IEEE Open Journal of
Circuits and Systems

Received 2 February 2024; revised 15 March 2024 and 11 April 2024; accepted 17 April 2024. Date of publication 22 April 2024;
date of current version 8 May 2024.

Digital Object Identifier 10.1109/OJCAS.2024.3391829

A Design of Fault-Tolerant Battery Monitoring IC for Electric Vehicles Complying With ISO 26262

BYAMBAJAV RAGCHAA[1,2], LIJI WU[1,2] (MEMBER, IEEE), AND XIANGMIN ZHANG[1,2]

[1]School of Integrated Circuits, Tsinghua University, Beijing 100084, China

[2]Beijing National Research Center for Information Science and Technology, Beijing 100084, China

This article was recommended by Associate Editor S.-H. W. Chiang.

CORRESPONDING AUTHOR: L. WU (e-mail: lijiwu@tsinghua.edu.cn)

ABSTRACT Battery monitoring integrated circuits (BMIC) employed in the battery management system (BMS) for electric vehicle (EV) application are subjected to rigorous requirements for accuracy, reliability, and safety. This paper presents a design of an 8-cell battery pack monitoring and balancing IC, which can be stacked to monitor and balance a total of 128 cells. The design of battery cell voltage detection is realized by a second order, incremental $\Sigma\Delta$ADC with a high-voltage channel multiplexing scheme. The accuracy of cell voltage detection, achieved with a margin of ± 10 mV, is confirmed by the test results. In this paper, we aim to enhance the reliability and robustness of the BMIC by implementing fault detection mechanisms within its circuits and incorporating fault recovery functionalities through digital circuits. To meet safety requirements, this paper adheres to the functional safety standard ISO 26262 for road vehicles. The quantitative analysis of hardware architectural metrics for the proposed BMIC demonstrates compliance with ASIL-D requirements for functional safety.

INDEX TERMS Battery management system, battery monitoring integrated circuit, fault detection, ISO 26262.

I. INTRODUCTION

In MODERN electric vehicles, a large number of rechargeable lithium-based battery cells are used as the primary power source. Misuses such as overcharging or deep discharging could lead to irreversible damage to the cell, and even could lead to potential thermal runaway, causing a life-threatening hazard such as fire in the electric vehicles (EVs).

Thus, a battery management system that monitors each of battery cells' parameters, including voltage, current and temperature, while keeping cell voltages at the safe operating range through balancing, is one of the crucial key technologies of EVs [1]. For optimizing system cost, reliability, and precision in measuring battery cell parameters, battery monitoring integrated circuits are used widely in the battery management system (BMS).

The proposed architecture of a battery monitoring IC (BMIC) is shown in Fig. 1. It consists of high-voltage power management (HVPM), high-voltage multiplexer (HVMUX), an analog-to-digital converter (ADC), precision reference voltage generator (REF), clock generator (CLK Gen), digital control (DCU), memory (MEM), communication interface (COM), passive cell balancer (CB) and general-purpose input/output (I/O).

FIGURE 1. Block diagram of proposed BMIC.

© 2024 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

The circuits in the BMIC such as ADC, REF, DCU, MEM, COM, I/O and the biasing generations are all powered by HVPM. The HVPM is a linear voltage regulator that generates a 5 V supply voltage from the series of battery cells monitored by the BMIC. A modern distributed BMS topology is based on a master-slave architecture, where the BMS master aggregates battery pack information from the BMS slaves that employ BMICs. When the BMIC receives a command packet from the BMS master via its communication interface, the DCU decodes and executes commands such as starting cell voltage measurement, controlling cell balancing switches, or loading the measured cell voltage data into the transmission buffers. The HVMUX is employed to select the specific battery cell voltage from the battery pack, which composed of 8 cells. The output of the HVMUX is in the HV domain. To leverage benefits such as better device mismatch, smaller chip area, lower power consumption, and the ease of biasing and controlling circuits, the ADC is implemented using low-voltage (LV) devices. Consequently, a level shifter (LS) is utilized to translate the output of HVMUX to LV domain. Memory is necessary to store digitized cell voltage values and configuration parameters of the BMIC. The REF provides a 3 V precision reference voltage to the ADC and CLK Gen. CLK Gen provides clock to the rest of the circuit.

A. CONTRIBUTIONS

As one of the crucial building blocks of BMS in EVs, the battery monitoring IC faces technical challenges related to precision, integration, and reliability. Previous design works [2], [3], [4], [5], [6] aimed to resolve precision and integration issues. However, due to strict automotive safety requirements, simply addressing these aspects is not sufficient, and those designs still fall short of industry-level contributions.

The recent design introduced in [7] features a BMIC with high measurement accuracy and robust communication, meeting the safety requirements of ASIL-D as defined by the ISO 26262 standard.

In this paper, our aim is to enhance the reliability and robustness of the BMIC by implementing fault detection features within its building blocks as part of the safety mechanisms (SMs) against the detected faults.

Furthermore, our design features a fault tolerance, a capability not present in previous designs, and closely aligns with the requirements of the ISO 26262 standard while addressing precision and integration challenges.

To assess the effectiveness of our proposed design, we evaluate it according to Part 5.7, 5.8 and 5.9 of ISO 26262.

B. OUTLINE

The remainder of this paper is organized as follows. In Section II, a literature review related to the functional safety standard ISO 26262 and BMS is conducted to establish the safety requirements of BMIC. Section III explores the safety analysis of the BMIC, aiming to identify weakness in its architecture that could potentially lead to a violation of the safety goal of the BMS. In Section IV, the paper discusses the proposed circuit implementations and their fault detection features. Section V, based on the fault detection features of the circuits, determines safety mechanisms and introduces the proposed architecture of the fault-tolerant BMIC. Then evaluates the hardware architectural metrics of the BMIC. In Section VI, the paper presents verification methods of SMs implemented in the BMIC and measurement results of core circuits. Section VII is the conclusion.

II. DEVELOPMENT OF BMIC AS A SAFETY ELEMENT OUT OF CONTEXT (SEOOC)

The international standard ISO 26262 for functional safety of electrical and/or electronic (E/E) systems within road vehicles [8] addresses the possible hazards caused by the malfunctioning behavior of all electrical and electronic related systems in the vehicle, including their interaction.

ISO 26262-10:2018, Clause 9 introduces the concept of Safety Elements out of Context (SEooC). An SEooC is developed based on assumptions in accordance with the ISO 26262 series of standards. In the scope of SEooC hardware component development, Part 4, Clause 6 “Technical safety concept”, is considered (fully, partially, or not), depending on the exact nature of the SEooC. Based on the decisions of assumed technical safety requirements (TSRs), the SEooC is developed according to Part 5 of ISO 26262-5:2018, “Product development at the hardware level”.

References [1], [9], [10], [11], [12] discussed the BMS at the system level, as outlined in Part 3 “Concept phase” and Part 4 “Product development at the system level” of ISO 26262. The Part 3, Clause 5 (ISO 26262-3:2018, 5) of ISO 26262 defines the item with descriptions of key functionalities and possible malfunctions.

The BMIC is an element of the item BMS and is defined as a cell voltage sensor, sensor signal processor, or cell monitoring device in [9] and [11]. Following the item definition, the hazard analysis and risk assessment (HARA) process (ISO 26262-3:2018, 6) determine the automotive safety integrity level (ASIL) of the item based on potential hazards, severity, exposure, and controllability in the scenario of malfunctions. References [1], [9], [11], [12] determined ASIL-C level for the BMS, considering the hazard case “battery cell overcharging causes thermal event”.

For each ASIL-rated hazard, safety goals (SG) are applied. A common safety goal proposed in these references is “battery overcharging shall be prevented”. Based on the safety goals, the definition of functional safety concepts (FSC) (ISO 26262-3:2018, 7) and the derivation of functional safety requirements (FSR) are conducted.

The FSRs are allocated to the technical safety requirements, which are assigned to more specific elements in the system architecture according to ISO 26262-4:2018, 6. In [7], [8], [10], [11], TSRs are derived from the FSRs and assigned to the elements of the BMS. More specific TSRs to the BMIC are defined in [9] and [1].

