List of Safety Requirements

N°	*ID*	*Name*	*Description*	*Kind*	*ASIL*	*Time constraint*	*Physical constraint*	*Comment*	*Traced FTA Events*	*Status*	*Related Goals*	*Contributions*	*Contributes To*	*Allocations*
1	SR020	Insulation resistance measurement performance	The BMS shall measure insulation resistance with range at least of xxx to xxx Mohm with accuracy of +- xxx Mohm at most and resolution of xxx Mohm at most and a sampling rate of at least xxx sample/sec	TECHNICAL	A				no traced events	PROPOSED		• SR341 (ASIL D) • SR343 (ASIL D)	• SR013 (ASIL A)	• Insulation Monitoring • BJB IC • MCU • TPL Transciever
2	SR022	HV switch timing	The BMS shall be able to open and close the HV switches of the battery	TECHNICAL	B				no traced events	PROPOSED		• SR243 (ASIL B)	• SR015 (ASIL B) • SR011 (ASIL B) • SR007 (ASIL B)	• FET / Contactor Driver (ASIL B) • MCU

2.1	SR023	Current Integrator HV switch timing	The BMS shall be able to open and close the HV switches of the battery upon a Current Integrator signal assignment within xxx ms and xxx ms respectively, preferably implemented in HW	TECHNICAL	B				no traced events	PROPOSED				• FET / Contactor Driver (ASIL B) • Short-circuit detection • FET / Contactor
3	SR024	Gas and/or pressure measurement performance	The BMS shall measure xxx gas(es) with at least range of xxx to xxx PPM with accuracy of +- xxx PPM at most and resolution xxx PPM at most and/or pressure with at least range of xxx to xxx bar at most with accuracy of xxx bar and resolution of xxx bar at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED		• SR346 (ASIL D) • SR347 (ASIL D)	• SR027 (ASIL B)	• MCU

4	SR025	Battery temperature measurement performance	The BMS shall measure battery temperature with at least range of xxx to xxx C° with accuracy of +- xxx C° at most and resolution xxx C° at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED		• SR353 (ASIL D) • SR354 (ASIL D)	• SR008 (ASIL B) • SR005 (ASIL B)	• MCU • AFE • TPL Transciever
5	SR027	TR detection algorithm	The BMS shall include an algorithm to predict TR event based on temperature and gases and/or pressure within xxx sec from it’s occurrence	TECHNICAL	B				no traced events	PROPOSED		• SR024 (ASIL B) • SR362 (ASIL D) • SR363 (ASIL D) • SR364 (ASIL D)	• SR005 (ASIL B)	• MCU

6	SR034	Cell voltages monitor performance	The BMS shall measure cell voltages with range at least of xxx to xxx V with accuracy of +-xxx mV at most and resolution of xxx mV at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED		• SR365 (ASIL C(D)) • SR366 (ASIL D)	• SR006 (ASIL B)	• MCU • AFE • TPL Transciever
7	SR036	Battery current monitor performance	The BMS shall measure battery current with range at least of xxx to xxx A with accuracy of +-xxx A at most and resolution of xxx A at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED		• SR381 (ASIL D) • SR382 (ASIL D) • SR030 (ASIL B)	• SR012 (ASIL B)	• MCU • BJB IC • TPL Transciever

8	SR039	Dynamic Current Limit message	The BMS shall compose and transmit a periodical message containing the maximum recommended discharging current, and charging current, as calculated by the Dynamic Current Limit	TECHNICAL	B				no traced events	PROPOSED		• SR394 (ASIL D) • SR536 (ASIL D)	• SR009 (ASIL B)	• MCU • CAN Transciever
9	SR040	DCL_STATUS: OVERLOAD	The BMS shall set the Flag DCL_STATUS to OVERLOAD in case the Dynamic Current Limit algorithm detects further increase in temperature due to overload	TECHNICAL	B				no traced events	PROPOSED			• SR009 (ASIL B)	• MCU

10	SR041	DCL_STATUS: NORMAL	The BMS shall set the Flag DCL_STATUS to NORMAL if the Dynamic Current Limit algorithm does not detect an overload during a time period as specified in the configuration parameter DCL_OVERLOAD_TIMEOUT	TECHNICAL	B				no traced events	PROPOSED			• SR009 (ASIL B)	• MCU

11	SR042	Set flags when system is outside of, or about to breach temperature SOA condition		TECHNICAL	B				no traced events	PROPOSED		• SR482 (ASILD) • SR486 (ASILD) • SR499 (ASILD) • SR143 (ASILB) • SR491 (ASILD) • SR495 (ASILD) • SR503 (ASILD) • SR507 (ASILD) •	• SR002 (ASILB) • SR010 (ASILB)	• MCU

												SR 505 (ASILD)		

12	SR043	Set flags when system in is outside of, or about to breach cell voltage SOA condition		TECHNICAL	B				no traced events	PROPOSED		• SR148 (ASIL B) • SR512 (ASIL D) • SR516 (ASIL D) • SR519 (ASIL D) • SR522 (ASIL D) • SR527 (ASIL D) • SR525 (ASIL D) • SR529 (ASIL D) •	• SR003 (ASIL B) • SR010 (ASIL B)	• MCU

												SR 53 1 (ASILD)		

13	SR044	Set flags when system in is outside of, or about to breach current SOA condition		TECHNICAL	B				no traced events	PROPOSED		• SR149 (ASIL B) • SR150 (ASIL B) • SR151 (ASIL B) • SR152 (ASIL B) • SR153 (ASIL B) • SR154 (ASIL B) • SR155 (ASIL B) • SR156 (ASIL B)	• SR004 (ASIL B) • SR010 (ASIL B)	• MCU

14	SR045	Set flags when battery is out of balance		TECHNICAL	B				no traced events	PROPOSED		• SR053 (ASIL B) • SR054 (ASIL B) • SR055 (ASIL B) • SR056 (ASIL B)	• SR010 (ASIL B)	• MCU
15	SR046	Start balancing battery	The BMS shall balance the cells while the Flag CELL_BALANCE_STATUS is in state UNBALANCE	TECHNICAL	B				no traced events	PROPOSED			• SR016 (ASIL B)	• MCU • AFE • TPL Transciever

16	SR047	Battery voltages monitor performance	The BMS shall measure battery voltage with range at least of 0 to xxxV with accuracy of xxx mV at most and resolution of xxxmV at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED		• SR398 (ASIL D) • SR400 (ASIL D)	• SR018 (ASIL B)	• MCU • BJB IC • TPL Transciever
16.1	SR048	Battery voltages monitor range	The BMS shall measure battery voltage with range at least of 0 to xxxV	UNSPECIFIED	B				no traced events	PROPOSED				
16.2	SR049	Battery voltages monitor accuracy		UNSPECIFIED	D				no traced events	PROPOSED				

17	SR050	Set flags when system in is outside of, or about to breach battery voltage SOA condition		TECHNICAL	B				no traced events	PROPOSED		• SR077 (ASIL B) • SR078 (ASIL B) • SR079 (ASIL B) • SR080 (ASIL B) • SR081 (ASIL B)	• SR010 (ASIL B)	• MCU
18	SR057	Protect against faulty measurement spikes by filtering		TECHNICAL	B				no traced events	PROPOSED		• SR408 (ASIL D) • SR409 (ASIL D)	• SR017 (ASIL B)	• MCU

