



Critical review and functional safety of a battery management system for large-scale lithium-ion battery pack technologies

K. W. See^{1,6} · Guofa Wang^{2,4} · Yong Zhang³ · Yunpeng Wang¹ · Lingyu Meng^{4,5} · Xinyu Gu⁶ · Neng Zhang¹ · K. C. Lim¹ · L. Zhao¹ · Bin Xie¹

Received: 8 September 2021 / Accepted: 2 April 2022
© The Author(s) 2022

Abstract

The battery management system (BMS) is the main safeguard of a battery system for electric propulsion and machine electrification. It is tasked to ensure reliable and safe operation of battery cells connected to provide high currents at high voltage levels. In addition to effectively monitoring all the electrical parameters of a battery pack system, such as the voltage, current, and temperature, the BMS is also used to improve the battery performance with proper safety measures within the system. With growing acceptance of lithium-ion batteries, major industry sectors such as the automotive, renewable energy, manufacturing, construction, and even some in the mining industry have brought forward the mass transition from fossil fuel dependency to electric powered machinery and redefined the world of energy storage. Hence, the functional safety considerations, which are those relating to automatic protection, in battery management for battery pack technologies are particularly important to ensure that the overall electrical system, regardless of whether it is for electric transportation or stationary energy storage, is in accordance with high standards of safety, reliability, and quality. If the system or product fails to meet functional and other safety requirements on account of faulty design or a sequence of failure events, then the environment, people, and property could be endangered. This paper analyzed the details of BMS for electric transportation and large-scale energy storage systems, particularly in areas concerned with hazardous environment. The analysis covers the aspect of functional safety that applies to BMS and is in accordance with the relevant industrial standards. A comprehensive evaluation of the components, architecture, risk reduction techniques, and failure mode analysis applicable to BMS operation was also presented. The article further provided recommendations on safety design and performance optimization in relation to the overall BMS integration.

Keywords Battery management system · Functional safety · Hazardous area · Lithium-ion batteries · Failure mode analysis · Electric transportation · Large-scale energy storage

✉ Lingyu Meng
mly929996@outlook.com

✉ Xinyu Gu
xg622@uowmail.edu.au

¹ Azure Mining Technology CCTEG, 821 Pacific Highway, Sydney, NSW 2067, Australia

² China Coal Research Institute, Beijing 100013, China

³ China Mining Products Safety Approval and Certification Center, Beijing 100013, China

⁴ School of Mechanical Electronic and Information Engineering, China University of Mining and Technology, Beijing 100083, China

⁵ Beijing Tianma Intelligent Control Technology Co., Ltd, Beijing 101399, China

⁶ Australian Institute for Innovative Materials, Institute for Superconducting and Electronic Materials, University of Wollongong, Innovation Campus, Wollongong, NSW 2500, Australia

1 Introduction

Unprecedented progress in battery development and technologies is paving the way to electrification of all machinery in almost every industry sector, particularly in transportation, to replace the conventional fuel or gas-powered systems to every possible extent and potential (Zhu et al. 2019; Nitta et al. 2015; Masias et al. 2021). Over the last decade, the surge in battery production, not only to accommodate the electronics industry, but also for the mining, manufacturing, energy storage, and automotive sectors has made research into battery materials one of the most crucial developments in the modern world. Alongside material improvement and innovation, a battery management system (BMS) is required to achieve the full potential of every battery cell employed in every application scenario or circumstance (Lelie et al. 2018; Rahimieichi et al. 2013). Battery cells in most applications are usually deployed with them connected in series or parallel, or both to increase the required power and energy to provide useful performance. As such the battery pack generically refers to the number of cells that are connected together, in accordance with the specific application, and a dedicated BMS caters for the pack and system. The purpose of a BMS, as the name implies, is to effectively manage each individual battery cell in a pack so that they are synchronized and operated in a regime or range that has been assigned by the cell's manufacturer (Xiong 2020; Bonfiglio and Roessler 2009; Bowkett et al. 2013).

Beyond the basic functionality of measuring cell voltages, cell temperatures, and total current flowing through the battery pack, a BMS must also provide a charge equalization solution to ensure each cell in the battery pack has a similar discharge and charge rate. In addition, a BMS is also required to provide reliable information on the available charge balance so as to avoid over-charging and over-discharging conditions (Andrea 2010; Wan et al. 2009). A more advanced BMS will indicate the health status of the battery pack, at an approximation, through the detailed diagnosis of each charge–discharge cycle of every battery cell in the pack.

In every application field that requires a battery pack system, in addition to the battery cells and BMS, it also essentially requires adequate isolation devices or a contactor controller that is managed and is supervised by the BMS. When it comes to a high energy battery pack (large-scale), the BMS can be a sophisticated hardware and software integrated system that not only monitors each cell's voltage, current, and temperature, but also (Faika et al. 2018; Kim et al. 2013a): (1) calculates the leftover charge, (2) calculates the remaining cycle life, (3) manages the acquisition of data, (4) performs battery uniformity and equalization processes, (5) dynamically controls the charging and discharging rate,

(6) transmits and receives signals from other electronic components in the system, (7) manages the thermal distribution if it is not passive, and (8) ensures all isolation components connected to the battery pack are functional.

A very important issue for large-scale high-energy battery pack systems that are in highly sensitive environments, such as in hazardous areas, is the reliability of the BMS to provide the system with the level of safety that is required (Zhu et al. 2017, 2020; Li et al. 2016). While considerable research has been conducted to deal with improvement of the BMS in from the hardware and calculation algorithm aspects, such as the state of charge (SoC), estimation accuracy, cell balancing circuit topology, and state of health (SoH) estimation, the standard for the safety aspect of the BMS functionality is rarely considered. The importance of determining the level of safety integrity of the BMS's functionality is crucial for the overall operation of a battery pack system. Hence, in this review article, the safety considerations in designing a BMS are discussed in detail and illustrated with a generic example. The paper firstly provides a brief introduction to the key composition of the BMS, specifically for high energy battery pack systems, and then illustrates the typical BMS topology in the current market, which is followed by the functional safety studies as stipulated in the ISO 26262 and IEC 61508 industrial standards (IEC 61508-1 2010, ISO 26262 2018). The authors hope to provide the readers with some inspiration on the latest research findings and design of the BMS for sophisticated requirements and conditions. Such as in the personnel and material transporters for underground coal mine applications.

2 Data acquisition

The basis of a BMS rests on the accurate measurement of every external battery cell parameter in the battery pack system. The significant dependence on the measurement reliability makes the design criteria of the monitoring and detection circuits highly stringent, and assessment is needed to ensure the required anticipated readings. The 3 main inputs to the system are the main current sensor, the cell voltage sensor, and the temperature sensors. Other supplementary sensors include the general analogue sensors (e.g., humidity, acceleration pedal, brake pedal, insulation detection, location, etc.) and general digital sensors (e.g., indicators, switches, etc.).

Typical accuracies for the battery pack current of an electric vehicle are 0.5%–1.0% up to 450 A, 1–2 mV for the cell voltages, and 0.1% for battery pack voltage up to 600 V (Brandl et al. 2012). Depending on the application and battery chemistry type, however, the required accuracy can be higher or lower. For instance, the lithium-ion phosphate (LFP) type battery chemistry requires high accuracy

for measuring the cell voltages because of the very flat characteristic (voltage-capacity) curves.

In addition to the voltage and current sensors, temperature sensors are used in the battery pack. In a hazardous environment, every cell’s temperature must be measured at its terminal for the highest allowable heat generation during the charging and discharging processes. In common automotive applications, temperature sensors are only placed at certain hot and cold spots inside the battery pack to generalise the overall temperature distribution across the pack.

The rate of data acquisition or, in other words, the sampling times for each data stream is determined through the priority assessment, in which shorter sampling times, in the range of 10^{-3} s, are required for critical measurements such as the cell voltages and current to allow precise state estimation. Other measurements can tolerate lower frequency, so as to reduce the power consumption and complexity of the design for the firmware system. Based on all the data or information acquired, the BMS will have outputs, such as switching the safety contactors to isolate the battery pack, only if any of the parameters are out of range, and there are other general analogue or digital outputs such as indicators, controlling the speed of the fan for heat management, switching contacts, communications, etc. Another essential consideration for the measurement circuitry is the electromagnetic compatibility of the layout design, particularly for automotive traction applications, so that, in most cases, all the power electronic components are in close proximity to the BMS. A good anti-electromagnetic interference design of the BMS will ensure the reliability and quality of the data acquired and further enhance the processing stage.

3 Data management, processing, storage, and communication

One of the most critical capabilities in the BMS software system is its ability to effectively estimate the remaining charge or energy left in every battery cell and also the remaining cycle life or useful life of each cell. The former is commonly known as the state of charge (SoC) and the latter is known as state of health (SoH). In some of the BMS literature (Lu et al. 2013; Wikner and Thiringer 2018), there are also terms as state of function (SoF) and depth of discharge (DoD), which are generally derived or calculated from the SoC and SoH. These battery parameters are said to be estimated because in most battery chemistry, especially the lithium-ion, they are not able to be measured directly as in the cases of voltage, temperature and current. These direct measurements will be used, however, as the input values for the estimation algorithms or models that anticipate and output the SoC and SoH values as accurately as possible.