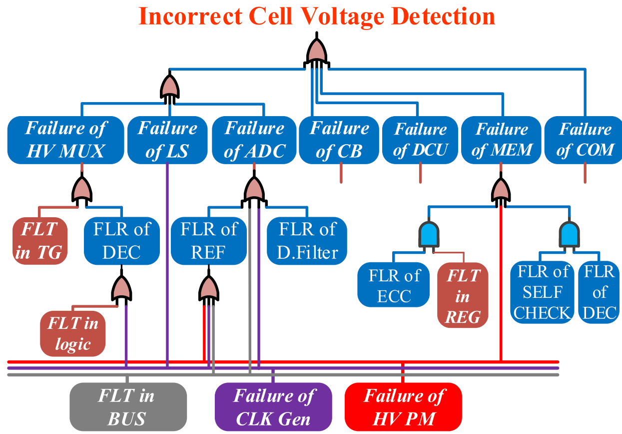


FIGURE 2. Fault Tree Analysis.

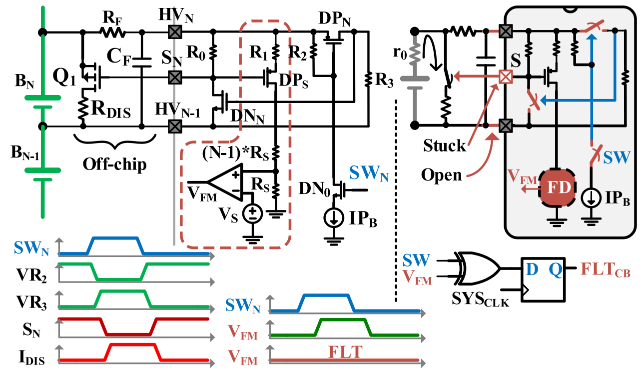


FIGURE 3. Passive cell balancing circuit.

III. SAFETY ANALYSIS

According to Part 5, Clause 7 of ISO 26262, "Hardware design" applies safety analyses as outlined in ISO 26262-9:2018, 8 to identify the causes of failures and the effects of faults that violate the safety goal. For this purpose, a fault tree analysis (FTA) is performed based on the block diagram of the proposed BMIC. The top-level event in the fault tree is the failure of the safety element BMIC in the item BMS, specifically the "incorrect cell voltage detection," which ultimately leads to a violation of the safety goal "battery cell overcharging shall be prevented." This SG contradicts the ASIL-C hazard "battery cell overcharging causes a thermal event," as mentioned previously.

In the FTA, as shown in Fig. 2, failures in HVPM, CLK Gen, and the BUS are considered common failures since they are shared with other circuits in the BMIC. Faults in HVPM manifests as its output voltage being under or over the expected voltage. When the supply voltage in a CMOS circuit falls below the expected nominal voltage, it can lead to various issues and potential failures, such as threshold voltage issues, reduced noise margins, signal integrity problems, increased sensitivity to process variations, slower switching speeds, memory cell instability, and insufficient output voltage swing. On the other hand, an overvoltage condition can lead to gate oxide breakdown, hot carrier injection, increased power dissipation, threshold voltage shift, and device degradation. Thus, these failures potentially lead to incorrect cell voltage detection of the BMIC. In ISO 26262-11:2018, Clause 5.2, Table 36 outlines failure modes of clock generators, which include output stuck, output floating, and incorrect output signals such as frequency and duty cycle of the clock signal. As the clock signal determines the timing and synchronization of the conversion process in ADC, failures in the clock can directly lead to the incorrect cell voltage detection. Faults in a bus line, such as stuck at a particular logic level due to a tri-state buffer fault, break in a bus line, temperature-induced impedance changes in the bus line that affects the signal characteristics, open connector due to electromigration, and EMI-induced disruptions, can lead to incorrect data transfer between circuits in the BMIC. The binary-form cell voltage data obtained by the ADC is transferred among the DCU, MEM, and COM. Thus, bus line faults can lead in incorrect cell voltage detection. Faults in HVMUX, such as address decoder stuck at, or LDMOS switch (TG) transistor stuck-open or stuck-on, faults in LS, faults in ADC, including incorrect REF voltage generation or decimation filter stuck-at, can lead to incorrect cell voltage detection. Since the cell voltage data is stored in the memory, faults in the memory circuit, such as bit flips, bit stuck, read and write disturb, or a stuck address decoder, can directly lead to incorrect cell voltage detection. Failures at the cell balancer port S_N, as shown in Fig. 1, stuck at high or low, could result in incorrect cell voltage detection. In the stuck at low fault, continuous uncontrolled cell discharging ultimately leads to a weak cell problem which increases internal resistance of the cell. In the stuck at high fault, the cells never reach a balanced state, and it may end up causing the charging process to finish before other cells nominally charged or the never-discharged cell is overcharged. Any stuck-at fault in the DCU can lead to the abnormal operation of the BMIC. Incorrect data transfer between the BMIC and the BMS master could result in incorrect cell voltage detection.

From this discussion, typical BMIC architecture is sensitive to the faults that could lead to the violation of SG. Thus, the circuit modules in the BMIC need to be modified with fault detection and safety mechanisms. The following section discusses the proposed circuit modules and their fault detection features.

IV. CIRCUIT DISCUSSION

A. PASSIVE CELL BALANCING CIRCUIT

In automotive applications, around 100 mA of discharging current is widely appreciated due to less stress on the battery cells and to avoid cell charge imbalance caused by increased cell temperature [4]. However, in some specific applications, smaller discharging currents are required.

The passive cell balancing circuit drives an external power MOSFET transistor, Q_1, which is used to discharge the battery cell via a low ohm resistor (R_{DIS}) when higher discharge current is required, as shown in Fig. 3.

The circuit is also able to sink discharging current via the LDNMOS transistor DN_N. The internal cell discharging switch DN_N, with the advantageous BCD process technology, ensures that the on-resistance of the internal LDNMOS for cell discharging is less than 10 Ω, preventing the IC from overheating during the discharge process. Here, up to 10 mA of sink current is chosen for safety considerations. The working principle of the cell balancing circuit is as follows: when the control signal SW_N sets high (5 V), the HV-NDMOS transistor DN_0 conducts the biasing current IP_B, which pulls down the gate potential of DP_N. Here, IP_B and R_2 are chosen as in (1), causing the LDPMOS transistor switch DP_N to close.

$$V_{GS,DPN} = IP_B \cdot R_2 \approx -4\ V \tag{1}$$

As a result, the gate-source voltage ($V_{GS,\,DNN}$) becomes approximately the cell voltage V_B, and the S_N port voltage drops to $V_{DS,\,DNN}$, which is nearly 100 mV. This turns on the off-chip power MOSFET transistor, initiating the cell discharging process.

In this circuit, any faults, including the sticking state of HV transistors used as switches and an open wire between the battery cell and the HV_N and HV_{N-1} pads, can be detected by the current detection circuit shown in the dashed brown line box. In the current detection circuit, the gate-source voltage of the HV-LDPMOS transistor DP_S is expressed as (2):

$$V_{GS,DPS} = V_{DS,DNN} - (V_{BAT} - I_S \cdot R_1) \tag{2}$$

Here, the turn-on condition of the DP_S is the drop of drain-source voltage $V_{DS,DNN}$ or the on state of the switch transistor DN_N triggered by the control signal SW_N. Since the gate-source voltage of DP_S is limited by the ($I_S \cdot R_1$) factor, the sensing current is restricted and predictable in the wide range of battery cell voltages. The comparator of the fault detection circuit is implemented in the low-voltage domain. The I_S sensing current is converted to voltage by a resistor divider. The ratio of the resistors is defined as 1/(N-1) to ensure that the input voltage of the comparator is always less than 5 V, where N is the stack number of the battery cells, ranging from 1 to 8. The output of the comparator V_{FM} is XORed with the control signal SW_N, and the output state of the XOR logic is captured on the rising edge of the system clock. In the faulty situation, the FLT_{CB} signal triggers the fault handler trap.

