AN215
Functional Safety Concept for BMS Solution: According to ISO 13849

By Diego Quintana

October 2024

TABLE OF CONTENTS

ABSTRACT

Battery-powered systems can be dangerous due to their sensitivity while operating outside of the safe operating area (SOA), and can lead to a fire or an explosion. These safety risks are unacceptable for users, and therefore require specific measures to reduce potential risks.

This application note will describe a battery management system (BMS) architecture solution with functional safety according to ISO 13849. This application note will discuss the safety functions, performance level, and the definitions of the implemented safety measures. These safety features reduce risk to an acceptable level by ensuring that the battery is always working within the SOA.

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 unit (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, details on how to configure the BM&P, and provides the structure details for each safety measure. It also clarifies 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 the function of a machine whose failure can result in an immediate increase of risk(s).

Performance Level (PL)

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

Required Performance Level (PLr)

The required performance level (PLr) must be met to achieve the required risk reduction for each safety function.

Dangerous Failure

A dangerous failure is the failure of an element, subsystem, and/or system that plays a part in implementing the safety function such that it:

a. Prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the machine/machinery is put into hazardous or potentially hazardous state; or

b. Decreases the probability that the safety function operates correctly when required.

Mean Time to Dangerous Failure (MTTF$_D$)

The mean time to dangerous failure (MTTF$_D$) is the expected mean time to a dangerous failure.

Diagnostic Coverage

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

Category

A category is the classification of the subsystem in respect to its resistance to faults and the subsequent behavior in the fault condition, which is achieved by the structural arrangement of the parts, fault detection, and/or by the subsystem’s reliability.

ARCHITECTURES

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 (see Figure 1). During a dangerous failure, the safety function cannot be carried out.

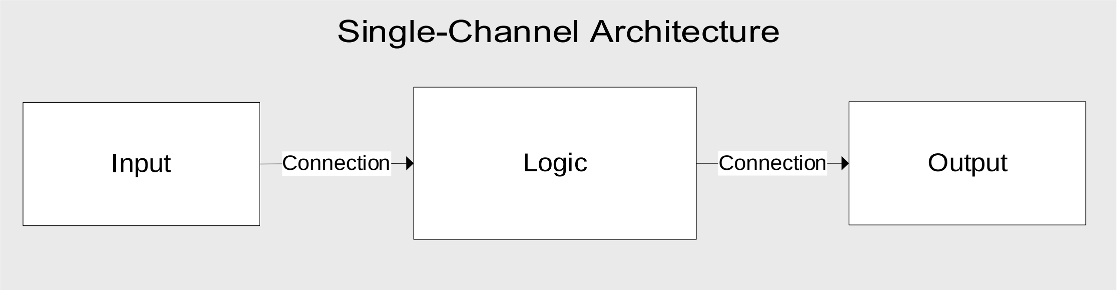

Figure 1: Single-Channel Architecture

Single-Channel Tested

A single-channel tested is similar to a single channel but includes a test of the logic block (see Figure 2). During a dangerous failure, the system can detect the failure and enter a safe state before the risk increases.

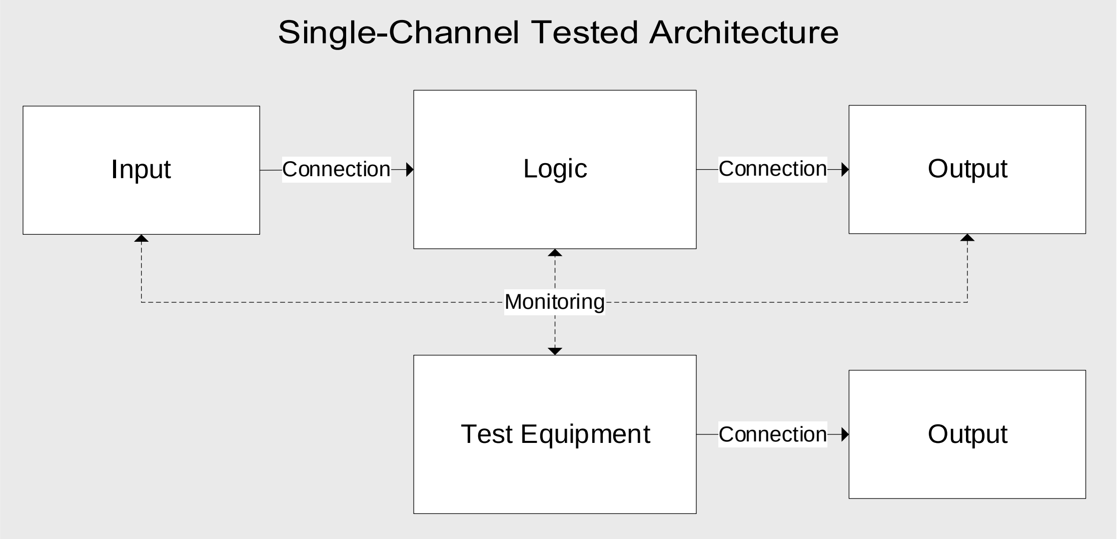

Figure 2: Single-Channel Tested Architecture

Redundant Channels

Redundant channels are two complete channels operating in parallel (see Figure 3 on page 7). During a dangerous failure, the channel that is not experiencing the failure can still perform the safety function.

