AN215
Functional Safety for BMS Solution: According to ISO 13849

By Diego Quintana

September 2023

TABLE OF CONTENTS

ABSTRACT

Battery powered systems can be potentially dangerous due to their sensitivity while operating outside of the safe operating area, which could lead to a fire or an explosion. These safety risks are unacceptable for users, and therefore require specific measures to be taken to reduce the risk.

This application note describes a battery management system (BMS) architecture solution with functional safety according to ISO 13849. This application note discusses the safety functions, performance level, and definition of the safety measures implemented. These safety features reduces the risk to an acceptable level by ensuring the battery is always working within the safe operating area.

INTRODUCTION

This application note discusses the recommended safety measures to be implemented in the BMS architecture based on an MPS battery monitor and protector (BM&P) in combination with a microcontroller (MCU) to achieve the target performance level (PL), according to the ISO 13849 functional safety standard.

The document includes an overview of the BMS architecture, configuration details on the BM&P, and structure details of each safety measure, clarifying the most important points to achieve and justify the PL according to the ISO 13849 functional safety standard.

TERMS AND DEFINITIONS

The following terms and definitions are used throughout the application note. These terms are primarily related to functional safety, specifically in the context of the ISO 13849 functional safety standard. This section is key to understanding this application note and its purpose.

Safety Function

The safety function is a machine's function of which failure may result in an immediate increase of the safety risks.

Performance Level (PL)

The performance level is the discrete level used to specify the ability of safety-related parts of the control systems (SRP/CS) to perform a safety function under specific conditions. PL ranges from PLa (lowest) to PLe (highest), based on the ability to perform the safety function.

Required PL

The required PL refers to the PL applied to achieve the required risk reduction for each safety function.

Dangerous Failure

A dangerous failure refers to a failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state.

The probability of dangerous failures can be reduced by the structure used, the components used (MTTF) and the diagnostic coverage (DC).

Mean Time-To-Failure (MTTF)

The mean time-to-failure (MTTF) is a measure a component's reliability that represents the average time a component can run before it breaks or fails. Not all failures are dangerous, as the components have different failure modes with different responses. Only failures impacting the performance of the safety functions are considered dangerous failures.

In terms of safety, another important term is the mean time-to-dangerous-failure ($MTTF_D$), which is the average time a component can run before it suffers a dangerous failure.

Diagnostic Coverage

The diagnostic coverage is the measure of the diagnostic effectiveness, which can be determined as the ratio between the failure rate of the detected dangerous failures and of the total dangerous failures.

Architecture

The architecture is essential to determine the influence that a dangerous failure may have in the system's ability to perform a safety function. ISO 13849 presents three pattern options, described below:

- Single channel: A single channel is composed of one input, one logic block, and one output. During a dangerous failure, the safety function cannot be carried out.
- Single channel tested: Single channel tested is similar to the single channel, but includes a test of the logic block. During a dangerous failure, the system can detect the failure and enter a safe state before the risk increases.

- Redundant channels: Redundant channels are two complete channels operating in parallel. During a dangerous failure, the other channel can still perform the safety function.

Categories

The ISO 13849 standard proposes a simplified method for determining the PL achieved by defining a set of five categories based on the implemented architecture, the components used ($MTTF_D$), and the DC. These categories are listed below:

- Category B:
  - Architecture: Single channel
  - $MTTF_D$: Low to medium
  - DC: None
  - Achievable PL: PLa to PLb
- Category 1:
  - Architecture: Single channel
  - $MTTF_D$: High
  - DC: None
  - Achievable PL: PLa to PLc
- Category 2:
  - Architecture: Single channel tested
  - $MTTF_D$: Low to high
  - DC: Low to medium
  - Achievable PL: PLa to PLd
- Category 3:
  - Architecture: Redundant channel
  - $MTTF_D$: Low to high
  - DC: Low to medium
  - Achievable PL: PLb to PLd
- Category 4:
  - Architecture: Redundant channel
  - $MTTF_D$: High
  - DC: High
  - Achievable PL: PLe

SAFETY FUNCTIONS

The first step in the risk reduction strategy is risk analysis, where all possible scenarios of the operating conditions, failures, and potential effects are analyzed. As an outcome of this process, the safety functions and their required performance levels (PLr) are identified. Table 1 shows the typical safety functions for a battery system, including a description and PLr.

