Manual

Functional Safety in Battery Management Systems Featuring Renesas Battery Front Ends

This manual covers several recommended usage and mechanisms of Renesas Battery Front Ends (BFEs) to feature functional safety in Battery Management Systems (BMSs). It offers guidelines to BMS designers for the operation of safety-related features of Renesas BFEs, and implementation of architecture patterns that cover the safety goals defined for BMS safety functions to meet safety standards such as ISO 13849, IEC 61508, and UL 60730-1 (IEC 60730).

Restrictions

Deploying the methods and implementations explained in this article does not guarantee the achievement of the safety level defined for the design. The final level assessment depends on the particularities of the design and the application, the documentation and justification of the applied methods, and the process before the certification authority. Renesas assumes no responsibility for guaranteeing the system achieves its safety goals.

Scope

This manual provides support for fulfilling standards such as ISO 13849, IEC 61508, and UL 60730-1 (IEC 60730). It describes the use of the Renesas BFEs features and the necessary and recommended operations provided by a host microcontroller to meet the fault coverage defined for a BMS. The operation of all external components, including the microcontroller, is expected to operate without error.

Renesas Electronics does not take any responsibility that the required safety performance is reached on the system level, which strictly depends on the system configuration used. The aim of this document is to provide supplemental information for the assumed software (SW) and system solutions to assist the compliance of safety standards in system integration.

The following sub-sections provide information and discussion about the device and application and examine the safety mechanisms of some BFEs.

In this document, Renesas Electronics provides only a judgment on suitability of the hardware (HW) or SW concepts but does not provide any suggestion about actual implementation or the test frequency.

Contents

1. Target System Architecture

Figure 1 shows the target BMS architecture this manual references. It consists of a Battery Front End (BFE) supervised by a Microcontroller Unit (MCU). The MCU oversees BFE functionalities and communicates with the BFE through intra-chip/inter-chip communication interfaces such as Serial Peripheral Interface (SPI) or Inter-Integrated Circuit (I^2C). The BFE monitors the battery pack status and its operating environment measuring pack parameters, typically cell voltage, temperature, and load current. Combined, MCU and BFE have the primary task of ensuring the safe operation of the battery pack.

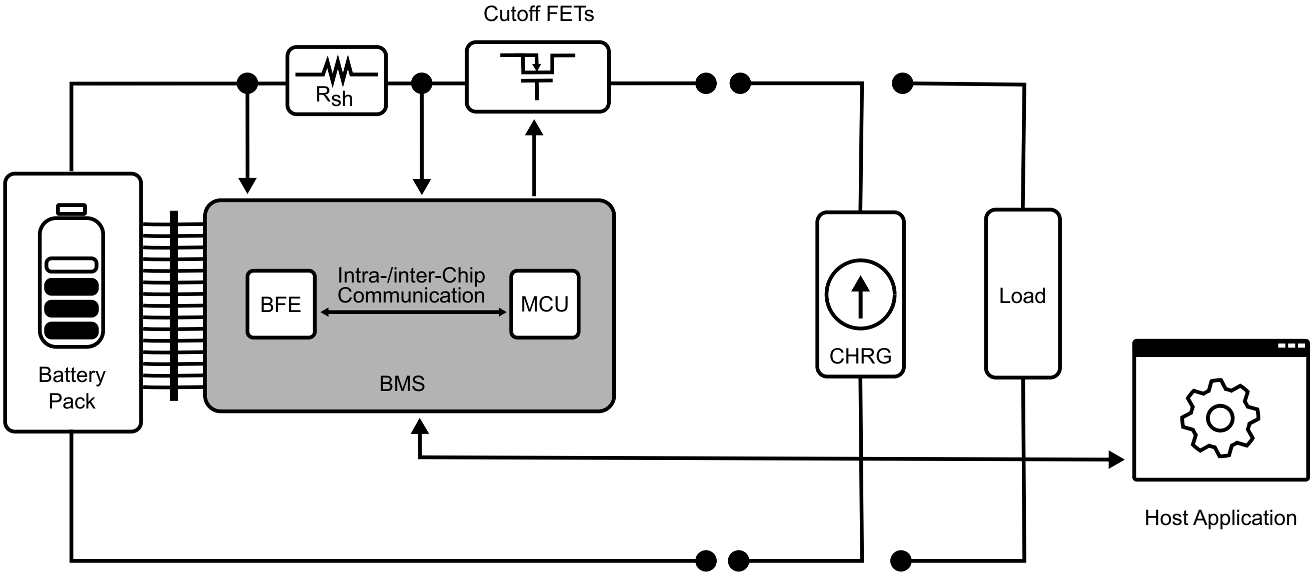

Figure 1. Commonly used Architecture of a Battery Management System

In battery-powered devices, events such as overvoltage/undervoltage (OV, UV), over-temperature (OT), and overcurrent (OC) can result in fire and explosion if the cells of the battery pack are incorrectly managed or not at all. To avoid these hazards, the BMS senses and monitors voltage, current, and temperature values to verify they are within the safety operational thresholds specified by the manufacturer. It also executes countermeasures if the pack is operating out of them.

1.1 Safety Functions of Battery Management Systems

A safety function is the function of a part whose failure can result in an immediate increase in risk[1]. In BMSs, the functions designated to monitor OV, UV, OT, and OC events are considered safety functions because the loss of such functionalities can derive in hazardous situations. Communication is also a safety function because a failing or unreliable communication interface leads to incorrect management procedures and the potential occurrence of hazards.

Figure 2 depicts the general functional blocks of a BFE involved in the execution the BMS safety functions. Table 1 defines the functional safety requirements for the BMS and specifies which blocks are required to execute them. Use the diagram and table to obtain the BFE failure rates, failure modes, and diagnostic capability in a Failure Modes, Effects, and Diagnostic Analysis (FMEDA).

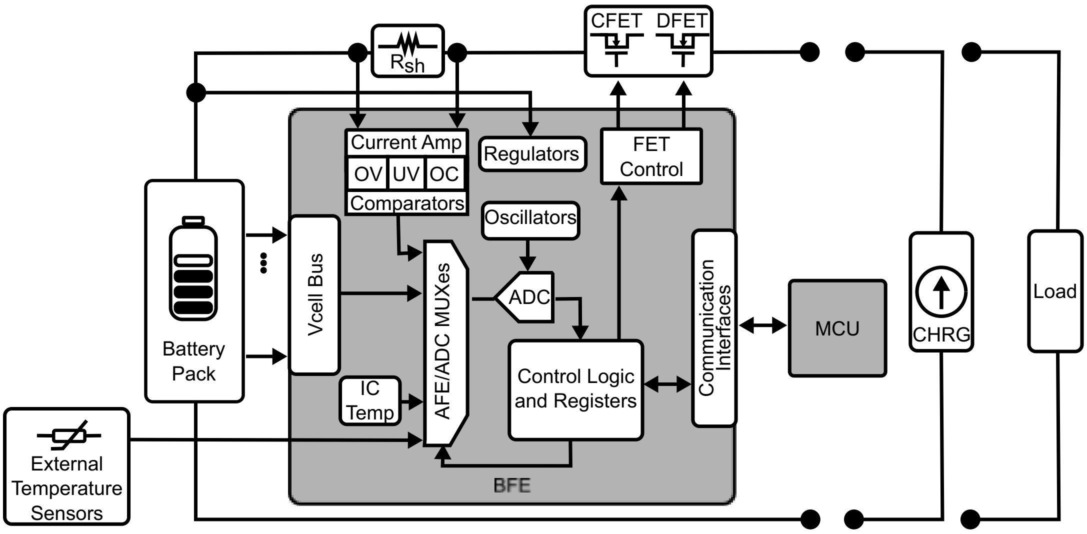

Figure 2. General Block Diagram of Battery Management Systems (BMSs)

Table 1. Functional Safety Requirements

Functional Safety Requirement		AFE-ADC MUX	ADC	Communication Interfaces	Cell Voltage, Regulators	Temperature	Oscillators	FET Control	Control Logic and registers	Current Amp
FSR01	The BMS detects overvoltage and report to the MCU	X	X	X	X		X		X	
FSR02	The BMS measures cell voltages and report to the MCU	X	X	X	X		X		X	
FSR03	The BMS detects over-temperature condition and report to the MCU	X	X	X		X	X		X	
FSR04	The BMS detects undervoltage and report to the MCU	X	X	X	X		X		X	
FSR05	The BMS is able to detect overcurrent and report to the MCU	X	X			X			X	X
FSR06	The BMS is able to generate a control signal to isolate the battery pack							X	X	

The following section summarizes some terms and definitions that are relevant to assess the safety level of BMS safety functions.

2. Functional Safety Terms and Definitions

The following terms and definitions are part of the formal language and context used in ISO 13849-1 to assessing the safety level of a system or sub-system. For a complete description of the safety-related vocabulary, see the ISO 13849 standard.[1]

2.1 Performance Level

The Performance Level (PL) indicates the ability of a system to perform a safety function under foreseeable conditions.[1] ISO 13849-1 defines five PLs in terms of the Probability of dangerous Failure per Hour (PFH_D), indicating how much risk reduction can be provided by the SRP/CS. The standard defines five PL = [a, b, c, d, e] according to the PFH_D determined for a system. In this scale, when PL = a, the lowest risk reduction is provided, whereas when PL = e, the highest is provided.

2.2 Required Performance Level

The required performance level (PLr)[1] is the PL at which the BMS achieves the risk reduction required by the safety objectives of the design. The greater the amount of risk reduction required, the higher the PL is.

2.3 Dangerous Failure

A dangerous failure is a failure that can potentially put the system in a state that exposes a person to a source of harm. In BMS, failures that convey the inability to execute properly their safety functions can expose users to events such as fire or explosion, so they are considered dangerous failures. The probability of dangerous failure depends on several factors of the BMS design, including hardware and software structure, fault detection mechanisms, reliability of the components, design process, operating stress, environmental conditions, and operation procedures.[1]

2.4 Mean Time To Dangerous Failure

Hardware components such as BMS and BFE have a probability of failure per unit time called component failure rate. The failure rate, a value usually given by component manufacturers, is denoted with the symbol λ and is usually indicated in Failures in time (FIT). A failure rate of 1 FIT is defined as the failure rate that occurs during one billion device hours, so

(EQ. 1)
$$\lambda = 1\ \text{FIT} = 10^{-9}\frac{\text{Failure}}{\text{hour}}$$

During the useful life period of a device, the Mean Time To Failure is calculated using Equation 2:

(EQ. 2)
$$\text{MTTF} = \frac{1}{\lambda}[\text{hours}]$$

The failure rate is distributed among the failure modes of the component under evaluation. Only the fraction of failure rate that have dangerous effects, denoted as λ_D, should be considered to calculate the Mean Time To Dangerous Rate ($MTTR_D$). If the manufacturer specifies explicitly the dangerous failure rate of the component, the Mean Time To Dangerous Failure ($MTTF_D$) can be calculated using the Equation 2. However, for complex components such BMS and BFEs that may have several failure modes, it is convenient to consider the worst-case scenario in which any failure leads to the loss of capacity to execute the safety function. Therefore, the $MTTF_D$ is calculated using Equation 3:

(EQ. 3)
$$\text{MTTF}_D = \frac{1}{\lambda_D} = \frac{1}{\lambda}[\text{hours}]$$

ISO 13849-1 defines three discrete levels to denote the $MTTF_D$. Table 4 in ISO 13849-1 shows the ranges of $MTTF_D$ defined for Low, Medium, and High levels.

2.5 Diagnostic Coverage

Diagnostic Coverage (DC) measures the ability to detect dangerous failures and handle them automatically. It is determined as the ratio between the failure rate of detected and handled dangerous failures denoted by $\lambda_{DD,}$ and the failure rate of total dangerous failures λ_D (detected and undetected) The DC is expressed in percentage as:

(EQ. 4) $$DC = \frac{\lambda_{DD}}{\lambda_D} \times 100\%$$

Table 5 in ISO 13849-1 defines four levels according to the calculated DC: None, low, medium, and high.

2.6 Common Cause Failure

A Common Cause Failure (CCF) is a failure with the potential of affecting or disabling the function provided by two different components of a system. For example, electromagnetic interference, out-of-operational-range temperatures, and power shortage can affect or disable both undervoltage and overvoltage detectors in BMS even if its architecture includes redundant functional blocks.

2.7 Architecture Patterns

The architecture determines BMS tolerance against failures. Architectures patterns are abstractions that aim at enhancing fail-safe and fail-operational properties while simplifying and standardizing the design process.[2] Most of the architectures implementations in systems like BMSs are based on three architecture patterns: single-channel untested, single-channel tested, and redundant tested architectures.[3] In ISO 13849-1, patterns are referred to as Designated Architectures and each one characterized by the resistance to faults and the behavior of system when a failure occurs. The three base architectures, their characteristics, and the correspondence with ISO 13849-1 categories are described in the following sections.

2.7.1 Single-Channel Untested Architecture

Figure 3 shows the functional view of a single-channel architecture[2], which corresponds to Category B and 1 in ISO 13849-1. This architecture is composed of a primary channel that executes the safety function implementing three basic blocks: input processing, data processing, and output processing. In BMSs, inputs are the measured physical variables (Voltage, Current, Temperature), and the communication commands between the BFE and the MCU. The input processing function converts the input data to useful information. It corresponds to the BFE functional blocks that acquire and condition voltage, current, and temperature inputs, such as V_{CELL} bus, current amplifier, comparators, multiplexers, IC for internal temperature, ADC and communication interfaces. The data processing function analyzes the processed inputs and determine the actions to take. This block corresponds to registers and control logic blocks in the BMS architecture. The output processing unit translates the control signals generated by the processing unit to outputs. Outputs may include signals to drive external modules such as cutting FETs, alerts to notify the MCU or the application of a fault condition, and response to commands received from the MCU over communication interfaces.

There is no hardware tolerance in single-channel untested architecture, so any dangerous failure leads to loss of the safety function. Its safety relies on the selection of components that meet the operational conditions with high $MTTR_D$. Safety functions implemented with this architecture do not offer DC, so the analysis of CCF is not relevant.

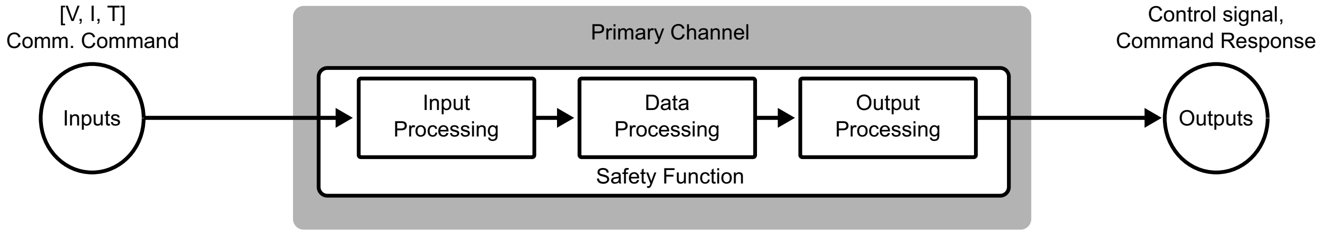

Figure 3. Single-Channel Architecture

2.7.2 Single-Channel Tested Architecture

Figure 4 depicts the single channel tested architecture, which corresponds to Category 2 in ISO 13849-1. The test mechanism can be performed on any demand of the safety function, or periodically as part of a system diagnostic routine to detect loss of the functionality. It either allows normal operation if no fault is detected or generates an output signal that sets a safe state until the fault is cleared. The time to detect the fault and set the system to a safe state must be shorter than the Fault Tolerant Interval (FTI). The output of the test block may include alert signals that notify the MCU of any failures in the safety function, and/or automatic measures that set the battery pack to a safe state, which usually is the isolation of the battery pack from the load and/or charger.