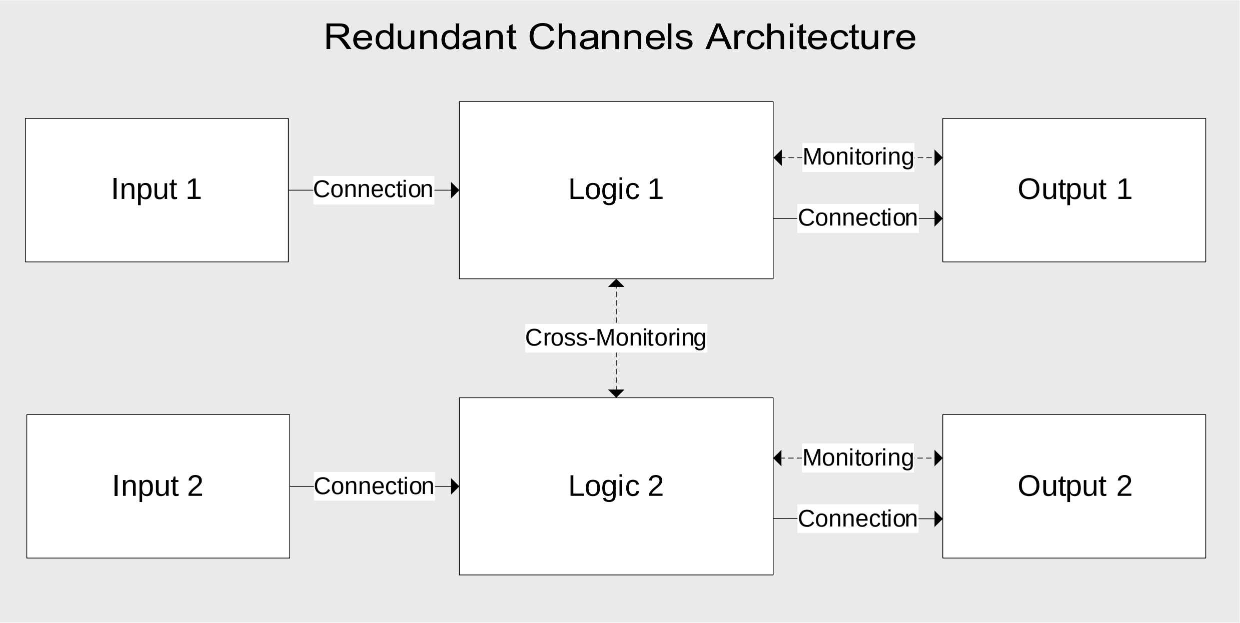

Figure 3: Redundant Channels Architecture

Categories

The ISO 13849 standard proposes a simplified method to determine the achieved PL 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 channels
  - $MTTF_D$: Low to high
  - DC: Low to medium
  - Achievable PL: PLb to PLd

- Category 4
  - Architecture: Redundant channels
  - 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. In addition, the safety measures, which are described later on in the document, are traced to each of the safety functions.

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, SM12, SM13, SM14, SM15, SM16, SM17
SF2	Prevents battery from over-charging	Isolate battery from charging and discharging	PLc	SM1, SM5, SM6, SM7, SM8, SM9, SM11, SM13, SM14, SM15, SM16, SM17
SF3	Prevents cells from under-charging	Isolate battery from charging and discharging	PLc	SM2, SM5, SM6, SM7, SM8, SM9, SM11, SM12, SM13, SM14, SM15, SM16, SM17
SF4	Prevents battery from under-charging	Isolate battery from charging and discharging	PLc	SM1, SM5, SM6, SM7, SM8, SM9, SM11, SM13, SM14, SM15, SM16, SM17
SF5	Prevents battery from charge over-current (OC) failures	Isolate battery from charging and discharging	PLc	SM3, SM5, SM6, SM9, SM11, SM13, SM14, SM15, SM16, SM17
SF6	Prevents battery from discharge OC failures	Isolate battery from charging and discharging	PLc	SM3, SM5, SM6, SM9, SM11, SM13, SM14, SM15, SM16, SM17
SF7	Prevents battery from charge short circuits	Isolate battery from charging and discharging	PLc	SM3, SM9, SM11, SM13, SM17
SF8	Prevents battery from discharge short circuits	Isolate battery from charging and discharging	PLc	SM3, SM9, SM11, SM13, SM17
SF9	Detects battery over-temperature (OT)	Isolate battery from charging and discharging	PLc	SM4, SM5, SM6, SM9, SM10, SM11, SM13, SM14, SM15, SM16, SM17
SF10	Detects battery under-temperature (UT)	Isolate battery from charging and discharging	PLc	SM4, SM5, SM6, SM9, SM10, SM11, SM13, SM14, SM15, SM16, SM17

BMS ARCHITECTURE

This section describes how the BMS architecture is used to implement the safety functions. Although a fuel gauge is typically used in a BMS, one is not shown or discussed in this document because it is not relevant to the functional safety features. Figure 4 shows the BMS system architecture.

