EMERGING TECH CONFERENCE – Edge Intelligence

Volume 02, 2023, Page 78 – 84

Proceedings of Emerging Tech Conference: Edge Intelligence 2023

Enhanced Safety Architecture with Fault Preventive Mechanisms for Automotive Li-ion Battery Management Systems

Apostolos Delizonas[1], Christos Mademlis[2], Evangelos Tsioumas[2], Di-mitrios Papagiannis[2], Nikolaos Jabbour[2], Christos Sansaridis[1], Tilemachos Matiakis[1]

[1] *KENOTOM P.C., Kalamaria-Thessaloniki, Greece*
a.delizonas@kenotom.com

[2] *School of Electrical and Computer Engineering Aristotle University of Thessaloniki, Thessaloniki, Greece*
mademlis@auth.gr

Abstract

Compliance of electric vehicle (EV) Battery Management Systems (BMS) with functional safety standard ISO 26262 is considered mandatory due to several risks associated with Lithium-Ion (Li-ion) batteries (BT). However, the high-criticality safety goals formed in accordance with the standard can significantly increase the implementation and verification complexity of the EV-BMS. Therefore, the aim of this paper is to propose an improved safety architecture which can provide effective mechanisms to prevent or mitigate both systematic and random faults and avoid single instances of failure. This architecture is applicable to a wide range of EV BT topologies and therefore, it can simplify and accelerate the development lifecycle of modern EVs.[1]

1 Introduction

Despite their multiple benefits, Li-ion BTs are vulnerable to venting, fire, and explosion in case of electrical, thermal, and mechanical abuses [1]. Thus, the main objectives of a BMS are to ensure safety, protection of the BTs' lifespan and satisfactory performance of the BTs. Therefore, the EV-BMSs must comply with the automotive safety standards since potential failures may have a great impact on the vehicle's safety.

ISO 26262 [2] safety standard imposes a set of processes and provides guidelines which can ensure the functional safety of an automotive electronic control unit (ECU). According to the standard's orders, hazardous events, that may be caused by system malfunctions, should be analyzed at vehicle level. The result of this process is the risk assessment of these events and the derivation of the respective safety goals.

In the ISO 26262, risk is assessed with automotive safety integrity level (ASIL) indicators, which combine severity, exposure, and controllability of a hazardous event. There are four ASIL indicators (A, B, C, D) rated

[1] The project KMP6-0126719 was implemented under the framework of the Action «Investment Plans of Innovation» of the Operational Pro-gram «Central Macedonia 2014 2020» that is co-funded by the European Regional Development Fund and Greece

from least to strictest one, respectively. Safety goals with higher ASILs (C and D) require stricter safety mechanisms and verification methods and consequently increase the complexity of the system.

Although safety goals for an automotive BMS have been determined in [3], the combination of criticality and complexity for the functionality of the state-of-charge estimation, significantly increases the implementation and validation effort. In [4], derived safety requirements are independent from the state-of-charge estimation of the BTs; however, the high ASILs (D, C) and due to the fact that the potential random faults have been ignored, several complexity and safety issues may arise. Mechanisms for prevention of random faults have been examined in [5]. However, the absence of redundancy may lead to adverse single instances of failure.

Although safety goals for an automotive BMS have been determined in [3], the combination of criticality and complexity for the functionality of the state-of-charge estimation, significantly increases the implementation and validation effort. In [4], derived safety requirements are independent from the state-of-charge estimation of the BTs; however, the high ASILs (D, C) and due to the fact that the potential random faults have been ignored, several complexity and safety issues may arise. Mechanisms for prevention of random faults have been examined in [5]. However, the absence of redundancy may lead to adverse single instances of failure.

The aim of this paper is to introduce a low-complexity automotive safety architecture compliant with the ISO 26262. Specifically, the high-ASIL safety goals are decomposed to lower-ASIL function-alities which can be implemented by redundant and adequately independent hardware and software elements. Thus, any fault of these independent elements is prevented from causing a single point failure and also, the overall development complexity is decreased. Moreover, a combination of Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) is performed to detect the possible random faults that can violate the determined safety goals and prevent or mitigate these faults. Various EV-BT systems are considered to validate that the proposed architecture can be adopted by almost all automotive BMSs.

