array #2 HGA																			
	HGA Gimbal																			,
ME-1.2.1.a			Fails to actuate when commanded (mechanical failure)	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	umbra violation	Autonomy	7	?	None				re-command, slew	nmand to a "safe" iition		
ME-1.2.1.b			Fails to actuate when commanded (electrical failure)		If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	umbra violation	Autonomy	?	?	None				Each motor winding goes to a different ECU.			
ME-1.2.1.c			Incorrect actuation when commanded		If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	umbra violation	Autonomy	?	?	None				re-command slew	nmand to a "safe" iition		

		_					Ef	fect						Detection Method		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes Pha	ase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)
ME-1.2.1.d			Mechanical bias of actuator			HGA consistently moves to incorrect position	Turn on back-up ECU to verify potentiometer readings. Switch to redundant ECU. Recommand to proper position.	Ground would review long- term trending to see what corrections need to be made in commanded position to compensate for bias. Possible decrease in gain, but should be no long-term mission effects.	N/A	4	Active	Yes	Long-term trending of commanded vs. actual position (verified by potentiometers connected to both ECUs and the motor's step count).	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-1.2.1.e			Moves when not commanded	Holding torque exceeded (need to have sufficient margin)		HGA is in wrong position	Re-command to proper position	None	If this occurs during encounter and if stuck at large enough angle, could be an umbra violation (~90-102deg is safe)	4	Active	Yes	Potentiometer telemetry, step count	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-1.2.1.f			Launch locks fail to release	1) Frangibolt pyro fails to actuate		Failure to blow first pyro	Command second pyro to blow	No effect.	N/A	4		Yes	??			
ME-1.2.1.g			Launch locks fail to release	1) Frangibolt fails to release completely (mechanical failure of frangibolt) 2) Separation interfaces fail to C release completely (mechanical clearance issues/unexpected interferences)		HGA stuck stowed	Could slew s/c to use HGA.	Difficulty in meeting mission science data return requirements.	Would exceed "safe" angle	2		Yes	Potentiometer telemetry			
ME-1.2.1.h			Launch locks premature release	1) Temperature exceeds ~65C and frangibolt releases 2) inadvertent command 3) Incorrect notch on frangibolt		Dish may vibrate more than expected (causing damage), gimbal may degrade	Reduced ability to return science data.	Potential loss of science if dish damaged, eventual loss of science with premature failure of gimbal	When bearing dies, if stuck in position outside of "safe"	2		No				
Inputs			ECU commands (pulsed power)			HGA is in wrong position	Switch to redundant ECU	No effect.	N/A	4		Yes	Potentiometer telemetry, step count			
ME-1.3 Pc	otentiometers	2 per actuator, each connected to a single ECU. Telemetry decribes actual motor position.											com			
ME-1.3.a			Open up (expected temporarily due to signal drop-out and reconnected after movement complete)			Powered potentiometer stops sending telemetry temporarily.	Can utilize step count for confirmation of motion, or power redundant ECU to check redundant potentiometer.	No effect.	N/A	4	Active	Yes	Lose potentiometer telemetry	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-1.3.b			Open up (permanent)			Powered potentiometer stops sending telemetry permanently.	Switch to redundant ECU/potentiometer. Still have 2nd vote from step count.	No effect.	N/A	4	Active	Yes	Lose potentiometer telemetry	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-1.3.c		-	Crack in substrate causes loss of both potentiometers			Both potentiometers fail.	Still have step count from motor (this is a relative motion measurement, not actual position, and only counts commands actually received by motor).	Loss of confidence in position of actuator.	N/A	4	Active	Yes	Lose potentiometer telemetry	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-1.3.d			Wrong value			Powered potentiometer indicates incorrect value.	Compare against step count, if they don't match, then power the redundant ECU to check against redundant potentiometer - 2 of 3 voting. May need to switch ECUs to avoid faulty potentiometer.		N/A	4	Active	Yes	Potentiometer telemetry, step count	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Time to Detect (System)
ME-1.2.1.d			Mechanical bias of actuator	?
ME-1.2.1.e			Moves when not commanded	?
ME-1.2.1.f			Launch locks fail to release	
ME-1.2.1.g			Launch locks fail to release	
ME-1.2.1.h			Launch locks premature release	
Inputs			ECU commands (pulsed power)	
ME-1.3		2 per actuator, each connected to a single ECU. Telemetry decribes actual motor position.		
ME-1.3.a			Open up (expected temporarily due to signal drop-out and reconnected after movement complete)	?
ME-1.3.b			Open up (permanent)	?
ME-1.3.c			Crack in substrate causes loss of both potentiometers	?
ME-1.3.d			Wrong value	?

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

Mech - 88 of 317

								Resp	onse						Quick Look		1			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally		Desired System	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Processor Switch	Safe Mode	Remediation/ notes	Autonomy?	Comments	Revisit
ME-1.2.1.d			Mechanical bias of actuator	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	umbra violation	Autonomy	?	?	None							
ME-1.2.1.e			Moves when not commanded	Local	Recommand? If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???		?	?	umbra violation	Autonomy	?	?	None				re-command, slew	command to a "safe" position		
ME-1.2.1.f			Launch locks fail to release														slew to Sun, oversized motor can bust through, recommand frangibolt		Are redundant pyro commands sent as part of deployment?	
ME-1.2.1.g			Launch locks fail to release																	
ME-1.2.1.h			Launch locks premature release														If HGA and fan beams are permanently off- pointed (boresight no longer aligns), would be able to compensate with more DSN time.			
Inputs			ECU commands (pulsed power)														re-command, slew	command to a "safe"		
ME-1.3	Potentiometers	2 per actuator, each connected to a single ECU. Telemetry decribes actual motor position.																position		
ME-1.3.a			Open up (expected temporarily due to signal drop-out and reconnected after movement complete)	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	?	?	?	?	None							
ME-1.3.b			Open up (permanent)		If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???		?	?	?	?	?	?	None							
ME-1.3.c			Crack in substrate causes loss of both potentiometers	Local	if potentiometer and step count are mismatched, turr on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch??? Not sure what to do when redundant pot also shows	Autonomy	?	7	?	?	?	?	None							
ME-1.3.d			Wrong value	Local	mistmatch? If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???		?	?	?	?	?	?	None							

	_				Ef	fect						Detection Method		
FMEA ID Name	Function	Failure Mode / Limit / Constraint	Possible Causes Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)
ME-1.3.e		Life-limiting # of cycles		Both potentiometers fail.	Still have step count from motor (this is a relative motion measurement, not actual position, and only counts commands actually received by motor).	Loss of confidence in position of actuator.	N/A	4	Active	Yes	Lose potentiometer telemetry	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-2 Instruments ME-2.1 FIELDS														
ME-2.1.1 Magnetometer Boom														
ME-2.1.1.a		Doesn't deploy (detail to come)	1) Launch lock doesn't release 2) Hinge jams/locks 3) Damper freezes	MAG boom is stowed	Degradation of science (loss of Magnetic field measurements, loss of redundant measurements for Electric Field and Plasma Waves)	Degraded science, but loss of	N/A (not with boom still stowed, loss of individual joint could cause violation)	3		Yes	MAG would see s/c noise and no change in MAG levels (expected as boom deploys)			
ME-2.1.1.b		Deploys prematurely (detail to come)	1) launch lock released prematurely 2) inadvertent command (safety-inhibited load - safety bus relay can't be uninhibited by SW)	Boom would deploy	depending on orientation of fold, could hit s/c, shroud, damage an instrument, might block thruster or instrument FOV; could affect flight path or thermal environment	potential damage to s/c, loss of sensors, etc.; unless failure corrects itself with release of shroud. Loss of MAG sensor is not enough to be a loss of science.	No	2 - if enough critical components/ instruments are damaged 3 - if only loss of MAG sensor		Yes	When instruments powered, might see damage caused by premature deployment			
ME-2.1.1.c		Partial deployment	One or more hinges jams or locks One potential design has one launch lock, one potential design has two launch locks. Revisit after decision has been made.	Boom would only partially deploy	Loss of MAG boom	If outside umbra, will outgas, melt, bring thermal load into s/c. Paticulate matter, thermal load, outgassing, etc., are potentially mission-ending. Loss of the MAG sensor does not equal loss of science.	Yes	2			GNC might be able to tell from mass properties, torque from solar pressure, etc. Science team may see thermal effects.			
Inputs		Electrical fault		Command sent by both sides. No single electrical failure should prevent deployment.	If entire command fails, ground can re-send. A-side PDU drivers may have failured, so an avionics (PDU) side switch could allow command to be resent.	None	N/A	2						

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Time to Detect (System)
ME-1.3.e			Life-limiting # of cycles	?
ME-2	Instruments			
ME-2.1 ME-2.1.1	FIELDS Magnetometer Boom			
ME-2.1.1.a			Doesn't deploy (detail to come)	
ME-2.1.1.b			Deploys prematurely (detail to come)	
ME-2.1.1.c			Partial deployment	
Inputs			Electrical fault	

Solar Probe Plus (SPP) Failure Modes and Effects Analysis (FMEA)

Mech - 91 of 317

								Resp	onse						Quick Look					
						Allegation of	Time to fix			Allocation of	Time to fin	Thurs he	Constant Description /	System Side	Processor	Safe Mode				
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of			Desired System	System	Time to fix	Time to	Ground Response /	Switch	Switch		Remediation/ notes	Autonomy?	Comments	Revisit
						Local Response	locally	Transmit Signal	Response	Response	system	Transmit Signal	Contingency							<u> </u>
				.]																
				1	If potentiometer and step															
					count are mismatched, turn	l l														
					on redundant ECU for 3rd]														
					vote; If third vote is correct															
				1	power off primary ECU]			I											
					otherwise system side	l l														
					switch???															
ME-1.3.e			Life-limiting # of cycles	Local		Autonomy	?	?	?	?	?	?	None							
					Not sure what to do when]														
					redundant pot also shows															
					mistmatch?															
						l l														
					Would not help in this case,															
					but detection/response															
					would look the same	i i														
	<u> </u>					<u> </u>										ļ			ļ	ļ
ME-2	Instruments					ļ										ļ			ļ	
ME-2.1	FIELDS					ļ										ļ			ļ	
ME-2.1.1	Magnetometer Boom			. .		ļ										ļ	ļļ			
									I											
ME-2.1.1.a			Doesn't deploy (detail to come)]			l								re-command, slew			х
									I											
	 			·•		ļ			·····					·		·	·		·	
						l l			İ											
ME-2.1.1.b			Deploys prematurely (detail to come)																	Х
				1]			I											
						l l														
						1														
						l l														
ME-2.1.1.c			Partial deployment																	
						i i														
						ļI														
									I											
									I											
Innute			Floateigal foult			1														
Inputs			Electrical fault						I											
	1	1	<u> </u>	•	1			•			.			1		i	1		1	i

Stewart Bushman (Propulsion)

Notes: Yellow highlighted blocks are redundant

Matter Robin Vaughan (Effects to S/C and/or G&C) components. Components are listed for completeness but failure mode and FMEA information is only displayed Expert(s): Type of FM Tlm for Diagnosis Tlm Path for FMEA ID Failure Mode / Limit / Constraint Possible Causes Phase Severity Time to Time to Detect Detect (Local) (System) Service Valves PR-1.1 Service Valve 1 (SV1) (Pressurant) ssion-ending with Over time will decrease Pressure decrease, wheels might Check presssure omplete loss of External leak (three seals would have to fail PR-1.1.a 1) Physical damage system pressure, may torque pressurant or if amount of torque see an unexpected torque (long- from P3 against for this to occur) ith 3 seals s/c (depends on size of leak) enough torque is and timing term trending) evious reading? pplied PR-1.2 Service Valve 2 (SV2) (Liquid) Depends on Pressure decrease, wheels might Check presssure External leak (three seals would have to fail mount of fuel, could omplete loss of fuel amount of fuel, could complete loss of fuel amount of torque damage if it impacted the s/c, or if enough torque is fuel loss annolied and timing 1) Physical damage see an unexpected torque (long-Leaking hydrazine for this to occur) ith 3 seals term trending) applied fuel loss PR-2 1) Physical damage Unusable propellan PR-2.a nternal leak (liquid into gas) that can't be pushed Less fuel overall You'd run out of fuel early (pinhole leak in ns out of usable fuel out of usable fuel diaphragm) out of the tank ver time will decrease mplete loss of Pressure decrease, wheels might 1) Physical damage PR-2.b External leak (pressurant) Leaking helium 2 system pressure, may torque pressurant or if amount of torque see an unexpected torque (long- from P3 against s/c (depends on size of leak) nough torque is and timing term trending) Over time will decrease sion-ending with Depends on Pressure decrease, wheels might Check presssure mount of fuel, could omplete loss of fuel PR-2.c External leak (fuel) L) Physical damage Leaking hydrazine damage if it impacted the s/c, or if enough torque is and timing amount of torque 2 see an unexpected torque (long- from P3 against term trending) vious reading applied PR-3 Pressure Transducers Pressure Transducer A (PTA Draw too much See high current draw in PDU current tlm for PTA nrush current issue use would blow o effect current telemetry PR-3.1.a nvalid output Check other transducer Output invalid Lack of knowledge of at least for every TCM), might No effect No current draw, if current is 1) Physical damage PDU current tlm PR-3.1.b Hard failure fine, but data is bad, might be in require switching avionics narness/sampling electronics sides (TBD) Over time will decrease Aission-ending with Depends on Pressure decrease, wheels might heck presssure mount of fuel, could External leakage (two seals would have to mplete loss of fuel PR-3.1.c L) Physical damage Leaking hydrazine damage if it impacted the s/c, or if enough torque is and timing amount of torque see an unexpected torque (longrom P3 against leak in order for this to occur) term trending) No power to r PTA; PDU transducer wer state for Filter 1 (F1) Yes if it happene 1) FOD in line at the wrong tim Blocked prevents all thruster PR-4.a Clogged or blocked 2) Contaminated rusters stopped working opellant done at that poir nyway PR-5 Orifice 1 (O1) Yes if it happene L) FOD in line at the wrong time Blocked prevents all thruster PR-5.a Heavy contamination blockage 2) Contaminated No fuel to thrusters but mission is Thrusters stopped working opellant done at that poin anyway Propulsion Diode Box (PDB es if it happene at the wrong time Could lose one PR-6.a tem is 1-fault tolerant Would this affect manuever? Any failure of any diode or resistor but mission is thruster or LV edundancy? done at that poin anyway Latch Valve A (LVA)

Subject Stewart Bushman (Propulsion) Notes: Yellow highlighted blocks are redundant
Matter Robin Vaughan (Effects to S/C and/or G&C)
Expert(s): Notes: Yellow highlighted blocks are redundant components are listed for completeness, but failure mode and FMEA information is only displayed

