FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)

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**

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look		
				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 fix system	Time to Transmit Signal	Ground Response/ Contingency	System Side Switch	Processor Switch	Safe Mode

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

L	Launch
M	Commision
E	Encounter
C	Cruise

Severity

1	Catastrophic	Failure modes that could result in serious injury, loss of life, or loss of **spacecraft**.
1R		Failure modes of identical or equivalent redundant hardware or software elements that could result in Category 1 effects if all failed.
1S		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	Critical	Failure modes that could result in loss of **three** or more mission objectives
2R		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):	Geff Ottman (Avionics) Richard Nichols (initial 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.

						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-1	Redundant Proc Module																
AV-1.1	Avionics Redundancy Controller																
AV-1.1.1	Processor A (Prime)																
AV-1.1.1.a			No output	1) failed power supply 2) software hangs 3) hardware failure (chips, connectors, FPGA, etc.)	all	No way to recongnize failure, so it'd just keep going	Hot spare or ARC would recognize issue and ARC demotes Prime, making Hot Spare Prime	Loss of redundancy for causes 1 & 3	If switchover doesn't happen within required amount of time, but system is designed to handle this situation	2R	Active	yes	Hot spare would see it via software, ARC acknowledge timer on Prime would trigger				
AV-1.1.1.b			Incorrect output/timing	1) LVDS driver is flaky 2) SW issues 3) Communications path connector/harness issue (intermittent connection)		Might get feedback from SpaceWire (either no data return or bad data return). May self-demote	Hot spare would recognize issue (error detection on data transfer) and ARC demotes Prime, making Hot Spare Prime	Loss of redundancy	If switchover doesn't happen within required amount of time, but system is designed to handle this situation	2R	Active	yes	Hot spare would see it via software, ARC watchdog timer on Prime would trigger				
AV-1.1.1.c	(Input?)		Loss of SPW Timecode	LVDS receiver fails		Depends on SW configuration. Prime would stay as Prime.	Autonomy would command a side switch.	Loss of redundancy	If switchover doesn't happen within required amount of time, but system is designed to handle this situation	2R	Active	yes	Hot spare or Prime would see it				
AV-1.1.1.d			Hard failure	1) PWB crack 2) Connector disconnects 3) Converter card fails 4) Component failing short (could look like an overcurrent, which could cause an overtemp issue)		Processor dies	Hot spare would recognize issue and ARC demotes Prime, making Hot Spare Prime. New Prime would eventually turn processor off.	Loss of redundancy	If switchover doesn't happen within required amount of time, but system is designed to handle this situation	2R	Active	yes	Hot spare would see it via software, ARC watchdog timer on Prime would trigger				
AV-1.1.1.1	Watchdog Timer																
AV-1.1.1.1.a			Failure to timeout (when it should)	1) FPGA or LEON fails		Lose software with no way locally to recover	Hot spare would recognize issue or ARC watchdog timer would time out and ARC would demote Prime, making Hot Spare Prime	Loss of redundancy if FSW branches to WDT again.	If switchover doesn't happen within required amount of time, but system is designed to handle this situation	2S/R	Active	yes	Hot spare would see it or ARC WDT				
AV-1.1.1.1.b			Timeout when it shouldn't	1) FPGA fails		Reboot	Hot spare would recognize issue or ARC watchdog timer would time out and ARC would demote Prime, making Hot Spare Prime	Loss of redundancy	If switchover doesn't happen within required amount of time, but system is designed to handle this situation	2R if whole processor is lost 3 if processor can keep working with no WDT	Active	yes	Hot spare would see it or ARC WDT				
Inputs			SpW Router A (only one router active at a given time)			S/C internal communications fail, SpW timecode fails	Switch avionics sides, detected at SpW link level by autonomy rule; Prime tells ARC to switch from REM A to REM B	Loss of redundancy		2R			Autonomy rule				
			SpW Router B														
			SSR 1 (Prime only)	(ongoing SSR trade to potentially change to one SSR local to each processor, but connected to the other two SSRs)		Couldn't access recorder	Lose playback ability	Loss of SSR redundancy, could switch to SSR 2 without needing to switch REM	N/A		Active						
			SSR 2 (Prime only)														
			ARC Mode Controller 1			Notes that Mode Controller 1 isn't providing data	No effect on spacecraft (loss of redundancy), assuming that design can catch all of the possible failure modes	Loss of redundancy		2R	Passive						
			ARC Mode Controller 2														
			ARC Mode Controller 3														
AV-1.1.2	Processor B (Hot)																
AV-1.1.2.a			No output	1) failed power supply 2) software hangs 3) hardware failure (chips, connectors, FPGA, etc.)	all	No way to recongnize failure, so it'd just keep going	ARC would recognize issue and demote Hot Spare, and promote the Warm Spare or wrong data would just be outvoted (via triple voting). If demoted, processor would be demoted to "failed."	Loss of redundancy for causes 1 & 3	None.	2R	Active	yes	ARC would see it				

Subject Matter Expert(s): Geff Ottman (Avionics)
Richard Nichols (initial 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.

				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**	**Remediation**	**Helpful Autonomy Rule**	**Flag**	**Revisit**	**Comments - KAF**
AV-1	Redundant Proc Module																				
AV-1.1	Avionics Redundancy Controller																				
AV-1.1.1	Processor A (Prime)																				
AV-1.1.1.a			No output	Local	Processor switch	HW - ARC									X		- Switch to 2nd set of SW - Cause 2 could possibly be fixed with reboot				
AV-1.1.1.b			Incorrect output/timing	Local	Processor switch	HW - ARC									X		Could try to reboot to fix software issue				
AV-1.1.1.c	(Input?)		Loss of SPW Timecode	Local	Side switch	HW - ARC								X				Loss of timecode - would need to diagnose that it's not a SCIF failure, but the LVDS receiver failing			
AV-1.1.1.d			Hard failure	Local	Processor switch	HW - ARC									X			Autonomy rule on hot spare to detect hard failure of Prime			
AV-1.1.1.1	Watchdog Timer																				
AV-1.1.1.1.a			Failure to timeout (when it should)	Local	Processor switch	HW - ARC									X					X	
AV-1.1.1.1.b			Timeout when it shouldn't	Local	Processor switch	HW - ARC	Less than 10 ms for demote/promote								X					X	
Inputs			SpW Router A (only one router active at a given time)																	X	
			SpW Router B																		
			SSR 1 (Prime only)	Local	Side switch	Autonomy								X						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)																		
			ARC Mode Controller 1	None									No action by ARC, but if ground identified the issue this processor could be marked "failed"							X	
			ARC Mode Controller 2																		
			ARC Mode Controller 3																		
AV-1.1.2	Processor B (Hot)																				
AV-1.1.2.a			No output	Local	Hot spare demoted to "faield"	HW - ARC											Cause 2 could possibly be fixed with reboot				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: Time to Detect (System)
AV-1.1.2.b			Incorrect output/timing 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			"Evil" hot spare														
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-1.1.3	Processor C (Warm Spare)																
AV-1.1.3.a			No output	1) failed power supply 2) software hangs 3) hardware failure (chips, connectors, etc.)	all	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-1.1.3.1	Watchdog Timer																
AV-1.1.3.1.a			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.	2S/R	None	yes	Prime via SpW				

				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**	**Remediation**	**Helpful Autonomy Rule**	**Flag**	**Revisit**	**Comments - KAF**
AV-1.1.2.b			Incorrect output/timing A)SpW->router B) commands to ARC C) SW issues	Local	Hot spare demoted to "faield"	HW - ARC											SW issue could possibly be fixed with reboot	Prime could look for Hot Spare to be demoted			
AV-1.1.2.c			"Evil" hot spare																	X	
AV-1.1.2.d			Loss of SPW Timecode ("1PPS")	Local	Side switch?	HW - ARC												Loss of timecode - would need to diagnose that it's not a SCIF failure, but the LVDS receiver failing			
AV-1.1.2.e			Hard failure	Local	Hot spare demoted to "faield"	HW - ARC												Prime could look for Hot Spare to be demoted			
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)	Local	Hot spare demoted to "faield"	HW - ARC	Less than 10 ms for demote/promote													X	
AV-1.1.2.1.b			Timeout when it shouldn't	Local	Hot spare demoted to "faield"	HW - ARC	Less than 10 ms for demote/promote													X	
AV-1.1.3	Processor C (Warm Spare)																				
AV-1.1.3.a			No output	None			N/A. No fix possible other than to demote to cold spare. ARC commanded to not use this board.						No action by ARC, but if ground identified the issue this processor could be marked "failed"				Reboot might help a SW issue				
AV-1.1.3.b			Incorrect output/timing	None			N/A. No fix possible other than to demote to cold spare. ARC commanded to not use this board.						No action by ARC, but if ground identified the issue this processor could be marked "failed"				Reboot might help a SW issue				
AV-1.1.3.c			Loss of SPW Timecode	None			N/A. No fix possible other than to demote to cold spare. ARC commanded to not use this board.						No action by ARC, but if ground identified the issue this processor could be marked "failed"								
AV-1.1.3.d			Hard failure	None			N/A. No fix possible other than to demote to cold spare. ARC commanded to not use this board.						No action by ARC, but if ground identified the issue this processor could be marked "failed"					Loss of timecode			
AV-1.1.3.1	Watchdog Timer																				
AV-1.1.3.1.a			Failure to timeout (when it should)	None			N/A. No fix possible other than to demote to cold spare. ARC commanded to not use this board.													X	

						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-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	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																
AV-2	Redundant Elec Module																
AV-2.1	REM A																
AV-2.1.1	TAC A																
AV-2.1.1.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 control interfaces b) Thruster or reaction wheel stuck on	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				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
				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					
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.													X	
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																				
AV-1.4	Avionics Redundancy Controller (ARC) - Mode Controller 3																				
AV-2	Redundant Elec Module																				
AV-2.1	REM A																				
AV-2.1.1	TAC A																				
AV-2.1.1.a			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				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
Inputs			SpaceWire			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				
			Propulsion bus			Loss of thrusters	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				
			G&C component data			Loss of 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				
			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	Prime, non-responsive SpW interface; G&C closed loop SW				
AV-2.1.2	SSR A																
AV-2.1.2.a			Locks up/resets	Bad FPGA		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 3) Converter fails		Loss of SSR data	? (ongoing trade)	None.	None		Active	Yes	Prime via SpW				
Inputs			SpaceWire			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-2.1.2.1	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	SSR B																
AV-2.1.4	SpW Router A																
AV-2.1.4.a			No output	Failed FPGA		Loss of SpW connectivity	Consider reinitializatin of SCIF, but otherwise Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
AV-2.1.4.b			Incorrect output	Failed FPGA		Bad data	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
AV-2.1.4.c			Incorrect timing	Failed FPGA		Bad data	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
Inputs			SpaceWire			Loss of SpW connectivity	Consider reinitializatin of SCIF, but otherwise Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
			Bus voltage			Loss of SpW connectivity	Consider reinitializatin of SCIF, but otherwise Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
			Incorrect input			Router continues functioning normally	Will detect incorrect input elsewhere (depending on what the input was and where it was routed to)				?						
			Bad input														
AV-2.1.5	SCIF 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 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	Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
Inputs			SpaceWire	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Try power cycle during check-out or ground contact				
			Propulsion bus	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Try power cycle during check-out or ground contact				
			G&C component data	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Try power cycle during check-out or ground contact				
			Secondary power	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Try power cycle during check-out or ground contact				
AV-2.1.2	SSR A																				
AV-2.1.2.a			Locks up/resets	Local	3 SSRs tied to each SBC, initial thought is that SBC sees error with SSR and requests demotion from ARC???	Processor	SSR switchover; File system mount										Try power cycle			X	
AV-2.1.2.b			Hard failure	Local	3 SSRs tied to each SBC, initial thought is that SBC sees error with SSR and requests demotion from ARC???	Processor	SSR switchover; File system mount										Try power cycle			X	
Inputs			SpaceWire	Local	3 SSRs tied to each SBC, initial thought is that SBC sees error with SSR and requests demotion from ARC???	Processor	SSR switchover; File system mount										Try power cycle			X	
			Secondary power	Local	3 SSRs tied to each SBC, initial thought is that SBC sees error with SSR and requests demotion from ARC???	Processor	SSR switchover; File system mount										Try power cycle			X	
AV-2.1.2.1	Memory																				
AV-2.1.2.1.a			Memory IC failure	Local	3 SSRs tied to each SBC, initial thought is that SBC sees error with SSR and requests demotion from ARC???	Processor	Add to bad block table										Try power cycle			X	
AV-2.1.3	SSR B																				
AV-2.1.4	SpW Router A																				
AV-2.1.4.a			No output	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
AV-2.1.4.b			Incorrect output	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
AV-2.1.4.c			Incorrect timing	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
Inputs			SpaceWire	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
			Bus voltage	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
			Incorrect input	?	?	?														X	
			Bad input																	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 interface)		Loss of interface with particular S/C component or instrument	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
AV-2.1.5.b			Hard failure	Cracked board; failed FPGA		Loss of interface with all S/C components and instruments	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
AV-2.1.5.c			Incorrect timing with transponder clock interface	Failed FPGA		Bad data	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
AV-2.1.5.d			Incorrect output	Failed FPGA		Bad data	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
Inputs			SpaceWire			Loss of interface with all S/C components and instruments	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
			Secondary Power			Loss of interface with all S/C components and instruments	Prime tells ARC to initiate side switch, ARC switches sides of avionics	None	Depends on side switch and reconfig time	2R	Active	Yes	Prime via SpW				
			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) components	Active	Yes	Prime via SpW				
			EMXO - EMXO lives in XCVR now; Rich Conde is working on a fault mitigation plan.	1) Harness break 2) Failure at source (see transponder)		Won't receive PPS or 50 Hz	May attempt to reconfigure first, but may also try side switch of REM (won't work unless transponders are switched too). Path taken would depend on first symptom seen.	None	Depends on side switch and reconfig time		Active						
AV-2.1.5.1	CCD (TBD - probably going away)																
AV-2.1.5.1.a			Hard failure	Failed FPGA		Loss of config commands	None	None	None	4		Yes	Ground verification of CCD commands				
AV-2.2	REM B																
AV-2.2.1	TAC B																
AV-2.2.2	SSR B																
AV-2.2.2.1	Memory																
AV-2.2.3	SpW Router B																
AV-2.2.4	SCIF B																
AV-2.2.4.1	CCD																
AV-2.2.4.2	EXMO																
AV-4	RIUs																
AV-3.1	RIU-A																
AV-3.1.01	RIU-A 1																
AV-3.1.01.a	RIUs are cross-strapped - two eight-RIU strips which can be powered by REM A or REM B. 16 RIUs total		No output	1) Broken wire 2) IC failure 3) Hard short on card		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. 3) REM would current-limit RIU power causing the loss of the string.	None	None	4	Active	yes	FSW detects bad data			2-3 seconds (for critical data)	
AV-3.1.01.b			Incorrect output	Loose wire or noise		Bad temp data from sensor	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)	
AV-3.1.01.c			Incorrect timing	Loose wire or noise		Bad temp data from sensor	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)	
Inputs			Secondary Power			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)	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
				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					
AV-2.1.5.a			Local failure	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
AV-2.1.5.b			Hard failure	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
AV-2.1.5.c			Incorrect timing with transponder clock interface	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
AV-2.1.5.d			Incorrect output	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
Inputs			SpaceWire	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
			Secondary Power	Local	Prime requests ARC side switch	HW - ARC	Side switchover							X			Power cycle during ground contact & perform REM check out				
			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			X	
			EMXO - EMXO lives in XCVR now; Rich Conde is working on a fault mitigation plan.	Local	Prime requests ARC side switch May reconfigure EMXO first????	HW - ARC								X						X	
AV-2.1.5.1	CCD (TBD - probably going away)																				
AV-2.1.5.1.a			Hard failure				Side switchover														
AV-2.2	REM B																				
AV-2.2.1	TAC B																				
AV-2.2.2	SSR B																				
AV-2.2.2.1	Memory																				
AV-2.2.3	SpW Router B																				
AV-2.2.4	SCIF B																				
AV-2.2.4.1	CCD																				
AV-2.2.4.2	EXMO																				
AV-4	RIUs																				
AV-3.1	RIU-A																				
AV-3.1.01	RIU-A 1																				
AV-3.1.01.a	RIUs are cross-strapped - two eight-RIU strips which can be powered by REM A or REM B. 16 RIUs total		No output	Local	For critical loads, switch to redundant unit if temp data above threshold or missing/stale?	Autonomy											Power cycle during ground contact.				
AV-3.1.01.b			Incorrect output	Local	For critical loads, switch to redundant unit if temp data above threshold or missing/stale?	Autonomy											Power cycle during ground contact.				
AV-3.1.01.c			Incorrect timing	Local	For critical loads, switch to redundant unit if temp data above threshold or missing/stale?	Autonomy											Power cycle during ground contact.				
Inputs			Secondary Power	Local	For critical loads, switch to redundant unit if temp data above threshold or missing/stale?	Autonomy											Power cycle during ground contact.				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (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)	
AV-3.1.02	RIU-A 2																
AV-3.1.03	RIU-A 3																
AV-3.1.04	RIU-A 4																
AV-3.1.05	RIU-A 5																
AV-3.1.06	RIU-A 6																
AV-3.1.07	RIU-A 7																
AV-3.1.08	RIU-A 8																
AV-3.2	RIU-B																
AV-3.2.01	RIU-B 1																
AV-3.2.02	RIU-B 2																
AV-3.2.03	RIU-B 3																
AV-3.2.04	RIU-B 4																
AV-3.2.05	RIU-B 5																
AV-3.2.06	RIU-B 6																
AV-3.2.07	RIU-B 7																
AV-3.2.08	RIU-B 8																
AV-3	Power Distribution Unit																
AV-4.1	Side A																
AV-4.1.1	CMD TLM A	1) Provides C&DH command interface to PDU 2) Provides PDU telemetry interface to C&DH 3) Provides +5V to Relay/Cap and FET Switching slices 4) Provides internal bus signals 5) Provides separation interface															
AV-4.1.1.a			Lock up	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		Unable to interface with REM and provide command/telemetry interface	Loads all get switched off. Switch sides of Avionics. Reset sequence in PDU switches loads back on.	No effect	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		