Table 1: Safety Function (SF) Definitions for BMS

SF ID	SF Description	Safe State	PLr	Safety Measures Applied
SF1	Prevents cells from over-charging	Isolate battery from charging and discharging	PLc	SM2, SM5, SM6, SM7, SM8, SM9, SM11
SF2	Prevents battery from over-charging	Isolate battery from charging and discharging	PLc	SM1, SM5, SM6, SM7, SM8, SM9, SM11
SF3	Prevents cells from under-charging	Isolate battery from charging and discharging	PLc	SM2, SM5, SM6, SM7, SM8, SM9, SM11
SF4	Prevents battery from under-charging	Isolate battery from charging and discharging	PLc	SM1, SM5, SM6, SM7, SM8, SM9, SM11
SF5	Prevents battery from charge over-current (OC) failures	Isolate battery from charging and discharging	PLc	SM3, SM5, SM6, SM9, SM11
SF6	Prevents battery from discharge OC failures	Isolate battery from charging and discharging	PLc	SM3, SM5, SM6, SM9, SM11
SF7	Prevents battery from charge short circuits	Isolate battery from charging and discharging	PLc	SM3, SM9, SM11
SF8	Prevents battery from discharge short circuits	Isolate battery from charging and discharging	PLc	SM3, SM9, SM11
SF9	Detects battery over-temperature (OT)	Isolate battery from charging and discharging	PLc	SM4, SM5, SM6, SM9, SM10, SM11
SF10	Detects battery under-temperature (UT)	Isolate battery from charging and discharging	PLc	SM4, SM5, SM6, SM9, SM10, SM11

BMS ARCHITECTURE

This section describes how the BMS architecture used to implement the safety functions. Although a fuel gauge is typically used in a BMS, one is not shown or discussed because it is not relevant to the functional safety features.

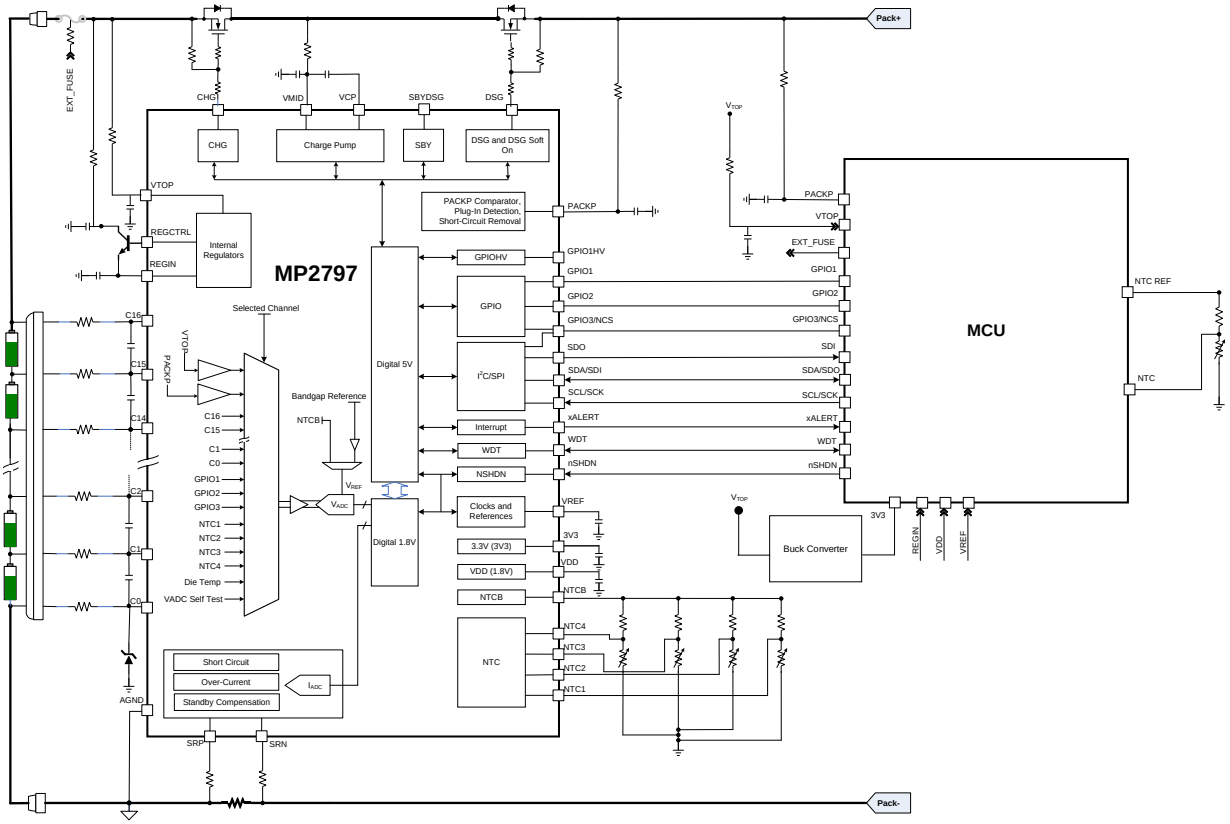

Figure 1: BMS System Architecture

The system architecture is based on an MPS BM&P (MP279x family) combined with an MCU. The BM&P senses the battery magnitudes (voltage, current, and temperature). The MCU also senses the battery and pack voltages and battery temperature. After the sensing stage, these values can be monitored by both the BM&P and the MCU, which are connected through several interfaces, described below:

