Advanced Safety of RAA489204 Battery Front End

The 14-cell stackable battery front end IC, RAA489204, has integrated system diagnostics for all the key functions and specialized commands so that the development of diagnostic software can be simplified. This application note provides relevant safety-specific information, a review of safety features, and procedures for operating the functional safety of a battery management system. The document assists system designers to achieve a level of performance required in safety standards for industrial applications.

Contents

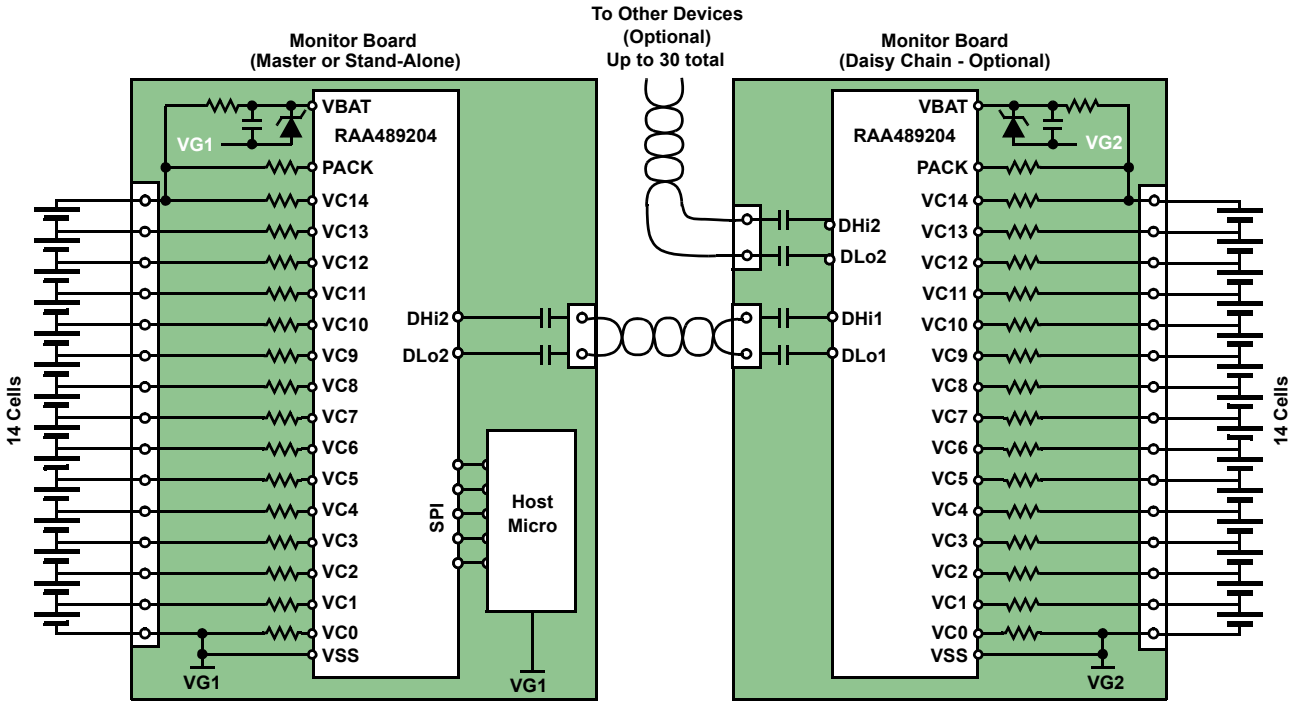

Figure 1. RAA489204 Typical Application

1. Product Overview

RAA489204 is an industrial-grade battery front-end IC that supervises up to 14 series connected cells. It can operate in standalone mode or with up to 30 devices in a stack, monitoring up to 420 battery cells in total from all standard Li-Ion chemistries. It has up to six external temperature monitoring inputs and two general-purpose I/O pins. It is controlled by an external microcontroller unit (MCU) through a high-speed SPI interface. Inside a stack, the bottom device acts as a master for the vertical daisy chain communication, which is secured by a robust 2-wire communication system. The 14-bit ADC provides accurate high-resolution voltage and temperature measurements helping in the implementation of State of Charge (SOC) algorithms and battery health optimization. There is also a built-in averaging mechanism. In large battery packs, the signed cell voltage measurement provides a detection mechanism for reverse installed cells. The ability to measure negative cell voltages allows applications where multiple small battery packs, connected in series with bus bars, are monitored by a single BFE. The RAA489204 offers comprehensive cell balancing features. You can select between internal cell balancing, which significantly reduces the number of external components and saves PCB area, or external cell balancing, which allows higher balancing currents and better input filter performance. Three cell balancing modes are available: Manual, Timed, and Auto Balance Mode. The last two relieve the MCU and prevent any hazardous total battery drain and unrecoverable damage of cells when cell balancing is enabled but the control unit is corrupted by a software issue or any external factor.