The heavy dependencies of almost every charging-discharging operation of the battery pack on these estimated values have directed significant attention to the design algorithm and have been the research priority in many battery research groups for the past decade (Duong et al. 2015, 2017; Gu et al. 2021; Kim et al. 2013b; Lee and Lee 2021; Lim et al. 2016; Lin et al. 2020) Table 1 shows the reported SoC and SoH estimation techniques that have been devised by various research groups. Both estimation techniques are complex in nature, due to the fact that various unforeseen factors that could considerably affect the estimation outcomes are inevitable.

The most frequent commercially employed SoC technique is through the Coulomb counting method or a modified version of it. In general, this algorithm integrates the current entering or leaving the battery pack with respect to time. The downsides are that the cell deteriorates over a period

Table 1 State of Charge (SoC) and State of Health (SoH) estimation techniques

Direct measurement	Book-keeping estimation	Adaptive system	Hybrid methods
<i>SoC estimation techniques</i>			
Open circuit voltage (OCV)	Coulomb counting (ampere-hour integral)	Neural network	Coulomb counting and OCV combination
Terminal voltage	Modified Coulomb counting	Support vector machine	Coulomb counting and Kalman filter
Impedance spectroscopy		Fuzzy neural Kalman filter	Extended Kalman filter
Experimental methods	Model-based methods	Machine/deep learning methods	
<i>SoH estimation techniques</i>			
Impedance measurement	Adaptive filtering (KF, EKF, UKF, RLS, etc.)	Support vector regression	
Internal resistance	Electrochemical model	Neural network	
Capacity level	Sliding mode observers	Fuzzy logic	
Incremental and differential of capacity and voltage		Long- or short-term memory network, transformer, etc	

of time and the initial value from the integral solution does not necessarily correspond to the state of the battery at that particular time. The deterioration process of a cell is caused by complex electrochemical reactions, which are not taken into account by the coulomb estimation. Furthermore, such techniques required high robustness and precision measurement of the current, since it is the main parameter in the estimation process.

Until now, the SoH estimation has not been successfully adopted by many commercial applications, since the complexity and unknown variations are yet to be deduced. There are essentially three main indicators that define this state: the battery internal resistance, the battery impedance, and its capacity. All of these are not able to be directly measured by any circuit or electronic chip design, and they require substantial knowledge of the cell electrochemistry over a lengthy period of time. In vehicular applications, the battery capacity can fade by up to 20%, while the internal resistance increases by up to 160% above its initial value (Berecibar et al. 2016). Therefore, in tracking these changes, it is necessary to estimate the battery SoH, which is a challenging task, since the both battery resistance and capacity find their origins not only in many different causes, but also in the interactions between them. The extensive contents of the estimation algorithms will not be discussed in this paper.

Besides calculating the SoC and SoH, the BMS is also required to store the usage history and profile (charge and discharge) of every battery cell, including fault occurrence, temperature, SoC, and SoH. This data is essential to allow for maintenance activities, recycling processes for second-life applications, short- and long-term predictions of the capability of the system to deliver power, and the usage life, anticipated upcoming faults and their diagnosis, battery cell comparison studies, and many more factors. The sophisticated management of these data might not necessarily be performed within the BMS system itself so as to reduce the complexity, cost, and computational power. Instead, the data management, calibration, and analysis can be performed through external devices such as through online cloud management or wireless portable computers. Apart from straightforward on-board diagnosis such as sensor faults, actuator faults, out-of-safety-range operation, loose connections, and insulation faults, the BMS usually contains a networking system to not only communicate with other electronic controllers, but also to allow transfer of data for additional essential diagnosis. In automotive applications, the BMS usually adopts the Controller Area Network (CAN) bus for communication and networking, while in other applications, the Universal Serial Bus (USB), Integrated Circuit (I2C) Bus, and RS232 and EIA485 (formerly RS485) connections (Divyashree et al. 2020; Gabbar et al. 2021) are equally well adopted.

4 Battery equalization management

Battery equalization is a generic term that refers to a method that is employed in BMS design to remediate the fact that the battery pack consists of cells connected in series that suffer from inconsistency in their degradation rate and consequently cause the measurement from each of the cells to have different values with respect to time. It is extremely unlikely that cells are still homogeneous after many cycles of operation, even if they were manufactured exactly at the same time and date, and with high quality control. The reasons are, among many, the different temperatures across the battery pack, environmental conditions, inconsistent mechanical and electrical stress, etc.

The more cells that are connected in series in a pack, the greater the variation between cells will be. When a battery pack that consists of a series of connected cells becomes imbalanced, the total output power or energy from the pack will be reduced and will result in premature cut-off of power supply, even though there is still a significant amount of unused energy in the pack. If this scenario is not corrected, the effect will be exacerbated with continual usage of the battery pack and subsequently, the cells will drift apart from each other.

There are various battery cell equalization techniques and algorithms that have been employed in the past decade, and Table 2 presents an overview of the circuitry topologies that have been widely reported (Omariba et al. 2019; Qi and Lu 2014; See et al. 2019; Wei et al. 2010). They are generally classified into two major types, passive equalization techniques and active equalization techniques. The passive technique is relatively simpler and lower in cost to implement, with excess energy from any of the cells in the pack dissipated through a parallel resistor connected to the cell. The current flow through the resistor is either fixed (for nickel and lead-acid type batteries) or controlled through switches (field effect transistors (FETs)) that are connected in parallel to each individual cell. The BMS will have the software commands built inside to allow the switches to open or close in accordance with the balancing requirements.

The active technique, on the other hand, is a non-dissipative method, which utilizes a mobile shunt component or a voltage or current converter to transfer energy from one cell to another cell. Under this technique, there are three main groups: the capacitor based, inductor/transformer-based, and converter-based techniques. For the capacitor-based group, there are generally two techniques that are commonly employed, and the differences, apart from the circuit topology, are the duration or time of the equalization process. The more complex the components used in the design, the shorter the time that will be required for the cells to equalize.

Table 2 Passive and active techniques for battery equalization management

Cell balancing/equalization	
Passive	<p>Fixed shunt resistors:—Cells with higher energy have it dissipated through parallel resistors as heat until all cells match</p> <p>Switched shunt resistors:—Cells with higher energy have it dissipated by switch control that decides which resistor should be shunted for balancing</p>
Active	<p>Capacitor Based Switched capacitors Double-tiered switched capacitors</p> <p>Inductor/Transformer Base Single inductor Multi- inductor Single transformer Multi-transformer</p> <p>Converter Based Cuk Converter Buck/boost Flyback Ramp Full-bridge Quasi-Resonant</p>

The inductor/transformer-based design employs electronic winding components (e.g., inductors or transformers) for the intermediate energy storage, instead of capacitors, to transfer charges from one cell to another cell. Generally this technique achieves faster times due to the higher current transfer and fast switching speed of the improved components.

The most sophisticated active equalizer is the converter-based equalizer, which has the highest flexibility for controlling the equalization process. This technique, in addition to bidirectional charge transfer from cell to cell, also allowed for charge transfer to the whole battery pack and vice versa. The higher efficiency of the equalization management comes with the expense of higher complexity and production costs. In addition to the hardware, the algorithms for the respective battery equalization techniques also essentially require tedious development. They are generally divided into 3 different strategies: cell’s voltage uniformity, SoC uniformity, and remaining capacity uniformity. At present, most commercial BMS systems utilise the voltage-based algorithm because of its simplicity and reliability, as the voltage data is acquired through the monitoring system rather than the SoC or SoH which are based on estimation algorithms.

5 Battery thermal management

High power or energy battery applications require efficient thermal management systems to ensure that the temperature gradients between cells are minimised, reducing the probability of hot spots, preventing thermal runaway, maintaining a healthy range of operation, and consequently increasing the battery pack lifetime. Battery pack thermal management is typically categorised (Bandhauer et al. 2011; Katoch and Eswaramoorthy 2020; Shuai et al. 2018; Smith et al. 2018) into the: (1) air-cooling method, (2) liquid-cooling method, (3) refrigerant-based cooling, (4) thermoelectric module cooling, (5) phase-change material (PCM)-cooling, and (6) hybrid methods. Cooling of the cells is complicated by the thermal resistance of the electrolyte and plastic components in the cell, limiting the heat transfer to the surfaces of the cells.

Depending on the environmental conditions, it might be required to heat the cells to bring the temperature into the allowable operating window. The air-cooling method is the simplest form of structure and is energy saving, but efficiency is low, and it is generally not recommended for high power or energy applications. Liquid-cooling, on the other hand, has the highest efficiency and provides good uniformity with a compromise in energy consumption, added complexity, and weight. More advanced methods, which include PCM, thermoelectric module, or hybrid cooling, are easy to

integrate, compact, and have good efficiency. Their implementation is higher cost, however, and in some cases adds significant maintenance complexity to the whole battery pack system.

