

List of Safety Requirements

Nº	ID	Name	Description	Kind	A	Time constraints	Physical constraints	Co	Trace FTA Event	Start	Relat. Goal.	Contrib. To	Contrib. To	Allocations
1	SR	[NOTIFY] Notify the driver / passengers about presence of unintended HV or leakage		FUN	A				no traced events	PRC	• G003 (ASIL A)	• SR227 (ASIL A)		• Master Controller • Master Controller (ASIL B)
2	SR	Prevent battery from operating outside temperature SOA		FUN	B				no traced events	PRC	• G004 (ASIL B)	• SR035 (ASIL B) • SR010 (ASIL B) • SR011 (ASIL B) • SR013 (ASIL B)		
3	SR	Prevent battery from operating outside voltage SOA		FUN	B				no traced events	PRC	• G004 (ASIL B)	• SR037 (ASIL B) • SR008 (ASIL B) • SR013 (ASIL B) • SR010 (ASIL B) • SR073 (ASIL B)		
4	SR	Prevent battery from operating outside current SOA		FUN	B				no traced events	PRC	• G004 (ASIL B)	• SR038 (ASIL B) • SR014 (ASIL B) • SR015 (ASIL B) • SR013 (ASIL B)		

5	SR	[DETECTION TIMING] Detect impending or occurrence of gassing or TR within xxx seconds of first occurrence	The BMS shall continuously monitor battery status to detect / predict an impending gassing or thermal runaway event.	FUN	B			no traced events	PRC	• G002 (ASIL A) • G004 (ASIL B) • SR009 (ASIL B) • SR334 (ASIL D) • SR243 (ASIL B)	• SR017 (ASIL B) • SR009 (ASIL B) • SR246 (ASIL B)	• Master Controller (ASIL B) • AFEs (ASIL B)
6	SR	[DETECT] Continuously monitor individual series cell voltages		FUN	B			no traced events	PRC	• G004 (ASIL B) • SR021 (ASIL B) • SR049 (ASIL B)	• SR004 (ASIL B) • SR049 (ASIL B)	
7	SR	[DEGR TR SS] Temporarily disconnect the battery if fault has been detected		FUN	B			no traced events	PRC	• G004 (ASIL B) • SR254 (ASIL B) • SR257 (ASIL B) • SR260 (ASIL B) • SR263 (ASIL B) • SR002 (ASIL B)	• SR003 (ASIL B) • SR004 (ASIL B) • SR049 (ASIL B)	
8	SR	[DETECT] Continuously monitor battery temperature		FUN	B			no traced events	PRC	• G004 (ASIL B) • SR009 (ASIL B)	• SR003 (ASIL B)	
9	SR	[AVOID] Provide battery performance limits to connected loads and sources		FUN	B			no traced events	PRC	• G004 (ASIL B) • SR031 (ASIL B) • SR032 (ASIL B) • SR033 (ASIL B)		

10	SR	[NOTIFY] Notify the driver and passengers about fault and warning condition related to battery or cells		FUN B			no traced events	PRC	• G004 (ASIL B) • SR037 (ASIL B) • SR046 (ASIL B) • SR038 (ASIL B) • SR059 (ASIL B)	• SR035 (ASIL B) • SR004 (ASIL B) • SR010 (ASIL B) • SR005 (ASIL B) • SR049 (ASIL B)	• SR003 (ASIL B)	
11	SR	[DEGR TR SS] Disconnect the battery if over-current fault has been detected	The BMS shall disconnect the battery within a stipulated time period of occurrence of the gassing event.	FUN B			no traced events	PRC	• G004 (ASIL B) • SR310 (ASIL B) • SR002 (ASIL B)	• SR266 (ASIL B) • SR005 (ASIL B)	• SR005 (ASIL B)	
12	SR	[DETECT] Continuously monitor battery current		FUN B			no traced events	PRC	• G004 (ASIL B) • SR314 (ASIL B)	• SR028 (ASIL B) • SR005 (ASIL B)	• SR005 (ASIL B)	
13	SR	[TIMING TOL DETECT] Detect HV exposure fault within xxx seconds of its occurrence		FUN A			no traced events	PRC	• G003 (ASIL A)	• SR000 (ASIL A)		<ul style="list-style-type: none"> • Master Controller • Slave module(s) • BJB sensor • Master Controller (ASIL B) • AFEs (ASIL B)
13.1	SR			UNSA			no traced events	PRC	• G003 (ASIL A)			