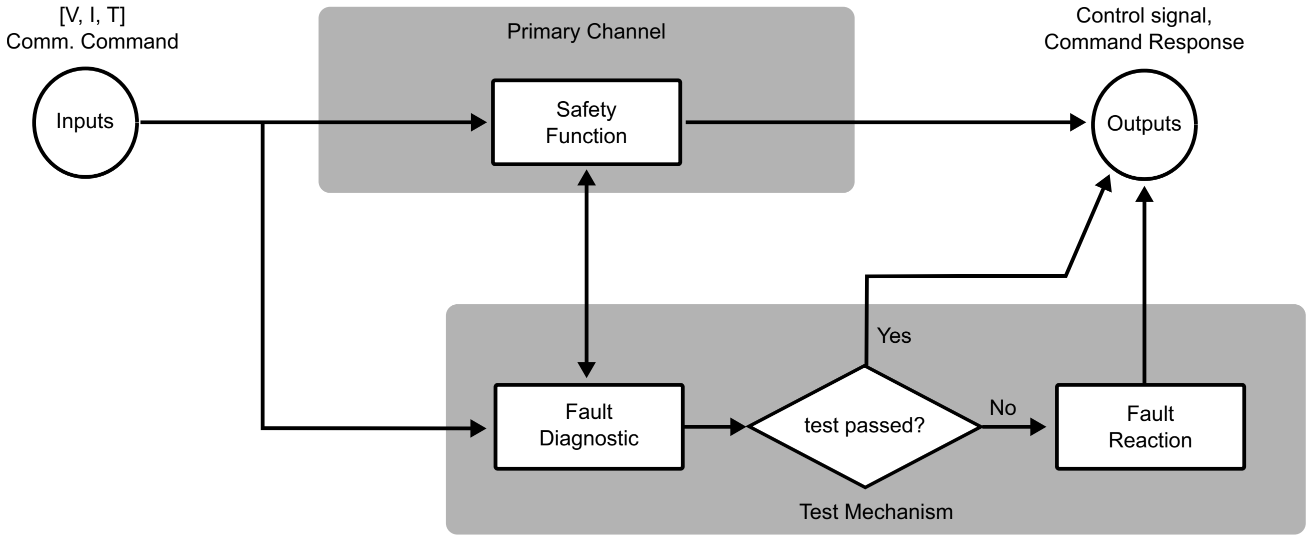

Figure 4. Single-Channel Tested Architecture

2.7.3 Redundant Tested Architecture

Figure 5 shows a general functional diagram of redundant architectures. This pattern corresponds to Category 3 and 4 in ISO 13849 and can be of two types of redundancy: homogeneous or heterogeneous. Homogeneous redundancy improves safety by copying the primary channel and switching between the two (or more) copies in case of a failure in one of them. Heterogeneous redundancy has the same logic with the addition that each channel is developed independently.[2]

Redundant architectures are single fault (or one less than the number of channels) tolerant architectures with high quality diagnostics, but measures against CCF must be applied to avoid loss of the safety function.

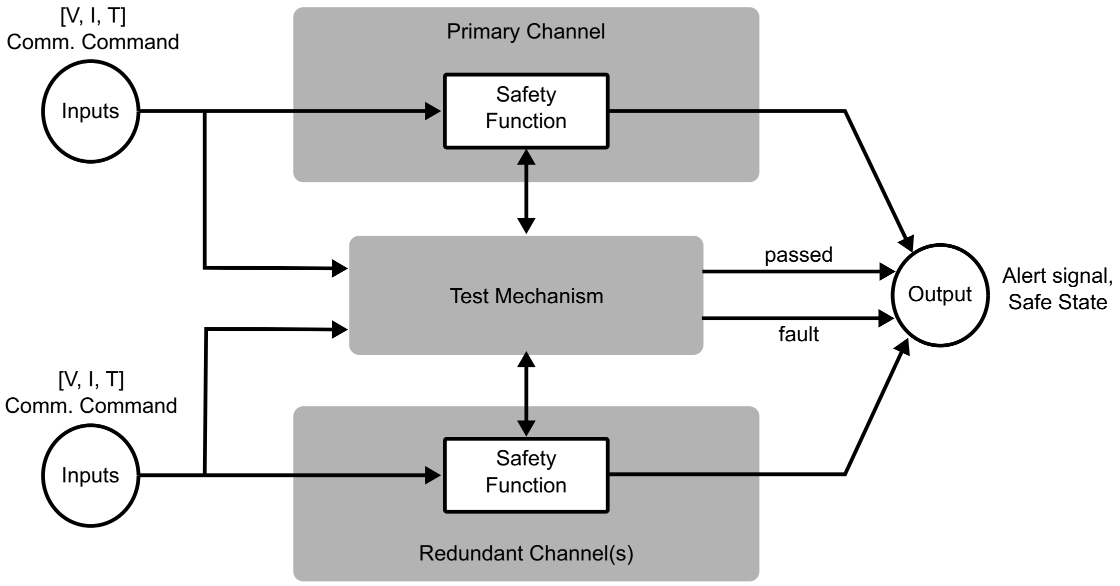

Figure 5. Redundant Architecture with Test Capability

3. Implementation of Architecture Patterns Featuring Renesas BFEs

During the design of a BMS, the designer must define its safety requirements and determine the architecture to achieve the safety level defined for BMS safety functions. The following sections exemplify this procedure, defining the safety requirements for BMS safety function and showing how to implement architecture patterns in an MCU-supervised BMS featuring Renesas BFEs.

3.1 Safety Goals

Table 2 defines the safety goals for BMS safety functions. The safety level of each requirement is defined in terms of Performance Level (PL) (ISO 13849). An approximate equivalence of the specified PL in terms of Class (IEC 60730), and Safety Integrity Level (SIL) (IEC 61508) are given for reference.

Table 2. Safety Requirements

Safety Requirements		Remarks	Safe State	PL (ISO 13849)	Class (IEC 60730)	SIL (IEC 61508)	Functional Safety Requirement					
							FSR01	FSR02	FSR03	FSR04	FSR05	FSR06
SR01	The BMS prevents overcharging (overvoltage) of battery	Avoids thermal events.	Isolate the battery pack from charging	D	B	2	X	X				X
SR02	The BMS communicates the correct battery parameters	The application uses this information to judge an imminent loss of voltage and warn the user. Maintains application operation or comes to a safe stop.	Isolate the battery pack from charging and discharging	D	B	2	X	X	X	X	X	X
SR03	The BMS always detects and reports over-temperature in the battery cells	Reports over-temperature to the application, which can then warn the user. The BMS also opens the drivers controlling pass of the current.	Isolate battery pack from charging and discharging	D	B	2				X		X
SR04	The BMS prevents over discharge of the battery	Discharging cells at high rates when the cell voltage is under manufacturer specifications can lead to a thermal event.	Isolate the battery pack from discharging	D	B	2		X		X		X
SR05	The BMS always detects and reports overcurrent in the battery pack	High discharging or charging rates can lead to a thermal event.	Isolate the battery pack from charging and discharging	D	B	2		X		X		X

3.2 Safety Mechanisms

Table 3 summarizes fault diagnostic functions that can be implemented using these Renesas BFEs:

- RAA489220 – 10-cell BFE and protector
- RAA489206 – 16-cell BFE
- RAA489204 – 14-cell stackable BFE

The selection of this BFEs intends to illustrate the deployment of BFE to provide functional safety for three different kinds of applications. The RAA489220 targets low to medium voltage applications such as power tools and hand-held electronics. The RAA489206 can be deployed in higher voltage applications such as light electric vehicles (e-bikes, e-scooters, and e-motorcycles), cordless gardening tools, home appliances, telecom and server farms, and energy storage systems. The RAA489204 is an industrial grade BFE intended for applications with stackable battery packs, such as high-capacity backup batteries, energy storage systems and portable equipment. For further information about these and other BFE ICs, visit our BFE family page.

Table 3. Safety Mechanism Summary

Block	Description	Architecture Pattern		
		Single-Channel Untested	Single-Channel Tested	Redundant
Cell/Pack Voltage Readings	SM1: Cell/Pack Overvoltage Detection		•	•
	SM2: Cell/Pack Undervoltage Detection		•	•
	SM3: V_{PACK} Compare	•	•	
Temperature	SM4: Internal Over-Temperature Detection		•	•
	SM5: External Input Over-Temperature Detection		•	•
Current	SM6: Discharge Overcurrent Detection			•
	SM7: Charge Overcurrent Detection			•
	SM8: Discharge Short-Circuit Detection	•		
Communications	SM9: Communication CRC		•	
	SM 10: Communication Timeout	•		
	SM 11: Communications Watchdog		•	

3.3 Scan All Command

All safety mechanisms are tied to the Scan All command, featured by Renesas BFEs in their command set. The Scan All command is the best option the BMS can use, because it performs the most operations within the least amount of time command. The execution of the Scan All command is different in each BFE, but the most common behavior is that, when received, the BFE performs a series of tests to:

- Measure current (available in the RAA4890206)
- Check for overcurrent conditions (available in the RAA489206)
- Measure cell voltages
- Measure the V_{BAT} voltage
- Check for Overvoltage and Undervoltage conditions
- Measure the internal and external temperatures
- Check for over-temperature conditions
- Other tests such as check of open wire on cell inputs, V_{BAT} and VSS may be performed, but are out of the scope of this manual

In some BFEs such as the RAA489202, the fault condition checked during the execution sequence of the command may be subject to filtering operations. Fault counting filtering, for example, sets the fault bit indicator when a specified number of consecutive thresholds violations are measure. In BFEs such as the RAA489206 and RAA489220, such filtering is only active when the device operates in Continuous Scan Mode and is bypassed when the Scan All command is performed. Other filtering operations are sample averaging and fault duration filtering, which uses timers to filter out fault conditions that do not exceed a specified duration time.

Table 4 overviews the implementation of the Scan All command in the three Renesas BFEs discussed in this manual. For further details on the use of the Scan All command, the sequence tests are executed, and the time they take, check the datasheet of the selected BFE.

Table 4. Scan All Command Implementation in some Renesas BFEs

Step	Description	BFE		
		RAA489220	**RAA489206**	**RAA489204**
1	Select measurements	Set the Measurement Selection (0x41.[4:0]) to Single System Scan	Set the V_{CELL} EN (0x02.7) Set the V_{BAT} EN (0x1F.7) Set the I_{PACK} EN (0x03.7) Set the I_{TEMP} EN (0x1F.6) Set the ETAUX EN (0x11.[7:6]) to 11 Set the Scan Select (0x01.1)	Send the Scan All command (0xC5)
2	Prepare Trigger	Clear the Trigger Measurement bit (0x41.7)	Clear the System Trigger (0x01.0)	
3	Trigger Measurements	Set the Trigger Measurement bit (0x41.7)	Set the System Trigger (0x01.0)	

3.4 Implementation of Safety Mechanisms

This section details the implementation of Safety Mechanisms in accordance with the architecture patterns previously described. It provides general recommended usage of BFEs features to implement BMS safety functions. Detailed information about registers, commands and MCU-BFE interactions, can be found in the datasheet and user manual of the selected BFE.

Flow diagrams are used to describe the suggested implementations. Figure 6 shows the convention used to group functionalities, indicate the executing unit, and specify BMS inputs and outputs.

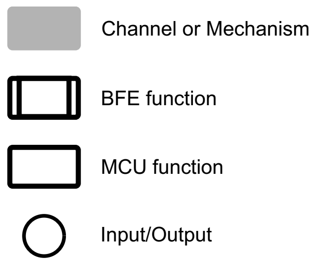

Figure 6. Convention used in Flow Diagrams to Describe Safety Mechanism Implementations

3.4.1 SM1: Cell/Pack Overvoltage Detection

The BMS detects overvoltage on cell inputs when at least one of the measured cell voltage is above the user-programmed threshold $V_{CELL}OV_{th}$. The BMS detects overvoltage on the pack input when the measured pack voltage is above the user-programmed threshold $V_{PACK}OV_{th}$.

3.4.1.1 Implementation Description

An OV fault is generated whenever the threshold specified by $V_{CELL}OV_{th}$ or $V_{PACK}OV_{th}$ threshold register(s) is exceeded.

3.4.1.2 Recommended Usage

Figure 7 shows the implementation of the single-channel architecture for OV detection. Figure 8 shows the redundant tested architecture for the same SM. In both implementations, the MCU can set either a unique flag to indicate OV detection on V_{PACK} or V_{CELL} inputs, or two individual flags to indicate the presence of each event.

Conversely, the test mechanism shall individually test V_{CELL} and V_{PACK} OV detection. Table 5 details the steps recommended to implement the functional blocks of both architectures.

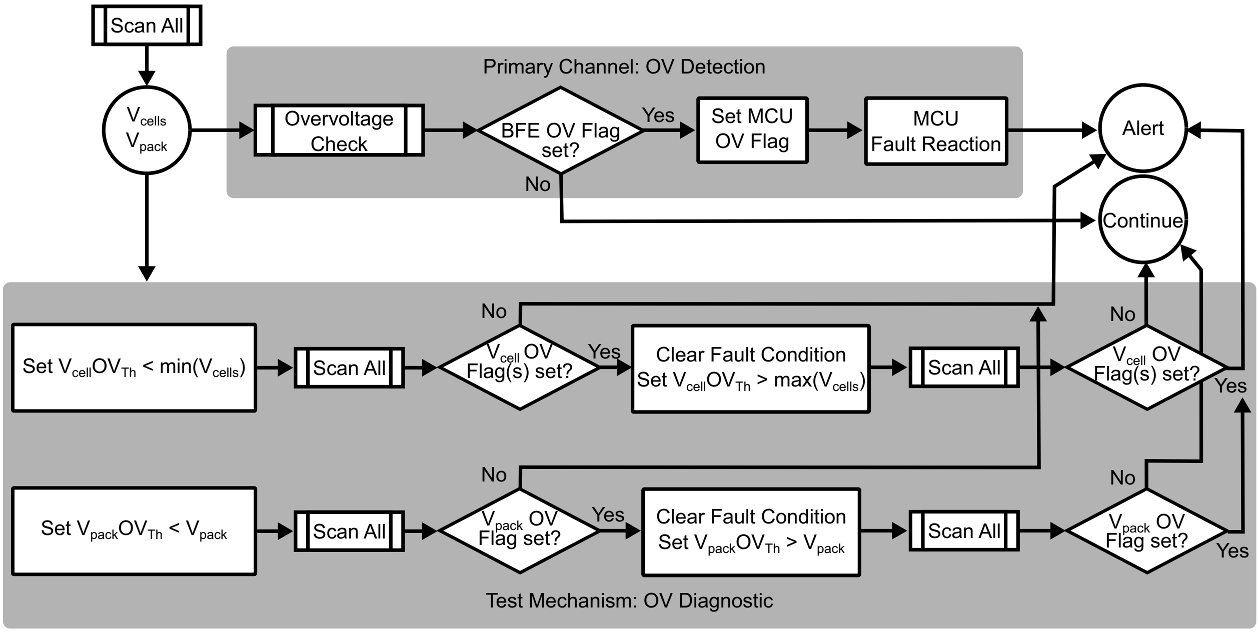
Scan All
V_{cells}
V_{pack}
Primary Channel: OV Detection
Overvoltage Check
BFE OV Flag set?
Yes
No
Set MCU OV Flag
MCU Fault Reaction
Alert
Continue
Set $V_{cell}OV_{Th}$ < min(V_{cells})
Scan All
V_{cell} OV Flag(s) set?
Clear Fault Condition Set $V_{cell}OV_{Th}$ > max(V_{cells})
Set $V_{pack}OV_{Th}$ < V_{pack}
V_{pack} OV Flag set?
Clear Fault Condition Set $V_{pack}OV_{Th}$ > V_{pack}
Test Mechanism: OV Diagnostic

Figure 7. Single-Channel Tested Implementation of Overvoltage (OV) Detection

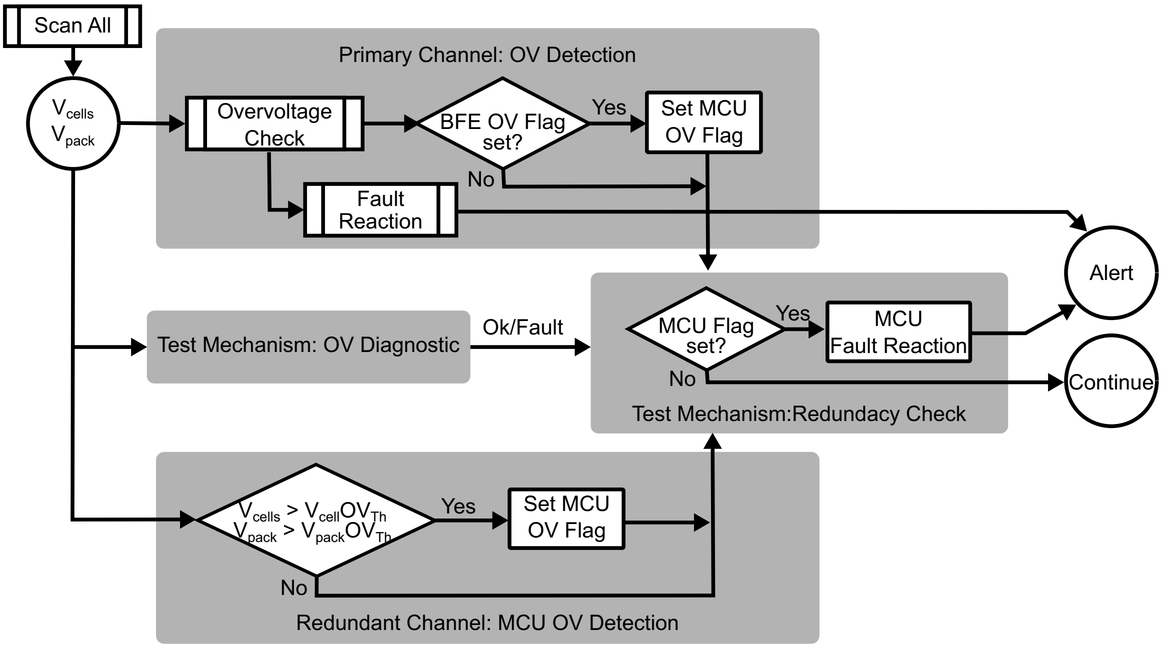
Scan All
V_{cells}
V_{pack}
Primary Channel: OV Detection
Overvoltage Check
BFE OV Flag set?
Yes
No
Set MCU OV Flag
Fault Reaction
Alert
Test Mechanism: OV Diagnostic
Ok/Fault
MCU Flag set?
MCU Fault Reaction
Continue
Test Mechanism:Redundacy Check
V_{cells} > $V_{cell}OV_{Th}$
V_{pack} > $V_{pack}OV_{Th}$
Set MCU OV Flag
Redundant Channel: MCU OV Detection

Figure 8. Redundant Tested Implementation of Overvoltage (OV) Detection

Table 5. SM1 Overvoltage Detection

Step	Operation	Description	RAA489220	RAA489206	RAA489204
Primary Channel: OV detection by BFE condition check and MCU fault reaction function					
1	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		

Table 5. SM1 Overvoltage Detection (Cont.)