				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**	**Remediation**	**Helpful Autonomy Rule**	**Flag**	**Revisit**	**Comments - KAF**
			I2C bus	Local	For critical loads, switch to redundant unit if temp data above threshold or missing/stale?	Autonomy											Power cycle during ground contact.				
			Telemetry input (temp sensor, tell tales)	Local	For critical loads, switch to redundant unit if temp data above threshold or missing/stale?	Autonomy											Power cycle during ground contact.				
AV-3.1.02	RIU-A 2																				
AV-3.1.03	RIU-A 3																				
AV-3.1.04	RIU-A 4																				
AV-3.1.05	RIU-A 5																				
AV-3.1.06	RIU-A 6																				
AV-3.1.07	RIU-A 7																				
AV-3.1.08	RIU-A 8																				
AV-3.2	RIU-B																				
AV-3.2.01	RIU-B 1																				
AV-3.2.02	RIU-B 2																				
AV-3.2.03	RIU-B 3																				
AV-3.2.04	RIU-B 4																				
AV-3.2.05	RIU-B 5																				
AV-3.2.06	RIU-B 6																				
AV-3.2.07	RIU-B 7																				
AV-3.2.08	RIU-B 8																				
AV-3	Power Distribution Unit																				
AV-4.1	Side A																				
AV-4.1.1	CMD TLM A	1) Provides C&DH command interface to PDU 2) Provides PDU telemetry interface to C&DH 3) Provides +5V to Relay/Cap and FET Switching slices 4) Provides internal bus signals 5) Provides separation interface																			
AV-4.1.1.a			Lock up	Local	System side switch; return to previous load configuration	Autonomy	n/a	TBD - based on autonomy rule						X			Autonomy would see stale data or would set a flag indicating stale/non-responsive PDU and switch to B side.				
AV-4.1.1.b			Unexpected reset	Local	System side switch; return to previous load configuration	Autonomy															
AV-4.1.1.c			PDU Power and reset sequence doesn't run when expected	Local	System side switch; return to previous load configuration	Autonomy															
AV-4.1.1.d			Hard failure	Local	System side switch; return to previous load configuration	Autonomy											Switch to side B				No PDU switch, this should be system side switch
Inputs			Command/ telemetry interfaces	Local	System side switch; return to previous load configuration	Autonomy														X	No PDU switch, this should be system side switch

						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)
			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	yes	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 failure) 2) Battery would discharge	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						

				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	Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
			2 Breakwires	Local	System side switch; return to previous load configuration	Autonomy											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)																		
AV-4.1.2.e			Fails to provide function #5 (connection to single																	X	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: Time to Detect (System)
AV-4.1.2.f			Fails to provide function #6 (power to unswitched services)			Heaters 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.	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.	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.	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 effect.	No effect.	N/A	4	None						
AV-4.1.2.j			Fails to provide function #9b (arming plug monitoring)		Ground only	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		Ground only	Detatches at launch.	No effect.	No effect.	N/A	4	None						
			Separation (from upper stage) indicators			Redundant separation indicators on each PDU.	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	Passive - Redundancy						
AV-4.1.2.1	Fuse Module	1) Provides fusing to all loads															
AV-4.1.2.1.a			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.)	1) Design	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	2S - 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.	Load current	PDU to REM		

				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	Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
AV-4.1.2.f			Fails to provide function #6 (power to unswitched services)																	X (check for double-insulated wires)	
AV-4.1.2.g			Fails to provide function #7 ("common relays")																		
AV-4.1.2.h			Fails to provide function #8 (connection to umbilical power)																		
AV-4.1.2.i			Fails to provide function #9a (fuse monitoring)																		
AV-4.1.2.j			Fails to provide function #9b (arming plug monitoring)																		
AV-4.1.2.k			Fails to provide function #9c (temperature monitoring)																		
Inputs			EPS Power	Local	System side switch; return to previous load configuration	Autonomy								X							
			Umbilical power																		
			Separation (from upper stage) indicators																		
AV-4.1.2.1	Fuse Module	1) Provides fusing to all loads																			
AV-4.1.2.1.a			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.)	Local	Consider having an over-current rule for each switched 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			X	
AV-4.1.2.1.b			Blows too soon	Local	Consider having an over-current rule for each switched 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			X	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: 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.	LOM	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			Incorrect PRIO 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	E, M, C	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	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 over-current 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		Pulsed load being sent continuous power (rather than pulsed) via high-side FET. Both FETs would need to fail for this to be a problem (see Propulsion Latch valves for example of what could happen if BOTH FETs failed stuck continuously on for a pulsed load).	Switch off low-side FET to turn off power to pulsed load.	No effect.	N/A	4	Active	yes	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	yes	Load continues to be powered off after power on command.	Load current	PDU to REM		
AV-4.1.3.d			Hard failure	1) Electronics failure 2) Connector/cable failure 3) Common electronics (redundant within FET slice)	E, M, C	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?					
			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	1) Provides over-current protection to fuse (set to short time period, high current)															

				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**	**Remediation**	**Helpful Autonomy Rule**	**Flag**	**Revisit**	**Comments - KAF**
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)																		
AV-4.1.2.2.b			Hard failure (could take out one or both PRIOs - need both on a side)																	X	
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			X	
AV-4.1.2.2.d			Lock-up/reset	Local	TBD	Autonomy											Switch to side B, and/or off-pulse			X	
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 over-current 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 current for TBD seconds and switch off low-side FET; LVs are one known load	Autonomy														X	
AV-4.1.3.c			FET stuck off	Local	TBD which loads, but monitor for one of two always on?	Autonomy														X	
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	1) Provides over-current protection to fuse (set to short time period, high current)																			

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
AV-4.1.3.1.a			Unable to reset	1) Part Failure	E, M, C	1) Assuming load has tripped circuit breaker, loss of switched load 2) If load has not tripped circuit breaker, then no effect	1) Potential loss of a single instrument suite. Cycling power to load may reset circuit breaker. Ground would probably investigate problem at next ground contact.	1) Degraded or LOM depending on which switched 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 continues to be powered off after power on command.	Load current	PDU to REM		
AV-4.1.3.1.b			Opens without stimuli	1) Part Failure	E, M, C	1) Loss of switched load	1) MOPs sends commands to reset circuit breaker	1) 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 4 - 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	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 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 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		
Inputs			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	Fuse Module	1) Provides fusing to all loads															
AV-4.1.3.2.a			Blows below rated current	1) Design 2) Transient voltage 3) "Smart" short (high current setting that is not detected - multiple failures)	E, M, C	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.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 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		
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 over-current protection															
AV-4.1.3.3.a			Hard failure	1) Electronics failure 2) Connector/cable failure 3) SW failure	E, M, C	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		

				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	Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
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											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			X	
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	Fuse Module	1) Provides fusing to all loads																			
AV-4.1.3.2.a			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)	Local	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 over-current 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			X	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
AV-4.1.3.3.b			Incorrect PRIO configuration	1) Radiation 2) Bad command sent to prio and corrupted 3) SW failure	E, M, C	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.	Yes if prop loads (thrusters, latch valves) 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.	Yes if prop loads (thrusters, latch valves) 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.	Yes if prop loads (thrusters, latch valves) 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 - 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.	Yes if prop loads (thrusters, latch valves) 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		
			i2c 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.	Yes if prop loads (thrusters, latch valves) 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-4.1.4	FET Slice 2																

				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**	**Remediation**	**Helpful Autonomy Rule**	**Flag**	**Revisit**	**Comments - KAF**
AV-4.1.3.3.b			Incorrect PRIO configuration	Local	TBD - if load stuck on when commanded off, consider rule for system side switch?	Autonomy											MOPs sends commands with PRIO reconfiguration scripts			X	
AV-4.1.3.3.c			Lock-up/reset	Local	TBD - if load stuck on when commanded off, consider rule for system side switch?	Autonomy											Switch to side B			X	
Inputs			i2c bus - clock	Local	TBD - if load stuck on when commanded off, consider rule for system side switch?	Autonomy														X	
			i2c bus - serial data	Local	TBD - if load stuck on when commanded off, consider rule for system side switch?	Autonomy														X	
			i2c bus - reset line	Local	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														X	
			i2c bus - ground	Local	TBD - if load stuck on when commanded off, consider rule for system side switch?	Autonomy														X	
			i2c bus - PRIO clock	Local	TBD - if load stuck on when commanded off, consider rule for system side switch?	Autonomy														X	
AV-4.1.4	FET Slice 2																				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (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																

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Remediation	Helpful Autonomy Rule	Flag	Revisit	Comments - KAF
				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					
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																				

Subject Matter Expert(s): Lew Roufberg

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

						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)**
EP-1	Power System Electronics																
EP-1.1	PSE-1																
EP-1.1.1	Bus Junction Slice																
EP-1.1.1.a			Loss of telemetry (load 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 load 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.b			Loss of telemetry (battery 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 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.	Battery could continue to discharge if no side switch. With side switch, no effect.	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.	N/a	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 voltage	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 Expert(s): Lew Roufberg

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

				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**	**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**	**Remediation**
EP-1	Power System Electronics																	
EP-1.1	PSE-1																	
EP-1.1.1	Bus Junction Slice																	
EP-1.1.1.a			Loss of telemetry (load current)	Local	Contingecy Procedure	Ground	?	~1 sec (action depends on persistence decided on by fault protection)	?	None	None	None	None	Long-term trending to identify way to adjust for change in scale; work-around for verifying load current				Possibility of reprogramming something
EP-1.1.1.b			Loss of telemetry (battery current)	Local	Contingecy Procedure	Ground	?	~1 sec (action depends on persistence decided on by fault protection)	?	None	None	None	None	Long-term trending to identify way to adjust for change in scale; work-around for verifying load current				Possibility of reprogramming something
EP-1.1.1.c			Loss of telemetry (battery voltage)	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	None				Side switch
Inputs			Buck converter power	None	None	Ground	?	?	?	None	None	None	None	If margin isn't sufficient, power cycle non-critical loads to reduce power needed by system				
			Relay command (only changes when a fault occurs and it needs to change state)	None	None	Ground	?	?	?	None	None	None	None	Ground contingency to bring buck converters back online (power cycle all?)				Wait until next ground contact, send command to reset relay.
				None	None	Ground	?	?	?	None	None	None	None	None - loss of mission, but double fault				
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				
EP-1.1.2.b			Open (isolation diodes)	None	None	None	None	None	None	None	None	None	None	None				
EP-1.1.2.c			Loss of telemetry (current)	Local	Contingecy Procedure	Ground	?	~1 sec (action depends on persistence decided on by fault protection)	?	None	None	None	None	Long-term trending to identify way to adjust for change in scale; work-around for verifying load current				Possibility of reprogramming something
EP-1.1.2.d			Loss of telemetry (voltage)	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				

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			
EP-1.1.1.a			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	X
			Relay command (only changes when a fault occurs and it needs to change state)	
				X
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")

						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)
Inputs			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	?	?
EP-1.1.3	Solar Array Junction Slice 2																
EP-1.1.4	Buck Converter Slice 1 of 4																
EP-1.1.4.a			No output	1) Open circuit output fuse		Converter slice will be off. Telemetry will indicate 0 amps	No effect. Can lose a single buck converter.	No effect.	N/a	4	None	Yes	Telemetry	Buck converter current	PSE to CDH	?	?
EP-1.1.4.b			Incorrect current	1) reference voltage drift		Current will be too high or too low. Excessive current will be limited internally.	Controller will compensate for low/high current from a single converter.	No effect.	N/a	4	Passive	Yes	Telemetry	Buck converter current	PSE to CDH	?	?
EP-1.1.4.c			Incorrect switching frequency	1) IC failure or input problem on controller slice		Potential impact on conducted emissions	Potential EMC/EMI issue for instruments; switch sides to clear problem	Worst case, lose data for one encounter	N/a	3	None	Not directly	Notice EMC/EMI in instruments, but wouldn't necessarily be able to pinpoint PSE	EMC/EMI in instruments	?	?	?
Inputs			Control signal from controller card			Could either produce too much power or not enough	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	Battery will either be undercharged or overcharged	SA current, Buck converter current?	PSE to CDH	?	?
			Solar array power from SAJB	1) relay inside buck converter fails 2) SAJB failure		No effect to card	Buck converter stops relaying power	No effect (s/c has sufficient margin to operate with loss of a single buck converter)	N/a	4	None	Yes	Battery discharging unexpectedly	Buck Converter Current	PSE to CDH	?	None
EP-1.2	PSE-2																
EP-1.2.1	CMD/TLM A																
EP-1.2.1.a			Hard failure	1) power supply input opens in feed path 2) FPGA fails		CMD/TLM A fails, no telemetry output.	Autonomy would see a lack of telemetry or problem with telemetry and would command PDU to switch to avionics side B. Would probably also try to reset card - would not fix problem, but it would be impossible to tell the difference between this failure mode and the "no telemetry output" failure mode.	No effect.	N/A	2R	Active	Yes	Loss of telemetry	PSE CMD/TLM heartbeat	PSE to CDH to Autonomy	?	None
EP-1.2.1.b			No telemetry output	1) output transmitter not powered 2) open circuit		Card would continue operating but no telemetry output.	Reset card. If necessary, switch to side B.	No effect.	N/A	4	Active	yes	Loss of telemetry	PSE CMD/TLM heartbeat	PSE to CDH to Autonomy	?	None
EP-1.2.1.c			Locks up/resets	1) SEU		Card requires a commanded reset, no telemetry output or hung telemetry.	Reset card. If necessary, switch to side B.	No effect.	N/A	4	Active	yes	Loss of telemetry	PSE CMD/TLM heartbeat	PSE to CDH to Autonomy	?	None
EP-1.2.1.d			Loss of ability to command	1) input receiver not powered (or open circuit in path) 2) FPGA fails		Loss of telemetry	Reset card. If necessary, switch to side B.	No effect.	N/A	4	Active	yes	Loss of telemetry	PSE CMD/TLM heartbeat	PSE to CDH to Autonomy	?	None

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response											Quick Look			Remediation
				Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	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	
Inputs			Solar array power	None	None	None	None	None	None	None	None	None	None	None				Solar arrays would extend to increase 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				
EP-1.1.4.b			Incorrect current	Local	Limit current on buck converter	HW	?	~1 sec	None	None	None	None	None	None				
EP-1.1.4.c			Incorrect switching frequency	Local	PSE side switch	Ground	?	?	?	None	None	None	None	Trending of EMC/EMI in instruments; ground would need to isolate where issue is coming from, PSE side switch to clear problem				Diagnose by turning each converter off individually to see if it fixes problem. Leave off the bad one.
Inputs			Control signal from controller card	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				Cycle power to controller card
			Solar array power from SAJB	None	None	Ground	?	?	?	None	None	None	None	If margin isn't sufficient, power cycle non-critical loads to reduce power needed by system				
EP-1.2	PSE-2																	
EP-1.2.1	CMD/TLM A																	
EP-1.2.1.a			Hard failure	Local	PSE reset PSE side switch	Autonomy	?	~1 sec	?	None	None	None	None	Do we want tiered autonomy response where we power cycle first and the PSE side switch? Or we can just side switch and allow the ground to try to power cycle to "fix" problem				
EP-1.2.1.b			No telemetry output	Local	PSE reset PSE side switch	Autonomy	?	~1 sec	?	None	None	None	None	Do we want tiered autonomy response where we power cycle first and the PSE side switch? Or we can just side switch and allow the ground to try to power cycle to "fix" problem				Reset card
EP-1.2.1.c			Locks up/resets	Local	PSE reset PSE side switch	Autonomy	?	~1 sec	?	None	None	None	None	Do we want tiered autonomy response where we power cycle first and the PSE side switch? Or we can just side switch and allow the ground to try to power cycle to "fix" problem				Reset card
EP-1.2.1.d			Loss of ability to command	Local	PSE reset PSE side switch	Autonomy	?	~1 sec	?	None	None	None	None	Do we want tiered autonomy response where we power cycle first and the PSE side switch? Or we can just side switch and allow the ground to try to power cycle to "fix" problem				Reset card

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Revisit
Inputs			Solar array power	
EP-1.1.3	Solar Array Junction Slice 2			
EP-1.1.4	Buck 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	
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-1.2.1.c			Locks up/resets	
EP-1.2.1.d			Loss of ability to command	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
Inputs			LVPS			CMD/TLM A fails, no telemetry output.	Autonomy would see a lack of telemetry or problem with telemetry and would command PDU to switch to side B.	No effect.	N/A	2R	Active	Yes	Loss of telemetry	PSE CMD/TLM heartbeat	PSE to CDH to Autonomy	?	None
			REM commands			Invalid telemetry	Reset card. If necessary, switch to side B.	No effect.	N/A	4	Active	yes	Loss of telemetry	PSE CMD/TLM heartbeat	PSE to CDH to Autonomy	?	None
EP-1.2.2	Controller A																
EP-1.2.2.a			Hard failure	1) Power input could be open/short 2) FPGA fails		Lose FPGA telemetry (depending on exact failure). No signal output to buck converters.	Buck converters will stay at last commanded level. Attempt to reset slice. Eventually load requirements will change, but provided power will not. Battery will discharge. Switch sides of Avionics.	No effect.	N/A	2R	Active	yes	Eventually provided power will not match up with load requirements.	Local level - ? System level - LBOSC?	PSE to CDH to Autonomy	?	?
EP-1.2.2.b			Incorrect output	1) Reference voltage drift 2) SEU affects a register value		Will either be over- or under-charging the battery	See over/under charge in telemetry and reset slice. Autonomy will direct PDU to switch to side B	No effect.	N/A	4	Active	yes	See battery over/under charge in telemetry.	SA current, Buck converter current?	PSE to CDH	?	?
Inputs			Telemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board			Signal from card would be incorrect.	Could cause buck converter to either over or under-current. Autonomy would see battery over-current or under-voltage and would direct PDU to switch to other side of PSE.	No effect with side switch.	N/a	4	Active	yes	battery over-current or under-voltage	SA current, Buck converter current?	PSE to CDH to Autonomy	?	?
			LVPS			Lose FPGA telemetry (depending on exact failure). No signal output to buck converters.	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. Battery will discharge.	No effect.	N/A	4	Active	yes	Telemetry indicates 0 buck converter output.	Buck converter current	PSE to CDH to Autonomy	?	?
EP-1.2.3	LVPS A																
EP-1.2.3.a			No output	Open circuit FET		Loss of power to controller and command/telemetry	No telemetry; Autonomy would see no power to LVPS or no telemetry or incorrect voltage someplace and would direct PDU to switch to redundant side	No effect.	N/A	2R	Active	Yes	Loss of telemetry	LVPS current or heartbeat	PSE to CDH to Autonomy	?	?
EP-1.2.3.b			Incorrect output	Reference voltage circuit failure		Drift in voltage, erratic operation, or no telemetry	Switch to redundant side	No effect.	N/A	2R	Active	Yes	Telemetry indicates drift in voltage, erratic operation, or no telemetry	LVPS heartbeat, how to detect drift in voltage?	PSE to CDH to Autonomy	?	?
Inputs			Bus voltage from PDU			Loss of power to controller and command/telemetry	No telemetry; Autonomy would see no power to LVPS or no telemetry or incorrect voltage someplace and would direct PDU to switch to redundant side	No effect.	N/A	4	Active	Yes	Loss of telemetry	LVPS current or heartbeat	PSE to CDH to Autonomy	?	?
EP-1.2.4	CMD/TLM B																
EP-1.2.5	Controller B																
EP-1.2.6	LVPS B																
EP-2	Li-Ion Battery																
EP-2.1	Cell 1 of n		20 parallel strings of 8 cells each, could lose any 1 string of cells.														