B. CLOCK GENERATION CIRCUIT

To provide a stable clock reference to the circuit modules in the IC, an on-chip clock generation circuit based on a three-stage differential ring oscillator is implemented in this paper, as shown in Fig. 4. The center frequency of the clock signal is chosen at 10 MHz, considering the highest speed requirement of the communication module where the width of the minimum pulse transition should be less than 100 ns in transformer isolated SPI interface for achieving a 1 Mbps data rate [6]. Duty cycle of the clock signal is 50%, and the frequency fluctuates less than 20% above and below the center value, accommodating changes in different process angles and temperature across a wide range of −45°C to +125°C.

FIGURE 4. Clock generation circuit.

FIGURE 5. Timing diagram of clock monitoring.

Our design incorporates a clock generation circuit with process and temperature compensation, as detailed in [13].

To detect output stuck and floating out failures, a pulse monitor is employed, while frequency and duty cycle failures are detected by frequency monitor circuits, as shown in Fig. 4.

When the charging current is constant, the voltage of the capacitor is expressed as (3), where 't' is the charging time, and 'C' is the capacitance:

$$V_C = \frac{I \cdot t}{C} \tag{3}$$

The pulse monitoring circuit continuously charges the capacitor with a constant current if $V_{CP} < V_{RP}$, and discharges when $V_{CP} > V_{RP}$, as illustrated in the timing diagram shown in Fig. 5. The decision to charge is made at the rising edge of the clock signal, while discharging occurs whenever V_{CP} exceeds the V_{RP} threshold. For this purpose, a D Flip-Flop (DFF) with asynchronous reset is utilized. In the scenario of a stuck-at or floating out fault in the clock generator, the capacitor discharges continuously and reaches the lower threshold V_{RN}, causing the assertion of the FLT_P signal.

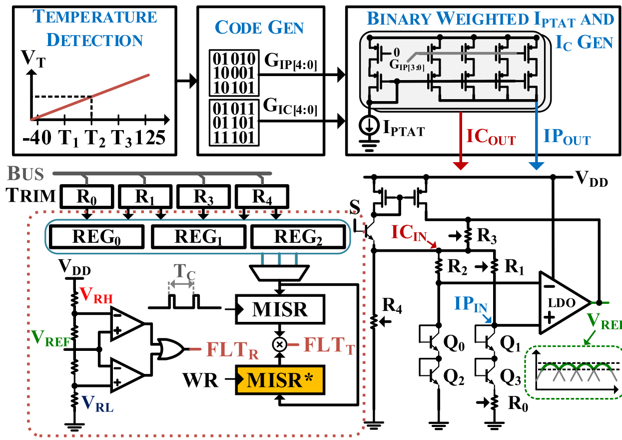


FIGURE 6. High precision voltage reference circuit.

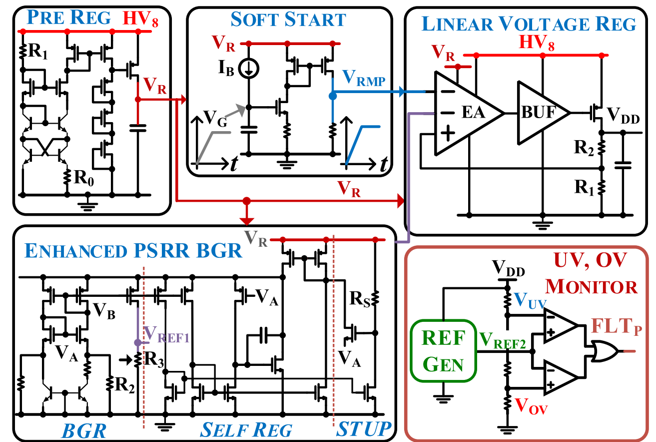


FIGURE 7. High voltage high-PSRR power management circuit.

The frequency monitoring circuit adopts the design of a low-power frequency monitoring circuit, as discussed in [14]. However, in this design, the main clock generator output F_1 (10 MHz) is used to generate control signals integrating Q_I, discharging Q_D, and holding and latching Q_L for measuring the clock divider's output 1 MHz frequency F_2. In a fault-free frequency range, V_{CF} is charged during Q_I, which is equal to the duty cycle of F_2, and discharging during the Q_D phase. The V_{CF} is compared with the upper threshold of V_R in the Q_L phase. If the duty cycle of F_2 is larger than the expected value or the frequency is beyond the expected range, V_{CF} is excessively charged or exceeds the V_R threshold, triggering the FLT_F signal. Since the clock divider is used to generate F_2 from F_1, a counter-based clock ratio monitoring is required.

C. VOLTAGE REFERENCE CIRCUIT

For achieving higher cell voltage measurement accuracy (less than 1 mV) in battery cell voltage detection circuit, voltage reference with lower temperature coefficient (less than 10 ppm/°C) is required. This design adopted our previous work of temperature curvature compensated high precision voltage reference. More detailed discussion on the design of the reference generator core circuit can be found in [15].

Output voltage is monitored by voltage range detection circuit as shown in Fig. 6. Here the V_{REF} is compared with upper threshold V_{RH} and lower threshold V_{RL}. In cases, where the output voltage is greater than upper threshold or less than lower threshold, FLT_R is set.

Due to the expected variation in the absolute values of resistors during the semiconductor manufacturing process, a trimming scheme is widely employed in the high-precision analog circuits of the BMIC [16], [17]. In this design, a 20-bit trim register is used for this purpose. Random hardware failures in the trim registers, such as single or multiple bits flips as transient faults or bit(s) stuck at 0/1 as permanent faults, could result in a change to the expected output voltage of the reference circuit. Thus, the corruption of trim register content is monitored by the Multiple Input Signature Register (MISR). When the trim values are written to Reg_0, Reg_1, Reg_3, and Reg_4 from the bus, the golden signature is generated by the MISR* from these originally written trim values. The start condition of the MISR* is triggered with the falling edge of the bus write (WR_4) signal of the last trim register, Reg_4. After that, the upper MISR, shown in Fig. 6, periodically generates a signature from the trim register values and compares the result with the golden signature. If these two signatures mismatch, it is considered that the trim values are corrupted, and the FLT_T is asserted. Here, the same primitive polynomial (4) is chosen for both MISR* and MISR.

$$G(x) = x^8 + x^2 + x^1 + 1 \quad (4)$$

When a fault is detected in this module, a fault recovery function is initiated by sending a fault trap to the digital control unit, which includes fault handler functionalities.

D. POWER MANAGEMENT CIRCUIT

The power management circuit provides a 5 V/20 mA power source to the circuits in the BMIC. The input voltage of the power management is 6 V to 40 V, which can meet the series requirements of 2 to 8 battery cells. During large dynamic charging and discharging processes of battery cells, the power management circuit must maintain a stable supply voltage for the precision voltage reference and analog-to-digital converter, to ensure accurate cell voltage detection. The safety design of the device under high voltage is a primary consideration, with a particular focus on protection during special conditions such as the power-up process.

Therefore, this circuit comprises an HV pre-regulator, an enhanced power supply rejection ratio (PSRR) self-regulated bandgap reference, and an HV linear regulator with the soft start, as shown in Fig. 7. In this design, we modified our previous high-voltage, high-PSRR power management circuit for BMIC. Thus, a more detailed discussion of this design can be found in our previous work [18].

The failure modes of under and over voltage in power management are monitored by a voltage window monitor,

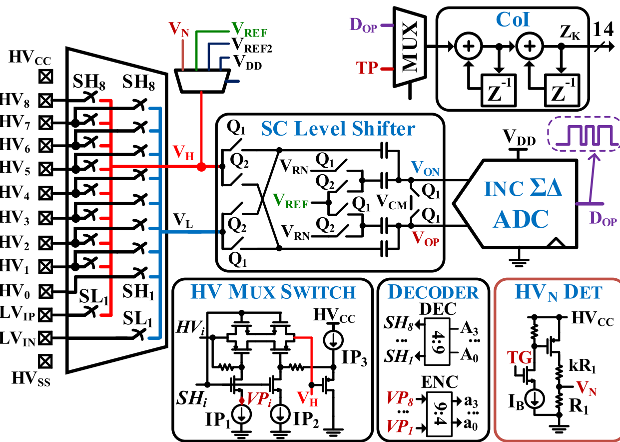


FIGURE 8. Battery cell voltage detection circuit.

as shown in Fig. 7. The reference generator provides an accurate and stable 3 V reference voltage, and a voltage divider generates ratioed under and over voltages from the output of the linear voltage regulator. When this fault condition is detected, FLT_P signal requests fault-handling from the digital control unit. The linear regulator's output voltage can be configured by changing trimmable R_3 resistor of the BGR core.