Step	Operation	Description	RAA489220	RAA489206	RAA489204
2	Overvoltage Check	The BFE compares the value of each cell voltage/V_{PACK} with the value stored in the corresponding OV threshold register and sets internal OV flag(s) after applying supported/configured filtering.	V_{CELL} thresholds: OV (0x81.[15:9]) OV lockout (0x81.[3:0]). V_{PACK} OV check not supported.	V_{CELL} OV (0x06) V_{PACK} OV check supported as OV_{VBAT1} (0x20)	Cell OV_{TH} (0x87) V_{PACK} OV check not supported.
3	Read BFE OV Flag	The MCU checks proactively or triggered by the BFE (such as assertion of a pin connected to an MCU IRQ-enabled pin) the BFE register(s) that indicates the presence of OV Fault in at least one cell/V_{PACK}.	OVF (0x10.6) LOF (0x10.11) ALERT pin asserted when a fault is detected.	V_{CELL} OVF (0x63.0) V_{PACK} OVF (0x65.7). Clear OVF MASK (0x83.0) and/or VBOVF MASK (0x85.7) to enable ALERT pin assertion	OV fault (0x80.5) OV cells (0x81). Clear OV mask (0x8A.5) to enable FAULT pin assertion
4	Set OV Fault	MCU Implementation	If the OV Flag is set, the MCU sets an internal flag and starts fault reaction functions.		
5	MCU Fault Reaction	The MCU starts fault reaction functions to isolate the battery pack from the load. These functions may include: turn cutoff FETs off, blow a fuse, and force the charge pump to off state.	Shuts off power FETs clearing LDFET En (0x40.1) and/or LCFET En (0x40.0).	Shuts off power FETs clearing DFET EN (0x24.1) and/or CFET EN (0x24.0)	No power FETs control supported. External isolation driver required
Test Mechanism: Fault/Non-Fault Condition Induction					
1	Set OV_{TH} to force fault detection	The MCU reads V_{CELLS} /V_{PACK} and sets the corresponding OV thresholds below the minimum cell voltage and V_{PACK}.	V_{CELL} OV threshold (0x81.[15:9]) and V_{CELL} OVL (0x81.[3:0] to Cell Min (0x02).	V_{CELLS} (0x31-0x4F) Set V_{CELL} OV threshold (0x06) to min (V_{CELLS}). V_{BAT} (0x5C-0x5D) Set OV_{BAT1} Threshold (0x20) below V_{BAT1}	V_{CELLS} (0x41-0x4E). Set OV limit (0x87) to min (V_{CELLS})
2	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
3	Read BFE OV Flag	The MCU reads the BFE flag, which should be set indicating V_{CELL}/V_{PACK} OV fault. If it is not set, the MCU outputs an Alert indicating failure of the OV detection and starts fault reactions.	Step 3 and 5 (in case of failure) of Primary Channel		
4	Clear fault and set OV_{th} to force no fault detection	The MCU executes a command to clear the fault condition in the BFE and sets the OV threshold above the maximum cell voltage/V_{PACK}.	Set Clear All Faults Bit (0x40.6). Cell Max (0x01) V_{CELL}OV threshold (0x81.[15:9]).	Set Clear All Faults Bit (0x02.1).	Clear OV Fault Register (0x81). Clear TOT[2:0] (0x86[6:4]).
5	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		

Table 5. SM1 Overvoltage Detection (Cont.)

Step	Operation	Description	RAA489220	RAA489206	RAA489204
6	Read BFE OV Flag	The MCU reads the BFE flag, which should be clear indicating no V_{CELL}/V_{PACK} OV fault. If it is set, the MCU outputs an Alert indicating failure of the OV detection and starts fault reactions.	Step 3 and 5 (in case of failure) of Primary Channel		
Redundant Channel: MCU Verification of OV Condition and BFE Fault Reaction					
1	Primary Channel: BFE Detection and Fault Reaction	The BFE checks the OV condition. If the OV fault is detected, the BFE initiates autonomously fault reactions to isolate the battery pack, and outputs an alert. Fault reactions may include turning off cut-off FETs and/or blowing up a fuse. BFE fault reactions ensure battery isolation in case of MCU failures.	Automatic fuse blow by clearing HVGPIO Mask (0x11.14). BFE FETs control in AutoScan mode. Transition to LP mode (safe state) after finishing system scan. ALERT pin assertion on fault detection	Automatic FETs control: set CELL CON (0x24.4) and/or V_{BAT1} CON (0x24.3). Clear OVF MASK (0x83.0) and/or VBOVF MASK (0x85.7) to enable ALERT pin assertion	No automatic fault reaction to isolate the battery pack(s). Fault pin asserted to indicate the presence of fault condition in at least one of the monitored packs.
2	Redundant Channel: MCU OV Detection	The MCU reads cells voltages/V_{PACK} and checks if all cell voltages/V_{PACK} are (is) below the OV threshold stored in the MCU.	Execute the command code Read Measurements (0xC1)	Execute the command code Measurement (0x9B)	Read Cell/Pack Voltage Registers (0x41 – 0x50).
3	Redundancy Check	MCU Implementation	The MCU checks its OV flag. If it is set, the MCU initiates fault functions such as sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state. The MCU outputs an alert to notify the application.		

3.4.1.3 Comments

The redundant channel implementation is susceptible to CCF such as ADC and Multiplexer failures. Mechanisms to tests those units (included in some BFEs) are necessary. Other countermeasures may include looping of the test block to test OV condition in each cell, and implementation of averaging, totalizer counts, and time series analysis in the MCU. For V_{PACK}, it is possible to implement a redundant architecture against the ADC CCF by adding conditioning hardware that enables the MCU to use its ADC to measure V_{PACK}, and then compare the value with the programmed OV threshold.

3.4.2 SM2: Cell/Pack Undervoltage Detection

The BMS detects undervoltage on cell inputs when at least one of the measured cell voltage is below the user-programmed threshold $V_{CELL}UV_{th}$. The BMS detects undervoltage on pack input when the measured pack voltage is below the user-programmed threshold $V_{PACK}UV_{th}$.

3.4.2.1 Implementation Description

An UV fault is generated whenever the threshold specified by $V_{CELL}UV_{th}$ or $V_{PACK}UV_{th}$ threshold register(s) is exceeded.

3.4.2.2 Recommended usage

Figure 9 shows the implementation of the single-channel for UV detection. Figure 10 shows the redundant tested architecture for the same SM. In both implementations, the MCU can set either a unique flag to indicate UV detection on V_{PACK} or V_{CELL} inputs, or two individual flags to indicate the presence of each event. Conversely, the test mechanism shall individually test V_{CELL} and V_{PACK} UV detection. Table 6 details the steps recommended to implement the functional blocks of both architectures.

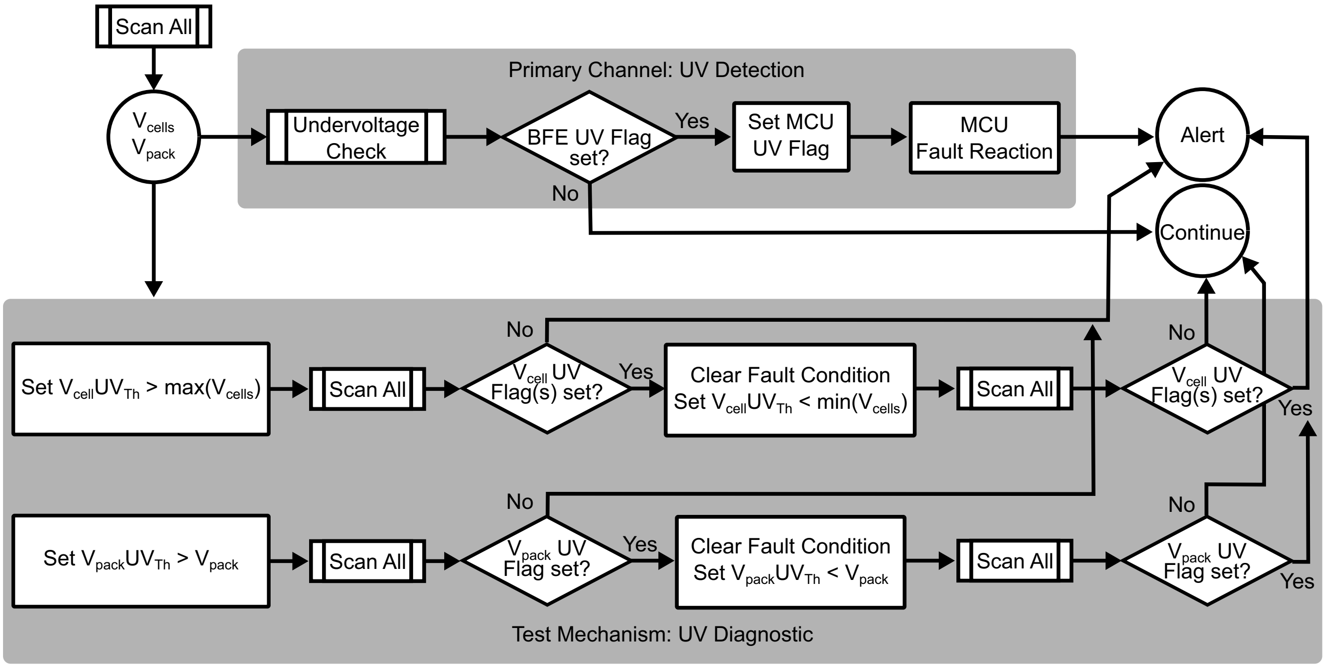

Figure 9. Single-Channel Tested Implementation of Undervoltage Detection

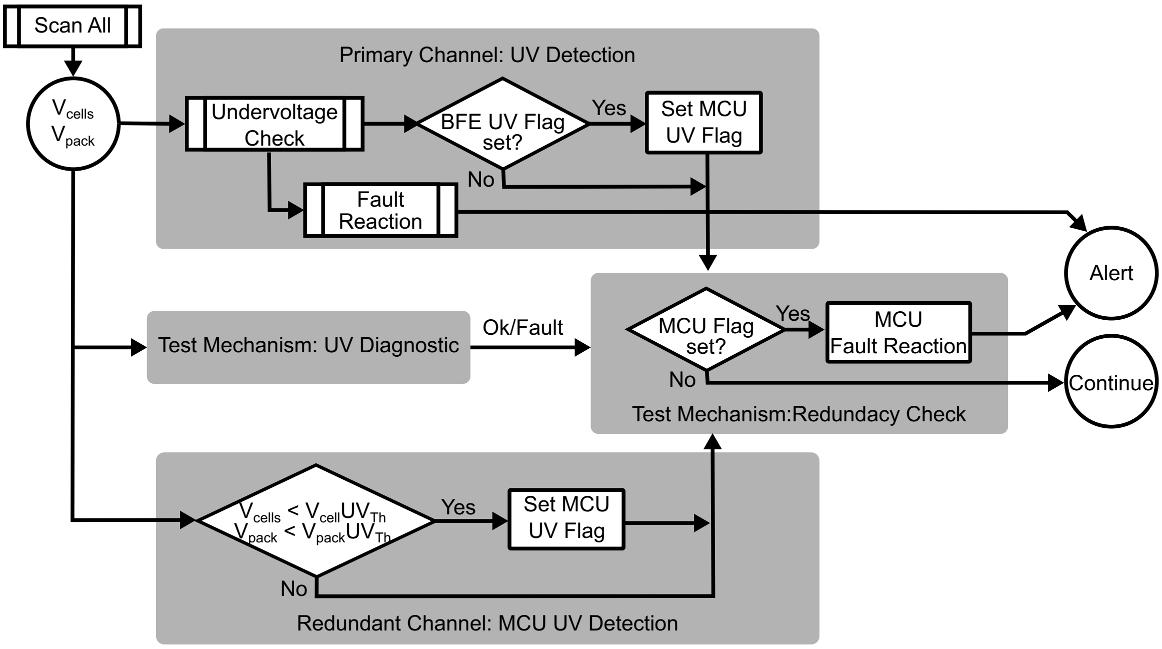

Figure 10. Redundant tested Implementation of Undervoltage Detection

Table 6. SM2 Undervoltage Detection

Step	Operation	Description	RAA489220	RAA489206	RAA489204
Primary Channel: UV Detection by BFE Condition Check and MCU Fault Reaction Function					
1	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
2	Under Voltage Check	The BFE compares the value of each cell voltage/V_{PACK} with the value stored in the corresponding UV threshold register and sets internal UV flag(s) after applying supported/configured filtering.	V_{CELL} thresholds: UV (0x82.[11:8]) UV lockout (0x82.[3:0]). V_{PACK} UV check not supported.	V_{CELL} UV (0x07) V_{PACK} UV check supported as UV_{VBAT1} (0x21)	Cell UV_{TH} (0x88) V_{PACK} UV check not supported.
3	Read BFE UV Flag	The MCU checks proactively or triggered by the BFE (such as assertion of a pin connected to an MCU IRQ-enabled pin) the BFE register(s) that indicates the presence of UV Fault in at least one cell/V_{PACK}.	UVF (0x10.5) LOF (0x10.11), ALERT pin asserted on a fault detection.	V_{CELL} UVF (0x63.1) V_{PACK} UVF (0x65.6). Clear UVF MASK (0x83.1) and/or VBUVF MASK (0x85.6) to enable ALERT pin assertion.	UV fault (0x80.6) UV cells (0x82). Clear UV mask (0x8A.6) to enable FAULT pin assertion
4	Set UV Fault	MCU Implementation	If the UV Flag is set, the MCU sets an internal flag and starts fault reaction functions.		
6	MCU Fault Reaction	The MCU starts fault reaction functions to isolate the battery pack from the load. These functions may include: sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state.	Shuts off power FETs clearing LDFET En (0x40.1) and/or LCFET En (0x40.0).	Shuts off power FETs clearing DFET EN (0x24.1) and/or CFET EN (0x24.0)	No power FETs control supported. External isolation driver required
Test Mechanism: Fault/Non-Fault Condition Induction					
1	Set UV_{th} to force fault detection	The MCU reads V_{CELLS}/V_{PACK} and sets the corresponding UV thresholds above the maximum cell voltage/V_{PACK}. This setup tests the detection of UV under fulfilment of the condition.	Set V_{CELL} UV threshold (0x82.[11:8]) and V_{CELL} UVLO (0x82.[3:0]) to Cell Max (0x01).	V_{CELLS} (0x31-0x4F) Set V_{CELL} UV threshold (0x06) to max (V_{CELLS}). V_{BAT} (0x5C-0x5D) Set UV_{BAT1} Threshold (0x21) above V_{BAT1}	V_{CELLS} (0x41-0x4E). Set OV limit (0x88) to max (V_{CELLS})
2	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
3	Read BFE UV Flag	The MCU reads the BFE flag, which should be set indicating V_{CELL}/V_{PACK} UV fault. If it is not set, the MCU outputs an Alert indicating failure of the UV detection and starts fault reactions.	Step 3 of Primary Channel		
4	Clear fault condition and set UV_{th} to force no fault detection	The MCU executes a command to clear the fault condition in the BFE and sets the UV threshold below the minimum cell voltage/V_{PACK}. This setup tests whether no UV fault is reported when the UV condition is not met.	Set Clear All Faults Bit (0x40.6). Set V_{CELL} UV threshold (0x82.[11:8]) and V_{CELL} UVLO (0x82.[3:0]) to Cell Min (0x02)	Set Clear All Faults Bit (0x02.1).	Clear UV Fault Register (0x82). Clear TOT[2:0] (0x86[6:4]).

Table 6. SM2 Undervoltage Detection (Cont.)