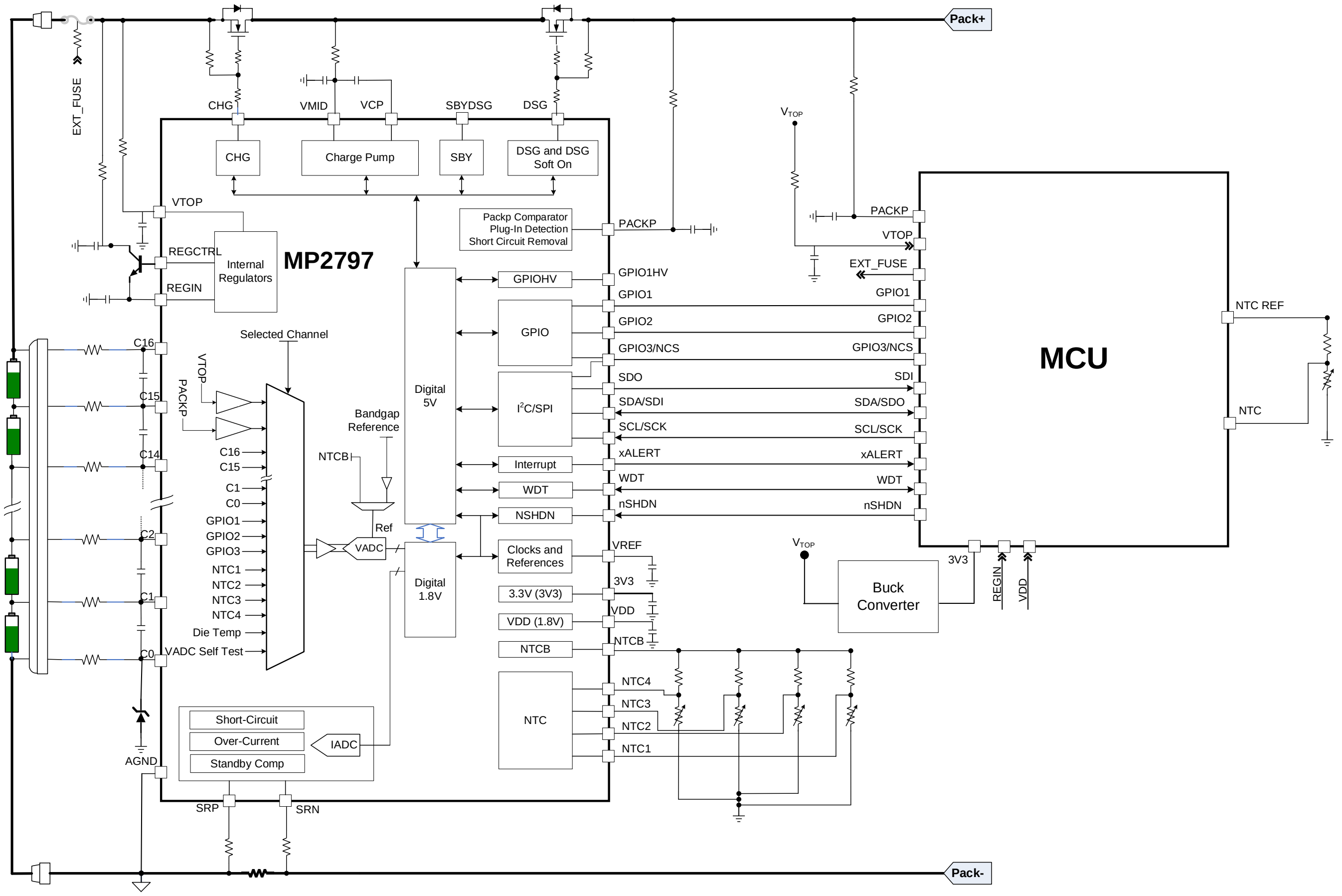

Figure 4: BMS System Architecture

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 the BM&P and the MCU. The BM&P and the MCU are connected through several interfaces, described below:

- I²C and SPI communication: The safety solution is configured for I²C communication.
- General-purpose input/output (GPIO): 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}).

The power supply architecture implemented in this concept ensures independence from the supply point of view between the BM&P and the MCU. The BM&P is connected directly to the battery voltage through a high-voltage input pin capable of withstanding voltage values that exceed the maximum battery voltage.

This battery voltage goes internally into a voltage regulator block from which the different internal supplies are generated. The MCU is supplied with an external buck converter; the converter's input is connected to the battery voltage, and its output is connected directly to the MCU. The only common point in the supply for both chips is the battery, which is monitored for over-voltage (OV) and under-voltage (UV) events by the analog front-end (AFE) and MCU.

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

The first protection layer consists of contactors or protection MOSFETs (see Figure 4 on page 10). 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. The SCP is a non-resettable device, and should be configured to only be triggered if the first protection layer fails.

The mechanism to blow the SCP through its internal heater has a power dissipation operational range that must be met to ensure that the SCP is blown safely. The standard method to blow the fuse through the heater is by closing the transistor that controls the current flow through the heater, then to keep the transistor closed until the fuse blows. Due to the battery voltage level, however, this method may not ensure that the power dissipation through the heater is within the power dissipation operational range, as the power dissipation depends on the battery voltage and the heater's internal resistor.

It is important to ensure that the power dissipation exceeds the lower threshold and is below the upper threshold. If the power dissipation is below the lower threshold, the fuse does not blow because of the heat produced in the heater. If the power dissipation exceeds the upper threshold, the heater can break before fusing the fuse.

If the standard method to blow the SCP does not ensure that the power dissipation generated in its internal heater is within its nominal range across the battery voltage's operational range, a method to overcome this SCP limitation is by choosing an SCP that has an internal heater with a sufficiently low resistance. In this scenario, the power dissipation through the heater is within the power dissipation operational range at the minimum battery voltage level; apply a pulse-width modulation (PWM) control signal with an adjustable duty cycle so that the average power dissipation of the SCP's internal heater is always within its power dissipation operational range.

The power dissipation operational range depends on the SCP used, so it should be addressed in each case by the system integrator. The system integrator is responsible for selecting the SCP and applying the correct control to it in order to ensure a safe and correct SCP is blown across the battery voltage's operational range.

BM&P Products Suitability

The present BMS concept supports the integration of the following BM&P devices in the MP279x family:

- MP2790
- MP2791
- MP2793
- MP2797

These chips only have one version available on the market. If new versions are developed, an impact analysis will be performed to evaluate their suitability in this concept.

ASSUMPTIONS OF USE

This section in intended to highlight the assumptions of use, which were identified during the analyses and reviews that were performed to ensure the robustness of this BMS concept.

- It is assumed the recommended operating conditions provided in the BM&P datasheet and the other selected components are considered and satisfied.
- The BM&P generates a 3V3 supply that can be used to supply an external device. For this concept, it is assumed that the 3V3 supply that the BM&P generates can not be used to supply the MCU, as this can lead to common cause failure (CCF) issues.
- Standby (SBY) mode is not supported in this concept; it is assumed that SBY mode is not used, and the P-channel MOSFET (P-FET) related to SBY mode is not present in the design.
- The pre-charge process is not supported in this concept; it is assumed that the pre-charge FET is not present in the design.
- The shunt resistor is assumed to be a high-accuracy, power metal strip resistor prepared to withstand short-term overloads. It is assumed that the shunt resistor works within its nominal tolerance limits until a short-term overload first occurs — after this point, the resistance cannot be relied upon. In this scenario, an action is required to ensure safe operation.
  To prevent this situation from occurring, it is assumed that a shunt resistor was selected with a minimum unloading factor of 2, so that the nominal operating current requirement is fulfilled.
- It is assumed that, if applicable, measures for electrical safety in high-voltage (HV) systems should be taken in the final design.
- It is assumed that all the mandatory Safety Measures should be implemented so that the final design can claim the PLc.
- It is assumed that the present document pretends to define just a BMS concept oriented to claim PLc according to ISO13849. To finally claim the PLc, further processes and activities should be carried out to demonstrate the suitability of the final design to achieve the desired safety level.

SAFETY MEASURES

This chapter presents a detailed analysis of the different safety measures (SM) shown in Table 1 on page 9.

