ISO 26262 Compliant High-Voltage Battery System Functional Safety Concept

JALAJAKSHI A
Systems Engineering Group Manager, BorgWarner, IPEC, Bengaluru

Abstract- ***Increasing concerns with the use of petroleum and the increasing regulations on fuel economy, electric powertrains have become more acceptable to automotive manufacturers. The Lithium-Ion batteries employed in such systems are typically managed by a High Voltage (HV) Battery Management System (BMS). Due to the presence of HV battery, the hazards involved in the Electric Vehicle (EV) such as Electric Shock, Thermal Event and Toxic Gas release are typical hazards. Therefore, functional safety plays a crucial role in designing safe BMS and mitigating hazards in EVs. The ISO 26262:2018 standard provides a framework for developing and validating automotive products to ensure they are free from electrical and electronic malfunctions. This paper introduces options for BMS system development in accordance with ISO 26262. Hazards and risks associated with BMS malfunctions identified and classified according to the standard. A concept BMS system is developed according to ISO 26262 methodologies, including item definition, hazard analysis and risk assessment, safety goal derivation and functional safety concept. Generic HV battery system architecture developed and discussed, with conclusions drawn based on the design and EV application.***

Indexed Terms- ***BMS, Electric Shock, EV, FSR, Functional Safety Concept, Hazard, HV, ISO 26262, OEM, PTC, Risk Assessment, Safety Goal, SOC, SOH, SOP, Thermal Event, Tire1.***

I. INTRODUCTION

Electrochemical battery technologies are critical to store and deliver energy to electric powertrains. The research is now highly focused on automotive battery technology to improve performance, reliability, safety, and cost reduction. Most of the batteries in EVs are using of lithium-ion chemistry. This chemistry is well suited to the volumetric energy and power density requirements for automotive applications and has seen improved cost and size margins as the technology has moved towards mass production. However, lithium-ion batteries require active monitoring and control to ensure the safety of the HV battery at the system level. This is because lithium-ion battery performance is dependent on operating range and environmental conditions. The battery pack consisting of multiple battery cells arranged in modules. The modules usually have an active cooling system to remove excess heat generated during use. For example, under some scenarios a cell or group of cells can overheat, producing excess energy that overwhelms the cooling system. The overheating can then propagate throughout a module or pack, which can lead to fire or explosion. This risk is strongly related to the delivery of appropriate energy to and from the battery. Battery overcharging beyond an energy capacity limit or battery over current beyond acceptable limits can lead to hazardous situations. At the cell level, charge and discharge management techniques need to consider the state of charge of all individual cells within a battery pack. Inconsistency in the capacity of individual cells within a pack is a significant performance and safety concern. The cell with the poorest capacity will limit the overall performance of the battery pack. Operation within the allowable window is maintained by the battery management system, which considers cell-to-cell variations and cell balancing, and enforces the window parameter limits. Failure of critical functions of the BMS can lead to operating outside the allowable window. Other risks, such as internal short circuit of the cells, high voltage exposure to humans, thermal management failure, cell balancing failure must addressed during the development process. All the risks are associated with electronic control systems, typically contained within a BMS. Typical BMS functions in the HV battery system are detailed in section II.

When we talk about problem statements, we must distinguish at least two areas; (1) the research community and (2) official norms and standards addressing this topic. The ISO 26262: 2018 [1] standard addresses functional safety of automotive E/E systems. The BMS malfunctions cause safety hazards, the ISO 26262 provides state-of-the-art

development processes and methods. The goal of functional safety is to minimize the risk to an acceptable level, with risk defined as the probability of occurrence of the damage and the impact of that damage to people. The measures employed to reduce risk are classified as fault avoidance, fault detection and fault handling measures.

ISO 26262 consists of twelve parts, with part 1 and part 2 introducing vocabulary and the management of functional safety. Part 3 describing the concept phase of the development process, part4, 5 and 6 focusing on product development and part 7 focusing on production and operation of the system. Part 8, 9 and 10 give guidance on the application of the standard. ISO 26262 encompasses the life cycle of a system from concept to decommissioning called safety life cycle in the standard; simplified safety life cycle is illustrated in Figure 1. This safety life cycle considers the functional safety development starting from the top OEM to Tire 1 suppliers or system providers. This paper discusses the concept phase key steps for ISO 26262 compliant development process for HV battery system.