14	SR	[DEGR SS] Permanent disconnect the battery from the external HV bus	While the goal is derived from ASIL A requirement it is assigned ASIL B because: the functional implementation of such requirement might (or might not) be through same mechanism which implement other such requirement such as SR040.	FUN	B				no traced events	PRC	• G002 (ASIL A) • B) • G003 (ASIL A) • B) • G004 (ASIL B) B)	SR232 (ASIL B) SR243 (ASIL B) SR002 (ASIL B)		
15	SR	Protect battery from accelerated aging and wear	Balancing of cells is required for optimal battery operation during charge and discharge cycles. An unbalanced battery will not contain the energy designed for and will experience accelerated aging and increased ware.	FUN	B				no traced events	PRC	• G004 (ASIL B) B) • SR013 (ASIL B) • SR010 (ASIL B) • SR051 (ASIL B)	SR008 (ASIL B) SR013 (ASIL B) SR010 (ASIL B) SR051 (ASIL B)		

16	SR	Balance the battery	The BMS shall balance the unbalanced cells in the battery when cell voltage imbalance between the cell with highest voltage and the one with lowest voltage exceeds xxx mV.	FUN	B			no traced events	PRC	• G004 (ASIL B) • SR047 (ASIL B) • SR313 (ASIL B) • SR323 (ASIL B)	• SR049 (ASIL B)	
17	SR	Maintain proper BMS operation	The BMS shall include methods for ensuring the intended operation	FUN	B			no traced events	PRC	• SR130 (ASIL B) • SR061 (ASIL B) • SR223 (ASIL B) • SR092 (ASIL B) • SR216 (ASIL B) • SR220 (ASIL B) • SR283 (ASIL B) • SR285 (ASIL B) • SR304 (ASIL B) • SR288 (ASIL B) • SR306 (ASIL B)		

18	SR	[DETECT] Continuously monitor battery voltage		FUN	B			no traced events	PRC	• G004 (ASIL B)	• SR050 (ASIL B)	• SR004 (ASIL B)	
19	SR	Protect BMS against internal communication errors	The BMS shall implement detection and correction mechanism for internal communication failures between various hardware units on the board.	FUN	B			no traced events	PRC	• G004 (ASIL B)	• SR270 (ASIL B)	• SR249 (ASIL B)	
20	SR	Prevent BMS from operating outside SOA		FUN	B			no traced events	PRC	• G004 (ASIL B)	• SR250 (ASIL B)	• SR249 (ASIL B)	
21	SR	[AVOID DET] Continuously monitor BMS state for internal faults		FUN	B			no traced events	PRC	• G004 (ASIL B)	• SR118 (ASIL B)	• SR248 (ASIL B)	

22	SR	[SS] Transition system into safe state upon encountering critical faults		FUN	B			no traced events	PRC	• G004 (ASIL B)	• SR101 (ASIL B)	• SR075 (ASIL B)	• SR278 (ASIL B)	• SR132 (ASIL B)	• SR213 (ASIL B)	• SR121 (ASIL B)	
23	SR	[NOTIFY] the driver against BMS faults or warnings		FUN	B			no traced events	PRC	• G004 (ASIL B)	• SR087 (ASIL B)	• SR095 (ASIL B)	• SR277 (ASIL B)	• SR161 (ASIL B)	• SR168 (ASIL B)	• SR207 (ASIL B)	• SR267 (ASIL B)
24	SR	[NOTIFY] Notify driver about gassing or thermal runaway event within xxx seconds of detection		FUN	B			no traced events	PRC	• G002 (ASIL A)	• SR246 (ASIL B)	• G004 (ASIL B)	• SR251 (ASIL B)				
25	SR	Ensure BMS components operate in their safe operating temperature limits		TEC	B			no traced events	PRC	• G004 (ASIL B)			• SR248 (ASIL B)				