18.1	SR058	Filter measurement	The BMS shall include filters for all measurements to filter out data spikes xxx	TECHNICAL	B				no traced events	PROPOSED				• MCU
18.1.1	SR059	Detect out-of-range battery voltage measurements		TECHNICAL	B				no traced events	PROPOSED				• MCU
18.1.2	SR060	Detect out-of-range current measurements		TECHNICAL	B				no traced events	PROPOSED				• MCU
18.1.3	SR061	Detect out-of-range temperature measurements		TECHNICAL	B				no traced events	PROPOSED				• MCU
18.1.4	SR063	Detect out-of-range cell voltage measurements		TECHNICAL	B				no traced events	PROPOSED				• MCU

19	SR064	Temporary disconnect the battery if overtemperature has been detected in BMS		TECHNICAL	B				no traced events	PROPOSED		• SR401 (ASIL D) • SR410 (ASIL D) • SR411 (ASIL D)	• SR028 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
19.1	SR065	Close switches at IC_TEMP_STATUS: NORMAL	The BMS shall assign signal(s) as to close the HV switches of the battery and charger upon Flag IC_TEMP_STATUS set to NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

19.2	SR074	Open switches at IC_TEMP_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag IC_TEMP_STATUS set to any of the following: - OVERTEMPERATURE_AFE - OVERTEMPERATURE_BJB - OVERTEMPERATURE_MCU - OVERTEMPERATURE_SBC - OVERTEMPERATURE_SHUNT - OVERTEMPERATURE_HVSWITCH	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
20	SR075	Notify driver and passengers about fault and warning condition of the HV Switch		TECHNICAL	B				no traced events	PROPOSED		• SR415 (ASIL D)	• SR029 (ASIL B)	• MCU

20.1	SR076	HV_SWITCH_STATUS: FAILURE	The BMS shall set the Flag HV_SWITCH_STATUS to FAILURE upon a detection of the event via the HV Switch failure detection algorithm. The parameters of this algorithm shall be stored in the configuration file	TECHNICAL	B				no traced events	PROPOSED				• MCU
20.2	SR082	HV_SWITCH_STATUS: NORMAL	The BMS shall set the Flag TR_STATUS to NORMAL upon clearing of the event via the HV Switch failure detection algorithm	TECHNICAL	B				no traced events	PROPOSED				• MCU

21	SR083	Protect BMS from undesired effects of uncontrolled uC power-down		TECHNICAL	B				no traced events	PROPOSED		• SR419 (ASIL D) • SR420 (ASIL D) • SR421 (ASIL D)	• SR017 (ASIL B)	• MCU • SBC (ASIL B)
21.1	SR084	Brownout		TECHNICAL	B				no traced events	PROPOSED				• MCU • SBC (ASIL B)

22	SR085	Notify the driver and passengers about BMS overtemperature		TECHNICAL	B				no traced events	PROPOSED		• SR072 (ASIL B) • SR071 (ASIL B) • SR070 (ASIL B) • SR069 (ASIL B) • SR068 (ASIL B) • SR067 (ASIL B) • SR066 (ASIL B)	• SR029 (ASIL B)	• MCU • CAN Transciever

23	SR086	Permanently disconnect the battery if Mosfets/ Contactor is faulty		TECHNICAL	B				no traced events	PROPOSED		• SR416 (ASIL D)	• SR028 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
23.1	SR654	SM: Recovery out of permanent failure shall only be possible through service station intervention.		TECHNICAL	B				no traced events	PROPOSED				
24	SR087	Continously monitor BMS internal temperatures		TECHNICAL	B				no traced events	PROPOSED			• SR026 (ASIL B)	• MCU • AFE • SBC (ASIL B) • BJB IC • TPL Transciever • Onboard thermistor[0..*]
24.1	SR088	IC die temperature measurements	The AFE, BJB, MCU, SBC main ICs of the BMS shall include internal temperature measurements to assess and prevent possible failures associated	TECHNICAL	B				no traced events	PROPOSED				• MCU • SBC (ASIL B) • BJB IC • AFE • TPL Transciever

24.1.1	SR089	Make BMS enter fault state in case of either of MCU, AFE, of SBC reaching high die temperatuure		TECHNICAL	B				no traced events	PROPOSED				
24.1.1.1	SR090	Recover BMS from fault state to normal state when temperatures are withing permissible operating range for each part on the BMS		TECHNICAL	B				no traced events	PROPOSED				
24.2	SR091	Shunt temperature measurement performance	The BMS shall measure Shunt temperature with at least range of xxx to xxx C° with accuracy of +- xxx C° at most and resolution xxx C° at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED				• MCU • Onboard thermistor[0..*] • TPL Transciever • BJB IC

24.3	SR092	HV Switch temperature measurement performance	The BMS shall measure HV Switch temperature with at least range of xxx to xxx C° with accuracy of +- xxx C° at most and resolution xxx C° at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED				• MCU • Onboard thermistor[0..*] • TPL Transciever • BJB IC
25	SR093	Perform BIST		TECHNICAL	B				no traced events	PROPOSED		• SR128 (ASIL B) • SR134 (ASIL B) • SR422 (ASIL D) • SR423 (ASIL D)	• SR026 (ASIL B)	• MCU • SBC (ASIL B) • AFE • BJB IC • TPL Transciever

25.1	SR094	IC self test	The AFE, BJB, MCU, SBC main ICs of the BMS shall include internal Build In Self Test (BIST) to assess and prevent possible random and latent failures	TECHNICAL	B				no traced events	PROPOSED				• AFE • MCU • SBC (ASIL B) • BJB IC • TPL Transciever
26	SR095	Continously monitor HV FETs voltages		TECHNICAL	B				no traced events	PROPOSED		• SR425 (ASIL D) • SR432 (ASIL D)	• SR026 (ASIL B)	• Insulation Monitoring • MCU • TPL Transciever • BJB IC
26.1	SR096	HV voltage measurement performance	The BMS shall measure both HV Switch voltages (HV input and output) with range at least of -xxx to xxxV with accuracy of xxx mV at most and resolution of xxxmV at most and a sampling rate of at least xxx sample/sec	TECHNICAL	B				no traced events	PROPOSED				• MCU • Insulation Monitoring • TPL Transciever • BJB IC

26.2	SR097	HV Switch failure detection algorithm	The BMS shall include an algorithm to detect failure of the HV Switch based on the input and output voltage measurements within xxx sec from it's occurrence	TECHNICAL	B				no traced events	PROPOSED				• MCU
26.2.1	SR098	Detect HV switch failure in short		TECHNICAL	B				no traced events	PROPOSED				• MCU
26.2.2	SR099	Detect HV switch failure in open		TECHNICAL	B				no traced events	PROPOSED				• MCU
27	SR100	Temporary disconnect the battery if external communication errors have been detected in BMS		TECHNICAL	B				no traced events	PROPOSED		• SR434 (ASIL D) • SR435 (ASIL D)	• SR028 (ASIL B) • SR121 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

27.1	SR101	Close switches at EXT_COM_STATUS: NORMAL	The BMS shall assign signal(s) as to close the HV switches of the charger and the battery upon a EXT_COM_STATUS to NORMAL within xxx ms	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
27.2	SR103	Close switches at EXT_COM_STATUS: WARNING or NORMAL	The BMS shall assign signal(s) as to close the HV switches of the battery and charger upon Flag EXT_COM_STATUS set to any of the following: - EXT_COM_WARN - NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