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response											Quick Look			Remediation
				Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	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	
Inputs			LVPS	Local	PSE reset PSE side switch	Autonomy	?	~1 sec	?	None	None	None	None	Do we want tiered autonomy response where we power cycle first and the PSE side switch? Or we can just side switch and allow the ground to try to power cycle to "fix" problem				
			REM commands	Local	PSE reset PSE side switch	Autonomy	?	~1 sec	?	None	None	None	None	Do we want tiered autonomy response where we power cycle first and the PSE side switch? Or we can just side switch and allow the ground to try to power cycle to "fix" problem				Reset card
EP-1.2.2	Controller A																	
EP-1.2.2.a			Hard failure	Local / System	Reset Controller A slice? (Not sure how to compare power vs load requirement)	Autonomy	?	?	?	Load shed / system side switch	Autonomy / HW?	?	?	?	x		x	Might combine some functions with CMD/TLM slice
EP-1.2.2.b			Incorrect output	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				
Inputs			Telemetry from bus junction slice and/or Cmd/Tlm interface, or signal from SAJ board	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				CMD/TLM slice reset
			LVPS	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				Might combine some functions with CMD/TLM slice
EP-1.2.3	LVPS A																	
EP-1.2.3.a			No output	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				
EP-1.2.3.b			Incorrect output	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				
Inputs			Bus voltage from PDU	Local	PSE side switch	Autonomy	?	?	?	None	None	None	None	?				
EP-1.2.4	CMD/TLM B																	
EP-1.2.5	Controller B																	
EP-1.2.6	LVPS B																	
EP-2	Li-Ion Battery																	
EP-2.1	Cell 1 of n		20 parallel strings of 8 cells each, could lose any 1 string of cells.															

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	Controller B			
EP-1.2.6	LVPS B			
EP-2	Li-Ion Battery			
EP-2.1	Cell 1 of n		20 parallel strings of 8 cells each, could lose any 1 string of cells.	

						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)
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	Yes	Long-term battery trending	Battery voltage	PSE to CDH	?	?
EP-2.1.b			Open	Open interconnect		Slight reduction in battery capacity	Slight reduction in battery storage capacity	No effect.	N/A	4	None	Yes	Long-term battery trending	Battery voltage	PSE to CDH	?	?
EP-2.1.c			High Impedance	Excessive degradation		Slight reduction in battery capacity	Slight reduction in battery storage capacity	No effect.	N/A	4	None	Yes	Long-term battery trending	Battery voltage	PSE to CDH	?	?
Inputs			Current from bus junction slice			Battery would discharge and voltage would decrease	Bus voltage would decrease	No effect	N/A	4	None	Yes	Battery current telemetry	Battery current and voltage?	PSE to CDH	?	?
EP-3	Solar Arrays																
EP-3.1	Solar Array 1																
EP-3.1.1	Primary Array																
EP-3.1.1.1	Strings																
EP-3.1.1.1.a			Short to ground	Insulator breakdown		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	?	?
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	?	?
EP-3.1.1.1.1	Cells (with bypass diodes)																
EP-3.1.1.1.1.a			Short	Shorted diode		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
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
EP-3.1.2	Secondary Array																
EP-3.1.2.1	Strings																
EP-3.1.2.1.a			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	?	?
EP-3.1.2.1.1	Cells (with bypass diodes)																
EP-3.1.2.1.1.a			Short	Shorted diode		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

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response											Quick Look			Remediation
				Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	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	
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?				
EP-2.1.b			Open	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?				
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?				
Inputs			Current from bus junction slice	None	None	None	?		?	None	None	Nne	None					Depends on root cause; switching PSE 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																	
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?				
EP-3.1.1.1.b			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?				
EP-3.1.1.1.1	Cells (with bypass diodes)																	
EP-3.1.1.1.1.a			Short	None	None	None	None	None	None	None	None	None	None	None				
EP-3.1.1.1.1.b			Open	None	None	None	None	None	None	None	None	None	None	None				
EP-3.1.2	Secondary Array																	
EP-3.1.2.1	Strings																	
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.
EP-3.1.2.1.b			Open	None	None	None	?	2 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?				
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	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	
Inputs			Current from bus junction slice	
EP-3	Solar Arrays			
EP-3.1	Solar Array 1			
EP-3.1.1	Primary Array			
EP-3.1.1.1	Strings			
EP-3.1.1.1.a			Short to ground	
EP-3.1.1.1.b			Open	
EP-3.1.1.1.1	Cells (with bypass diodes)			
EP-3.1.1.1.1.a			Short	
EP-3.1.1.1.1.b			Open	
EP-3.1.2	Secondary Array			
EP-3.1.2.1	Strings			
EP-3.1.2.1.a			Short to ground	
EP-3.1.2.1.b			Open	
EP-3.1.2.1.1	Cells (with bypass diodes)			
EP-3.1.2.1.1.a			Short	

						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)
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		Loss of telemetry for one sensor cell (used for fault protection and calibration)	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	1) Cracked cell 2) Excessive darkening (should affect all cells equally)		Out of limit or incorrect telemetry for one sensor cell (used for fault protection and calibration). Would likely only decrease output, not trip safing limit.	Use redundant sensor cell (no side switching is required). Might need to adjust autonomy parameters based on trending (via ground analysis).	No effect.	N/A	4	Active	Yes	Telemetry	Sensor Cell Tlm	PSE to CDH to Autonomy	?	None
EP-3.1.2.2.c			Debond failure			Solar array temperature would increase	Take sensor offline. Might need to adjust autonomy parameters based on trending (via ground analysis).	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	Primary Array																
EP-3.2.1.1	Strings																
EP-3.2.1.1.1	Cells																
EP-3.2.2	Secondary Array																
EP-3.2.2.1	Strings																
EP-3.2.2.1.1	Cells																
EP-4	Connect Relays					Loss of battery telemetry to controller	Invalid, stale, or missing battery telemetry would require controller switch.	None	N/A	4							
EP-5	Heaters																

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response											Quick Look			Remediation
				Response Level	Desired Local Response	Allocation of Local Response	Time to fix locally	Time to Transmit Signal	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	
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	X	Depends on root cause; likely requires action to hardware beyond EPS (e.g., avionics processor to correct S/A pointing error)
EP-3.2	Solar Array 2																	
EP-3.2.1	Primary Array																	
EP-3.2.1.1	Strings																	
EP-3.2.1.1.1	Cells																	
EP-3.2.2	Secondary Array																	
EP-3.2.2.1	Strings																	
EP-3.2.2.1.1	Cells																	
EP-4	Connect Relays																	
EP-5	Heaters																	

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-3.2.1	Primary Array			
EP-3.2.1.1	Strings			
EP-3.2.1.1.1	Cells			
EP-3.2.2	Secondary Array			
EP-3.2.2.1	Strings			
EP-3.2.2.1.1	Cells			
EP-4	Connect Relays			X
EP-5	Heaters			X

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.

						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)**
ECU-1	ECU																
ECU-1.1	ECU Side A																
ECU-1.1.1	Control and Status Side A																
ECU-1.1.1.a			Hard Failure	Circuitry Failure - FPGA, ASIC, etc…		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 switch).	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 commanded	Autonomy should command switch to redundant ECU side and should set flag indicating ECU Fault/Failure.	no effect	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)	Potentiometer telemetry ; ECU step count telemetry; redundant ECU telemetry	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)			ECU continues to command actuation.	Autonomy recognizes that actuator continues beyond expected value and switches sides of ECU.	no effect	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	1) Observe commands not executed 2) Loss of Status Telemetry (Send Telemetry command not executed)	Potentiometer telemetry ; ECU step count telemetry; redundant ECU telemetry	ECU to REM	?	?

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.

				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 Side**	**Safe Mode**	**Remediation**	**Revisit**
ECU-1	ECU																	
ECU-1.1	ECU Side A																	
ECU-1.1.1	Control and Status Side A																	
ECU-1.1.1.a			Hard 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??? 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	
ECU-1.1.1.b			Inability to execute control commands	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	None	None	None	None				Switch to redundant ECU side (power cycle will clear non-harness fault). Could diagnose a harness problem by switching sides of avionics.	
ECU-1.1.1.c			Inability to send status telemetry	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 (power cycle will clear fault). Next step would be avionics side switch.	X
ECU-1.1.1.d			Hung (repeating a command)	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	None	None	None	None				Switch to redundant ECU side or switch sides of avionics.	X
ECU-1.1.1.e			Hung/Locked up state (not commanding)	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	None	None	None	None				Switch to redundant ECU side (power cycle will clear fault)	X

						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)
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	Autonomy should notice problem (ex. lack of status telemetry) and command switch to redundant ECU side (does not require avionics side switch).	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	?	?
			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 switch).	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	Power Side A																
ECU-1.1.2.a			No Power	Open Circuit		Complete Loss of power to ECU Side	Autonomy should notice no power 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	?	?
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										Quick Look			Remediation	Revisit
				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 Side	Safe Mode		
Inputs			REM generated commands for control and status - cross-strapped (REM A and REM B)	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	
			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-1.1.2	Power Side A																	
ECU-1.1.2.a			No 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	
ECU-1.1.2.b			Incorrect Power Regulation	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	

						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)**
Inputs			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 switch).	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	ECU current / voltage ? ECU Power State ECU Aliveness	ECU to REM PDU to REM	?	?
ECU-1.2	ECU Side B																
ECU-1.2.1	Control and Status Side B																
ECU-1.2.2	Power Side B																

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Remediation	Revisit
				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 Side	Safe Mode		
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 Side B																	
ECU-1.2.1	Control and Status Side B																	
ECU-1.2.2	Power Side B																	

Subject Matter Expert(s): Robin Vaughan

Notes: Much of this is dependent on the exact sensors selected. Selection will probably not occur until 2014. Yellow highlighted blocks are redundant components. Components are listed

						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)
GC-1	Star Trackers																
GC-1.1	Star Tracker A																
GC-1.1.a			**Input command not received or acted on.** (When turned on, trackers 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 these commands, it can fail to reach the normal tracking mode where it would start generating attitude solutions.)	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	All	Tracker does not reach normal operating mode; either degraded attitude solutions are generated or no attitude solutions are generated.	G&C software may accept degraded attitude solutions and generate less accurate spacecraft attitude solutions. G&C software will attempt to propagate attitude from last available tracker solution (or attitude solution saved from previous processor on shut down if processor reset or switch) and continuing gyro rate data. No attitude solution would eventually lead to an umbra violation if G&C is unable to attempt attitude control and never gets some knowledge of actual attitude.	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. Still meet full mission science requirements.	Unlikely that a localized change in attitude large enough to cause an umbra violation would be accepted by the G&C software even if it were generated by the tracker. A slowly drifting attitude solution might be harder to detect and could eventually result in an umbra violation if undetected. Similarly, propagation using only gyro rates could eventually result in an umbra violation since gyro errors will build up over time.	3		Probably	If tracker is able to output telemetry, it should indicate it's current operating mode. 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	
GC-1.1.b			**Input message not received or processed.** (The trackers typically need some information from the avionics/FSW to generate correct attitude solutions. Examples are s/c velocity wrt Sun for aberration corrections, timing pulse to get the equivalent of TDT for star position calculation. A fault on the s/c side 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 degraded.)	1) Faulty connector or harness/wiring inside unit 2) Localized electronics fault that affects message processing logic 3) Error in tracker processor internal software/firmware	All	Tracker uses old or incorrect information to generate attitude solution; solution accuracy is degraded	G&C software may reject the attitude solution if it's inconsistent with recent solutions. G&C software may use the degraded attitude solution and generate less accurate spacecraft 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. Still meet full mission science requirements.	Unlikely that a localized change in attitude large enough to cause an umbra violation would be accepted by the G&C software even if it were generated by the tracker. A slowly drifting attitude solution might be harder to detect and could eventually result in an umbra violation if undetected.	3		Maybe	Some trackers have status telemetry that will indicate if it is receiving the timing pulse 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	
GC-1.1.c			**Failure to output requested telemetry; output messages not generated.** (Tracker does not output any attitude solutions.)	1) Sensor/detector not able to collect measurements a) Permanent damage to detector elements (baffle, optics, APS detector, etc.): - Permanent radiation damage to detector - Surface damage to baffle or design error allows too much stray light into tracker optical path - Glint/reflection from other parts of the s/c gets into tracker optical path as stray light - Cracks, puts, or material deposits (contamination) on lenses make images unusable - Radiation exposure darkens glass so that not enough light gets to detector to detect stars in image b) Temporary environmental/viewing conditions degrading star images (not enough bright stars found in images): - Dust obscuring images - CME or other radiation event temporarily causing too much noise in star images - Plume particles from thruster firing passing through tracker FOV - High or low temperature that can't be compensated by internal cooler (thermal "noise" on detector) 2) Electronics/software not able to process or communicate measurements: a) Hardware fault prevents image bring read out from detector b) Hardware damage or fault in internal electronics boards or harnessing that prevents image c) Hardware damage or fault in internal electronics boards or harnessing or connectors that prevents generation of properly-formatted telemetry d) Error in tracker processor internal software/firmware - problem with image processing that detects star images and/or algorithms that form attitude solution from		Tracker may transition to a mode where it doesn't try to generate attitude solutions if it doesn't succeed 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 propagate s/c attitude using gyro 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 umbra violation.	3		Maybe	Some trackers have status telemetry that will indicate that they can no longer generate attitude solutions. G&C software will be monitoring some of these health & status flags. G&C attitude estimation software will flag a problem if too many consecutive attitude solutions from the same tracker are missing. Telemetry will also be downlinked occasionally as part of ground monitoring of G&C component performance. Most STs provide telemetry 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	
GC-1.1.d			**Output telemetry contains insufficient measurements,** (Tracker does not output the expected number/quantity of attitude solutions or does not generate telemetry 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 star field images a) Damage to detector elements (baffle, optics, APS, detector, etc.) - Temporary radiation damage to detector - Glint/reflection from other parts of the s/c temporarily gets into tracker optical path as stray light (could be dependent on attitude relative to Sun) b) Environmental/viewing conditions degrading star field images (not enough bright stars in images): - Dust obscuring star images - CME or other radiation event temporarily causing too much noise in star images - Plume particles from thruster firing passing through tracker FOV - High or low temperature that can't be compensated by internal cooler (thermal "noise" on detector) 2) Electronics/software not able to process or communicate measurements: a) Hardware fault prevents image bring read out from detector b) Hardware damage or fault in internal electronics boards or harnessing that prevents image c) Hardware damage or fault in internal electronics boards or harnessing or connectors that prevents generation of properly-formatted telemetry d) Error in tracker processor internal software/firmware - problem with image processing that detects star images and/or algorithms that form attitude solution from		Tracker may transition to a mode where it doesn't try to generate attitude solutions if it doesn't succeed 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 propagate s/c attitude using gyro rate data from between valid star tracker attitude solutions	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 umbra violation if 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 telemetry. G&C software will be monitoring some of these health & status flags. G&C attitude estimation software will flag a problem if too many consecutive attitude solutions from the same tracker are missing. 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	
GC-1.1.e			**Output telemetry contains degraded measurements.** (Tracker outputs attitude solutions whose quality is less than expected (not meeting spec).)	1) Sensor/detector sporadically unable to collect star field images a) Damage to detector elements (baffle, optics, APS, detector, etc.) - Temporary radiation damage to detector - Glint/reflection from other parts of the s/c temporarily gets into tracker optical path as stray light (could be dependent on attitude relative to Sun) b) Environmental/viewing conditions degrading star field images (not enough bright stars in images): - Dust obscuring star images - CME or other radiation event temporarily causing too much noise in star images - Plume particles from thruster firing passing through tracker FOV - High or low temperature that can't be compensated by internal cooler (thermal "noise" on detector) 2) Intermittent fault in electronics/software disrupts processing of some star field images or prevents communicaiton of some attitude solutions: a) Hardware fault sporadically prevents image bring read out from detector b) Hardware damage or fault in internal electronics boards or harnessing that sporadically prevents image c) Hardware damage or fault in internal electronics boards or harnessing or connectors that sporadically prevents generation of properly-formatted telemetry d) Error in tracker processor internal software/firmware - sporadic problem with image		Trackers usually output some quality flags along with the attitude solution. Some trackers will transition to a mode where they no longer generate attitude solutions if low-quality solutions persist for some predefined time period.	G&C software will check the quality flags and reject the measurement if it's too poor. Attitude estimates will continue using solutions from the other tracker if available and acceptable; otherwise attitude will be propagated from last valid tracker solution using gyro rate data.	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 umbra violation if time between measurements is very long; less likely in this case since we will likely be getting some valid solutions of acceptable quality from the tracker	3		Maybe	Some trackers have status telemetry. G&C software will be monitoring some of these health & status flags. 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	
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.)	1) Temporary environmental/viewing conditions degrading star images (not enough bright stars found in images): a) Dust obscuring images b) CME or other radiation event temporarily causing too much noise in star images c) Plume particles from thruster firing passing through tracker FOV d) High or low temperature that can't be compensated by internal cooler (thermal "noise" on detector) 2) Error in software or related memory degrades procesing of star field images: a) Star locations or pattern matching is not quite correct b) Time stamp associated with attitude solution from star field image is biased from correct time		None - tracker thinks everything is ok	G&C software will reject a measurement if it's not consistent with recent past history of s/c attitude & rate or if time tag is out of order. 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.	If not corrected (and somehow detected), 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.	Possible, but not likely. The attitude solutions 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 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	
Inputs			Power			ST not powered	Can't meet WISPR pointing requirements during encounter. Switch to other ST if not already active.	No effect.	N/A	3							
			Time code			ST will keep working	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							
			S/c velocity from FSW			ST will keep working, but will report that 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/or command muliplexer to correct setting. Can't meet WISPR pointing requirements during encounter with a single ST.	No effect.	N/A	3							
GC-1.2	Star Tracker B																