Step	Operation	Description	RAA489220	RAA489206	RAA489204
5	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
6	Read BFE OV Flag	The MCU reads the BFE flag, which should be clear indicating no V_{CELL}/V_{PACK} UV fault. If it is set, the MCU outputs an Alert indicating failure of the UV detection and starts fault reactions.	Step 3 of the Primary Channel		
Redundant Channel: MCU Verification of UV Condition and BFE Fault Reaction					
1	Primary Channel: BFE Detection and Fault Reaction	The BFE checks the UV condition. If the UV fault is detected, the BFE initiates autonomously fault reactions to isolate the battery pack, and outputs an alert. Fault reactions functions may include turning off cut-off FETs, and/or blowing up a fuse. BFE fault reactions ensure battery isolation in case of MCU failures.	Automatic fuse blow by clearing HVGPIO Mask (0x11.14). BFE FETs control in AutoScan mode. Transition to LP mode (safe state) after finishing system scan. ALERT pin asserted on a fault detection.	Automatic FETs control: set CELL CON (0x24.4) and/or V_{BAT1} CON (0x24.3). Clear UVF MASK (0x83.1) and/or VBUVF MASK (0x85.6) to enable ALERT pin assertion.	No automatic fault reaction to isolate the battery pack(s). Fault pin asserted to indicate the presence of fault condition in at least one of the monitored packs.
2	Redundant Channel: MCU UV Detection	The MCU reads the cells voltages and verifies whether all cell voltages/V_{PACK} are(is) above the UV threshold.	Execute the command code Read Measurements (0xC1)	Execute the command code Measurement (0x9B)	Read Cell/Pack Voltage Registers (0x41 – 0x50).
3	Redundancy Check	MCU Implementation	The MCU checks its UV flag. If it is set, the MCU initiates fault functions such as sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state. The MCU outputs an alert to notify the application.		

3.4.2.3 Comments

The redundant channel implementation is susceptible to CCF. The same mechanisms mentioned in SM1 can be implemented to counteract the effects of ADC and Multiplexer failures.

3.4.3 SM3: V_{PACK} Compare

The system should ensure accurate cell voltage measurements.

3.4.3.1 Implementation Description

The MCU compares the sum of individual cell readings with the V_{PACK} reading. Differences outside a specific range are flagged as faults.

3.4.3.2 Recommended Usage

Figure 11 and Figure 12 show the implementation of the V_{PACK} compare mechanism adopting single channel untested and tested architectures, respectively. Table 7 details the implementation.

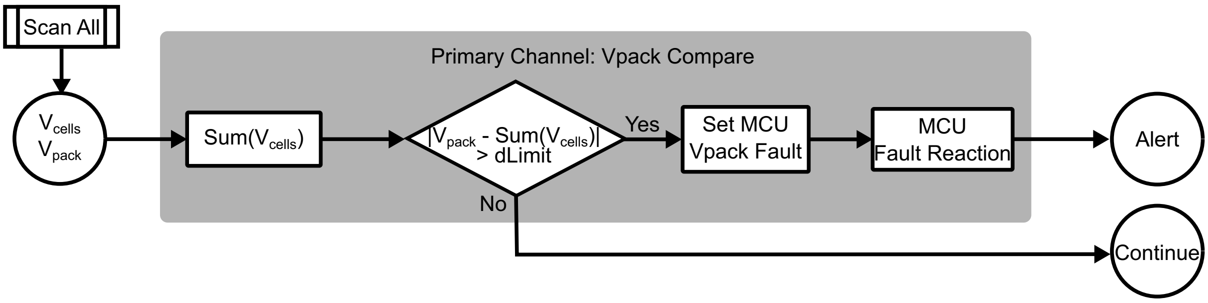

Figure 11. Single-Channel Untested Implementation of Pack Compare

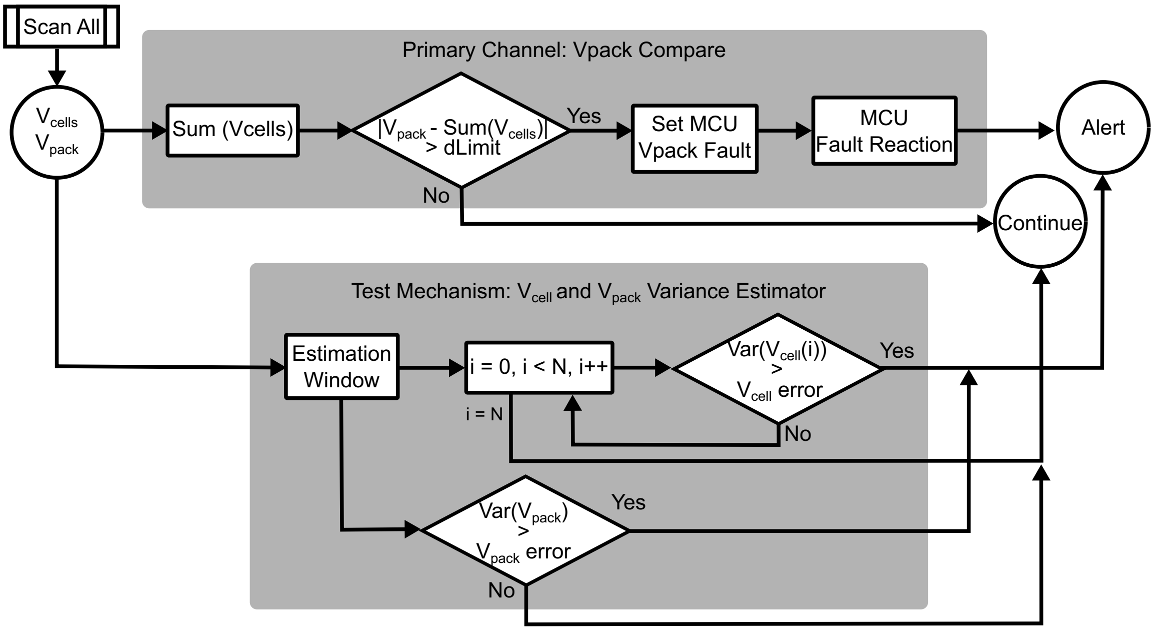

Figure 12. Single-Channel Tested Implementation of Pack Compare

Table 7. V_{PACK} Compare Mechanism

Step	Operation	Description	RAA489220	RAA489206	RAA489204
Primary Channel: Inaccurate Measurements Detection by V_{PACK} and V_{CELLS} Sum Comparison					
1	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
2	Read V_{CELLS} and V_{PACK} registers	The MCU reads BFE registers containing cells and V_{PACK} voltages, and sums V_{CELLS} measurements.	V_{CELLS} requires triggering individual measurement: Measurement Selection (0x41.[4:0]) to V_{CELL1} – V_{CELL10} (0x09-0x12). Result stored in Therm 2 Register (0x04). Pack Voltage (0x00).	V_{CELLS} (0x31-0x4F). V_{PACK} available as V_{BAT1} Voltage (0x5C-0x5D)	V_{CELLS} (0x41-0x4E). PACK Voltage (0x50)

Table 7. V_{PACK} Compare Mechanism (Cont.)

Step	Operation	Description	RAA489220	RAA489206	RAA489204
3	Comparison of the Sum with V_{PACK}	MCU Implementation	The MCU compares the sum of the cell voltages with the V_{PACK} value retrieved from the BFE, checking whether the difference between them exceeds a maximum allowable error dLimit. If the difference is higher than dLimit, the MCU sets its V_{PACK} fault indicator and starts fault reactions.		
4	MCU Fault Reaction	Because the V_{PACK} calculated by two different methods diverges above the maximum allowable error, the MCU may start fault reaction functions to isolate the battery pack and alert the application.	Shuts off power FETs clearing LDFET En (0x40.1) and/or LCFET En (0x40.0).	Shuts off power FETs clearing DFET EN (0x24.1) and/or CFET EN (0x24.0)	No power FETs control supported. External isolation driver required
Test Mechanism: V_{CELL} and V_{PACK} Variance Estimator					
1	Estimation Window	The MCU commands the BFE to measure V_{CELLS} and V_{PACK} during a time window. The MCU accumulates reported values and calculates their variances.	Trigger individual measures using Measurement Selection (0x41.[4:0]: V_{PACK} (0x08), V_{CELLS} (0x09-0x12). Clear and set Trigger Measurement (0x41.7). Read THERM 2 register (0x04) after finishing each measurement.	Clear and Trigger V_{BAT1} Trigger (0x1F.0). Clear and set V_{CELL} Trigger (0x02.0). Read V_{BAT1} (0x5C-0x5D) and V_{CELLS} (0x31- 0x4F).	Perform Scan Voltages (0xC1) command. Read V_{CELLS} (0x41-0x4E) and PACK Voltage (0x50)
2	Variance verification	The MCU checks whether V_{CELL} or V_{PACK} variances exceed the measurement errors specified in the BFE datasheet. The MCU generates an alert to notify inaccurate measurements if variances are out of spec	Calculate var(V_{CELLS}) and compare with ±16mV. Calculate var(V_{PACK}) and compare with ±0.5%.	Calculate var(V_{CELLS}) and compare with ±10mV. Calculate var(V_{BAT1}) and compare with ±0.5%	Calculate var(V_{CELLS}) and compare with ±10mV. Calculate var(V_{PACK}) and compare with ±230mV

3.4.3.3 Comments

To ensure validity of the variance, run the test mechanism when voltages are expected to remain invariant. This is, when the system is off and there are not voltage transients.

The V_{PACK} compare safety mechanism can be also used as a method to detect ADC and Multiplexer failures. A stock multiplexer generates divergence of V_{PACK} with respect to the sum of individual cell voltages, and a failing ADC results in too low measurement variance or higher than the specified in the datasheet.

To implement redundancy and counteract CCF, the architecture may include conditioning hardware to enable the MCU ADC to measure V_{PACK}. The MCU converts the digitalized samples and verifies whether the divergence of the values reported by the BFE (V_{PACK} and V_{CELLS}) is acceptable. The use of filters and different ADC resolutions can be used as additional countermeasures against CCF.

3.4.4 SM4: Internal Over-Temperature Detection

The BMS determines if there is an internal over-temperature condition.

3.4.4.1 Implementation Description

During a Scan All command, the BFE reads the voltage of an internal temperature sensor to determine if there is an over-temperature fault. A fault is registered by the ADC readings below the OT limit value.

In some BFEs such as the RAA489220, the internal over-temperature threshold is factory-set and cannot be programmed by the user. Therefore, there is not a mechanism to force the detection as it has been described for previous mechanisms. However, the validity of the internal temperature reading can be checked using an external temperature sensor mounted on the board close to the BFE. The MCU validates the internal reading evaluating the correlation between the internal and the external temperature values. The evaluation should not be made in terms of voltage, but in temperature after converting each voltage to its respective temperature. The reason for doing so is that the internal voltage of BFE temperature sensors varies linearly with the temperature, whereas the voltage variation of external thermistors is polynomial. The MCU can use the external temperature measurements featured by Renesas BFEs, or include conditioning circuits to enable its ADC to measure the voltage of the external temperature sensors.

Other BFEs such as the RAA489206 and the RAA489204 feature programmable thresholds for Warning and Fault over-temperature limits, so the test mechanism that forces fault detection to test the integrity of the OT detection circuit can be adopted. In this case, using the readings of a sensor close to the BFE would constitute a redundant channel.

3.4.4.2 Recommended Usage

Figure 13 shows the implementation of OT detection adopting single channel architecture, which includes an external thermistor input to verify the internal temperature measurement. The test mechanism uses an on-board thermistor to verify the validity of the internal sensor measurement. Figure 14 shows the redundant architecture using external OT detection with autonomous fault reaction function, and a path to the redundancy check mechanism executed by the MCU. Table 8 details the implementation of both architectures.

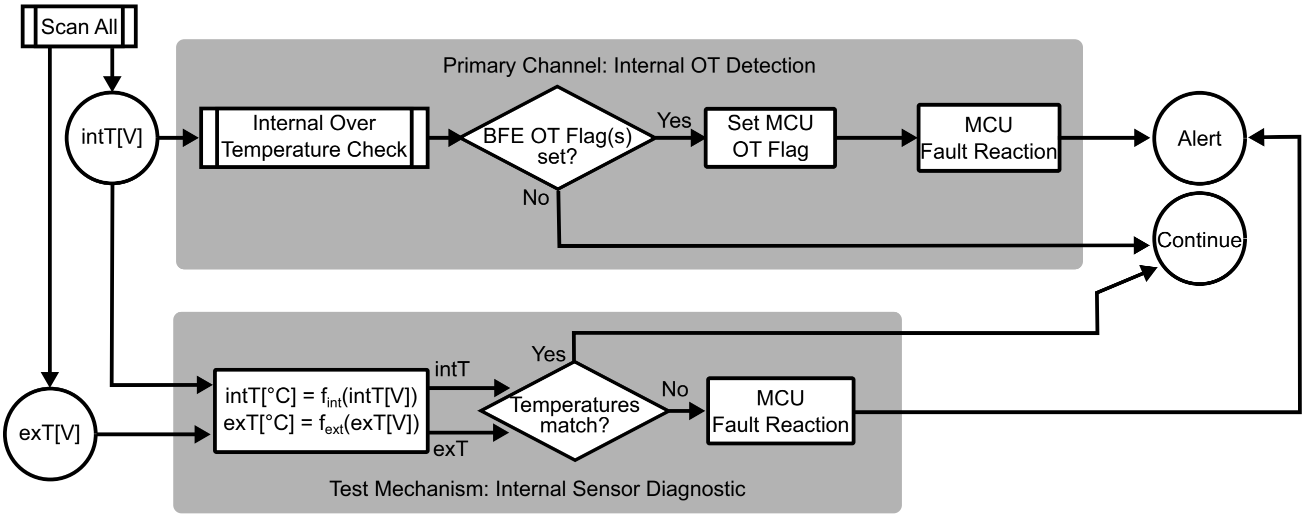
Scan All
Primary Channel: Internal OT Detection
intT[V]
Internal Over Temperature Check
BFE OT Flag(s) set?
Yes
No
Set MCU OT Flag
MCU Fault Reaction
Alert
Continue
Yes
intT
intT[°C] = f_{int}(intT[V])
exT[°C] = f_{ext}(exT[V])
exT
Temperatures match?
No
MCU Fault Reaction
exT[V]
Test Mechanism: Internal Sensor Diagnostic

Figure 13. Single-Channel Tested Implementation of Internal Over-Temperature Detection

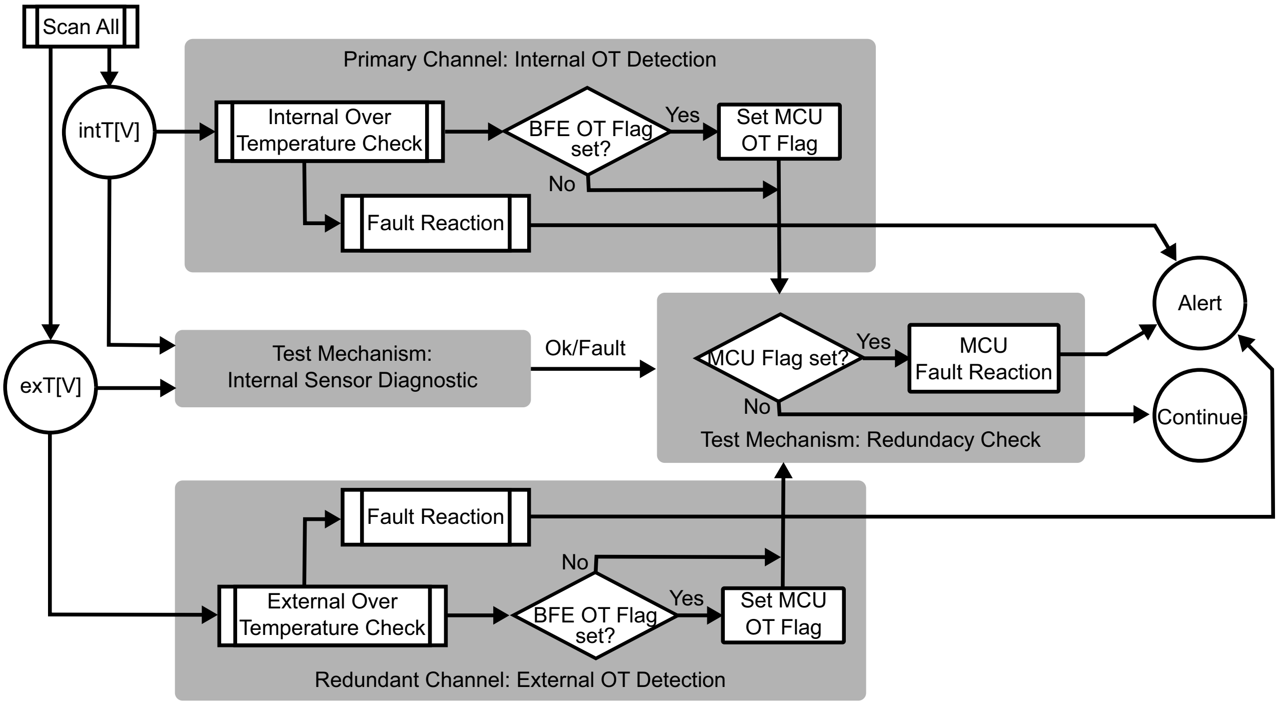
Scan All
intT[V]
exT[V]
Primary Channel: Internal OT Detection
Internal Over Temperature Check
BFE OT Flag set?
Yes
No
Set MCU OT Flag
Fault Reaction
Alert
Test Mechanism: Internal Sensor Diagnostic
Ok/Fault
MCU Flag set?
Yes
No
MCU Fault Reaction
Continue
Test Mechanism: Redundacy Check
Fault Reaction
No
External Over Temperature Check
BFE OT Flag set?
Yes
Set MCU OT Flag
Redundant Channel: External OT Detection

Figure 14. Redundant Channel Implementation of Internal Over-Temperature Detection

Table 8. External Temperature Sensor Mechanism

Step	Operation	Description	RAA489220	RAA489206	RAA489204
Primary Channel: Internal OT Detection					
1	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
2	Internal OT Check	The BFE compares the value of the voltage reported by the internal temperature sensor with the value stored in the internal OT threshold register and sets the internal OT flag if the measured voltage is lower than the limit.	Fixed Internal Over-Temperature threshold: 100°C.	Internal Over-Temperature Fault (IOTF) threshold (0x23). Internal Over-Temperature Warning (IOTW) threshold (0x22).	Internal Temperature Warning (0x8C). Internal Over-Temperature Limit (0x8D) factory-programmed (default value 139°C).
3	Read BFE OT Flag	The MCU checks proactively or triggered by the BFE (such as assertion of a pin connected to an MCU IRQ-enabled pin) the BFE register that indicates the presence of internal OT Fault.	IOTF (0x10.13). ALERT pin asserted on a fault detection.	IOTF (0x63.5) IOTW (66.6). Clear IOTF MASK (0x83.5) and/or IOTW MASK (0x86.6) to enable ALERT pin assertion.	ITWFG (0x80.15) OT (0x80.4) OTIT (0x84.0) Clear ITWGF mask (0x8A.15) and/or OT mask (0x8A.4) to enable FAULT pin assertion.
4	Set OT Fault	MCU Implementation	If the OT Flag is set, the MCU sets its internal OT flag and starts fault reaction functions.		