The battery thermal management and BMS are treated by many researchers as the subjects of distinctively separate investigation due to the fact that BMS is more involved with algorithms and circuit topology whereas battery thermal management is more relevant to mechanical considerations, thermodynamics, and fluid dynamics. Nevertheless in real application scenarios, the battery thermal management system, which is involved in air and liquid cooling, is monitored and controlled by the BMS, because the battery sensory circuits are all embedded inside the BMS and the output from the system (either digital or analogue), will adjust the power required for the thermal management to heat, equalise, or cool the battery cell. Hence, it is absolutely paramount to adequately manage the power requirement for the thermal system through an effective algorithm inside the BMS to ensure the optimum operation of the whole battery pack.

6 BMS for electric transportation

Electric transportation has been experiencing a rise in popularity over the past few years as the technology has matured and costs have declined, and support for clean transportation has promoted awareness, increased charging opportunities, and facilitated electrification adoption. BMS has a significant role in safe operation, energy usage optimization, charging functionality, communication with the vehicle control unit, and user interfaces and interactions.

Figure 1 shows a typical powertrain system structure of a battery-powered traction system. The battery is the only single source of power and energy, and consists of hundreds of individual battery cells connected together to deliver large

capacity and power to the system. It has essentially only two modes of operation, charging and discharging. In charging mode, the battery receives power from an external charger designated for the battery pack or at least meet the requirements or specifications of the battery pack.

The battery also receives power through the regenerative mechanism of the electric motors and controllers during operations, these are the momentary events that only occur when the vehicle initiates braking. In discharge mode, the battery powers the electric motor that converts the electrical energy to mechanical energy. The mechanical drive transmits the rotational energy to the wheels of the vehicle. The battery also satisfies the remaining on-board power requirements such as sensing, communication, infotainment, the heater, air conditioning, thermal management, etc.

7 Topology of BMS

In high-power applications such as traction battery packs, the energy and power required by the electric drivetrain are entirely provided by cells connected in parallel and series with voltage up to 600 V. Note that parallel cells are no different from one cell for BMS monitoring circuits because the parallel connection has the same voltage across the terminals. The BMS topologies in general can be classified into four different types or networks (Jinrui and Meng 2013; Rahimieichi et al. 2013, Reindl et al. 2020): (1) centralized, (2) modularized, (3) distributed, and (4) decentralized. In the centralized system (Fig. 2a), all the series battery cells in the pack are monitored and managed by an entire single control unit. The advantages are obviously cost effectiveness, and easy maintenance and fault diagnosis. Due to only one electronic board that performs everything, however, the complexity of a large number of lengthy cable connections for a large battery pack increases the risk of short

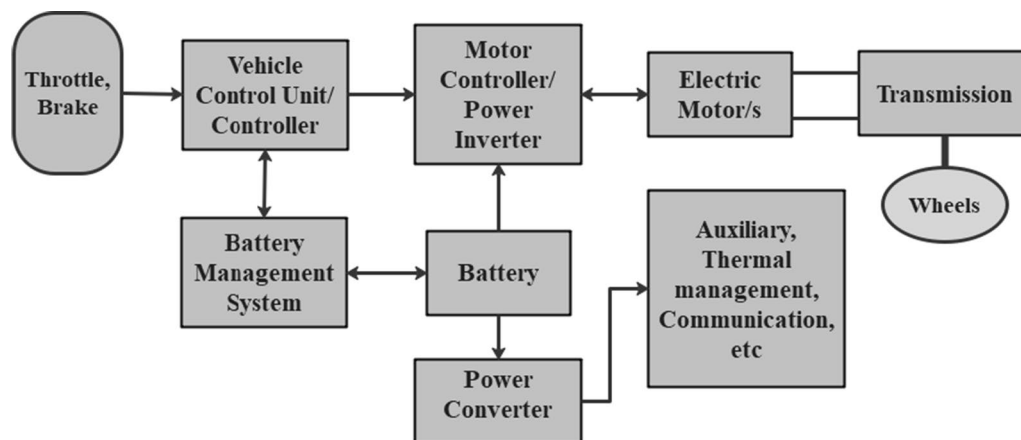


Fig. 1 Typical BMS operation inside an electric powertrain system

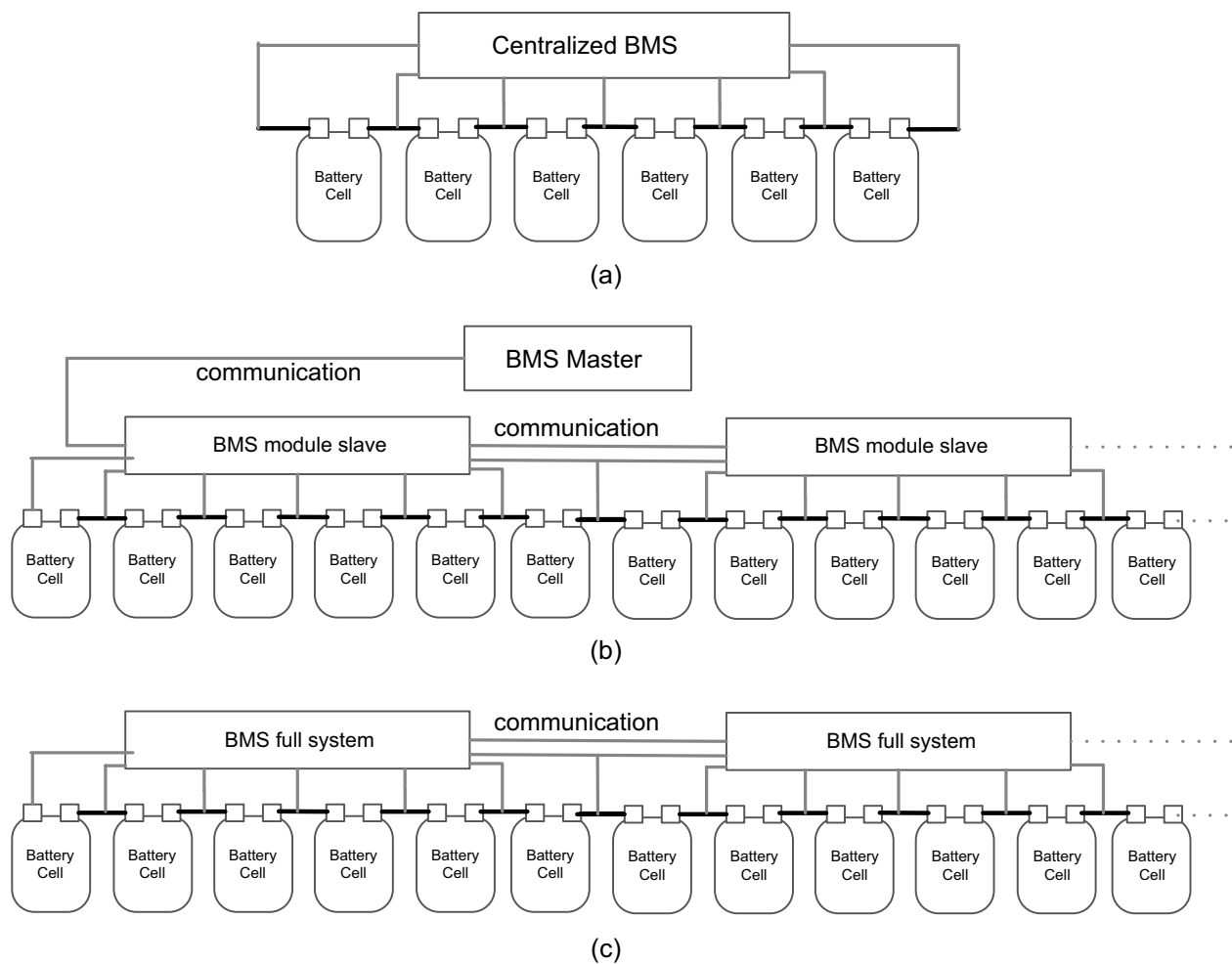


Fig. 2 Typical topology of large-scale battery pack BMS systems. **a** Centralized network; **b** Modularized/distributed network; **c** Decentralized network

circuits, loose connections, and susceptibility to errors. It also lacks scalability and flexibility, since only a predefined number of battery cells are allowed and a new reconstruction or design is required if additional cells or different battery pack configurations are needed in different application areas. Modularized BMSs, as shown in Fig. 2b, are similar to the centralized network, but now the battery cells are connected through several identical electronic boards that are evenly distributed among the cells. These boards are then usually connected to one larger control board that serves as the manager for all the distributed boards. This is commonly known as the master–slave configuration, with the slave represented by the boards connected directly to the battery cells for monitoring, acquisition, equalization, and communication. The master control board manages all the commands and decisions by consolidating all the data received from each slave board and transmits all communication to all components in the application system. The modularized topology potentially improves the performance

of the BMS by providing a safe, reliable, and cost-efficient solution for large-scale battery pack systems that are utilized in smart grids and automotive systems. The advantages of such topology include manageability, scalability and flexibility. In most system design, one master control board is capable of managing up to ten slave boards with no added complexity and compromise on the system integrity. As the slave boards can be distributed along the series battery cells in the pack, the issues of connection robustness and lengthy cables are no longer relevant. Nevertheless, the modularized BMS can sometimes incur higher cost as compared to the centralized system, and a control master board can only have a fixed number of slave boards connected to it.