27.3	SR105	Open switches at EXT_COM_STATUS: TIMEOUT	The BMS shall assign signal(s) as to open the HV switches of the battery upon a EXT_COM_STATUS to TIMEOUT within xxx ms	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
27.4	SR106	Open switches at EXT_COM_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag EXT_COM_STATUS set to EXT_COM_FAILURE	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
28	SR107	Protect BMS from hanging		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• MCU • SBC (ASIL B)
28.1	SR108	Watchdog	The BMS shall be reset in case the Watchdog(s) did not receive periodic pulses as specified in configuration parameter(s)	TECHNICAL	B				no traced events	PROPOSED				• MCU • SBC (ASIL B)

29	SR109	Temporary disconnect the battery if bit-flip has been detected in memory		TECHNICAL	B				no traced events	PROPOSED			• SR028 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
29.1	SR110	Close switches at MEMORY_STATUS: WARN or NORMAL	The BMS shall assign signal(s) as to close the HV switches of the battery and charger upon Flag COM_STATUS set to any of the following: - MEMORY_ECC_WARN - NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
29.2	SR111	Open switches at MEMORY_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag MEMORY_STATUS set to MEMORY_ECC_FAILURE	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

30	SR112	Notify the driver and passengers about BMS external communication error		TECHNICAL	B				no traced events	PROPOSED		• SR436 (ASIL D)	• SR029 (ASIL B) • SR121 (ASIL B)	• MCU
30.1	SR113	- EXT_COM_FAILURE_TIMEOUT - COMS_STATUS: TIMEOUT	The BMS shall assign the Flag EXT_COM_STATUS to TIMEOUT upon failure to receive regular communication from external controller for a period equal to or greater than specified in configuration parameter EXT_COM_FAILURE_TIMEOUT presented in ms	TECHNICAL	B				no traced events	PROPOSED				• MCU

30.2	SR114	EXT_COM_STATUS: NORMAL	The BMS shall set the Flag EXT_COM_STATUS to NORMAL upon no CRC error nor EDC being necessary in external communication	TECHNICAL	B				no traced events	PROPOSED				• MCU
30.3	SR115	EXT_COM_STATUS: EXT_COM_WARN	The BMS shall set the Flag EXT_COM_STATUS to EXT_COM_WARN upon detected CRC error and successful correction of the error by the EDC in external communication	TECHNICAL	B				no traced events	PROPOSED				• MCU
30.4	SR116	EXT_COM_STATUS: EXT_COM_FAILURE	The BMS shall set the Flag EXT_COM_STATUS to EXT_COM_FAILURE upon detected CRC error and inability of the EDC to correct the error in external communication	TECHNICAL	B				no traced events	PROPOSED				• MCU

31	SR117	Notify driver and pesseng ers about internal memory errors	Memory bit-flip	TECHNICAL	B				no traced events	PROPOSED			• SR029 (ASIL B)	• MCU
31.1	SR118	MEMORY_STATUS: MEMORY_ECC_FAILURE	The BMS shall set the Flag MEMORY_STATUS to MEMORY_ECC_FAILURE upon detected of any memory error by the ECC and inability to correct it	TECHNICAL	B				no traced events	PROPOSED				• MCU
31.2	SR119	MEMORY_STATUS: MEMORY_ECC_WARN	The BMS shall set the Flag MEMORY_STATUS to MEMORY_ECC_WARN upon detected of any memory error by the ECC and successful correction of it	TECHNICAL	B				no traced events	PROPOSED				• MCU
31.3	SR120	MEMORY_STATUS: NORMAL	The BMS shall set the Flag MEMORY_STATUS to NORMAL upon no memory error beind detected bu the ECC of any memory	TECHNICAL	B				no traced events	PROPOSED				• MCU

32	SR121	Continously monitor BMS external communications		TECHNICAL	B				no traced events	PROPOSED		• SR112 (ASIL B) • SR100 (ASIL B) • SR437 (ASIL D) • SR439 (ASIL D) • SR440 (ASIL D)	• SR026 (ASIL B)	• MCU
32.1	SR122	EDC on external comunication	The external BMC communication shall include EDC to correct possible communication errors	TECHNICAL	B				no traced events	PROPOSED				• MCU

32.2	SR124	CRC on external comunication	The external BMS communication shall include CRC to detect possible communication errors	TECHNICAL	B				no traced events	PROPOSED				• MCU
32.3	SR125	Periodic external communication timers	The BMS shall keep timers associated to periodic communication packets with external controller and reset them for every packet that was successful received	TECHNICAL	B				no traced events	PROPOSED				• MCU
33	SR126	Implement ECC in all memories		TECHNICAL	B				no traced events	PROPOSED			• SR026 (ASIL B)	• MCU
33.1	SR127	ECC memory	All memory of used in the BMS shall include ECC	TECHNICAL	B				no traced events	PROPOSED				• MCU
34	SR128	Notify driver and passengers about BIST detected failure		TECHNICAL	B				no traced events	PROPOSED			• SR029 (ASIL B) • SR093 (ASIL B)	• MCU

34.1	SR129	IC_BIST_STATUS: BIST_FAILURE_SBC	The BMS shall set the Flag IC_BIST_STATUS to BIST_FAILURE_SBC upon inability of the SBC's BIST to complete successfully	TECHNICAL	B				no traced events	PROPOSED				• MCU
34.2	SR130	IC_BIST_STATUS: BIST_FAILURE_MCU	The BMS shall set the Flag IC_BIST_STATUS to BIST_FAILURE_MCU upon inability of the MCU's BIST to complete successfully	TECHNICAL	B				no traced events	PROPOSED				• MCU
34.3	SR131	IC_BIST_STATUS: BIST_FAILURE_BJB	The BMS shall set the Flag IC_BIST_STATUS to BIST_FAILURE_BJB upon inability of the BJB's BIST to complete successfully	TECHNICAL	B				no traced events	PROPOSED				• MCU

34.4	SR132	IC_BIST_STATUS: BIST_FAILURE_AFE	The BMS shall set the Flag IC_BIST_STATUS to BIST_FAILURE_AFE upon inability of the AFE's BIST to complete successfully //vtpl-dngsrvapp:50000/RM:user=db2amin;password={password};	FUNCTIONAL	B				no traced events	PROPOSED				• MCU
34.5	SR133	IC_BIST_STATUS: NORMAL	The BMS shall set the Flag IC_TEMP_STATUS to NORMAL upon completion of all BIST completed successfully	TECHNICAL	B				no traced events	PROPOSED				• MCU
35	SR134	Temporary disconnect the battery if BIST detected failure in BMS		TECHNICAL	B				no traced events	PROPOSED			• SR028 (ASIL B) • SR093 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

35.1	SR157	Close switches at IC_BIST_STATUS: NORMAL	The BMS shall assign signal(s) as to close the HV switches of the battery and charger upon Flag IC_BIST_STATUS set to NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
35.2	SR160	Open switches at IC_BIST_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag IC_BIST_STATUS set to any of the following: - BIST_FAILURE_AFE - BIST_FAILURE_BJB - BIST_FAILURE_MCU - BIST_FAILURE_SBC	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
36	SR161	Provide BMS with absolute time		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• MCU