Table 8. External Temperature Sensor Mechanism (Cont.)

Step	Operation	Description	RAA489220	RAA489206	RAA489204
5	MCU Fault Reaction	The MCU starts fault reaction functions to isolate the battery pack. Fault reactions may include turning cut-off FET drivers off, blowing a fuse, and forcing the charge pump to the off state.	Shuts off power FETs clearing LDFET En (0x40.1) and/or LCFET En (0x40.0).	Shuts off power FETs clearing DFET EN (0x24.1) and/or CFET EN (0x24.0)	No power FETs control supported. External isolation driver required
Test Mechanism: Internal Sensor Diagnostic with External Temperature Sensor Reading					
1	Transform the voltages reported by the internal and the on-board sensor	The MCU reads the voltages reported by the BFE on the internal temperature sensor and the external temperature pin connected to an on-board thermistor. The MCU transforms the voltage to their respective temperature value according to sensor T(V) characteristic.	Internal temperature sensor is only intended for comparison with OT fault threshold. Read Therm1 (0x03) and/or Therm2 (0x04). Calculate Voltage as: $\mathrm{Therm1/2[V]} = (\mathrm{RegVal} + 0.5) \times 0.0005 - 0.128$	Read Internal Temperature (0x5E). Calculate temperature as: $\mathrm{IT[°C]} = (-1.82 \times 10^{-4}) \times (\mathrm{REgVal}^2) - 0.79605 \times (\mathrm{RegVal}) + 151.11$ Read xT0/AUX0 (0x58-59) and/or xT1/AUX1 (0x5A-0x5B) and calculate Voltage as: $\mathrm{Vtemp[V]} = (24.52 \times 10^{-6}) \times (\mathrm{RegVal} + 0.5)$	Read Internal Temperature Reading (0x60). Calculate temperature as: $\mathrm{IT[°C]} = \frac{\mathrm{RegVal}}{128} - 273$ Read exTX (0x61-0x64) pin connected to on-board thermistor. Calculate Voltage on ExTX as: $\mathrm{Vtemp[V]} = \frac{\mathrm{RegVal} \times 2.5}{16384 \times 4}$
2	Temperature Match	Considering measures accuracy, the MCU evaluates sensor readings correlation and verifies if temperatures match.	N/A	IT_{err} = ±5°C V_{ETAUX} Gain Error = ±1%	Ext Temperature Input Error = ±30mV
3	MCU Fault Reaction	If values diverge out of accuracy margins, the MCU initiates fault reaction functions to isolate the battery pack and outputs an alert.	N/A	Step 5 of the Primary Channel	Step 5 of the Primary Channel
4	Optional Test Mechanism	If BFE features programmable internal OT threshold, the MCU tests OT detection inducing fault and no-fault.	N/A	IOTF threshold (0x23). IOTW threshold (0x22).	Internal Temperature Warning Value (0x8C)
Redundant Channel: External Over-Temperature Detection					
1	Primary Channel: BFE Detection and Fault Reaction	The BFE checks the internal OT condition using the input of the internal temperature sensor. If OT fault is detected, the BFE initiates fault reactions to isolate the battery pack, and outputs an alert. Fault reactions functions may include turning off cut-off FETs, and/or blowing up a fuse. The BFE reads the BFE internal OT flag and sets its internal flag if the BFE reports the fault.	ALERT pin asserted when the device die temperature exceeds 100°C. Transition to Low Power Mode on a fault detection. Monitor Therm1 and Therm2 voltages and react if values are below OT threshold	Power FETs are disable and System Scan stops on a IOTF detection.	No automatic fault reaction to isolate the battery pack(s). Fault pin asserted to indicate the presence of fault condition in at least one of the monitored packs. Set OT mask (0x8A.4) to enable FAULT pin assertion.

Table 8. External Temperature Sensor Mechanism (Cont.)

Step	Operation	Description	RAA489220	RAA489206	RAA489204
2	Redundant Channel: External OT detection	The MCU sets an external OT threshold to the same internal OT limit. After a Scan All operation, the BFE verifies the external temperature pin is below the programmed OT threshold. If the value is lower than the limit, the BFE starts autonomously fault reactions to isolate the pack. The MCU reads the external OT BFE flag and sets its internal flag accordingly.	Set DOT (0x83.[13:11] and/or COT (0x83.[5:3]) to voltages equivalent to the required over-temperature threshold. Power FETs are turned off on a OTF detection	Set Charge/ Discharge Over temperature (COT, DOT) Thresholds (0x14, 16, 18, 1A) to voltages equivalent to required over-temperature threshold. Clear ETAUX Fault Masks (0x84[7,5,3,1]) to enable ALERT pin assertion. set ETA Connect (0x24.2) to enable automatic power FETs control.	Set External Temperature limit (0x89) to the required over-temperature warning threshold. Set OT mask (0x8A.4) to enable FAULT pin assertion. No power FETs control supported. External isolation driver required.
3	Redundancy Check	MCU Implementation	The MCU checks if its internal OT flag is set. If it is, the MCU initiates fault functions such as sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state. The MCU outputs an alert to notify the application.		

3.4.4.3 Comments

The described implementations are susceptible to CCF of the BFE ADC and the multiplexer. To counteract CFF, it is possible to add an independent channel by conditioning the external thermistor signal to be measured by the MCU ADC. The measures of the MCU ADC (correctly scaled) are then compared with the values BFE reported by the BFE and the internal OT limit to backup the BFE detection system.

3.4.5 SM5: External Input Over-Temperature Detection

The BMS determines if any of its pins designated to measure input voltages of external thermistors has an over-temperature condition.

3.4.5.1 Implementation Description

During a Scan All command, the BFE reads the voltage on pins designated to measure external temperature. These inputs readings are compared against corresponding threshold voltages to determine if there is an OT fault. A fault is registered by the ADC readings below the programmed OT limit value. This considers that the external thermistors have Negative Temperature Coefficient (NTC), whose resistance decreases with higher temperature. When the BFE detects the OT condition, the BFE sets internal fault flag(s) to indicate the OT event and may assert an Alert pin connected to the MCU. In Renesas BFEs, several pins can be configured to monitor external temperature sensors, so the BMS can monitor the temperature of different parts of the battery pack or use redundant sensors as countermeasure against thermistor failures.

3.4.5.2 Recommended Usage

Figure 15 shows the implementation of external OT detection adopting single channel tested architecture. In this implementation, two external inputs with independent thresholds are configured to detect external OT conditions at either different or redundant battery pack points. It includes the possibility of having two (or more) thermistor inputs, which are compared internally in the BFE with the programmed threshold. The test mechanism uses minimum and maximum threshold values to induce fault and no-fault, respectively. Figure 16 and Figure 17 depict two redundant architecture approaches. In Figure 16, the redundant channel uses the reading of the BFE to verify the external OT condition, whereas the architecture shown in Figure 17 uses the MCU ADC to implement a redundant channel independent from the BFE to counteract the CCF of the BFE ADC. Table 9 details their implementations.

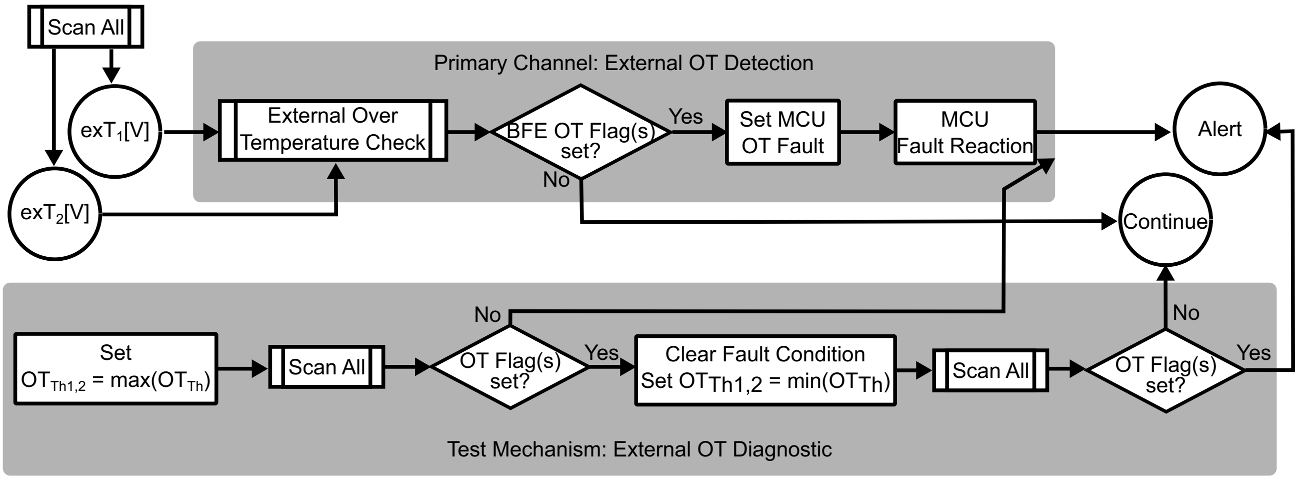
Scan All
$exT_1[V]$
$exT_2[V]$
Primary Channel: External OT Detection
External Over Temperature Check
BFE OT Flag(s) set?
Yes
No
Set MCU OT Fault
MCU Fault Reaction
Alert
Continue
Set $OT_{Th1,2}$ = max(OT_{Th})
Scan All
OT Flag(s) set?
No
Yes
Clear Fault Condition Set $OT_{Th1,2}$ = min(OT_{Th})
Scan All
OT Flag(s) set?
No
Yes
Test Mechanism: External OT Diagnostic

Figure 15. Single-Channel tested Implementation of External Over-Temperature Detection

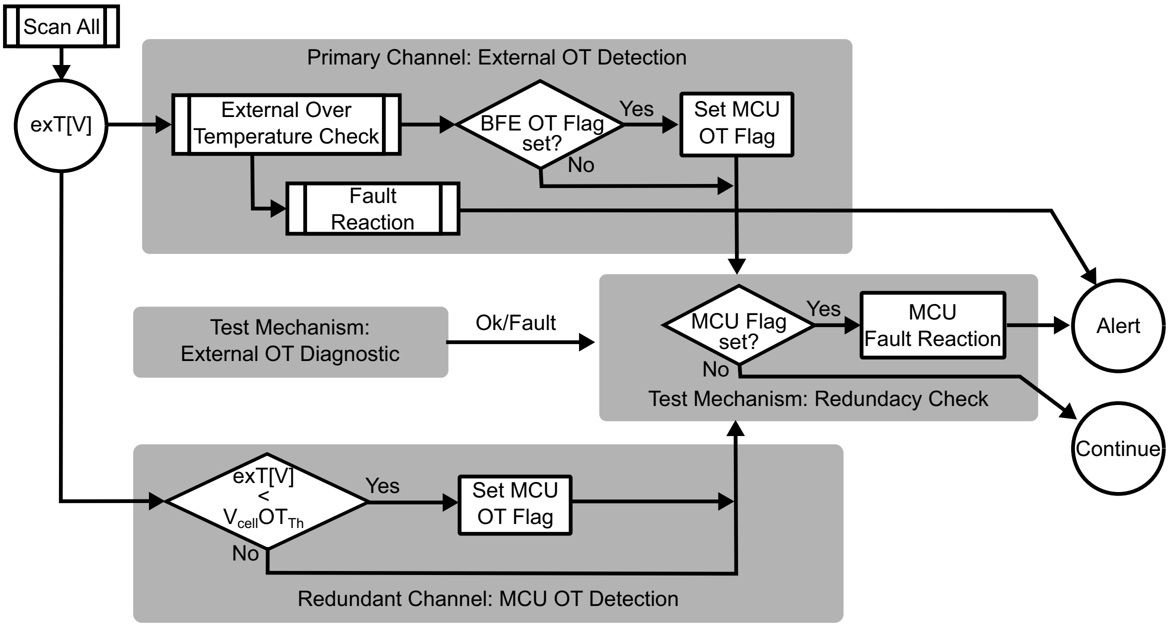
Scan All
exT[V]
Primary Channel: External OT Detection
External Over Temperature Check
BFE OT Flag set?
Yes
No
Set MCU OT Flag
Fault Reaction
Test Mechanism: External OT Diagnostic
Ok/Fault
MCU Flag set?
Yes
No
MCU Fault Reaction
Alert
Continue
Test Mechanism: Redundacy Check
exT[V] < $V_{cell}OT_{Th}$
Yes
No
Set MCU OT Flag
Redundant Channel: MCU OT Detection

Figure 16. Redundant Channel Implementation of External OT Detection using BFE Value

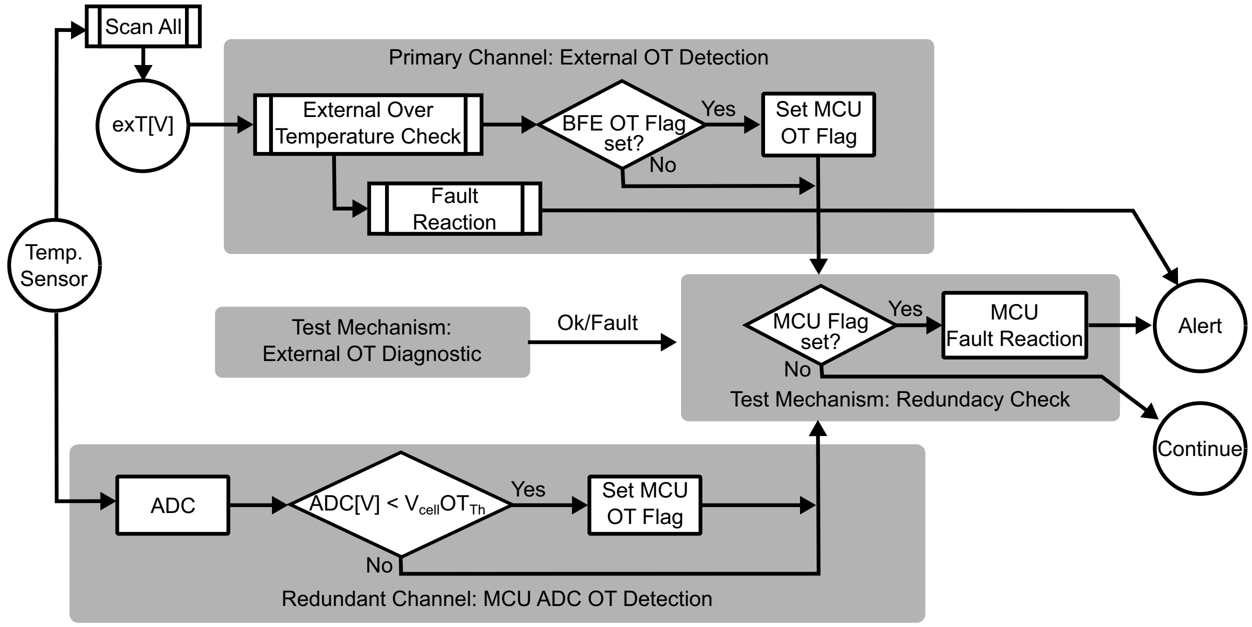
Scan All
exT[V]
Primary Channel: External OT Detection
External Over Temperature Check
BFE OT Flag set?
Yes
No
Set MCU OT Flag
Fault Reaction
Temp. Sensor
Test Mechanism: External OT Diagnostic
Ok/Fault
MCU Flag set?
Yes
No
MCU Fault Reaction
Test Mechanism: Redundacy Check
Alert
Continue
ADC
ADC[V] < VcellOTTh
Yes
No
Set MCU OT Flag
Redundant Channel: MCU ADC OT Detection

Figure 17. Redundant Channel Implementation of External OT Detection using MCU ADC

Table 9. External Temperature Detection Mechanism

Step	Operation	Description	RAA489202	RAA489206	RAA489204
Primary Channel: External OT Detection by BFE Condition Check and MCU Fault Reaction Function					
1	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
2	Undervoltage Check	The BFE compares the value of the external temperature pins with the value stored in the external OT threshold register and sets the corresponding internal OT flag(s) if the measured voltage(s) is lower than the programmed limit.	Charge/Discharge Over-temperature thresholds COT (0x83.[5:3]) DOT (0x83.[13:11])	Charge/ Discharge Over-temperature thresholds COT0 (0x14) COT1 (0x18) DOT0 (0x16) DOT1 (0x1A)	External Temperature limit (0x89)
3	Read BFE OT Flag	The MCU checks proactively or triggered by the BFE (such as assertion of a pin connected to an MCU IRQ-enabled pin) the BFE register(s) that indicates the presence of external OT Fault(s).	OTF (0x10.4) ALERT pin asserted on a fault detection.	COT1 (0x64.7) DOT1 (0x64.5) COT0 (0x64.3) DOT0 (0x64.1) Clear ETAUX Fault Masks (0x84.[7,5,3,1]) to enable ALERT pin assertion.	OT (0x80.4). OTF[4-1] (0x84.[4:1]). Clear OT mask (0x8A.4) to enable FAULT pin assertion.
4	Set OT Fault	MCU Implementation	If the OT Flag(s) is set, the MCU sets its internal flag(s) and starts fault reaction functions.		
5	MCU Fault Reaction	The MCU starts fault reaction functions to isolate the battery pack from the load. These functions may include: sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state.	Shuts off power FETs clearing LDFET En (0x40.1) and/or LCFET En (0x40.0).	Shuts off power FETs clearing DFET EN (0x24.1) and/or CFET EN (0x24.0)	No power FETs control supported. External isolation driver required

Table 9. External Temperature Detection Mechanism (Cont.)