E. CELL VOLTAGE DETECTION CIRCUIT

In this design, we adopt our previous design of high-precision multi-cell battery cell voltage detection (BCVD) circuit, where a battery pack with 8 cells is monitored [19]. The BCVD circuit consists of an HV multiplexer, switched capacitor (SC)-based voltage level shifter, and a second order, incremental ΣΔADC with a two-level cascade of integrators (CoI) digital filter, as shown in Fig. 8. The LDMOS-based HV multiplexer selects a specific HV battery cell voltage signal from the battery pack. Since there is no resistive load between the HV multiplexer and the switched-capacitor ADC, no static load current introduced, helping to avoid non-ideal conduction problems with the MOS switch. This greatly improves voltage detection accuracy. The more detailed circuit design of an efficient SC level shifter, which converts the HV multiplexer output into the low-voltage domain, is presented in [2].

Faults in transmission gates (LDMOS) and the address decoder are detected through direct and indirect methods. The address decoder is a 4-to-9 one-hot digital decoder, where only one of the signals SH_i is set high to enable the current bias of LDPMOS in the HV multiplexer, depending on the four-bit address input A [3:0] signal. Faults in the address decoder and biasing circuits, such as constant current sources IP_1, IP_2 and IP_3, or open wires in the LDMOS control circuit, can be detected by sensing the VP_i potential, as shown in Fig. 8. Thus, a feedback encoder is added for this purpose. If the address A [3:0] doesn't match with the encoder output a [3:0], the fault signal FLT_{DEC} is asserted. However, this method alone cannot detect faults of LDMOSs in HV multiplexer, such as stuck-at-on or stuck-at-off states.

The sum of the voltages across all individual cells in the pack is equal to the voltage of the highest cell relative to the ground potential, as expressed in (5)

$$\sum_{i=1}^{n} CV_i = \ HV_n - HV_{SS} \tag{5}$$

On the other hand, the voltage of the top cell HV_n can be directly measured by the ADC with an attenuation factor 1/n, where n is the number of cells in the pack. Since HV_n is a high-voltage signal and the ADC input is in a low-voltage domain (0 ∼ 5 V), a resistor-based voltage divider is employed as an attenuator, as shown in Fig. 8. If the condition (6) is not met, it is considered that there is a fault in the transmission gates.

$$\sum_{i=1}^{n} CV_i = \left[(k+1) \cdot V_N \pm V_{ERR.MEAS}\right] \tag{6}$$

Here, V_N represents the 1/(k+1) voltage divider output, as shown in the box titled "HV_N detection" in Fig. 8, and $V_{ERR.MEAS}$ represents the absolute measurement error of the ADC. In this design, k is chosen as 7 to ensure that the 1/8 division of the maximum pack voltage (40 V) is always less than 5 V. Faults of the level shifter and ADC are manifested through accuracy error. Thus, judging the accuracy of the ADC with different reference voltage inputs is used for detecting faults in the level shifter and ADC. The low-voltage analog multiplexer is used for selecting different reference voltages to the ADC input, as shown in Fig. 8. After trimming the high-precision voltage references, if the accuracy is outside the expected range, the fault flag is set, indicating the detection of a fault in the level shifter or ADC. The fault in the digital filter can be easily detected using pre-defined test pattern inputs and observing its responses.

F. MEMORY CIRCUIT

To store 8 digitized battery cell voltage measurement values, 1 digitized low-voltage input sensor voltage value, battery cell voltage under/over threshold flags, a summary of all cell value, along with the configuration and calibration parameters of analog modules and intermediate processing variables, a total of 64 bytes of volatile memory is required in this BMIC. The memory circuit mostly consists of an address decoder and a register array as shown in Fig. 9.

To detect bit flips and bit stuck faults, single-bit error correction and double-bit error detection (SECDED) are implemented by employing the extended Hamming (13,8) code where the integrity of the 8 data bits is checked with 5 parity bits.

The data to be stored at memory is transferred through a shared bus that has 8 data lines and 5 parity lines as shown in Fig. 9. Thus, first the integrity of the received data needs to be checked. When data is written to the memory, the active high write (WR) signal is set. The parity bits generated on

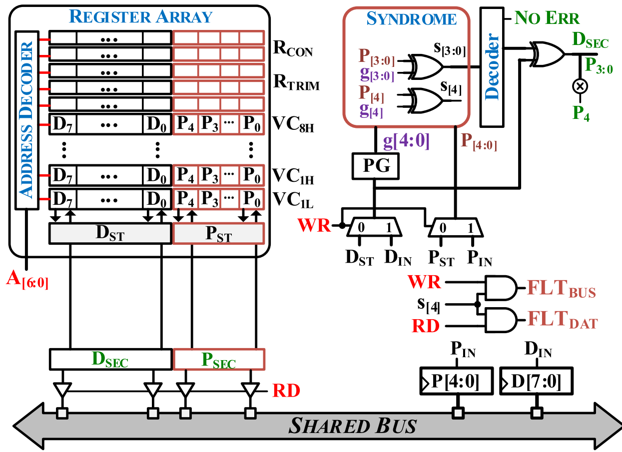


FIGURE 9. Memory circuit.

the D_{IN} buffer are XORed with the received parity bits P_{IN} to obtain the syndrome $s = [s_0, s_1, s_2, s_3]$. Depending on the syndrome, the corresponding output of one-hot decoder is set and XORed with the D_{IN} to complement the corresponding corrupted bit, correcting the error. If no error occurred, the no-error line sets, and no bit is complemented in the received data. If the global parity (g_4), generated from the received data, doesn't match the received global parity P_4, it indicates that a double error occurred due to shared bus fault, and the FLT_{BUS} line is activated. When there is no-error or a single-bit error is corrected, the data is stored in the memory.

When the stored data is requested, integrity of stored data D_{ST} is checked with its stored parity bits P_{ST} in a similar way. Data is placed on the shared bus if there is no-error or after a single-bit error is corrected. Otherwise, it is considered that the stored data is corrupted and FLT_{DATA} line sets for informing the status of the corrupted data. Because the discussed scheme cannot detect faults in the address decoder, the March C- memory test (ISO 26262-11:2018, 5.1.13) is employed to address this specific fault.

G. COMMUNICATION CIRCUIT

Due to the large number of battery cells in an electric vehicle, communication lines between adjacent BMICs and the master controller of the BMS may span several meters or even tens of meters. Thus, considering lower energy consumption in longer distance transmission and better noise immunity in the harsh electromagnetic environments of electric vehicles, transformer isolated differential signal interfacing is chosen in this design.

The data communication between a specific BMIC and the BMS master is achieved through a multi-drop configuration in the distributed BMS topology, as shown in Fig. 10. In this setup, each BMIC has its own unique 4-bit physical address, facilitating peer-to-peer communication between the BMIC and the BMS master. The choice of a 4-bit physical address takes into account the number of addressable BMICs needed to monitor a battery pack voltage of 400 V, which

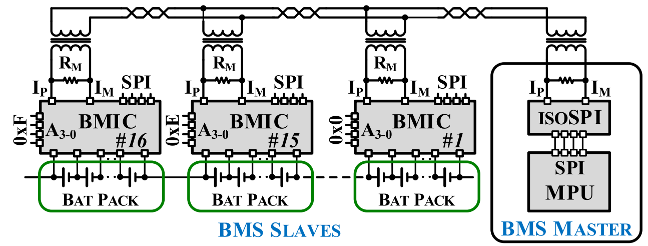


FIGURE 10. Transformer isolated multi-drop communication architecture.

