FMEA Ref.	Item	Potential failure mode	Potential cause(s) / mechanism	Mission phase	Local effects of failure	Next higher level effect	System-level end effect	(P) Probability (estimate)	(S) Severity	(D) Detection (indications to operator, maintainer)	Detection dormancy period	Risk level P*S*D
C.1.1	Cryocooler Failure	Coolant Contamination/Leakage	Air contamination in UHP bottles, Internal metal decay, He gas leakage at tube welding points	All	Mass flow rate of gas decreases	Cooling lift of the cryocooler decreases	Tank propellants boil-off	(2) Remote	(4) Critical	(2) Continous monitoring of gas flow sensors for cryocoolers	Actively monitor sensors	16 - Acceptable with proper measures
C.1.2		Structural Failure in Mount	Stress from vibrations and vehicle acceleration	All	Mount connections to tank become weaker	Mount detaches from the tank	Loss of cryocooling system from the tank results in propellant boil-off	(2) Remote	(5) Catastrophic	(1) Vibration testing will reveal weaknesses. Continuous monitoring.	Visual Inspection upon breaking	10 - Acceptable with proper measures
C.1.3		Individual Component Failure	Compressor stall or turbine blade corrosion/cracks	All	Compressor/Turbine becomes non-functional	Cooling loop flow becomes stagnant	He Gas heats up causing eventual propellant boil off	(4) Reasonably Possible	(2) Very Minor	(2) Continous monitoring of gas flow sensors for cryocoolers. Drastic changes in He mass flow rate	Visual Inspection prior to mounting. Actively monitor gas sensors	16 - Acceptable with proper measures
C.1.4		Pressure Vessel Explosion	Blocked or malfunctioning pressure relief valve/overpressurization	All	Components malfunction and ruins the mount's surface	Entire system becomes non-functional and the tanks heat up	Total System Loss	(3) Possible/Occassional	(5) Catastrophic	(1) Limited warning before the error since the explosion is sudden except with sensor alarming the system being	Actively monitor sensors for pressure, temperature and Helium	15 - Acceptable with proper measures
C.2.1	Tank Failure	Liner Cracking (titanium layer)	Hydrogen embrittlement from cryogenic exposure	Operation	Micro-cracks in liner	Increased permeability, potential leakage (primarily Hydrogen)	Loss of structural integrity, risk of explosion (catastrophic)	2	4	2	Weeks to months	16
C.2.2		Tank wall expansion/contraction	Thermal effects from cryogenics	All	Stress on materials	Fatigue or cracks	Liner deformation or burst	2	4	4	Weeks to months	32
C.2.3		CFRP Delamination	Poor resin bonding or cure	Any	Loss of CFRP structural integrity	Reduced Tank Strength	Loss of structural integrity, risk of explosion (catastrophic)	1	4	3	Weeks to months	12
C.2.4		Seals Failure	Small leaks (from cryogenic temperatures)	Operation	Gradual propellant loss	Reduced Efficiency (Flammable risk)	Fire/explosion hazzard	2	3	3	Weeks to months	18
C.3.1	Propellant Feed System Failure	Main actuated valve fails to open or partially opens	Mechanical jam, debris, or actuator electrical fault	Ignition	Starved flow to engine	Engine fails to ignite or underperforms	Mission abort or unstable burn	2	4	2	Seconds	16
C.3.2		Pressure transducer reads incorrect values	Sensor drift, ice blockage, connector fault	All	Inaccurate pressure readout	Pressurant controller reacts improperly	Over/under-pressurization	3	3	2	Minutes	18
C.3.3		Pressurant line regulator stuck open or incorrect set pressure	Ice blockage, diaphragm fatigue	Burn	LOX tank pressure too high or low	Feed pressure unstable	Engine underperforms or aborts	2	5	3	Seconds to minutes	30
C.3.4		Flow sensor fails or freezes	Condensation or icing in cryogenic line; electrical fault	Ignition / Burn	Flow not reported accurately	Cannot confirm propellant delivery rate	Risk of operating engine with wrong mixture ratio	2	4	3	Seconds	24
C.3.5		Check valve fails to open or leaks back	Debris, ice buildup, seal wear	All	Reverse flow into upstream lines	Pressurant backflows or tank pressure loss	Tank may depressurize unexpectedly	1	4	3	Minutes to hours	12
C.3.6		Purge line valve fails to open after burn	Actuator fault or command logic error	Post-Burn	Propellant left in feed lines after burn	Erosion of feed lines over time	Life expectancy and structural integrity of feed lines decreases	2	2	5	Weeks to months	20