36.1	SR162	Absolute time life	The BMS shall include an absolute timer that is self powered with sufficient energy to count time for up to xxx days from when the BMS was last powered	TECHNICAL	B				no traced events	PROPOSED				• MCU
36.2	SR163	Absolute time resolution	The BMS shall track absolute time with a resolution of seconds and an accuracy of xxx PPM	TECHNICAL	B				no traced events	PROPOSED				• MCU
37	SR164	Provide BMS counter for timestamped Reset events		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• MCU
37.1	SR165	Store RESET Count in NV memory	The BMS shall include sufficient NV memory to store the absolute time of the last boot and the RESET_COUNT Flag for at least 100 entries	TECHNICAL	B				no traced events	PROPOSED				• MCU

37.2	SR166	Access RESET Count	The BMS shall allow access of the RESET Count file in memory download mode	TECHNICAL	B				no traced events	PROPOSED				• MCU
38	SR167	Maintain proper operation at re-boot		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• MCU • CAN Transciever
38.1	SR168	Store configuration & Flags	The BMS shall include sufficient NV memory to store the configuration file and Flags	TECHNICAL	B				no traced events	PROPOSED				• MCU
38.2	SR169	Retrieve configuration & Flags at boot	At boot the BMS will retrieve the configuration and Flags from NV memory	TECHNICAL	B				no traced events	PROPOSED				• MCU
38.3	SR170	Program configuration & Flags	Configuration file and Flags in NV memory shall be able to be programmed by the BMS in configuration upload and Flag clearance mode respectively	TECHNICAL	B				no traced events	PROPOSED				• MCU • CAN Transciever

39	SR171	HV or leakage FAULT counter and FAILURE assignment	Keep a FAULT counter for the amount the insulation resistance measurement has been detected to be lower than a threshold. When the counter registers a certain amount assign a FAILURE.	TECHNICAL	A				no traced events	PROPOSED			• SR001 (ASIL A)	• MCU
39.1	SR172	HV_STATUS: FAULT	The BMS shall set the Flag HV_STATUS to FAULT upon a valid measurement of insulation resistance lower than specified in configuration parameter INS_RES_THR	TECHNICAL	A				no traced events	PROPOSED		• SR443 (ASIL D)		• MCU

39.2	SR173	HV_STATUS: NORMAL	The BMS shall set the Flag HV_STATUS to NORMAL upon a valid measurement of insulation resistance higher or equal than specified in configuration parameter INS_RES_THR	TECHNICAL	A				no traced events	PROPOSED		• SR442 (ASILD)		• MCU
39.3	SR174	HV_FAULT_COUNT HV_STATUS: FAILURE	The BMS shall keep a counter HV_FAULT_COUNT in Flag HV_STATUS of the times the Flag is assigned to FAULT and cleared again. Upon counting an amount equal to or higher than specified in configuration parameter HV_FAULT_COUNT_LIMIT the Flag HV_STATUS shall be set to FAILURE.	TECHNICAL	A				no traced events	PROPOSED		• SR444 (ASILD)		• MCU
39.3.1	SR175	Store HV_STATUS: HV_FAULT_COUNT	The BMS shall write in NV memory any update of the HV_FAULT_COUNT	TECHNICAL	A				no traced events	PROPOSED				• MCU

39.3.2	SR176	HV_STATUS Fault clearance	Once the system has entered HV_STATUS as fault, it shall only be cleared if a specific signal is received over CAN.	TECHNICAL	A				no traced events	PROPOSED				
39.4	SR177	Store failure count	The BMS shall store the faults in two counters: local and lifetime	TECHNICAL	A				no traced events	PROPOSED				
39.4.1	SR185	Keep track of lifetime fault counts	Lifetime counts shall be stored on non-volatile memory, and shall not be reset at any time.	TECHNICAL	A				no traced events	PROPOSED				

39.4.2	SR186	Local fault counter	Local faults shall be stored for xxx days, post which the counter shall be reset. This counter shall keep track of the number of faults occurred in the past xxx days. The BMS shall clear the local fault counter if no new fault is detected within xxx days of the previous one.	TECHNICAL	A				no traced events	PROPOSED				
39.4.2-1	SR187		The BMS shall clear the local fault counter if no new fault is detected within xxx seconds of the previous one.	TECHNICAL	A				no traced events	PROPOSED				
40	SR188	Permanent HV FAILURE disconnect	Open HV Switch at HV FAILURE and store in NV memory so the action is permamnent	TECHNICAL	B				no traced events	PROPOSED			• SR015 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

40.1	SR189	Open switches at HV_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag HV_STATUS set FAILURE	TECHNICAL	B				no traced events	PROPOSED		• SR449 (ASIL D)		• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
40.2	SR190	Store HV_STATUS: FAILURE	The BMS shall write in NV memory if Flag HV_STATUS set FAILURE	TECHNICAL	B				no traced events	PROPOSED		• SR447 (ASIL D)		• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
41	SR191	Permanent TR FAILURE disconnect	Open HV Switch at TR FAILURE and store in NV memory so the action is permamnent	TECHNICAL	B				no traced events	PROPOSED			• SR015 (ASIL B) • SR005 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
41.1	SR192	Open switches at TR_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag TR_STATUS set FAILURE	TECHNICAL	B				no traced events	PROPOSED		• SR451 (ASIL D)		• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
41.2	SR193	Store TR_STATUS: FAILURE	The BMS shall write in NV memory if Flag TR_STATUS set FAILURE	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

42	SR194	TR FAULT to FAILURE timeout	Upon detection of a FAULT by the TR detection algorithm initiate a timer. Upon elapsing of pre-programmed time assign a FAILURE	TECHNICAL	B				no traced events	PROPOSED		• SR005 (ASIL B)	• SR031 (ASIL B)	• MCU
42.1	SR195	TR_STATUS: FAULT	The BMS shall set the Flag TR_STATUS to FAULT upon a detection of the event via the TR detection algorithm. The parameters of this algorithm shall be stored in the configuration file	TECHNICAL	B				no traced events	PROPOSED				• MCU

42.2	SR196	TR_STATUS: NORMAL	The BMS shall set the Flag TR_STATUS to NORMAL upon clearing of the event if either of the conditions are met: 1. The TR detection algorithm indicates that no thermal runaway is present anymore 2. Reception of relevant signal over CAN	TECHNICAL	B				no traced events	PROPOSED				• MCU
42.3	SR197	TR_FAILURE_TIMEOUT, TR_STATUS: FAILURE	While on TR_STATUS on FAULT, the BMS shall initiate a timer of duration as specified in configuration parameter TR_FAILURE_TIMEOUT. On expiration of the counter TR_STATUS Flag shall be set to FAILURE if FAULT is still persisting	TECHNICAL	B				no traced events	PROPOSED				• MCU

43	SR198	Temporary disconnect the battery if fault has been detected related to temperature		TECHNICAL	B				no traced events	PROPOSED		• SR452 (ASIL D) • SR453 (ASIL D)	• SR007 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
44	SR199	Temporary disconnect the battery if fault has been detected related to cell voltages		TECHNICAL	B				no traced events	PROPOSED		• SR454 (ASIL D) • SR455 (ASIL D)	• SR007 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
45	SR200	Temporary disconnect the battery if fault has been detected related to battery voltage		TECHNICAL	B				no traced events	PROPOSED		• SR456 (ASIL D) • SR457 (ASIL D)	• SR007 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