Expert(s).		Dut famale into	ac and TWEA mornation is only displayed						Response					Quick Look					
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency System Side Switch	Processor Switch	Safe Mode	KAF Comments	Remediation	Autonomy?	Revisit
	Service Valves																		
PR-1.1 PR-1.1.a	Service Valve 1 (SV1) (Pressurant)		External leak (three seals would have to fail for this to occur)	None	None	None	None	None	None	None	None	None	None			P3 and P4 are not powered at the same time, need to understand how to determine pressure	Nope		
		ļ												ļ		decrease			<u>i</u>
PR-1.2 PR-1.2.a	Service Valve 2 (SV2) (Liquid)		External leak (three seals would have to fail for this to occur)	None	None	None	None	None	None	None	None	None	None				Nope		
PR-2	Tank	ļ						· • • • • • • • • • • • • • • • • • • •											<u></u>
PR-2.a			Internal leak (liquid into gas)	None	None	None	None	None	None	None	None	None	None				Nope		
PR-2.b			External leak (pressurant)	None	None	None	None	None	None	None	None	None	None				Nope		
PR-2.c			External leak (fuel)	None	None	None	None	None	None	None	None	None	None				Nope		
PR-3	Pressure Transducers																	In-rush current issue	i
PR-3.1	Pressure Transducer A (PTA)								·									issue	
			Inrush current issue	Local	Pwr off PTA	Autonomy			None	None	None	None	Yes - Ground/Prop will need to assess tlm associated with PTA and determine whether they want to power it back on or do a side switch to use PTB			No CB on this load; probably want to just power off PT and not do side switch			
PR-3.1.a			Invalid output	None	None	None	None	None	None	None	None	None	Will need to be contingency procedure for this? PT's are not powered at same time, if PT data is required would need to side switch; would power cycling/hard reset of PT be worth trying?						
PR-3.1.b			Hard failure	None	None	None	None	None	None	None	None	None	Will need to be contingency procedure for this? PT's are not powered at same time, if PT data is required would need to side switch				Hard reset		х
PR-3.1.c			External leakage (two seals would have to leak in order for this to occur)	None	None	None	None	None	None	None	None	None	None				Nope		
Input			Bus voltage	None	None	None	None	None	None	None	None	None	Will need ground contingency? Power cycle/hard reset PT; if PT data is required would need side switch						х
	Pressure Transducer B (PTB) Filter 1 (F1)																		·····
PR-4.a			Clogged or blocked	None	None	None	None	None	None	None	None	None	None				None		
PR-5	Orifice 1 (O1)																		<u></u>
PR-5.a			Heavy contamination blockage	None	None	None	None	None	None	None	None	None	None				None		
PR-6	Propulsion Diode Box (PDB)																		
PR-6.a			Any failure of any diode or resistor														None		
	Latch Valves Latch Valve A (LVA)																		······
	tamananinainahaihidamananananananananan	.i					·····		·	i	· i	i	iiiii		ā				

Section Sect								Effect							Detection Method			
March Marc	FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis			Time to Dete (System)
Marie Mari																	(Local)	
Property Property					1) Particulate, FOD					,	_							
Marie Mari				Internal leakage			closed, opened	None	None	N/a	4	None	No	No	N/A	N/A	N/A	N/A
Second Property			ļ			ļ	nominally	Over time will decrease	Mission anding with	ļ		ļ	ļ			ļ	ļ	ļ
Second S	DD 71h			External leakage (multiple seals would have	1) Physical damago		Loaking bydrazino				,	Passive -	Voc			N/A	NI/A	N/A
Registration of the second process of the se	PK-7.1.U			to fail in order for this to happen)	1) Physical damage		Leaking nyurazine				2	redundancy?	res			IN/A	N/A	N/A
Part Part			ļ					1003	аррпец									
State Stat															N/A : LV			
State Stat	PR-7.1.c			Fails open			closed, opened	None	None	N/a	4	None	No	No		N/A	N/A	N/A
					,		nominally											
Second S					1) Particulate, FOD		No effect, assuming											
Companies Comp	PR-7.1.d			Fails closed				None	None	N/a	4		No	No		N/A	N/A	N/A
Part Part			ļ			ļ	орен					ļ	ļ			ļ	ļ 	ļ
State Stat					2) Constant "ON"		1) Couldn't cycle	1) None assuming 2nd LV	1) None		1) 4			Current draw temperature	1) PDU LV current			
Market M	nputs			Bus voltage						N/a			Yes				N/A	N/A
Market M			ļ			Ļ	-, · · · ·	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		ļ					low side tlm			ļ
March Marc	PR-7.2 PR-8					ļ	<u> </u>					<u> </u>	ļ			ļ	ļ	
Registration of the second of	R-8.01																	
See Language and the property of the control of the	K-8.U1.1	Catbed Heater-Primary				ļ												
See Language and the property of the control of the																		
															PDU current tlm			
	R-8.01.1.a			Fails on			No effect	Power drain on s/c	Probably not mission- ending	N/A	4		Yes					N/A
Series of the se					apstream				chang			, aconomy, m						
Series of the se																		
Series of the se						ļ	¢		ç									
Significant properties of the							Switch to redundant											
AD IN THE PROPERTY OF THE PROP	PR-8.01.1.b			Fails off				None	None	N/A	4		Yes		:		N/A	N/A
The state of the control of the cont					2) Pilysical dalilage							Autonomy		current/voitage uraw	thrusters active?			
The state of the control of the cont			<u> </u>			<u> </u>	<u> </u> 	<u> </u>	<u> </u>			<u> </u>	<u> </u>			<u> </u>	<u> </u>	<u> </u>
The state of the control of the cont							Reduced heating											
The second of th	PR-8.01.1.c			Heater debonds from Cathed	1) Physical damage		(depends on		None	N/A	4	None	Yes		IMU tlm?		N/A	N/A
The second of th					-, ,												,,,,	,,,,
State of the control							·											
10.1.2 Filtration Filtratio	nput			Bus voltage			No power to heater		None	N/A	4						N/A	N/A
18.52 Section of the federal from Crited Final Processing of F		Catbed Heater-Secondary				<u>.</u>	<u> </u>	WUIKS		<u> </u>		Reduildancy	<u> </u>		current um			<u>.</u>
Mode: Assumpting for Collected Valvers) And 1, 1 extract claims and the control to the control	R-8.01.2.a R-8.01.2.b					ļ] 										ļ	
20.1.3.8 Under NSZ. 20.1.4 Under NSZ. 20.1.4 Under NSZ. 20.1.4 Under Not suith to exponsive for interest to find effect on which is not such as under volution by control of suite in the surface of the	R-8.01.2.c		ļ	······································			\$ 					·••				}		ļ
8.01.3.1 Water would continue to fire unless text to whe close of the failed open or both leak	R-8.01.3	Valve Assembly (NC Solenoid Valves)				ļ												
8.01.3.2 Both failed open or both leak 21 FOD 1 leak middle open or both leak 21 FOD 2 leak 21 FOD 2 lea																		
8.01.3.b Roth failed open or both leak 2 FOD																		
SOLIA De la Bus voltage Bus vo	D 0 01 2 5			Dath failed open or both look	1) electrical failure		Valves wouldn't	Thruster would continue to		Voc	significantly depleted	Passive -	Mauha	Thruster continues to fire after				NI/A
8.01.3.b	N-0.U1.3.a			Both falled open of both leak	2) FOD		close	fire unless latch valve closed	AU). Probably mission	res	changeu	redundancy	iviaybe	commanded to stop	tlm			N/A
8.01.3.b																		
8.01.3.b long or both failed closed 2) Popular and the set of thrusters, 4c might be set of thrusters, 5c might be set of thrusters, 5c might be set of thrusters, 5c might be set of thrusters, 5c might be set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters, 5c might be detectable through current/voltage sensing under the set of thrusters available, but TCMs would probably need to be aborted. Couldn't use thrusters, 5c might be detectable through current/voltage sensing under the sepected vs. actual under the set of thrusters, 5c might be detectable through current/voltage sensing under the set of thrusters, 5c might be sepected, an electrical issue might be detectable through current/voltage sensing under the									would curtain it.			3						
8.01.3.b long or both failed closed 2) Popular and the set of thrusters, 4c might be set of thrusters, 5c might be set of thrusters, 5c might be set of thrusters, 5c might be set of thrusters, 5c might be set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters are surmountable under the set of thrusters, 5c might be detectable through current/voltage sensing under the set of thrusters available, but TCMs would probably need to be aborted. Couldn't use thrusters, 5c might be detectable through current/voltage sensing under the sepected vs. actual under the set of thrusters, 5c might be detectable through current/voltage sensing under the set of thrusters, 5c might be sepected, an electrical issue might be detectable through current/voltage sensing under the						ļ												
8.01.3.b																		
8.01.3.b One or both failed closed One or both closed One or both failed closed One or both failed closed One or both failed closed One or both closed One or both failed closed One or both closed One or					1) plactrical failure				timing). Momentum					Post-burn attitude isn't as				
switch-over and momentum but TCMs would probably need to be aborted. **Description** **De	R-8.01.3.b			One or both failed closed			Couldn't use thruster			Yes	2	None	Maybe					
probably need to be aborted. Bus voltage Bus voltage Couldn't use thruster ob, depending on speed of switch or another steef of thrusters, syc might be distributed for switch-over and momentum issues are surmountable probably need to be aborted. Couldn't use thruster ob, depending on speed of switch-over and momentum issues are surmountable probably need to be aborted. Couldn't use thruster ob, depending on speed of switch-over and momentum issues are surmountable probably need to be aborted. None Maybe Post-burn attitude isn't as expected, an electrical issue emight be detectable through current/voltage sensing Attitude tim-expected vs. actual probably need to be aborted.					3) Physical issue										expected vs. actual			
Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Couldn't use thruster of could switch to another set of thrusters, syc might be oble, ok, depending on speed of switch-over and momentum issues are surmountable but TCMs would probably need to be aborted. Bus voltage Post-burn attitude isn't as expected, an electrical issue might be detectable through current/voltage sensing Attitude tIm - expected vs. actual current/voltage sensing Bus voltage Rottinde tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude tim - expected vs. actual current/voltage sensing Bus voltage Attitude									probably need to be									
ending (depending on things). Momentum that a large service of thrusters, s/c might be severed year and such as the sum of the sex of thrusters, s/c might be sex of thrusters, s/c might be sex of thrusters, s/c might be sex of thrusters, s/c might be sex of thrusters, s/c might be sex of thrusters, s/c might be sex of thrusters available, but TCMs would probably need to be abovred. 8.02 Thruster A2 8.02 Thruster A2 8.02 To be dieater-Primary 8.03 To be dieater-Primary 8.04 Thruster A2 8.05 Thruster A2 8.06 Thruster A2 8.07 Thruster A2 8.08 Thruster A2 8.09 Thruster A2 8.00 Thruster A2 8.			 			ļ	ļ		aborted.	ļ		ļ	ļ			ļ		ļ
Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Bus voltage Couldn't use thruster of couldn't use thruster on the county of the county																		
Bus voltage Bus v								If s/c could switch to another						Dark house and the first				
Bus Voltage Coulon't use through switch-over and momentum intrusters available probably need to be aborted. 8.02 Thruster AZ Subsequence Coulon't use through of the probably need to be aborted.	nout			Rus voltago			Couldn't use the	set of thrusters, s/c might be	dumps would be ok	Voc	2	None	Maybo		Attitude tlm -			
8.02 Thruster A2 8.02 Catbod Healer-Primary	nput			ous voltage			Coulan t use thruster			res	2	ivone	iviaybe	might be detectable through				
8.02 Truster AZ								issues are surmountable						carreing voitage sensing				
8.02.1 Catbed Heater-Primary																		
	R-8.02					<u> </u>	(<u> </u>								ļ
			 			ļ	<u> </u>		<u> </u>	<u> </u>		<u> </u>	<u> </u>			<u> </u>	<u> </u>	<u> </u>

	_							Respons						Quick Look					_
MEA ID	Name	Function Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Processor Switch	Safe Mode	KAF Comments	Remediation	Autonomy?	Revisi
'.1.a	(redundant, in parallel, opened during launch countdown or directly after launch, not closed again during nominal mission)	Internal leakage	None	None	None	None	None	None	None	None	None	None - Cycle valve? But if this isn't observable how would we know to cycle?					Cycle valve		
.1.b		External leakage (multiple seals would have to fail in order for this to happen)	e None	None	None	None	None	None	None	None	None	None					Nope		ļ
'.1.c		Fails open	None	None	None	None	None	None	None	None	None	None - Cycle valve? But if this isn't observable how would we know to cycle?				Leaky thruster in combo with open/leaky latch valve would cause loss of fuel	Cycle valve		
'.1.d		Fails closed	None	None	None	None	None	None	None	None	None	None - Cycle valve? But if this isn't observable how would we know to cycle?				If both fail closed, thrusters won't work	Cycle valve		ļ
ts		Bus voltage	None	None	None	None	None	None	None	None	None	None							
7.2 3 3.01 3.01.1	Latch Valve B (LVB) Thrusters Thruster A1 Catbed Heater-Primary																		
-8.01.1.a		Fails on	Local	1) Power off Catbed heater 2) CB trips	1) Autonomy 2) HW				None	None	None					Is there a CB for this load?	Cycle power, circuit breaker would take down primary heater power to several thrusters		
.01.1.b		Fails off	Local	If primary catbed heater off & thrusters active, switch to redundant heater	Autonomy			None	None	None	None	Cycle power to primary catbed heater during next ground contact?					Cycle power		
8.01.1.c		Heater debonds from Catbed	None	None	None	None	None	None	None	None	None	None				W/Aerojet thruster, both heaters are in a single cartridge and would debond at the same time			
ıt		Bus voltage	None	None	None	None	None	None	None	None	None	None				Same time			
.01.2 .01.2.a	Catbed Heater-Secondary	Fails on																	ļ
3.01.2.b 3.01.2.c		Fails off Heater debonds from Catbed													d				ļ
	Valve Assembly (NC Solenoid Valves)																		
·8.01.3.a		Both failed open or both leak	Local?	If thrusters firing when maneuver not active, close latch valves	Autonomy			None	None	None	None	None					Close latch valves		
-8.01.3.b		One or both failed closed															Cycle power to valves		
ut		Bus voltage															Cycle power to valves		
8.02	Thruster A2									<u></u>									<u> </u>
	Catbed Heater-Primary		1			i	1		i	:		i	;	:	•		:		