2 Derivation of Safety Goals for the Automotive BMS

Modern EV BTs contain multiple Li-ion cells which are connected in series and parallel and ar-ranged in modules. Considering that the dominant operating voltages are 400Vdc and 800Vdc, EV BTs should contain several modules and thus, a high number of BT cells. Therefore, the BMS adopts a modular architecture with two subsystems, as presented in Figure 1. The Supervisor Units are respon-sible for the voltage, temperature, and current monitoring of the cells of each module. The Master Unit undertakes the task of

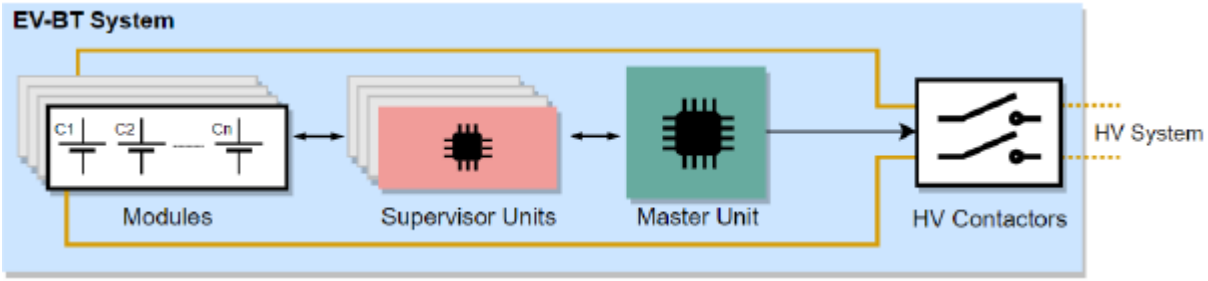

Figure 1 Overview of the modular BMS for Li-ion BTs

undertakes the task of the BT state estimation, the communication with other vehicle ECUs, as well as the connection/disconnection of the BT system from the rest HV system.

Severity	Exposure	Controllability		
		C1 (Lower)	C2	C3(Higher)
S1 (Lower)	E1 (Lower)	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4 (Higher)	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3 (Higher)	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	A	C	D

Table 1 ASIL ratings

Li-ion battery cells are susceptible to thermal runaways when abused, either electrically or ther-mally. Since Li-ion cells have significantly high energy density, the rapid self-heating may lead to ex-tended fire and violent explosions [6]. Regarding electrical abuses, Li-ion cell overcharge is the main cause for thermal runaways. In this situation, it operates above its voltage limits which leads to chemical reactions that can trigger a thermal runaway. On the contrary, deep overdischarges and excessive cur-rents may form dendrites leading to internal short circuits within the cell and eventually, thermal runa-way. Moreover, operation above 55°C - 60°C may bring the battery cell to a situation where excessive heat cannot be properly dissipated and a thermal runaway event may be initiated. On the other hand, operation of Li-ion cells at low temperatures may also form dendrites that in the worst case may pene-trate the cell's separator and lead to internal short circuits. Low temperature operation is mostly dan-gerous when charging a Li-ion cell below 0°C since charge-transfer resistance of discharged cells is much higher to that of charged ones [7].

Table 1 shows the various combinations of Severity, Exposure and Controllability classes that form the four ASIL ratings. The quality management (QM) rating represents hazards of low risk that does not need to comply with ISO 26262 processes.

A thermal runaway event in a single Li-ion cell inside a module may easily propagate to neighbor cells due to the firm assembly of an EV-BT system [6]. Under these conditions, multiple sources of potential fire and explosion are present within the BT system. In addition, a thermal runaway occurring during the end of a charging process may have critical consequences since the Li-ion cells have all their energy available [6]. Thus, these events must be assigned to the strictest severity class S3, according to Table B.1 of ISO26262-3. Moreover, internal reactions of the cells cannot be controlled or prevented by the driver and thus, the strictest C3 class is considered.

The probability of exposure for vehicle charging depends on modern EV ranges. Considering a typical range of 340km [8] and average monthly travel of 1000km, an EV is charged approximately three times per month. Therefore, E3 exposure class is assigned as per Table B.3 of ISO 26262. On the other hand, vehicle charges at low temperatures (below 0°C) are less probable considering yearly aver-age temperatures and hence, E2 exposure class is assigned. Moreover, as Li-ion cells have a slow self-discharging rate of 5% per

month, periods of no charging should last more than two months to cause dangerous deep overdischarges, as defined in [1]. Thus, E2 class is considered according to Table B.3.

Tables 2 and 4 present the Hazard Analysis and Risk Assessment for various cause events of Li-ion BT fire or explosion, as well as the respective safety goals of a BMS.