Step	Operation	Description	RAA489202	RAA489206	RAA489204
Test Mechanism: Fault/Non-Fault Condition Induction					
1	Set external OT_{th} to minimum temperature threshold	The MCU sets the temperature voltage threshold to full scale.	Set DOT (0x83.[13:11] and/or COT (0x83.[5:3]) to 0xFF	Set DOTX/COTX to 0xFF	Set External Temperature limit (0x89) to 0xFF
2	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
3	Read BFE external OT Flag(s)	The MCU reads BFE flag(s), which should be set indicating external OT fault. If it is not set, the MCU outputs an Alert indicating failure of the external OT detection and starts fault reactions.	OTF (0x10.4)	COT1 (0x64.7) DOT1 (0x64.5) COT0 (0x64.3) DOT0 (0x64.1)	OT (0x80.4). OTF[4-1] (0x84.[4:1]).
4	Clear fault condition and set OT_{th} to minimum threshold	The MCU executes a command to clear the fault condition in the BFE and sets the temperature voltage threshold to empty scale.	Set Clear All Faults Bit (0x40.6). Set DOT (0x83.[13:11] and/or COT (0x83.[5:3]) to 0x00	Set Clear All Faults Bit (0x02.1). Set DOTX/COTX to 0x00	Clear OTF[4-1] (0x84[4:1]) and OTIT (0x84.0)
5	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4		
6	Read BFE external OT Flag(s)	The MCU reads its internal BFE flag(s), which should be clear indicating no OT fault. If it is set, the MCU outputs an Alert indicating failure of the external OT detection and starts fault reactions.	Step 5 of the Primary Channel if failure detected		
Redundant Channel: MCU Verification of External OT Condition and BFE Fault Reaction					
1	Primary Channel: BFE Detection and Fault Reaction	The BFE checks the external OT condition. If OT fault(s) is detected, the BFE initiates fault reactions to isolate the battery pack, and outputs an alert. Fault reactions functions may include turning off cut-off FETs, and/or blowing up a fuse. BFE fault reactions ensure battery isolation in case of MCU failures.	BFE FETs control in AutoScan mode.	Automatic FETs control: Set ETA Connect (0x24.2) to enable automatic power FETs control. Clear ETAUX Fault Masks (0x84[7,5,3,1]) to enable ALERT pin assertion.	No automatic fault reaction to isolate the battery pack(s). Fault pin asserted to indicate the presence of fault condition in at least one of the monitored packs.
2	Redundant Channel 1: MCU external OT Detection using BFE measurements	The MCU reads BFE registers containing measurements of external pins. The MCU verifies whether they are below the programmed OT threshold. If any of them is lower than the limit, the MCU sets its external OT flag.	Read Therm1 (0x03) and Therm2 (0x03) and convert their values to temperature as: $\text{Therm1/2[V]} = (\text{RegVal} + 0.5) \times 0.0005 - 0.128$	Read xT0/AUX0 (0x58-59) and/or xT1/AUX1 (0x5A-0x5B) and calculate Voltage as: $\text{Vtemp[V]} = (24.52 \times 10^{-6}) \times (\text{RegVal} + 0.5)$	Read exTX (0x61-0x64) pin connected to on-board thermistor. Calculate Voltage on ExTX as: $\text{Vtemp[V]} = \frac{\text{RegVal} \times 2.5}{16384 \times 4}$

Table 9. External Temperature Detection Mechanism (Cont.)

Step	Operation	Description	RAA489202	RAA489206	RAA489204
2	Redundant Channel 2: MCU ADC	MCU Implementation	The MCU triggers an ADC conversion, reads its ADC register, and transforms the value to voltage. The MCU sets its external OT flag if the value is below the voltage corresponding to the external OT threshold.		
3	Redundancy Check		The MCU checks its external OT flags. If they are set, the MCU initiates fault functions such as sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state. The MCU outputs an alert to notify the application.		

3.4.5.3 Comments

The described implementations are susceptible to CCF of the BFE ADC. To counteract CFF, it is possible to add an independent channel by conditioning the signals of the external thermistors to enable the MCU to use its ADC to measure either the same points monitored by the BFE, or totally independent temperature sensors. The measures of the MCU ADC are then compared with BFE values and analyzed to backup the OT detection system of the BFE.

3.5 Current Events Detection

The RAA489204 and RAA489220 do not support current sensing, whereas the RAA489206 does feature discharge and charge current sensing. Therefore, the description of the safety mechanisms that detects current events refers to their implementation using the RAA489206.

The implementation of architectures for current event detection does not include test mechanism that can be executed during the system FTI. Test mechanisms that force fault/no-fault detection require that the current flows through the load, so modifying the current thresholds while the system is actively operating affects the safety function. Monitoring periodically the variance of the current measurement may work as verification of the current measurement accuracy but does not test the event detection. On the other hand, the implementation of a redundant channel can act as test mechanism of the fault detection registering and reporting failures if the fault is not detected while the current flows. This redundant channel approach with two different implementations is adopted for discharge and charge overcurrent detection (SM6 and SM7, respectively). In the first implementation, the MCU reads the current value reported by the BFE as the voltage across the sense resistor, convert it to current and compare the obtained value with the current limit. The second implementation uses the MCU ADC to measure the conditioned voltage across the sense resistor and compare the corresponding current with the current threshold. This implementation can be used to counteract the CCF of the BFE ADC but requires additional hardware to condition the sensed voltage. Short-circuit current detection (SM8) requires fast reaction, so an analog comparator is used instead of the sampled I_{PACK} measurement generated by the Scan All command. Therefore, it is only possible to implement the untested single channel pattern relying on the high reliability of the analog comparator included in the RAA489206. Redundant mechanisms would need additional hardware, such as an external analog comparator with its conditioned output connected to an MCU IRQ pin, but such mechanisms are out of the scope of this manual.

3.5.1 SM6: Discharge Overcurrent Detection

The BMS detects Discharge Overcurrent (DOC) when the magnitude of the pack current is above user-programmed threshold DOC_{th}.

3.5.1.1 Implementation Description

Discharge currents produce a negative voltage across the sense resistor. Therefore, the BFE reports the negative I_{PACK} voltage while the battery pack discharges. During a Scan All command, the BFE reads the voltage across the current sense resistor and sets the DOC flag if its voltage is less than or equal to the DOC_{th} during discharge. The BFE may assert an Alert pin connected to the MCU.

3.5.1.2 Recommended Usage

Figure 18 and Figure 19 depict two implementations of the DOC detection safety mechanism using redundant channels. Figure 18 shows the redundant channel that uses the current pack voltage reported by the BFE, whereas Figure 19 shows the redundant channel that counteracts the CCF by using MCU ADC. Table 10 details their implementations.

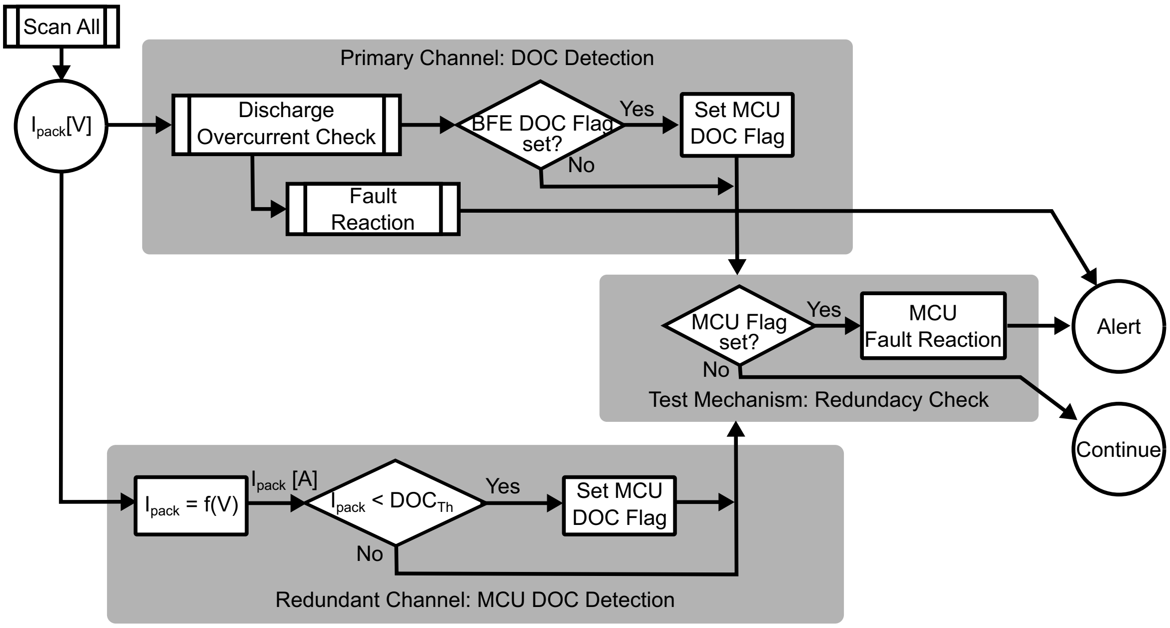

Figure 18. Redundant Channel Implementation of DOC Detection using I_{PACK} Reported by BFE

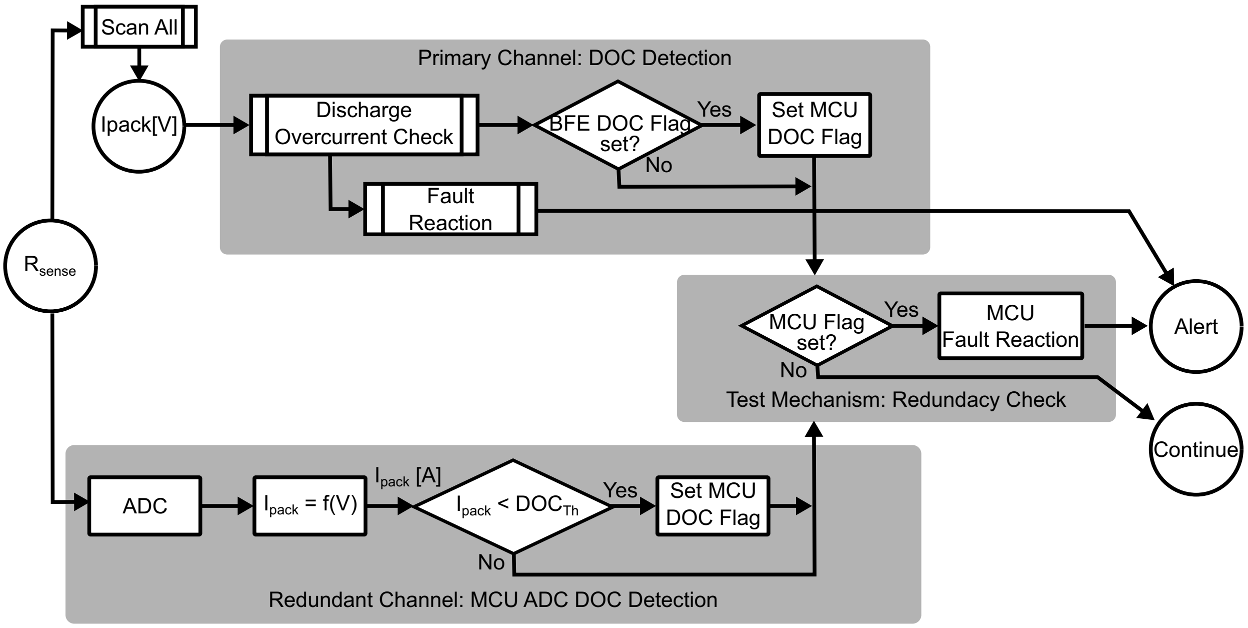

Figure 19. Redundant Channel Implementation of DOC Detection using MCU ADC

Table 10. Discharge Overcurrent (DOC) Detection Mechanism

Step	Operation	Description	RAA489206
Primary Channel: DOC Detection by BFE Condition Check and MCU Fault Reaction Function			
1	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4
2	Discharge Overcurrent Check	During discharge, the BFE compares the value of I_{PACK} voltage with the value stored in DOC threshold register and sets its internal DOC flag if the voltage is less than or equal to the programmed limit.	Discharge Overcurrent (DOC) Threshold (0x0B). This register represents a negative value without a sign bit.
3	Read BFE DOC Flag	The MCU checks proactively or triggered by the BFE (such as assertion of a pin connected to an MCU IRQ-enabled pin) the BFE register(s) that indicates the presence of DOC Fault.	DOCF (0x63.3) Clear DOCF MASK (0x83.3) to enable ALERT pin assertion on a fault detection.
4	Set DOC Fault	MCU Implementation	If the DOCF is set, the MCU sets its internal flag and starts fault reaction functions.
5	MCU Fault Reaction	The MCU starts fault reaction functions to isolate the battery pack from the load. These functions may include: sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state.	Shuts off power FETs clearing DFET EN (0x24.1) and/or CFET EN (0x24.0)
Redundant Channel: MCU Verification of DOC Condition and BFE Fault Reaction			
1	Primary Channel: BFE Detection and Fault Reaction	The BFE checks the DOC condition. If DOC fault is detected, the BFE initiates fault reactions to isolate the battery pack, and outputs an alert. Fault reactions functions may include turning off cut-off FETs, and/or blowing up a fuse. BFE fault reactions ensure battery isolation in case of MCU failures.	Automatic FETs control: Set CFD (0x0E.7) to enable automatic power FETs control. Clear DOCF MASK (0x83.3) to enable ALERT pin assertion on a fault detection.
2	Redundant Channel 1: MCU DOC Detection using BFE measurements	The MCU reads the BFE register containing measurement of the voltage across the sense resistor. The MCU converts its value to current and sets its DOC flag if it is below the programmed (signed) DOC_{th}.	Read I_{PACK} Voltage (0x52-0x53) and convert its value to signed voltage $V(I_{PACK})$ as specified in Section 5.3.6 of the datasheet. Calculate the I_{PACK} current as: $I_{PACK}[A] = \frac{V(I_{PACK})}{R_{SENSE}}$ Where R_{SENSE} is the sense resistance in Ohms. Set MCU DOC flag if $I_{PACK}[A] \leq$ (signed) I_{DOCth}

Table 10. Discharge Overcurrent (DOC) Detection Mechanism (Cont.)

Step	Operation	Description	RAA489206
2	Redundant Channel 2: MCU ADC	MCU Implementation	The MCU triggers an ADC conversion, reads its ADC register and transforms the value to voltage. The MCU converts the voltage value to current as $I_{PACK}[A] = \frac{-V_{ADC}}{R_{SENSE}}$ Set MCU DOC flag if $I_{PACK}[A] \le$ (signed) I_{DOCth}
3	Redundancy Check		The MCU checks its internal DOC flag. If it is set, the MCU initiates fault functions such as sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state. The MCU outputs an alert to notify the application.