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

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

BATTERY_OV and BATTERY_UV can be configured by the user. At the end of the document, Table 2 on page 23 shows reference values for these thresholds.

Implementation

SM1 is implemented in a structure of redundant channels. The input consists of a voltage divider connected from the battery voltage to the BM&P, and another voltage divider — independent from the battery voltage — connected 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 OVP and UVP if the voltage exceeds BATTERY_OV or drops below BATTERY_UV, respectively. 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^{2}C. This allows the user to perform a plausibility check of the sensed voltage (see the SM8: Battery Voltage Plausibility Check section on page 18 for more details).

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_OV and BATTERY_UV.

If BATTERY_VOLT_MCU exceeds BATTERY_OV or BATTERY_UV, 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.

Figure 5 on page 14 shows the SM1 block diagram.

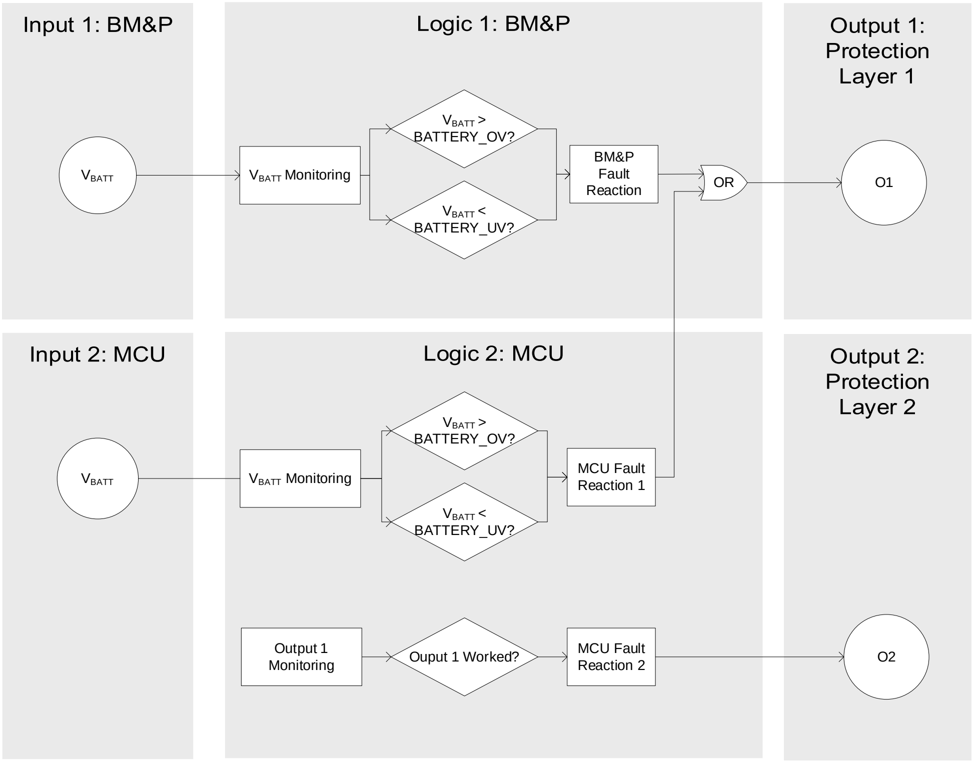

Figure 5: SM1 Block Diagram

SM2: Cell OVP and UVP

The BMS detects cell OV and UV conditions if any of the cell voltages exceed or drop below the respective thresholds (CELL_OV or CELL_UV). Then OVP or UVP is triggered (the system triggers a fault reaction and opens the protections to reach a safe state).

CELL_OV and CELL_UV can be configured by the user. At the end of the document, Table 2 on page 23 shows reference values for these thresholds.

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 if the voltage exceeds CELL_OV or drops below CELL_UV. 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_OV and CELL_UV.

If CELLx_VOLT_HR exceeds CELL_OV or drops below CELL_UV, 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.

Figure 6 on page 15 shows the SM2 block diagram.

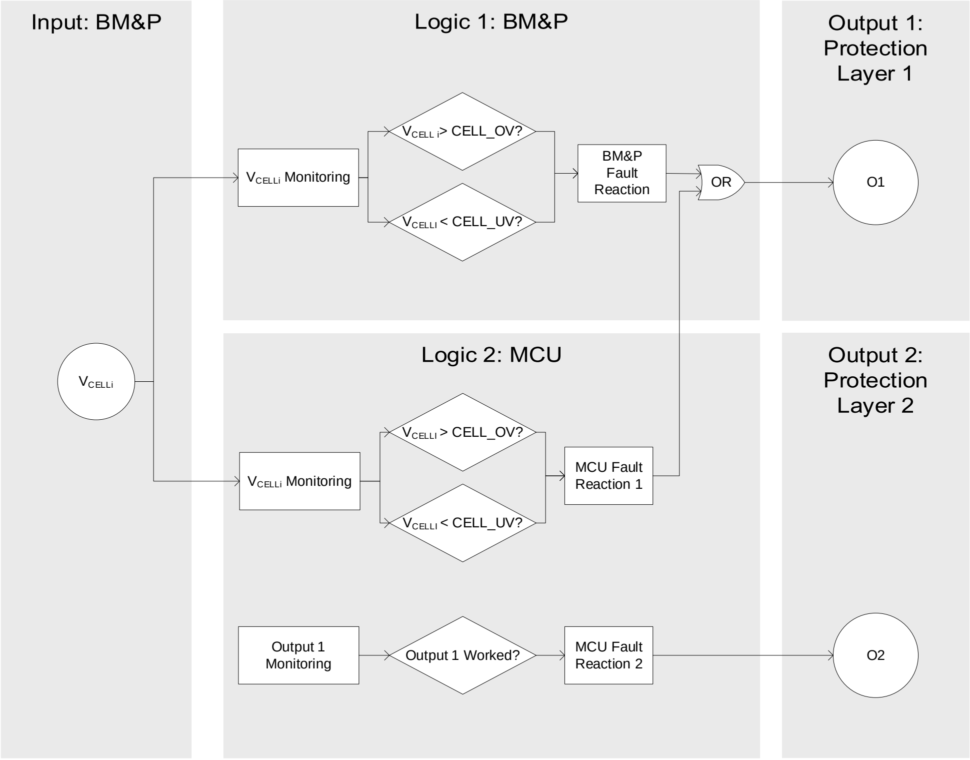

Figure 6: SM2 Block Diagram

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). Then 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 above the OC thresholds. BATTERY_DSG_OC2 should be set to exceed BATTERY_DSG_OC1. At the end of the document, Table 2 on page 23 shows reference values for these thresholds.