							Effect							Detection Method			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
	Valve Assembly															(2000)	
PR-8.03 PR-8.03.1	Thruster A3	-		<u> </u>	 .				ļ								[
	Catbed Heater-Primary Catbed Heater-Secondary				 									-			f
	Valve Assembly				······				ļ								<u>!</u>
PR-8.04	Thruster A4				······												 !
	Catbed Heater-Primary						D		ð)		::
PR-8.04.2	Catbed Heater-Secondary																å
	Valve Assembly																<u> </u>
PR-8.05	Thruster B1	<u>.</u>															<u> </u>
	Catbed Heater-Primary								ļ								;·····
	Catbed Heater-Secondary Valve Assembly								ļ								[
PR-8.06	Thruster B2				······												
	Catbed Heater-Primary							***************************************									······
	Catbed Heater-Secondary				į												
	Valve Assembly								ļ								<u> </u>
PR-8.07	Thruster B3																·
	Catbed Heater-Primary Catbed Heater-Secondary				·····				ļ								<u>:</u>
	Valve Assembly																i
PR-8.08	Thruster B4				······												
PR-8.08.1	Catbed Heater-Primary			į	ĺ												į
	Catbed Heater-Secondary				<u>į</u>				ļ								j
PR-8.08.3	Valve Assembly				<u></u>												}
PR-8.09 PR-8.09.1	Thruster C1				.												} ^j
PR-8.09.2	Catbed Heater-Primary Catbed Heater-Secondary			-					ļ								
	Valve Assembly								<u> </u>					·			
PR-8.10	Thruster C2			i	ì												i
	Catbed Heater-Primary																į
	Catbed Heater-Secondary				ļ.				ļ								j [†]
PR-8.10.3 PR-8.11	Valve Assembly								ļ								;
	Thruster C3 Catbed Heater-Primary								ļ								i
	Catbed Heater-Secondary				·····-												
	Valve Assembly																
PR-8.12	Thruster C4																
	Catbed Heater-Primary																} []]
	Catbed Heater-Secondary			 					ļ					·			r
	Valve Assembly Temperature Sensors				<u> </u>				·					·			/ <i>[</i>
	Temperature Sensor (generic - still deciding				<u>-</u>				1					·			
	locations)				i												į
	Platinum RTDs		No output		Į	ack telemetry	No effect	No effect		4		Yes	Lack temp telemetry				j
PR-9.1.b			Incorrect output														<u>}</u>
Inputs PR-9.2	Temperature Sensor Ghe		Bus voltage														;·····;
PR-9.2.a	remperature sensor dire		No output						ļ					·			/ <i>[</i>
PR-9.2.b			Incorrect output											-			
PR-9.3	Temperature Sensor N2H2																i
PR-9.3.a			No output						ļ								}
PR-9.3.b	T		Incorrect output						ļ								}
PR-9.4 PR-9.4.a	Temperature Sensor F1		No output						ļ					ļ			<i>[</i>
PR-9.4.b			No output Incorrect output						ļ								
	Temperature Sensor LV Manifold	1							İ								
PR-9.5.a			No output														
PR-9.5.b			Incorrect output						ļ								}
	Temperature Sensor Thruster Manifold								ļ								}
PR-9.6.a PR-9.6.b			No output Incorrect output	ļ	ļ.									-			<i>[</i>
	Temperature Sensor A4		meorrect output	 	 				<u> </u>								[
PR-9.7.a			No output		······												······································
PR-9.7.b			Incorrect output		······				1								i
PR-9.8	Temperature Sensor B4				Ì												\$
PR-9.8.a			No output						ļ								}
PR-9.8.b	T		Incorrect output						ļ					ļ			}
PR-9.9 PR-9.9.a	Temperature Sensor C4		No output						ļ					-			········
PR-9.9.a PR-9.9.b			No output Incorrect output						<u> </u>								
			in the second se				ā	·····	å	i	`	i			······		

								Response						Quick Look					
FMEA ID	Name	Function Failure Mode / Limit / Constraint	Response Level	Desired Local	Allocation of	Time to fix	Time to	Desired System	Allocation of System	Time to fix	Time to Transmit	t Ground Response / Contingency	System Side	Processor Switch	1 Safe Mode	KAF Comments	Remediation	Autonomy?	Revisit
				Response	Local Response	locally	Transmit	Response	Response	system	Signal	,	Switch				i '		
							Signal										 '		
R-8.02.3	Valve Assembly																		
PR-8.03	Thruster A3																i		
	Catbed Heater-Primary																į		
	Catbed Heater-Secondary		<u>.</u>		<u>.</u>		Ĭ			i	<u>.</u>		<u>.</u>	<u>.</u> 				<u>.</u>	
	Valve Assembly				<u>.</u>		į)			<u>.</u>			<u>.</u> 			į	<u>.</u>	
PR-8.04	Thruster A4				<u>.</u>		į)			<u> </u>			<u>.</u> 			į	<u>.</u>	
	Catbed Heater-Primary				ļ		į			<u></u>	<u> </u>			į				<u> </u>	
	Catbed Heater-Secondary				ļ		Į			ļ	ļ			į 			į	<u> </u>	
	Valve Assembly				ļ					ļ							j	ļ	
PR-8.05	Thruster B1				ļ												ļ'		
	Catbed Heater-Primary						ļ			ļ							ļ		
	Catbed Heater-Secondary						ļ			ļ							ļ	ļ	
PR-8.05.3	Valve Assembly	ļ			ļ		ā			ļ	ļ			ļ 			<u> </u>	ļ	
PR-8.06	Thruster B2 Catbed Heater-Primary	·			ļ		ļ			ļ				ļ			<u> </u>	ļ	
	Catbed Heater-Primary Catbed Heater-Secondary			- 	ļ		<u> </u>			ļ	ļ						<u> </u>	ļ	
PR-8.06.3	Valve Assembly						ļ			!	ļ			ļ			į [']	ļ	
PR-8.07	Thruster B3	<u> </u>			ł		<u> </u>			!	ļ			ļ			·	†	
	Catbed Heater-Primary	1		1	†		i			į Į	ļ	1		 !	1		<i>[</i>	<u> </u>	
	Catbed Heater-Secondary			·	1		······································			 [ļ				1		[
PR-8.07.3	Valve Assembly									ļ									
PR-8.08	Thruster B4						 !										: :		
	Catbed Heater-Primary						Ĭ			İ							i		
PR-8.08.2	Catbed Heater-Secondary						Ĭ										i		
PR-8.08.3	Valve Assembly				[I										i		
PR-8.09	Thruster C1				<u> </u>												į		
	Catbed Heater-Primary				j									<u></u>				<u></u>	
PR-8.09.2	Catbed Heater-Secondary				ļ		Į			ļ							į	<u> </u>	
	Valve Assembly				ļ	,	Į	,		ļ	ļ			,			ļ	ļ	
PR-8.10	Thruster C2				ļ					ļ							ļ		
	Catbed Heater-Primary																ļ'	<u> </u>	
	Catbed Heater-Secondary						ļ							ļ			ļ	ļ	
	Valve Assembly						ļ			.							ļ	ļ	
PR-8.11 PR-8.11.1	Thruster C3 Catbed Heater-Primary	·			ļ					ļ	ļ			ļ			! [']	ļ	
	Catbed Heater-Secondary						ļ				ļ						į [']	}	
PR-8.11.3	Valve Assembly				······································		·····										į	<u> </u>	
PR-8.12	Thruster C4			·	······		·····				ļ						f	<u> </u>	
	Catbed Heater-Primary				·		ō Ī)		₫				;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;			 Í		
PR-8.12.2	Catbed Heater-Secondary						•·····································]				;			······································) 	
R-8.12.3	Valve Assembly																i		
PR-9	Temperature Sensors		<u></u>		<u> </u>		<u> </u>			<u> </u>	<u> </u>		<u></u>	<u> </u>	<u>.]</u>		<u> </u>	<u> </u>	
PR-9.1	Temperature Sensor (generic - still deciding																'		
	locations)						ļ										ļ	<u> </u>	
PR-9.1.a	Platinum RTDs	No output					Į										ļ	ļ	Х
PR-9.1.b		Incorrect output			,		ļ)		ļ							j	ļ	X
nputs	Tomporatura Sansar Cha	Bus voltage			ļ		<u> </u>)		ļ	ļ			· ·	·•		<u> </u>	ļ	Х
PR-9.2 PR-9.2.a	Temperature Sensor Ghe	No output		-	†												ļ		
PR-9.2.b		Incorrect output		·	}					<u></u>	ļ						i	ļ	
PR-9.3	Temperature Sensor N2H2	полес окри			1		1			1					1		·	1	
PR-9.3.a		No output		1	†		1			İ					1		(<u> </u>	1
PR-9.3.b		Incorrect output					Ī			Ī					1		 !		
PR-9.4	Temperature Sensor F1				I		I			İ					1		i		
PR-9.4.a		No output					Ĭ			İ							i	<u></u>	
PR-9.4.b		Incorrect output								<u></u>									
PR-9.5	Temperature Sensor LV Manifold				<u></u>		Į			<u></u>							į		
PR-9.5.a		No output			<u> </u>		Į								.[
PR-9.5.b		Incorrect output			<u> </u>		Į			ļ	<u> </u>			ļ	.]		i	<u> </u>	
PR-9.6	Temperature Sensor Thruster Manifold	<u> </u>			ļ					ļ	ļ						j		
PR-9.6.a		No output		.	ļļ	ļ				ļ	ļ			ļ			į		
PR-9.6.b	-	Incorrect output			ļ						ļ						ļ'		
	Temperature Sensor A4	No. and and an annual a			ļ		ļ			ļ	ļ			ļ			ļ	ļ	
PR-9.7.a		No output			ļ		<u> </u>			ļ	ļ			ļ			ļ	ļ	
PR-9.7.b	Tomporatura Cancar B4	Incorrect output		-	ļ												ļ	<u></u>	
D O O	Temperature Sensor B4	No output		-	}												·	<u></u>	
PR-9.8				i						ļ	ļ			}			ł	}	
PR-9.8.a		Incorrect output		1															
PR-9.8.a PR-9.8.b	Temperature Sensor C4	Incorrect output															ļ	ļ	
R-9.8.a	Temperature Sensor C4	Incorrect output No output																	

Subject Liz Abel (Thermal)

Matter Jack Ercol (Active Cooling)

Expert(s):

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode

Expert(s):		listed for completen	ess, but failure mode			•	-	Host		:				Detection Metho	al .		
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	ffect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	TIm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
	MLI Spacecraft MLI	Insulate spacecraft															
TH-1.1.a		bus	Degraded/damaged	1) Dust 2) Optical properties		MLI degraded/damaged.	Depends on amount of damage, but would increase/decrease local temperatures.	Depends on area affected by degradation/damage.	Depends on area affected by degradation/damage - critical system damaged by high temperature could lead to an umbra violation.	2	None		Component temperature change			N/A	
TH-1.2	High-temperature MLI	Insulate exposed portions of spacecraft (solar arrays, radiators, etc.)															
TH-1.2.a			Degraded/damaged	1) Dust 2) Optical properties		MLI degraded/damaged.	Depends on amount of damage, but would increase/decrease local temperatures.	Depends on area affected by degradation/damage.	High-temp MLI is not covering equipment that could lead to an umbra violation.	2	None		Component temperature change			N/A	
	Louvers 20-blade #1	Regulate temperature of spacecraft bus															
TH-2.1.a			Doesn't open/close	1) Bi-metalic spring failure 2) bearing/bushing bound iup [3] Louver has been overheated, so spring has a new set-point - would require additional failure causing overheating]		Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	system includes margin	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design		Temperature change over time			N/A	
TH-2.1.b			Blade breaks	1) Dust		Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over time			N/A	
TH-2.2 TH-2.2.a	20-blade #2		Doesn't open/close	1) Bi-metalic spring failure 2) bearing/bushing bound up [3] Louver has been overheated, so spring has a new set-point - would require additional failure causing overheating]		Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	res	Temperature change over time			N/A	
TH-2.2.b			Blade breaks	1) Dust		Increase/decrease temperature slightly.	system includes	system includes margin	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design		Temperature change over time			N/A	
TH-2.3 TH-2.3.a	14-blade		Doesn't open/close	1) Bi-metalic spring failure 2) bearing/bushing bound up [3) Louver has been overheated, so spring has a new set-point - would require additional failure causing overheating)		Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design		Temperature change over time			N/A	
TH-2.3.b			Blade breaks	1) Dust		Increase/decrease temperature slightly.	system includes	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over time			N/A	

Subject Liz Abel (Thermal)

Matter Jack Ercol (Active Cooling)

Expert(s):

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode

Expert(s):		listed for completen	iess, but failure mode						Response					E	Quick Look		l .	
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal		Allocation of System Response	Time to fix System	Time to Transmit Signal	Ground Response / Contingency		Processor Switch	Safe Mode	Comments - KAF	Revisit
	MLI Spacecraft MLI	Insulate spacecraft																
TH-1.1.a			Degraded/damaged				N/A	Depends on severity of degradation/d amage (time required to see temperature change in component)										
TH-1.2	High-temperature MU	Insulate exposed portions of spacecraft (solar arrays, radiators, etc.)																
TH-1.2.a			Degraded/damaged				N/A	Depends on severity of degradation/d amage (time required to see temperature change in component)										
	Louvers 20-blade #1	Regulate temperature of spacecraft bus																
TH-2.1.a			Doesn't open/close				N/A	Time required to see temperature change in component										х
TH-2.1.b			Blade breaks				N/A	Time required to see temperature change in component				ō						х
TH-2.2	20-blade #2		Doesn't open/close				N/A	Time required to see temperature change in component										х
TH-2.2.b			Blade breaks				N/A	Time required to see temperature change in component										х
TH-2.3 TH-2.3.a	14-DIAGE		Doesn't open/close				N/A	Time required to see temperature change in component										х
TH-2.3.b			Blade breaks				N/A	Time required to see temperature change in component				8						х

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	' Possible Causes Phase	Local	Next Higher	ffect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Metho TIm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
TH-2.4.a			Doesn't open/close	1) Bi-metalic spring failure 2) bearing/bushing bound up (3) Louver has been overheated, so spring has a new set-point - would require additional failure causing overheating)	Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margir to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over time			N/A	
TH-2.4.b			Blade breaks	1) Dust	Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margir to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over time			N/A	
TH-2.5 7-blade #1 TH-2.5.a			Doesn't open/close	1) Bi-metalic spring failure 2) bearing/bushing bound up [3) Louver has been overheated, so spring has a new set-point - would require additional failure causing overheating]	increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margir to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over time			N/A	
TH-2.5.b			Blade breaks	1) Dust	Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margir to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over			N/A	
TH-2.6			Doesn't open/close	1) Bi-metalic spring failure 2) bearing/bushing bound up (3) Louver has been overheated, so spring has a new set-point - would require additional failure causing overheating]	Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margir to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over time			N/A	
TH-2.6.b			Blade breaks	1) Dust	Increase/decrease temperature slightly.	No effect. Thermal system includes margin to account for loss of one blade.	No effect. Thermal system includes margir to account for loss of one blade.	No effect. Thermal system includes margin to account for loss of one blade.	2R/4	Passive - Design	Yes	Temperature change over			N/A	
TH-3 Heaters																
TH-3.1. Propulsion Tank Heaters TH-3.1.a	A&B (22 Ω switched)		Fails on	1) Thermostat failure 2) Failure of switch 3) Failure in heater	Autonomy will detect tank temperature and switch off power to that heater and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Tank temperature telemetry	Heater current; tank temperature	PDU to REM RIU to REM	N/A	
TH-3.1.b			Fails off	1) Thermostat failure 2) Failure of switch 3) Failure in heater	Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Tank temperature telemetry	Heater current; tank temperature	PDU to REM RIU to REM	N/A	
TH-3.1.c			Debonds from surface	1) Assembly/ installation failure 2) adhesive failure/defect	Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Tank temperature telemetry	Heater current; tank temperature	PDU to REM RIU to REM	N/A	
Inputs			Switched Power		Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	4	Active	Yes	Tank temperature telemetry	Heater current; tank temperature	PDU to REM RIU to REM	N/A	
TH-3.2 Propulsion Line and Valv	re Heaters A&B (37 Ω switched)															
TH-3.2.a			Fails on	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect high temperature and switch off power to that heater and switch to othe side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; line & valve temperatures	PDU to REM RIU to REM	N/A	
TH-3.2.b			Fails off	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; line & valve temperatures	PDU to REM RIU to REM	N/A	
TH-3.2.c			Debonds from surface	1) Assembly/ installation failure 2) adhesive failure/defect	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; line & valve temperatures	PDU to REM RIU to REM	N/A	
Inputs			Switched Power		Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	4	Active	Yes	Tank temperature telemetry	Heater current; line & valve temperatures	PDU to REM RIU to REM	N/A	