Subject Matter Expert(s): Robin Vaughan

Notes: Much of this is dependent on the exact sensors selected. Selection will probably not occur until 2014. Yellow highlighted blocks are redundant components. Components are listed

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response: Response Level	Response: Desired Local Response	Response: Allocation of Local Response	Response: Time to fix locally	Response: Time to Transmit Signal	Response: Desired System Response	Response: Allocation of System Response	Response: Time to fix system	Response: Time to Transmit Signal	Response: Ground Response / Contingency	Quick Response: System Side Switch	Quick Response: Processor Switch	Quick Response: Safe Mode	Remediation	Revisit
GC-1	Star Trackers																	
GC-1.1	Star Tracker A																	
GC-1.1.a			**Input command not received or acted on.** (When turned on, trackers 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 these commands, it can fail to reach the normal tracking mode where it would start generating attitude solutions.)		G&C attitude estimation software will flag a problem if too many consecutive attitude solutions from the same tracker are missing or rejected (fail to pass the sanity checks - mostly consistency checks on the time sequence of 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 outputting flags that are used in the premise of various autonomy rules.								Software reboot, tracker reset, or tracker power cycle may fix some problems with electronics 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 need some information from the avionics/FSW to generate correct attitude solutions. Examples are s/c velocity wrt Sun for aberration corrections, timing pulse to get the equivalent of TDT for star position calculation. A fault on the s/c side 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 degraded.)		G&C attitude estimation software will flag a problem if too many consecutive attitude solutions from the same tracker are rejected (fail to pass the sanity checks - mostly consistency checks on the time sequence of 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 outputting flags that are used in the premise of various autonomy rules.								Inernal reset (no ground or autonomy action required), software reboot, tracker reset, or tracker power cycle may fix some problems with electronics or software. Switching to redundant unit may not alleviate problems if 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 outputting flags that are used in the premise of various autonomy rules.				Might be able to boil off contamination material (anti-ram ST only - some STs have internal coolers that could be turned off to aid in this process), work around parts of the image field that have suspect image content, change attitude relative to stray light source I don't think any of these can be addressed with a fault protection response on the spacecraft. We'd have to get the ground 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 electronics or software. Switching to redundant unit may not alleviate problems if the error lies in common software.	
GC-1.1.d			**Output telemetry contains insufficient measurements,** (Tracker does not output the expected number/quantity of attitude solutions or does not generate telemetry messages at expected rate for read out or full complement of measurements not generated for single data message.)						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 outputting flags that are used in the premise of various autonomy rules.				Might be able to boil off contamination material (anti-ram ST only - some STs have internal coolers that could be turned off to aid in this process), work around parts of the image field that have suspect image content, change attitude relative to stray light source I don't think any of these can be addressed with a fault protection response on the spacecraft. We'd have to get the ground 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 electronics or software. Switching to redundant unit may not alleviate problems if the error lies in common software.	
GC-1.1.e			**Output telemetry contains degraded measurements.** (Tracker outputs attitude solutions whose quality is less than expected (not meeting spec).)						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 outputting flags that are used in the premise of various autonomy rules.								Software reboot, tracker reset, or tracker power cycle may fix some problems with electronics or software. Switching to redundant unit may not alleviate problems if the error lies in common 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 outputting flags that are used in the premise of various autonomy rules.								Software reboot, tracker reset, or tracker power cycle may fix some problems with electronics or software. Switching to redundant unit may not 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																	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: Time to Detect (System)
GC-2	Solar Limb Sensors	In the current design, there is one electronics box which is internally redundant - has two separate interfaces to the sensor heads and to the spacecraft (two identical, separate cards, similar to an internally-redundant IMU/SSIRU). There are 4 sensor heads, each is redundant in that there are physically two separate sets of solar cells that can sense the Sun on each head. They are connected to a different side of the electronics. There is a single connector for both cells on a sensor head, and a single pane of glass over the two cells (two common-cause failures for a sensor head). The entries in this sheet are restricted to solar distances where the nominal attitude is to have +Z(TPS) aligned with the Sun.			At default attitude when <0.82 AU from Sun				Note on umbra violation for SLS: When any of the SLS heads see the Sun, then the spacecraft attitude has already drifted enough off the nominal attitude that the umbra for the SLS placement has been violated. This column is interpreted to mean that the s/c packaging umbra is or can be violated. The SLS heads will see the Sun before the s/c packaging umbra is violated. Just having an SLS head see the Sun does not constitute an umbra violation (but it does mean we are closer to a violation than we should be).								
GC-2.1	Solar Limb Sensor A																
GC-2.1.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) Faulty connector or harness/wiring inside unit 2) Localized electronics fault that affects message processing logic 3) Error in solar limb sensor internal firmware (FPGA)		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	Control correction will be wrong because offset angle is wrong. Will not meet WISPR pointing requirements when controlling based on SLS data. S/C may think it's seeing the Sun earlier than it actually is, or may "see" it too late.	Loss of mission if umbra violation occurs while trying to correct attitude using degraded offset angles from 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 we'd never get a second occurence where we would test if we had made the right correction.)	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.	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 +Z/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-2.1.b			**Case 1: Failure to output requested telemetry; output messages not 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 so that it should be outputting Sun presence flags and offset angle values).)	Sensor/detector not able to collect measurements; damage to detector elements (shield, cover glass, solar cells, etc.) - Permanent radiation damage to detector element - Failure in detector solar cells (no output current) - Cracks, pits, or material deposits (contamination) on cover glass blocks or alters path of Sun light reaching detector cells - Alignment shifts during flight so some part of the spacecraft blocks the FOV of the head or shield/housing of head moves relative to the FOV so Sun light doesn't get to the cells - Radiation exposure darkens glass so that not enough light gets to detector solar cells - Broken connection in wiring of solar cells		none - SLS is trying to communicate and isn'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 ok). The other side of the head would detect the Sun and alert G&C software 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 redundant heads/electronics	No if data still available from other side of detector head or electronics. Yes if fault is common to both electronics or both sides of a single sensor head	2R	None	Probably 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 isn't assuming that head is seeing the Sun	SLS output	SLS to CDH	?	None
GC-2.1.c			**Case 2: Failure to output requested telemetry; output messages not generated.** (One side of SLS electronics does not output any Sun presence or offset angle data (presumes that we get to an attitude where one or more heads would see the Sun so that it should be outputting Sun presence flags and offset angle values).)	Electronics not able to process or communicate measurements - Hardware fault prevents data being read out from detector head, e.g., harness leading back to the electronics is damaged or broken. - 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 that prevents generation of properly formatted data messages. - Error in solar limb sensor processor internal firmware - problem with data processing that generates Sun presence flags and offset angle.		none - SLS is trying to communicate and isn'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 ok). The other side of the head would detect the Sun and alert G&C software 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 redundant heads/electronics	No if data still available from other side of detector head or electronics. Yes if fault is common to both electronics or both sides of a single sensor head	2R	None	Maybe	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 output	SLS to CDH	?	None
GC-2.1.d			**Case 1: Output telemetry contains incorrect measurements which 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 1 False Sun detection - Indicating Sun presence when head is not seeing the Sun.)	1) Environmental/viewing conditions cause false Sun detection a) Glint reflected off other spacecraft components illuminates the detector head enough to cause it to think it sees the Sun b) Some other bright body (e.g., Earth) wanders through the FOV of the detector head (probably very very unlikely that any other light source would be strong enough to be mistaken for the Sun) 2) Error in hardware corrupts processing of detector cell readings a) Failure of some component in processing chain causes signals to appear to be over thresholds for Sun presence b) Short or other electrical problem in the solar cells causes high current readings or otherwise makes it appear that the cell is seeing the Sun 3) Error in firmware in electronics (FPGA logic) - logic error generates incorrect output for Sun presence flag or angle value - possibly incorrect thresholds here as well		None - solar limb sensor thinks everything is ok	Depends how we program the G&C software when looking at SLS data. If we decide to respond to any single detection by one of side of the SLS heads, then we may take control action when it isn't necessary. If we are always getting information from both sides of each head, we may be able to detect that just one side thinks it's seeing the Sun and the other side doesn't. But then it's not clear which side we should believe.	If false detection is not rejected, G&C system could try to change the attitude when it's at the correct attitude and end up moving the spacecraft off Sun, maybe enough to cause an actual umbra violation	Possible if responding to an isolated false detection.	2R	Active	Maybe	G&C software may be able to isolate the false reading if data available from both sides of the head (and fault is not common to both sides). May be difficult to determine which side is sending the "wrong" data.	Error flag?	G&C to CDH to Autonomy	?	None
GC-2.1.e			**Case 2: Output telemetry contains incorrect measurements which 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 2 Grossly incorrect Sun offset angle data - not tracking true Sun-relative geometry.)	1) Environmental/viewing conditions cause false Sun detection - misalignment between detector head and TPS edge. 2) Error in hardware corrupts processing of detector cell readings - failure of some component in processing chain causes signals to be combined incorrectly when computing Sun offset angle. 3) Error in firmware in electronics (FPGA logic) - logic error generates incorrect output for Sun presence flag or angle value - possibly incorrect thresholds here as well.		None - solar limb sensor thinks everything is ok	Depends how we program the G&C software when looking at SLS data. If we decide to respond to any single detection by one of side of the SLS heads, then we may take control action when it isn't necessary. If we are always getting information from both sides of each head, we may be able to detect a gross difference between what the two sides are outputting. But then it's not clear which side we should believe.	If false detection is not rejected, G&C system could try to change the attitude when it's at the correct attitude or make the wrong change to an off-Sun attitude. Either way we end up moving the spacecraft off Sun, maybe enough to cause an actual umbra violation	Possible if responding to isolated false readings.	2R	Active	Maybe	G&C software may be able to isolate the false reading if data available from both sides of the head (and fault is not common to both sides). Seriously bad readings - like being 40 deg off Sun near periapse - can probably be rejected since the s/c 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	?	None
GC-2.1.f			**Case 3: Output telemetry contains incorrect measurements which 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 come too late relative to the true Sun-relative geometry.)	1) Error in hardware between heads and electronics - signals not received or collected at the correct rate or not collected at regular intervals. 2) Error in electronics interface with s/c a) Mismatch in timing between output of messages by SLS and readout of interface by s/c avionics b) Internal delay in outputting data grows larger due to parts failure		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 software. G&C can't take action to correct attitude until SLS data indicate a violation. If we are always getting information from both sides of each head, and the delay only affects one side then we can use the readings from the other side.	Loss of mission if G&C is unable to respond soon enough.	Possible if failure is common to both sides of head or electronics. If delay is too long between SLS head first seeing the Sun and reporting it to G&C, s/c may have drifted even more off Sun during the delay - maybe to the umbra boundary. Or G&C may pause in taking action if there are long time gaps in the SLS data. If delay is isolated to one side, the differences in readings between the two sides would have to be dealt with somehow so the control is not confused about how much correction is needed.	2R	Active	Maybe	G&C software may be able to deal with differences between sides and use data from the "earliest" side to correct attitude.	Error flag?	G&C to CDH to Autonomy	?	None
Inputs			Power			No effect if power is only lost to one side of electronics,	No effect.	No effect.	N/A	4							
GC-2.2	Solar Limb Sensor B																

				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 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**	**Remediation**	**Revisit**
GC-2	Solar Limb Sensors	In the current design, there is one electronics box which is internally redundant - has two separate interfaces to the sensor heads and to the spacecraft (two identical, separate cards, similar to an internally-redundant IMU/SSIRU). There are 4 sensor heads, each is redundant in that there are physically two separate sets of solar cells that can sense the Sun on each head. They are connected to a different side of the electronics. There is a single connector for both cells on a sensor head, and a single pane of glass over the two cells (two common-cause failures for a sensor head). The entries in this sheet are restricted to solar distances where the nominal attitude is to have +Z(TPS) aligned with the Sun.																
GC-2.1	Solar Limb Sensor A																	
GC-2.1.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 parameters 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-2.1.b			**Case 1: Failure to output requested telemetry; output messages not 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 so that it 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 hardware - redundant sections of single electronics unit and redundant sections of detector heads. (Assuming the failure is not common to both sides of a head or the electronics). If common to both sides of a head, we've lost data from one of the 4 heads. Depending on where the Sun is actually drifting off from +Z, we may not detect the drift and get to an umbra violation. Any contamination or alignment shifts will likely affect both sides of a single head. It's hard to think of optical failures that would only affect a single side of a head (but not impossible) Might be able to boil off contamination material - assuming we ever realized it was there in the first place.	
GC-2.1.c			**Case 2: Failure to output requested telemetry; output messages not generated.** (One side of SLS electronics does not output any Sun presence or offset angle data (presumes that we get to an attitude where one or more heads would see the Sun so that it 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 electronics. 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 firmware.	
GC-2.1.d			**Case 1: Output telemetry contains incorrect measurements which 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 1 False Sun detection - Indicating Sun presence when head is not seeing the Sun.)	Local	?	Autonomy	?	?	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 our last defense against attitude drifting off Sun. Use of redundant sensor or electronics may not solve problems due to common or similar equipment. SLS rest or poewr cycle may clear an electronics or SW/FW fault, but may not. Also, it's not clear if it's a good idea to power cycle the SLS while in view of the Sun.	
GC-2.1.e			**Case 2: Output telemetry contains incorrect measurements which 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 2 Grossly incorrect Sun offset angle data - not tracking true Sun-relative geometry.)	Local	?	Autonomy	?	?	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 getting really bad angle values 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 HW fault.	
GC-2.1.f			**Case 3: Output telemetry contains incorrect measurements which 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 come too late relative to the true Sun-relative geometry.)	Local	?	Autonomy	?	?	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 getting long time delays or erratic behavior on the data interface,	
Inputs			Power															X
GC-2.2	Solar Limb Sensor B																	

						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)
GC-3	Inertial Measurement Unit	The IMU Accelerometers are only used for TCMs in closed-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 IMU gyros) with the exception of the lesser criticality of the accelerometers.	Note that the current design has redundancy in both the number of individual gyros and in the electronics/power supplies. Minimum requirement for controllability is 3 gyros covering 3 orthogonal directions. Either we will have one unit with 4 gyros and 2 electronics/power supplies (more likely) or 2 units that each have 3 gyros and 1 electronics/power supply (less likely). In the latter case, we would have to run with both units on (an probably mount them in different orientations) to ensure we'd have 3 good gyros at all times.														
GC-3.1	IMU Side A																
GC-3.1.a			**Input command not received or acted on** (When turned on, some IMUs need to be sent a series of commands that configure them to the correct operational mode. If the IMU is unable to correctly process these commands, it can fail to reach the normal operating mode where it would start outputting gyro rate data.)	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 IMU processor internal software/firmware	All	IMU does not reach normal operating mode; either limited gyro data are generated or no gyro data are generated.	If some gyro data are available, G&C software may generate less accurate spacecraft attitude & rate solutions. If no gyro data is available, G&C software may be unable to generate attitude/rate solutions and possibly unable to control the spacecraft. G&C software will try to use rate info from star tracker measurements if gyro data are available.	If not corrected, the IMU could be deemed unusable for the rest of the mission. This would be a loss of mission if redundant IMU/gyros are not available. G&C cannot control the spacecraft without good rate data.	No attitude solution would eventually lead to an umbra violation if G&C is unable to attempt attitude control and never gets some knowledge of actual attitude. A slowly drifting attitude solution might be harder to detect and could eventually result in an umbra violation if undetected. Similarly, propagation using star tracker rates could eventually result in an umbra violation since the data are noisier than gyro rates.	2R	Active	Probably	If IMU is able to output telemetry, it should indicate its current operating mode. 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.	IMU Operating Mode G&C IMU error flag	CDH to Autonomy	?	None
GC-3.1.b			**Input message not received or processed** (The IMU typically needs some timing information from the avionics/FSW to generate correct time tags on the gyro rate data solutions. A fault on the s/c side or inside the IMU that causes this information to not be available will cause problems for the IMU in that the rate measurements coming out will be misleading or dropped due to the incorrect time tags.)	1) Faulty connector or harness/wiring inside unit 2) Localized electronics fault that affects message processing logic 3) Error in IMU processor internal software/firmware	All	IMU uses internal timing mechanisms to time tag data; time tag accuracy may be degraded; synch with s/c avionics for data read out may be corrupted	G&C software may reject the gyro measurements if their time tags are inconsistent with the recent sequence. G&C software may use the gyro rates with incorrect time tags and generate less accurate spacecraft attitude/rate solutions.	If not corrected, the gyro data could be deemed unusable for the rest of the mission. If no other source of spacecraft rate data is available, this would be loss of mission because G&C cannot maintain attitude control without good rate data.	Unlikely that a localized change in gyro rates large 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 detect and could eventually result in an umbra violation if undetected.	2R	Active	Maybe	Most IMUs have status telemetry that will indicate if it is receiving the timing pulse 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.	IMU health and status flags	IMU to GNC/CDH to Autonomy	?	None
GC-3.1.c			**Failure to output requested telemtry; output messages not generated** (IMU does not output any gyro rate measurements)	1) Sensor/detector not able to collect measurements a) Damage to detector elements internal to the gyros (damage mechanisms are specific to the tupe of gyro selected (FOG, RLG, HRG, MEMS); examples for HRG are particle trapped inside or misalighnment of resonator pieces causes friction or disturbs the normal resonance) b) Environmental conditions degrading gyro measurements (sensitivity to different environmental factors depends on the type of gyro that we select (FOG, RLG, HRG, MEMS); temperature, radiation, sources of vibration close to the IMU are typical factors that can affect gyro measurement accuracy) 2) Electronics/software not able to process or communicate measurements a) Hardware fault prevents data being reead out from gyro b) Hardware damage or fault in internal electronics boards or harnessing that prevents gyro data processing c) Hardware damage or fault in internal electronics boards or harnessing or connectors that prevents generation of properly-formatted telemetry messages d) Error in IMU processor internal software/firmware - problem with algorithms that read gyro data and formulate telemetry messages		Gyros may transition 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 tracker measurements or attempt to propagate s/c attitude through continuing star tracker attitude solutions. Rate knowledge 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 accuracy requirements without gyro rate data. May be loss of mission.	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 IMUs have status telemetry that will indicate that they can no longer generate gyro data. G&C software will be monitoring some of these health & status flags. G&C attitude estimation software will flag a problem if too many consecutive measurements from the same IMU are missing. 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	None
GC-3.1.d			**Output telemetry contains insufficient measurements** (IMU does not output the expected number/quantity of gyro rate measurements or does not generate telemetry 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 a) Damage to gyros (damage mechanisms are specific to the tupe of gyro selected (FOG, RLG, HRG, MEMS); examples for HRG are particle trapped inside or misalighnment of resonator pieces causes friction or disturbs the normal resonance) b) Environmental/viewing conditions degrading gyro measurements (sensitivity to different environmental factors depends on the type of gyro that we select (FOG, RLG, HRG, MEMS); temperature, radiation, sources of vibration close to the IMU are typical factors that can affect gyro measurement accuracy) 2) Intermittent fault in electronics/software disrupts processing of some gyro measurements or prevents communication of some gyro measurements a) Hardware fault sporadically prevents data being reead out from gyro b) Hardware damage or fault in internal electronics boards or harnessing that sporadically prevents gyro data processing c) Hardware damage or fault in internal electronics boards or harnessing or connectors that sporadically prevents generation of properly-formatted telemetry messages d) Error in IMU processor internal software/firmware - sporadic problem with algorithms that pick off gyro data and package it in telemetry messages		Gyros may transition 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 are 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. Rate knowledge 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 accuracy requirements without gyro rate data. May be loss of mission.	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 IMU have status telemetry that will indicate that they can no longer generate gyro data. G&C software will be monitoring some of these health & status flags. G&C attitude estimation software will flag a problem if too many consecutive measurements from the same IMU are missing. 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	None
GC-3.1.e			**Output telemetry contains degraded measurements** (IMU outputs gyro rate data whose quality is less than expected or not meeting spec)	1) Environmental conditions degrading gyro data a) CME or other radiation event temporarily causing too much noise in rate data b) Local source of IMU stimulation (e.g. vibration) causing "noise" in rate data c) High or low temperature that can't be compensated by internal temperature control mechanisms 2) Error in software or related memory degrades processing of gyro rate measurements a) Gyro read out or data processing algorithms are incorrect b) Time stamp associated with gyro rate data is biased 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, bu they will not be as accurate. Rate knowledge 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 accuracy requirements without gyro rate data. May be loss of mission.	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 IMU have status telemetry that will indicate that they can no longer generate gyro data. G&C software will be monitoring some of these health & status flags. G&C attitude estimation software will flag a problem if too many consecutive measurements from the same IMU are missing. 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	None
GC-3.1.f			**Output telemetry contains incorrect measurements which are flagged valid** (IMU outputs gyro rate data whose time or rate is wrong but without indicating any problems with the data inits own quality flags)	1) Environmental/viewing conditions degrading gyro rate data a) CME or other radiation event temporarily causing too much noise in rate data b) Local source of IMU stimulation (e.g. vibration) causing "noise" in rate data c) High or low temperature that can't be compensated by internal temperature control mechanisms 2) Error in software or related memory corrupts processing of gyro rate measurements a) Error in formulas that package raw gyro readout info rate message telemetry b) Error in algorithm that generates time stamps for gyro rate data 3) Error in hardware chain for gyro 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	G&C software will reject a measurement if it's not consistent with recent past history of s/c attitude & rate or if time tag is out of order. 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.	If sufficiently accurate 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 accuracy requirements without gyro rate data. May be loss of mission.	Possible, but not likely. The 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 pointing.	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	None
Inputs			Power			IMU shuts down	Switch sides of IMU	No effect.	N/A	2R							
			Relay commands			IMU remains in current configuration	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. Rate knowledge 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 accuracy requirements without gyro rate data. May be loss of mission.	Propagated attitude with missing or degraded rate data will slowly drift from true attitude and could eventually result in an umbra violation.	2R							
GC-3.2	IMU Side B																
GC-4	Reaction Wheels																
GC-4.1	Rx Wh 1																