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 there are implemented two different current sensing paths. The first path consists of an internal ADC (IADC) that converts the sensed voltage difference signal into a digital value (BATTERY_CURR) that will be used on the digital logic side afterwards. The second path consist of a full analog path in which the sensed voltage difference is input into analog comparators. This path is 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.

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

Figure 7 shows the SM3 block diagram.

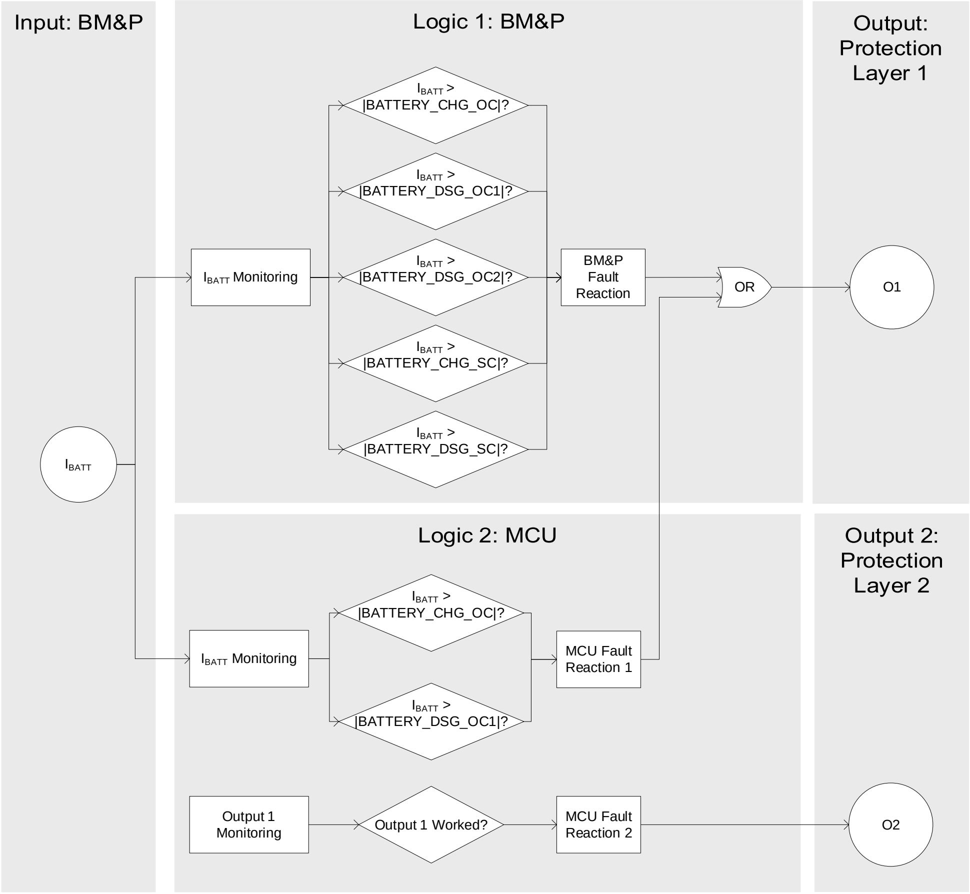
Input: BM&P
Logic 1: BM&P
Output: Protection Layer 1
I_BATT > |BATTERY_CHG_OC|?
I_BATT > |BATTERY_DSG_OC1|?
I_BATT Monitoring
I_BATT > |BATTERY_DSG_OC2|?
BM&P Fault Reaction
OR
O1
I_BATT > |BATTERY_CHG_SC|?
I_BATT > |BATTERY_DSG_SC|?
I_BATT
Logic 2: MCU
Output 2: Protection Layer 2
I_BATT > |BATTERY_CHG_OC|?
I_BATT Monitoring
MCU Fault Reaction 1
I_BATT > |BATTERY_DSG_OC1|?
Output 1 Monitoring
Output 1 Worked?
MCU Fault Reaction 2
O2

Figure 7: 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_CHG_OT, BATTERY_CHG_UT, BATTERY_DSG_OT, or BATTERY_DSG_UT). Then OT or UT protection is triggered (the system triggers a fault reaction and opens the protections to reach a safe state).

BATTERY_CHG_OT, BATTERY_CHG_UT, BATTERY_DSG_OT, or BATTERY_DSG_UT can be configured by the user. At the end of the document, Table 2 on page 23 shows reference values for these thresholds.

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 an NTC thermistor circuit placed next to an 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 the 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 OT protection and UT protection if the temperature exceeds BATTERY_CHG_OT or BATTERY_DSG_OT, or drops below BATTERY_CHG_UT or BATTERY_DSG_UT, depending on whether there is a charging or discharging process in progress. 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^{2}C. This allows the user to perform a plausibility check of the sensed temperatures in the MCU (see the SM10: Temperature Plausibility Check section on page 19 for more details).

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_CHG_OT and BATTERY_CHG_UT, or BATTERY_DSG_OT and BATTERY_DSG_UT, depending on whether there is a charging or discharging process in progress.

If BATTERY_TEMP_MCU exceeds BATTERY_CHG_OT or BATTERY_DSG_OT (or drops below BATTERY_CHG_UT or BATTERY_DSG_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.

Figure 8 shows the SM4 block diagram.