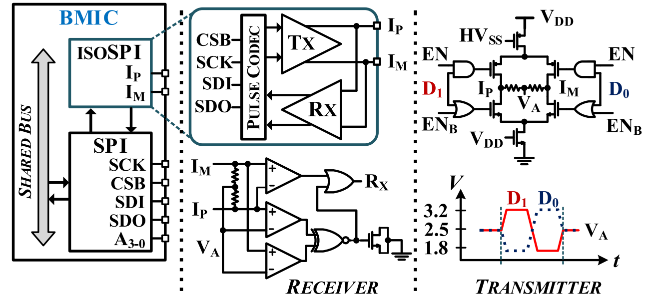


FIGURE 11. Communication module with addressable SPI circuits.

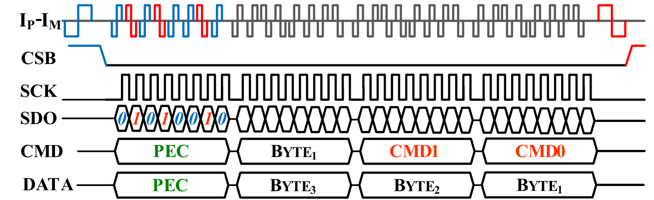


FIGURE 12. Timing diagram of physical layer data transfer.

is prevalent in modern electric vehicles. The advantages of multi-drop communication over chip-to-chip daisy chained communication in this application are fault isolation, easier troubleshooting, parallelism in communication, and reduced susceptible to single points of failure.

The communication module of our proposed BMIC supports TTL-level Serial Peripheral Interface (SPI) and Isolated SPI (isoSPI), as shown in Fig. 11. In isolated SPI, the data transmission signal is in the form of a differential pulse [6], [20]. Thus, the transmitter structure uses low-voltage differential signaling (LVDS) with common-mode DC biasing. Data being transmitted is distinguished by pulse pole, as shown in Fig. 11. Conversely, the receiver side is composed of three comparators that identify the data signals and bus status of idle or active. The pulse codec encodes and decodes pulses, where a long (300 ns) +1, long −1 represent for CSB rise and fall signals, and a short (100 ns) +1, short −1 pulses represent for SCK rising edge while SDI is 1 and SCK rising edge while SDI is 0, as which is shown in Fig. 12.

The BMS master to BMIC data transfer consists of command bytes (CMD_0, CMD_1), data bytes, and packet error code (PEC), as shown in Fig. 12. When the BMS master initiates the command packet transmission, all BMICs on

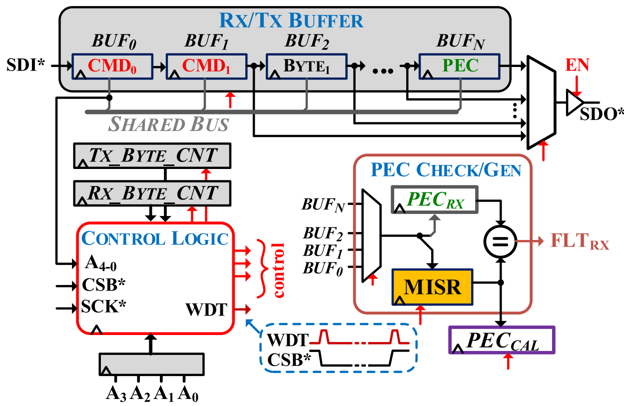


FIGURE 13. Data packet error check.

the bus receive the packet. If the address bit A_4 encoded in CMD_0 byte is set, all the BMICs accept the command and data bytes as the bus master is broadcasting. Otherwise, only the BMIC with its physical address matching A_{3-0} in CMD_0 byte receives the command packet. After the command packet transmission, the master provides the serial clock (SCK) for reading data and calculated PEC in the BMIC's serial transmission buffer. In both direction of data transfer, the integrity of the transmitted data is checked with the 8 bits of PEC.

Both in isolated and TTL-level data signal transmission, the transferred packet is captured in a 16-byte Rx/Tx buffer with the rising edge of the CSB signal. After that, the SPI control logic checks the transferred address bits in BUF_0 with the physical address latch data. If the address matches, further validation processes are performed, such as the calculation of the packet error check (PEC) based on received data bytes by the MISR, as shown in Fig. 13. Here, the same primitive polynomial given in (4) is used. Since the size of the data packet ranges from 3 to 16 bytes depending on the command, the transferred byte is counted based on the SCK* signal transition. Based on the received byte count, the location of the received PEC byte is determined. If the received PEC_{RX} and the calculated PEC_{CAL} match, transferred data packet is accepted. Otherwise, FLT_{RX} is set to inform data transfer corruption. When the BMS master requested data from the BMIC, the data and its calculated PEC_{CAL} are located on the buffers. In the scenario of failures such as a communication line break or BMS master MCU failure, the BMIC needs to immediately stop safety-related processes, such as cell discharging, in order to prevent further violation of safety goals. Thus, the status of normal communication needs to be monitored. For this purpose, a programmable watchdog timer (WDT) is employed. The WDT is reset after successful packet transfer, and its period ranges from 500 ms to 2000 ms depending on configuration parameters.

V. FAULT-TOLERANT BMIC ARCHITECTURE

When the BMIC powers up, the digital control logic (DCU) does start-up tasks. These tasks include calibration-related

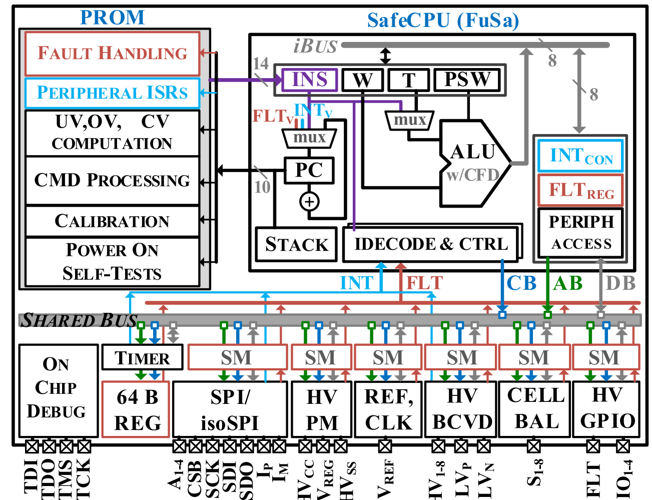


FIGURE 14. Proposed fault-tolerant BMIC architecture.

activities, such as trimming precision analog circuits, set cell balancer switch to off state and configure specific operation control registers in the circuit modules. Additionally, self-test procedures are executed, involving repetitive read/write test patterns in different memory locations. The DCU also compares the sum of all cell voltages with the directly measured pack voltage to diagnose the status of BCVD. Moreover, open wire detection is carried out in conjunction with the cell balancing circuit. The result flags are written to memory as status flags. After that, depending on the logic level at the input pin, the BMIC shifts to one of its operating modes.

In this design, there are two operating modes: stand-alone monitoring mode and communication mode. In communication mode, the BMIC receives a command data packet from the BMS master. Thus, the DCU in the BMIC needs to decode and execute the command, involving arithmetic and logical operations. As discussed in Section IV, the circuit modules are equipped with fault-detection mechanisms. Now, the detected faults need to be handled by the DCU as a safety mechanism. Therefore, the DCU needs to perform specific tasks depending on the activated fault line. To satisfy these functional requirements, the proposed fault-tolerant BMIC architecture is shown in Fig. 14. In this design, the digital control and fault handler are implemented using a tiny microprocessor dedicated to functional safety (SafeCPU), with its program stored in the code memory. The code vector is allocated for various tasks, including power on self-tests, calibration, command processing, setting under/over threshold voltage flags, computing total cell voltages, handling peripheral interrupts, and managing fault handling trap vectors.

It should be noted here that the architecture gains an advantage from the small-scale memory test and the repetitive nature of the testing algorithm, allowing for the omission of MBIST hardware in the memory circuit. The tasks, as

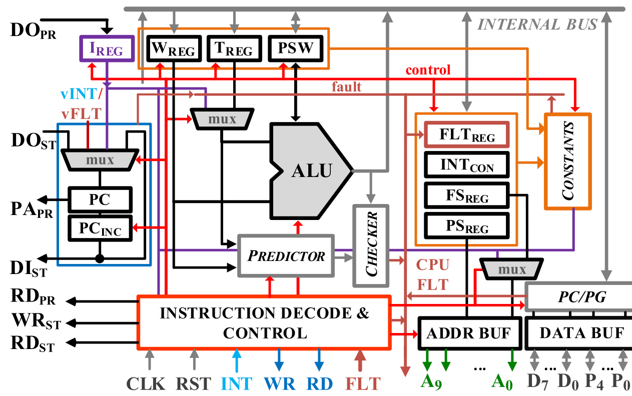


FIGURE 15. Proposed architecture of dedicated FuSa microprocessor.