				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 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	Remediation	Revisit
GC-3	Inertial Measurement Unit	The IMU Accelerometers are only used for TCMs in closed-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 IMU gyros) with the exception of the lesser criticality of the accelerometers.	Note that the current design has redundancy in both the number of individual gyros and in the electronics/power supplies. Minimum requirement for controllability is 3 gyros covering 3 orthogonal directions. Either we will have one unit with 4 gyros and 2 electronics/power supplies (more likely) or 2 units that each have 3 gyros and 1 electronics/power supply (less likely). In the latter case, we would have to run with both units on (an probably mount them in different orientations) to ensure we'd have 3 good gyros at all times.															
GC-3.1	IMU Side A																	
GC-3.1.a			**Input command not received or acted on** (When turned on, some IMUs need to be sent a series of commands that configure them to the correct operational mode. If the IMU is unable to correctly process these commands, it can fail to reach the normal operating mode where it would start outputting gyro rate data.)	Local	IMU switch	Autonomy	?	?	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 electronics problem. Switching to the redundant IMU may not fix a problem that lies in common electronics or software. No remediation is necessary if >=3 gyros continue to operate normally. If < 3 gyros are providing data, then the full attitude state is not observable and G&C software would have to supplement the gyro data with another source of rate data (ie star tracker measurements) if available. In other words, we are tolerant to loss of some gyros, but we can get down to the single-point failure state if we lose too many gyros.	
GC-3.1.b			**Input message not received or processed** (The IMU typically needs some timing information from the avionics/FSW to generate correct time tags on the gyro rate data solutions. A fault on the s/c side or inside the IMU that causes this information to not be available will cause problems for the IMU in that the rate measurements coming out will be misleading or dropped due to the incorrect time tags.)	Local	IMU switch	Autonomy	?	?	None	None	None	None	None				Use star tracker rate data if redundant gyro hardware is not available. If the error in the time tags for the IMU data could be characterized on the ground, the G&C FSW could be modified to correct the time tags on-board. If the star tracker kept working, we should have time to detect and 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 issue. Any faults due to common components or software would not be corrected with an IMU switch.	
GC-3.1.c			**Failure to output requested telemtry; output messages not generated** (IMU does not output any gyro rate measurements)	Local	IMU switch If G&C software flags a problem either from the health & status telemetry or with the gyro measurements, it will request action from fault protection. Usually this is by outputting flags that are used in the premise of various autonomy rules.	Autonomy	?	?	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 electronics problem. Switching to the redundant IMU may not fix a problem that lies in common electronics or software.	
GC-3.1.d			**Output telemetry contains insufficient measurements** (IMU does not output the expected number/quantity of gyro rate measurements or does not generate telemetry messages at expected rate for read out or full complement of measurements not generated for single data message)	Local	IMU switch If G&C software flags a problem either from the health & status telemetry or with the gyro measurements, it will request action from fault protection. Usually this is by outputting flags that are used in the premise of various autonomy rules.	Autonomy	?	?	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 electronics problem. Switching to the redundant IMU 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	IMU switch If G&C software flags a problem either from the health & status telemetry or with the gyro measurements, it will request action from fault protection. Usually this is by outputting flags that are used in the premise of various autonomy rules.	Autonomy	?	?	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 electronics problem. Switching to the redundant IMU may not fix a problem that lies in common electronics or software.	
GC-3.1.f			**Output telemetry contains incorrect measurements which are flagged valid** (IMU outputs gyro rate data whose time or rate is wrong but without indicating any problems with the data inits own quality flags)	Local	IMU switch If G&C software flags a problem either from the health & status telemetry or with the gyro rates, it will request action from fault protection. Usually this is by outputting flags that are used in the premise of various autonomy rules.	Autonomy	?	?	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 electronics problem. Switching to the redundant IMU may not fix a problem that lies in common electronics or software.	
Inputs			Power															X
			Relay commands															X
			Data (commands from the SCIF)															X
GC-3.2	IMU Side B																	
GC-4	Reaction Wheels																	
GC-4.1	Rx Wh 1																	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: Time to Detect (System)
GC-4.1.a			**Unable to exert force/torque on spacecraft** (flywheel is not being acted on to maintain or change its spin; flywheel naturally spins down due to losses in the system (friction); flywheel is unable to rotate)	1) Wheel not responding to commands at all - mechanical failure a) Large increase in internal friction so that motor cannot overcome friction forces and move the flywheel (loss of lubricant, serious degradation of lubricant or bearings) b) Imbalance/misalignment in flywheel relative to motor or housing causes it to get stuck (unable to rotate) c) Particles break off inside housing and eventually get stuck in the wrong place so flywheel can't move 2) Wheel not responding to commands at all - electrical failure a) Electric motor fails - can't control electric and magnetic fields to move flywheel b) No power reaching wheel c) Internal break in wiring for power or in lines between electronics and motor 3) Wheel not responding to commands at all - communication failure - electronic interface that receives torque commands is broken (internal harness fault, board fault, etc.)	All except launch (of less concern when thrusters are being used for attitude control, but still will have some effect since we continue to command the wheels during TCMs and momentum dumps)	1) Flywheel effectively stopped. 2) Flywheel will naturally spin down if not actively controlled by motor; should reach a low or zero speed equilibrium but could be kicked up again by external forces (i.e., thruster firing). If motor has failed wheel will consume less or no power. 3) Flywheel will naturally spin down if not actively controlled by motor; should reach a low or zero speed equilibrium but could be kicked up again by external forces (i.e., thruster firing).	Controller will continue to command all 4 wheels but resulting torque will be in error because one of the wheels is not responding as expected. Most likely the other 3 wheels will be able to 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. G&C SW will stop using affected wheel in control loop, but will eventually also flag autonomy to power down wheel.	If wheel cannot be used again, control is still possible with the remaining 3 wheels, but momentum dumps will be more frequent (use more fuel) since less momentum storage capacity with 3 wheels. Might shorten the mission if we use too much more fuel for momentum dumps.	Unlikely since the other 3 wheels should maintain attitude, although they may be running at higher speeds/momentum.	2R		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.b			**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.		The "stuck" or "run away" wheel will eventually reach saturation (max speed) with how long that takes depending on the speed magnitude when command first froze.	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 correctable in the time available depending on how we design the auto dump logic and fault checks for wheels	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			**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 violation it may not be correctable in the time available depending on how we design the auto dump logic and fault checks for wheels	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 torque that fights against the desired control. Won't necessarily reach saturation (max speed) since direction sign can still change with time.	The controller will mistakenly keep sending commands to all the wheels. The other wheels 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 when this occurs. There should be time for G&C software to detect wheel is not responding and request action from autonomy.	Loss of mission in the worst 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 logic and fault checks for wheels	Probably not in this case.	2							
GC-4.1.e			**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.		Wheel will spin in correct direction from 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 against it.	Might be survivable if low magnitude - wheel will 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 performed before 2 wheels saturate, we lose controllability	Loss of mission in the worst 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 logic and fault checks for wheels	Possible, but less likely if torque magnitude is lower.	2							
GC-4.1.f			**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.		a) If wheel is sluggish, it puts out less torque than commanded and may 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 random disturbance torque on the system. Sometimes it may contribute to what the controller wants done, but not reliably so. Wheel may consume more power depending on how the erractic behavior manifests itself.	a) Turns will take longer to complete, may deviate more 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 guessing at the nature of the erratic behavior. But if it's intermittent even at max torque, the other 3 wheels should be able to counter it.	Loss of mission in the worst 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 logic and fault checks for wheels	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 fault logic (to turn off misbehaving wheel) b) 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) c) Unlikely in this case	2							
GC-4.1.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) Wheel responding slightly out-of-spec a) More friction than expected b) Imbalance causing irregular rotation of flywheel c) 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/torque; might consume more power in trying to get to commanded state	1) Other 3 wheels will make up the slack; turns may take slightly longer. 2) May not meet jitter requirements if wheel disturbance is out of spec; probably can continue to meet pointing accuracy requirements if the other 3 wheels are still performing in spec.	Science measurements possibly degraded (WISPR) if jitter requirements are violated. If offending wheel is disabled, will need momentum dumps more often, using more fuel	Probably not	2R		Possibly - but by ground analysis, not on-board fault protection	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				

				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 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**	**Remediation**	**Revisit**
GC-4.1.a			**Unable to exert force/torque on spacecraft** (flywheel is not being acted on to maintain or change its spin; flywheel naturally spins down due to losses in the system (friction); flywheel is unable to rotate)										Ground might attempt a power switch.				First action would be to switch sides (REM) for commanding of the wheels (or just this wheel if we can do it on a per wheel basis) - assuming the failure is in the communication chain and 3 other wheels are responding. I don't think the wheel itself will have internally redundant command interfaces that could be switched. If the wheel is still not responding after side 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. For this case, we are assuming that the failed wheel either isn't rotating at all or only rotates at very low rate, mostly constrained by friction in the system. Non-redundant controller input from multiplexer to wheel. Order of remediation probably depends on wheel selected (depends on available telemetry)	
GC-4.1.b			**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 wheel 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). A side 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 switched . If the wheel is still not responding after side 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	
GC-4.1.c			**Case 2: Incorrect force/torque exerted on spacecraft**															
GC-4.1.d			**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			**Case 4: Incorrect force/torque exerted on spacecraft**															
GC-4.1.f			**Case 5: Incorrect force/torque exerted on spacecraft**															
GC-4.1.g			**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.	

						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)**
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 relay speed data. Calculation of wheel speed can be done in wheel itself or in flight software using counts or similar data output by wheel tachometer. 2) Loss of feedback of torque or other health & status telemetry - may only be loss of monitor data, these data are not directly used in the control loop; failure in wheel electronics - can't read data from internal source, can't correctly generate telemetry message, etc.		None - wheel continues to respond to commands, it just doesn't talk back	1) 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 valid speed estimates and we have valid angular rate estimate, we should be ok. 2) G&C software loses ability to detect some problems with the wheel.	1) No effect. 2) G&C will have less data for long-term trending of wheel performance.	1) Unlikely 2) No	4		Yes	1) No wheel speed messages for some long period of time. 2) No wheel telemetry messages received for some long period of time.				
GC-4.1.i			**Output telemetry contains insufficient measurements**	1) Temporary loss of tachometer counts or wheel speed data - intermitten skips or repeats, short periods of no data 2) Skips and gaps in feedback of torque or other health & status telemetry - may only be loss of monitor data, these data are not directly used in the control loop		None - wheel continues to respond to commands, it just doesn't talk back every time it's expected to.	1) Incorrect estimate of wheel and system momentum if can't include a wheel speed in 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 slower than it actually is. 2) G&C has gaps in ability to detect some problems with the wheel.	1) 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). 2) G&C will have less data for long-term trending of wheel performance.	1) Unlikely - if too much time lapses between momentum dumps, the SLSes will see the Sun prior to umbra violation and safe the s/c. 2) No	4		Probably - depends on how the data loss manifests itself	G&C 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 doesn't talk back every time it's expected to.	Incorrect estimate of wheel and system momentum. Might initiate a dump when not needed or wait too long to initiate a dump if wheel appears to be rotating much faster or slower than it actually is	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).	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							
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 - G&C SW should flag it and tell FSW.				
			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-4.2	Rx Wh 2																
GC-4.3	Rx Wh 3																
GC-4.4	Rx Wh 4																

				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 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**	**Remediation**	**Revisit**
GC-4.1.h			**Failure to output requested telemetry; output messages not generated**														Switch to other side for wheel telemetry interface to see if telemetry 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 switch for on-board autonomy. Might try a flight software change to propagate wheel speed from last valid estimate and torque commands. Might try turning off wheel, depending on lost telemetry.	
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 wheel could clear an electronics problem. May not help if the problem is internal to the wheel. Would not recommend anything other than side switch for on-board autonomy. If error persists, might take wheel off-line.	
GC-4.1.j			**Output telemetry contains incorrect measurements which are flagged valid**														Power cycling the wheel could clear an electronics problem. May not help if the problem is internal to the wheel. Might try a flight software change to propagate wheel speed using torque commands - ignore erroneous telemetry. Or might be possible to correct telemetry if we can back out correct wheel speeds from ground analysis of telemetry 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-4.2	Rx Wh 2																	
GC-4.3	Rx Wh 3																	
GC-4.4	Rx Wh 4																	

Subject Matter Expert(s): Jack Ercol, HSSSS contact

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

						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)**
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 N2 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	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.	Redundant pump failures due to cavitation common cause would lead to loss TCS and mission.	N/A	2			1) Pump delta-p sensor and/or current and temp sensors detect cavitation; 2) 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. Holds TBD in3 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/or current and temp sensors detect cavitation; 3) P2 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 in3 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 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.	N/A	2			1) Tank pressure sensor detects loss of pressurization; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop 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 N2 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	1) Jammed bellows (interference of moving parts); 2) 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.	N/A	2			1) Tank pressure and temperature sensors may detect pressure fluctuations due to temperature excursions; 2) Pump delta-p sensor and/or 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	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 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 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			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 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	All	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			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 coolant 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	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 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-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	Valve is open, as commanded	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			1) Accumulator pressure sensor sees drop in accumulator pressure 2) Temperature telemetry will 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 commanded.	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 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	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.	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.				