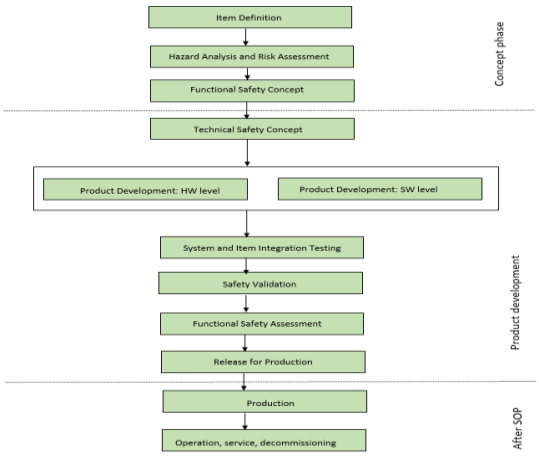

Figure 1. Simplified lifecycle of a system defined by ISO 26262

II. ISO 26262 APPLIED TO HV BATTERY SYSTEM DEVELOPMENT

Item definition: ISO 26262 states that the item (a system that implements a function at the vehicle level) needs to be defined to start the concept phase development. This will clarify the scope and the boundaries of the intended item and interfaces shown in Figure 2, as well as promote an adequate understanding of the item along with the preliminary item architecture shown in Figure 3 and the allocated functional assumption. For the item "HV battery system" comprises of the battery pack and BMS, the ISO 26262 development process is employed.

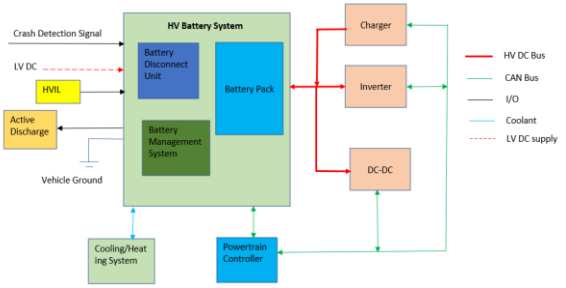

Figure 2. Item boundary and external interfaces of HV battery system in EV

In this example, the purpose of the HV battery system is to receive, store and supply energy transferred between the vehicle and battery pack over the High Voltage DC bus. The content is Li-ion battery cells packed together in "cell-modules." A number of cell modules are packed together with the battery casing to build the battery pack. The battery pack is controlled by the BMS. The battery pack is interfaced to the CAN bus, HV DC bus, 12V LV DC supply, crash detection signal line, active discharge, cooling/heating fluid supply manifolds and HVIL return signal. The battery pack specifications like battery voltage, the max energy stored, and max currents are not discussed in this paper.

The HV battery pack will collect and distribute electrical power as directed by the vehicle powertrain controller (PTC) based on information provided by the BMS via CAN-interface. The BMS is responsible for providing charge and discharge power limits during driving and current and voltage limits during charging. The HV relays, from battery disconnect unit connecting the HV battery to the HV bus, will be controlled by the BMS. The BMS is also responsible for keeping the battery cells at an appropriate temperature to ensure the life of the battery by opening the coolant valve and sending a cooling/heating request to the concerned system. The HV safety functions such as the HV interlock, active discharge and isolation detection are conducted by the BMS.

The general functional requirements of the battery system:

1. Accepts and stores HV electrical energy from both on-board and off-board chargers (DC fast) and regenerative braking.
2. Delivers HV electrical energy to the vehicle's high-voltage DC bus.
3. Provides HVIL safety system monitoring.
4. Provides thermal management of the battery cells.
5. Balances battery cell voltage.
6. Provides cell voltage measurements.
7. Provides cell temperature measurements.
8. Estimate battery pack state of charge (SOC).
9. Estimates battery state of health (SOH).
10. Estimates battery state of power (SOP).
11. Measures the current in/and out of the battery pack.
12. Monitors battery pack voltage.
13. Monitors battery pack current.
14. Controls HV Relays during charging and discharging.
15. Receive crash/Impact signal.
16. Detect ground fault isolation.
17. BMS communicates within battery systems (between BMS and sensors).
18. BMS communicates with another vehicle module (vehicle CAN communication).