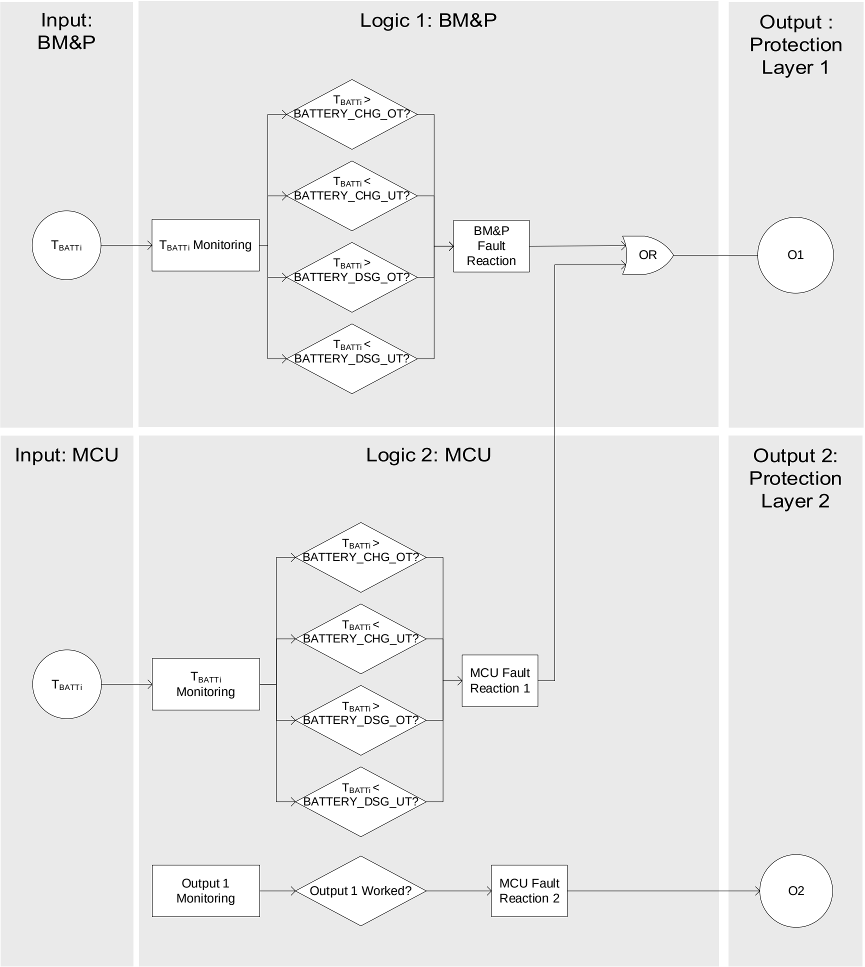

Figure 8: SM4 Block Diagram

SM5: I^{2}C Corruption Protection

To ensure that the values sent via the I^{2}C are correct, a cyclic redundancy check (CRC) is implemented to ensure I^{2}C 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

The BM&P and MCU generate a CRC and include it as part of the transmitted signal. The receiver device (can be the 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: I^{2}C Loss Protection

The BM&P implements an internal watchdog timer (WDT) with a configurable timeout time (WDT_TIMEOUT) to detect I^{2}C communication loss.

The WDT is reset every time an I^{2}C communication request occurs. If a communication request does not occur before the timeout, I^{2}C communication is lost. This could cause chip malfunctions or other faults that may prevent the MCU from performing the safety function correctly.

If a 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. Then 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 between 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 for the sensed battery voltages to detect a voltage-sensing failure if the difference between the two values exceeds BATTERY_VOLT_MAX_DIFF.

SM8 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 it 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: BM&P Self Diagnostics

The BM&P implements self-diagnostic measures 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

SM11.1: 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], 3V3, 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 VADC. If any of these supplies exceed or drop below their respective thresholds, the BM&P may behave unexpectedly, which may prevent it from performing the safety function correctly.

- REGIN and VDD supply different internal blocks of the BM&P, including the digital logic. If the REGIN or VDD supplies are outside the nominal range, the IC's behavior can be unpredictable. To prevent this, the BM&P outputs these supplies to the MCU for monitoring. This allows the MCU, which is not supplied by any of these internal supplies, to monitor these signals, ensuring freedom from 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.

- 3V3 supplies the I/O ports. If this supply experiences a UV condition, there may not be a correct voltage level through any of the outputs (communications, GPIOs). To prevent this situation from occurring, the BM&P implements internal UV protection on the digital side after the 3V3 signal is sensed through the VADC. If a UV condition is detected, the BM&P opens the first protection layer.

- V_{REF} is the supply of the VADC, and a variation in this supply corrupts the converted digital values, leading the system misjudge the battery conditions. The failures related to V_{REF} are covered by SM11.2, SM7, SM8, and SM10.

SM11.2: BM&P's Analog-to-Digital Converter (ADC) Self-Test

The BM&P self-tests the VADC, which is the ADC used for voltage and temperature measurements, to detect possible malfunctions. The VADC 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 xALERT 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 pin low, which opens the first protection layer via the BM&P.

In addition, there is another test for the VADC commanded from the MCU to add more robustness to VADC and V_{REF} failure detection. This test consists of using GPIO2's value, which can be driven by the MCU, as an additional VADC test. In the MCU, the GPIO2 pin should be configured as an output; in the BM&P, GPIO2 should be configured as an input that can be read through the VADC (the GPIOs can be an input of VADC if they are configured this way). Then the MCU can set a 3.3V value (the value of the supply of the MCU) or 0V value (GND of the MCU) via GPIO2.

The MCU reads the converted value in the RD_VGPIO2 register. Then the MCU compares the values to the expected result. This method also tests the extreme values of the VADC. The MCU can perform this periodically during operation. Once a failure is detected, the MCU pulls the GPIO1 pin low, which opens the protection FETs.

To implement this feature, it is important that the BM&P's FET control mode is configured to "simple mode." In this mode, FET control can be accomplished through the MCU by just using GPIO1, then leaving GPIO2 free for the VADC test.

SM11.3: BM&P One-Time Programmable (OTP) Memory Cyclical Redundancy Check (CRC)

The BM&P implements an internal OTP memory to store some trimming and configuration values. Some of these values are critical for the correct functionality of the BM&P, and having corrupt data can lead to a violation of one or more safety functions. Because of this, the OTP memory implements a CRC that covers all the data stored internally.

The OTP includes some reserved memory to store the CRC values that should match the CRC calculations from the data stored in the OTP. Every start-up, the BM&P reads the OTP values, calculates the CRC values, and compares them to the values stored in the OTP. If there is a mismatch, the BM&P detects a failure, stays in a safe state, and does not start operation.