A distributed topology system is generally similar to the modularized network, with the difference that each slave board is given more authority and control over the battery cells that are respectively connected to them. This network system is usually employed with the modular battery pack configuration. Each battery pack module contains its own

BMS, which resembles a fully independent system, and then, all the modules are connected together to make a larger battery pack. Such a topology is commonly employed in energy storage for renewable integration systems. Then, each BMS pack module communicates with the central control management system merely for data collection, storage, analysis, and safety control. Depending on the application requirements, the central management system could have little or quite substantial control over each modular system, and it provides additional protection to the battery cells through system integrity by checking on every modular pack system. No maximum number of inputs is defined, and cells or modules can be added or removed at any time required by the applications. The decentralization of BMSs in Fig. 2c means that each battery pack unit contains its BMS with full functionality, locally and autonomously. The communication lines that exist between the battery pack systems are used to enable information exchange and sometimes to provide power sharing among connected components and battery packs. As the operation of each battery pack system works independently, the failure of an individual functional unit has very minor or no impact on the functioning of the whole system. As such, the reliability of the system is improved, with the robustness and adaptability increasing to match the requirements of a wide range of applications.

8 The safety considerations of BMS

The BMS of an electric propulsion system and large energy storage pack has tremendous critical responsibility, as it supervises and controls a large number of high-capacity cells connected in series. The safety of the battery pack system, particularly for applications in hazardous environments such as in underground coal mining, is of paramount concern. There are various essential aspects to be considered to assure the safety of the integrated battery pack systems, such as, high voltage (HV) safety, functional safety, and safety from unauthorised manipulation (security). In this section, the authors will introduced all three components with a brief generic example of an electric traction system, which is most common in general mobile applications.

8.1 Functional safety applied to BMS development

The goal of functional safety is to minimize the risk to an acceptable level, with risk defined as the probability of the occurrence of damage and the impact of the damage on personnel or, to a lesser extent, on equipment and the surrounding environment (Kumar and Balakrishnan 2019). The methods that can be employed to reduce risks are typically grouped into three: fault avoidance, fault detection, and fault handling measures (fault control). The safety standard IEC

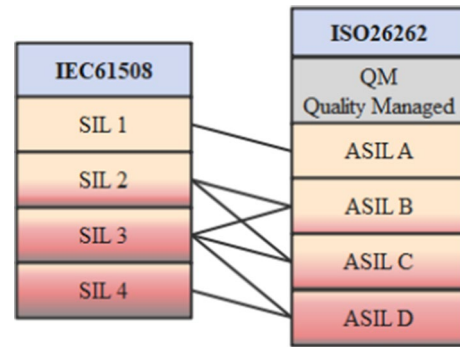


Fig. 3 Approximate cross-mapping of Safety Integrity Levels

61508 is the umbrella (general) standard that covers electric, electronic, and programmable electronic safety-related systems for all relevant sectors of industry. Through this reference, various specific safety standards have been derived to cater for specific industries, such as ISO 26262 for automotive sector (Kafka 2012).

IEC 61508 calls its stringency levels Safety Integrity Levels (SILs), whereas ISO 26262 uses Automotive Safety Integrity Levels (ASILs). This stringency is defined as: SIL 1 being the least critical followed by 2, 3, and 4 being the most critical, and similarly, ASIL A being the least stringent, and B, C, and D being the most stringent. The safety levels of both standards are generally quite different, and there is no direct correlation between the IEC 61508 SIL and ISO 26262 ASIL levels. To roughly compare the two, Fig. 3 illustrates the approximated mapping of the safety levels. In the ASIL system, there is a classification called Quality Management, which indicates that there is no need to implement additional risk reduction measures and that management under the ISO 26262 Standard is not required, which is similar to SIL 0.

In this article, although the focus is generally on battery pack systems for electric propulsion systems, the functional safety review will be based on the IEC 61508 SIL Standard instead, as it represents a more generic approach and complements the IEC 60079 Standard for hazardous environment such as in underground coal mining. Henceforth, the acronym SIL will be used for the rest of this article. The Safety Integrity Level (SIL) is used to define the reliability of a Safety Instrumented Function (SIF) as a way to measure the performance of a system. The SIF is a protection layer with the objective of achieving or maintain a safe state of the particular process when a specific dangerous event occurs. The SIF is implemented in the (Safety Instrumented System (SIS), which is normally composed of several Safety Functions. The SIF is a combination of sensor(s), logic solver(s), and final element(s) that detect a hazard and bring the system to a safe state. Its ability to detect, decide, and act is designated by the safety integrity

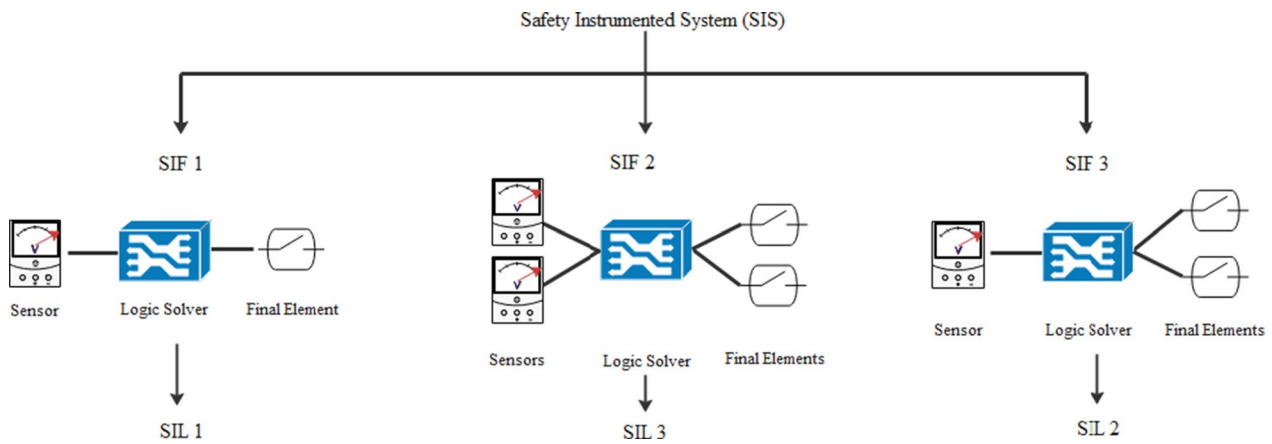


Fig. 4 Relationship between the Safety Instrument System (SIS), Safety Instrumented Function (SIF), and Safety Integrity Level (SIL)

Table 3 Safety integrity levels for a safety function operating in low and high demand modes of operation, with SIL 4 having the highest level of safety integrity and SIL 1 the lowest

SIL	Reliability (%)	PFDD (low demand)	RRF (1/RRF)—low demand	PFDD (high demand, failures per hour)
1	90.00–99.00	0.1–0.01	10 to 100	$\geq 10^{-6}$ to $< 10^{-5}$
2	99.00–99.90	0.01–0.001	100 to 1000	$\geq 10^{-7}$ to $< 10^{-6}$
3	99.90–99.99	0.001–0.0001	1000 to 10,000	$\geq 10^{-8}$ to $< 10^{-7}$
4	> 99.99	0.0001–0.00001	10,000 to 100,000	$\geq 10^{-9}$ to $< 10^{-8}$

level (SIL) of the function. Each SIF has a stated SIL that is related to the probability that the SIF will not work when challenged (when needed). Figure 4 shows the relationship between the SIS, SIF, and SIL through the example of a typical SIF configuration.

The SIL of a SIF system defines a reliability range, and this can be expressed as the Probability of Failure on Demand (PFDD) or Risk Reduction Factor (RRF), which is the inverse of the PFDD (Innal et al. 2010). As is shown in Table 3 the higher the SIL level, the more reliable the system design is, but it comes with trade-offs such as higher hardware costs, more frequent maintenance operations, and higher exposure to more nuisance trips. Hence, it is vitally important to determine the proper SIL level of each SIF system during the design process and through a comprehensive risk assessment process. Note that there are two operating modes when classifying the SIL of equipment or a system: (1) low demand mode and (2) high demand mode. Low demand functions have less stringent requirements, which are expressed in a period of years. For instance, a SIL 1 rated safety function has a maximum hazard frequency of once in every 10 years. High demand or continuous demand functions certainly have more stringent requirements, such as for transportation applications where constant monitoring and safety

functions are required continuously. The hazard frequency is therefore expressed on an hourly basis with the SIL 1 rated safety function. For instance, the maximum allowable hazard frequency is 10^{-5} in 1 h or 1 in 100,000 h.