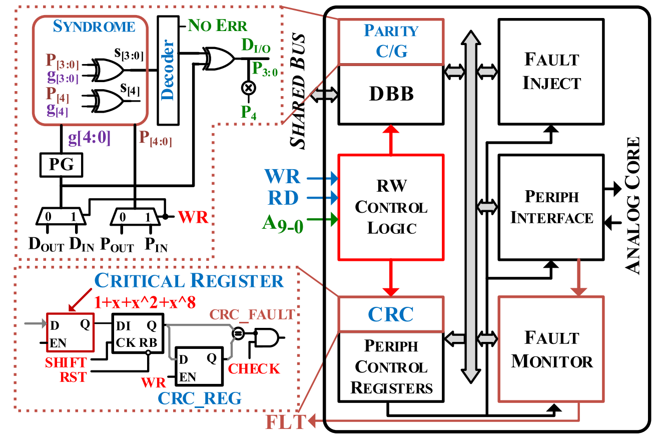


FIGURE 16. Integrating circuit modules with the system.

mentioned, are implemented via SafeCPU with concurrent fault detection. In this architecture, if a fault is detected within any of the BMIC circuits or the SafeCPU components, the fault handling functions are triggered. As illustrated in Fig. 14, the architecture features circuit modules as bus system peripherals. In the event of a detected fault, the FLT line is activated to notify the SafeCPU as a fault trap. Subsequently, the program counter (PC) of the SafeCPU loads the fault handler vector address and performs the necessary fault handling tasks.

Configuration parameters for operation modes, transferred from the BMS master, are stored in both peripheral configuration registers and the SECDED-protected 64B register array. In the presence of a fault, the fault handler identifies the fault and reconfigures the peripheral based on the operation mode parameters stored in the register array to restore the BMIC to a safe state.

A. FUNCTIONAL SAFETY TINY MICROPROCESSOR (SAFECPU) FOR FAULT-TOLERANT BMIC

The SafeCPU is an 8-bit RISC machine that supports a 14-bit instruction opcode. Each functional block within the machine is monitored with concurrent fault detection mechanisms [21]. The ALU operations are monitored by Berger code, and the instruction decode and control logic use complete redundancy. The shared bus used for data transfer between the microprocessor and BMIC system peripherals is checked with extended Hamming (13,8) code, as discussed in Section IV-F. Specific test instructions are implemented to check for stuck faults in registers by writing test patterns to the register and comparing them with hardwired constants (0x00, 0x55, 0xaa, 0xff), as shown in Fig. 15. These instructions, in combination with stack access, can be used for fault-detection purposes when the SafeCPU is free to execute the BMS master's request. Each instruction is executed in 16 clock cycles (T_C), and the fault status flag is checked during the 12th to 16th clock cycles after the PC is incremented. If the fault flag is set, the PC, which points to the next instruction's address, is stored into the stack memory and loaded with the fault trap program vector address. Embedding the fault status check in the instruction execution process contributes to the BMIC achieving the shortest fault-tolerant time interval (FTTI).

B. CIRCUIT MODULES AS SYSTEM PERIPHERALS

Based on the IC process technology (1-poly, 3-metal, 60 V BCD) and our previous test tape-out experiences, we have chosen a modular design to avoid routing congestions in the physical design integration of BMIC. In the proposed bus peripheral architecture, each circuit module of the BMIC is accessed as a memory with a unique address. The peripherals include a data bus buffer (DBB), read-write (RW) control logic, peripheral control registers, fault monitor, fault injector, and the analog core as shown in Fig. 16.

In this design, the application profile of the BMIC is considered as an automotive chip. Therefore, wear-out faults related to the aging (electromigration) and thermal cycling are taken into account. The integrity of the shared bus is checked using multiple parity codes (Hamming) of the transferred data via the bus. To address transient faults induced by radiations and the EMI environments of the BMIC's working conditions, the critical peripheral control registers are monitored with CRC to prevent unexpected operations of circuit modules due to corrupted control words. The fault monitor is implemented to detect abnormalities in the operations of analog circuits based on statuses and test points, which are circuit nodes with diagnostic properties. It incorporates analog fault-detection mechanisms such as voltage level monitors and pulse monitors, as discussed in Section IV. Additionally, it includes a fault counter (flt_cntr) to determine whether the faults are transient or permanent. In the event of a detected abnormality, this module asserts the fault trap via FLT line. The peripheral interface mostly consists of small state-machines that provide control signals to the analog circuits and generate interrupt (INT) signals indicating the readiness of data. The fault injector is used during the validation process of safety mechanisms, as outlined in ISO 26262-11:2018, 4.7 and [10], [22].

TABLE 1. Safety mechanisms.

Part	Fault	Safe State
Cell Bal (CB)	S_N port stuck at high or low	Rewrite the switch control word, and check flt_cntr. If flt_cntr incremented, alert by FLT pin.
	Control word corrupted	Rewrite the control word. If flt_cntr incremented, alert by FLT pin.
GLK Gen	Clock out stuck	FLT pin sets high to alert.
	Incorrect clock frequency	Reset the CB control register. Alert by FLT pin.
REF	Output voltage is out of expected range	Try to clear FLT_R by inc/dec trim value. Give up after N try and alert by FLT pin.
	Trim value corrupted	Rewrite the Trim register. If flt_cntr incremented, alert by FLT pin
HVPM	Output voltage OoER	Try to clear FLT_P by inc/dec trim value. Give up after N try and alert by FLT pin.
BCVD	Decoder fault	Re-set channel address. If the FLT is still, alert by FLT pin
	HVMUX, LS, ADC fault	Alert by FLT pin.
	Control word corrupted	Rewrite the control word. If flt_cntr incremented, alert by FLT pin.
MEM	Corrupted data	Perform memory self-test. If the test fails, alert by FLT pin. If test passes, require BMS master to rewrite config by setting flag.
	Data bus fault	Alert by FLT pin.
COM	RX data incorrect	Alert by FLT pin.
	Communication stuck	Alert by FLT pin.
BUS	Wear-out	Alert by FLT pin
MPU	ALU,	Redo the ALU operation, if still the FLT is, alert by FLT pin.
	Registers,	Alert by FLT pin
	IDC	Reset MPU, re-execute the master's request. If still the FLT is, alert by FLT pin.
PROM	Corrupted CMD code,	Alert by FLT pin.
	Address fault	Alert by FLT pin.

C. SAFETY MECHANISMS

Table 1 lists the implemented safety mechanisms that prevent further violation of the SG of the BMS. The detected faults are classified as transient or permanent based on their persistence after correction using the fault counter. Transient faults are corrected without disturbing the BMS master. Thus, the BMIC can be considered fault-tolerant, as it can detect and correct transient faults without disturbing the BMS master. Transient fault is detected, and the implemented SMs bring the BMIC to a safe state. Detected permanent faults are alerted by the FLT pin of the BMIC to the BMS master. This greatly helps to reduce BMS master overhead since the BMS master doesn't have to check the normal operation of the BMICs periodically.

D. EVALUATION OF THE HARDWARE ARCHITECTURAL METRICS

As introduced in Section II, required safety integrity level of the item BMS is ASIL-C, D. Thus, the elements used in the BMS needs to satisfy same level of safety level as well. Quantitative evaluation metric is used as proof of the achieved safety integrity level in the design. This metric implies the implemented SMs are good enough to prevent violation of the SGs. The estimation of quantitative metrics is based on failure rates of system components and the efficiency of SMs represented by diagnostic coverage (DC). ISO 26262-11:2018, 4.6 describes several methods for the hardware failure rate estimation. One of used approaches is to use the failure rate data from a recognized industry source. In this paper, the calculation of the hardware failure rate is based on SN 29500-2[23], where complexity, represented by transistor/gate/bit count, and structure of the circuit (regulator, reference, VCO, ADC, etc.) are used as input.