Cause Event	(S)	(E)	(C)	ASIL
Cell overcharging at vehicle charging	S3	E3	C3	ASIL C
Cell overheating at vehicle charging	S3	E3	C3	ASIL C
Cell internal short circuit due to vehicle charging after long period of no charging	S3	E2	C3	ASIL B
Cell internal short circuit due to vehicle charging at temperatures below 0°C	S3	E2	C3	ASIL B
BT conducting excessive currents due to faulty DC charger or extended acceleration at low traction surfaces	S3	E1	C3	ASIL A

Table 2 HARA for the BMS

Safety Goal	Description	ASIL
1	Prevention of cell overcharging	ASIL C
2	Prevention of cell overheating	ASIL C
3	Prevention of cell overdischarging or charging after an overdischarge	ASIL B
4	Prevention of cell charging at temperatures below 0°C	ASIL B
5	Prevention of BT overcurrents	ASIL A

Table 3 Safety Goals of the BMS

3 Proposed Safety Architecture

To achieve the safety goals, the BMS must ensure the transition to a safe state within one second, whenever a systematic fault appears. Regarding the safety goals 1 and 3, the BMS should detect operation of cells outside the overvoltage (OV) and undervoltage (UV) limits. Since these limits occur for different Li-ion chemistries, they should be configurable for our BMS to cover various EV-BT systems. For safety goals 2 and 4, operation of cells above overtemperature (OT) limit and below undertemper-ature (UT) limit of 0°C must be detected. Configurability should also be ensured for overcurrent (OC) limits since they differ for charging and discharging process and depend on Li-ion chemistry.

Since the analyzed hazards are related to charging and discharging of the BT, the BMS should achieve a safe state by disconnecting the BT from the rest system and interrupting any charge transfer.

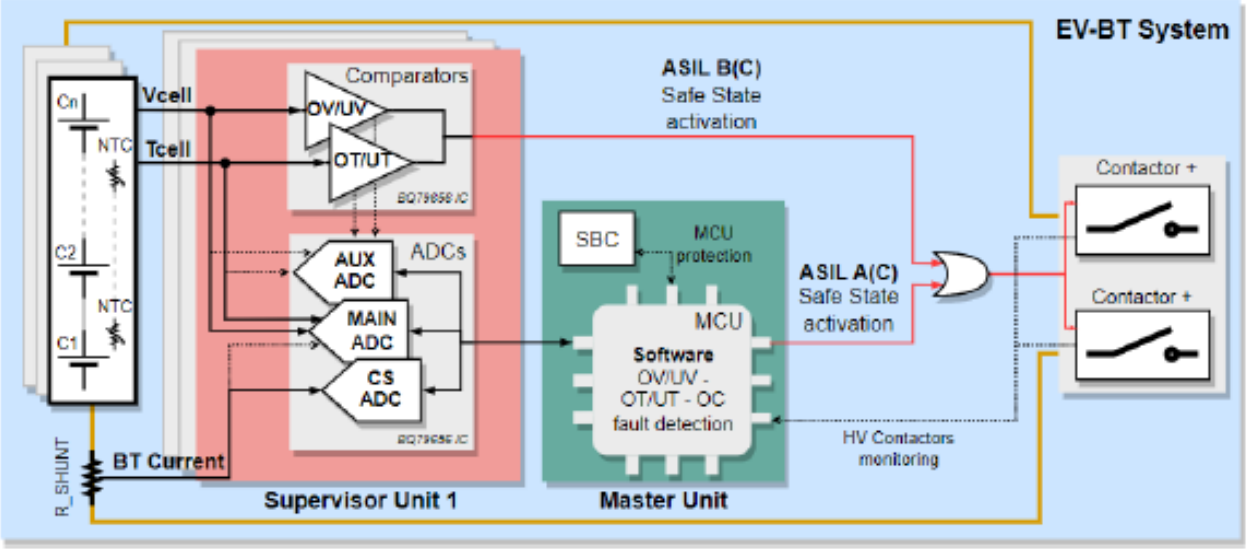

Figure 2 Layout of the proposed safety architecture

For the proposed architecture, the BQ79656-Q1 is utilized [9] as the main cell monitoring integrated circuit (IC) of the Supervisor Units and also, a microcontroller (MCU) protected by a system basis chip (SBC), for the Master Unit, is used. The proposed architecture is illustrated in Figure 2. The IC uses the main ADC for the measurements of cell voltages and temperatures and the current sense (CS) ADC for current measurement. A third auxiliary (AUX) ADC is used for the additional safety mechanisms. The measurements are transmitted via UART communication protocol. Moreover, the IC provides independent hardware comparators with configurable limits, directly connected to cell voltages and thermistor outputs with the ability to trigger a hardware reaction.

Therefore, safety goals 1-4 are decomposed to two redundant functionalities with lower ASILs. The first one [ASIL B(C)] takes over the hardware comparison of cell voltages and temperatures and also, immediate disconnection of the BT from the rest of the system, in case of faults. The second one [ASIL A(C)], is responsible for voltage and temperature measurements from the ADCs and the detection of potential faults as well as the disconnection of the BT from the software of the MCU. Safety goal 5 is allocated only to the second functionality.

4 Safety mechanisms for prevention of random hardware faults

The proposed architecture can prevent any hazardous event due to systematic faults, as analyzed above. Since random hardware failures may also lead to a violation of a safety goal, an FTA is per-formed as presented in Figure 3 which is referred to safety goals 1-4.