- I²C and SPI communication: The safety solution is configured for I²C communication
- GPIOs: GPIO1, GPIO2, and GPIO3
- xALERT: Sensing interrupts from the BM&P to the MCU
- Watchdog timer (WDT): Resets the MCU from the BM&P
- nSHDN: Resets the BM&P from the MCU
- REGIN, VDD, and VREF: The BM&P's internal supplies (REGIN, VDD) and internal reference voltage (V_{REF})

Both ICs can implement protections and trigger a fault reaction for transitioning to the safe state. The safe state can be achieved by opening the different protection layers implemented in the power line, which are capable of isolating the battery from charging and discharging.

The first protection layer consists of contactors or protection MOSFETs (see Figure 1). The second protection layer consists of a self-controlled protector (SCP), which is a fuse that can be triggered both with and without an external command. Note that the SCP is a non-resettable device, and should be configured to only be triggered if the first protection layer fails.

SAFETY MEASURES

This chapter presents a detailed analysis of the different safety measures (SM) shown in Table 1.

SM1: Battery Over-Voltage Protection (OVP) and Under-Voltage Protection (UVP)

The BMS detects battery over-voltage (OV) and under-voltage (UV) conditions once the battery voltage exceeds or drops below the respective threshold (BATTERY_OV1, BATTERY_OV2, BATTERY_UV1, or BATTERY_UV2). OVP or UVP is triggered (the system triggers a fault reaction and opens the protections to reach a safe state).

BATTERY_OV1, BATTERY_OV2, BATTERY_UV1, and BATTERY_UV2 can be configured by the user. BATTERY_OV2 should be set higher than BATTERY_OV1 and BATTERY_UV2 lower than BATTERY_UV1.

Implementation

SM1 is implemented in a structure of redundant channels. The input consists of a voltage divider from the battery voltage to the BM&P, and another voltage divider — independent from the battery voltage — to the MCU. In the BM&P, an internal analog-to-digital converter (ADC) converts the sensed signal into two digital signals (BATTERY_VOLT and BATTERY_VOLT_HR).

BATTERY_VOLT is used by the BM&P for internal over-voltage protection (OVP) and under-voltage protection (UVP), for if the voltage exceeds BATTERY_OV1 or drops below BATTERY_UV1. If either of these occur, the BM&P triggers the first protection layer. BATTERY_VOLT_HR is stored in the BM&P's registers and is read by the MCU via the I^2C. This allows the user to perform a plausibility check of the sensed voltage (see the SM8: Battery Voltage Plausibility Check section on page 13).

In the MCU, an internal ADC converts the sensed signal into a digital signal (BATTERY_VOLT_MCU). Once the MCU has read the values, it monitors these values and compares them to BATTERY_OV1, BATTER_OV2, BATTERY_UV1, and BATTERY_UV2.

If BATTERY_VOLT_MCU exceeds BATTERY_OV1 or BATTERY_UV1, the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer via the BM&P. If BATTERY_VOLT_MCU exceeds BATTERY_OV2 or BATTERY_UV2, the MCU sets the EXT_FUSE pin high, which opens the second protection layer.

In applications with up to 60A of nominal current, the second protection layer can be triggered by the MCU across the entire nominal battery voltage range. In applications with higher nominal current, triggering the second protection layer cannot be ensured at lower nominal battery voltages. Only the first protection layer can be relied on for UVP.