ISO 26262 recommends using applicable national and international standards for deriving safety requirements. The HV DC bus on and EV typically operate at 400 to 800 volts, well above the thresholds of 60V DC and 30V AC typically considered safe by electrical vehicle safety standards (SAE J2344 [2] and ISO 6469-3 [3]). It is well known that a crash can damage insulation and electrical protection systems. Additionally, a thermal event caused by Li-ion cell or battery overheating could melt or combust electrical insulation and insulators, potentially allowing occupants, maintenance personnel or first responders direct contact with high-voltage components. The regulation or standards require protection against electric shock, either by direct contact with live parts or by indirect contact. Sufficient isolation resistance keeps the body currents within safe limits. To ensure this protection the HV power grid must be kept separate from the LV vehicle grid and vehicle chassis using enclosures. Further, the regulation requires an insulation resistance between the HV bus and the LV vehicle ground of at least 100Ω/V for HV DC buses and 500Ω/V for HV AC buses.

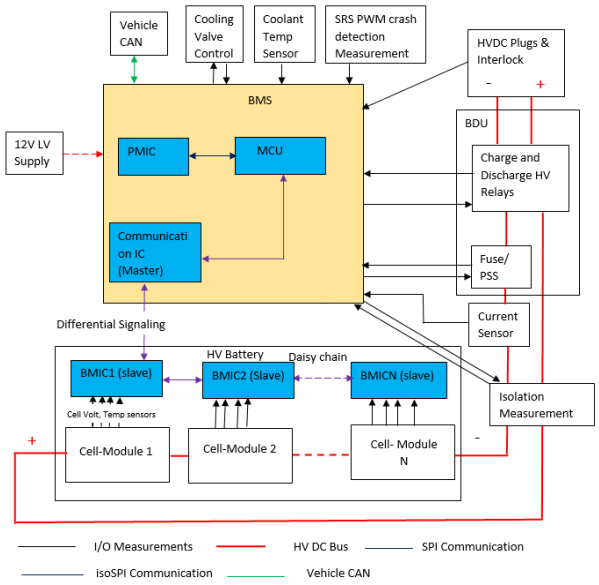

Figure 3. Preliminary Battery System Architecture for EV

For cell measurements, including cell voltage, cell temperature and cell balancing. The hardware setup and number of sensors based on the selection of the battery monitoring integrated circuit (BMIC) and number of series connected cells in the battery pack and its operating voltage range (min, nominal and max cell voltage and battery voltage), that decides number of BMICs required for measuring HV battery. Readers that would like to obtain detailed information about commercially available BMICs can find the actual data sheets in the following references: [4], [5], [6], [7] and [8]. In Figure 3, the BMICs communicates daisy chained SPI communication. The Communication IC that converts the SPI protocol to differential data stream. It can communicate with the slave devices via an isolation device. All slave ICs are connected in series with daisy-chain. The microcontroller unit (MCU) sends command to BMICs to operate or report information. Power management IC (PMIC) provides supervised supply voltage to the MCU and sensors. The SRS ECU can send the alarm signal to the BMS in two forms, via a pulse width modulation (PWM) signal and using a CAN [9]. Battery disconnect unit (BDU) contains charge and discharge relays, pre-charge unit and Pyrotechnical Safety Switches (PSS). PSS in BDU should open and provide one pole HV separation during the crash and load side PSS should close to active discharging of stored energy in HV

load lines. The different operating modes of BMS are sleep mode, power on mode, power off mode, standby mode, drive mode and charge mode.

Hazard analysis and risk assessment: The definition of the hazard analysis and risk assessment (HARA) and the safety goal (SG) is normally done at the item level of OEM and delivered to the tire 1 supplier as requirements for the system to be developed. This process is defined in ISO 26262 part 3 with a goal of identifying the hazards in vehicle level due to the malfunctioning behavior of the item. Two techniques, namely functional failure analysis (FFA) and hazard and operability study (HAZOP) [10] are used for hazard identification. All E/E system malfunctions associated with all driving and non-driving scenarios identified, while considering the operating and environmental conditions. Once, the hazards are identified, they are classified according to the severity of potential harm to the vehicle occupants (driver, passengers) and the other road users outside of the vehicle(from class S0 for no injuries to class S3 for life-threatening and fatal injuries) and according to their controllability, meaning the ability of the vehicle's occupants or other traffic participants to handle the hazardous situation (with a rating of C0 for generally controllable situations to C3 for difficult or uncontrollable situation). The driving situation and an exposure rating for this situation is assigned to each hazard as well, with a rating of E0 for situations that almost never occur to E4 for situations encountered with a high probability. Based on the assigned classes of severity, probability, and controllability, an ASIL (automotive safety integrity level) is assigned to each hazard, using ISO 26262-3 ASIL table shown in Table 1. In this, four ASILs are defined, with ASIL A being the lowest safety integrity level and ASIL D the highest integrity level.