Risk Category	Actions for further investigation / evidence	Mitigation / requirements	Category	Details	Required Actions	Explanation	Acceptability Reasoning	Acceptability Justification	Unacceptable Condition
		Ensure that tube welding is appropriately performed. Establish and follow a strict vacuum drying and purging process prior to He gas fill.	**Risk Level Range**	2 – 21	Active monitoring (sensors + inspection)	Failures in this range must be detected early to trigger response systems.	Elimination of all failure modes is impossible	Mechanical systems will always have some degree of risk due to complexity and material limits.	Severity = 5 (Catastrophic)
	Perform Tank/Cryo FEA	Allow for adequate mounting space on tank. Ensure structural supports on mount can withstand high-g's	**Acceptability Thresholds**	< 25: Acceptable	Redundancy or structural reinforcement where possible	Design measures to tolerate or delay failure are crucial here.	Structural integrity is finite	Materials under high-g loads will eventually fatigue or fail—only mitigation is possible.	Probability = 4 or 5 (Likely/Frequent)
		Implement a redundant cryocooler system that kicks in upon failure		**NOTE: If the severity is catastrophic, but the risk level is acceptable, explain why it is "Acceptable with Proper Measures"**	Failure mitigation must limit system impact	Backup cooling, pressure relief systems, and fail-safes must engage automatically.	Full redundancy is not feasible	A second cryocooler would increase mass and reduce efficiency—must compromise between reliability and design constraints.	Detection = 1 (No early warning)
		Redundant Helium K-bottles to act as a pressure regulator within the tubing of the component connections		26-50: Marginally Acceptable/Borderline, Requires Strong Justification			Detection systems aren't foolproof	Failures can happen faster than sensors or human inspection can react.	Combined Risk (P × S) + D > 15
				> 50: Unacceptable			**Conclusion**	**We have to accept this risk range with the best engineering responses—we have no alternative.**	
Acceptable	Material testing/stress analysis	Pre-treating could be a solution. This is acceptable for now as long term effects are hard to quantify until extensive testing is feasible.							
Marginally acceptable	Thermal cycle testing	Test validation is a possible solution. This could also be modeled using finite element analysis and updated after results are found							
Acceptable	Monitor wrapping or curing process	Validate manufacturing process							
Acceptable	Leak detection/seal permeability tests	Redundant seals or leak detection systems							
Acceptable	Pre-flight valve cycling tests	Use dual-redundant actuation or valve health feedback							
Acceptable	Pressure sensor calibration & drift validation	Redundant pressure sensors with cross-checking logic							
Marginally acceptable	Regulator dynamic response testing	Use redundant regulators in parallel with check valves							
Acceptable	Sensor thermal qualification and EMI testing	Use redundant or backup flow verification (temperature gradient, pressure drop)							
Acceptable	Backflow testing during pre-flight check	Install dual check valves or add isolation valve							
Acceptable	Test valve isolation logic	Add purge valve lockout logic post-start							

Explanation	Mitigation Strategy	Effect on Risk
Explosion, total vehicle/system loss, or crew hazard—must be fully prevented.	Reduce **Probability (P)**	Enhanced venting, better pressure relief, more rigorous testing for blockage resistance.
Indicates high likelihood of failure during the mission lifecycle.	Reduce **Severity (S)**	Redirect failure modes into safe paths using burst discs, isolators, or segmented pressure zones.
Inability to detect pressure or thermal failure in time leads to disaster.	Improve **Detection (D)**	Add redundant sensors, faster warning systems, and more responsive fail-safe logic.
Risk is too high for acceptable design—it exceeds system tolerance even with mitigations.	Example: Mitigation reduces risk from 17 to 12	Still borderline. Further structural or procedural redesign needed to push down to ≤11.