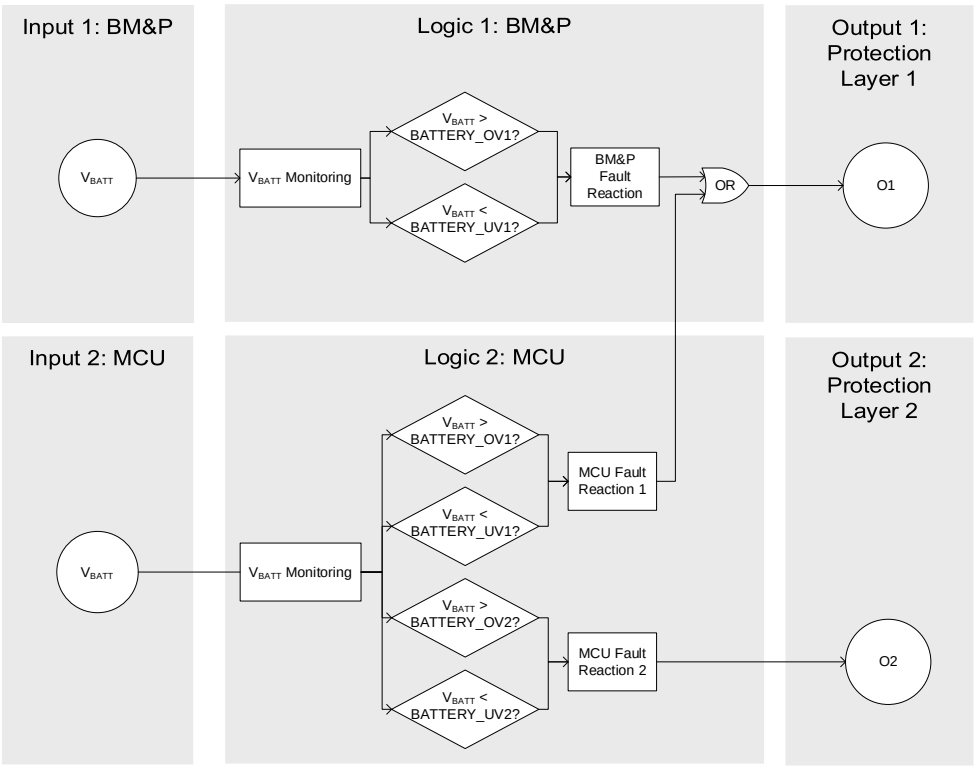

Figure 2: SM1 Block Diagram

SM2: Cell OVP and UVP

The BMS detects cell OV and UV conditions once any of the cell voltages exceed or drop below the respective thresholds (CELL_OV1, CELL_OV2, CELL_UV1, or CELL_UV2). OVP or UVP is triggered (the system triggers a fault reaction and opens the protections to reach a safe state).

CELL_OV1, CELL_OV2, CELL_UV1, and CELL_UV2 can be configured by the user. CELL_OV2 should be set higher than CELL_OV1 and CELL_UV2 shall be lower than CELL_UV1.

Implementation

SM2 is implemented in a structure with a single input and redundant logic and output. The input consists of the voltage divider from each cell to the BM&P. An internal ADC converts the input into two digital signals per cell (CELLx_VOLT and CELLx_VOLT_HR).

CELLx_VOLT and CELLx_VOLT_HR are generic names for the cell voltage measurement of each cell, where “x” is the cell (from 1 to *n*), depending on the configuration (e.g. CELL1_VOLT or CELL2_VOLT).

CELLx_VOLT is used by the BM&P for internal OVP and UVP, for if the voltage exceeds CELL_OV1 or drops below CELL_UV1. If either of these occur, the BM&P triggers the first protection layer. CELLx_VOLT_HR is stored in the BM&P’s registers and is read by the MCU via the I^2C. Then the MCU compares CELLX_VOLT_HR to CELL_OV1, CELL_OV2, CELL_UV1, and CELL_UV2.

If CELLx_VOLT_HR exceeds CELL_OV1 or drops below CELL_UV1, the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer via the BM&P. If CELLx_VOLT_HR exceeds CELL_OV2 or drops below CELL_UV2, the MCU sets the EXT_FUSE pin high, which opens the second protection layer.

In applications with up to 60A of nominal current, the second protection layer can be triggered by the MCU across the entire nominal battery voltage range. In applications with higher nominal current, triggering the second protection layer cannot be ensured at lower nominal battery voltages. Only the first protection layer can be relied on for UVP.