Severity S	**Exposure E**	**Controllability C**		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Table 1. ASIL Table

In addition, HARA can lead to a hazard being classified as QM (quality management), which means that it is not required to comply with the standard for handling of that hazard. Table 2 shows an example of simplified HARA for the BMS developed in this section to illustrate the classification of hazards and resulting ASIL for that hazard. The identified hazards related to thermal events, cell venting, electric shock, and unintended deceleration due to loss of HV power. For each identified hazard that was assigned an ASIL, safety goals must be defined to form the top-level safety requirements for an item; the safety goal is not a technical solution for the issue presented by the hazard but a functional objective for the item. Table 3 shows an example of safety goals of HV battery system.

Driving Situation	**Hazard**	**S**	**E**	**C**	**ASIL**
AC Charging in public	Battery fire due to cells reaching a voltage value over the maximum voltage limit for a significant amount of time during	S3	E4	C2	C

	charging.				
Driving, acceleration, braking	Battery fire due to high current flowing for a considerable time during the charging or discharging operations.	S 3	E 4	C 2	C
DC Charging in public	Battery fire due to cells reaching a temperature higher than the maximum temperature a battery cell can be exposed to.	S 3	E 4	C 2	C
Driving, acceleration, braking	Battery fire due to cells reaching a temperature higher than the maximum temperature a battery cell can be exposed to.	S 3	E 4	C 2	C
Service of HV-Parts	Electric shock due to failure of detecting the isolation fault.	S 3	E 1	C 3	A
Service of HV-Parts	Electric shock due to failure of detecting the HVIL open loop fault.	S 3	E 1	C 3	A
Crash	Electric shock after a crash due to failure of responding to SRS signal.	S 3	E 1	C 3	A
Driving, acceleration, braking	Loss of propulsion due to unintended complete loss of HVDC.	S 3	E 4	C 2	C

Table 2. example of vehicle level hazards for HV Battery System

ID	Safety Goal	ASIL
SG 1	Overheating of the cells of the battery system with the potential of a thermal event, including propagation on the vehicle must be prevented.	ASIL C
SG 2	Overcurrent in the HV components of the battery system shall be prevented.	ASIL C
SG 3	Robustness of contactor weld checks shall be sufficient to determine whether the contactors are able to open after an impact event.	ASIL A
SG 4	In case of crash the HV battery shall be disconnected from the HV distribution system.	ASIL A
SG 5	Unintended complete loss of HVDC shall be prevented.	ASIL C
SG 6	The Isolation resistance value of all HV components shall be always displayed correctly, especially from a service perspective.	ASIL A

SG 7	The HVIL loop value of all HV components shall be always displayed correctly, especially from a service perspective.	ASIL A

Table 3. example of vehicle level safety goals of HV Battery System

Functional Safety Concept: The functional safety concept (FSC) contains the functional safety requirement (FSRs) that are derived from the safety goals and describes that are to be implemented at a functional level to prevent safety goal violation. The functional safety concept should address fault detection and failure mitigation, safe states, including system operation degradation strategy and operator warning strategy. Assuming here the ASIL decomposition has not applied. The preliminary architecture for an HV battery system can be resumed to the following FSRs for safety functions. Table 4 shows the example FSRs.

ID	Description	ASIL	Related SG	Allocation	FTTI
FSR 1	The BMS shall detect battery cell voltage above safe charge limit.	C	SG1	BMIC	200 ms
FSR 2	The BMS shall detect battery cell temperature above the safe limit.	C	SG1	BMIC	200 ms
FSR 3	HV components in the battery system shall be self-protected from thermal events.	C	SG2	BMS	One driving cycle
FSR 4	The BMS shall monitor over current of HV battery.	C	SG1	BMS	200 ms
FSR 5	The BMS shall monitor contactor weld check to ensure disconnection functionality.	A	SG3	BMS	One driving cycle
FSR 6	After detecting a crash, the HV battery must be disconnected from the HV distribution system.	A	SG4	BDU	One driving cycle
FSR 7	SoC limits of battery pack shall be determined and communicated to other items.	C	SG5	BMS	200 ms
FSR 9	The BMS must implement an E2E protected CAN	C	SG5	BMS	200 ms