FMEA ID	Name Funct	tion Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit	Response Desired System Response	Allocation of System Response	Time to fix System	Time to Transmit	Ground Response / Contingency	Quick Look Processor Switch	Safe Mode	Comments - KAF	Revisit
							Signal				Signal					
																Į.
							Time required to see									į
TH-2.4.a		Doesn't open/close					temperature change in									Х
							component									į
																I
							Time required							ļ		
TH-2.4.b		Blade breaks					to see temperature									x
111-2.4.0		Diage Dieaks					change in									^
TH-2.5 7	7 blada #1					ļ	component						 			<i></i>
111-2.3 /	-Diade #1					ļ Ī							 			 !
							Time a service of									<u>!</u>
							Time required to see									!
TH-2.5.a		Doesn't open/close					temperature change in									Х
							component									!
																!
							Time required									
TH-2.5.b		Blade breaks				•	to see temperature									х
							change in									 I
TH-2.6 7	7-blade #7						component									
						<u> </u>										 !
							Time required									İ
							to see									į
TH-2.6.a		Doesn't open/close					temperature change in									Х
							component									<u>!</u>
																<u>!</u>
							Time required									
TH-2.6.b		Blade breaks					to see temperature									х
							change in component									İ
TH-3 F	-leaters					<u> </u>	<u> </u>									 !
	Propulsion Tank Heaters A&B (22 Ω switched)															······································
				Switch heater												<u>!</u>
TH-3.1.a		Fails on	Local	power off, power on	Autonomy	N/A	TBD time	None							No CB for switched heater; prop heaters were different than what Stewart expected	<u>!</u>
				redundant												İ
				Switch heater												••••••••••••••••••••••••••••••••••••••
TH-3.1.b		Fails off	Local	power on	Autonomy	N/A	TBD time									<u>!</u>
				redundant Switch heater			<u> </u>									
TH-3.1.c		Debonds from surface	Local	power off, power on	Autonomy	N/A	TBD time									İ
				redundant									 			j
Inpute		Switched Power	Local	Switch heater power off,	Autonomy	N/A	TBD time									i
Inputs		Switched POWEI	Local	power on redundant	Autonomy	14/15	100 title									i
TH-3.2 P	Propulsion Line and Valve Heaters A&B (37 Ω switched)															······
				Switch heater		j										
TH-3.2.a		Fails on	Local	power off,	Autonomy	N/A	TBD time								No CB for switched heater; prop heaters	i
				power on redundant											were different than what Stewart expected	i
				Switch heater			1									 !
TH-3.2.b		Fails off	Local	power off, power on	Autonomy	N/A	TBD time									i
				redundant Switch heater									 			······
TH-3.2.c		Debonds from surface	Local	power off, power on	Autonomy	N/A	TBD time									į
				redundant		ļ	ļ									;
Innuts		Switched Power	local	Switch heater power off,	Autonomy	N/A	TRD time									i
Inputs		owitched Power	Local	power on redundant	Autonomy	N/A	TBD time									i
ТН-3.3 р	Propulsion Internal Heaters A&B (28 Ω switched)					İ	<u> </u>							<u></u>		

FMEA ID Name	Function	Failure Mode / Limit / Constraint	Possible Causes Phase	Local	E Next Higher	ffect Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Metho TIm for Diagnosis	od TIm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
TH-3.3.a		Fails on	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect high temperature and switch off power to that heater and switch to othe side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; internal prop temperature	PDU to REM RIU to REM	N/A	
TH-3.3.b		Fails off	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; internal prop temperature	PDU to REM RIU to REM	N/A	
TH-3.3.c		Debonds from surface	1) Assembly/installation failure 2) adhesive failure/defect	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; internal prop temperature	PDU to REM RIU to REM	N/A	
Inputs		Switched Power		Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	4	Active	Yes	Tank temperature telemetry	Heater current; internal prop temperature	PDU to REM RIU to REM	N/A	
TH-3.4. S/C Panel Survival Heaters A&B (16 Ω switched) TH-3.4.a		Fails on	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect high temperature and switch off power to that heater and switch to othe side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; various temperatures?	PDU to REM RIU to REM	N/A	
TH-3.4.b		Fails off	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; various temperatures?	PDU to REM RIU to REM	N/A	
TH-3.4.c		Debonds from surface	1) Assembly/installation failure 2) adhesive failure/defect	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; various temperatures?	PDU to REM RIU to REM	N/A	
Inputs		Switched Power		Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	4	Active	Yes	Tank temperature telemetry	Heater current; various temperatures?	PDU to REM RIU to REM	N/A	
TH-3.5 CSPR Manifold 1&4 Heaters A&B (16 Ω switched) TH-3.5.a		Fails on	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect high temperature and switch off power to that heater and switch to othe side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
TH-3.5.b		Fails off	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
TH-3.5.c		Debonds from surface	1) Assembly/installation failure 2) adhesive failure/defect	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
Inputs		Switched Power		Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	4	Active	Yes	Tank temperature telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
TH-3.6. CSPR Manifold 2&3 Heaters A&B (14 Ω switched) TH-3.6.a		Fails on	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect high temperature and switch off power to that heater and switch to othe side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
TH-3.6.b		Fails off	1) Thermostat failure 2) Failure of switch 3) Failure in heater	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
TH-3.6.c		Debonds from surface	1) Assembly/installation failure 2) adhesive failure/defect	S/C will detect low temperature and switch to other side.	No effect.	No effect.	N/A	2R	Active	Yes	Temperature sensor telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
Inputs		Switched Power		Autonomy will detect low temperature and switch to other side.	No effect.	No effect.	N/A	4	Active	Yes	Tank temperature telemetry	Heater current; CSPR manifold temp	PDU to REM RIU to REM	N/A	
TH-3.7 Battery Heater A & Solar Array Drive Heater A (unswitched)				Dual thermostats at											
TH-3.7.a		Fails on		different set points will cause heater to turn off, switch to other side		No effect.	N/A	2R	None	Yes	Thermostats			N/A	
ТН-3.7.b		Fails off		Dual thermostats at different set points will cause heater to turn on, switch to other side	No effect.	No effect.	N/A	2R	None	Yes	Thermostats			N/A	
TH-3.7.c		Debonds from surface		2nd side thermostats would detect low temp and would turn on	No effect.	No effect.	N/A	2R	None	Yes	Thermostats			N/A	
Inputs		Unswitched power		Dual thermostats at different set points will cause heater to turn on, switch to other	No effect.	No effect.	N/A	4	None	Yes	Thermostats			N/A	
TH-3.8 Battery Heater B & Solar Array Drive Heater B (unswitched)				side											

FMEA ID	Name Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	Response Desired System Response	Allocation of System Response	Time to fix System	Time to Transmit Signal	Ground Response / Contingency	Quick Look Processor Switch	Safe Mode	Comments - KAF	Revisit
TH-3.3.a		Fails on	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time								No CB for switched heater; prop heaters were different than what Stewart expected	
TH-3.3.b		Fails off	Local	Switch heater power off, power on redundant Switch heater	Autonomy	N/A	TBD time									
TH-3.3.c		Debonds from surface	Local	power off, power on redundant Switch heater	Autonomy	N/A	TBD time				,		 g			
Inputs TH-3.4 S	/C Panel Survival Heaters A&B (16 Ω switched)	Switched Power	Local	power off, power on redundant	Autonomy	N/A	TBD time									
TH-3.4.a		Fails on	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time								No CB for switched heater; prop heaters were different than what Stewart expected	
TH-3.4.b		Fails off	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time									
TH-3.4.c		Debonds from surface	Local	Switch heater power off, power on redundant Switch heater	Autonomy	N/A	TBD time									
Inputs TH-3.5 C	SPR Manifold 1&4 Heaters A&B (16 Ω switched)	Switched Power	Local	power off, power on redundant	Autonomy	N/A	TBD time									
TH-3.5.a		Fails on	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time								No CB for switched heater; prop heaters were different than what Stewart expected	
TH-3.5.b		Fails off	Local	Switch heater power off, power on redundant Switch heater	Autonomy	N/A	TBD time									
TH-3.5.c		Debonds from surface	Local	power off, power on redundant Switch heater	Autonomy	N/A	TBD time									
Inputs TH-3.6 C	SPR Manifold 2&3 Heaters A&B (14 Ω switched)	Switched Power	Local	power off, power on redundant	Autonomy	N/A	TBD time	Single thermostat								
TH-3.6.a		Fails on	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time								No CB for switched heater; prop heaters were different than what Stewart expected	
TH-3.6.b		Fails off	Local	Switch heater power off, power on redundant Switch heater	Autonomy	N/A	TBD time									
TH-3.6.c		Debonds from surface	Local	power off, power on redundant Switch heater	Autonomy	N/A	TBD time									
Inputs TH-3.7 Bi	attery Heater A & Solar Array Drive Heater A (unswitched)	Switched Power	Local	power off, power on redundant	Autonomy	N/A	TBD time									
TH-3.7.a		Fails on				N/A	TBD time	dual thermostats							No FM since these are unswitched loads	
TH-3.7.b		Fails off				N/A	TBD time									
TH-3.7.c		Debonds from surface				N/A	TBD time									
Inputs		Unswitched power				N/A	TBD time									
TH-3.8 B	attery Heater B & Solar Array Drive Heater B (unswitched)															

							Ef	fect						Detection Method	d		
FMEA ID	Name	Function	Failure Mode / Limit /	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to	Time to
			Constraint													Detect (Local)	Detect (System)
TH-3.8.a			Fails on	1) Thermostat failure 2) Failure of switch 3) Failure in heater		Dual thermostats at different set points will cause heater to turn off, switch to other side		No effect.	N/A	2R	None	Yes	Thermostats			N/A	
TH-3.8.b			Fails off	1) Thermostat failure 2) Failure of switch 3) Failure in heater		Dual thermostats at different set points will cause heater to turn on, switch to other side		No effect.	N/A	2R	None	Yes	Thermostats			N/A	
TH-3.8.c			Debonds from surface	1) Assembly/installation failure 2) adhesive failure/defect		2nd side thermostats would detect low temp and would turn on	No effect.	No effect.	N/A	2R	None	Yes	Thermostats			N/A	
Inputs			Unswitched power			Dual thermostats at different set points will cause heater to turn on, switch to other side		No effect.	N/A	4	None	Yes	Thermostats			N/A	
TH-4 1	Femperature Sensors									<u> </u>					<u> </u>		
TH-4.a				1) mechanical break 2) RIO failure		Bad reading at sensor	redundant sensor	No effect.	N/A	4	?	Yes	Component temp			N/A	
TH-4.b			Incorrect output	1) debond		Bad reading at sensor	Determine whether or		N/A	4	?	yes	Component temp			N/A	

									Response						Quick Look			
FMEA ID	Name	Function	Failure Mode / Limit /	Response Level	Desired Local	Allocation of		Time to	Desired System	Allocation of System	Time to fix	Time to	Ground Response /	System Side	Processor Switch	Safe	Comments - KAF	Revisit
			Constraint		Response	Local Response	locally	Transmit	Response	Response	System	Transmit	Contingency	Switch		Mode		
			<u> </u>					Signal				Signal						<u> </u>
			ļ															
TH-3.8.a			F-II				A1 / A	TDD time	dual thermostats								No FM since these are unswitched loads	
1H-3.8.a			Fails on				N/A	TBD time	duai thermostats								NO FIXI SINCE these are unswitched loads	
			<u> </u>			1	ļ !	1	!			 !	1					! !
TH-3.8.b			Fails off				N/A	TBD time										
-																		
			ļ			ļ	ļ	. 	ļ	ļ		ļ	-					ļ
TH-3.8.c			Debonds from surface				N/A	TBD time										
						<u> </u>		<u> </u>										
							N/A	T00 .:										
Inputs			Unswitched power			1	N/A	TBD time		!								
-																		
TH-4 T	emperature Sensors					1	<u> </u>	1										<u> </u>
								Time required										
								to see	all components will								Not sure that all components do have	
TH-4.a			No output				N/A	tomporatura	have redundant temp sensors (current								redundant temp sensors? Would we want to do a side switch for critical components if the	
									baseline)								temp info was not available/stale?	
								component	baselille)								terrip into was not available; state:	
			· · · · · · · · · · · · · · · · · · ·			<u> </u>		Time required	d	ō			·					
								to see										
TH-4.b			Incorrect output				N/A	temperature										
							·	change in										
								component										
i				.i	i	i	i		ā	ā	t	ă						å