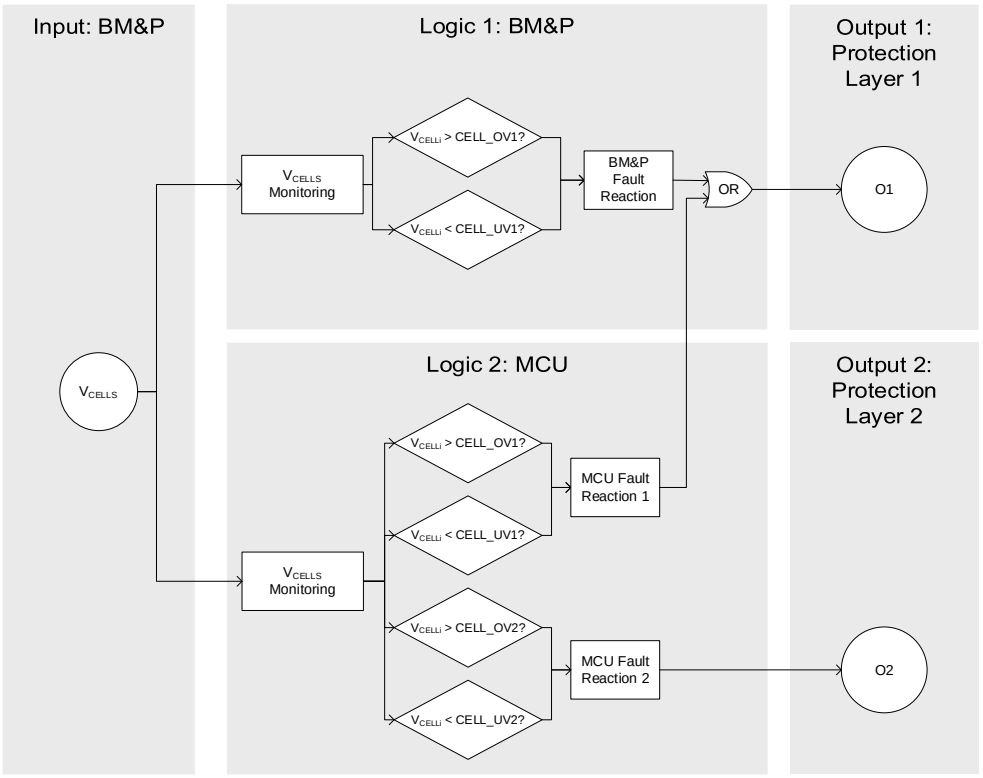

Figure 3: SM2 Block Diagram

SM3: Battery Over-Current Protection (OCP) and Short-Circuit Protection

The BMS detects battery charge and discharge over-current (OC) and short-circuit conditions once the current exceeds the respective threshold (BATTERY_CHG_OC, BATTERY_DSG_OC1, BATTERY_DSG_OC2, BATTERY_CHG_SC, or BATTERY_DSG_SC). OCP or short-circuit protection is triggered (the system triggers a fault reaction and opens the protections to reach a safe state).

BATTERY_CHG_OC, BATTERY_DSG_OC1, BATTERY_DSG_OC2, BATTERY_CHG_SC, and BATTERY_DSG_SC can be configured by the user. The short-circuit thresholds should be set higher than the OC thresholds. BATTERY_DSG_OC2 should be set higher than BATTERY_DSG_OC1.

Implementation

SM3 is implemented in a structure with a single input and redundant logic and output. The input consists of a shunt resistor placed on the low-side power line, which is connected directly to the BM&P. In the BM&P, an internal ADC converts the sensed voltage difference signal into a digital value (BATTERY_CURR) and are placed analog comparators, independent from the ADC path.

The analog comparators in the BM&P detect OC and short-circuit conditions by comparing the sensed current to the respective thresholds. If the sensed current exceeds one of the thresholds, the BM&P triggers the first protection layer.

BATTERY_CURR is stored in the BM&P's registers and is read by the MCU via the I^2C. Then the MCU compares BATTERY_CURR to BATTERY_CHG_OC and BATTERY_DSG_OC1. If BATTERY_CURR exceeds BATTERY_CHG_OC or BATTERY_DSG_OC1, the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer via the BM&P. After this reaction, if the MCU detects that the first protection layer is not opened, the MCU sets the EXT_FUSE pin high, which opens the second protection layer.

Note that short-circuit protection is not implemented in the MCU, as it is not fast enough to safely react to a short circuit.

In applications up to 60A of nominal current, the second protection layer can be triggered by MCU in the whole nominal battery voltage range. In applications with higher nominal current, trigger the second protection layer cannot be ensured in the lower range of the nominal battery voltage. In this case, only the first protection layer can be relied on for OCP.