46	SR201	Temporary disconnect the battery if fault has been detected related to high imbalance detected in the battery	The BMS shall set the signal(s) to _____ if the voltage imbalance (i.e. voltage difference) between cell(s) at the lowest voltage, and the cell(s) at the highest voltage exceeds xxx mV for atleast xxx ms duration.	TECHNICAL	B				no traced events	PROPOSED		• SR458 (ASIL D) • SR459 (ASIL D)	• SR007 (ASIL B)	• FET / Contactor Driver (ASIL B) • MCU • FET / Contactor
47	SR202	Temporary disconnect the battery if fault has been detected related to battery current		TECHNICAL	B				no traced events	PROPOSED			• SR011 (ASIL B)	• FET / Contactor Driver (ASIL B) • MCU • FET / Contactor

47.1	SR203	Open switches at BAT_CURR_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag BAT_CURR_STATUS set to any of the following: - OVERCURRENT_CHARGE - OVERCURRENT_DISCHARGE - SHORT_CHARGE - SHORT_DISCHARGE	TECHNICAL	B				no traced events	PROPOSED				• FET / Contactor Driver (ASIL B) • MCU • FET / Contactor
47.2	SR204	Close switches at BAT_CURR_STATUS: NORMAL	The BMS shall assign signal(s) as to close the HV switches of the battery upon Flag BAT_CURR_STATUS set to NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

48	SR205	Continously monitor BMS internal communications	The controller shall implement mechanisms to monitor the communication status, and detect anomalies between the following: 1. Controller to AFE(s) 2. Controller to current sensor IC 3. Controller to SBC 4. Controller to HV switches	TECHNICAL	B				no traced events	PROPOSED			• SR019 (ASIL B)	• MCU
48.1	SR206	CRC on internal comunication	The AFE to AFE and AFE, BJB, SBC to MCU communication shall include CRC to detect possible communication errors	TECHNICAL	B				no traced events	PROPOSED		• SR460 (ASIL D)		• MCU • SBC (ASIL B) • AFE • BJB IC
48.2	SR207	EDC on internal comunication	The AFE to AFE and AFE, BJB, SBC to MCU communication shall include EDC to correct possible communication errors	TECHNICAL	B				no traced events	PROPOSED				• MCU • BJB IC • SBC (ASIL B) • AFE

48.3	SR208	Periodic external communication timers	The BMS shall keep timers associated to periodic communication packets with external controller and reset them for every packet that was successful received	TECHNICAL	B				no traced events	PROPOSED		• SR462 (ASIL D)		• MCU
48.4	SR209	Periodic internal communication timers	The BMS shall keep timers associated to periodic internal communication packets between AFE, BJB, SBC to MCU and reset them for every packet that was successful received	TECHNICAL	B				no traced events	PROPOSED		• SR463 (ASIL D)		• MCU
48.5	SR210	Retry communication	The BMS shall retry internal communication xxx times in case internal communication failures are encountered	TECHNICAL	B				no traced events	PROPOSED				• MCU

48.5.1	SR211	The BMS shall raise flag COMM ERROR in case of continued failure	The BMS shall set flag COMM ERROR in case there is continued internal communication failure	TECHNICAL	B				no traced events	PROPOSED				• MCU
49	SR212	Notify the driver and passengers about BMS internal communication error		TECHNICAL	B				no traced events	PROPOSED		• SR466 (ASIL D)	• SR029 (ASIL B)	• MCU
50	SR213	Temporary disconnect the battery if internal communication is faulty		TECHNICAL	B				no traced events	PROPOSED		• SR464 (ASIL D) • SR465 (ASIL D)	• SR028 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

50.1	SR214	Open switches at INT_COM_STATUS: TIMEOUT	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag INT_COM_STATUS set to any of the following: - AFE_TIMEOUT - BJB_TIMEOUT - SBC_TIMEOUT	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
50.2	SR215	Close switches at INT_COM_STATUS: NORMAL	The BMS shall assign signal(s) as to close the HV switches of the charger and the battery upon a INT_COM_STATUS to NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

50.3	SR216	Open switches at COM_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag COM_STATUS set to any of the following: - COM_FAILURE_AFE_AFE - COM_FAILURE_AFE_MCU - COM_FAILURE_BJB_MCU - COM_FAILURE_SBC_MCU	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

50.4	SR217	Close switches at COM_STATUS: WARNING or NORMAL	The BMS shall assign signal(s) as to close the HV switches of the battery and charger upon Flag COM_STATUS set to any of the following: - COM_WARN_AFE_AFE - COM_WARN_AFE_MCU - COM_WARN_BJB_MCU - COM_WARN_SBC_MCU - NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor
51	SR218	Protect against SW errors by use of adecuate SW design approach		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• MCU

51.1	SR219	Use of 2-level software architecture	The software architecture shall be atleast 2-level, and can be based on the EGAS architecture concept.	TECHNICAL	B				no traced events	PROPOSED				• MCU
52	SR220	The BMS shall receive external commands and send external information over CAN		TECHNICAL	B				no traced events	PROPOSED		• SR467 (ASIL D) • SR468 (ASIL D) • SR469 (ASIL D) • SR470 (ASIL D)	• SR017 (ASIL B)	• MCU • CAN Transciever • FET / Contactor Driver (ASIL B) • FET / Contactor
52.1	SR221	Flags over CAN	The BMS shall periodically broadcast packets with all Flags	TECHNICAL	B				no traced events	PROPOSED				• MCU • CAN Transciever
52.2	SR222	E2E protected CAN	The BMS shall include E2E protected CAN communication	TECHNICAL	B				no traced events	PROPOSED				• MCU

52.3	SR223	Open HV switch	The BMS shall assign signal(s) as to open the HV switches of the charger and/or the battery upon a reception of valid command from the external controller including HV_SWITCH Flag to OPEN	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • CAN Transciever • FET / Contactor
52.4	SR224	Permanent Flag	The BMS shall store in NV memory Flags upon reception of special store request packet. Storing in NV memory shall only be allowed for Flags requiring open HV switches.	TECHNICAL	B				no traced events	PROPOSED				• MCU

52.5	SR225	Close HV switch	The BMS shall assign signal(s) as to close the HV switches of the charger and/or the battery upon a reception of valid command from the external controller including HV_SWITCH Flag to Close	TECHNICAL	B				no traced events	PROPOSED				• MCU • CAN Transciever • FET / Contactor Driver (ASIL B) • FET / Contactor
52.6	SR226	Prevent BMS failures related to production quality		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• Battery Management System
52.6.1	SR227	PCB manufacturing	Shall be class 2 or higher grade	TECHNICAL	B				no traced events	PROPOSED				• Battery Management System
53	SR228	The BMS shall keep track and act upon internal and external events		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• MCU

53.1	SR229	Flags	The BMS shall keep track of events that represent that current state of the BMS in digital representations called Flags	TECHNICAL	B				no traced events	PROPOSED				• MCU
54	SR230	The BMS shall provide means of measurement calibration		TECHNICAL	B				no traced events	PROPOSED			• SR017 (ASIL B)	• MCU
54.1	SR231	Store calibration	The BMS shall include sufficient NV memory to store the calibration data	TECHNICAL	B				no traced events	PROPOSED				• MCU
54.2	SR232	Retrieve configuration & Flags at boot	At boot the BMS will retrieve the calibration data from NV memory	TECHNICAL	B				no traced events	PROPOSED				• MCU
54.3	SR233	Program configuration & Flags	Calibration data in NV memory shall be able to be programmed by the BMS in calibration upload mode	TECHNICAL	B				no traced events	PROPOSED				• MCU • CAN Transciever