The IEC 61508 standard requires a specific hardware fault tolerance (HFT) in connection with a specific proportion of safe failures, defined as 1—the proportion of unrevealed hazardous failures, for each designated SIL classification. HFT refers to the ability of a device to continue carrying out the safety function correctly when an error occurs. It is determined by the number N , which means that $N + 1$ faults can lead to the loss of the safety function. The proportion of safe failures is called the Safe Failure Fraction (SFF), and it is determined based on the individual failure rates (λ values) of the individual components. Hence the SFF is defined as the ratio of the rate of safe failures to the total failure rate of the component, as shown in Eq. (1) (Smith 2011)

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} \tag{1}$$

where the sum is taken over all relevant items:

λ is measured in Failures in Time (FIT), which denotes the number of failures that can be expected in one billion (10^9) device-hours of operation.

λ_S is the rate of safe failures, which comprises the safe detected failure rate λ_{SD} and the undetected failure rate λ_{SU} .

λ_D is the rate of dangerous failures comprising the rate of dangerous detected failures λ_{DD} and the undetected failure rate λ_{DU} .

Safe failures or ‘Fail Safe’ means that the equipment has no impact on safety functions and will not endanger lives or facilities when it fails. These failures are often referred to as spurious failures or nuisance failures, since operation is unnecessarily stopped. Dangerous failures are the opposite, and they inhibit the system from taking action when it is called upon to do so. The undetected dangerous failures are


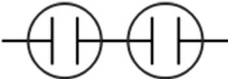
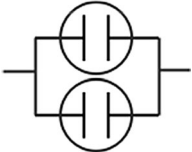
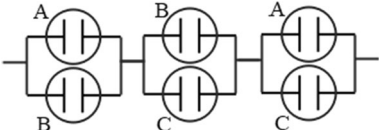
the ones that are of great concern, since the failure does not reveal itself, lying in wait until the system is called on to take its safety action but it cannot. Such failures have to be kept to a minimum using all possible corresponding measures, including the detailed risk assessment process.

The determination of SIL based on HFT and SFF is illustrated in Table 4 below for both low and high complexity subsystems. They are called Type A and Type B systems, respectively. Type A products are simple products for which all failure modes are known, such as metal film resistors, transistors, relays, etc., whereas the Type B products are complex products with failure behaviour that is not fully known, e.g., microprocessors and semiconductor circuits. IEC 61508 imposes architectural constraints to limit the SIL that can be claimed for any safety function on the basis of its HFT and SFF. It requires a subsystem to have a minimum level of redundancy based on its SFF to ensure the required

Table 4 Maximum allowable safety integrity level for a safety function carried out by a Type A or Type B safety-related element or subsystem

Safe failure fraction (SFF)	Hardware fault tolerance (HFT) Type A—simple component			Hardware fault tolerance (HFT) Type B—complex component		
	0	1	2	0	1	2
<60%	SIL 1	SIL 2	SIL 3	Not permitted	SIL 1	SIL 2
60%–<90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90%–<99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Table 5 Safety function configuration with respect to the architecture or voting arrangement of a particular SIF

Voting arrangement	Safety configuration	PF _D (probability of failure)	STR (spurious trip rate)
1oo1	 One switch with one contact	1.0×10^{-2}	1.0×10^{-6}
1oo2	 Either one of the two switches can shut down the operation	1.0×10^{-3}	2.0×10^{-6}
2oo2	 Both switches must ‘agree’ to shut down the entire system	2.0×10^{-2}	1.0×10^{-9}
2oo3	 Each switch needs two contacts	3.0×10^{-3}	3.0×10^{-9}

The PF_D and STR values are for comparison purposes

hardware fault tolerance. Such a device or component with a low SFF requires a certain degree of redundancy to achieve the targeted SIL level. A system with $HFT=0$ means that 1 fault may lead to loss of safety function, while $HFT=1$ means that 2 or more faults are needed for loss of safety function.

One of the key design parameters in calculating the safety function is the architecture or voting arrangements of the various subsystems that comprise a safety instrumented function (Torres-Echeverria et al. 2011). The architecture/voting arrangement is essentially the use of redundant pieces of equipment or devices for the purpose of creating the ability to tolerate a failure of one component and still have the safety function perform its action (Hokstad 2005). The selection or design of an appropriate voting arrangement will be taken into account. The level of safety, the failure modes, the rate of spurious failures, and all the associated consequences in terms of cost effectiveness and necessity must be achieved. The most commonly used voting arrangements are: (1) One-out-of-one (1oo1), (2) One-out-of-two (1oo2), (3) Two-out-of-two (2oo2), and (4) Two-out-of-three (2oo3). The first number in this arrangement is the number of devices that must 'vote' to cause a trip for the trip to occur. The second number is the total number of devices. Hence, for 2oo2 arrangement, 2 devices out of a total of 2 must vote to trip for the shutdown to occur. Table 5 illustrates the safety function configurations of the respective voting arrangements, taking the component as a switch or contactor, for example. The 1oo1 arrangement is the easiest and cheapest, but there is no failure tolerance towards either dangerous failures or safe failures. In contrast, the 1oo2 arrangement allows for one dangerous failure ($HFT=1$) because if one of the switches is welded closed, the other switch could still open to de-energize the system. On the other hand, if any of the switches suffers from safe failure (open circuit), the entire system will fail spuriously. Hence this voting has a lower PFD but doubles the Spurious Trip Rate (STR). It is used to achieve the SIL target but at the cost of tolerating a higher spurious failure rate. In the 2oo2 arrangement, both switches must 'agree' to shut down the entire system. De-energizing either one of the switches alone will not cause the entire system to stop. There is no tolerance towards dangerous failures. If any of the switches fails 'to open', it will result in dangerous failure of the entire system, although it has one degree of tolerance to safe failures. If any of the switches spuriously fail in open circuit mode, power will still be conducted through the other switch, preventing spurious shutdown. The more complex configuration is the 2oo3 arrangement. This system provides one degree of tolerance to dangerous failures and also to safe failures. If any one of the switches suffers a dangerous failure, the other two switches will still be able to stop the system. The same is true for spurious shutdown. This system is complex

and costly, with targeted SIL levels of 2 and above, while also reducing the spurious trip rate. For the purpose of comparison, the values of PFD and STR are set to a baseline so that the characteristics of the different voting arrangements can be quantitatively compared. In the Table, each of the arrangements are distinctively shown to employ a particular safety function. Thorough consideration of the benefits and drawbacks is required when a voting architecture is chosen for a system. The PFD figure is essentially the reference for the required SIL target while the STR figure corresponds to the tolerance of the system towards safe failures.

BMS development has stemmed from the emergence of lithium-based batteries. Unlike conventional nickel/lead-based batteries, they do not tolerate any overvoltage and may require secondary functions to work safely, e.g., thermal management. BMS has to monitor the voltage and temperature, measure current in different vehicle operating modes, and effectively take the necessary action to protect the battery cells from operating out of their specifications and from degradation. The safety function hence entails monitoring the battery pack state via the BMS sensors, which then transfers the information to the BMS processor units, which further take action on the power contactors and actuators. The safety requirements for BMS hardware and software architecture and design are covered, with express directives given for BMS hardware components, architectures, and software module design. In order to do this, it is necessary to understand the detailed working mechanism of the BMS design architecture. The hardware software interface (HSI) has to be defined in the system design phase, which specifies the elements' hardware interfaces that are controlled by software and resources that support the software components, which includes the operating modes of the hardware devices and software configuration parameters. An HSI specification further includes hardware features that assure element independence, define the use of hardware resources, and describe the access mechanisms and timing constraints for hardware components (Macher et al. 2015a, 2015b). The IEC 61508 Standard introduces the concept of an overall safety lifecycle as well as software development processes with guidelines and design principles that jointly contribute to the formation of integrated elements and items to be incorporated into the whole vehicle/application system. The details of these processes have been discussed and studied by other research groups (Brissaud and Turcinovic 2015; IEC 61508-1 2010; Kriaa et al. 2015).