Subject Matter Expert(s): Jack Ercol, HSSSS contact

Notes: Initially filled out by Jack Ercol, but basically redone by HSSSS. Clay is talking to 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 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**	**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 N2 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 N2 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 N2 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 N2 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	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-LV1-3	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 launch 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 / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: Time to Detect (System)
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			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-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)	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.	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-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	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 sensor detects loss of flow; 2) Loop temp sensors detect loss of cooling 3) Position indicator on LV 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.	Valve closes when not commanded to close	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			1) Pump delta-p sensor detects loss of flow; 2) Loop temp sensors detect loss of cooling 3) 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.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant; 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-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	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			1) Accumulator pressure sensor sees drop in accumulator pressure 2) Temperature telemetry will show that system is operating				
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	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 initial cooling system activation, will see that the temperatures surrounding Radiators 2 & 3 do not change. Will eventually assuming a PI sensor failure.	No effect.	N/A	4			Accumulator pressure sensor does not detect drop in accumulator pressure.				
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	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 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.	External leakage, downstream 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 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-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 can no longer keep up.	N/A	2			1) Pump delta-p sensor detects flow degradation; 2) Loop temperature sensors detect degraded cooling performance				
TCS-CV1-2	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.	Loss of pump redundancy. If next failure is PM1, then loss of TCS and vehicle.	N/A	2R			1) Pump delta-p sensor detects loss of flow while PM2 is running; 2) PM2 current and speed sensors detect dead head condition; 3) Loop temperature sensors detect loss of cooling while PM2 is active				
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 sensor detects loss of flow while PM1 is running; 2) PM1 current and speed sensors detect dead head condition; 3) Loop temperature sensors detect loss of cooling while PM1 is active				

				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 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	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	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: 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.	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-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	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.	N/A	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-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	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.	N/A	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	1) 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.	N/A	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 performance				
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-PM1-6	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 draw 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.	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-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.	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-PM2-1	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.	N/A	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.	N/A	2R			1) Pump delta-p sensor detects flow degradation; 2) Loop temperature sensors detect degraded cooling performance				
TCS-PM2-3	Pump 2	Provides coolant flow through the solar arrays and radiators	Locked rotor	1) 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.	N/A	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 performance				
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				

				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 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	Remediation	Revisit
TCS-CV1-4	Pump check valve	Check valve prevents back flow through the inactive pump 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								X
TCS-PM1-5	Pump 1	Provides coolant flow through the solar arrays and radiators	Overcurrent	Seconds					N/A	None								X
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 radiators	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								X
TCS-PM2-5	Pump 2	Provides coolant flow through the solar arrays and radiators	Overcurrent	Seconds					N/A	None								X

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: 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 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 draw from inactive pump; 3) Loop 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 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.	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	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-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) Electrical/ Electronics failure	All	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 cavitation; 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	All	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	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			1) Tank pressure and temperature sensors detect loss of coolant; 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				

				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 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	Remediation	Revisit
TCS-PM2-6	Pump 2	Provides coolant flow through the solar arrays and radiators	Fails on	Seconds					N/A	None								
TCS-PM2-7	Pump 2	Provides coolant flow through the solar arrays and radiators	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	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	Seconds/minutes					N/A	None								

Subject Matter Expert(s): Dave Copeland (Telecomm)
Chris Haskins (FR)

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

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
TM-1	Transponder																
TM-1.1	FR A																
TM-1.1.1	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.	S/C would attempt to cycle power. S/C might switch to RF side B. 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. PDU would detect overcurrent condition.	PDU tlm 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 ground.	Heartbeat from FR	?	N/A	?
TM-1.1.1.c			Out of regulation secondary voltage	1) Overcurrent 2) Circuit-level failure anywhere in radio		Ranges from negligible to hard failure of radio.	worst case: switch to RF side B (would lose heart beat)	No effect.	N/A	2R	None	Yes, with human-in-the-loop	Analyze downlink telemetry (long-term trending)	Trending by RF 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 check run state to see if FSW, etc. is responding (command loss timer, etc.)				
TM-1.1.2.1.b			Corrupt data (both to and from 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.	S/C wouldn't receive uplink data stream, request for downlink data, configuration data, status data. Could clog up SpaceWire at s/c level. Switch to side B either in avionics or radio. Could also switch off radio.	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		UART (output)															
TM-1.1.2.2.a			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 during 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 during 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)															
TM-1.1.2.3.a			No/out-of-tolerance output	Hardware failure (broken harness, pin, or circuit 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-1.1.2.3.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															
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 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		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			Corrupt data	FPGA, logic or clock failure		Ground use only	No effect.	No effect.	N/A	4	None	N/A					
TM-1.1.3	X-Band Rx (function - includes at least two cards)																

Subject Matter Expert(s): Dave Copeland (Telecomm) Chris Haskins (FR)

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

				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	Remediation	Revisit
TM-1	Transponder																	
TM-1.1	FR A																	
TM-1.1.1	Power Converter																	
TM-1.1.1.a			Overcurrent (in power converter or one of its loads)	Local	Power cycle radio and if condition still exists power down radio and re-enforce other side? Question on how to implement....limit power cycle rule fire count and use longer persistence for side switch rule? 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?	Autonomy	N/A	~1 sec (next telemetry status packet from radio)	None	None	None	None	?				ARC cycles power to converter, avionics would need to redirect signal through switching matrix to switch to side B. Switching is done through the ARC, but autonomy would detect a fault and then tell ARC to power cycle or power off	
TM-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	?					
TM-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			28V and return (applies to whole radio)															X
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	None	None	Ground?							RF side switch, then avionics side switch (is avionics side switch different from system side switch?)				Power cycle, switch to side B	
TM-1.1.2.1.b			Corrupt data (both to and from the radio)	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)																
TM-1.1.2.2.a			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	?	?	Ground contingency to reacquire SC Need to talk through all the combinations within RF system that ground should try when attempting to reacquire	Maybe?				
TM-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 cycle	Autonomy			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	Maybe?				
TM-1.1.2.3		Clock (output)																
TM-1.1.2.3.a			No/out-of-tolerance output	Local	RF side switch	Autonomy	?	?	None	None	None	None	None					
TM-1.1.2.3.b			Corrupt data	Local	RF side switch	Autonomy	?	?	None	None	None	None	None					
TM-1.1.2.4		Baseband																
TM-1.1.2.4.a			No/out-of-tolerance output	Local/System	Power cycle FR, RF side switch? Possible system side switch? Part of CLT response should include re-enforcing RF Could use 2 CLTs, first to power cycle	Autonomy			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	Maybe?				
TM-1.1.2.4.b			Corrupt data	Local/System	Power cycle FR, RF side switch? Possible system side switch? Part of CLT response should include re-enforcing RF Could use 2 CLTs, first to power cycle	Autonomy			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	Maybe?				
TM-1.1.2.4		MET Synch																
TM-1.1.2.4.a			No/out-of-tolerance output															
TM-1.1.2.4.b			Corrupt data															
TM-1.1.3	X-Band Rx (function - includes at least two cards)																	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
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		yes	CLT will expire. CCD commands are only sent during ground contact (failure of commands will be seen in trending). No autonomous reaction.	Heartbeat from FR; FR reset type		N/A	N/A
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 B of telecomm. Would likely follow common response to CLT timeout - soft reset of radio, power 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.	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."	3	Active	Yes	S/c would know that it didn't acquire an uplink signal. If in contact with ground, FCs would notice failure to acquire.	Ground - loss of signal/lock CLT not tickled		?	N/A
TM-1.1.3.d			Failure to detect commands	1) Component failure 2) Radiation effects 3) Failure to acquire		No critical commands, although there would be signal lock with ground.	Ground would try to reaquire s/c. Eventually CLT would timeout. Would likely follow common response to CLT timeout - soft reset of radio, power 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.	No effect.	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."	3		yes	CLT will expire. CCD commands are only sent during ground contact (failure of commands will be seen in trending). No autonomous reaction.	Ground - loss of signal/lock CLT not tickled		?	N/A
TM-1.1.3.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.	Ground would try to reaquire s/c. Eventually CLT would timeout. Would likely follow common response to CLT timeout - soft reset of radio, power 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.	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."	3	Active	Yes	Non-incrementing command counters, incrementing bad command counters, bad s/c ID, BCH errors. Margin might hide problems, would need to look at data trending.	Ground - loss of signal/lock CLT not tickled		?	N/A
Inputs			RF Signal from ground	1) No signal 2) corrupted signal 3) reduced signal 4) incorrect data rate or corrupted data (misconfiguration of ground station)		1) Receiver would show loss of lock and AGC would report no signal 2) Could be reporting lock and valid AGC, but still have corrupted data 3) Possible intermittent lock, loss of lock, or increased errors 4) Would see a loss of lock or reduced signal strength	Would likely follow common response to CLT timeout - soft reset of radio, power cycle to radio, side switch of RF, then sideswitch of avionics. 1) switch sides of radio, check switch assembly, no data from ground. S/c unaffected 2, 3) bad frame counts would go up. Similar to failure to detect commands. 4) Similar to failure to acquire	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. CLT should timeout prior to this happening and s/c should "safe."	3	Active	Yes	1) Would show loss of lock, unexpected AGC voltage 2) Could show lock, but bad frame counter would increment or command counter would not increment 3) Varying AGC levels, lower than expected AGC level, increased error count. 4) Ground would notice failure to acquire	Ground - loss of signal/lock CLT not tickled		?	N/A
			Configuration commands from C&DH			Could be reporting lock and valid AGC, but still have corrupted data. Would see a loss of lock or reduced signal strength	S/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 RF, then sideswitch of avionics.	Assuming you receive all 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."	3	Active	Yes	Reported status telemetry	Ground - loss of signal/lock CLT not tickled		?	N/A
TM-1.1.4	X-Band Tx																
TM-1.1.4.a			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.	No effect.	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 detect failure, but ground would see loss of comm	Heartbeat from FR		N/A	N/A
TM-1.1.4.c			Reduced performance	1) Radiation effects 2) 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	Tlm for reducecd performance defined by RF team		None	None

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response: 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	Quick Look: System Side Switch	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	?	?	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	?	?	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	?	?	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	?	?	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	
			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	X-Band Tx																	
TM-1.1.4.a			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	Local	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	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
Inputs			Configuration commands from C&DH			Could be reporting lock and valid AGC, but still have corrupted data (wrong MOD index, data rate, mode, etc.). Would see a loss of lock or reduced signal strength	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	Tlm for reducecd performance defined by RF team		None	None
TM-1.1.5	Ka-Band Tx																
TM-1.1.5.a			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.	No effect.	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 detect failure, but ground would see loss of comm	Heartbeat from FR		N/A	N/A
TM-1.1.5.c			Reduced performance	1) Radiation effects 2) 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	Tlm for reducecd performance defined by RF team		None	None
Inputs			Configuration commands from C&DH			Could be reporting lock and valid AGC, but still have corrupted data (wrong MOD index, data rate, mode, etc.). Would see a loss of lock or reduced signal strength	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	Tlm for reducecd performance defined by RF team		None	None
TM-1.2	FR B																
TM-1.2.1	Power Converter																
TM-1.2.2	Spacecraft Interfaces (except power)																
TM-1.2.2.1		Spacewire															
TM-1.2.2.2		UART															
TM-1.2.2.3		Clock															
TM-1.2.2.4		Baseband															
TM-1.2.2.4		MET Synch															
TM-1.2.3	X-Band Rx																
TM-1.2.4	X-Band Tx																
TM-1.2.5	Ka-Band Tx																
TM-2	TWTA																
TM-2.1	X TWTA A/EPC																
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	Current and voltage would be out-of-spec, ground would lose 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.	EPC anode voltage How to catch TWTA on/off?	?	?	?
TM-2.1.b			Fault reported in TWTA tlm lines / No RF output	1) High helix current 2) Overcurrent 3) High temperature 4) 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	1) High voltage monitored by the s/c 2) 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 mimic 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	?	?	None
			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-2.2	X TWTA B/EPC																
TM-2.3	Ka TWTA A/EPC																
TM-2.3.a			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 lose 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 and current	PDU to CDH/Autonomy	?	?

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Remediation	Revisit
				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		
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 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-1.2	FR B																	
TM-1.2.1	Power Converter																	
TM-1.2.2	Spacecraft Interfaces (except power)																	
TM-1.2.2.1		Spacewire																
TM-1.2.2.2		UART																
TM-1.2.2.3		Clock																
TM-1.2.2.4		Baseband																
TM-1.2.2.4		MET Synch																
TM-1.2.3	X-Band Rx																	
TM-1.2.4	X-Band Tx																	
TM-1.2.5	Ka-Band Tx																	
TM-2	TWTA																	
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	?	?	?					
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	None	None	?					
			RF input from radio	Locacl	RF side switch	Autonomy	?	?	None	None	None	None	?					
TM-2.2	X TWTA B/EPC																	
TM-2.3	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.	

						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)
TM-2.3.b			Fault reported in TWTA tlm lines / No RF output	1) High helix current 2) Overcurrent 3) High temperature 4) 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	1) High voltage monitored by the s/c 2) Only ground would notice variation in received power	PDU TWTA current	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 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.	PDU TWTA current	PDU to CDH/Autonomy	?	?
			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.	None No RF output on ground CLT expiration	?	?	?
TM-2.4	Ka TWTA B/EPC																
TM-3	Low Noise Amplifier																
TM-3.1	LNA A																
TM-3.1.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 effect.	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 CLT expiration	?	?	?
TM-3.1.b			Incorrect output	1) Degraded performance (gain, noise figure)		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 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.	No effect.	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.	None - degraded performance	None	None	None
Inputs			Secondary voltage from Radio			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 effect.	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.	None No RF output on ground CLT expiration	?	?	?
TM-3.2	LNA B																
TM-4	Hybrid																
TM-4.1	Ka-Band HYB-2																
TM-4.1.a			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.	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	Filter																
TM-5.1	Filter A (component may be removed from design)																
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 failure is in the LNA.	None CLT expiration	?	?	?
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 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.	No effect.	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			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 failure is in the LNA.	None CLT expiration	?	?	?
TM-5.2	Filter B																

				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	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	None	None	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
			RF input from radio	Local	RF side switch	Autonomy	?	?	None	None	None	None	SC reacquire contingency - no downlink					X
TM-2.4	Ka TWTA B/EPC																	
TM-3	Low Noise Amplifier																	
TM-3.1	LNA A																	
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			Incorrect 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	LNA B																	
TM-4	Hybrid																	
TM-4.1	Ka-Band HYB-2																	
TM-4.1.a			No output / incorrect output	Local / Ground	RF side switch	Ground	?	?	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	Filter																	
TM-5.1	Filter A (component may be removed from design)																	
TM-5.1.a			No output	Local	RF side switch	Autonomy	?	?	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			Uplink signal from diplexer	Local	RF side switch	Autonomy	?	?	None	None	None	None	Ground to reacquire SC					
TM-5.2	Filter B																	

						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)**
TM-6	Diplexer																
TM-6.1	DP A																
TM-6.1.a			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 - degraded performance	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 - degraded performance	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 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 - degraded performance	None	None	None
TM-6.2	DP B																
TM-7	RF Switch																
TM-7.1	SW1																
TM-7.1.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-7.1.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 (electrical fault)	Redundant coils burnt out (two failures)		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 (mechanical fault)	not a credible failure		Not a credible failure	No effect.	No effect.	N/A	4	None		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 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 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	?	?
TM-7.2	SW2																
TM-7.2.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-7.2.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 (electrical fault)	Redundant coils burnt out (two failures)		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 (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 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 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	?	?
TM-7.3	SW3																

				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	Remediation	Revisit
TM-6	Diplexer																	
TM-6.1	DP A																	
TM-6.1.a			No output (uplink or downlink)	Local	RF side switch	Autonomy	?	?	None	None	None	None	Ground to reacquire SC					
TM-6.1.b			Degraded output (uplink or downlink)	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
Inputs			Uplink signal from switch assembly	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
			Downlink signal in from X-band TWTAs	Local / Ground	RF side switch	Ground	?	?	None	None	None	None	Ground to monitor performance; contingency for RF side switch					
TM-6.2	DP B																	
TM-7	RF Switch																	
TM-7.1	SW1																	
TM-7.1.a			Switch stuck in a single position	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					
TM-7.1.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					
TM-7.1.c			Switch not in any position (electrical fault)	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; this fault would result in RF side switch?					
TM-7.1.d			Switch not in any position (mechanical fault)	None	None	None	None	None	None	None	None	None	None					
Inputs			RF signal from previous switch, diplexer, or antenna	Local	CLT expires and performs RF side switch	Autonomy	?	?	CLT 2 expires and performs system side switch	Autonomy	?	?	?					
TM-7.2	SW2																	
TM-7.2.a			Switch stuck in a single position	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					
TM-7.2.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					
TM-7.2.c			Switch not in any position (electrical fault)	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; this fault would result in RF side switch?					
TM-7.2.d			Switch not in any position (mechanical fault)	None	None	None	None	None	None	None	None	None	None					
Inputs			RF signal from previous switch, diplexer, or antenna	Local	CLT expires and performs RF side switch	Autonomy	?	?	CLT 2 expires and performs system side switch	Autonomy	?	?	?					
TM-7.3	SW3																	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	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 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 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	?	?
TM-7.4	SW4																
TM-7.4.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-7.4.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 (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 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	?	?
TM-8	Flex Waveguide																
TM-8.1	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	None	Yes. (After process of elimination)	Gournd would see reduced downlink power. Autonomy would not act.	None	None	None	None
TM-8.2	FW B																
TM-9	Antennae																
TM-9.1	HGA																
TM-9.1.a			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 power or corrupted signal	None Loss of comm with HGA	None	None	None
TM-9.2	LGA 1																
TM-9.2.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. Only used during TCMs, may lose comm due to s/c pointing requirements for TCM. Ground would command s/c to switch antennae.	Mission success impacted by loss of LGA	N/A	3	None	Yes. (After process of elimination)	No more comm to/from LGA.	None Loss of comm with LGA	None	None	None
TM-9.3	LGA 2																
TM-9.4	FB 1																

				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	Remediation	Revisit
TM-7.3.a			Switch stuck in a single position	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					
TM-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					
TM-7.3.c			Switch not in any position (electrical fault)	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; this fault would result in RF side switch?					
TM-7.3.d			Switch not in any position (mechanical fault)	None	None	None	None	None	None	None	None	None	None					
Inputs			RF signal from previous switch, diplexer, or antenna	Local	CLT expires and performs RF side switch	Autonomy	?	?	CLT 2 expires and performs system side switch	Autonomy	?	?	?					
TM-7.4	SW4																	
TM-7.4.a			Switch stuck in a single position	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					
TM-7.4.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					
TM-7.4.c			Switch not in any position (electrical fault)	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; this fault would result in RF side switch?					
TM-7.4.d			Switch not in any position (mechanical fault)	None	None	None	None	None	None	None	None	None	None					
Inputs			RF signal from previous switch, diplexer, or antenna	Local	CLT expires and performs RF side switch	Autonomy	?	?	CLT 2 expires and performs system side switch	Autonomy	?	?	?					
TM-8	Flex Waveguide																	
TM-8.1	FW A																	
TM-8.1.a			Crack	Local / Groound	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; this fault would result in RF side switch?					
Inputs			RF output from Ka-band TWTAs	Local / Groound	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; this fault would result in RF side switch?					
TM-8.2	FW B																	
TM-9	Antennae																	
TM-9.1	HGA																	
TM-9.1.a			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			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					
TM-9.2	LGA 1																	
TM-9.2.a			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-9.3	LGA 2																	
TM-9.4	FB 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)
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 Z 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.	Mission success impacted by loss of FB	N/A	3	None	Yes. (After process of elimination)	No more comm to/from FB.	None Loss of comm with FB	None	None	None
TM-9.5	FB 2																
TM-10	RFDU																
TM-10.a			Loss of single diode/resistor in cross-strapping section			Loss of cross-strapping capability to one side	Could probably still use that 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.	No effect. Ground will need to infer position based on 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 lose downlink.				
			Control lines from avionics to switch assembly			Switch stuck in single configuration	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.				