The RAA489204 has extensive system diagnostics for all key functions and uses a high-security communication protocol, tolerant to EMC and transients. The device is an industrial version of the automotive ISL78714 BFE and thus brings the benefits of comprehensive safety mechanisms typically required to comply with the relevant automotive standards. Nevertheless, it is not intended for such applications. The typical applications of RAA489204 are industrial electric mobility battery packs; backup batteries; energy storage systems; portable and semi-portable equipment.

2. On-Chip Safety Mechanisms

The RAA489204 BFE contains built-in on-chip diagnostic and safety mechanisms that facilitate the effectiveness of diagnostic procedures and therefore increase the average diagnostic coverage of the battery management system. They are summarized into two groups: automatic and command-driven. The automatic safety mechanisms run with no host intervention. They include:

- **Power-good range check –** The BFE continuously performs monitoring of the levels of all internally stabilized supply and reference voltages. It does not require any interaction with the MCU.
- **Daisy chain communication -** The high-speed communication between BFE devices inside the stack is provided by robust daisy chain hardware. It uses differential, AC-coupled signaling with either capacitive or transformer coupling, providing full EMI and transient immunity.
- **CRC engine –** The high-speed SPI and daisy chain communications are secured by standard 16-bit and 32-bit CRCs that are parts of the communication protocol. A checksum mismatch generates an automatic NAK response and generates a fault so that the MCU can identify a failure. Also, after receiving the header the MCU knows exactly how many bytes to clock out to receive the whole packet and the integrity of this data can be verified.
- **Communication timeout -** For all commands that require a response, each device in the stack waits for the response from the device above. If this response is not received within a timeout period, the device reports a communication failure to the device below in the stack until the master device and the MCU are reached. This is part of the communications integrity checking. It typically indicates a break in the daisy chain or a component failure.
- **Enlarged internal communication buffer –** The BFE has an enlarged communication buffer to manage long multiple registers read when the MCU cannot service the communication channel fast enough. In that way, the master BFE device does not overflow, and communication is not compromised.

The command-driven safety mechanisms require sending a command from the host to perform the fault check. They include:

- **Memory checksum –** Two mechanisms for the detection of memory corruption are available. The first one protects the system registers, that are loaded from EEPROM into the shadow registers (such as factory calibration). The checksum is internally calculated and compared during the diagnostic procedure. The secondary mechanism protects page 2 of the volatile memory where the configuration registers values are stored so that the temporary device setting is secured. The checksum is calculated and compared internally but these actions are triggered by the MCU.
- **Scan add-ons –** The scan procedures incorporate self-check mechanisms that include the open-wire checks of power supply pins, memory checks, and multiplexer tests. The BFE offers a wide variety of scan commands that are sent by the MCU or automatic monitoring feature using a complete scan. For more details, see the product datasheet.
- **Watchdog function –** The watchdog is another part of the communications integrity checking mechanism. The timer resets after the device has received a valid communication packet and inhibits any scan continuous or balancing activity before putting the device into sleep mode. When the BFE is already in sleep mode but simultaneously balancing the pack, the watchdog timer is still operational. It protects the battery pack if communication is lost or the MCU malfunctions. Renesas highly recommends the usage of the watchdog function.
- **Measurement averaging –** The BFE contains an averaging module for cell voltage and temperature measurement. After a scan or measure command, it forces the device to make multiple consecutive scans that are automatically added up and the averaged result is written in the relevant registers. This approach minimizes measurement inaccuracies in noisy environments and helps to work with loads with high current transients.
- **Fault registers write protection –** The BFE fault registers are protected from accidental clearing and ignoring a fault flag. Modification of the content of any of the fault registers requires writing 1s to clear one or more flags or sending a preceding command to unlock a direct register write.

More information about the fault diagnostic functions of RAA489204 and their application is available in the Fault Diagnostics section in the product datasheet.