TABLE 2. Quantitative evaluation metrics.

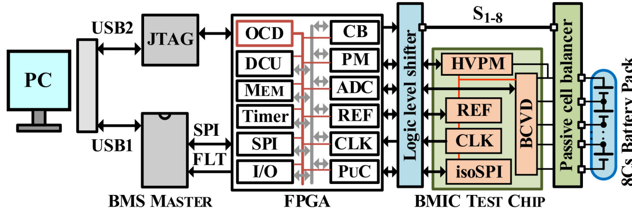
Parts/ subparts	**MOS/** *Gate* count	FLR rate **(FIT)**	FLR mode	DC **(%)** of SMs	Est latent failure rate
Cell Bal[3]	**47**	**5**	**MPF**	**99**	**0.05**
GLK Gen[4]	**90**	**15**	**MPF**	**99**	**0.15**
REF[4]	**251**	**6**	**MPF**	**99**	**0.06**
HVPM[4]	**121**	**20**	**MPF**	**99**	**0.2**
BCVD[5]	**628**	**20**	**MPF**	**99**	**0.2**
MEM[1]	**104B**	**15**	**MPF**	**100**	**0**
COM[5]	**83**	**20**	**MPF**	**99**	**0.2**
BUS[3]	**13**	**8**	**MPF**	**100**	**0**
CPU[2]	**1588**		**MPF**		
ALU	*112*	**25**	**MPF**	**96**	**1**
IDEC&CL	*143*	**25**	**MPF**	**99**	**0.25**
Registers	*88*	**25**	**MPF**	**99**	**0.25**
Interconnect	*28*	**25**	**MPF**	**100**	**0**
I/O BUF	*26*	**25**	**MPF**	**100**	**0**
PROM[1]	**1KB**	**50**		**100**	
Σ Failure rate		**264**			**2.36**
SPFM		**100%**			
LFM		**99.1%**			
PMHF		**2.36**			

SN 29500-2: 2010-09, *Table*-**1,2,3,4,5**

Table 2 lists the failure rates of the circuits in the BMIC measured in units of FIT (1 FIT $= 1 \times 10^{-9}$ h^{-1}), and the DCs of the implemented SMs. DC is the proportion of the hardware element failure rate that is detected or controlled by the implemented SMs. DCs of various SMs are discussed in ISO 26262-5: 2018, Annex D and ISO 26262-11:2018, 5.1.12. However, in our paper, we confirmed the DC in analog SMs by formal fault case simulations. First, the possible faults such as open wire, bridging of circuit nodes, transistor stack-open and stuck-on are extracted from the layout of the analog circuits. Then, transient simulation is carried on the faulty circuit in different conditions (TT, SS, FF, temperature) and observing fault detector's responses. In digital circuits, since the information redundancy-based fault detection (Berger, CRC, etc.) are able to detect any faults, DC can be claimed 100%. But, the test coverage of automatic test pattern generation (ATPG) needs to be considered. DCs of memory, shared bus, CPU interconnects, registers and I/O buffers are claimed to be 100%, since the March C- test and

TABLE 3. ISO 26262 target values for ASIL determination.

Metrics	ASIL B	ASIL C	ASIL D
SPFM	> 90%	>97%	**>99%**
LFM	>60%	>80%	**>90%**
PMHF	<100 FITs	< 100 FITs	**< 10 FITs**



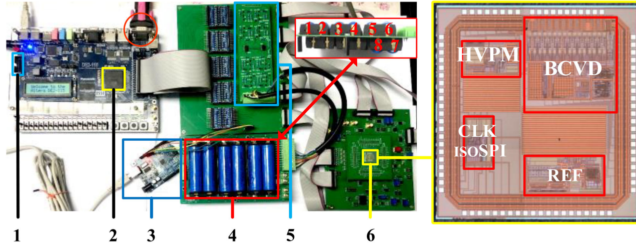


FIGURE 17. Experimental BMS setup. 1) JTAG port, 2) BMIC digital core, 3) BMS master MCU, 4) Battery pack, 5) Passive cell balancer, 6) BMIC test chip.

TABLE 4. Key parameters of the BMIC subcircuits.

Subcircuit	Design specs	Simulate	Measure
HVPM	Input voltage range [V]	5.5 ~ 40	6 ~ 40
	Output voltage [V]	5	5
	Max load [mA]	20mA	20mA
	LiR [mV/V], LoR [mV/mA]	0.03, 0.4	0.2, 1.5
BCVD	Cell Voltage [V]	1~5	1~5
	8 CV Conv.Time [µS]	340*8	340*8
	Conv.Error [mV]	< 0.3 mV	< 10mV
REF	Supply voltage [V]	3.6 ~ 5.5	3.6 ~ 5.5
Gen	Output voltage [V]	3	3
	Temp.Coef [ppm/C]	<3	<15

TABLE 5. Comparison of BMIC specifications.

Properties	IEICE' 2015 [2]	TII' 2020 [4]	ISSCC 2023 [7]	This work
Technology [nm]	350	350	180	**350**
Process	BCD	HV-CMOS	BCD	**BCD**
Number of cells	12	7	14	**8**
Min Pack Volt [V]	n/a	14	12	**6**
Max Pack Volt[V]	60	24	70	**40**
Meas. Error [mV]	<3	<7	<2	**<10**
Cell Balancer	No	Act/Pas	Passive	**Passive**
Stackable	Yes	Yes	Yes	**Yes**
ISO 26262	No	No	Yes	**Yes**
Open path detects	No	No	Yes	**Yes**
Fault Tolerance	No	No	No	**Yes**

self-check process detects any multiple faults and any single stuck at faults are detected concurrently. In our BMIC, since every circuit module is protected with SM, the failure mode is categorized as multiple point failure (MPF). Estimated fault metrics according to ISO 26262-5:2018, Annex C, such as single point (SPFM), latent (LFM) and probabilistic metric of hardware failure (PMHF) are listed in the bottom of Table 2.

According to Table 3, the quantitative metrics of the discussed BMIC satisfies ASIL-D functional safety metrics.

VI. TEST AND VERIFICATION

The experimental BMS, which monitors and balances 8 rechargeable battery cells, is shown in Fig. 17. In this prototype of the proposed BMIC, all the modules to be tested and verified, such as HVPM, BCVD, REF, CLK Gen, and the TX/RX modules of the isolated SPI interface, are fabricated using automotive process of ASMC's 0.35 μm, HV60, BCD technology in a single chip die. The passive cell balancer is implemented using discrete MOSFETs based on the principal structure of the proposed circuit, as shown in Fig. 3, for testing purpose. To optimize the size of the program code implementing DCU and fault-handler, and to verify the integration of digital peripherals with the analog circuits, an FPGA-based (Altera Cyclone IV, DE2-115 board) verification method is employed. Most importantly, this approach helps us to test the SMs with the fault injection as according to ISO 26262-11:2018, 4.8. For this purpose, on-chip debugger (OCD) and fault injector module are added, as shown in Fig. 14 and Fig. 16. The OCD is a JTAG TAP controller, and the fault injector mostly consists of boundary scan cells (BSCs). When a fault is injected, BSCs alter the normal circuit operation or cause an error to trigger the SMs. Table 4 lists the simulation and measurement results of the BMIC circuits. Table 5 summarizes the key specifications of the BMIC and provides a comparison with previously published designs.

VII. CONCLUSION

This paper addresses the challenges related to the accuracy, reliability, and safety of battery monitoring ICs within Electric Vehicle Battery Management Systems. The presented BMIC design mitigates transient faults and detects permanent faults, preventing the violation of ASIL-C and D level safety goal of BMS in EVs. Fault detection mechanisms are validated through transistor-level simulations, and the dedicated BMIC architecture, supporting the implementation of safety mechanisms, is verified using fault injection methods. In the context of automotive electrification, the methodology used in this paper contributes to the development of integrated circuits for automotive semiconductors.