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Remediation	Revisit
				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		
TM-9.4.a			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-9.5	FB 2																	
TM-10	RFDU																	
TM-10.a			Loss of single diode/resistor in cross-strapping section	Local	RF side switch													X
TM-10.b			Loss of soft-start circuitry for TWTs	Local	RF side switch													X
Inputs			Tell tale signal from switch assembly	Local	RF side switch													
			DC power to TWTs	Local	RF side switch			? Depends on how often those values are sampled. Probably 1Hz tick.										
			Control lines from avionics to switch assembly	Local	RF side switch													

Subject Matter Expert(s): Tim Cole
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.

						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)**
ME-1	Gimbals															
ME-1.1	Solar Array															
ME-1.1.1	Solar Array #1															
ME-1.1.1.1	Flap Actuator															
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	E, C	Solar array stuck in position	1) 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)	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	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			Incorrect actuation when commanded	1) incorrect potentiometer reading 2) residual torque (should have sufficient margin) 3) 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)	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 margin)	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)	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	?
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 release completely (mechanical clearance issues/unexpected interferences) (probably adding a push-off spring to ensure deployment)	C	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) 3) Incorrect notch on frangibolt (controlled by 100% inspection of notch by vendor, will add a double-check to notch in I&T)	L	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 position or not moving at expected rate (too fast or two 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.	ECU switch should correct problem.	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 Expert(s): Tim Cole, 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.

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			
ME-1.1.1.1	Flap Actuator			
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)	?

Subject Matter Expert(s): Tim Cole, 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.

				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**	**Remediation/ notes**	**Autonomy?**	**Comments**	**Revisit**
ME-1	Gimbals																			
ME-1.1	Solar Array																			
ME-1.1.1	Solar Array #1																			
ME-1.1.1.1	Flap Actuator																			
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	?	?	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			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				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	?	?	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	?	?	If problem persists, umbra violation or LBSOC	Autonomy	?	?	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		

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method				
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)
			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			Fails to actuate when commanded	1) bad/bound bearing/mechanical failure 2) stepper motor failure 3) loose/separated connector	C	Solar array stuck in position	1) generates insufficient power 2) generates too much power 3) feathering makes it impossible for array to retract sufficiently for encounter	1) eventually drain battery, may be able to slew s/c to retain partial power for a time; cooling system might get too cold 2) overheat cooling system 3) lose mission	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			Incorrect actuation when commanded	1) incorrect potentiometer reading 2) residual torque (should have sufficient margin) 3) Motor coil or winding is open	C	Solar array in incorrect position	1) generates insufficient power 2) generates too much power 3) feathering makes it impossible for array to retract sufficiently for encounter	1) eventually drain battery, may be able to slew s/c to retain partial power for a time; cooling system might get too cold 2) overheat cooling system 3) lose mission	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			Actuates when not commanded	Holding torque exceeded (need to have sufficient margin)	C	Solar array in incorrect position	1) generates insufficient power 2) generates too much power 3) feathering makes it impossible for array to retract sufficiently for encounter	1) eventually drain battery, may be able to slew s/c to retain partial power for a time; cooling system might get too cold 2) overheat cooling system 3) lose mission	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	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	?
			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	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-1.1.2	Solar Array #2															
ME-1.2	HGA															
ME-1.2.1	HGA Gimbal															
ME-1.2.1.a			Fails to actuate when commanded (mechanical failure)	1) 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 (~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	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			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.	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	Yes	Potentiometer telemetry, step count	Potentiometer telemetry ; redundant ECU telemetry	ECU to REM	?
ME-1.2.1.c			Incorrect 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. Re-command 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	Solar Array #2			
ME-1.2	HGA			
ME-1.2.1	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	?

				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	Remediation/ notes	Autonomy?	Comments	Revisit
			Harness too cold	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							
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	?	?	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			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			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				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		
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	?	?	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		
			Harness too cold	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							
ME-1.1.2	Solar Array #2																			
ME-1.2	HGA																			
ME-1.2.1	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	?	?	None				re-command, slew	command to a "safe" position		
ME-1.2.1.b			Fails to actuate when commanded (electrical 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	?	?	None				Each motor winding goes to a different ECU.			
ME-1.2.1.c			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	?	?	umbra violation	Autonomy	?	?	None				re-command, slew	command to a "safe" position		

						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)
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. Re-command 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	C	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 release completely (mechanical clearance issues/unexpected interferences)	C	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	L	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	Potentiometers	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)			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.	No effect.	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	Potentiometers	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	?

				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	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???	Autonomy	?	?	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" position		
ME-1.3	Potentiometers	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)	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)	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.c			Crack in substrate causes loss of both potentiometers	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??? Not sure what to do when redundant pot also shows mistmatch?	Autonomy	?	?	?	?	?	?	None							
ME-1.3.d			Wrong value	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							

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: 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 MAG sensor is not enough to be a loss of science.	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 re-sent.	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	FIELDS			
ME-2.1.1	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	

				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**	**Remediation/ notes**	**Autonomy?**	**Comments**	**Revisit**
ME-1.3.e			Life-limiting # of cycles	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??? Not sure what to do when redundant pot also shows mistmatch? Would not help in this case, but detection/response would look the same	Autonomy	?	?	?	?	?	?	None							
ME-2	Instruments																			
ME-2.1	FIELDS																			
ME-2.1.1	Magnetometer Boom																			
ME-2.1.1.a			Doesn't deploy (detail to come)														re-command, slew			X
ME-2.1.1.b			Deploys prematurely (detail to come)																	X
ME-2.1.1.c			Partial deployment																	
Inputs			Electrical fault																	

Subject Matter Expert(s): Stewart Bushman (Propulsion)
Robin Vaughan (Effects to S/C and/or G&C)

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FMEA information is only displayed

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: Time to Detect (System)
PR-1	Service Valves																
PR-1.1	Service Valve 1 (SV1) (Pressurant)																
PR-1.1.a			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)	Mission-ending with complete loss of pressurant or if enough torque is applied	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	Service Valve 2 (SV2) (Liquid)																
PR-1.2.a			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	Mission-ending with complete loss of fuel or if enough torque is applied	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-2	Tank																
PR-2.a			Internal leak (liquid into gas)	1) Physical damage (pinhole leak in diaphragm)		Unusable propellant that can't be pushed out of the tank	Less fuel overall	No effect until s/c runs out of usable fuel	N/A until s/c runs out of usable fuel	2	None	No	You'd run out of fuel early	No	N/A	N/A	N/A
PR-2.b			External leak (pressurant)	1) Physical damage		Leaking helium	Over time will decrease system pressure, may torque s/c (depends on size of leak)	Mission-ending with complete loss of pressurant 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-2.c			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	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	Pressure Transducers																
PR-3.1	Pressure Transducer A (PTA)																
			Inrush current issue			Draw too much current	Fuse would blow	No effect	N/A	4	Active - Autonomy rule	Yes	See high current draw in telemetry	PDU current tlm for PTA			
PR-3.1.a			Invalid output			Output invalid	Check other transducer	No effect	N/A	4	None				N/A	N/A	N/A
PR-3.1.b			Hard failure	1) Physical damage 2) Electronics failure		Lack of knowledge of tank pressure	Turn other transducer on, when it's necessary (probably at least for every TCM), might require switching avionics sides (TBD)	No effect	N/A	4	None	Yes	No current draw, if current is fine, but data is bad, might be in harness/sampling electronics	PDU current tlm for PTA	N/A	N/A	N/A
PR-3.1.c			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	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	N/A
Input			Bus voltage			No power to transducer				4	None			PDU current tlm for PTA; PDU power state for PTA	N/A	N/A	N/A
PR-3.2	Pressure Transducer B (PTB)																
PR-4	Filter 1 (F1)																
PR-4.a			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	Orifice 1 (O1)																
PR-5.a			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-6	Propulsion Diode Box (PDB)																
PR-6.a			Any failure of any diode or resistor			Could lose one thruster or LV	System is 1-fault tolerant	No effect	Yes if it happened at the wrong time, but mission is done at that point anyway	4	Passive - redundancy?		Would this affect manuever?				
PR-7	Latch Valves																
PR-7.1	Latch Valve A (LVA)																

Subject Matter Expert(s): Stewart Bushman (Propulsion)
Robin Vaughan (Effects to S/C and/or G&C)

Notes: Yellow highlighted blocks are redundant components. Components are listed for completeness, but failure mode and FMEA information 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**
PR-1	Service Valves																			
PR-1.1	Service Valve 1 (SV1) (Pressurant)																			
PR-1.1.a			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	Service Valve 2 (SV2) (Liquid)																			
PR-1.2.a			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																			
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	
PR-3.1	Pressure Transducer A (PTA)																			
			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		X
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							X
PR-3.2	Pressure Transducer B (PTB)																			
PR-4	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)																			
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		
PR-7	Latch Valves																			
PR-7.1	Latch Valve A (LVA)																			

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
PR-7.1.a	(redundant, in parallel, opened during launch countdown or directly after launch, not closed again during nominal mission)		Internal leakage	1) Particulate, FOD 2) Physical damage		No effect, propellant on both sides when closed, opened nominally	None	None	N/a	4	None	No	No	N/A	N/A	N/A	N/A
PR-7.1.b			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-7.1.c			Fails open	1) Particulate, FOD 2) Physical damage 3) Damage to coil		No effect, propellant on both sides when closed, opened nominally	None	None	N/a	4	None	No	No	N/A ; LV open/close tlm?	N/A	N/A	N/A
PR-7.1.d			Fails closed	1) Particulate, FOD 2) Physical damage 3) Damage to coil		No effect, assuming 2nd latch valve is open	None	None	N/a	4	Passive - redundancy ?	No	No	N/A ; LV open/close tlm?	N/A	N/A	N/A
Inputs			Bus voltage	1) No voltage 2) 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 works 2) Propellant heats up	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-7.2	Latch Valve B (LVB)																
PR-8	Thrusters																
PR-8.01	Thruster A1																
PR-8.01.1	Catbed Heater-Primary																
PR-8.01.1.a			Fails on	1) electrical anomaly upstream		No effect	Power drain on s/c	Probably not mission-ending	N/A	4	Active - Autonomy, HW	Yes	PDU would sense current/voltage draw	PDU current tlm for catbed on when thrusters not active?			N/A
PR-8.01.1.b			Fails off	1) electrical damage 2) Physical damage		Switch to redundant heater (both will probably be on at perihelion and TCMs)	None	None	N/A	4	Active - Autonomy	Yes	PDU would sense lack of current/voltage draw	PDU current tlm for catbed on when thrusters active?		N/A	N/A
PR-8.01.1.c			Heater debonds from Catbed	1) Physical damage		Reduced heating (depends on manufacturer of thruster)	Cold start has slight possibility of damaging thruster.	None	N/A	4	None	Yes	Wonky IMU data. Undetectable during encounter, might see in long-term trending telemetry	IMU tlm?		N/A	N/A
Input			Bus voltage			No power to heater	None, as long as secondary works	None	N/A	4	Passive - Redundancy			PDU catbed current tlm		N/A	N/A
PR-8.01.2	Catbed Heater-Secondary																
PR-8.01.2.a			Fails on														
PR-8.01.2.b			Fails off														
PR-8.01.2.c			Heater debonds from Catbed														
PR-8.01.3	Valve Assembly (NC Solenoid Valves)																
PR-8.01.3.a			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 within 0.7 AU). Probably mission-ending or at least would curtail it.	Yes	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
PR-8.01.3.b			One or both failed closed	1) electrical failure 2) FOD 3) Physical issue		Couldn't use thruster	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			Bus voltage			Couldn't use thruster	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			
PR-8.02	Thruster A2																
PR-8.02.1	Catbed Heater-Primary																
PR-8.02.2	Catbed Heater-Secondary																

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			KAF Comments	Remediation	Autonomy?	Revisit
				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				
PR-7.1.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		
PR-7.1.b			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-7.1.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		
PR-7.1.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		
Inputs			Bus voltage	None	None	None	None	None	None	None	None	None	None							
PR-7.2	Latch Valve B (LVB)																			
PR-8	Thrusters																			
PR-8.01	Thruster A1																			
PR-8.01.1	Catbed Heater-Primary																			
PR-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		
PR-8.01.1.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		
PR-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			
Input			Bus voltage	None	None	None	None	None	None	None	None	None	None							
PR-8.01.2	Catbed Heater-Secondary																			
PR-8.01.2.a			Fails on																	
PR-8.01.2.b			Fails off																	
PR-8.01.2.c			Heater debonds from Catbed																	
PR-8.01.3	Valve Assembly (NC Solenoid Valves)																			
PR-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		
PR-8.01.3.b			One or both failed closed															Cycle power to valves		
Input			Bus voltage															Cycle power to valves		
PR-8.02	Thruster A2																			
PR-8.02.1	Catbed Heater-Primary																			
PR-8.02.2	Catbed Heater-Secondary																			

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
PR-8.02.3	Valve Assembly																
PR-8.03	Thruster A3																
PR-8.03.1	Catbed Heater-Primary																
PR-8.03.2	Catbed Heater-Secondary																
PR-8.03.3	Valve Assembly																
PR-8.04	Thruster A4																
PR-8.04.1	Catbed Heater-Primary																
PR-8.04.2	Catbed Heater-Secondary																
PR-8.04.3	Valve Assembly																
PR-8.05	Thruster B1																
PR-8.05.1	Catbed Heater-Primary																
PR-8.05.2	Catbed Heater-Secondary																
PR-8.05.3	Valve Assembly																
PR-8.06	Thruster B2																
PR-8.06.1	Catbed Heater-Primary																
PR-8.06.2	Catbed Heater-Secondary																
PR-8.06.3	Valve Assembly																
PR-8.07	Thruster B3																
PR-8.07.1	Catbed Heater-Primary																
PR-8.07.2	Catbed Heater-Secondary																
PR-8.07.3	Valve Assembly																
PR-8.08	Thruster B4																
PR-8.08.1	Catbed Heater-Primary																
PR-8.08.2	Catbed Heater-Secondary																
PR-8.08.3	Valve Assembly																
PR-8.09	Thruster C1																
PR-8.09.1	Catbed Heater-Primary																
PR-8.09.2	Catbed Heater-Secondary																
PR-8.09.3	Valve Assembly																
PR-8.10	Thruster C2																
PR-8.10.1	Catbed Heater-Primary																
PR-8.10.2	Catbed Heater-Secondary																
PR-8.10.3	Valve Assembly																
PR-8.11	Thruster C3																
PR-8.11.1	Catbed Heater-Primary																
PR-8.11.2	Catbed Heater-Secondary																
PR-8.11.3	Valve Assembly																
PR-8.12	Thruster C4																
PR-8.12.1	Catbed Heater-Primary																
PR-8.12.2	Catbed Heater-Secondary																
PR-8.12.3	Valve Assembly																
PR-9	Temperature Sensors																
PR-9.1	Temperature Sensor (generic - still deciding locations)																
PR-9.1.a	Platinum RTDs		No output			Lack telemetry	No effect	No effect		4		Yes	Lack temp telemetry				
PR-9.1.b			Incorrect output														
Inputs			Bus voltage														
PR-9.2	Temperature Sensor Ghe																
PR-9.2.a			No output														
PR-9.2.b			Incorrect output														
PR-9.3	Temperature Sensor N2H2																
PR-9.3.a			No output														
PR-9.3.b			Incorrect output														
PR-9.4	Temperature Sensor F1																
PR-9.4.a			No output														
PR-9.4.b			Incorrect output														
PR-9.5	Temperature Sensor LV Manifold																
PR-9.5.a			No output														
PR-9.5.b			Incorrect output														
PR-9.6	Temperature Sensor Thruster Manifold																
PR-9.6.a			No output														
PR-9.6.b			Incorrect output														
PR-9.7	Temperature Sensor A4																
PR-9.7.a			No output														
PR-9.7.b			Incorrect output														
PR-9.8	Temperature Sensor B4																
PR-9.8.a			No output														
PR-9.8.b			Incorrect output														
PR-9.9	Temperature Sensor C4																
PR-9.9.a			No output														
PR-9.9.b			Incorrect output														

				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
PR-8.02.3	Valve Assembly																			
PR-8.03	Thruster A3																			
PR-8.03.1	Catbed Heater-Primary																			
PR-8.03.2	Catbed Heater-Secondary																			
PR-8.03.3	Valve Assembly																			
PR-8.04	Thruster A4																			
PR-8.04.1	Catbed Heater-Primary																			
PR-8.04.2	Catbed Heater-Secondary																			
PR-8.04.3	Valve Assembly																			
PR-8.05	Thruster B1																			
PR-8.05.1	Catbed Heater-Primary																			
PR-8.05.2	Catbed Heater-Secondary																			
PR-8.05.3	Valve Assembly																			
PR-8.06	Thruster B2																			
PR-8.06.1	Catbed Heater-Primary																			
PR-8.06.2	Catbed Heater-Secondary																			
PR-8.06.3	Valve Assembly																			
PR-8.07	Thruster B3																			
PR-8.07.1	Catbed Heater-Primary																			
PR-8.07.2	Catbed Heater-Secondary																			
PR-8.07.3	Valve Assembly																			
PR-8.08	Thruster B4																			
PR-8.08.1	Catbed Heater-Primary																			
PR-8.08.2	Catbed Heater-Secondary																			
PR-8.08.3	Valve Assembly																			
PR-8.09	Thruster C1																			
PR-8.09.1	Catbed Heater-Primary																			
PR-8.09.2	Catbed Heater-Secondary																			
PR-8.09.3	Valve Assembly																			
PR-8.10	Thruster C2																			
PR-8.10.1	Catbed Heater-Primary																			
PR-8.10.2	Catbed Heater-Secondary																			
PR-8.10.3	Valve Assembly																			
PR-8.11	Thruster C3																			
PR-8.11.1	Catbed Heater-Primary																			
PR-8.11.2	Catbed Heater-Secondary																			
PR-8.11.3	Valve Assembly																			
PR-8.12	Thruster C4																			
PR-8.12.1	Catbed Heater-Primary																			
PR-8.12.2	Catbed Heater-Secondary																			
PR-8.12.3	Valve Assembly																			
PR-9	Temperature Sensors																			
PR-9.1	Temperature Sensor (generic - still deciding locations)																			
PR-9.1.a	Platinum RTDs		No output																	X
PR-9.1.b			Incorrect output																	X
Inputs			Bus voltage																	X
PR-9.2	Temperature Sensor Ghe																			
PR-9.2.a			No output																	
PR-9.2.b			Incorrect output																	
PR-9.3	Temperature Sensor N2H2																			
PR-9.3.a			No output																	
PR-9.3.b			Incorrect output																	
PR-9.4	Temperature Sensor F1																			
PR-9.4.a			No output																	
PR-9.4.b			Incorrect output																	
PR-9.5	Temperature Sensor LV Manifold																			
PR-9.5.a			No output																	
PR-9.5.b			Incorrect output																	
PR-9.6	Temperature Sensor Thruster Manifold																			
PR-9.6.a			No output																	
PR-9.6.b			Incorrect output																	
PR-9.7	Temperature Sensor A4																			
PR-9.7.a			No output																	
PR-9.7.b			Incorrect output																	
PR-9.8	Temperature Sensor B4																			
PR-9.8.a			No output																	
PR-9.8.b			Incorrect output																	
PR-9.9	Temperature Sensor C4																			
PR-9.9.a			No output																	
PR-9.9.b			Incorrect output																	