SM11.4: BM&P Drivers' Output Value Monitoring

The protection FETs are controlled by the drivers that are implemented as part of the BM&P. The drivers are the last link of the chain to open or close the transistors, and a failure in one of the drivers can lead to a violation of the safety functions.

To mitigate this issue, the BM&P implements an internal analog monitoring circuit to detect the actual status of the output drivers (CHG, DSG, and SBY FET drivers), which get stored in the following registers: CHG_DRV, DSG_DRV, and SBYDSG_DRV. The MCU reads these values and compares them to the commanded status of the drivers. If these values do not match, the MCU detects a failure in the output drivers and sets the nSHDN pin low, which resets the BM&P and opens the protection FETs. If the failure appears again after the BM&P is reset, this means that the failure is permanent and the MCU blows the SCP through the EXT_FUSE pin, and the system reaches a safe state.

SM12: Cell Mismatch

The BMS performs a cell voltage comparison with all the sensed cell voltages. If the voltage difference between the cell with the highest voltage and the cell with the lowest voltage exceeds CELL_MISMATCH_THRESHOLD, a mismatch failure is detected.

Once the failure is detected, the BM&P generates an interrupt through the GPIO3 pin. The interrupt is read by the MCU, which checks the CELL_MISMATCH_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.

This measure is useful because it detects cell voltage-sensing drifts and increases the coverage of SM7.

SM13: First Protection Layer Status Check

The MCU monitors the status of the first protection layer by monitoring the battery current (BATTERY_CURR) and the commanded status of the first protection layer.

If the first protection layer is commanded to be open and BATTERY_CURR ≠ 0A ± CURR_THRESHOLD, then a failure in the first protection layer occurs.

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

SM14: GPIO Verification

The BMS uses different interfaces between the BM&P and the MCU to control the first protection layer status from the MCU (GPIO1 and GPIO2) and to send safety-related interruptions to the MCU (GPIO3). These GPIOs must be verified to ensure their correct functionality during normal operation.

The MCU performs a start-up test in which the MCU commands the GPIOs high and low, and confirms that the BM&P is reading the same pattern internally.

For this purpose, the GPIOs in the BM&P should be configured as digital inputs and not connected to the output drivers, so that the test does not force the system to leave the safe state.

If the MCU detects that the BM&P is not reading the pattern sent through the GPIOs, the MCU detects a GPIO failure (either from the MCU side or BM&P side), and the BMS performs a reset. If the fault appears again after the reset, the BMS gets stuck in a safe state, and the MCU sends the status so that the user is aware of the system’s unavailability.

SM15: nSHDN Verification

The BM&P implements an nSHDN pin to trigger an internal reset commanded from the MCU. This reaction is used as part of some safety measures to reach a safe state. The nSHDN pin should be verified during start-up of the BMS.

The MCU should perform a start-up test in which the MCU commands the nSHDN pin high and low, and confirms that the BM&P is being reset.

If the MCU detects that the BM&P is not being reset, the MCU should not be allowed to start operation, and the system stays in a safe state.

SM16: MCU Self Diagnostics

The MCU should implement self-diagnostic measures to prevent malfunction of the main components. SM16 is comprised of the following:

- MCU CPU Test
- MCU Flash Test
- MCU RAM Test
- MCU Clock Monitor

The measures listed as part of SM16 are not defined in the document, as the responsibility falls on the customer side. The measures would cover the critical parts of the MCU (memories, CPU, and clock). The ADC does not need to be checked, as the implementation of SM7, SM8, and SM10 means that a failure in the ADC would be detected. I^2C communication is also protected with the implementation of SM5 and SM6.

SM16 represents the minimum requirements that should be considered for the MCU, alongside SM5, SM6, SM7, SM8, and SM10 for the intended functionality. If the system integrator (end customer of this BMS concept) is using other functionalities in the MCU that might violate the safety goal or interfere with the safety function, measures must be taken by the integrator to achieve the required diagnostic coverage.

SM17: BM&P Registers Readback

The MCU can configure the BM&P (e.g. enable protections, configure protection thresholds, and configure deglitch times for the protections) by modifying the values of certain registers through the I^2C. It is important to verify that the configuration written in the registers is the correct value, as it can impact one of the safety-related behaviors if an error occurs.

The MCU should perform a readback of the modified configuration registers and check that the written values are intended to be written. Every time the MCU modifies a register, a readback should be performed. The MCU should detect a BM&P register failure if, after three consecutive readback retries, the written values do not match with the intended values.

If a BM&P register failure is detected, the MCU sets the nSHDN pin low, which resets the BM&P and opens the first protection layer.

REFERENCE VALUES FOR DESCRIBED THRESHOLDS

Table 2 shows reference values for the previously described thresholds. This table is included to facilitate the interpretation of the thresholds and have a reference for the thresholds. However, the end customer is the responsible for setting their values according to the experience and the application of the BMS system.

Table 2: Reference Values

Threshold ID	Recommended Values
BATTERY_OV	*n* [1] x (V_{CELL_MAX} [2] - 100mV)
BATTERY_UV	*n* x (V_{CELL_MIN} [3] + 100mV)
CELL_OV	V_{CELL_MAX} - 50mV
CELL_UV	V_{CELL_MIN} + 50mV
BATTERY_CHG_OC	*m* x [4] x $I_{CELL\_CHG\_MAX}$ [5]
BATTERY_DSG_OC1	*m* x $I_{CELL\_DSG\_MAX}$ [6]
BATTERY_DSG_OC2	2 x *m* x $I_{CELL\_DSG\_MAX}$
BATTERY_CHG_SC	4 x *m* x $I_{CELL\_CHG\_MAX}$
BATTERY_DSG_SC	4 x *m* x $I_{CELL\_CHG\_MAX}$
BATTERY_CHG_OT	$T_{CELL\_CHG\_MAX}$ [7]
BATTERY_CHG_UT	$T_{CELL\_CHG\_MIN}$ [8]
BATTERY_DSG_OT	$T_{CELL\_DSG\_MAX}$ [7]
BATTERY_DSG_UT	$T_{CELL\_DSG\_MIN}$ [8]