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Method TIm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
Severity 1s Avionics																	(System)
AV-4.1.2.2.a	PRIO		Hard failure (could take out one or both PRIOs - need both on a		L	If hard failure occurs prior to safety bus relay on, couldn't turn on safety bus.	Not able to power safety- inhibited loads.	LOM	N/A	1	Passive - Redundancy??	yes	Safety buses wouldn't turn on				
	Rxn Wheel 1		Higher friction in a wheel happens in combination with a side switch (for other reasons)			Wheel spins down due to side switch. Only a single wheel is affected by the friction, but all wheels are affected by the side switch.	Spacecraft turns (direction and speed depends on conditions a time of side switch).		Possible, depending on where in orbit, how fast, and which direction it's turning.	1		No					
Propulsion Inputs	Latch Valve A		Bus voltage	No voltage Constant "ON" from PDU high side and low side (instead of pulses)		1) Couldn't cycle valve 2) LV heats up	1) None assuming 2nd LV work 2) Propellant heats up	s 1) None 2) S/C explodes	N/a	1) 4 2) 1	1) Passive - redundancy? 2) None	Yes	Current draw, temperature readings	1) PDU LV current tlm? 2) PDU high and low side tlm		N/A	N/A
PR-8.01.3.a	Valve Assembly (NC Solenoid Valves)		Both failed open or both leak	1) electrical failure 2) FOD		Valves wouldn't close	Thruster would continue to fire unless latch valve closed	Depends on when in orbit it happens and how quickly it's caught (especially withir 0.7 AU). Probably mission- ending or at least would curtail it.		1 - if causes an umbra violation 2 - if fuel is significantly depleted or orbit significantly changed 3 - if mission is impacted by fuel loss or orbit change	Passive - redundancy	Maybe	Thruster continues to fire after commanded to stop	Thruster fire tlm; maneuver active tlm			N/A
Severity 2s Avionics																	
	SCIF A		Component/ Instrument telemetry			Lose telemetry from component or instrument	Depends on component/instrument lost - worst case would cause a side switch	None	Depends on side switch and reconfig time	2 - if FIELDS is lost 2R - if a critical component is lost 3 - if another instrument is lost 4 - for other (non-critical)	Active	Yes	Prime via SpW				
AV-4.1.2.a	Relay Cap A		Fails to provide function #1 (main bus voltage for critical and non- critical loads)	1) Incoming power wire breaks/bad connection 2) Short to ground (double- insulated wires)		1) Multiple pairs (6) of incoming power wires (power & return) per RC slice. The loss of a single wire/pair would be within margin for s/c. The loss of more than one (multiple failures) would cause there to be too little power available to the s/c. 2) An unconstrained short would melt the wires and discharge the battery.		1) No effect (assuming a single failure) 2) LOM	N/A	1) 4 2) 2	Active			State of charge			
AV-4.1.2.b	Relay Cap A		Fails to provide function #2 (load current telemetry)			PSE also supplies total current telemetry. Non-critical failure.	Worst case, switch off a single load.	Worst case would switch off one of the instruments, degrading (but not failing) science.		2 - If FIELDS is lost 2R - if a critical component is lost 3 - if another instrument is lost 4 - for other (non-critical) components	Active						
AV-4.1.2.1.b	Relay Cap A - Fuse Module		Blows too soon	1) Design 2) Transient voltage 3) "Smart" short (high current setting that is not detected)	E, M, C	Lose power to a load.	Switch to side B	No effect.	N/A	2 - If load is FIELDS 2A - If load is critical component 3 - If load is another instrument 4 - If load is non-critical component	Active	yes	current telemetry would be zero. Would be indistinguishable from an ARC switch failure. Would probably have ground recommand, but wouldn't fix problem.	Load current	PDU to REM		
AV-4.1.3.c	FET Slice 1		FET stuck off	FET failure		Load stuck powered off.	Switching sides of avionics would not fix problem (FET itself is common to both PDUs)	Loss of load.	N/A	2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical	Active	yes	Load continues to be powered off after power on command.	Load current	PDU to REM		
AV-4.1.3.d	FET Slice 1		Hard failure	Electronics failure Connector/cable failure Common electronics (redundant within FET slice)	E, M, C	Some or all slice functions fail	Possible loss of power to any o all loads powered through FET slice 1. With redundancy of components and effective placement of loads on FET cards, the loss of a single FET card should not fail the mission	Possibly degraded mission.	N/A	2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	Loss of power to load(s)	Load current	PDU to REM		
AV-4.1.3.1.a	FET Slice 1 - Circuit Breaker		Unable to reset	1) Part Failure	Е, М, С	Assuming load has tripped circuit breaker, loss of switched load If load has not tripped circuit breaker, then no effect	Potential loss of a single instrument suite. Cycling power to load may reset circuit breaker. Ground would probably investigate problem at next ground contact.	Degraded or LOM depending on which switched load.		2 - if load is PIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component 2 - if load is PIELDS	Active	yes	Load continues to be powered off after power on command.	Load current	PDU to REM		
AV-4.1.3.1.b	FET Slice 1 - Circuit Breaker		Opens without stimuli	1) Part Failure	E, M, C	1) Loss of switched load	1) MOPs sends commands to reset circuit breaker	Degraded science or loss of redundancy if breaker continually trips for critical switched loads		2 - if load is PIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	Load switches off unexpectedly	Load current	PDU to REM		
AV-4.1.3.1.c	FET Slice 1 - Circuit Breaker		Trips too soon	1) Trip Value Set Too Low	E, M, C	1) Load constantly trips circuit breaker	1) Ground command to disable or override the CB	1) None		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical	None	yes	Load switches off unexpectedly				
AV-4.1.3.1.d	FET Slice 1 - Circuit Breaker		Failure to trip (assumes load is drawing too high of a current)	1) Sense value incorrect (should be caught in testing)		Fuse would blow if current high enough.	Loss of load. Autonomy would turn off load permanently.	Degraded science or loss of redundancy, depending on load.		component 2 - If load is PIELDS 2R - If load is critical component 3 - If load is another instrument 4 - If load is non-critical component	Active	yes	Power drain higher than expected. Load switches off when fuse blows.	Load current	PDU to REM		

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	t Response Level	Desired Local Response	Allocation of Local	Time to fix locally		Desired System			Time to	Ground Response /		Quick Look Processor Switch	Safe Mode	Remediation	Helpful Autonomy	Revisit	Comments - KAF
Severity 1s						Response		Signal	Response	Response	system	Transmit Signal	Contingency	Switch				Rule		<u> </u>
Avionics AV-4.1.2.2.a	PRIO		Hard failure (could take out one or both PRIOs - need both on a side)																	
G&C GC-4.1.k	Rxn Wheel 1		Higher friction in a wheel happens in combination with a side switch (for other reasons)																	
Propulsion								!	! !				I							·
Inputs	Latch Valve A		Bus voltage	None	None	None	None	None	None	None	None	None	None							
PR-8.01.3.a	Valve Assembly (NC Solenoid Valves)		Both failed open or both leak	Local?	if thrusters firing when maneuver not active, close latch valves	Autonomy			None	None	None	None	None					Close latch valves		
Severity 2s Avionics										<u> </u>										
Inputs	SCIF A		Component/ Instrument telemetry	Local	Depends on component affected: 1)Prime requests ARC side switch 2)Switch to redundant component	1) HW - ARC 2) Autonomy	Side switchover							X			Power cycle during ground contact & perform REM check out		х	
AV-4.1.2.a	Relay Cap A		Fails to provide function #1 (main bus voltage for critical and non- critical loads)	System	LBSOC Safing	Autonomy											None			Relay Cap A & B on same card? So nothing we can do? Would look like unexpected battery discharge fault, but not fixable??
AV-4.1.2.b	Relay Cap A		Fails to provide function #2 (load current telemetry)	Local	For some loads, may want to re-enforce that one is always on?	Autonomy													х	
	Relay Cap A - Fuse Module		Blows too soon	Local	Consider having an over- current rule for each witched load with out a CB in order to protect the fuse? In some cases this might be a complete system side switch or just component switch for those loads that are cross strapped	Autonomy											Critical loads are redundant, so a single fuse blowing would not cause a critical load to fail		х	
AV-4.1.3.c	FET Slice 1		FET stuck off	Local	TBD which loads, but monitor for one of two always on?	Autonomy													х	
AV-4.1.3.d	FET Slice 1		Hard failure	Local	TBD which loads, but monitor for one of two always on?	Autonomy											1) MOPs tries to command load(s) on/off 2) Cycle power		х	
	FET Slice 1 - Circuit Breaker		Unable to reset	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy											1) Send commands to turn load on 2) Send commands to turn load on and override CB 3) Cycle power		х	
	FET Slice 1 - Circuit Breaker		Opens without stimuli	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy											1) If CB continually trips, can override CB and rely solely on autonomy rule for over-current protection		х	
	FET Slice 1 - Circuit Breaker		Trips too soon														1) Turn load on 2) If CB continually trips, can override CB and rely solely on autonomy rule		х	
	FET Slice 1 - Circuit Breaker		Failure to trip (assumes load is drawing too high of a current)	Local	Consider having an over- current rule for each switched load with CB in order to protect the fuse?	Autonomy											1) Autonomy rules also protect against over-current 2) LVS protection if both CB and autonomy rule fail		х	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Method Tlm for Diagnosis	Tim Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
Inputs	FET Slice 1 - Circuit Breaker		Power from Fuse Module			Loss of load	Potential loss of entire instrument suite.	Degraded science or loss of redundancy, depending on load.		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	Load not powered.	Load current	PDU to REM		
AV-4.1.3.2.a	FET Slice 1 - Fuse Module		Blows below rated current	1) Design 2) Transient voltage 3) "Smart" short (high current setting that is not detected - multiple failures)	Е, М, С	Loss of load	Potential loss of entire instrument suite.	Degraded science or loss of redundancy, depending on load.		2 - if load is FIEEDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	Load not powered.	Load current	PDU to REM		
AV-4.1.3.2.0	FET Slice 1 - Fuse Module		Failure to blow (assumes a failure in the load, causing it to draw a high current)	1) Design		Loss of load	Anything other than a short to chassis, autonomy would see and turn off load. Also will have circuit breakers for non-redundant loads like instruments and some other critical loads.	Degraded science or loss of redundancy, depending on load.		2 - if load is FIELDS 2R - if load is critical component 3 - if load is another instrument 4 - if load is non-critical component	Active	yes	Not short to chassis: excess current draw by load. Short to chassis: difficult to diagnose. Eventually would load shed and side switch. Would probably see problem when switching loads back on one-by- one.	Load current	PDU to REM		
EPS Inputs	Bus Junction Slice		Relay command (only changes when a fault occurs and it needs to change state)	No command when necessary (2nd failure)		No effect to card.	Buck converter would draw too much power. Battery would discharge.	Loss of mission		2	None	Yes.	With current sensors on buck converter slice	Buck Converter Current	PSE to CDH	?	None
Inputs G&C	Solar Array Junction Card 1		Solar array power			Slice is ok.	S/c not receiving power.	Loss of mission.	N/a	2	None	Yes	Current might not be correct, but long-term, battery voltage decreases	Battery voltage	PSE to CDH	?	?
GC-2.1.a	Solar Limb Sensor A		Input message not received or processed. (The solar limb sensors may need some information from the avionics/FSW to set gains or parameters that are used in computing Sun offset angle from cell intensity readings. A fault on the s/c side or inside the solar limb sensor that causes this information to not be available will cause problems for the solar limb sensor in that the angle solutions coming out will be degraded. (cases where angle solutions coming out will be included in another section below))			Sun geometry when first detected is unchanged so time of detection is unaffected; solar limb sensor uses old or incorrect information to generate Sun offset angle; angle accuracy is degraded and time when first angle is output may be delayed	based on SLS data.	parameter values before we have another attitude anomaly where SLS would	taken soon enougn.	2	1) None 2) Active 3) Active	Probably not	Don't think there is a way to detect this. If we are using the wrong parameters in the SLS signal processing, we won't have any way to conclude that we are getting wrong answers. (This assumes that target attitude is +2/TPS to Sun.)	1) None 2) SLS heartbeat? 3) SLS heartbeat?	1) None 2) SLS to CDH to Autonomy 3) SLS to CDH to Autonomy	1) None 2) ? 3) ?	None
GC-4.1.b	Rxn Wheel 1		Case 1: Incorrect force/torque exerted on spacecraft	Frozen torque command - direction and magnitude stay at some fixed value; include both max and below max magnitude values.		with how long that takes depending on the speed magnitude when command firs	impact depends on what level the command was when frozen - if large we get in trouble faster. The momentum will be higher, but may or may not be at the dump limit when the wheel reaches max speed. The other wheels will try to fight the one wheel but will likely saturate and once 2 of them are saturated, we lose controllability, if the system can do a momentum dump before 2 of the wheels reach saturation, we may survive longer but dumps will be done more frequently (if allowed) since the failed wheel has reached its mom storage limit.	Loss of mission in the worst case - even if solar limb sensors detect the umbra violation it may not be	Possible if failed wheel is still considered available, but depends on momentum state of system when wheel failure occurs and timing of momentum dump logic and wheel fault logic (to turn off misbehaving wheel)	2		Yes	compare wheel speed/torque to commanded wheel speed/torque (most wheels have feedback telemetry with actual torque and all have some means of measuring wheel speed). G&C software will be monitoring wheel speeds and other health status telemetry (if any) from the wheels and will request action from autonomy if needed.			TBD - probably will wait for a few control cycles to declare a wheel unresponsive	
GC-4.1.c	Rxn Wheel 1		Case 2: Incorrect force/torque exerted on spacecraft	Direction stuck at + or -, magnitude correct responding only to magnitude part of command.		The "stuck" wheel will eventually reach saturation (max speed) with how long that takes depending on the speed magnitude when direction first got stuck.	The controller will mistakenly keep sending commands to all the wheels. The one that's only responding to torque magnitude will eventually saturate at max speed. The momentum will be higher, but may or may not be at the dump limit when the wheel reaches max speed. The other wheels will try to fight the one wheel but will likely saturate and once 2 of them are saturated, we lose controllability. If the system can do a momentum dump before 2 of the wheels reach saturation, we may survive longer but dumps will be done more frequently (if allowed) since the failed wheel has reached its mom storage limit.	Loss of mission in the worst case - even if solar limb sensors detect the umbra	Possible if too many wheels reach saturation before a momentum dump can be	2							

FMEA ID	Name	Function	Failure Mode / Limit / Constrain	t Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Response Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
Inputs	FET Slice 1 - Circuit Breaker		Power from Fuse Module	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy													х	
AV-4.1.3.2.a	FET Slice 1 - Fuse Module		Blows below rated current	Local	TBD which loads, but monitor for one of two always on? Would not help with instruments	Autonomy											1) Circuit breakers are used to prevent fuses from blowing 2) Critical loads have redundant power paths, so a single fuse blowing would not cause a critical load to fail		х	
AV-4.1.3.2.b	FET Slice 1 - Fuse Module		Failure to blow (assumes a failure in the load, causing it to draw a high current)		Consider having an over- current rule for each switched load with CB in order to protect the fuse?	Autonomy											1) Circuit breakers are used to prevent fuses from blowing 2) Critical loads have redundant power paths, so a single fuse blowing would not cause a critical load to fail		х	
EPS Inputs	Bus Junction Slice		Relay command (only changes when a fault occurs and it needs to change state)	None	None	Ground	?	?	?	None	None	None	None	None - loss of mission, but double fault						
Inputs G&C	Solar Array Junction Card 1		Solar array power	None	None	None	None	None	None	None	None	None	None	None				Solar arrays would extend to increase voltage		
GC-2.1.a	Solar Limb Sensor A		input message not received or processed. (The solar limb sensors may need some information from the avionics/FSW to set gains or parameters that are used in computing Sun offset angle from cell intensity readings. A fault on the s/c side or inside the solar limb sensor that causes this information to not be available will cause problems for the solar limb sensor in that the angle solutions coming out will be degraded. (cases where angle solutions are grossly incorrect are included in another section below!)	1) None 2) Local 3) Local	1) None 2) Power cycle SLS 3) Power cycle SLS	1) None 2) Autonomy 3) Autonomy	None	1) None 2) ? 3) ?	None	None	None	None	None				Redundant heads may not help because the parameter are probably the same for both sides of the head. Redundant electronics might help if the other side of the electronics doesn't have the internal problem that causes it to miss getting updated parameters. But then we have to figure out how to pick the "right" data from the two readings from each side. Might be able to do in-flight calibration at larger solar distances, but unlikely since will be at the saturation limit for low intensity most of the time where we could attempt calibration. Trying to calibrate at small solar distances would require intentionally going far enough off sun for the SLS head to see the Sun and generate angle data - assuming that the star tracker and ephemeris models would hold us at an attitude that was still outside the s/c packaging umbra and using the attitude and ephemeris info to get the "true" offset angle to compare against the SLS offset angle.			
GC-4.1.b	Rxn Wheel 1		Case 1: Incorrect force/torque exerted on spacecraft														For this case, we are assuming that the failed wheel is still actively rotating and not in the way the controller commanded it to. The best first action may depend on how the wheel is not responding. If we see that a whee is ramping up to max speed, it might be better just to turn it off than to try switching sides. Some wheels have a built-in feature to turn off when a max speed is reached (which is over the max possible command). As des switch might fix a problem with direction or magnitude part of the torque command being frozen. I don't think the wheel itself will have internally redundant command interfaces that could be switch, power off the wheel and set it unavailable to the control system. In theory we can take one wheel out of the loop and still control with 3 wheels only. May need a momentum dump sooner when down to 3 wheels. If 2 or more wheels fail, we switch to thrusters for attitude control. If we are able to reliably detect that the wheel persists in not responding to toqrue commands, we should shut it down. We may take other actions first to be sure it's really not able to respond normally.			
GC-4.1.c	Rxn Wheel 1		Case 2: Incorrect force/torque exerted on spacecraft																	