REFERENCES

[1] D. Marcos et al., "A safety concept for an automotive lithium-based battery management system," in *Proc. Electr. Veh. Int. Conf. Show (EV)*, 2019, pp. 1–6, doi: 10.1109/EV.2019.8892986.

[2] X. Wang, H. Zhang, J. Zhang, C. Li, X. Du, and Y. Hao, "A multi-cell battery pack monitoring chip based on 0.35-μm BCD technology for electric vehicles," *IEICE Electron. Express*, vol. 12, no. 12, 2015, Art. no. 20150367, doi: 10.1587/elex.12.20150367.

[3] G. Zhu, L. Qian, Y. Li, W. Guo, R. Ding, and Y. Yang, "16-Cell stackable battery monitoring and management integrated circuit for electric vehicles," *Microelectron. J.*, vol. 136, Jun. 2023, Art. no. 105782, doi: 10.1016/j.mejo.2023.105782.

[4] V. B. Vulligaddala et al., "A 7-cell, Stackable, li-ion monitoring and active/passive balancing ic with in-built cell balancing switches for electric and hybrid vehicles," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3335–3344, May 2020, doi: 10.1109/TII.2019.2953939.

[5] K. Kadirvel, J. Carpenter, P. Huynh, J. M. Ross, R. Shoemaker, and B. Lum-Shue-Chan, "A Stackable, 6-cell, li-ion, battery management ic for electric vehicles with 13, 12-bit $\Sigma\Delta$ ADCs, cell balancing, and direct-connect current-mode communications," *IEEE J. Solid-State Circuits*, vol. 49, no. 4, pp. 928–934, Apr. 2014, doi: 10.1109/JSSC.2014.2300861.

[6] T. Wang, Y. Zhao, and J. Chen, "A battery monitoring IC with an isolated communication interface for electric vehicles," *IEICE Electron. Express*, vol. 15, no. 12, 2018, Art. no. 20180513, doi: 10.1587/elex.15.20180513.

[7] J.-K. Lee et al., "ASIL-D compliant battery monitoring IC with high measurement accuracy and robust communication," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2023, pp. 322–324, doi: 10.1109/ISSCC42615.2023.10067607.

[8] *ISO 26262 Road vehicles—Functional Safety*, ISO Standard, ISO/TC 22/SC 32, 2018.

[9] B. Tabatowski-Bush, "Functional safety for battery monitoring integrated circuits," presented at the *WCX^{TM}* 17 SAE world congress experience, Mar. 2017, Art. no. 2017-01-1202, doi: 10.4271/2017-01-1202.

[10] J. Khan, "ISO 26262 system level functional safety validation for battery management systems in automobiles," in *Proc. Innov. Power Adv. Comput. Technol. (i-PACT2017)*, 2017, pp. 1–5, doi: 10.1109/IPACT.2017.8245081.

[11] M. N. S. Kumar and K. Balakrishnan, "Functional safety development of battery management system for electric vehicles," in *Proc. IEEE Transp. Electr. Conf. (ITEC)*, 2019, pp. 1–6, doi: 10.1109/ITEC-India48457.2019.ITECINDIA2019-267.

[12] G. Hofmann and G. Scharfenberg, "Random hardware failure compliance of a cell balancing circuit with the requirements of automotive functional safety," in *Proc. Int. Conf. Appl. Electron. (AE)*, 2015, pp. 61–66.

[13] K. Sundaresan, P. E. Allen, and F. Ayazi, "Process and temperature compensation in a 7-MHz CMOS clock oscillator," *IEEE J. Solid-State Circuits*, vol. 41, no. 2, pp. 433–442, Feb. 2006, doi: 10.1109/JSSC.2005.863149.

[14] R. Capeleiro, J. M. Leitao, R. Chaves, and M. B. Santos, "Low-power frequency monitoring circuit for clock failure detection," in *Proc. Conf. Design Circuits Integr. Syst. (DCIS)*, 2018, pp. 1–6, doi: 10.1109/DCIS.2018.8681489.

[15] B. Ragchaa, X. He, L. Wu, and X. Zhang, "A high precision voltage reference circuit for battery management system chip of new energy electric vehicle," in *proc. IEEE 16th Int. Conf. Solid-State Integr. Circuit Technol. (ICSICT)*, 2022, pp. 1–3, doi: 10.1109/ICSICT55466.2022.9963270.

[16] G. Zhu, Y. Yang, and Q. Zhang, "A 4.6-ppm/°C high-order curvature compensated bandgap reference for BMIC," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 9, pp. 1492–1496, Sep. 2019, doi: 10.1109/TCSII.2018.2889808.

[17] G. Zhu, Z. Fu, T. Liu, Q. Zhang, and Y. Yang, "A 2.5 V, 2.56 ppm/°C curvature-compensated bandgap reference for high-precision monitoring applications," *Micromachines*, vol. 13, no. 3, p. 465, Mar. 2022, doi: 10.3390/mi13030465.

[18] X. He, L. Wu, X. Zhang, and M. X. Cheng, "A high-voltage high-PSRR power management circuit for bms chip of new energy vehicle," in *Proc. 13th IEEE Int. Conf. Solid-State Integr. Circuit Technol. (ICSICT)*, 2016, pp. 1387–1389, doi: 10.1109/ICSICT.2016.7998747.

[19] X.-C. Man, L.-J. Wu, X.-M. Zhang, T.-K. Ma, and W. Jia, "A high precision multi-cell battery voltage detecting circuit for battery management systems," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC)*, 2016, pp. 1–5, doi: 10.1109/VTCSpring.2016.7504072.

[20] "LTC6820 isoSPI isolated communication interface." analog. Accessed: Jan. 9, 2024. [Online]. Available: https://www.analog.com/en/products/ltc6820.html

[21] Y.-C. Chang, L.-R. Huang, H.-C. Liu, C.-J. Yang, and C.-T. Chiu, "Assessing automotive functional safety microprocessor with ISO 26262 hardware requirements," in *Proc. Int. Symp. VLSI Design, Autom. Test Techn. Papers*, 2014, pp. 1–4 doi: 10.1109/VLSI-DAT.2014.6834876.

[22] J. Han, Y. Kwon, K. Byun, and H.-J. Yoo, "A fault-tolerant cache system of automotive vision processor complying with ISO26262," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 63, no. 12, pp. 1146–1150, Dec. 2016, doi: 10.1109/TCSII.2016.2620997.

[23] *Siemens NORM SN 29500-2: Expected Values for Integrated Circuits*, Siemens Autom. Co., Munich, Germany, 2010.

BYAMBAJAV RAGCHAA received the B.S. and M.S. degrees in electronic engineering from the Mongolian University of Science and Technology (MUST), Ulaanbaatar, Mongolia, in 2007 and 2009, respectively. He is currently pursuing the Ph.D. degree with the School of Integrated Circuits, Tsinghua University, Beijing, China. Since 2010, he has been working with the Department of Electronic Engineering, MUST, where he is currently an Assistant Lecturer. His main research interests are in CMOS integrated circuits and automotive electronics.

LIJI WU (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1988, 1991, and 1997, respectively. From April 1997 to May 2000, he worked with the Center for Advanced Technology in Telecommunications, Polytechnic Institute of New York University, Brooklyn, NY, USA, as a Postdoctoral Fellow, and worked on design and implementation of high-speed control circuits and systems utilized in WDM ATM multicast optical switching systems sponsored by DARPA. Then he worked in High-Tech industry, USA, for more than four years, including TyCom Laboratories (former AT&T Bell Labs on Undersea Optical Fiber Communications), Eatontown, NJ, USA, as a Senior Member of Technical Staff. Since 2005, he has been a Full-Time Faculty with Tsinghua University. He received Tsinghua University Outstanding Graduate Award and Medal in 1988. He is the General Chair of Conference on Cryptographic Hardware and Embedded Systems in 2021.

XIANGMIN ZHANG was born in Beijing, China, in 1966. He received the B.S. degree in microelectronics from Peking University, Beijing, in 1988, and the M.S. degree in electronic engineering from Tsinghua University, Beijing, in 1991. In 1991, he joined the Institute of Microelectronics, Tsinghua University. His main research interests are in information security and automotive electronics.