Notes:

1) *n* represents the number of cells connected in series.
2) V_{CELL_MAX} represents the maximum cell voltage specified in the cell datasheet and/or according to the intended application.
3) V_{CELL_MIN} represents the minimum cell voltage specified in the cell datasheet and/or according to the intended application.
4) *m* represents the number of cells connected in parallel.
5) $I_{CELL\_CHG\_MAX}$ represents the maximum charge current specified in the cell datasheet and/or according to the intended application.
6) $I_{CELL\_DSG\_MAX}$ represents the maximum discharge current specified in the cell datasheet and/or according to the intended application.
7) $T_{CELL\_CHG\_MAX}$ and $T_{CELL\_DSG\_MAX}$ represent the maximum cell temperatures specified in the cell datasheet and/or according to the intended application for charging and discharging the cell.
8) $T_{CELL\_CHG\_MIN}$ and $T_{CELL\_DSG\_MIN}$ represent the minimum cell temperatures specified in the cell datasheet and/or according to the intended application for charging and discharging the cell.

CCF COMPLIANCE

The probability of two or more separate faults having a common cause should be taken into account for the subsystems of category 2, 3, and 4. To ensure that these situations are covered, sufficient measures against the common cause failure (CCF) should be carried out. Table 3 shows a list of measures against CCF with a corresponding score. The measures should be fully implemented to obtain the full score, if a non-zero score should be assumed. At the least, a 65 score should be achieved to demonstrate that there is a sufficient level of coverage against CCF.

Table 3: CCF Compliance

No.	Measure Against CCF	Score	Achieved? (Yes/No)	Rationale
1	Separation/ segregation	15	Yes [9]	The described architecture offers physical separation/segregation in the different redundant channels, in which safety functions up to category 3 are implemented. Nonetheless, the final customer should ensure a robust design process (complying with design rules in the PCB design such as the routing, clearance, and creepage distances), to ensure that there is no crosstalk or short-circuit between vias.
2	Diversity	20	No [9]	The logic devices used implement some degree of diversity as one is an ASIC (just HW) and the other device is an MCU (HW + SW). The outputs used use different technology (transistors and fuse). To claim full-scoring, some diversity should be ensured in the input devices as well.
3	Design/application/ experience	-	-	-
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature	15	Yes	The aim of this system is to cover all the situations mentioned in the statement. Over-pressure conditions are not applicable to this electronic system.
3.2	Components used are well-tried	5	No	The system implements complex ICs. This is not compatible with complying with well-tried principles.
4	Assessment/analysis	5	Yes [9]	Assessment done by TÜV, analysis such as FMEA. Further analysis to be performed by customer (e.g. FMEDA).
5	Training	5	Yes	Development performed by a team with experience in BMS and Functional Safety. In addition, a workshop of ISO13849 has been conducted and the development is assessed by TÜV ISO13849 experts.
6	Environmental	-	-	-
6.1	Prevention of EMI or impurity of fluidic medium	25	Yes [9]	Achievable, but the responsibility relies on the customer side to perform and pass EMI tests according to the applicable standards.
6.2	Other influences	10	Yes [9]	Achievable, but the responsibility relies on the customer side to perform and pass environmental tests (e.g. chemical, mechanical, temperature tests).
	Total	75	>65	Considering the previous topics, this BMS concept can potentially pass the CCF analysis, ensuring enough level of coverage against common cause failures. This total score can be achieved considering the final customer complies with all the topics mentioned in the notes of each one of the measures listed in the table.

Note:

9) To claim full-scoring, extra processes are required by the system integrator, as explained in the Rationale column.

CONCLUSION

There is an increasing importance regarding the safety implications of battery-powered applications, with a particular focus on BMS development according to the ISO 13849 standard. The BMS must implement safety measures to ensure robustness and risk reduction to an acceptable level, as described throughout this application note. This application note described 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	-
1.1	1/22/2025	Added "Concept" to title.	1
		Updated the Table of Contents.	
		Updated the Terms and Definitions section.	6
		• Added the Architecture section. • Added Figures 1, 2, and 3.	6–7
		Updated the Categories section.	7–8
		Added the sentence starting with "In addition, the safety measures…" to the Safety Functions section.	9
		Updated the BMS Architecture section: • Updated all paragraphs starting at, "The power supply architecture implemented…" • Added all paragraphs starting at, "The mechanism to…" • Updated Figure 1 to Figure 4.	10–11
		Added the BM&P Product Suitability section.	11
		Added the Assumptions of Use section.	12
		Updated the SM1: Battery Over-Voltage Protection (OVP) and Under-Voltage Protection (UVP) section with only two thresholds.	13
		• Updated the Implementation section. • Updated Figure 2 to Figure 5.	13–14
		Updated the SM2: Cell OVP and UVP section: • Updated with two thresholds instead of four. • Updated SM block diagram. • Updated Figure 3 to Figure 6.	14–15
		Updated the SM3: Battery Over-Current Protection (OCP) and Short-Circuit Protection section: • Updated SM block diagram. • Removed paragraph starting with, "In applications with up to 60A…" • Updated Figure 4 to Figure 7.	15–16
		Updated the SM4: Battery Over-Temperature Protection (OTP) and Under-Temperature Protection (UTP) section: • Differentiated between OT and UT thresholds in charge and discharge scenarios. • Removed paragraph starting with, "In applications with up to 60A…" • Updated Figure 5 to Figure 8.	16–17
		Updated the SM11: BM&P Self Diagnostics section: • Updated SM11.1, SM11.2, SM11.3, and SM11.4. • Removed SM11.5.	20–21
		Added the SM12: Cell Mismatch section.	21
		Added the SM13: First Protection Layer Status Check section.	22
		Added the SM14: GPIO Verification, SM15: nSHDN Verification, and SM16: MCU Self Diagnostics section.	22
		Added the SM17: BM&P Registers Readback section.	23

		Added the Reference Values for Described Thresholds section.	24
		Added the CCF Compliance section.	25–26

Notice: The information in this document is subject to change without notice. Users should warrant and guarantee that third-party Intellectual Property rights are not infringed upon when integrating MPS products into any application. MPS will not assume any legal responsibility for any said applications.