As shown in Fig. 5, a generic example of a basic BMS hardware architecture is utilised to illustrate the preliminary system design analysis considering the risk modes and functional safety requirements. The BMS is divided into a battery cell/module, an analogue front end (AFE), a microcontroller (MCU), and a control unit for digital output to control external components. Based on the sensing

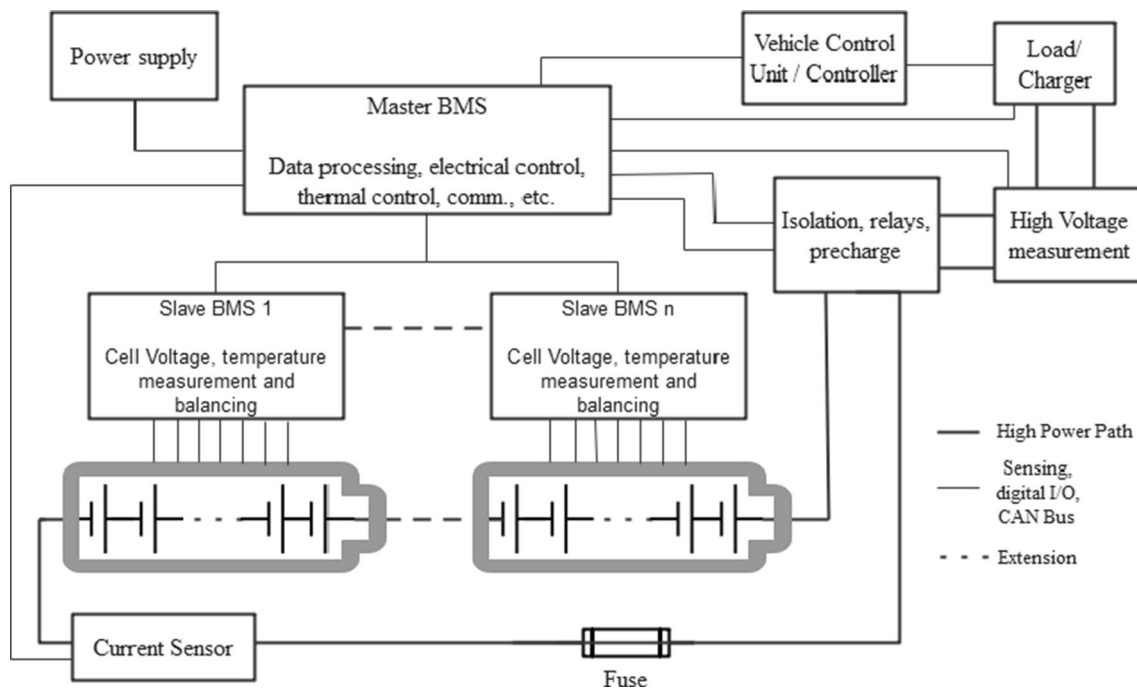


Fig. 5 Example of a basic BMS architecture and the functional safety concept

parameters (voltage, current, temperature) through the AFE, the MCU will decide whether the data is out of the safety range and take action through the control unit to de-energize or disconnect the battery cells from the external circuit through the relays or power contactors. The failure rate for these components should be obtained from the manufacturers and calculated to obtain the relevant PFD and SFF figures, which then are input into the voting arrangement to obtain the SIL level of the respective safety functions. If the targeted SIL level is not achieved, improvement in the voting arrangement, higher quality components, or more frequent maintenance operations are required to reach the target. In the underlying process of identifying all the associated risks and hazards, the Failure Modes, Effects and Diagnostics Analysis (FMEDA) is essentially required as the tool for risk assessment and for certification against IEC 61508 in most certification agencies. FMEDA is a detailed analysis of the different failure modes and diagnostic capabilities of equipment, devices or components. Table 6 shows a preliminary FMEDA analysis for all the corresponding major components, as shown in the example in Fig. 5. These components constitute the key functionalities of the BMS and can effectively detect all the possible abnormalities in the battery cells, sensing system, processing system, and isolation system. From the functional safety point of view:

(1) The voltage, current, and temperature measurement of the battery cell involves a single channel (voting

arrangement is 1oo1), and hence there is no redundancy or lack of reliability of the sensing system.

- (2) Since the sensing system has no redundancy, any malfunction of the sensors will cause catastrophic failure, as the BMS has lost its most critical functionality, which is the diagnostic system.
- (3) Instability of the microcontroller clock frequency will cause malfunction in the BMS control system and subsequently trigger the dangerous failure condition, even if the sensing elements are healthy.
- (4) Any error or failure in the microcontroller firmware will caused inability of the BMS to diagnose and control the electrical system. Such circumstances will further escalate to system failures that might cause severe damage or even injuries to personnel.

Based on the functional assessment, the following suggestions or remedies could be implemented for risk reduction procedures that will further reduce the PFD to achieve the targeted SIL level:

- (1) Additional sensing elements through the addition of hardware and relative comparisons and logic assessments made in the MCU to ensure the reliability and robustness of every sensor.
- (2) Implement two channel and the 1oo2 architecture arrangement for the control unit and isolation system so as to provide at least one redundancy.

Table 6 Basic FMEDA analysis for corresponding BMS major components

Main component	Potential failure mode	Potential causes	Potential effects
Lithium-ion battery	Short-circuit	Cell balancing error, wrong connection	Battery damage, degradation, fire
	Abnormal output voltage	Low battery capacity, overheating	Load damage, battery fire, explosion
	No output	Poor performance	System malfunction
	Cracking	Lower battery capacity	System performance degradation
	Discontinuous operation	Lower battery capacity	System performance degradation
Analog Front End IC	AFE IC fault	Component Fault	Monitoring and control fault, dangerous failure
	Voltage measurement error	Measurement circuit component error	No over-/under-voltage control, dangerous failure
	Current measurement error	Measurement circuit component error	No overcurrent control, dangerous failure
	Temperature measurement error	Measurement circuit component error	Dangerous Failure, fire or explosion
Microcontroller unit	Operation error	Unstable source voltage/clock	No battery control, dangerous failure
	Bits error (SRAM/flash memory)	Unstable source voltage/clock	No battery control, dangerous failure
	Communication failure	Circuit fault, unstable source voltage	Not receiving measurement data
	ADC read error	Measurement circuit error, unstable source voltage	Current and temperature error, dangerous failure
Charging, discharging relays and isolation	Inoperative	Component fault, wire disconnection	No safety function, dangerous failure, fire and explosion
Driver IC (for FETs, MOSFETs)	IC/component fault	Component flaw, damage	No isolation control, dangerous failure, fire and explosion
	Control failure	Circuit abnormality, component fault	No isolation control, dangerous failure, fire and explosion
Sensing component (voltage, temperature, and current)	Abnormal readings, no readings, abnormal behaviour	Component fault, IC damage, circuit abnormality	No battery parameters measurement, error readings, dangerous failure, fire and explosion

IC: integrated circuit; MOSFET: metal-oxide semiconductor field effect transistor; SRAM: static random-access memory

- (3) Include an external crystal oscillator to remedy the problem of instability of the MCU internal clock and make a relative comparison between the two clock frequencies. If any difference in value exceeds the set-value, isolate the battery cell.
- (4) In the event of an error detected in the firmware operation procedures, the system should be designed to de-energise, and disconnect or isolate the battery cell from all the external circuitry after a set period of time.

The functional safety concept is introduced in this example, although simplified, but nonetheless it provides several important considerations that need to be taken into account when designing a full-scale SIL compatible BMS for a large energy or capacity battery pack. The key points presented are those routes by which the most common failures that a BMS could encounter occur and potentially cause severe mishap to the system applications, operators, and consumers.

Performing quality FMEDA analysis is significant not only to ensure that the risk is tolerable and manageable, but also to prevent unnecessary excess in design complexity, cost, and maintenance operations. A full introduction on how to conduct an FMEDA is beyond the scope of this paper and can be found in (Löw et al. 2011).

8.2 High voltage safety system

The importance of recognising the high voltage (HV) and low voltage (LV) circuitry in a battery pack system design is paramount to ensure adequate isolation requirements and hence the overall safety of the battery pack. The HV system is defined as the path for the main current from the battery pack to flow to the application load system. In practice, it is visible through the size of the current carrying conductors, which are considerably larger than for the rest of the wiring system and connected to several bulky components

in the entire power train system. One of the most fundamental operations is to effectively isolate the poles of the battery pack so that further charging and discharging of the entire battery pack is terminated when the allowed voltage, current, or temperature operating limits are violated. To do this, pole-cutting relays or contactors are employed. These components have high make-and-break current tolerances at high voltages and allow safe disconnection of the poles even under load. Functional safety analysis, as mentioned in Sect. 8.1, shows the necessity of isolating both the HV+ and HV− battery poles to safeguard the complete separation, even if one of the contactors remains trapped in the closed position. Employing relays with auxiliary contacts in place is highly recommended, so as to allow the detection of the position of the main current-carrying contactor and to facilitate diagnostic mechanisms such as detecting faulty operations or logics. In addition to the isolation system, it is also essential to limit the inrush current once the contactor is closed to protect the relays and other power electronics from damage. The inrush current is caused by the rapid closing of the contact between the HV source and the electrical load, such as an electric motor. This function can be performed through a pre-charge circuit that consists of a power resistor that limits the initial peak current and a relay to switch the resistor into the current path. The power resistor also serves to discharge any DC link capacitor that can be sourced from the power electronic components inside the electric motor controller. Discharging the left-over charge of the capacitor after deactivation of the battery pack allows safe disassembly of the HV system during maintenance or troubleshooting

operations. Figure 6a presents a schematic of a typical example of the HV relays and pre-charge circuit configuration that are employed in automotive battery pack systems (Johnson 2014).

Fuses are another type of critical and essential component that are employed in HV battery pack systems for isolation purposes through high or excess current conditions. Excess current, commonly caused by short circuits or malfunctions of sensing elements, can lead to dangerous types of failure such as fire and explosion. It is extremely critical that every fuse employed in an HV battery pack system needs to be thoroughly scrutinised through the manufacturer's data-sheets and found to comply with all relevant safety standards to make certain that the safety operation of the large-scale battery pack system is not compromised. Apart from the electronically-controlled safety devices, manual interlocks and breakers should be integrated into the HV system. This is to ensure that no HV connectors are left open with exposed cable contacts, while also making certain that the isolation procedures are effective.