3. System-Level Safety

System-level safety is divided into two methods: inline diagnostics and diagnostic procedures. This classification is based on how the diagnostic code is integrated into the control software.

3.1 Inline Diagnostics

Inline diagnostics take place inside functions that directly interact with the BFE to perform control (such as voltage or temperature measurement, balance control, device configuration). They are an instrument for increasing reliability and achieving higher diagnostic coverage. They are fragments of code placed inside the normal functions that carry out a quick verification of certain actions or comparison of parameters. For example, reading the registers between addresses 9'h041 and 9'h050 returns all cell voltages and the pack voltage. A quick inline diagnostic of the measurement network (except the ADC) would be comparing Vpack with the sum of all cell voltages. To do so all values must be converted to comparable units as the numbers written in measurement registers that can be related to physical values using the equations from the product datasheet and the pack voltage must be compensated from the input bias current. This technique can detect a parametric failure of only one or a group of measurement inputs.

Despite the highly reliable SPI and daisy chain communication protocol, controlled by both MCU and each BFE using a CRC, a physical transfer of data packet through the SPI does not guarantee successful register write inside the target device memory or command reception. Numerous factors can interfere with and disturb the communication, forcing a NAK or communication failure response. However, it can be challenging for the MCU to detect the exact moment of appearance for such a fault and hook it up to the particular command that needs to be

resent. Therefore, applying a couple of techniques as a verification tool increases the diagnostic coverage of the system.

3.1.1 Response Monitoring

Some commands like SLEEP or BALANCE ENABLE cause a direct ACK (acknowledgment) response from the master BFE. It is sent back within an expected time window that depends on the stack size and command specifics. The lack of response implies a communication failure and command re-transmission. A repeated failure should be interpreted as a general system fault and lead to communication recovery procedure, general system reset, or pack disabling.

3.1.2 Register Write Verification

An important inline diagnostic tool is the register write verification. The verification flowchart is given in Figure 2. The write command is followed by a read command for the same address and a comparison of both values. Keep in mind that verification of a register that contains read-only bits requires a logical conjunction with a bitmask. It ignores the states of the bits that cannot be modified. If values mismatch, new write attempts should be made until reaching a predefined maximum number and registering a fault. The block transfer capabilities of RAA489204 for working on multiple addresses within a single data transfer imply optimization of communications, and register block writes can be followed by block reads for verification purposes. Write commands cannot be broadcasted and always target a particular device from the stack, so that verification is accomplished for a particular register or group of registers in a particular device.