Subject Matter Expert(s): Liz Abel (Thermal), Jack Ercol (Active Cooling)

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

						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)**
TH-1	MLI																
TH-1.1	Spacecraft MLI	Insulate spacecraft bus															
TH-1.1.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.	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	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	Yes	Component temperature change			N/A	
TH-2	Louvers	Regulate temperature of spacecraft bus															
TH-2.1	20-blade #1																
TH-2.1.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 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-2.1.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	20-blade #2																
TH-2.2.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 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.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-2.3	14-blade																
TH-2.3.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 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-2.3.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-2.4	10-blade																

Subject Matter Expert(s): Liz Abel (Thermal), Jack Ercol (Active Cooling)

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

				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**	**Comments - KAF**	**Revisit**
TH-1	MLI																	
TH-1.1	Spacecraft MLI	Insulate spacecraft bus																
TH-1.1.a			Degraded/damaged				N/A	Depends on severity of degradation/damage (time required to see temperature change in component)										
TH-1.2	High-temperature MLI	Insulate exposed portions of spacecraft (solar arrays, radiators, etc.)																
TH-1.2.a			Degraded/damaged				N/A	Depends on severity of degradation/damage (time required to see temperature change in component)										
TH-2	Louvers	Regulate temperature of spacecraft bus																
TH-2.1	20-blade #1																	
TH-2.1.a			Doesn't open/close				N/A	Time required to see temperature change in component										X
TH-2.1.b			Blade breaks				N/A	Time required to see temperature change in component										X
TH-2.2	20-blade #2																	
TH-2.2.a			Doesn't open/close				N/A	Time required to see temperature change in component										X
TH-2.2.b			Blade breaks				N/A	Time required to see temperature change in component										X
TH-2.3	14-blade																	
TH-2.3.a			Doesn't open/close				N/A	Time required to see temperature change in component										X
TH-2.3.b			Blade breaks				N/A	Time required to see temperature change in component										X
TH-2.4	10-blade																	

						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)
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 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-2.4.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 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-2.5	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 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-2.5.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 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-2.6	7-blade #2																
TH-2.6.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 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-2.6.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 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-3	Heaters																
TH-3.1	Propulsion Tank Heaters A&B (22 Ω switched)																
TH-3.1.a			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 Valve 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	
TH-3.3	Propulsion Internal Heaters A&B (28 Ω switched)																

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Comments - KAF	Revisit
				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		
TH-2.4.a			Doesn't open/close				N/A	Time required to see temperature change in component										X
TH-2.4.b			Blade breaks				N/A	Time required to see temperature change in component										X
TH-2.5	7-blade #1																	
TH-2.5.a			Doesn't open/close				N/A	Time required to see temperature change in component										X
TH-2.5.b			Blade breaks				N/A	Time required to see temperature change in component										X
TH-2.6	7-blade #2																	
TH-2.6.a			Doesn't open/close				N/A	Time required to see temperature change in component										X
TH-2.6.b			Blade breaks				N/A	Time required to see temperature change in component										X
TH-3	Heaters																	
TH-3.1	Propulsion Tank Heaters A&B (22 Ω switched)																	
TH-3.1.a			Fails on	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time	None								No CB for switched heater; prop heaters were different than what Stewart expected	
TH-3.1.b			Fails off	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.1.c			Debonds from surface	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
Inputs			Switched Power	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.2	Propulsion Line and Valve Heaters A&B (37 Ω switched)																	
TH-3.2.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-3.2.b			Fails off	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.2.c			Debonds from surface	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
Inputs			Switched Power	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.3	Propulsion Internal Heaters A&B (28 Ω switched)																	

						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)
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)																
TH-3.7.a			Fails on			Dual thermostats at different set points will cause heater to turn off, switch to other side	No effect.	No effect.	N/A	2R	None	Yes	Thermostats			N/A	
TH-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 side	No effect.	No effect.	N/A	4	None	Yes	Thermostats			N/A	
TH-3.8	Battery Heater B & Solar Array Drive Heater B (unswitched)																

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response										Quick Look			Comments - KAF	Revisit
				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		
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	Autonomy	N/A	TBD time										
TH-3.3.c			Debonds from surface	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
Inputs			Switched Power	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.4	S/C Panel Survival Heaters A&B (16 Ω switched)																	
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	Autonomy	N/A	TBD time										
Inputs			Switched Power	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.5	CSPR Manifold 1&4 Heaters A&B (16 Ω switched)																	
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	Autonomy	N/A	TBD time										
TH-3.5.c			Debonds from surface	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
Inputs			Switched Power	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.6	CSPR Manifold 2&3 Heaters A&B (14 Ω switched)								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	Autonomy	N/A	TBD time										
TH-3.6.c			Debonds from surface	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
Inputs			Switched Power	Local	Switch heater power off, power on redundant	Autonomy	N/A	TBD time										
TH-3.7	Battery Heater A & Solar Array Drive Heater A (unswitched)																	
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	Battery Heater B & Solar Array Drive Heater B (unswitched)																	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	Detection Method: How Observed?	Detection Method: Tlm for Diagnosis	Detection Method: Tlm Path for Diagnosis	Detection Method: Time to Detect (Local)	Detection Method: Time to 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.	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.	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.	No effect.	N/A	4	None	Yes	Thermostats			N/A	
TH-4	Temperature Sensors																
TH-4.a			No output	1) mechanical break 2) RIO failure		Bad reading at sensor	Determine whether or not to switch on 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 not to switch on redundant sensor	No effect.	N/A	4	?	yes	Component temp			N/A	

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	Comments - KAF	Revisit
				Response										Quick Look				
TH-3.8.a			Fails on				N/A	TBD time	dual thermostats								No FM since these are unswitched loads	
TH-3.8.b			Fails off				N/A	TBD time										
TH-3.8.c			Debonds from surface				N/A	TBD time										
Inputs			Unswitched power				N/A	TBD time										
TH-4	Temperature Sensors																	
TH-4.a			No output				N/A	Time required to see temperature change in component	all components will have redundant temp sensors (current baseline)								Not sure that all components do have redundant temp sensors? Would we want to do a side switch for critical components if the temp info was not available/stale?	
TH-4.b			Incorrect output				N/A	Time required to see temperature change in component										

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect: Local	Effect: Next Higher	Effect: Mission	Effect: Umbra Violation	Severity	Type of FM	Detection Method: Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to Detect (System)
Severity 1s **Avionics**																	
AV-4.1.2.2.a	PRIO		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.	LOM	N/A	1	Passive - Redundancy??	yes	Safety buses wouldn't turn on				
G&C																	
GC-4.1.k	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 at time of side switch).	Possibly mission-ending.	Possible, depending on where in orbit, how fast, and which direction it's turning.	1		No					
Propulsion																	
Inputs	Latch Valve A		Bus voltage	1) No voltage 2) 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 works 2) Propellant heats up	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 within 0.7 AU). Probably mission-ending or at least would curtail it.	Yes	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**																	
Inputs	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) components	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) Battery would discharge	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.	N/A	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 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.	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 component	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	1) Electronics failure 2) Connector/cable failure 3) Common electronics (redundant within FET slice)	E, M, C	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		
AV-4.1.3.1.a	FET Slice 1 - Circuit Breaker		Unable to reset	1) Part Failure	E, M, C	1) Assuming load has tripped circuit breaker, loss of switched load 2) If load has not tripped circuit breaker, then no effect	1) Potential loss of a single instrument suite. Cycling power to load may reset circuit breaker. Ground would probably investigate problem at next ground contact.	1) Degraded or LOM depending on which switched 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 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	1) 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 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 component	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.		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	Power drain higher than expected. Load switches off when fuse blows.	Load current	PDU to REM		

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Response: Response Level	Response: Desired Local Response	Response: Allocation of Local Response	Response: Time to fix locally	Response: Time to Transmit Signal	Response: Desired System Response	Response: Allocation of System Response	Response: Time to fix system	Response: Time to Transmit Signal	Response: Ground Response / Contingency	Quick Look: System Side Switch	Quick Look: Processor Switch	Quick Look: Safe Mode	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
Severity 1s																				
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																				
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																				
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		X	
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													X	
AV-4.1.2.1.b	Relay Cap A - Fuse Module		Blows too soon	Local	Consider having an over-current rule for each switched 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		X	
AV-4.1.3.c	FET Slice 1		FET stuck off	Local	TBD which loads, but monitor for one of two always on?	Autonomy													X	
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		X	
AV-4.1.3.1.a	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		X	
AV-4.1.3.1.b	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		X	
AV-4.1.3.1.c	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		X	
AV-4.1.3.1.d	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		X	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm 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)	E, M, C	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.b	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	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	?	?
G&C																	
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) Faulty connector or harness/wiring inside unit 2) Localized electronics fault that affects message processing logic 3) Error in solar limb sensor internal firmware (FPGA)		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	Control correction will be wrong because offset angle is wrong. Will not meet WISPR pointing requirements when controlling based on SLS data. S/C may think it's seeing the Sun earlier than it actually is, or may "see" it too late.	Loss of mission if umbra violation occurs while trying to correct attitude using degraded offset angles from 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 we'd never get a second occurence where we would test if we had made the right correction.)	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.	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 +Z/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.		The "stuck" or "run away" wheel will eventually reach saturation (max speed) with how long that takes depending on the speed magnitude when command first froze.	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 correctable in the time available depending on how we design the auto dump logic and fault checks for wheels	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 violation it may not be correctable in the time available depending on how we design the auto dump logic and fault checks for wheels	Possible if too many wheels reach saturation before a momentum dump can be performed.	2							

				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**	**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													X	
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		X	
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)	Local	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	
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	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		
G&C																				
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 parameters 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 wheel 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). A side 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 switched. If the wheel is still not responding after side 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 (System)
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.	The controller will mistakenly keep sending commands to all the wheels. The other wheels 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 when this occurs. There should be time for G&C software to detect wheel is not responding and request action from autonomy.	Loss of mission in the worst 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 logic and fault checks for wheels	Probably not in this case.	2							
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.		Wheel will spin in correct direction from 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 against it.	Might be survivable if low magnitude - wheel will 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 performed before 2 wheels saturate, we lose controllability	Loss of mission in the worst 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 logic and fault checks for wheels	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.		a) If wheel is sluggish, it puts out less torque than commanded and may 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 random disturbance torque on the system. Sometimes it may contribute to what the controller wants done, but not reliably so. Wheel may consume more power depending on how the erractic behavior manifests itself.	a) Turns will take longer to complete, may deviate more 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 guessing at the nature of the erratic behavior. But if it's intermittent even at max torque, the other 3 wheels should be able to counter it.	Loss of mission in the worst 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 logic and fault checks for wheels	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 fault logic (to turn off misbehaving wheel) b) 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) c) Unlikely in this case	2							
Cooling																	
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 N_2 gas charge that is applied between the bellows and the tank shell. Holds TBD in3 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 N_2 and coolant cavities due to temperature excursions.	N_2 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.	Redundant pump failures due to cavitation common cause would lead to loss TCS and mission.	N/A	2			1) Pump delta-p sensor and/or current and temp sensors detect cavitation; 2) 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 N_2 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	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/or current and temp sensors detect cavitation; 3) P2 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 N_2 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	1) Over stress (ext induced); 2) Corrosion; 3) Fatigue; 4) Material/process (weld) flaw.	All	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.	N/A	2			1) Tank pressure sensor detects loss of pressurization; 2) Pump delta-p sensor and/or current and temp sensors detect cavitation; 3) P2 detects loss of main loop 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 N_2 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	1) Jammed bellows (interference of moving parts); 2) 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.	N/A	2			1) Tank pressure and temperature sensors may detect pressure fluctuations due to temperature excursions; 2) Pump delta-p sensor and/or 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	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 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 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			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-LV1-4	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	All	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			1) Pump delta-p sensor detects loss of flow; 2) Loop temp sensors detect loss of cooling				

				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**	**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																				
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 N2 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 N2 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 N2 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 N2 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	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	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			Observable	How Observed?	Tlm for Diagnosis	Tlm Path for Diagnosis	Time to Detect (Local)	Time to 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			1) Tank pressure and temperature sensors detect loss of coolant 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	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 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-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	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.	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			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-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	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 sensor detects loss of flow; 2) Loop temp sensors detect loss of cooling 3) Position indicator on LV 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.	Valve closes when not commanded to close	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			1) Pump delta-p sensor detects loss of flow; 2) Loop temp sensors detect loss of cooling 3) 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.	N/A	2			1) Tank pressure and temperature sensors detect loss of coolant; 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-LV3-1	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	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 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.	External leakage, downstream 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 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-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 can 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 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				

				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	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
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	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-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			
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-LV2-4	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-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-CV1-4	Pump check valve	Check valve prevents back flow through the inactive pump leg	External Leakage	Seconds/minutes					N/A	None										

						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)
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	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-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 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.	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			1) Tank pressure and temperature sensors detect loss of coolant; 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				
Telecomm																	
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.	N/A	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 process 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	Yes. (After process of elimination)	Ground would see lower power or corrupted signal	None Loss of comm with HGA	None	None	None
Mech																	
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	1) 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)	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	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	1) incorrect potentiometer reading 2) residual torque (should have sufficient margin) 3) 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)	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	Solar Array Flap Actuator		Actuates when not commanded	Holding torque exceeded (need to have sufficient margin)	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)	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	?	?

				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**	**Remediation**	**Helpful Autonomy Rule**	**Revisit**	**Comments - KAF**
TCS-PM1-4	Pump 1	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	Minutes					N/A	None								X		
TCS-PM1-5	Pump 1	Provides coolant flow through the solar arrays and radiators	Overcurrent	Seconds					N/A	None								X		
TCS-PM1-8	Pump 1	Provides coolant flow through the solar arrays and radiators	External leakage	Seconds/minutes					N/A	None										
TCS-PM2-4	Pump 2	Provides coolant flow through the solar arrays and radiators	Pump/motor overheat	Minutes					N/A	None								X		
TCS-PM2-5	Pump 2	Provides coolant flow through the solar arrays and radiators	Overcurrent	Seconds					N/A	None								X		
TCS-PM2-8	Pump 2	Provides coolant flow through the solar arrays and radiators	External leakage	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 leakage to exterior.	External leakage, tank side	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							
Mech																				
ME-1.1.1.1.a	Solar Array Flap Actuator		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	?	?	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???	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, 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 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				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

						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-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)	C	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	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)	L	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 commanded	1) bad/bound bearing/mechanical failure 2) stepper motor failure 3) loose/separated connector	C	Solar array stuck in position	1) generates insufficient power 2) generates too much power 3) feathering makes it impossible for array to retract sufficiently for encounter	1) eventually drain battery, may be able to slew s/c to retain partial power for a time; cooling system might get too cold 2) overheat cooling system 3) lose mission	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	1) incorrect potentiometer reading 2) residual torque (should have sufficient margin) 3) Motor coil or winding is open	C	Solar array in incorrect position	1) generates insufficient power 2) generates too much power 3) feathering makes it impossible for array to retract sufficiently for encounter	1) eventually drain battery, may be able to slew s/c to retain partial power for a time; cooling system might get too cold 2) overheat cooling system 3) lose mission	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)	C	Solar array in incorrect position	1) generates insufficient power 2) generates too much power 3) feathering makes it impossible for array to retract sufficiently for encounter	1) eventually drain battery, may be able to slew s/c to retain partial power for a time; cooling system might get too cold 2) overheat cooling system 3) lose mission	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	Solar Array Feather Actuator		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	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-1.2.1.a	HGA Gimbal		Fails to actuate when commanded (mechanical failure)	1) 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 (~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	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.	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	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	1) Frangibolt fails to release completely (mechanical failure of frangibolt) 2) Separation interfaces fail to release completely (mechanical clearance issues/unexpected interferences)	C	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	L	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)	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				

				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**	**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	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	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 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	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				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		
Inputs	Solar Array Feather Actuator		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	?	?	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-1.2.1.a	HGA Gimbal		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	?	?	None				re-command, slew	command to a "safe" position		
ME-1.2.1.b	HGA Gimbal		Fails to actuate when commanded (electrical 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	?	?	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)																X	

FMEA ID	Name	Function	Failure Mode / Limit / Constraint	Possible Causes	Phase	Effect				Severity	Type of FM	Detection Method					
						Local	Next Higher	Mission	Umbra Violation			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 solar pressure, etc. Science team may see thermal effects.				
Inputs	MAG Boom		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 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)	Mission-ending with complete loss of pressurant or if enough torque is applied	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	Mission-ending with complete loss of fuel or if enough torque is applied	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-2.a	Tank		Internal leak (liquid into gas)	1) Physical damage (pinhole leak in diaphragm)		Unusable propellant that can't be pushed out of the tank	Less fuel overall	No effect until s/c runs out of usable fuel	N/A until s/c runs out of usable fuel	2	None	No	You'd run out of fuel early	No	N/A	N/A	N/A
PR-2.b	Tank		External leak (pressurant)	1) Physical damage		Leaking helium	Over time will decrease system pressure, may torque s/c (depends on size of leak)	Mission-ending with complete loss of pressurant 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-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	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	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	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		Couldn't use thruster	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			Couldn't use thruster	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		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	Yes	Component temperature change			N/A	
TH-1.2.a	High-temperature MLI		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	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 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	Remediation	Helpful Autonomy Rule	Revisit	Comments - KAF
ME-2.1.1.c	MAG Boom		Partial deployment																	
Inputs	MAG Boom		Electrical fault																	
Propulsion																				
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	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		
Input	Valve Assembly (NC Solenoid Valves)		Bus voltage															Cycle power to valves		
Thermal																				
TH-1.1.a	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)												