In some circumstances, such as in underground coal mining, extreme conditions such as strong and frequent vibration, extreme temperature, dirt, dust, or water encountered throughout the lifetime of the operational battery pack system can affect the safety components through unintentional connections between the HV power lines and low voltage (LV) grids. Such conditions will lead to severe consequences such as loss of BMS functionality and subsequent dangerous failures. To prevent these from happening, the isolation resistance between the HV and LV grids has to be monitored through the Insulation

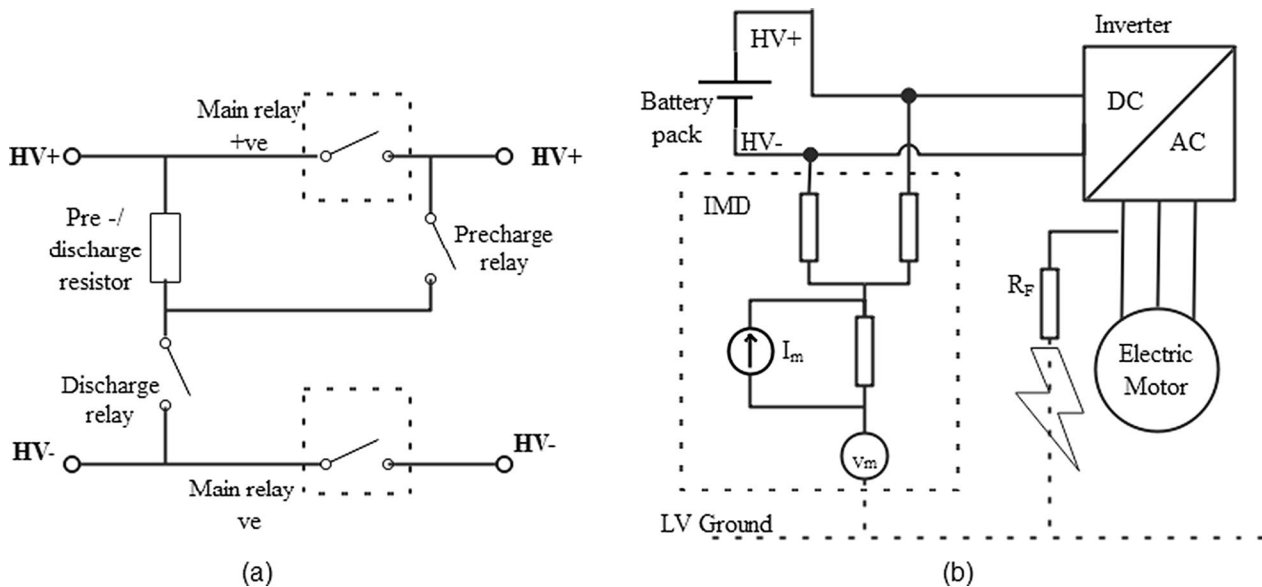


Fig. 6 High voltage system safety components: **a** Pole cutting relays and pre-charge/discharge circuit; **b** Working principle of insulation monitoring device

Monitoring Device (IMD). The IMD is connected to the HV lines, both the HV+ and HV−, and to the multiple points of the LV ground, which is the chassis of the vehicle for the traction system. The device will then superimpose a voltage signal on the HV lines, and if there is a current flow between the HV and LV grids due to accidental connection, the device will pick up the voltage drop across the measuring resistance R_m . If the voltage drop exceeds the set value proportional to the insulation resistance R_F , an alarm will be issued, and the isolation system will be triggered. Figure 6b shows the general measurement principle schematically, and more information can be found in other sources (Bender and KG 2013; Hauser and Kuhn 2015).

In general, the two important aspects of HV safety that need to be taken into thorough consideration for any development of a BMS for use in large-scale battery pack applications are (1) safety of the development personnel or engineers at the manufacturer and the maintenance level, and (2) safety of the system operators and end users or customers when the product is in operation (Brandl et al. 2012; Chatzakis et al. 2003; Jossen et al. 1999).

8.3 Unauthorised manipulation of the safety system

The concerns about security flaws in the embedded control systems of BMS and other related components has been extensively addressed. Regrettably, security issues are not uncommon in modern and advanced society. In the past, many embedded systems were developed without considering the security of the information technology (IT), and the communication channels were often unprotected and vulnerable to manipulation by others. As the main task of a BMS is to prevent dangerous failures or hazards originating from the battery cells, manipulation or corruption of the data received by the BMS will lead to catastrophic events. Therefore, any developers of the system must consider whether IT security is taken into account during the development process. A thorough review on the scope of this focus is presented in (Sagstetter et al. 2013), which includes the basic protection principles. For example, the separation of communication channels and use of gateways (private bus, internal vehicle control network, and external charging communication bus) to complicate access to control information is of great importance. The security development should also consider limited or controlled access of personnel to the system firmware and data, and initiate plausibility checks for critical commands such as control of pole cutting relays, charging operations, activation of balancing circuits, and transferring information to external devices.

9 Concluding remarks

The increasing number of large-capacity and high-energy lithium ion battery packs in both mobile and stationary applications have certainly had an impact on the progress of development of Battery Management Systems (BMSs) with more stringent requirements on both safety and functionality. The BMS is one of the basic units in every battery pack system and the only one interacting with the connected battery cells that receives and gives information and instructions on all internal and external events. In this article, the details of BMS systems for electrical transportation and large-scale storage applications have been discussed, including components, functionalities, topology, operation, functional safety, and internal architectures.

Depending on the application, the BMS can have several configurations, but the essential operational goal and safety aspects of the BMS remain the same, which is to protect the battery and the whole associated system. The industry standards covering the BMS functionality and safety are also presented, and some recommendations are provided to pave the way for the development of future BMS systems to facilitate a more robust, versatile, and demanding working environment. Furthermore, the development of novel safety devices such as high-power electronic fuses and unidirectional pole-cutting relays are well under way and will lead to faster reaction times and non-destructive activation or deactivation. Together, these devices create the opportunity to provide the industry with a more comprehensive energy storage system that not only exhibits excellent functionality, but also delivers the highest quality safety features.

In addition to improving the safety and reliability of battery systems, advances in battery state estimation, power optimization, and the user interface experience are of great significance for the next generation of BMS. All of these are conducive to making the battery pack system more transparent, not only to the external components, but also to the operators and users. More powerful embedded processors and feasible data storage solutions enable the use of more elaborate cell models and power-usage history data, and support complex functionality to improve the remaining range predictions as well as the operating life of the battery pack. Compatibility between various systems and corresponding safety functions must be meticulously studied, and the BMS and battery should undergo various test run programmes before operation. These can be performed through a dedicated test bench with multiple test modes available for implementation and the ability to communicate all diagnostics via common communication buses.

Acknowledgements This work was greatly supported by Azure Mining Technology, CCTEG, and the University of Wollongong.

Author Contribution KS: Conceptualization, Methodology, Writing-Original draft preparation; GW: Supervision; YZ: Funding acquisition; YW: Validation; LM: Writing- Reviewing and Editing; XG: Data curation; NZ: Project administration; KL: Resources; LZ: Methodology; BX: Investigation. All authors read and approved the final manuscript.

