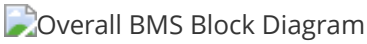
Assumptions of SEooC

Objective

This document is:

- To show the assumption on intended functionalities, and usage of the SEooC element.
- To show the assumption on the interaction with other elements external to this SEooC element(external safety mechanisms).
- To show the functional safety requirement assumptions on the SEooC element.
- The form basis for further correct implementation of assumed safety requirement.

Assumptions of System Architecture



Overall BMS Architecture

Block and interface description

Block Name	Function Description	ASIL
BM02A	HV battery pack supplies power for BM02A. BM02A is responsible for monitoring HV battery pack's cell voltage, bus bar voltage and thermal sensors' voltage. BM02A will protect battery pack from battery cell OVUV and thermal sensors OTUT. BM02A can discharge separate battery cell to realize cell balance. BM02A can reversely wake up MCU during MCU sleep mode when unmasked faults are detected. BM02A can communicate with other BM02As by daisy-chain UART. BM02A will communicate with MCU through BM04A (communication transceiver) by daisy-chain UART.	D
Isolator	Isolator can be a capacitor pair or a transformer, it is used as the high voltage communication isolator.	/
BM04A	12V LV battery pack is the power supply for BM04A. BM04A is a communication transceiver, which is responsible for the conversion between SPI and daisy-chain UART protocol. During sleep mode, BM04A can detect wake tone from BM02A, then MCU will be waked up by SBC when SBC accepts an enable signal from BM04A.	D
SBC	12V LV battery pack is the power supply for the SBC. Convert 12V battery output to 5V low voltage to supply MCU. Convert 12V battery output to 5V low voltage to supply BM04A' SPI communication block. SBC can communicate with other systems by CAN bus. SBC can communicate with MCU by CAN/SPI inside transceiver. Can accept the enable signal from BM04A to power up MCU when MCU is powered off in shutdown mode.	/
MCU	MCU is responsible for collecting information from BM02A and BM04A and controlling BM02A and BM04A by SPI interface. MCU will cooperate with BM02A and BM04A to realize the safety mechanisms. MCU will command BM02A or BM04A to enter safe state once needed. MCU will also monitor the HV battery pack's current.	/
Current Sensor	Sense the HV battery pack's current.	/
HV Relay	HV battery pack's relay.	/
HV Board	PCB and BOM for HV system circuitry.	/
LV Board	PCB and BOM for LV system circuitry.	/

Interface ID	Interface Name	Interface Type	Description	Remark
IFE_001	Channel Voltage & Temperature Signal	Power/Analog	Inputs for monitoring battery cell voltages plus bus bar voltages. Used to balance battery cell. Power supply input and ground. Used for external temperature sense.	Passive network between HV battery pack and BM02A is present.
IFE_002	Daisy-chain UART	Digital/Communication	For the communication between BM04A and BM02A. For the communication between daisy-chained BM02As.	Differential signal.

Operating mode

Operating mode diagram

BMS Operating Mode Diagram

BMS Operating Mode Diagram

Operating mode description

Mode ID	Mode Name	Description	Remark
MOD_01	Shutdown Mode	During shutdown mode, whole BMS is off.	/
MOD_02	Active Mode	During active mode, the BMS can achieve full functions, including communication, data collection, balance control, diagnostic control and the rest; MCU, BM04A, BM02A and SBC are thus all fully active.	/
MOD_03	Sleep Mode	The sleep mode is a low power consumption state, during sleep mode, MCU is powered off by SBC, BM02A and BM04A are all in sleep mode.	Customer decides SBC status during sleep mode.
MOD_04	Fault Mode	During fault mode, it depends on if the fault is critical, host can decide if that BMS just alerts a fault to driver, BMS takes proper actions or BMS needs to enter shutdown mode.	Customer decides the fault strategy.

Operating mode transition conditions

Condition ID	Condition Name	Description	Remark
CON_01	Enable BMS	Whole BMS is enabled and powered by HV battery and LV battery.	/
CON_02	Turn BMS into sleep mode	MCU sends command to BM02A and BM04A to make them enter sleep mode, then MCU itself enters shutdown mode by SBC.	/
CON_03	Wakes up BMS	MCU is waked up by SBC's power supply, then MCU send command to wake up BM02A and BM04A into active mode.	SBC wakes up MCU due to the CAN bus command or BM04A's enable signal.
CON_04	Disable BMS	Whole BMS is disabled but still powered from HV battery and LV battery.	

Condition ID	Condition Name	Description	Remark
CON_05	Fault occurred	Unmasked fault occurred insides the BMS.	The fault may occur during sleep mode or active mode, separate strategy should be taken to deal with the fault.