							Effect							Detection Method			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect
GC-4.1.d	Rxn Wheel 1		Case 3: incorrect force/torque exerted on spacecraft	Direction reversed, magnitude correct - error in wheel interface electronics; most wheels have separate inputs for the direction and magnitude of the commanded torque that are probably processed separately in the wheel electronics.		wheel will spin in opposite direction from commanded direction and exert a torque that fights against the desired control. Won't necessarily reach saturation (max speed) since direction sign can still change with time.	will try to counter the effect of the wheel that's outputting its torque in the wrong direction. They will probably succeed if they aren't close to saturation	sensors detect the umbra violation it may not be correctable in the time available depending on how we design the auto dump logic and fault checks for	Probably not in this case. w	2							(System)
GC-4.1.e	Rxn Wheel 1		Case 4: Incorrect force/torque exerted on spacecraft	Magnitude stuck, direction correct; responding only to direction part of command, but non-zero magnitude; include both max and below max magnitude values.		commanded direction but torque magnitude will be larger or smaller than commanded. Won't necessarily reach saturation (max speed) since direction sign can still change with time. It's essentially adding in some disturbance torque that can work with the system or	momentum aump isn t	sensors detect the umbra violation it may not be correctable in the time available depending on how we design the auto dump logic and fault checks for	Possible, but less likely if torque magnitude is lower.	2							
GC-4.1.f	Rxn Wheel 1		Case 5: Incorrect force/torque exerted on spacecraft	Wheel responding significantly out-of-spec - magnitude and direction of torque command are correct, but torque output to spacecraft deviates from it a) Localized increase in friction in parts of flywheel rotation; general increase in friction causing wheel to be sluggish bot not enough to completely stop it from moving. b) Imbalance causing very irrecular rotation of flywheel. c) Electric motor failure - intermittent glitch in motor configuration causes very erratic resopnse to the wheel torque commands.		consume more power as the motor works to overcome bigger loss effects. b) If wheel is "energetic", it puts out more torque than commanded. (unlikely - usually it's the losses that are bigger than expected). c) If wheel is erratic, it essentially acts as a frandom disturbance torque on the	from target attitude than desired as remaining wheels work to pick up the slack from the one sluggish wheel. b) Turns may complete faster. c) Hard to predict without	case - even if solar limb sensors detect the umbra violation it may not be correctable in the time available depending on how we design the auto dump	a) Possible if failed wheel is still considered available, but depends on momentum state of system when wheel failure occurs and timing of momentum dump logic and wheel failt logic (to turn off misbehaving wheel) b) Possible if failed wheel is still with state of system when wheel failure occurs and timing of system when wheel failure occurs and timing of momentum dump logic and wheel fault logic (to turn off misbehaving wheel)	2							
Cooling	<u>}</u>		Y	1	······	·	ļ	·,········	·,····································				·	·,·····	······································	.i	
TCS-ACCU-1		Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed N2 gas charge that is applied between the bellows and the tank shell. Holds TBD in 3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	Cross-bellows Internal Leakage	1) Over stress (ext induced); 2) Contaminants induced; 3) Corrosion; 4) Fatigue; 5) Material/process (weld) flaw.	All	The bellows will extend to its neutral no- load position; Interchanging and mixing of fluids between N2 and coolant cavities due to temperature excursions.	(items PM1/PM2); Decrease or	cause would lead to loss TCS and mission.	N/A	2			Pump delta-p sensor and/or current and temp sensors detect cavitation; loop temp sensors detect degraded cooling				
TCS-ACCU-2	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed N2 gas charge that is applied between the bellows and the tank shell. Holdst BD in Bin in. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Coolant Leakage	Over stress (ext induced); Corrosion; Fatigue; Material/process (weld) flaw.	All	Coolant leaks to external from the accumulator.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and mission.	N/A	2			Tank pressure and temperature sensors detect loss of coolant; Pump delta-p sensor and/or current and temp sensors detect cavitation; 19 2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				
TCS-ACCU-3	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed N2 gas charge that is applied between the bellows and the tank shell. Holds TBD in Min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Gas Leakage	1) Over stress (ext induced); 2) Corrosion; 3) Fatigue; 4) Material/process (weld) flaw.		Gas leaks to external from the accumulator, resulting in loss of pressure.	Unable to maintain a net positive pump input pressure resulting in pump cavitation. Inability to provide thermal for expansion could result in bellows rupture.	Redundant pump failures due to cavitation common cause or loss of coolant due to rupture would lead to loss TCS and mission.		2			Tank pressure sensor detects loss of pressurization; Pump delta-p sensor and/or current and temp sensors detect cavitation; 19 2 detects loss of main loop pressurization; 41 Loop temp sensors detect loss of cooling				
TCS-ACCU-4	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. Holds TBD in3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	Fails to Expand/Contract	Jammed bellows (interference of moving parts); Contamination.	All	Inability to expand during high temp operation could cause bellows over pressure and potential rupture. Inability to contract during low temp operation could cause pump cavitation.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause or loss of coolant due to rupture would lead to loss TCS and mission.		2			Tank pressure and temperature sensors may detect pressure fluctuations due to temperature excursions; Temp delta-p sensor and/or current and temp sensors detect cavitation; Loop temp sensors detect loss of cooling				
TCS-LV1-1	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Fails open	1) Contamination; 2) Seal failure; 3) FSW Failure; 4) Electrical/ Electronics failure; 5) Autonomy failure; 6) Failed sequence	All	Coolant would be allowed into the main loop before it is desired.	Coolant would freeze, potentially leading to rupture.	Rupture due to freezing results in loss of TCS and mission.	N/A	2			1) Tank pressure and temperature sensors may detect loss of coolant into the main loop; 2) Pump delta-p sensor and systen pressure and temp sensors will all detect rupture resulting in loss of TCs.	n			
TCS-LV1-2	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	internal leakage (large leak)	1) Contamination; 2) Seal failure	All	Coolant would be allowed into the main loop before it is desired.	Sufficient coolant leaks into system to cause a blockage when it freezes, potentially leading to rupture.	Rupture due to freezing results in loss of TCS and mission.	N/A	2			Tank pressure and temperature sensors may detect loss of coolant into the main loop; Pump delta-p sensor and systen pressure and temp sensors will all detect rupture resulting in loss of TCs.	n			
TCS-LV1-4	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Valve stays closed when commanded to open	1) Contamination; 2) Jamming; 3) Binding; 4) Seal failure; 5) FSW Failure; 6) Electrical/ Electronics failure; 7) Autonomy failure; 8) Failed sequence		Valve stays closed.	Re-send command to open valve, but if failure persists, no coolant is available to the TCS.	Loss of TCS. Loss of mission.	N/A	2			Pump delta-p sensor detects loss of flow; Loop temp sensors detect loss of cooling				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	t Response Level Desired Local Response	Allocation of Local Response	Time to fix locally	Response Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Quick Look Processor Switch Safe Mode	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
GC-4.1.d	Rxn Wheel 1		Case 3: Incorrect force/torque exerted on spacecraft												Will do polarity tests pre-launch that should detect mis wiring or miscommunication between control software and wheels, but I guess it's possible that something can break or be affected by environment to introduce errors in the command chain. These are really errors in how we wire up the command interface to the wheels. The vendors would not give us a wheel that responded in the reverse direction to the interface in their ICDs and other documentation. I suppose something in the electronics could spontaneously flip that might cause this, but a miswiring on our side is more likely.			
GC-4.1.e	Rxn Wheel 1		Case 4: Incorrect force/torque exerted on spacecraft															
GC-4.1.f	Rxn Wheel 1		Case 5: Incorrect force/torque exerted on spacecraft															
Cooling	<u> </u>	·	λ Υ				λγ	۸ پرستان	.3	 ү	i		λ γ	i	·	λ	i	
TCS-ACCU-1	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. Holds TBD in3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	Cross-bellows Internal Leakage	Seconds/minutes				N/A	None						Historically this has been an accepted risk in similar spaceflight applications, based on it's a highly reliable all welded pressure barrier metal bellow assembly design, rigourous design stress analyses, manufacturing process controls, mandatory hardware inspection points, and qual/accept tests.			
TCS-ACCU-2	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. HoldS TB0 in3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Coolant Leakage	Seconds/minutes				N/A	None									
TCS-ACCU-3	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. HoldS TBD in3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	External Gas Leakage	Seconds/minutes				N/A	None									
TCS-ACCU-4	Accumulator	Stores coolant water prior to system charge; Provides thermal expansion and loop leakage compensation. Coolant is internal to the accumulator tank bellows and the fluid is expelled using a fixed NZ gas charge that is applied between the bellows and the tank shell. Holds TBD in 3 min. of coolant; TBD psig MDP; Bellows neutral position is TBD.	Fails to Expand/Contract	Seconds/minutes				N/A	None									
TCS-LV1-1	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Fails open	Minutes				N/A	None									
TCS-LV1-2	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	internal leakage (large leak)	Minutes				N/A	None									
TCS-LV1-4	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Valve stays closed when commanded to open	Minutes				N/A	None						Redundant, independent opening electronics. This would require two failures.			

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation		Type of FM	Observable	How Observed?	Detection Method Tlm for Diagnosis	Tlm Path for	Time to Detect	Time to
								Donatora dona An bish	,	Severity					Diagnosis	(Local)	Detect (System)
TCS-LV1-5	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	Valve closes when not commanded to close	Mechanical failure (cannot be commanded to close after ground testing is completed)	All	Valve closes.	The system loses access to the accumulator, resulting in potential rupture or pump cavitation as a result of high/low temperature excursions, respectively.	Rupture due to high temperatures leads to loss of coolant, loss of TCS, and loss of mission. Pump cavitation due to low temperatures leads to pump failures, loss of TCS, and loss of mission.	N/A	2			Tank pressure and temperature sensors detect loss of coolant due to rupture; Pump delta-p sensor detects loss of flow; Loop temp sensors detect loss of cooling				
TCS-LV1-6	Accumulator isolation valve	Valve is launched closed and isolates the coolant in the accumulator from the rest of the system. Opens following launch to allow coolant into radiators 1 and 4 and solar arrays.	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	All	Coolant leaks to space.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant; 2) Pump deltap- sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop pressure; 4) Loop temp sensors detect loss of cooling				
TCS-LV2-1	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails open	1) Contamination; 2) Seal failure; 3) FSW Failure; 4) Electrical/ Electronics failure; 5) Autonomy failure; 6) Failed sequence	(radiators 1 & 4)	Coolant would be allowed into the loop containing Radiators 2&3 before it is desired.	Potential coolant freezing, potentially leading to rupture and subsequent leakage.	Rupture due to freezing results in loss of TCS and vehicle	N/A	2			Pump delta-p sensor and system pressure and temp sensors will all detect rupture resulting in loss of TCs.				
TCS-LV2-2	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Internal leakage (large leak)	1) Contamination; 2) Seal failure	From initial cooling system activation (radiators 1 & 4) through final cooling system activation (radiators 2 & 3)	Coolant would be allowed into the loop containing Radiators 2&3 before it is desired.	Sufficient coolant leaks into system to cause a blockage when it freezes, potentially leading to rupture.	Rupture due to freezing results in loss of TCS and mission.	N/A	2			Tank pressure and temperature sensors may detect loss of coolant into the main loop; Pump delta-p sensor and system pressure and temp sensors will all detect rupture resulting in loss of TCs.				
TCS-LV2-4	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.		1) Contamination; 2) Jamming; 3 Binding; 4) Seal failure; 5) FSW Failure; 6) Electrical/ Electronics failure; 7) Autonomy failure; 8) Failed sequence	From final cooling system activation	Valve stays closed.	Re-send command to open valve, but if failure persists, no coolant is available to radiator 2 & 3.		N/A	2			Pump delta-p sensor detects loss of flow; Loop temp sensors detect loss of cooling Spooling Indicates closed state				
TCS-LV2-5	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.		Mechanical failure (cannot be commanded to close after ground testing is completed)	From final cooling system activation (radiators 2 & 3) on.	Valve closes.	The system loses access to Radiators 2 & 3.	Loss of TCS. Loss of mission.	N/A	2			Pump delta-p sensor detects loss of flow; Dos temp sensors detect loss of cooling Position indicator on LV indicates closed state				
TCS-LV2-6	Upstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	From initial cooling system activation (radiators 1 & 4) on.	Coolant leaks to space.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	Ν/A	2			Tank pressure and temperature sensors detect loss of coolant; Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop pressure; 4) Loop temp sensors detect loss of cooling				
TCS-LV3-1	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails open/Internal leakage	1) Contamination; 2) Seal failure; 3) Software Failure; 4) Electrical/ Electronics failure		Coolant may be allowed into the radiator 2/3 segment of the cooling loop before it is desired.		Rupture due to freezing results in loss of TCS and vehicle	N/A	2			P3 detects pressure rise as coolant leaks in				
TCS-LV3-2	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	Fails closed	1) Contamination; 2) Jamming; 3 Binding; 4) Seal failure; 5) Software Failure; 6) Electrical/ Electronics failure	All	Valve doesn't open when commanded, or valve closes inadvertently.	Loss of flow to radiators 2 and 3.	inability to supply coolant to radiators 2 and 3 results in inability to handle nominal heat loads, which eventually leads to loss of vehicle when the TCS can no longer keep up.	N/A	2			Loop temp sensors detect failure to supply flow to radiators 2 and 3.				
TCS-LV3-3	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.	External leakage, upstream side	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	All	Coolant leaks to external from the downstream side of the valve beginning when LV2 and LV3 are opened.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant after LV2 has been opened; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				
TCS-LV3-4	Downstream radiator isolation valve	Valve is launched closed and isolates radiators 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into radiators 2 and 3.		1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	АШ	Coolant leaks to external from the downstream side of the valve beginning when LV1 is opened post launch.	Potential pump cavitation and eventual loss of coolling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant after LV1 has been opened; 2) Pump delta-p sensor and/or current and temp sensors detect cavilation; 3) P2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				
TCS-CV1-1	Pump check valve	Check valve prevents back flow through the inactive pump leg	Internal Leakage	1) Ball/seat deformation; 2) Contamination	All	Some coolant recirculation flow is allowed through the check valve.	Degraded flow performance through the solar arrays and radiators.	If the leakage is severe enough, then inability to handle nominal heat loads is possible, leading to loss of vehicle when the TCS car no longer keep up.	N/A	2			1) Pump delta-p sensor detects flow degradation; 2) Loop temperature sensors detect degraded cooling performance				
TCS-CV1-4	Pump check valve	Check valve prevents back flow through the inactive pump leg	External Leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	All	Coolant leaks to external beginning when LVI is opened post launch.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant after LV1 has been opened; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				