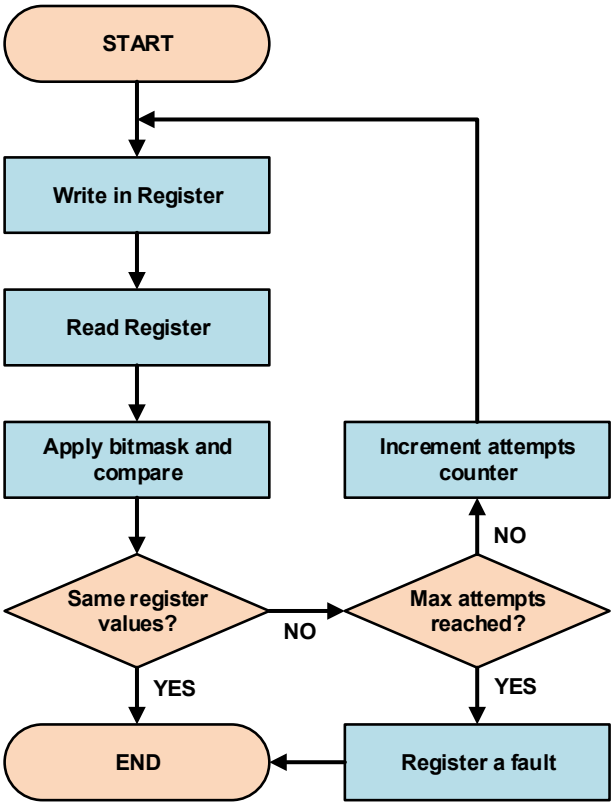

Figure 2. Register Write Verification Flowchart

3.1.3 Verification of Command Reception

Some commands do not generate a direct response from the target device (such as Scan, Measure, Balance Enable, and Scan Continuous Enable). The verification mechanism includes checking particular bits or values that are directly affected after the execution of such commands. Looking at the cell balancing control, there are two ways to enable it. You can directly broadcast the Balance Enable command to all BFEs within the stack to trigger the desired (pseudo) simultaneous action or modify the 9'h090.5 BEN bit in each individual Cell Balance Setup register. The first approach is appropriate and resource-saving for large battery packs. However, both are followed by verification of the state of the BEN bit in the Cell Balance Setup register of each device similarly to the described method in the previous section. On the other hand, the Scan and Measure commands do not result in a change of any bit inside status or setup registers. RAA489204 contains scan and diagnostic counters that increment after command completion and allow confirmation of execution. Although these commands can be broadcasted, a verification must be accomplished for each device from the stack. The verification flowchart is given in Figure 3. The scan counter is read before and after the transmission of the scan command. The second counter must be read after the scan command was executed, which is determined with a time delay. Keep in mind that the counters are 6-bit and wrap to zero when overflowed. If both values do not match, the scan command should be resent until the maximum number of attempts is reached and a fault is registered. The same approach is used for the diagnostic counter and the commands affecting it. For more information, see the product datasheet. The application of the described techniques is important to achieve advanced safety levels inside battery packs with stacked BFEs that operate in noisy industrial environments.

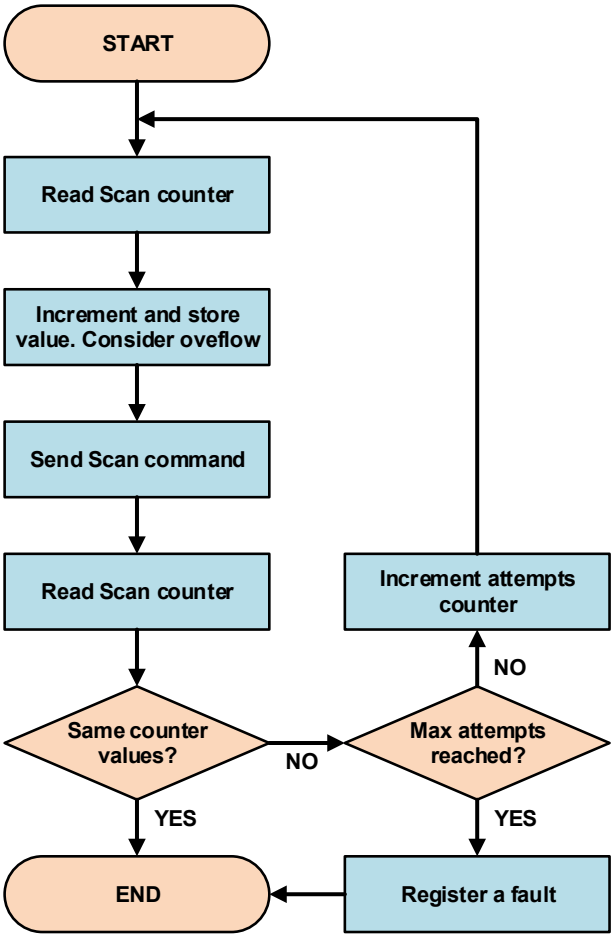

Figure 3. Scan Command Confirmation of Execution Flowchart

3.2 Diagnostic Procedures

Diagnostic procedures are specialized functions that check the performance and integrity of various parts of the system by running tests and discovering faults and issues. They are placed in the battery management system control unit – in most cases an MCU. Examples for diagnostic procedures are a damaged ADC giving wrong measurements of cell voltages or broken cell balancing circuitry resulting in hazardous situations and a battery pack with severely reduced capacity. The organization of internal processes and the dedicated test commands facilitate the diagnostic procedures. Fault conditions detected on upper stack devices in some cases may not assert the master device Fault pin. Therefore, monitoring it is insufficient for in-time faults discovery. Moreover, monitoring all Fault pins requires galvanic insulation and adds cost to the system. Renesas recommends that the host microcontroller checks the Fault Status register contents of all devices whenever a Fault Response is received from any device. Also, to prevent the accumulation of undetected faults and comply with higher fault detection and reliability category, the following diagnostic procedures must be periodically called in addition to using the inline diagnostic approaches:

- **Broadcast a memory check command to all devices from the stack to generate and compare the checksum of the volatile memory -** must be combined with a fault check as the output from a checksum mismatch is raising a flag inside the Fault Status register.
- **Device internal self-test** - Includes testing and looking for a malfunction of internal blocks such as the ADC, MUX. The internal self-test consumes time and inhibits all other processes. This procedure should be called with medium to low frequency, (for example, every 100 seconds).
- **Device external circuitry test.** This includes open-wire checks of cell, battery, supply and temperature measurement inputs, and testing the external cell balancing circuitry. This procedure consumes time, energy, and inhibits all other processes. It should be called with the lowest frequency (for example, every 1000 seconds).