3.5.2 SM7: Charge Overcurrent Detection

The BMS detects Charge Overcurrent (COC) when the magnitude of the pack current is above user-programmed threshold COC_{th}.

3.5.2.1 Implementation Description

Charge currents produce a positive voltage across the sense resistor. Therefore, the BFE reports the positive I_{PACK} voltage while the battery pack is being charged. During a Scan All command, the BFE reads the voltage across the current sense resistor and sets the COC flag if its voltage is greater than or equal to the COC_{th} during charge. The BFE may assert an Alert pin connected to the MCU.

3.5.2.2 Recommended Usage

Figure 20 and Figure 22 depict two implementations of the COC detection safety mechanism using redundant channels. Figure 20 shows the redundant channel that uses the current pack voltage reported by the BFE, whereas Figure 22 the redundant channel that counteracts the CCF by using MCU ADC to measure the voltage on the sense resistor. Table 11 details the mechanisms implementation.

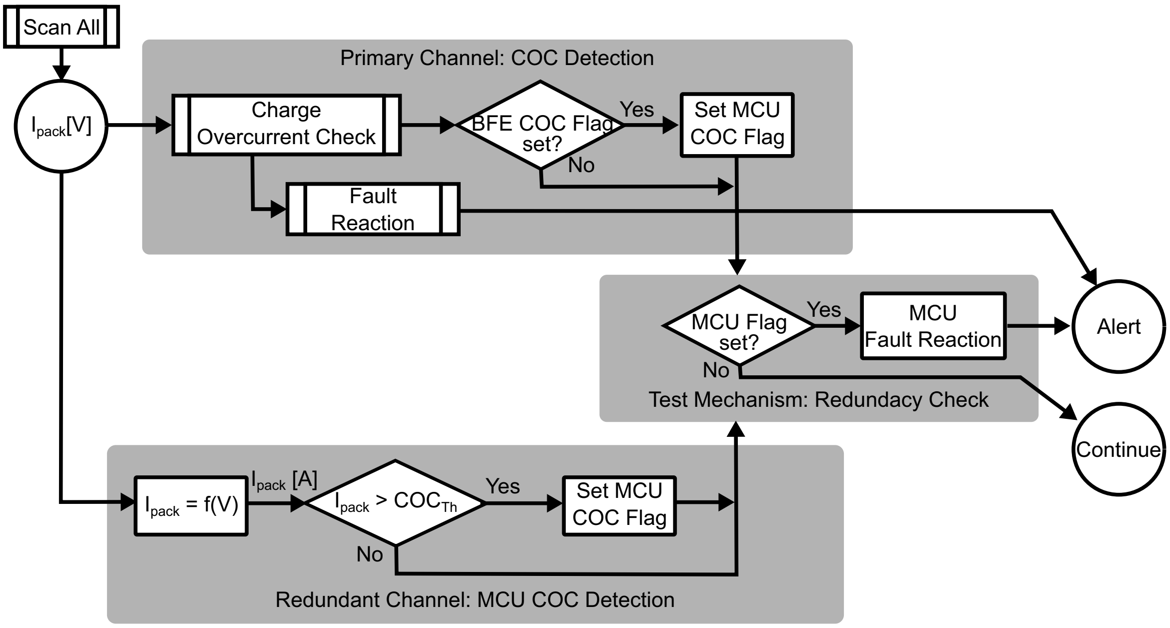

Figure 20. Redundant Channel Implementation of COC Detection using I_{PACK} Reported by BFE

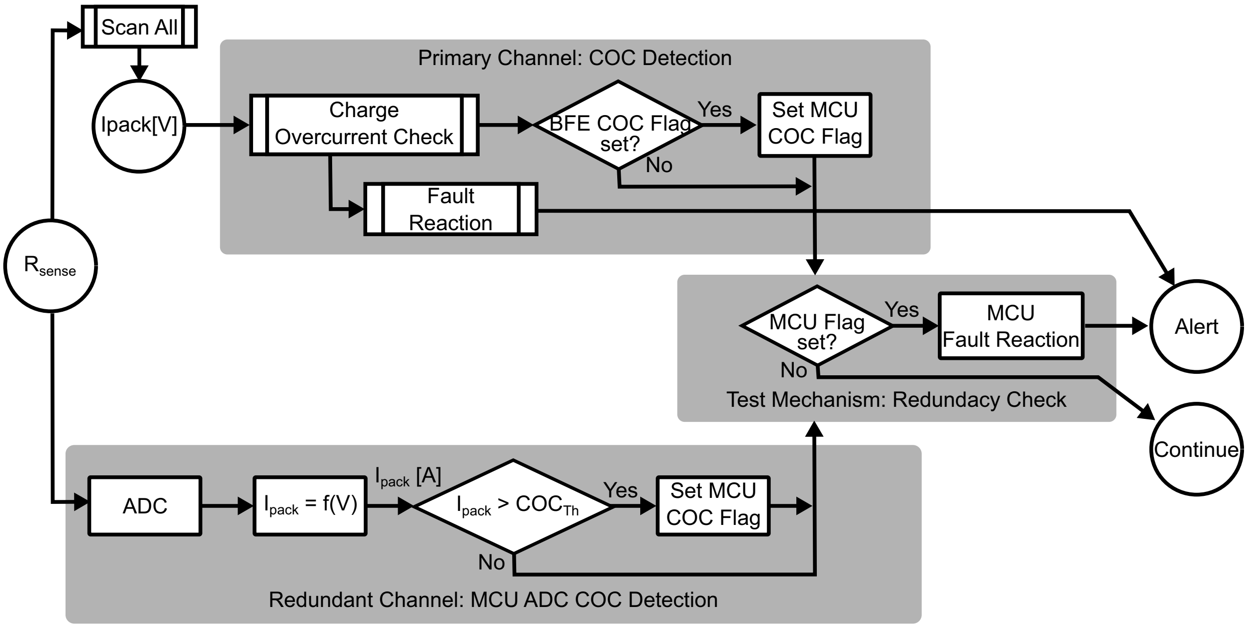

Figure 21. Redundant Channel Implementation of COC Detection using MCU ADC

Table 11. Charge Overcurrent (COC) Detection Mechanism

Step	Operation	Description	RAA489206
Primary Channel: Charge Overcurrent Detection by BFE Condition Check and MCU Fault Reaction Function			
1	Scan All	The MCU commands the BFE to execute a Scan All operation.	See Table 4
2	Charge Overcurrent Check	During discharge, the BFE compares the value of I_{PACK} voltage with the value stored in COC threshold register and sets its internal COC flag if the voltage is greater than or equal to the programmed limit.	Charge Overcurrent (COC) Threshold (0x0F).
3	Read BFE COC Flag	The MCU checks proactively or triggered by the BFE (such as assertion of a pin connected to an MCU IRQ-enabled pin) the BFE register(s) that indicates the presence of DOC Fault.	COCF (0x63.4) Clear COCF MASK (0x83.4) to enable ALERT pin assertion on a fault detection.
4	Set COC Fault	MCU Implementation	If COCF is set, the MCU sets its internal flag and starts fault reaction functions.
5	MCU Fault Reaction	The MCU starts fault reaction functions to isolate the battery pack from the load. These functions may include: sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state.	Shuts off power FETs clearing DFET EN (0x24.1) and/or CFET EN (0x24.0)

Table 11. Charge Overcurrent (COC) Detection Mechanism (Cont.)

Step	Operation	Description	RAA489206
Redundant Channel: MCU Verification of External OT Condition and BFE Fault Reaction			
1	Primary Channel: BFE Detection and Fault Reaction	The BFE checks the COC condition. If COC fault is detected, the BFE initiates fault reactions to isolate the battery pack, and outputs an alert. Fault reactions functions may include turning off cut-off FETs, and/or blowing up a fuse. BFE fault reactions ensure battery isolation in case of MCU failures.	Automatic FETs control: Set FCDC (0x0E.2) to enable automatic power FETs control. Clear COCF MASK (0x83.4) to enable ALERT pin assertion on a fault detection.
2	Redundant Channel 1: MCU COC Detection using BFE measurements	The MCU reads the BFE register containing measurement of the voltage across the sense resistor. The MCU converts its value to current and sets its COC flag if it is above the programmed COC_{th}.	Read I_{PACK} Voltage (0x52-0x53) and convert its value to signed voltage $V(I_{PACK})$ as specified in Section 5.3.6 of the datasheet. Calculate the I_{PACK} current as: $I_{PACK}[A] = \frac{V(I_{PACK})}{R_{SENSE}}$ Where R_{SENSE} is the sense resistance in Ohms. Set MCU DOC flag if $I_{PACK}[A] \geq I_{COCth}$
2	Redundant Channel 2: MCU ADC	MCU Implementation	The MCU triggers an ADC conversion, reads its ADC register and transforms the value to voltage. The MCU converts the voltage value to current as $I_{PACK}[A] = \frac{V_{ADC}}{R_{SENSE}}$ Set MCU DOC flag if $I_{PACK}[A] \geq I_{COCth}$
3	Redundancy Check		The MCU checks its internal COC flag. If it is set, the MCU initiates fault functions such as sending signals to cut-off FET drivers to turn them off, blowing a fuse, and forcing the charge pump to the off state. The MCU outputs an alert to notify the application.

3.5.3 SM8: Discharge Short-Circuit Detection

The BMS detects Discharge Short-Circuit (DSC) when the magnitude of the pack current is above user-programmed threshold DSC_{th}.

3.5.3.1 Implementation Description

Discharge currents produce a negative voltage across the sense resistor. Therefore, the BFE reports the negative I_{PACK} voltage while the battery pack discharges. For short-circuit detection, the BFE uses an analog comparator, so the fault detection is not subject to the execution of the Scan All command. The BFE sets its DSC fault flag when the magnitude of the discharge current exceeds DSC_{th} beyond a chosen duration of time (see the 0x0C - DSC Delay section of the *RAA489206 datasheet* for further information) and may assert an Alert pin connected to the MCU to indicate the presence of the fault.

3.5.3.2 Recommended Usage

The implementation of this SM relays on the reliability of the analog comparator featured by the RAA94206 BFE. Figure 22 shows the implementation of the untested single channel architecture. Table 12 details the implementation.

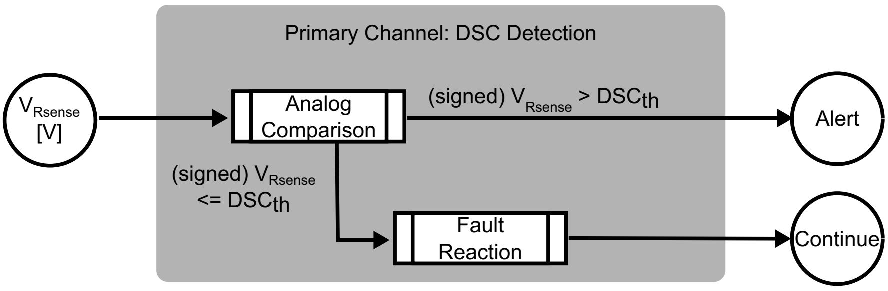
Primary Channel: DSC Detection
V_{Rsense} [V]
Analog Comparison
(signed) V_{Rsense} > DSC_{th}
Alert
(signed) V_{Rsense} <= DSC_{th}
Fault Reaction
Continue

Figure 22. Single-Channel Untested Implementation of Discharge Short-Circuit Current (DSC) Mechanism

Table 12. Discharge Short-Circuit (DSC) Detection Mechanism

Step	Operation	Description	RAA489206
Primary Channel: DSC Detection by BFE Condition Check and MCU Fault Reaction Function			
1	Analog Comparison	If the current sense voltage is more negative than the DSC threshold for the time set by DSC delay, the BFE sets its DSC fault bit and starts reaction functions	DSC Threshold (0x0A) DSC Delay (0x0C) DSCF (0x83.2)
2	BFE Fault Reaction	The BFE shuts both CFET and DFET and stops System Scan, and triggers a transition to IDLE mode. It may assert the ALERT pin.	Clear DSCF MASK (0x83.2) to enable ALERT pin assertion on a fault detection.

3.5.4 SM9: Communication CRC

The BFE detects CRC faults on commands from the MCU and the MCU detects CRC errors in the BFE response.

3.5.4.1 Implementation Description

Write and read commands, and their responses include CRC bytes to ensure the integrity of the data being sent to and received from the BFE. The CRC is calculated by the sending part and added to the packet to be delivered. The receiving entity calculates the CRC value of the received data and compares the result with the bytes designated to contain the CRC data. If the receiving unit is the MCU, a mismatch of the values sets a CRC fault flag and triggers corrective measures such as retrying to send the command. If the receiving unit is the BFE, a CRC error is indicated by sending back a Negative Acknowledgment (NAK) response to the MCU.

The test mechanism induces CRC checksum error detection in the BFE by sending a command with a deliberately incorrect CRC. Correct handling of this condition is indicated by the NAK response from the BFE.

3.5.4.2 Recommended Usage

Figure 23 shows the implementation of the tested single channel for CRC communication when the BFE receives a command from the MCU. Figure 24 shows the equivalent mechanism when the BFE delivers its response and the MCU verifies the CRC of the received data. This mechanism assumes the CRC sent to the BFE is correct and includes a loop to retry to send the command if a wrong CRC is received in the BFE response. If the number of retry attempts is greater than a given maximum number, the mechanism generates an alert that indicates that either the CRC mechanism of the BFE or communication interface is failing.

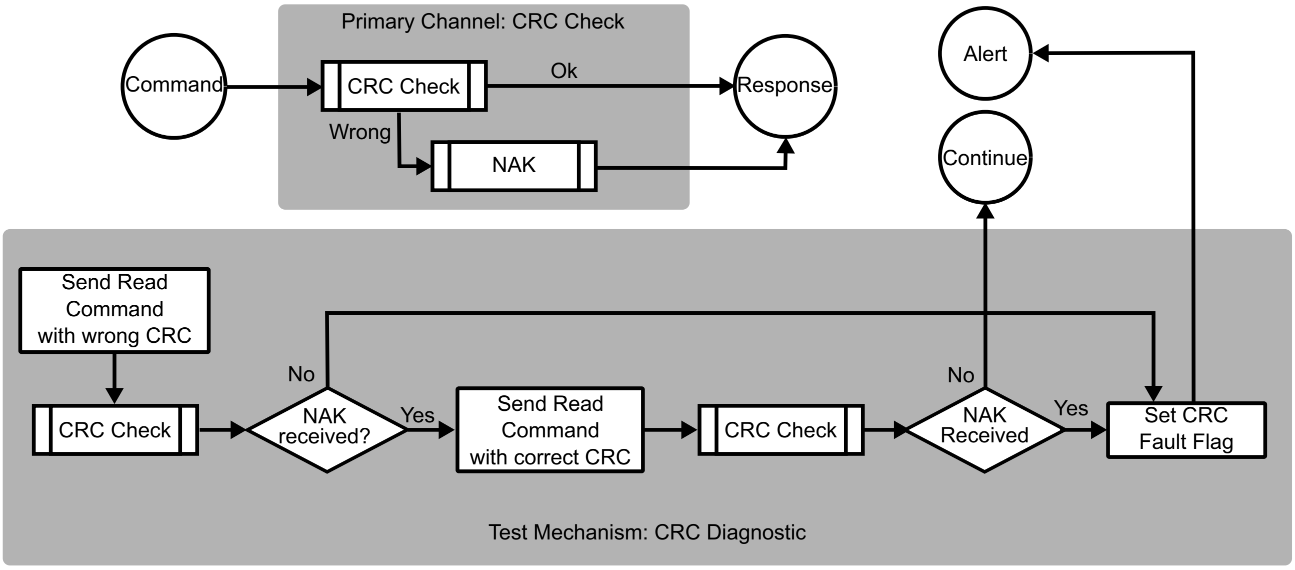
Primary Channel: CRC Check
Command
CRC Check
Ok
Response
Wrong
NAK
Alert
Continue
Send Read Command with wrong CRC
CRC Check
No
NAK received?
Yes
Send Read Command with correct CRC
CRC Check
No
NAK Received
Yes
Set CRC Fault Flag
Test Mechanism: CRC Diagnostic

Figure 23. Single-Channel Tested Implementation of Communication CRC Mechanism at the BFE

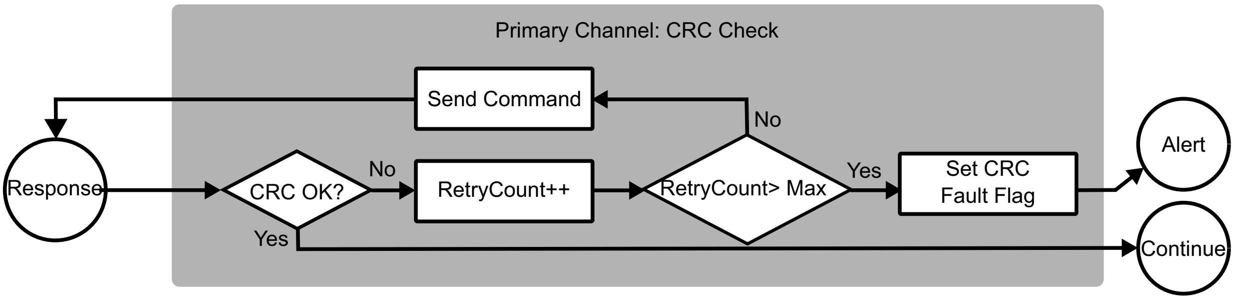

Figure 24. Single-Channel Implementation of Communication CRC Mechanism at the MCU

Table 13. CRC Communication Mechanism

Step	Operation	Description	RAA489202	RAA489206	RAA489204
Primary Channel: CRC Communication at the BFE					
1	Command	The BFE receives a command that contains the CRC bytes specified for the communication interface between the MCU and the BFE	CRC over I^{2}C. 8-bit CRC. Minimum Hamming distance of 4 Use slave address (7-Bit Binary) 1010 110	CRC over SPI 16-bit CRC Use the slave address 0x4E	CRC over SPI 16- and 32-bit CRC Minimum Hamming distance of 4
2	CRC Check	BFE Implementation	The CRC calculates the CRC of the received data and compares the value with the CRC sent by the MCU. If no CRC fault is detected, the BFE sends to the MCU the response to the command containing the corresponding CRC. Otherwise, NAK is sent as response.		
3	NACK	If the BFE detects mismatch between the received CRC and the CRC internally calculated, it send back a NAK	NACK of the I^{2}C interface. ALERT pin is asserted.	The BFE holds the MISO high for the entire read back sequence	The BFE returns the address 0xD1. The FAULT pin is asserted

Table 13. CRC Communication Mechanism (Cont.)