The content of the co	FAMEA ID	. N	i s	ir-il Mada / Limit / Country int	Daniel I was	Desired Level Description	Allersking of Level	Time to find a seller	Response		Allowation of Contam	Time to five Time to	Converd Donoscon /	Contant Cida	Quick Look	C-f- Ba-d-	David disting	lusted a second	n	Community WAF
Series of the se	FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response		Time to fix locally		Desired System Response		system Transmit			Processor Switch	Safe Mode	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
Service of the servic	TCS-LV1-5		coolant in the accumulator from the rest of the system. Opens following launch to allow	commanded to close	Minutes					N/A	None									
Secure Se	TCS-LV1-6	Accumulator isolation valve	coolant in the accumulator from the rest of the system. Opens following launch to allow	•	Seconds/minutes					N/A	None									
Section Sect	TCS-LV2-1	isolation valve	2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into	:	Minutes					N/A	None						Can adjust vehicle orientation to prevent freezing			
Secretary Secretary and Control Contro	TCS-LV2-2		2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into	internal leakage (large leak)	Minutes					N/A	None						Can adjust vehicle orientation to prevent freezing			
Fig. 10-2 Sections and the control of the control o	TCS-LV2-4	isolation valve	2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into		Minutes															
State of the second process of the second pr	TCS-LV2-5		2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into		Minutes															
TCS-LV3-1 For the formatter and the formatter and the mission is allow content in a fine open/internal lockage from the formatter and the mission is allow content in a fine open free in and the formatter and th	TCS-LV2-6	isolation valve	2 and 3 on the upstream side. Opens about 1 month into the mission to allow coolant into	:	Seconds/minutes															
TCS-LV3-2 and 3 on the downstream Substruction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 2 and 3. The contraction 3 and 3 and 3 and 3 and 3 and 3 and 3 and 3 and 3 and 3 and 3 and 3 and 3	TCS-LV3-1	radiator isolation	2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into		Minutes					N/A	None						Can adjust vehicle orientation to prevent freezing			
TCS-1V3-3 realistor solution in the mission to allow coolant into realistors 2 and 3. TCS-1V3-4 Powerstream radiator solution when the mission to allow coolant into radiators 2 and 3. TCS-1V3-4 Powerstream radiator solution radiators 2 and 3. TCS-1V3-4 Powerstream radiator solution radiators 2 and 3. TCS-1V3-4 Powerstream radiator solution radiators 2 and 3. TCS-1V3-4 Powerstream radiator solution radiators 2 and 3. TCS-1V3-4 Powerstream radiator solution radiators 2 and 3. TCS-1V3-4 Powerstream radiator solution radiators 2 and 3. TCS-1V3-4 Powerstream radiators 2 and 3. TCS-1V3-4 Powerstream radiators solution radiators 2 and 3.	TCS-LV3-2	radiator isolation	2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into		Minutes					N/A	None									
TCS-LV3-4 radiators isolation valve 2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into iside 5 conds/minutes 5 conds/minutes 5 conds/minutes 5 conds/minutes 6 conds/minutes 6 conds/minutes 6 conds/minutes 6 conds/minutes 6 conds/minutes 6 conds/minutes 7 conds/m	TCS-LV3-3	radiator isolation	2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into	External leakage, upstream side	Seconds/minutes					N/A	None									
TCS-CV1-1 Pump check value Check valve prevents back flow through the internal Leakage Minutes N/A None	TCS-LV3-4	radiator isolation	2 and 3 on the downstream side. Opens about 1 month into the mission to allow coolant into	External leakage, downstream	Seconds/minutes					N/A	None									
	TCS-CV1-1	Pump check valve	Check valve prevents back flow through the inactive pump leg	Internal Leakage	Minutes					N/A	None									
TCS-CV1-4 Pump check valve Prevents back flow through the inactive pump leg Check valve prevents back flow through the inactive pump leg N/A None	TCS-CV1-4	Pump check valve	Check valve prevents back flow through the inactive pump leg	External Leakage	Seconds/minutes					N/A	None									

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Method Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
TCS-PM1-4	Pump 1	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	1) Pump cavitations; 2) Flow blockage; 3) High heat load/environment; 4) High coolant temp; 5) Bearing degradation	All	Potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment	Potential loss of TCS and vehicle	??	2			Loop temp sensors may provide an indirect indication that the pump is overheating				
TCS-PM1-5	Pump 1	Provides coolant flow through the solar arrays and radiators	Overcurrent	1) Electronics failure; 2) Bearing drag	All	Local heating, potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment	Potential loss of TCS and vehicle	??	2			Pump current sensor and vehicle level overcurrent protection features (TBD) will catch many overcurrent scenarios in time to allow for pump shutdown				
TCS-PM1-8	Pump 1	Provides coolant flow through the solar arrays and radiators	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure		Coolant leaks to external from the pump beginning when LV1 is opened post launch.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant after LV1 has been opened; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				
TCS-PM2-4	Pump 2	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	1) Pump cavitations; 2) Flow blockage; 3) High heat load/environment; 4) High coolant temp; 5) Bearing degradation	All	Potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment	Potential loss of TCS and vehicle	??	2			Loop temp sensors may provide an indirect indication that the pump is overheating				
TCS-PM2-5	Pump 2	Provides coolant flow through the solar arrays and radiators	Overcurrent	1) Electronics failure; 2) Bearing drag	All	Local heating, potential for a fire	If a fire occurs, potential damage to pump and surrounding equipment	Potential loss of TCS and vehicle	??	2			Pump current sensor and vehicle level overcurrent protection features (TBD) will catch many overcurrent scenarios in time to allow for pump shutdown				
TCS-PM2-8	Pump 2	Provides coolant flow through the solar arrays and radiators	External leakage	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or iveld flaw; 5) Seal failure	All	Coolant leaks to external from the pump beginning when LV1 is opened post launch.	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant after LV1 has been opened; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop pressure. 4) Loop temp sensors detect loss of cooling				
TCS-MV-3	Manual fill valve	Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant leakage to exterior.	External leakage, tank side	1) Over-stress; 2) Corrosion; 3) Fatigue; 4) Material/process or weld flaw; 5) Seal failure	All	Coolant leaks to external from the manual valve	Potential pump cavitation and eventual loss of cooling capability.	Redundant pump failures due to cavitation common cause and loss of coolant would lead to loss TCS and vehicle.	N/A	2			Tank pressure and temperature sensors detect loss of coolant; Pump delta-p sensor and/or current and temp sensors detect cavitation; P2 detects loss of main loop pressure. Uoop temp sensors detect loss of cooling				
TM-4.1.a	Ka-Band HYB-2		No output / incorrect output	1) Mechanical failure in device 2) Failure at waveguide flange		No output to expected device from Hybrid.	No RF or degraded RF signal. Ground would notice lack or degradation of signal and command RF to switch sides and/or switch Ka-band TWTAs, but degraded signal would remain even after switch.	Eventually overwhelm SSRs due to only having fanbeam downlink.		2	None		Ground detects data errors, incorrect power, or loses downlink. Autonomy would not react.	None - degraded performance	None	None	None
TM-9.1.a	HGA Antenna		Mechanical failure	1) Material defect 2) Dust strike		Antenna fails to send/receive communications.	S/C unable to return data in a timely fashion. Ground would attempt to switch antenna polarization, but would not correct problem.	Mission success severely impacted by data rate loss.	N/A	2 - if data return is too low 3 - if science requirements can still be met	None	Yes. (After proces: of elimination)	No more comm to/from HGA.	None Loss of comm with HGA	None	None	None
TM-9.1.b	HGA Antenna		Degraded performance			Poor perfomance (either less power or corrupted signal)	Run at lower data rates. Ground would switch antenna polarization.	Mission success severely impacted by data rate loss.	N/A	2 - if data return is too low 3 - if science requirements can still be met	None		Ground would see lower power or corrupted signal	None Loss of comm with HGA	None	None	None
ME-1.1.1.1.a	Solar Array Flap Actuator		Fails to actuate when commanded	1) bad/bound bearing/mechanical failure 2) stepper motor failure 3) loose/separated connector	E, C	Solar array stuck in position	if SA needs to move out, generates insufficient power 2) if SA needs to move in, generates too much power, potential overheating of wing (cells burned)		If in encounter, and SAs stuck out too far	2	Active	Yes	Potentiometer telemetry. Turn on redundant ECU for 3rd vote.	Potentiometer telemetry; redundant ECU telemetry Battery state of charge	ECU to REM	?	?
ME-1.1.1.1.b	Solar Array Flap Actuator		Incorrect actuation when commanded	incorrect potentiometer reading residual torque (should have sufficient margin) Motor coil or winding is open	E, C	Solar array in incorrect position	1) if SA needs to move out, generates insufficient power (different than required). 2) if SA needs to move in, generates too much power (different than expected), potential overheating of wing (cells burned)	eventually drain battery, may be able to slew s/c to retain partial power for a time lose mission	If in encounter, and SAs stuck out too far	2	Active	Yes	Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	?	?
ME-1.1.1.1.c	Solar Array Flap Actuator		Actuates when not commanded	Holding torque exceeded (need to have sufficient margin)	E, C	Solar array in incorrect position	I) if SA needs to move out, generates insufficient power (different than required) 2) if SA needs to move in, generates too much power (different than expected), potential overheating of wing (cells burned)	1) eventually drain battery, may be able to slew s/c to retain partial power for a time 2) lose mission	If in encounter, and SAs stuck out too far	2	Active	Yes	Power level	Potentiometer telemetry; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	?	?

FMEA ID	Name	Function Failure Mode / Limit / Const	aint Response Leve	l Desired Local Response	Allocation of Local Response	Time to fix locally	Response Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Quick Look Processor Switch Safe Mode	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
TCS-PM1-4	Pump 1	Provides coolant flow through the solar arrays and radiators	Minutes					N/A	None							х		
TCS-PM1-5	Pump 1	Provides coolant flow through the solar arrays and radiators	Seconds					N/A	None							х		
TCS-PM1-8	Pump 1	Provides coolant flow through the solar arrays and radiators	Seconds/minutes					N/A	None									
TCS-PM2-4	Pump 2	Provides coolant flow through the solar arrays and radiators	Minutes			į		N/A	None							х		
TCS-PM2-5	Pump 2	Provides coolant flow through the solar arrays and radiators	Seconds					N/A	None							х		
TCS-PM2-8	Pump 2	Provides coolant flow through the solar arrays and radiators	Seconds/minutes					N/A	None									
TCS-MV-3	Manual fill valve	Open for tank charging. Closed for the rest of the mission to provide a barrier against coolant External leakage, tank side leakage to exterior.	Seconds/minutes					N/A	None									
Telecomm TM-4.1.a	Ka-Band HYB-2	No output / incorrect output	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch						
TM-9.1.a	HGA Antenna	Mechanical failure	Local / Ground	Contingency Procedure	Ground	?	?	None	None	None	None	Need to talk through all the combinations within RF system that ground should try when attempting to reacquire						
TM-9.1.b	HGA Antenna	Degraded performance	Local / Ground	Contingency Procedure	Ground	?	?	None	None	None	None	Need to talk through all the combinations within RF system that ground should try when attempting to reacquire						
ME-1.1.1.1.a	Solar Array Flap Actuator	Fails to actuate when comm	nded <mark>Local</mark>	if potentiometer and step count are mismatched, turn on redundant ECU fo 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	r Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None			Power other ECU to compare potentiometer readings. If necessary, switch ECUs. re-command, slew, coolant system change	During encounter: if tip current sensors detect current, autonomously bring in solar arrays		Discuss with FSW about making on ECU "active"
ME-1.1.1.1.b	Solar Array Flap Actuator	Incorrect actuation when commanded	Local	if potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	r Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	7	?	None			Power other ECU to compare potentiometer readings. If necessary, switch ECUs. re-command, slew, coolant system change, go back to "home position" then re-count/recalibrate	During encounter: if tip current sensors detect current, autonomously bring in solar arrays		
ME-1.1.1.1.c	Solar Array Flap Actuator	Actuates when not command	ed Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	r Autonomy	?	2	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None			Power other ECU to compare potentiometer readings. If necessary, switch ECUs. re-command, slew, coolant system change, go back to "home position" then re-count/recalibrate	During encounter: if tip current sensors detect current, autonomously bring in solar arrays		This is designed to be non- credible