The described order and time intervals are indicative and must be modified and fitted according to the exact application specifics.

3.2.1 ADC and MUX Test Procedure

RAA489204 supports commands that facilitate verification of the two multiplexers and the ADC. The described test sequence together with an open-wire check are needed to assure correct measurement of cell voltages and temperatures. The Device Setup 2 register contains configuration bits 9’h093.14 FFSP and 9’h093.15 FFSN that force the ADC inputs to full scale positive or negative values for cell scan and external temperature readings. The test procedure flowchart is given in Figure 4. Initially, the ADC is forced to full scale positive by setting 9’h093.14 FFSP bit into Device Setup register and followed by Measure Cell1 and ExT1 Voltage Commands. It is not necessary to scan and read all cells and external temperature inputs as the multiplexers are not used when force saturating the ADC. Note that comparators are still operating and would probably detect an overvoltage and over-temperature faults. To avoid this false detection, the relevant bits in the Overvoltage, Undervoltage, and Over-Temperature Fault registers must be cleared. Then, Cell1 and ExT1 registers containing the saturated voltage measurements are read and compared with the expected values. Keep in mind that they are different for signed cell voltage and unsigned temperature reading. For more information, see the product datasheet. If the values do not match, a fault is registered and the system takes the appropriate actions such as restarting the system or disabling the pack. The same sequence is repeated for the ADC saturated to full-scale negative. Afterward, the Device Setup 2 register is reverted to proceed with the test of the multiplexers. There is a dedicated Scan Cell MUX Command that runs an automatic internal test of the cell voltage multiplexer. If a MUX issue is discovered, the 9’h080.14 CMX bit in the Fault Status register is set. Therefore, after enough time to ensure that the multiplexer test has finished, the CMX bit must be checked. The temperature multiplexer is tested when a Scan Temperatures Command is sent as it includes this particular test. In the same manner, the 9’h080.13 TMX bit in the Fault Status register must be monitored.