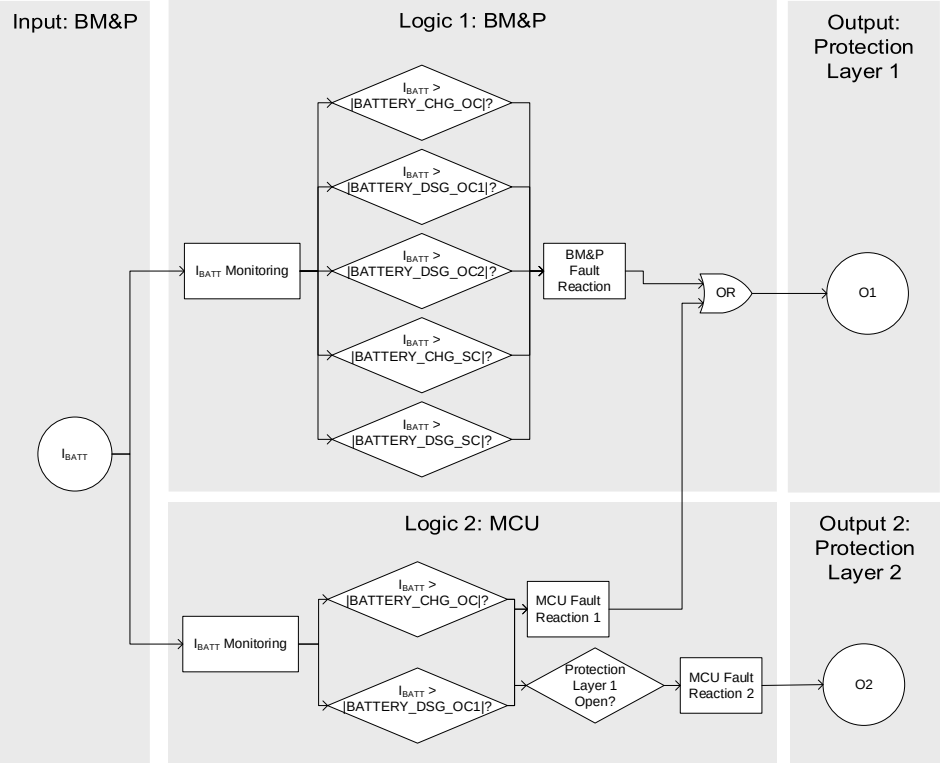

Figure 4: SM3 Block Diagram

SM4: Battery Over-Temperature Protection (OTP) and Under-Temperature Protection (UTP)

The BMS detects battery over-temperature (OT) and under-temperature (UT) conditions once the battery temperature exceeds or drops below the respective threshold (BATTERY_OT or BATTERY_UT). OT or UT protection is triggered (the system triggers a fault reaction and opens the protections to reach a safe state).

BATTERY_OT or BATTERY_UT can be configured by the user.

Implementation

SM4 is implemented in a structure of redundant channels. The BM&P input consists of at least two negative temperature coefficient (NTC) thermistor circuits, placed at sensitive points of the battery, and the MCU input consists of a NTC thermistor circuit placed next to a NTC from BM&P input. In the BM&P, an internal ADC converts the input into two signals (BATTERY_TEMPx and BATTERY_TEMPx_HR) per NTC sensor.

BATTERY_TEMPx and BATTERY_TEMPx_HR are generic names for the battery temperature measurement, where “x” is the NTC sensor (from 1 to *n*), depending on the configuration (e.g. BATTERY_TEMP1 or BATTERY_TEMP2).

BATTERY_TEMPx is used by the BM&P for internal over-temperature protection and under-temperature protection, for if the temperature exceeds BATTERY_OT or drops below BATTERY_UT. If either of these occur, the BM&P triggers the first protection layer. BATTERY_TEMPx_HR is stored in the BM&P’s registers and is read by the MCU via the I^2C. This allows the user to perform a plausibility check of the sensed temperatures in the MCU (see SM10: Temperature Plausibility Check section on page 13).

In the MCU, an internal ADC converts the sensed signal into a digital signal (BATTERY_TEMP_MCU). Once the MCU has read the values, it monitors these values and compares them to BATTERY_OT and BATTERY_UT.

If BATTERY_TEMP_MCU values exceed BATTERY_OT or drop below BATTERY_UT, the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer via the BM&P. After this reaction, if the MCU detects that the first protection layer is not opened, the MCU sets the EXT_FUSE pin high, which opens the second protection layer.

In applications up to 60A of nominal current, the second protection layer can be triggered by MCU in the whole nominal battery voltage range. In applications with higher nominal current, trigger the second protection layer cannot be ensured in the lower range of the nominal battery voltage. In this case, only the first protection layer can be relied on for OTP and UTP.

