List of Safety Goals

ID	*Name*	*Safe State*	*ASIL*	*Fault Tolerant Time Interval*	*Warning & Degradation Concept*	*Necessary Driver Actions*	*Emergency Operation Time Interval*	*Contributing requirements*	*Single-Point Fault Metric Target Achieved*	*Latent Fault Metric Target Achieved*	*Diagnostic Coverage Worksheets*	*PMHF in FIT*	*PMHF*	*FTA for PMHF*

G001	Prevent exposure to high voltage	Put battery in "Safe" state and prevent battery restart until service	D			- Pull vehicle on a side - Turn off vehicle - Put vehicle in "safe state" - Evacuate vehicle without touching metallic parts		• [SR001] [a] Prevent exposure to unintended high voltage to passengers, drivers, and other nearby people • [SR002] [b] Detect presence of unintended high-voltage / leakage • [SR003] [c] Safe state: Completely disa	• No	• No		No fault tree selected for PMHF		

								ble batt ery outp ut until vehi cle has been servi ced • [SR0 04] [e] Degr aded state : In case of dete ction of unin tend ed high volta ge, do not allo w vehi cle oper ation for mor e than xx kmp h / yy minu tes • [SR0 05] [d] Unin tend ed expo						

								sure to high voltage fault shall not exist in the system for more than xxx seconds • [SR006] [f, g] Notify driver with a warning indication within xxx seconds of detection of high voltage exposure risk • [SR007] [i] Fault through						

								Exposure to high voltage error shall override all other vehicle-level functions • [SR059] [h] The battery shall enter safe state in a maximum of xxx seconds						

G002	Prevent battery from operating outside SOA	Put battery in "protected state" until battery recovers	D			- Slow down the vehicle and pull vehicle on a side - Put vehicle in "safe state" -> Emergency Disconnect button is engaged - Evacuate the vehicle - Wait until battery reports recovery		• [SR012] Prevent battery from operating outside temperature SOA • [SR013] Prevent battery from operating outside voltage SOA • [SR014] Ptrevent battery from operating outside current SOA • [SR056] Prevent battery from operating outsi	• No	• No		No fault tree selected for PMHF		

								de Pressure SOA							

G003	Prevent incorrect vehicle operation due to unreliable transmission or reception of critical hardware and software signals.	Limit battery current draw	D			- Slow down the vehicle - Do not exceed vehicle speed beyond "safe speed" until fault recovers		• [SR051] [a] Provide alternate path of communication for critical signals • [SR052] [b] Provide mechanism to detect faulty hardware and software signals • [SR053] [c, e] Transition vehicle to limp mode upon detection	• No	• No		No fault tree selected for PMHF		

								of faulty signals • [SR054] [d] Fault tolerance (TBD) • [SR055] [f] Notify driver upon encountering communication failures						