Declarations

Competing interests The authors declare that they have no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Andrea D (2010) Battery management systems for large lithium-ion battery packs. Artech House, Boston, pp 44–49
- Bandhauer TM, Garimella S, Fuller TF (2011) A critical review of thermal issues in lithium-ion batteries. *J Electrochem Soc* 158(3):R1–R25
- Bender G & KG C (2013) Electrical safety for emobility. Grünberg. http://www.bender-emobility.com/fileadmin/products/b/e/Emobility_PROSP_en.pdf
- Berecibar M, Gandiaga I, Villarreal I et al (2016) Critical review of state of health estimation methods of li-ion batteries for real applications. *Renew Sustain Energy Rev* 56:572–587
- Bonfiglio C, Roessler W (2009) A cost optimized battery management system with active cell balancing for lithium ion battery stacks. In: IEEE vehicle power and propulsion conference proceedings, pp 304–309
- Bowkett M, Thanapalan K, Stockley T et al (2013) Design and implementation of an optimal battery management system for hybrid electric vehicles. In: Proceedings of IEEE 19th international conference on automation and computing, pp 1–5
- Brandl M, Gall H, Wenger M et al (2012) Batteries and battery management systems for electric vehicles. In: Design, automation and test in Europe conference and exhibition (DATE), pp 971–976. <https://doi.org/10.1109/DATE.2012.6176637>
- Brissaud F, Turcinovic D (2015) Functional safety for safety-related systems: 10 common mistakes. In: 25th European safety and reliability conference, Zurich, Switzerland
- Chatzakis J, Kalaitzakis K, Voulgaris NC et al (2003) Designing a new generalized battery management system. *IEEE Trans Ind Electron* 50(5):990–999
- Divyashree S, Madhavan P, Ranjeev A (2020) Battery management system integrated with CAN BUS safety control environment for electric vehicle. *Int J Eng Tech Res Technol* 9(9)
- Duong VH, Bastawrous HA, Lim KC et al (2015) Online state of charge and model parameters estimation of the lifepo4 battery in electric vehicles using multiple adaptive forgetting factors recursive least-squares. *J Power Sources* 296:215–224
- Duong VH, Bastawrous HA, See KW (2017) Accurate approach to the temperature effect on state of charge estimation in the LiFePO₄ battery under dynamic load operation. *Appl Energy* 204:560–571
- Faika T, Kim T, Khan M (2018) An Internet of Things (IoT)-based network for dispersed and decentralized wireless battery management systems. In: 2018 IEEE transportation electrification conference and expo (ITEC), pp 1060–1064
- Gabbar HA, Othman AM, Abdussami MR (2021) Review of battery management systems (BMS) development and industrial standards. *Technologies* 9:28
- Gu X, See KW, Wang Y et al (2021) The sliding window and SHAP theory—an improved system with a long short-term memory network model for state of charge prediction in electric vehicle application. *Energies* 14(12):3692
- Hauser A, Kuhn R (2015) High-voltage battery management systems (BMS) for electric vehicles. In: Scrosati B, Garche J, Tillmetz W (eds) Woodhead Publishing series in energy. Advances in battery technologies for electric vehicles. Woodhead Publishing, Sawston, pp 265–282
- Hokstad PR (2005) Probability of Failure on demand (PFD)—the formulas of IEC 61508 with focus on the 1oo2D voting. In: Esrel 05 IEC 61508-1 (2010) Functional safety of electrical/electronic/programmable electronic safety-related systems—part 1: general requirements. International Standard 2010-04-30 IEC 61508-1
- Innal F, Dutuit Y, Rauzy A et al (2010) New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Proc Inst Mech Eng Part O J Risk Reliab* 224:75–86
- ISO 26262 (2018) 2:2018, road vehicles—functional safety—part 2: management of functional safety
- Jinrui N, Meng G (2013) Studies on equalization strategy of battery management system for electric vehicle. *Sens Transducers* 19:57–63
- Johnson NM (2014) 19—Battery technology for CO₂ reduction. In: Folkson R (ed) Alternative fuels and advanced vehicle technologies for improved environmental performance. Woodhead Publishing, Sawston, pp 582–631
- Jossen A, Spath V, Doring H et al (1999) Reliable battery operation—a challenge for the battery management system. *J Power Sources* 84(2):283–286
- Kafka P (2012) The automotive standard ISO 26262, the innovative driver for enhanced safety assessment & technology for motor cars. *Procedia Eng* 45:2–10
- Katoch SS, Eswaramoorthy M (2020) A detailed review on electric vehicles battery thermal management system. *IOP Conf Ser Mater Sci Eng* 912(4):042005
- Kim CH, Kim MY, Moon GW (2013a) A modularized charge equalizer using a battery monitoring IC for series-connected Li-Ion battery strings in electric vehicles. *IEEE Trans Power Electron* 28(8):3779–3787
- Kim T, Wei Q, Qu L (2013b) Online SOC and SOH estimation for multicell lithium-ion batteries based on an adaptive hybrid battery model and sliding-mode observer. In: Proceedings of 2013b IEEE energy conversion congress and exposition, pp 292–298
- Kriaa S, Bouissou M, Ludovic P-C et al (2015) A survey of approaches combining safety and security for industrial control systems. *Reliab Eng Syst Saf* 139:156–178
- Kumar MNS & Balakrishnan K (2019) Functional safety development of battery management system for electric vehicles. In: 2019 IEEE transportation electrification conference (ITEC-India), pp 1–6
- Lee JH, Lee IS (2021) Lithium battery SOH monitoring and an SOC estimation algorithm based on the SOH result. *Energies* 14:4506

- Lelie M, Braun T, Knips M et al (2018) Battery management system hardware concepts: an overview. *Appl Sci* 8(4):534
- Li X, Yao L, Hui D (2016) Optimal control and management of a large-scale battery energy storage system to mitigate fluctuation and intermittence of renewable generations. *J Mod Power Syst Clean Energy* 4(4):593–603
- Lim KC, Bastawrous HA, Duong VH et al (2016) Fading Kalman filter-based real-time state of charge estimation in LiFePO₄ battery-powered electric vehicles. *Appl Energy* 169:40–48
- Lin CP, Cabrera J, Yu DYW et al (2020) SOH estimation and soc recalibration of lithium-ion battery with incremental capacity analysis & cubic smoothing spline. *J Electrochem Soc* 167(9):090537
- Löw P, Pabst R, Petry E (2011) Functional safety in practice: application of DIN EN 61508 and ISO/DIS 26262 in the development of series products. dpunkt.verlag
- Lu L, Han X, Li J et al (2013) A review on the key issues for lithium-ion battery management in electric vehicles. *J Power Sources* 226:272–288. <https://doi.org/10.1016/j.jpowsour.2012.10.060>
- Macher G, Sporer H, Armengaud E et al (2015a) Using model-based development for ISO26262 aligned HSI definition. In: CARS 2015a—critical automotive applications: robustness & safety. Paris, France
- Macher G, Sporer H, Armengaud E et al (2015b) A versatile approach for an ISO26262 compliant hardware-software interface definition with model-based development. SAE technical papers 2015b
- Masias A, Marcicki J, Paxton WA (2021) Opportunities and challenges of lithium ion batteries in automotive applications. *ACS Energy Lett* 6(2):621–630
- Nitta N, Wu F, Lee JT et al (2015) Li-ion battery materials: present and future. *Mater Today* 18(5):252–264
- Omariba ZB, Zhang L, Sun D (2019) Review of battery cell balancing methodologies for optimizing battery pack performance in electric vehicles. *IEEE Access* 7(99):1–1
- Qi J, Lu D (2014) Review of battery cell balancing techniques. In: 2014 Australasian universities power engineering conference, AUPEC 2014—proceedings, pp 1–6
- Rahimieichi H, Ojha U, Baronti F et al (2013) Battery management system: an overview of its application in the smart grid and electric vehicles. *Ind Electron Mag IEEE* 7(2):4–15
- Reindl A, Meier H, Niemetz M (2020) Scalable, decentralized battery management system based on self-organizing nodes. In: Brinkmann A, Karl W, Lankes S, Tomforde S, Pionteck T, Trinitis C (eds) *Architecture of computing systems—ARCS 2020. Lecture notes in computer science*, vol 12155. Springer, Cham. https://doi.org/10.1007/978-3-030-52794-5_13
- Sagstetter F, Lukasiewicz M, Steinhorst S et al (2013) Security challenges in automotive hardware/software architecture design. In: Proceedings of the design, automation & test in Europe conference & exhibition, Grenoble, pp 458–463
- See KW, Kai CL, Batternally S et al (2019) Charge-based self-equalization for imbalance battery pack in an energy storage management system: developing a time-based equalization algorithm. *IEEE Consum Electron Mag* 8(2):16–21
- Shuai M, Jiang M, Peng T et al (2018) Temperature effect and thermal impact in lithium-ion batteries: a review. *Prog Nat Sci* 28(006):653–666
- Smith DJ (2011) Chapter 22—integrity of safety-related systems. In: Smith DJ (ed) *Reliability, maintainability and risk*, 8th edn. Butterworth-Heinemann, Oxford, pp 331–342
- Smith J, Singh R, Hinterberger M et al (2018) Battery thermal management system for electric vehicle using heat pipes. *Int J Therm Sci* 134:517–529
- Torres-Echeverria AC, Martorell S, Thompson HA (2011) Modeling safety instrumented systems with MoonN voting architectures addressing system reconfiguration for testing. *Reliab Eng Syst Saf* 96(5):545–563
- Wan XF, Wu JP, Hu HL (2009) The smart battery management system. In: Proceedings of IEEE international test conference, pp 29–32
- Wei H, Ng KS, Hu JH et al (2010) Charge equalization of battery power modules in series. In: Proceedings of international power electronics conference, pp 1568–1572
- Wikner E, Thiringer T (2018) Extending battery lifetime by avoiding high SOC. *Appl Sci* 8(10):1825. <https://doi.org/10.3390/app8101825>
- Xiong R (2020) *Battery management algorithm for electric vehicles*. Springer, Singapore. <https://doi.org/10.1007/978-981-15-0248-4>
- Zhu F, Liu G, Tao C et al (2017) A battery management system for Li-ion battery. *J Eng* 13:1437–1440
- Zhu GL, Zhao CZ, Huang JQ et al (2019) Fast charging lithium batteries: recent progress and future prospects. *Small* 15:1805389
- Zhu W, Shi Y, Lei B (2020) Functional safety analysis and design of BMS for Lithium-Ion battery energy storage system. *Energy Storage Sci Technol* 9(1):271–278

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.