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Effect Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Detection Method TIm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
ME-1.1.1.1.d	Solar Array Flap Actuator		Launch locks fail to release	1) Frangibolt fails to release completely (electrically redundant, so more concerned with a mechanical fault) 2) Separation interfaces fail to release completely (mechanical clearance issues/unexpected interferences) (probably adding a push-off spring to ensure deployment)		Solar arrays are stuck stowed	No/limited power to s/c	Lost mission (insufficient power/heat generated at 1 AU with only one solar array)	N/A	2	Active		Potentiometer telemetry, battery fails to charge. Turn on redundant ECU for 3rd vote.	Potentiometer telemetry; redundant ECU telemetry Battery state of charge	ECU to REM	?	?
ME-1.1.1.1.e	Solar Array Flap Actuator		Launch lock premature release (two tie downs)	1) Temperature exceeds ~65C and frangibolt releases 2) inadvertent command (no power to safety bus until after s/c separation from 3rd stage) 3) Incorrect notch on frangibolt (controlled by 100% inspection of notch by vendor, will add a double-check to notch in I&T)		Array will not deploy, but will "chatter"	May damage cells and/or cooling system	With sufficient losses in Solar Arrays and cooling system, would lose mission	N/A	2	None	No	N/A	None	None	N/A	N/A
ME-1.1.1.2.a	Solar Array Feather Actuator		Fails to actuate when commander	1) bad/bound bearing/mechanical failure 2) stepper motor failure 3) loose/separated connector		Solar array stuck in position	generates insufficient power generates too much power gl geathering makes it impossible for array to retract sufficiently for encounter	retain partial power for a time; cooling system might	3) excessive feathering prevents array from retracting sufficiently for encounter	2	Active	Yes	Potentiometer telemetry. Turn on redundant ECU for 3rd vote.	Potentiometer telemetry; redundant ECU telemetry Battery state of charge	ECU to REM	?	?
ME-1.1.1.2.b	Solar Array Feather Actuator		Incorrect actuation when commanded	incorrect potentiometer reading residual torque (should have sufficient margin) Motor coil or winding is open		Solar array in incorrect position	generates insufficient power generates too much power feathering makes it impossible for array to retract sufficiently for encounter	retain partial power for a time; cooling system might	3) excessive feathering prevents array from retracting sufficiently for encounter	2	Active	Yes	Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Potentiometer telemetry; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	?	?
ME-1.1.1.2.c	Solar Array Feather Actuator		Actuates when not commanded	Holding torque exceeded (need to have sufficient margin)		Solar array in incorrect position	generates insufficient power generates too much power gal feathering makes it impossible for array to retract sufficiently for encounter	retain partial power for a time; cooling system might	3) excessive feathering prevents array from retracting sufficiently for encounter	2	Active	Yes	Power level	Potentiometer telemetry; redundant ECU telemetry Battery state of charge How do we detect power level?	ECU to REM	7	?
Inputs	Solar Array Feather Actuator		ECU commands ("commands" really are pulses of power to the motor)			Solar array in incorrect position	if SA needs to move out, generates insufficient power (different than required) if SA needs to move in, generates too much power (different than expected), potential overheating of wing (cells burned)	1) eventually drain battery, may be able to slew s/c to retain partial power for a time 2) lose mission	If in encounter, and SAs stuck out too far	2	Active	Yes	Power level, step count, (potentiometer telemetry). Turn on redundant ECU for 3rd vote.	Battery state of charge	ECU to REM	?	?
ME-1.2.1.a	HGA Gimbal		Fails to actuate when commander (mechanical failure)	bad/bound bearing/mechanical failure Exceeded life limit of bearing stepper motor failure d) loose/separated connector		HGA stuck in position	in some cases, may be able to slew spacecraft to point HGA to Earth.	Would have difficulty meeting minimum mission science return requirements. Worst case, loss of science.	If stuck at large enough angle, could be an umbra violation (~90-102deg is safe)	2 - if data return is too low 3 - if science requirements can still be met	Active		Potentiometer telemetry, step count	Autonomy could power up the other ECU to check redundant potentiometer telemetry against primary potentiometer telemetry and motor step count (3rd vote)	ECU to REM	?	?
ME-1.2.1.b	HGA Gimbal		Fails to actuate when commanded (electrical failure)	Short in redundant windings within actuator (two failures)		HGA stuck in position	In some cases, may be able to slew spacecraft to point HGA to Earth.		If stuck at large enough angle, could be an umbra violation (~90-102deg is safe)	2 - if data return is too low 3 - if science requirements can still be met	Active	Yes	Potentiometer telemetry, step count	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?	?
ME-1.2.1.g	HGA Gimbal		Launch locks fail to release	Frangibolt fails to release completely (mechanical failure of frangibolt) Sparation interfaces fail to crelease completely (mechanical clearance issues/unexpected interferences)		HGA stuck stowed	Could slew s/c to use HGA.	Difficulty in meeting mission science data return requirements.	Would exceed "safe" angle	2		Yes	Potentiometer telemetry				
ME-1.2.1.h	HGA Gimbal		Launch locks premature release	1) Temperature exceeds ~65C and frangibolt releases 2) inadvertent command 3) Incorrect notch on frangibolt		Dish may vibrate more than expected (causing damage), gimbal may degrade	Reduced ability to return science data.	Potential loss of science if dish damaged, eventual loss of science with premature failure of gimbal	When bearing dies, if stuck in position outside of "safe"	2		No					
ME-2.1.1.b	MAG Boom		Deploys prematurely (detail to come)	launch lock released prematurely 2) Inadvertent command (safety-inhibited load - safety bus relay can't be uninhibited by SW)		Boom would deploy	depending on orientation of fold, could hit s/c, shroud, damage an instrument, might block thruster or instrument FOV; could affect flight path or thermal environment	release of shroud. Loss of	No	2 - if enough critical components/ instruments are damaged 3 - if only loss of MAG sensor		Yes	When instruments powered, might see damage caused by premature deployment				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	t Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Response Time to Transmit Signal	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit Signal	Ground Response / Contingency	System Side Switch	Quick Look Processor Switch	Safe Mode	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
ME-1.1.1.1.d	Solar Array Flap Actuator		Launch locks fail to release	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC		?		None				slew to Sun, oversized motor can bust through, recommand frangibolt		ir	Could be mitigated by design if push springs were added - Wellun to consider
ME-1.1.1.1.e	Solar Array Flap Actuator		Launch lock premature release (two tie downs)	None	N/A	N/A	N/A		None	N/A	N/A	N/A	N/A							
ME-1.1.1.2.a	Solar Array Feather Actuator		Fails to actuate when commander	d Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	7	?	If problem persists, umbra violation or LBSOC		?	?	None				re-command, slew, coolant system change	During encounter: if tip current sensors detect current, autonomously bring in solar arrays; go to "safe" feathering position		
ME-1.1.1.2.b	Solar Array Feather Actuator		incorrect actuation when commanded	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None				re-command, slew, coolant system change, go back to "home position" then re-count/recalibrate	During encounter: If tip current sensors detect current, autonomously bring in solar arrays		
ME-1.1.1.2.c	Solar Array Feather Actuator		Actuates when not commanded	Local	if potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None					During encounter: if tip current sensors detect current, autonomously bring in solar arrays		
Inputs	Solar Array Feather Actuator		ECU commands ("commands" really are pulses of power to the imotor)	Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	None					During encounter: if tip current sensors detect current, autonomously bring in solar arrays		
ME-1.2.1.a	HGA Gimbal		Fails to actuate when commander (mechanical failure)	d _{Local}	If potentiometer and step. count are mismatched, turn on redundant ECU for 3rd vote; if third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	umbra violation	Autonomy	?	?	None				re-command, slew	command to a "safe" position		
ME-1.2.1.b	HGA Gimbal		Fails to actuate when commander (electrical failure)	d Local	If potentiometer and step count are mismatched, turn on redundant ECU for 3rd vote; If third vote is correct power off primary ECU otherwise system side switch???	Autonomy	?	?	umbra violation	Autonomy	?	?	None				Each motor winding goes to a different ECU.			
ME-1.2.1.g	HGA Gimbal		Launch locks fail to release																	
ME-1.2.1.h	HGA Gimbal		Launch locks premature release														If HGA and fan beams are permanently off-pointed (boresight no longer aligns), would be able to compensate with more DSN time.			
ME-2.1.1.b	MAG Boom		Deploys prematurely (detail to come)																х	

					1		Effect							Detection Method			
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Local	Next Higher	Mission	Umbra Violation	Severity	Type of FM	Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
ME-2.1.1.c	MAG Boom		Partial deployment	One or more hinges jams or locks One potential design has one launch lock, one potential design has two launch locks. Revisit after decision has been made.		Boom would only partially deploy	Loss of MAG boom	If outside umbra, will outgas, melt, bring thermal load into s/c. Paticulate matter, thermal load, outgassing, etc., are potentially mission-ending. Loss of the MAG sensor does not equal loss of science.	Yes	2			GNC might be able to tell from mass properties, torque from sola pressure, etc. Science team may see thermal effects.				
Inputs	MAG Boom		Electrical fault			electrical failure should prevent	If entire command fails, ground can re-send. A-side PDU drivers may have failured, so an avionics (PDU) side switch could allow command to be re- sent.	None	N/A	2							
Propulsion PR-1.1.a	Service Valve 1 (SV1) (Pressurant)		External leak (three seals would have to fail for this to occur)	1) Physical damage		Leaking helium	Over time will decrease system pressure, may torque s/c (depends on size of leak)		Depends on amount of torque and timing	2	Passive - design with 3 seals	Yes	Pressure decrease, wheels might see an unexpected torque (long- term trending)	Check presssure from P3 against previous reading?		N/A	N/A
PR-1.2.a	Service Valve 2 (SV2) (Liquid)		External leak (three seals would have to fail for this to occur)	1) Physical damage		Leaking hydrazine	Over time will decrease amount of fuel, could damage if it impacted the s/c, fuel loss	enough torque is applied	Depends on amount of torque and timing N/A until s/c runs out of usable	2	Passive - design with 3 seals	Yes	Pressure decrease, wheels might see an unexpected torque (long- term trending)	Check presssure from P3 against previous reading?		N/A	N/A
PR-2.a PR-2.b	Tank Tank		Internal leak (liquid into gas) External leak (pressurant)	in diaphragm) 1) Physical damage		out of the tank	Less fuel overall Over time will decrease system pressure, may torque s/c (depends on size of leak)	of usable fuel Mission-ending with complete loss of pressurant or if enough torque is	fuel Depends on amount of torque and timing	2	None None	No Yes	You'd run out of fuel early Pressure decrease, wheels might see an unexpected torque (long- term trending)	No Check presssure from P3 against previous reading?	N/A	N/A N/A	N/A N/A
PR-2.c	Tank		External leak (fuel)	1) Physical damage		Leaking hydrazine	Over time will decrease amount of fuel, could damage if it impacted the s/c, fuel loss	applied Mission-ending with complete loss of fuel or if enough torque is applied	Depends on amount of torque and timing	2	None	Yes	Pressure decrease, wheels might see an unexpected torque (long- term trending)	Check presssure from P3 against previous reading?		N/A	N/A
PR-3.1.c	Pressure Transducer A		External leakage (two seals would have to leak in order for this to occur)	1) Physical damage		Leaking hydrazine	Over time will decrease amount of fuel, could damage if it impacted the s/c, fuel loss		Depends on amount of torque and timing	2	None	Yes	Pressure decrease, wheels might see an unexpected torque (long- term trending)	Check presssure from P3 against previous reading?	N/A	N/A	N/A
PR-4.a	Filter 1 (F1)		Clogged or blocked	1) FOD in line 2) Contaminated propellant		No fuel to thrusters	Blocked prevents all thruster use	Mission ending	Yes if it happened at the wrong time, but mission is done at that point anyway	2	None	Yes	Thrusters stopped working	?	N/A	N/A	N/A
PR-5.a	Orifice 1 (O1)		Heavy contamination blockage	1) FOD in line 2) Contaminated propellant		No fuel to thrusters	Blocked prevents all thruster use	Mission ending	Yes if it happened at the wrong time, but mission is done at that point anyway	2	None	Yes	Thrusters stopped working	?	N/A	N/A	N/A
PR-7.1.b	Latch Valve A		External leakage (multiple seals would have to fail in order for this to happen)	1) Physical damage		Leaking hydrazine	Over time will decrease amount of fuel, could damage if it impacted the s/c, fuel loss	Mission-ending with complete loss of fuel or if enough torque is applied	Depends on amount of torque and timing	2	Passive - redundancy ?	Yes	Pressure decrease, wheels might see an unexpected torque (long- term trending)	Check presssure from P3 against previous reading?	N/A	N/A	N/A
PR-8.01.3.b	Valve Assembly (NC Solenoid Valves)		One or both failed closed	1) electrical failure 2) FOD 3) Physical issue			If s/c could switch to another set of thrusters, s/c might be ok, depending on speed of switch-over and momentum issues are surmountable	Potentially mission-ending (depending on timing). Momentum dumps would be ok with a 2nd set of thrusters available, but TCMs would probably need to be aborted.	Yes	2	None	Maybe	Post-burn attitude isn't as expected, an electrical issue might be detectable through current/voltage sensing	Attitude tlm - expected vs. actual			
Input	Valve Assembly (NC Solenoid Valves)		Bus voltage				If s/c could switch to another set of thrusters, s/c might be ok, depending on speed of switch-over and momentum issues are surmountable	Potentially mission-ending (depending on timing). Momentum dumps would be ok with a 2nd set of thrusters available, but TCMs would probably need to be aborted.	Yes	2	None	Maybe	Post-burn attitude isn't as expected, an electrical issue might be detectable through current/voltage sensing	Attitude tlm - expected vs. actual			
Thermal TH-1.1.a	Spacecraft MLI		Degraded/damaged	1) Dust 2) Optical properties			Depends on amount of damage, but would increase/decrease local temperatures.	Depends on area affected by degradation/damage.	Depends on area affected by degradation/damage - critical system damaged by high temperature could lead to an umbra violation.	2	None	Yes	Component temperature change			N/A	
TH-1.2.a	High-temperature MLI		Degraded/damaged	1) Dust 2) Optical properties		MILI dograded (damaged	Depends on amount of damage, but would increase/decrease local temperatures.	Depends on area affected by degradation/damage.	High-temp MLI is not covering equipment that could lead to an umbra violation.	2	None	Yes	Component temperature change			N/A	

								Response							Quick Look					
FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit	Desired System Response	Allocation of System Response	Time to fix system	Time to Transmit	Ground Response / Contingency	System Side Switch	Processor Switch	Safe Mode	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
						response		Signal	kespolise	response	system	Signal	Contingency	Switch				Rule		
ME-2.1.1.c	MAG Boom		Partial deployment																	
Inputs Propulsion	MAG Boom		Electrical fault																	
PR-1.1.a	Service Valve 1 (SV1) (Pressurant)		External leak (three seals would have to fail for this to occur)	None	None	None	None	None	None	None	None	None	None				P3 and P4 are not powered at the same time, need to understand how to determine pressure decrease	Nope		
PR-1.2.a	Service Valve 2 (SV2) (Liquid)		External leak (three seals would have to fail for this to occur)	None	None	None	None	None	None	None	None	None	None					Nope		
PR-2.a	Tank		Internal leak (liquid into gas)	None	None	None	None	None	None	None	None	None	None					Nope		
PR-2.b	Tank		External leak (pressurant)	None	None	None	None	None	None	None	None	None	None					Nope		
PR-2.c	Tank		External leak (fuel)	None	None	None	None	None	None	None	None	None	None					Nope		
PR-3.1.c	Pressure Transducer A		External leakage (two seals would have to leak in order for this to occur)		None	None	None	None	None	None	None	None	None					Nope		
PR-4.a	Filter 1 (F1)		Clogged or blocked	None	None	None	None	None	None	None	None	None	None					None		
PR-5.a	Orifice 1 (O1)		Heavy contamination blockage	None	None	None	None	None	None	None	None	None	None					None		
PR-7.1.b	Latch Valve A		External leakage (multiple seals would have to fail in order for this to happen)	None	None	None	None	None	None	None	None	None	None					Nope		
PR-8.01.3.b	Valve Assembly (NC Solenoid Valves)		One or both failed closed															Cycle power to valves		
	Valve Assembly (NC Solenoid Valves)		Bus voltage															Cycle power to valves		
Thermal	Spacecraft MLI		Degraded/damaged				N/A	Depends on severity of degradation/damage (time required to see temperature change in component)												
TH-1.2.a	High-temperature MLI		Degraded/damaged				N/A	Depends on severity of degradation/damage (time required to see temperature change in component)												