Step	Operation	Description	RAA489202	RAA489206	RAA489204
4	Response	BFE Implementation	The response containing either the requested data (for read commands) or NAK is sent to the MCU.		
Test Mechanism: CRC Diagnostic					
1	Send Read Command with wrong CRC	MCU Implementation	The MCU selects a read command and sent it to the BFE containing a wrong CRC value. This intends to induce CRC error detection in the BFE.		
2	CRC Check	BFE Implementation	The BFE checks the received command as described in the primary channel.		
3	NAK verification	MCU Implementation	The MCU verifies whether an NAK is received as BFE response. If no NAK is received, the MCU sets its CRC fault failure and report failure of the CRC communication mechanism.		
4	Send Read Command with correct CRC	MCU Implementation	The MCU send a read command with the correct CRC value.		
5	CRC Check	BFE Implementation	The BFE checks the received command as described in the primary channel.		
6	NAK verification	MCU Implementation	The MCU verifies whether an NAK is received as BFE response. If a NAK is received, the MCU must report failure of the CRC communication mechanism. Otherwise, the normal operation flow continues.		
Primary Channel: CRC Communication at the MCU					
1	Response	MCU Implementation	After successful verification of the MCU command, the BFE sends back its response including the calculated CRC		
2	CRC Check		The MCU calculates internally the CRC from the received data and verifies if it matches the CRC of the BFE response.		
3	CRC is not OK		If the BFE detects mismatch between the received CRC and the CRC internally calculated, and attempts to resend the command.		
4	Retry		If a given maximum number of attempts to send successfully the command has not been reached, the MCU tries to send the command again.		
5	Maximum number of attempts is reached		If the maximum attempts number is reached, the MCU sets its CRC Fault flag, indicates an alert to notify the application.		

3.5.5 SM 10: Communication Timeout

The MCU detects a time out waiting for a response from the BFE.

3.5.5.1 Implementation Description

For commands that require a response, the MCU waits long enough for a response from the BFE, but should set a fault flag if that response does not come within the expected time limit. In stacked configuration using the RAA489204, there is an additional timeout adopted by the stack. Each device waits for a response from the device above. If no response is detected within the specified timeout, the detecting device reports a communication failure to the device below in the stack until the master device and the MCU are reached. In this configuration, the MCU sets the fault flag if either the failure notification or no response is received from the stack. The reaction of the MCU to a Communication Timeout event can be retrying to send the command as described in the CRC Communication SM.

Regarding the test system for diagnostic of the safety function, it is not possible to force communication timeout fault. Therefore, the architecture adopted for this SM is the single channel untested pattern.

3.5.5.2 Recommended Usage

Figure 25 shows the single channel untested architecture for the communications timeout, which is entirely implemented in the MCU. Table 14 details the implementation.

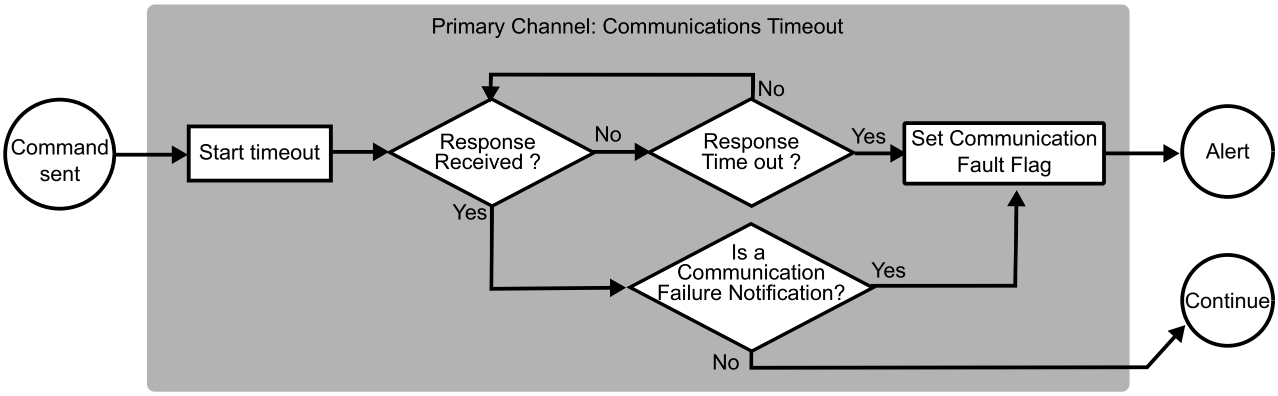
Primary Channel: Communications Timeout
Command sent
Start timeout
Response Received ?
No
Yes
Response Time out ?
No
Yes
Set Communication Fault Flag
Alert
Is a Communication Failure Notification?
Yes
No
Continue

Figure 25. Single-Channel Untested Implementation of Communications Timeout Mechanism

Table 14. Communications Timeout Mechanism

Step	Operation	Description	RAA489202	RAA489206	RAA489204
Primary Channel: Communications Timeout					
1	Command Sent	MCU Implementation	The MCU sends a command to the BFE for which a response is expected.		
2	MCU Timeout		The MCU sets the timeout applied to wait for the response of the BFE, and starts the internal timer that indicates the time since the command was delivered to the BFE.		
3	Response Verification		If the response is not received within the time limit or a Failure Communication Notification (for stacked devices) is received, the MCU sets its Communication Fault flag and indicates an Alert to notify the application. The MCU can also retry to send the command as in the CRC Communication SM (Table 13). If the response is received within the defined timeout interval, the process continues normally.		

3.5.6 SM 11: Communications Watchdog

The BFE stops the current operation and shuts down to a safety state if its communication watchdog timer expires.

3.5.6.1 Implementation Description

Renesas BFEs feature programmable communications WatchDog Timer (WDTs) that resets each time a valid communication is received. The communications watchdog primarily protects against loss of communication from the MCU, so that a device that has lost communications always transitions to a safe state that protects the battery pack. If required, the watch dog can be tested by setting a short watchdog timeout and allowing the watchdog to expire. The safe state of the target BFE is then confirmed by communicating with the BFE to receive a Communications Failure notification (RAA489204), or verifying the BFE has transitioned to Low Power mode (RAA489220 and RAA489206).

The Communications Watchdog mechanism addresses the need of both the MCU and the BFE to set a safe state if the communication between them fails. The Communications Timeout mechanism (SM 10) is made from the

MCU perspective, whereas the Communication Watchdog enables the BFE to accomplish its main task of keeping the battery pack in safe state despite of the loss of the communication with the MCU. Moreover, the implementation of both mechanisms in parallel constitute a redundant channel implementation for the communication safety function.

3.5.6.2 Recommended Usage

Figure 26 depicts the single channel tested architecture of the Communications Watchdog mechanism. The value of the minimum programmable Watchdog Timer communications timeout period must be carefully considered when performing the test of the mechanism. The shortest timer of the RAA489204, for example, is 1s, which might be too long time to be performed during the system FTI. The RAA489220 and RAA489206 have 128ms and 100ms minimum WDT period, respectively, so the test mechanism may meet the FTI restriction. It is then important ensure the test mechanism is executed only during the OFF state of the system, and interrupted on demand of the system activity. Table 15 details the mechanism implementation.

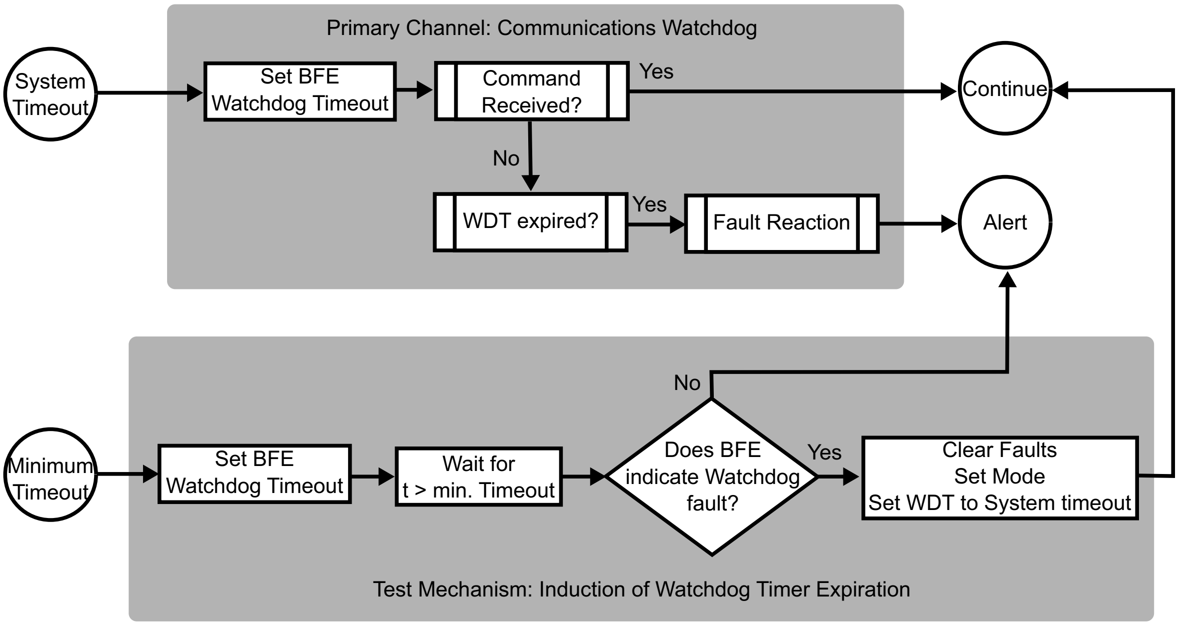
Primary Channel: Communications Watchdog
System Timeout
Set BFE Watchdog Timeout
Command Received?
Yes
Continue
No
WDT expired?
Yes
Fault Reaction
Alert
No
Minimum Timeout
Set BFE Watchdog Timeout
Wait for t > min. Timeout
Does BFE indicate Watchdog fault?
Yes
Clear Faults
Set Mode
Set WDT to System timeout
Test Mechanism: Induction of Watchdog Timer Expiration

Figure 26. Single-Channel Tested Implementation of Communications Watchdog

Table 15. Communication Watchdog Mechanism

Step	Operation	Description	RAA489202	RAA489206	RAA489204
Primary Channel: Communications Watchdog					
1	System Timeout	The application defines a Watchdog according to its safety requirements and the WDT timeout period selections featured by the BFE.	Communication Timeout Selections (0x80.[14:13]): 100ms, 1s, 5s	Communication Timeout Selections (0x1B.[7:6]): 128ms, 512ms, 2048ms, 4096ms. Set Communication Timeout EN (0x1F.1] to enable the WDT	Watchdog/Balance Time Register (0x91) [1, 63] s (1s increment) 2 and 4 min [8, 150] min (8 min intervals). Password-protected configuration
2	Command Reception Verification	BFE Implementation	The BFE waits for the reception of a command to reset the WDT.		

Table 15. Communication Watchdog Mechanism (Cont.)

Step	Operation	Description	RAA489202	RAA489206	RAA489204
3	WDT Expiration	BFE Implementation	If the WDT expires, the BFE starts fault functions and transitions to a safe state		
4	BFE Fault Reaction	BFE Implementation	Set COMMTO (0x10.8) Transition to Low Power Mode, which turns power FETs off.	Transition to Low Power Mode, which turns power FETs off.	Set the WDGF bit, assert the FAULT output, ceases all scanning and balancing activity and enters in Sleep mode
Test Mechanism: Induction of Watchdog Timer Expiration					
1	Set the Minimum Timeout	The MCU selects the minimum timeout period	Communication TO = 100ms (01)	Communication TO = 128ms (00)	WDG[7:0] = 0x01
2	Wait for t > minimum WDT period	MCU Implementation	The MCU waits for more than the configured minimum WDT period		
3	Verification of the WDT fault	The MCU verifies if the BFE reports WDT timeout expiration. If the BFE does not indicate the fault, the MCU generates an Alert signal to notify the application about failure of the WDT timeout mechanism.	Verify COMMTO (0x10.8) is set	Verify the BFE is in Low Power Mode: Read System Mode Register (0x2E) Check 0x2E.[7:6] = 10	Send HRESET/WAKEUP Precursor Command (0xDE) Send Wakeup Command (0xD5) Read WDTF flag (0x80.3)
4	Clear Faults, Set System Mode and Set WDT to System Timeout	The MCU executes a command to clear the fault condition in the BFE and sets the mode to the state the BFE was before performing the test.	Set Clear All Faults Bit (0x40.6). Mode transitions automatically to IDLE on command reception. Set Communication Timeout Selections (0x80.[14:13]) to System WDT Timeout.	Set BFE mode to IDLE or SCAN mode. Set Clear All Faults Bit (0x02.1). Set Communication Timeout Selections (0x1B.[7:6]) to System WDT Timeout	Reset WDGF writing 0x0008 to Fault Status and Setup Registers (0x80). Select system WDT timeout writing the Watchdog/Balance Time Register (0x91).
5	CRC Check	BFE Implementation	The BFE checks the received command as described in the primary channel.		

4. Conclusion

The growing demand of battery-powered products in industrial applications with safety requirements is pushing Battery Management Systems into the implementation of Functional Safety (FuSa) mechanisms. As fundamental component of a BMS, the Battery Front End (BFE) must provide functionalities to enable the implementation of such mechanisms. This manual provides fundamentals of safety concepts and architectures, and the guidelines to implement FuSa mechanisms in BMSs featuring Renesas BFEs. The article reviews FuSa terms and definitions, describes the architecture patterns commonly used in FuSa mechanisms, and provides examples of their implementation featuring three Renesas BFEs that are intended to be used in BMSs of low, medium and high power applications.

5. References

1. International Institute for Internationalization, *ISO 13849-1 Safety of Machinery - Safety-related parts of control systems Part 1: General Principles for Design*, ISO, 2015.
2. Y. Luo, A. K. Saberi, T. Bijlsma, J. J. Lukkien and M. van den. Brand, *An Architecture Pattern for Safety Critical Automated Driving applications: Design and Analysis*, in Annual IEEE International Systems Conference (SysCon), Montreal, Canada, 2017.
3. Deutsche Gesetzliche Unfallversicherung (DGUV), *Functional safety of machine controls - Application of EN ISO 13849,* IFA Report 2/2017e, 2017.
4. J. Hedberg, A. Soederberg and J. Tagehall, *How to design safe machine control systems - a guide to EN ISO 13849-1,* SP Research Institute of Sweden, 2011.

6. Revision History

Revision	Date	Description
1.00	Sep 19, 2022	Initial release.

IMPORTANT NOTICE AND DISCLAIMER

RENESAS ELECTRONICS CORPORATION AND ITS SUBSIDIARIES (“RENESAS”) PROVIDES TECHNICAL SPECIFICATIONS AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for developers skilled in the art designing with Renesas products. You are solely responsible for (1) selecting the appropriate products for your application, (2) designing, validating, and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. Renesas grants you permission to use these resources only for development of an application that uses Renesas products. Other reproduction or use of these resources is strictly prohibited. No license is granted to any other Renesas intellectual property or to any third party intellectual property. Renesas disclaims responsibility for, and you will fully indemnify Renesas and its representatives against, any claims, damages, costs, losses, or liabilities arising out of your use of these resources. Renesas' products are provided only subject to Renesas' Terms and Conditions of Sale or other applicable terms agreed to in writing. No use of any Renesas resources expands or otherwise alters any applicable warranties or warranty disclaimers for these products.

(Rev.1.0 Mar 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/