55	SR238	Temporary disconnect the battery if fault has been detected related to battery short circuit	Disconnect the battery if short-circuit is detected	TECHNICAL	B				no traced events	PROPOSED			• SR011 (ASIL B)	• MCU • FET / Contactor Driver (ASIL B) • Short-circuit detection • FET / Contactor
55.1	SR239	Close switches upon latch signal true	The BMS shall assign signal(s) as to close the HV switches of the battery upon either of the following conditions: 1. Elapsing of timer CURRENT_INTEGRATOR_OPEN_TIME held in configuration parameter in case Current Integrator error is relieved due to previous HV switch opening action 2. Reception of _____ signal over CAN	TECHNICAL	B				no traced events	PROPOSED				• MCU • FET / Contactor Driver (ASIL B) • Short-circuit detection • FET / Contactor

55.2	SR240	Short-circuit definition	The BMS shall assign signal(s) as to open the HV switches of the battery upon detecting instantaneous current higher than xxx A, within xxx us.	TECHNICAL	B				no traced events	PROPOSED				• FET / Contactor Driver (ASIL B) • Short-circuit detection • FET / Contactor
56	SR241	Stop balancing battery	The BMS shall stop balancing the cells while the Flag CELL_BALANCE_STATUS is in state STOP_BALANCING or in cases when balancing are not being met	TECHNICAL	B				no traced events	PROPOSED		• SR471 (ASIL D) • SR472 (ASIL D)	• SR0116 (ASIL B)	• MCU • AFE • TPL Transciever

57	SR242	Current integrator	The BMS shall be equipped with current integrator with SW selectable integration period of a range of xxx to xxx ms. In case the integration period is SW selectable the BMS shall select the value stored in configuration parameter.	TECHNICAL	B				no traced events	PROPOSED			• SR012 (ASIL B)	• MCU • Short-circuit detection
58	SR243	SW HV switch timing	Upon actuation signal provided, the HV switches shall not take more than xxx ms and xxx ms to open and close respectively.	TECHNICAL	B				no traced events	PROPOSED			• SR022 (ASIL B)	• FET / Contactor Driver (ASIL B) • MCU • FET / Contactor
59	SR244	AIS-156 and AIS_004 compliance		TECHNICAL	NONE				no traced events	PROPOSED				• Battery Management System
60	SR245	Provide protections for internal voltage faults	Provide protections for cases where isolation failure can occur (optocouplers, isolated transcievers, etc.)	TECHNICAL	B				no traced events	PROPOSED			• SR026 (ASIL B)	• Battery Management System

61	SR246	Set status to Unbalanced	The BMS shall set the CELL_BALANCE_STATUS to UNBALANCED if the cell voltage difference between the cell(s) with minimum voltage and those with maximum voltage exceeds xxx mV.	TECHNICAL	B				no traced events	PROPOSED		• SR474 (ASIL D)	• SR016 (ASIL B)	
62	SR247	The system shall use suitable sensors to detect thermal runaway		TECHNICAL	D				no traced events	PROPOSED			• SR005 (ASIL B)	
63	SR252	Open switches at HV_SWITCH_STATUS: FAILURE	The BMS shall assign signal(s) as to open the HV switches of the battery upon Flag HV_SWITCH_STATUS set to FAILURE	TECHNICAL	B				no traced events	PROPOSED		• SR477 (ASIL D) • SR478 (ASIL D)		• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

64	SR253	Close switches at HV_SWITCH_STATUS: NORMAL	The BMS shall assign signal(s) as to close the HV switches of the battery upon Flag HV_SWITCH_STATUS set to NORMAL if no other protections are activated that require open HV switches	TECHNICAL	B				no traced events	PROPOSED		• SR479 (ASIL D) • SR480 (ASIL D)		• MCU • FET / Contactor Driver (ASIL B) • FET / Contactor

65	SR312	[A] Continuously monitor battery voltage		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR251 (ASIL B) • SR260 (ASIL B) • SR257 (ASIL B) • SR104 (ASIL B) • SR269 (ASIL B) • SR282 (ASIL B) • SR548 (ASIL B) • SR561 (ASIL B) •	

													SR 559 (ASIL B)	
65.1	SR307	[A] Battery Voltage Monitoring Performance		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
65.1.1	SR308	[A] Battery Voltage Range	The BMS shall measure battery voltage with range at least of 0 to xxxV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR663 (ASIL D) • SR664 (ASIL D)		

65.1.2	SR309	[A] Battery Voltage Accuracy	The BMS shall measure battery voltage with accuracy of xxx mV, across operating temperature -25 degree celcius to 125 degree celcius	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR659 (ASIL D) • SR660 (ASIL D) • SR661 (ASIL D) • SR662 (ASIL D) • SR665 (ASIL D)		
65.1.3	SR310	[A] Battery Voltage Resolution	The BMS shall measure battery voltage with at most and resolution of xxxmV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR658 (ASIL D)		

65.1.4	SR311	[A] Battery Voltage Sampling	The BMS shall measure battery voltage at a sampling rate of at least xxx sample/sec.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR656 (QM) • SR657 (ASIL D)		

66	SR318	[A] Continuously monitor battery temperature		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR035 (ASIL B) • SR104 (ASIL B) • SR051 (ASIL B) • SR038 (ASIL B) • SR269 (ASIL B) • SR282 (ASIL B) • SR330 (ASIL B) • SR561 (ASIL B) •	

													SR 559 (ASIL B)	
66.1	SR313	[A] Battery Temperature Monitor		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
66.1.1	SR314	[A] Battery Temperature Range	The BMS shall measure battery Temperature with range at least of 0 to xxxV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
66.1.2	SR315	[A] Battery Temperature Accuracy	The BMS shall measure battery Temperature with accuracy of xxx mV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
66.1.3	SR316	[A] Battery Temperature Resolution	The BMS shall measure battery Temperature with at most and resolution of xxx °C	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
66.1.4	SR317	[A] Battery Temperature Sampling	The BMS shall measure battery Temperature vat a sampling rate of at least xxx sample/sec.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			

67	SR324	[A] Continuously monitor battery current.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR274 (ASIL B) • SR104 (ASIL B) • SR277 (ASIL B) • SR269 (ASIL B) • SR282 (ASIL B) • SR276 (ASIL B) • SR559 (ASIL B) • SR561 (ASIL B) •	

												SR 560 (ASIL D) • SR 583 (ASIL D) • SR 597 (ASIL B) • SR 599 (ASIL B)	
67.1	SR319	[A] Battery Current Monitor		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
67.1.1	SR320	[A] Battery Current Range	The BMS shall measure battery Current with range at least of 0 to xxxV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
67.1.2	SR321	[A] Battery Current Accuracy	The BMS shall measure battery Current with accuracy of xxx mV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			

67.1.3	SR322	[A] Battery Current Resolution	The BMS shall measure battery Current with at most and resolution of xxxmV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
67.1.4	SR323	[A] Battery Current Sampling	The BMS shall measure battery Current at a sampling rate of at least xxx sample/sec.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR666 (ASIL D) • SR668 (ASIL D) • SR669 (ASIL D)		
68	SR325	Sned data over UART		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR284 (ASIL B)	
69	SR326	Sned data over CAN		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR284 (ASIL B)	
70	SR329	[F] Send data over CAN to IPC		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR283 (ASIL B)	