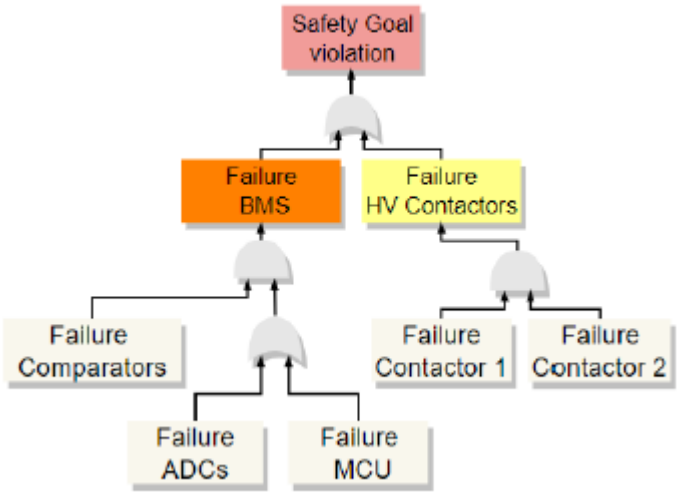

Figure 3 FTA for safety goals 1-4

From the FTA, it is revealed that none of the analyzed failures can lead directly to a violation of safety goals 1-4. Therefore, it is verified that the decomposition of these goals to redundant functional-ities has led to avoidance of single instances of failure. However, if combined, these failures may raise threats for overall system safety. Thus, the proposed architecture implements proper safety mechanisms to detect dual-point faults that may lead to these failures. The most relevant mechanisms based on FMEA are presented in Table 4. Moreover, as implied by ISO 26262, safety mechanisms for dual-point faults can be performed during start-up of the system and set to safe state instead of running continu-ously during its operation. Therefore, the implementation complexity of these mechanisms is signifi-cantly decreased.

Failure Mode	Random Fault	Safety Mechanism
Failure Comparators	Fault at value of OV/UV – OT/UT limit	Limits are measured from the AUX ADC and diagnosed by MCU
	Random Comparator Fault	MCU injects fault at comparators to verify their proper functionality
Failure ADC	Fault at Main ADC	Voltage and temperature are also measured by AUX ADC and deviations are diagnosed by MCU
	Fault at Current sense ADC	Current is measured also by Main ADC and deviations are diagnosed by MCU
	Communication fault	Both MCU and IC detect faults with communication timeouts and CRC calculations at UART messages
Failure MCU	Loss of power and other random faults	External watchdog implemented with SBC monitors the proper functionality of the MCU
Failure HV contactors	Contactors + and - stuck at closed	MCU monitors the actual state of Contactors and informs VCU in case both contactors are stuck

Table 4 Safety mechanisms for random hardware faults

5 Conclusions

The proposed BMS safety architecture provides improved safety and low complexity by covering both systematic and random faults, while critical single instances of failure can be avoided. Moreover, it can be adopted for a wide range of EV BT systems due to its modularity. Therefore, it effectively contributes to the overall safety of the EV and the acceleration of its development lifecycle.

6 References

[1] C. Yuqing, et al, "A review of lithium-ion battery safety concerns: The issues, strategies, and testing standards", *Journal of Energy Chemistry*, vol. 59, pp 83-99, Aug. 2021

[2] ISO 26262:2018 – Road Vehicles – Functional Safety – All Parts, ISO: Geneva, Switzerland, 2018

[3] W. Taylor, G. Krithivasan, J.J. Nelson, "System Safety and ISO 26262 Compliance for Automotive Lithium-Ion Batteries" in Proc. *IEEE Symposium on Product Compliance Engineering*, 2012

[4] B. Li, et al, "Research on Functional Safety of Battery Management System (BMS) for Electric Vehicles", in Proc. *Int. Conf. on Intelligent Computing, Automation and Applications (ICAA)*, 2021

[5] D. Marcos, et al, "A Safety Concept for an Automotive Lithium-based Battery Management System", in Proc. *Electric Vehi-cles Int. Conf. & Show (EV2019)*, Oct 2019

[6] F. Xuning, et al, "Thermal runaway mechanisms of lithium-ion battery for electric vehicles: A review", *Energy Storage Materials*, vol. 10, pp 247-267, Jan. 2018

[7] Shuai Ma, et al, "Temperature effect and thermal impact in lithium-ion batteries: A review", *Progress in Natural Science: Materials International*, vol. 28, pp. 653-666, Dec.2018

[8] "Range of full electric vehicles" ev-database.org, Available [Online]: https://ev-database.org/cheatsheet/range-electric-car, 2022

[9] Texas Instruments, "Automotive 16-S precision battery monitors, balancer, current sensor with ASIL-D compliance", BQ79656-Q1 datasheet, May 2021 [Rev. Jun. 2022