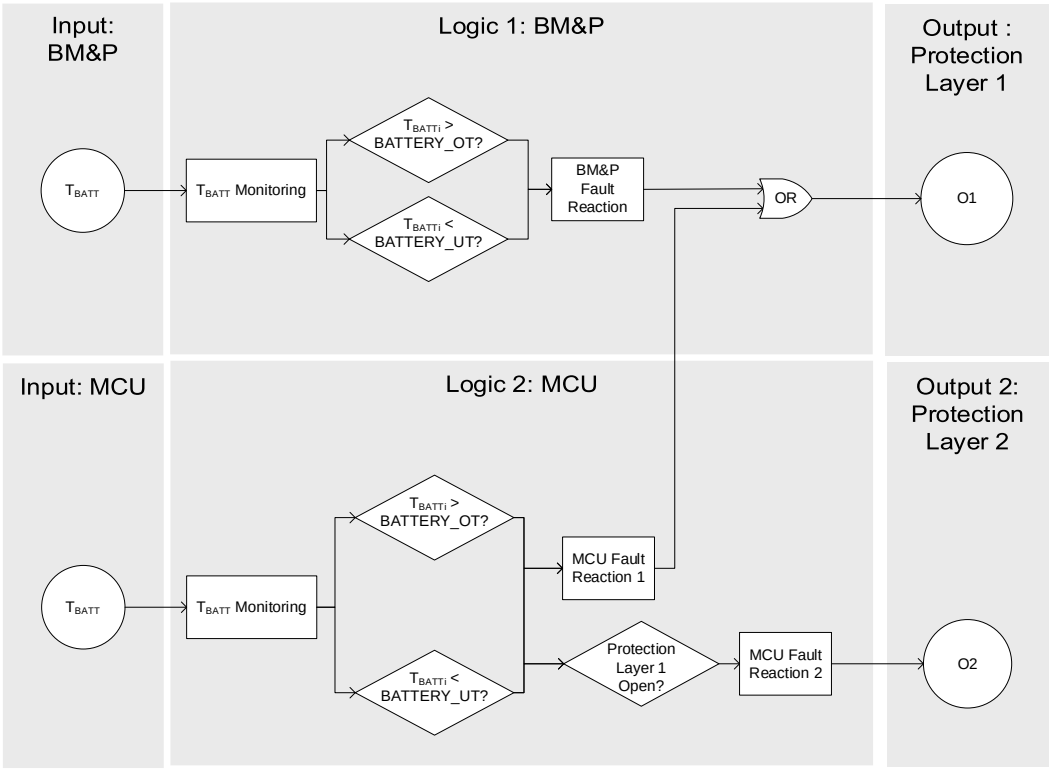

Figure 5: SM4 Block Diagram

SM5: I²C Corruption Protection

To ensure that the values sent via I²C are correct, a cyclic redundancy check (CRC) is implemented to ensure I²C communication corruption is detected up to 2 erroneous bits. This protects the following safety signals among other signals:

- BATTERY_VOLT_HR
- CELLX_VOLT_HR
- BATTERY_CURR
- BATTERY_TEMPX_HR

Both BM&P and MCU generate a CRC and include it as part of the transmitted signal. The receiver device (can be both MCU and BM&P) checks the CRC with the values received in the signal.

If the CRC fails, the receiver requests the transmitter for the value again. If the CRC fails after three retries, the MCU sets the nSHDN pin low, which resets the BM&P and opens the first protection layer.

SM6: I²C Loss Protection

The BM&P implements an internal watchdog timer (WDT) with a configurable timeout time (WDT_TIMEOUT) to detect I²C communication loss.

The WDT is reset every time an I²C communication request occurs. If a communication request does not occur before the timeout, I²C communication is lost. This could cause chip malfunctions or other faults that may prevent the MCU from performing the safety function correctly.

When WDT timeout occurs, the BM&P opens the first protection layer and the WDT pin is pulled high during WDT_RSTPULSE_LEN, which resets the MCU. The BM&P self-resets.

SM7: Cell Voltage Plausibility Check

The BMS performs a voltage plausibility check of the battery voltage and the sum of all the cell voltages to detect a voltage sensing failure if the difference of the two values exceeds CELL_VOLT_MAX_DIFF.

SM7 is carried out by the MCU, which already has BATTERY_VOLT_MCU and CELLX_VOLT_HR signals to perform part of SM1 and SM2. The MCU internally adds all of the CELLX_VOLT_HR signals and calculates the difference between that result and BATTERY_VOLT_MCU.

If the difference exceeds CELL_VOLT_MAX_DIFF, the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer.

SM7 adds robustness to SM1 and SM2, as it validates the sensed voltages.

SM8: Battery Voltage Plausibility Check

The BMS performs a voltage plausibility check of the sensed battery voltages to detect a voltage sensing failure if the difference of the two values exceeds BATTERY_VOLT_MAX_DIFF.

SM7 is carried out by the MCU, which already has BATTERY_VOLT_MCU and BATTERY_VOLT_HR signals to perform part of SM1, SM2 and SM7. The MCU internally calculates the difference between both battery voltage measurements.

If the difference exceeds BATTERY_VOLT_MAX_DIFF, the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer.

SM8 adds robustness to SM1, SM2 and SM7, as it validates the sensed voltages.

SM9: Protective Fuse

The BMS implements an SCP in the power line to isolate the battery against some faults. The SCP is a fuse that can be triggered internally due to the amount of power and heat dissipation in the power line (e.g. a short circuit occurs) or can be assisted by an external circuit.

SM9 corresponds to the second protection layer used in SM1, SM2, SM3 and SM4. It also makes short-circuit protection more robust.