Operating mode mapping

BMS' Operating mode	BM02A's Operating mode	BM04A's Operating mode
Shutdown mode	SD mode	SLEEP mode
Active mode	ACTIVE mode	ACTIVE mode
Sleep mode	SLEEP mode	SLEEP mode
Fault mode	Customer decides	Customer decides

Mission Profile

Take passenger compartment as the mission profile (IEC TR 62380):


Mission profile

Assumptions on Functional Safety Requirement

Safety goals

Safety Goal ID	SG_1
Description	Prevent HV battery cell voltage from OV/UV when BMS is during active mode.
ASIL	D
Safe state	Disconnect HV relays or customer decides the fault strategy.
FTTI	200ms

Safety Goal ID	**SG_2**
Description	Prevent HV battery pack temperature from OT when BMS is during active mode.
ASIL	D
Safe state	Disconnect HV relays or customer decides the fault strategy.
FTTI	200ms

Safety Goal ID	**SG_3**
Description	Prevent HV battery cell voltage from OV/UV when BMS is during sleep mode.
ASIL	A
Safe state	Disconnect HV relays or customer decides the fault strategy.
FTTI	120s

Safety Goal ID	**SG_4**
Description	Prevent HV battery pack temperature from OT when BMS is during sleep mode.
ASIL	A
Safe state	Disconnect HV relays or customer decides the fault strategy.
FTTI	120s

Functional safety requirements

Functional Safety Requirement ID	**FSR_01**
Traced to Safety Goal ID	SG_1
Allocated to	BM02A and its peripheral circuits
Description	The BM02A's ADC measurement data of battery cell for the OVUV judgement of MCU shall be detected from 30mV error at full temp when BM02A is during active mode.
ASIL	D
Safe state	Fault flag set in communication frame is provided to transceiver or information (including communication loss) for fault detection/diagnosis is provided to host by transceiver
FTTI	100ms

Functional Safety Requirement ID	**FSR_02**
Traced to Safety Goal ID	SG_2
Allocated to	BM02A and its peripheral circuits
Description	The BM02A's ADC measurement data of battery pack for the OT judgement of MCU shall be detected from 5℃ error at full temp when BM02A is during active mode.
ASIL	D
Safe state	Fault flag set in communication frame is provided to transceiver or information (including communication loss) for fault detection/diagnosis is provided to host by transceiver
FTTI	100ms

Functional Safety Requirement ID	**FSR_03**
Traced to Safety Goal ID	SG_1, SG_2
Allocated to	BM02A and its peripheral circuits
Description	The end-to end communication among BM02As and BM04A shall be detected from failure at full temp when BM02A is during active mode.
ASIL	D
Safe state	Fault flag set in communication frame is provided to transceiver or information (including communication loss) for fault detection/diagnosis is provided to host by transceiver
FTTI	100ms

Functional Safety Requirement ID	**FSR_04**
Traced to Safety Goal ID	SG_3
Allocated to	BM02A and its peripheral circuits
Description	The BM02A's OVUV judgement shall be detected from 30mV error at full temp when BM02A is during sleep mode.
ASIL	A
Safe state	FLT tone is generated to transceiver
FTTI	60s

Functional Safety Requirement ID	FSR_05
Traced to Safety Goal ID	SG_4
Allocated to	BM02A and its peripheral circuits
Description	The BM02A's OT judgement shall be detected from 5℃ error at full temp when BM02A is during sleep mode.
ASIL	A
Safe state	FLT tone is generated to transceiver
FTTI	60s

Functional Safety Requirement ID	FSR_06
Traced to Safety Goal ID	SG_3, SG_4
Allocated to	BM02A and its peripheral circuits
Description	The fault signal propagation among BM02As and BM04A shall be detected from failure at full temp when BM02A is during sleep mode.
ASIL	A
Safe state	FLT tone is generated to transceiver
FTTI	60s

Assumptions of External Hardware Safety Requirements

EHWSR001

HWSR ID	EHWSR001
Highest ASIL	D
Related SM	ESM001: Regular frame counter host check
Allocated to HW	There shall be a frame counter to count all the received command and response frames, the counter shall increase by 1 after each command and response frame is received (without CRC fault).

EHWSR002

HWSR ID	EHWSR002
Highest ASIL	D
Related SM	ESM002: Response CRC host check
Allocated to HW	There shall be a frame CRC encoder to generate CRC to each response frame.

EHWSR003

HWSR ID	EHWSR003
Highest ASIL	D
Related SM	ESM003: Command CRC detection ESM004: Command CRC host diagnosis
Allocated to HW	There shall be a frame CRC decoder to detect the received command frame per SPFDTI, once detected, the fault flag shall be recorded in register and the fault flag shall be set in communication frame

Assumptions of System Level Safety Mechanisms

External SM ID	Failure mode to be dectected	Description	FSR ID
ESM1	SPF	The host MCU will execute the SPF detection procedure per SPFDTI (100ms) during active mode	FSR_01,FSR_02,FSR_03
ESM2	SPF	Fault flag set in communication frame will be monitored by transceiver per SPFDTI (100ms) during active mode, once detected, FLTB is asserted	FSR_01,FSR_02,FSR_03
ESM3	SPF	The host MCU will execute the SPF detection procedure per SPFDTI (60s) during sleep mode	FSR_04,FSR_05,FSR_06
ESM4	SPF	HB tone fault will be monitored by transceiver per SPFDTI (60s) during sleep mode, once detected, INH and FLTB are asserted	FSR_04,FSR_05,FSR_06
ESM5	MPF	The host MCU will execute the MPF diagnose procedure per MPFDTI (once at power on/off)	FSR_01,FSR_02,FSR_03,FSR_04,FSR_05,FSR_06