71	SR334	[F] Send data over CAN within xxx msec after detection of temperature fault.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR123 (ASIL B)	
72	SR335	Sned data over CAN		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR271 (ASIL B)	
73	SR336	Sned data over CAN		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR248 (ASIL B)	
74	SR445	Sned data over UART		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR271 (ASIL B)	
75	SR446	Sned data over UART		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR248 (ASIL B)	
76	SR537	[E] BMS shall send max permisible charging and dichargi ng current limits every xxx sec.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR104 (ASIL B) • SR035 (ASIL B)	

77	SR538	[E] BMS shall send max permisible charging and dichargi ng current limits every xxx sec.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR266 (ASIL D) • SR269 (ASIL B) • SR251 (ASIL B)	
78	SR539	[E] BMS shall send max permisible charging and dichargi ng current limits every xxx sec.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR279 (ASIL D) • SR282 (ASIL B) • SR274 (ASIL B)	
79	SR542	[D] FHTI should be less than xxx sec[FTTI]		TECHNICAL	D				no traced events	PROPOSED				

80	SR549	[B] The rate of change of voltage must not be more than xxx mV/msec for more than yyy sec		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR548 (ASIL B)	
81	SR551	[B] The rate of change of voltage must not be more than xxx.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR330 (ASIL B)	
82	SR565	[C] Permanently disconnect the battery within xx msec of receiving the signal.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR556 (ASIL B) • SR560 (ASIL D) • SR552 (ASIL B)	

83	SR567	[F] Send data over CAN within xxx msec after detection of thermal runaway.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR564 (ASIL B)	
84	SR568	[G] Send data over CAN		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR555 (ASIL B)	
85	SR569	[G] Send data over UART		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR555 (ASIL B)	
86	SR570	[A] Continuously monitor cell voltage		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR571 (ASIL D)	• SR251 (ASIL B)	
87	SR571	[A] Cell Voltage Monitoring Performance		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR570 (ASIL D)	
87.1	SR572	[A] Cell Voltage Range	The BMS shall measure battery voltage with range at least of 0 to xxxV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			

87.2	SR573	[A] Cell Voltage Accuracy	The BMS shall measure battery voltage with accuracy of xxx mV, across operating temperature -25 degree celcius to 125 degree celcius	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
87.3	SR574	[A] Cell Voltage Resolution	The BMS shall measure battery voltage with at most and resolution of xxxmV.	TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)			
87.4	SR575	[A] Cell Voltage Sampling	The BMS shall measure cell voltage at a sampling rate of at least xxx sample/sec.	TECHNICAL	D				no traced events	ASSUMED	• G002 (ASIL B)			
88	SR576			TECHNICAL	D				no traced events	PROPOSED				

89	SR577	The BMS shall transition from the safe state to the operational state when the battery voltage remains below the overvoltage threshold of [XXX] V for a duration of [XXX] time, ensuring fault recovery conditions are met.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR268 (ASIL B)	

90	SR578	he BMS shall transition from the safe state to the operational state when the battery voltage remains above the undervoltage threshold of [XXX] V for a duration of [XXX] time, ensuring fault recovery conditions are met		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR267 (ASIL B)	

91	SR579	The BMS shall transition from the safe state to the operational state when the battery temperature remains above the undertemperature threshold of [XXX]°C for a duration of [XXX] time, ensuring fault recovery conditions are met.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR073 (ASIL B)	

92	SR580	The BMS shall transition from the safe state to the operational state when the battery temperature remains below the overtemperature threshold of [XXX]°C for a duration of [XXX] time, ensuring fault recovery conditions are met.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR102 (ASIL B)	

93	SR581	The BMS shall transition from the safe state to the operational state when the charging current remains below the overcurrent threshold of [XXX] A for a duration of [XXX] time, ensuring fault recovery conditions are met.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR281 (ASIL B)	

94	SR582	The BMS shall transition from the safe state to the operational state when the discharging current remains below the overcurrent threshold of [XXX] A for a duration of [XXX] time, ensuring fault recovery conditions are met.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR280 (ASIL B)	

95	SR584	[G] The BMS shall give warning to driver regarding the increasing temperature so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR616 (ASIL D) • SR617 (ASIL D)	• SR248 (ASIL B) • SR035 (ASIL B)	
96	SR585	[G] The BMS shall give warning to driver regarding the increasing voltage so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR612 (ASIL D) • SR613 (ASIL D)	• SR271 (ASIL B) • SR251 (ASIL B)	

97	SR586	[G] The BMS shall give warning to driver regarding the breach in current SOA so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR618 (ASIL D) • SR619 (ASIL D)	• SR284 (ASIL B) • SR274 (ASIL B)	
98	SR588	[C] The BMS shall transit to safe state within xxx msec after detecting under voltage fault signal.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR267 (ASIL B) • SR272 (ASIL B)	
99	SR589	[C] The BMS shall transit to safe state within xxx msec after detecting over voltage fault signal.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR268 (ASIL B) • SR272 (ASIL B)	

100	SR590	[C] The BMS shall transit to safe state within xxx msec after receiving under temperature fault signal.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR073 (ASIL B) • SR249 (ASIL B)	
101	SR591	[C] The BMS shall transit to safe state within xxx msec after receiving the over-current fault signal during discharging.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR281 (ASIL B) • SR285 (ASIL B)	
102	SR592	[C] The BMS shall transit to safe state within xxx msec after receiving the over-current fault signal during charging.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR280 (ASIL B) • SR285 (ASIL B)	

103	SR593	[C] The BMS shall transit to safe state within xxx msec after receiving the sort circuit fault signal.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR594 (ASIL D) • SR603 (ASIL B) • SR600 (ASIL B)	
104	SR595	Temporary disconnect recovery for SC		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR594 (ASIL D)	
105	SR328	[F] Send data over CAN within xxx msec after detection of current fault.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR283 (ASIL B)	
106	SR596	SM: Recovery out of permanent failure shall only be possible through service station intervention.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR556 (ASIL B)	

107	SR544	[B] The BMS shall detect under-voltage fault within xxx msec of occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR260 (ASIL B) • SR272 (ASIL B) • SR267 (ASIL B) • SR270 (ASIL B)	

108	SR587	[B] The BMS shall detect short circuit fault within xxx usec of occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR583 (ASIL D) • SR599 (ASIL B) • SR600 (ASIL B) • SR603 (ASIL B) • SR602 (ASIL B)	

109	SR566	[B] The BMS shall detect possibility of thermal runaway witihn xx msec of occurence of such conditions		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR561 (ASIL B) • SR556 (ASIL B) • SR552 (ASIL B) • SR564 (ASIL B)	
110	SR604	[G] The BMS shall give warning to driver regarding the increasing temperature so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR555 (ASIL B) • SR559 (ASIL B)	

111	SR605	[G] The BMS shall give warning to driver regarding the increasing current so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED				
112	SR606	[F] Send data over CAN within xxx msec after detection of sshort circuit.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR602 (ASIL B)	