SM10: Temperature Plausibility Check

The BMS performs a temperature plausibility check between the different battery temperatures values, and detects a temperature sensing failure if the difference between the values exceeds TEMP_MAX_DIFF.

SM10 is carried out by the MCU, which already has BATTERY_TEMP_MCU and BATTERY_TEMPX_HR signals to perform part of SM4. The MCU internally calculates the difference between the BATTERY_TEMP_MCU and BATTERY_TEMPX_HR values. If the difference exceeds MAX_TEMP_DIFF, the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer.

SM10 adds robustness to SM4, as it validates the sensed temperatures from the NTC circuits.

SM11: Self-Diagnostics

The BMS implements self-diagnostic capabilities to prevent malfunction of the main components. SM11 is comprised of the following:

- BM&P internal supply monitoring
- BM&P ADC self-test
- BM&P OTP CRC check
- BM&P drivers' output value monitoring
- First protection layer status check

BM&P Internal Supply Monitoring

The BM&P is connected to the battery voltage. This voltage is used internally as an input for the voltage regulators to obtain the different internal supplies (REGIN [5V] and VDD [1V8] rails) and V_{REF}. These supplies and V_{REF} are used internally to supply the different parts of the device, including the digital parts where the logic is implemented and the reference for the ADC measurements are set. If any of these supplies exceed or drop below the respective threshold (REGIN_OV, REGIN_UV, VDD_OV, VDD_UV, VREF_OV, or VREF_UV), the BM&P may behave unexpectedly, which may prevent it from performing the safety function correctly.

To prevent this, the BM&P outputs its supplies to the MCU for monitoring. This allows the MCU, which is not supplied by any of these internal supplies, to monitor these signals and ensure there is no interference.

If the MCU detects that one of the signals is above or below the defined thresholds, the MCU sets the nSHDN pin low, which resets the BM&P and opens the first protection layer.

BM&P's Analog-to-Digital Converter (ADC) Self-Test

The BM&P self-tests the ADC used for voltage and temperature measurements to detect possible malfunctions. The ADC input is selected by a multiplexer. One of the inputs of the multiplexer is a known value which, once converted into a digital value, matches the expected value with a maximum difference of MAX_SELFTEST_DIFF.

If the converted value is outside the expected range, the BM&P generates an interrupt through the GPIO3 pin. The interrupt is read by the MCU, which checks the SELF_TEST_INT_STS register and — if the value of the register is 1 — the MCU sets the GPIO1 and GPIO2 pins low, which opens the first protection layer via the BM&P.

BM&P One-Time Programmable (OTP) Memory Cyclical Redundancy Check (CRC)

The BM&P implements one-time programmable (OTP) memory with CRC check to detect OTP errors that could lead to a BM&P malfunction.

If the OTP CRC fails, safe operation cannot be ensured, so the BM&P opens the first protection layer, which isolates the battery to reach a safe state.

BM&P Drivers' Output Value Monitoring

The BM&P monitors the drivers' output values in such a way that if the value of the drivers' output is not the expected value before DRIVERS_TIMEOUT, a driver fault is detected.

If a driver fault is detected, safe operation cannot be ensured, so the BM&P opens the first protection layer, which isolates the battery to reach a safe state.

First Protection Layer Status Check

The MCU monitors the status of the first protection layer by sensing and comparing the battery voltage (BATTERY_VOLTAGE_MCU) and the pack voltage (PACK_VOLTAGE_MCU).

If BATTERY_VOLTAGE_MCU = PACK_VOLTAGE_MCU ± VOLT_THRESHOLD, the first protection layer is closed.

If BATTERY_VOLTAGE_MCU ≠ PACK_VOLTAGE_MCU ± VOLT_THRESHOLD, the first protection layer is open.

If the status of the first protection layer differs from the expected status, then the MCU sets the EXT_FUSE pin high, which triggers the second protection layer.

In applications with up to 60A of nominal current, the second protection layer can be triggered by the MCU across the entire nominal battery voltage range. In applications with higher nominal current, triggering the second protection layer cannot be ensured at lower nominal battery voltages. Only the first protection layer can be relied on for UVP.

CONCLUSION

The increasing importance of products powered by batteries in industrial applications with safety implications is putting the focus on BMS development according to the ISO 13849 standard. BMS must implement safety measures to ensure robustness and risk reduction to an acceptable level, as described throughout this application note. This application note describes a BMS concept (with both architecture and safety measures) aligned with the ISO 13849 safety standard to achieve a specific PL by following the process described in the standard.

REVISION HISTORY

Revision #	Revision Date	Description	Pages Updated
1.0	9/20/2023	Initial Release	-