	communication for all safety relevant messages.				
FSR 11	The isolation monitor shall be implemented to measure isolation resistance between HV and LV ground with required accuracy.	A	SG6	BMS	200 ms
FSR 12	The BMS shall detect HVIL open loop condition.	A	SG7	BMS	One driving cycle
FSR 13	The BMS shall detect the energize or deenergize state of HV relays	C	SG1	BMS	200 ms
FSR 14	MCU shall be supervised by an error monitor	C	SG1	BMS	200 ms
FSR 15	MCU shall be monitored by an external watchdog	C	SG1	BMS	200 ms
FSR 16	BMS shall detect under/over voltage of the battery	C	SG1	BMS	200 ms

Table 4. example functional safety requirements

For multiple point faults not detected, that would be considered as undetected latent faults. Diagnose potential latent faults ones per drive cycle and monitor continuously during operation.

Safe state, warning, and degradation concept

- Safe state is not the same for all FSRs, for example, FSR1: safe state is opening of contactors before the system enters an unsafe state. That means, depending on cell chemistry, the charging will stop sufficiently low voltage.
- Allowed power limit (charge/discharge), the control strategy is judged by individual cell voltage. All HV battery system elements are allocated fully responsible for ASIL C; therefore, relays would be opened by cell voltage upper and lower limits. When a crash detection signal is received as crash, relays will be opened within milliseconds. To secure relays opening ability, BMS will check relays weld status in every driving cycle. If any contactor's weld status is detected, closing contactor will be inhibited as safe state.
- The warning concept should warn the user regarding the inability to reach a safe state and about the reduced functionality. If a failure is detected a DTC will be set and warn the driver regarding the fault reaction level.
- In degradation concept, if hardware failure in BMS will be detected and the fault reaction will lead to HV off.

Confirmation reviews: As per standard, independent reviews to be performed for HARA, functional safety concept. For HARA, ASIL C discussed in Table. 2, the verification of the resulting document by a person or group of people not part of the HARA team and independent from the relevant department. The verification of FSC document by a person independent from the team.

CONCLUSION

This paper briefly introduced hazards and the BMS safety related functions in electric vehicles. Started with general and very high-level considerations about the hazards related to lithium-ion batteries involved in the Electric Vehicle (EV) such as Electric Shock, Thermal Event and Toxic Gas release and through the process described in ISO 26262. It has also highlighted how the risk-based approach of ISO 26262 can influence the safety integrity level of some safety related functions in electric vehicles. The functional safety concept aiming at reaching the safety goals (SG1, SG2 and SG5) keeps it to a controllable level, ASIL C for an electric vehicle was presented. The HV battery system safety concept relies on the monitoring of the safety function by the BMS.

REFERENCES

[1] ISO 26262:2018, Road Vehicles— Functional Safety, All Parts 1-10.

[2] SAE J2344:2010, Guidelines for electric vehicle safety.

[3] international standard 'Electrically propelled road vehicles – Safety specifications – Part 3: Protection of persons against electric shock' ISO standard 6469-3:2021.

[4] Linear Technologies, LTC6813-1/LTC6820 datasheets, available from https://www.analog.com/media/en/technical-documentation/data-sheets/LTC6813-1.pdf

[5] Texas Instruments, bq76PL455A, available from https://www.ti.com/sitesearch/docs/universalsearch.tsp?searchTerm=bq76pl455a#q=bq76pl455a&t=everyt hing&linkId=1

[6] Maxim, MAX1492X family, available from https://www.maximintegrated.com/en/products/power/battery-management/MAX14920.html/tb_tab0

[7] NXPs, MC33771B, available from https://www.nxp.com/products/power-management/battery-management/battery-cell-controllers/14-channel-li-ion-battery-cell-controller-ic:MC33771B

[8] ST Microelectronics, L9963, available from https://www.st.com/en/applications/electro-mobility/automotive-battery-management-system-bms.html

[9] Yubo Lion, "High-Voltage Safety Improvement Design for Electric Vehicle in Rear Impact", Springer, Automotive Innovation 1, 211-225 (2018).

[10] SAE J2980:202310, "Considerations for ISO 26262 ASIL Hazard Classification".