113	SR607	[G] The BMS shall give warning to driver regarding the increasing temperature so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR614 (ASIL D) • SR615 (ASIL D)	• SR248 (ASIL B) • SR035 (ASIL B)	
114	SR608	[G] The BMS shall give warning to driver regarding the increasing voltage so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR610 (ASIL D) • SR611 (ASIL D)	• SR271 (ASIL B) • SR251 (ASIL B)	

115	SR609	[G] The BMS shall give warning to driver regarding the breach in current SOA so that the driver and can take precautionary actions and avoid the fault occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)	• SR621 (ASIL D) • SR620 (ASIL D)	• SR274 (ASIL B) • SR284 (ASIL B)	

116	SR610	The BMS shall trigger a warning to the driver when the battery voltage drops below the undervoltage warning threshold of [XXX] V for a duration of [XXX] time, allowing precautionary actions to be taken."		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR608 (ASIL D)	
117	SR611	The BMS shall clear the undervoltage warning when the battery voltage rises above [XXX] V and remains stable for [XXX] time.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR608 (ASIL D)	

118	SR612	The BMS shall trigger a warning to the driver when the battery voltage exceeds the overvoltage warning threshold of [XXX] V for a duration of [XXX] time, allowing precautionary actions to be taken.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR585 (ASIL D)	
119	SR613	The BMS shall clear the overvoltage warning when the battery voltage returns below [XXX] V and remains stable for [XXX] time.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR585 (ASIL D)	

120	SR614	The BMS shall trigger a warning to the driver when the battery temperature drops below the undertemperature warning threshold of [XXX]°C for a duration of [XXX] time, allowing precautionary actions to be taken.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR607 (ASIL D)	
121	SR615	The BMS shall clear the undertemperature warning when the battery temperature rises above [XXX]°C and remains stable for [XXX] time.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR607 (ASIL D)	

122	SR616	The BMS shall trigger a warning to the driver when the battery temperature exceeds the overtemperature warning threshold of [XXX]°C for a duration of [XXX] time, allowing precautionary actions to be taken.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR584 (ASIL D)	
123	SR617	The BMS shall clear the overtemperature warning when the battery temperature falls below [XXX]°C and remains stable for [XXX] time.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR584 (ASIL D)	

124	SR618	The BMS shall clear the charging overcurrent warning when the charging current remains below [XXX] A and stable for [XXX] time.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR586 (ASIL D)	
125	SR619	The BMS shall trigger a warning to the driver when the charging current exceeds the overcurrent warning threshold of [XXX] A for a duration of [XXX] time, allowing precautionary actions to be taken.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR586 (ASIL D)	

126	SR620	The BMS shall trigger a warning to the driver when the discharging current exceeds the overcurrent warning threshold of [XXX] A for a duration of [XXX] time, allowing precautionary actions to be taken.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR609 (ASIL D)	
127	SR621	The BMS shall clear the discharging overcurrent warning when the discharging current remains below [XXX] A and stable for [XXX] time.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR609 (ASIL D)	

128	SR622	SM: Recovery out of permanent failure shall only be possible through service station intervention.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR603 (ASIL B)	
129	SR545	[B] The BMS shall detect over-voltage fault within xxx msec of occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR257 (ASIL B) • SR272 (ASIL B) • SR268 (ASIL B) • SR270 (ASIL B)	
130	SR331	[F] Send data over CAN to IPC		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR270 (ASIL B)	

131	SR333	[F] Send data over CAN within xxx msec after detection of voltage fault.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR270 (ASIL B)	
132	SR332	[F] Send data over CAN to IPC		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR123 (ASIL B)	
133	SR543	[B] The BMS shall detect over-temperature fault within xxx msec of occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR038 (ASIL B) • SR249 (ASIL B) • SR123 (ASIL B) • SR102 (ASIL B)	

134	SR540	[B] The BMS shall detect under-temperature fault within xxx msec of occurence.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR051 (ASIL B) • SR249 (ASIL B) • SR123 (ASIL B) • SR073 (ASIL B)	
135	SR541	[C] The BMS shall transit to safe state within xxx msec after receiving over temperature fault signal.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR102 (ASIL B) • SR249 (ASIL B)	

136	SR547	[B] The BMS shall detect over-current fault within xxx msec of occurence during charging.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR277 (ASIL B) • SR283 (ASIL B) • SR285 (ASIL B) • SR280 (ASIL B)	
137	SR546	[B] The BMS shall detect over-current fault within xxx msec of occurence during dischargi ng.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR276 (ASIL B) • SR283 (ASIL B) • SR285 (ASIL B) • SR281 (ASIL B)	

138	SR623	SM: Bms shall implement method to detect and react to short circuit fault through hardware without requiring intervention of software.		TECHNICAL	D				no traced events	PROPOSED	• G002 (ASIL B)		• SR599 (ASIL B)	
139	SR624	In case of existance of any permanent failure, the system shall not recover		TECHNICAL	D				no traced events	PROPOSED				
140	SR625	The BMS shall implement the following states: "NORMAL", "SLEEP", "DEEPSLEEP", "WARNING", "FAULT". "FAULT_PERMANENT", "LIMP"		TECHNICAL	D				no traced events	PROPOSED		• SR626 (ASIL D)		

141	SR626	<TRANSITION between states>		TECHNICAL	D				no traced events	PROPOSED			• SR625 (ASIL D)	
142	SR627	SM: Inline controllable fuse / switch in series with mosfets	From FMEA: mosfets short	TECHNICAL	D				no traced events	PROPOSED				
143	SR628	SM: Mosfet control feedback mechanism		TECHNICAL	D				no traced events	PROPOSED				
144	SR629	SM: Precharge control feedback mechanism		TECHNICAL	D				no traced events	PROPOSED				
145	SR630	SM: measure voltage of different voltage rails		TECHNICAL	D				no traced events	PROPOSED				
146	SR631	SM: emergency operation FHTI definition	Software level 2 reaction time interval	TECHNICAL	D				no traced events	PROPOSED				
147	SR632	Reliability requirement: precharge resistor	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				

148	SR633	Reliability requirement: precharge mosfet	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
149	SR634	Reliability requirement:fuse	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
150	SR635	Reliability requirement: main mosfets	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
151	SR636	Reliability requirement: signal connectors	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
152	SR637	Reliability requirement shunt	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
153	SR638	Reliability requirement power connector	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
154	SR639	Access control		TECHNICAL	D				no traced events	PROPOSED				
155	SR640	cyber security		TECHNICAL	D				no traced events	PROPOSED				
156	SR641	Boot Loader		TECHNICAL	D				no traced events	PROPOSED				
157	SR642	Size		TECHNICAL	D				no traced events	PROPOSED				
158	SR643	Size		TECHNICAL	D				no traced events	PROPOSED				

159	SR644	Boot Loader		TECHNICAL	D				no traced events	PROPOSED				
160	SR645	Reliability requirement: precharge mosfet	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
161	SR646	cyber security		TECHNICAL	D				no traced events	PROPOSED				
162	SR647	Reliability requirement power connector	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
163	SR648	Access control		TECHNICAL	D				no traced events	PROPOSED				
164	SR649	Reliability requirement: signal connectors	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
165	SR650	Reliability requirement: precharge resistor	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
166	SR651	Reliability requirement:fuse	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
167	SR652	Reliability requirement: main mosfets	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				
168	SR653	Reliability requirement shunt	<move to BMS TSR>	TECHNICAL	D				no traced events	PROPOSED				