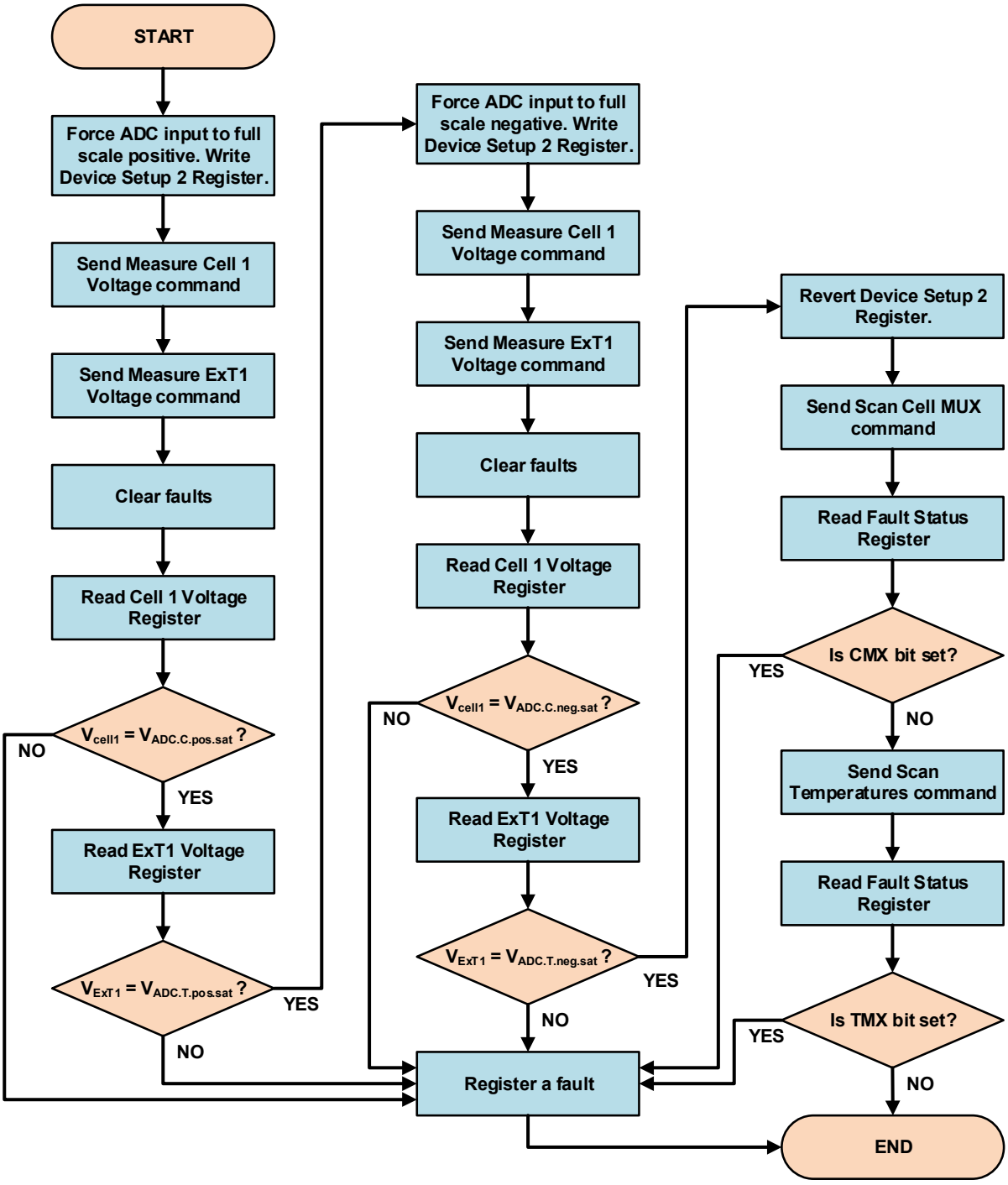

Figure 4. Internal Device Test Flowchart

3.2.2 External Balancing Circuitry Diagnostic Procedure

The external balancing circuitry can be tested to verify the ability of the system to balance the cells. To do so, the cell balancing current is detected by measuring the voltage drop across each balancing resistor. This method is trustworthy but requires a special circuitry and connection of the cell voltage measurement inputs, which is shown in Figure 5. Another option is to use the cell ESR and measure the voltage drop across it, which is much smaller and might be difficult to detect, especially when cells in parallel are connected, despite the high accuracy of the ADC. For better diagnostics, Renesas recommends using the higher magnitude balancing resistor voltage drop. The test flowchart is given in Figure 6. The first step is to inhibit any automatic background activities such as scan continuous and any cell balancing. The Balance Setup register must be rewritten to set the timed balancing mode, which prevents draining any cell if the procedure is interrupted. Also, you must ensure that cell balancing is not interrupted during any scan activity by clearing the 9'h090.6 BDDS bit. Then, a Scan Voltages Command is sent to measure the initial voltages of all cells while balancing is disabled. All cell voltage registers are read and the values are temporarily stored into a temporary data array. Keep in mind that there must be a time delay between sending scan command and reading values. Next, cell balancing is enabled for all odd cells, followed by Scan Voltages, Balancing Inhibit commands, and read Cell 1-14 Voltage registers to acquire the new values and calculate the voltage drop for all odd cells. Each voltage drop is compared to a predefined limit, representing the minimum possible value for the given hardware, taking into account the cell chemistry, ESR, balancing current, connecting cables resistance, headers resistance, and MOSFET on-channel resistance. The same procedure is repeated for the even cells. Keep in mind that cells 11 and 12 produce a different result from the others. Cell 11 uses an N-channel MOSFET while Cell 12 uses a P-channel. The circuit arrangement produces approximately half the normal cell voltage between VC10/VC11 and VC11/VC12 when balancing is enabled rather than only the voltage drop across the MOSFET induced channel. More information can be found in the Cell Voltage Measurements During Balancing section in the product datasheet. When an enabled balancing circuitry for a given cell is not generating enough voltage drop between the measurement inputs, a fault is registered and the system responds accordingly with limiting the pack performance or totally disabling it. After the test is completed, the cell balancing configuration is reverted and a command is sent to calculate configuration registers checksum and avoid false fault detection on the next memory check. Also, continuous scan and automatic balancing actions are restored.

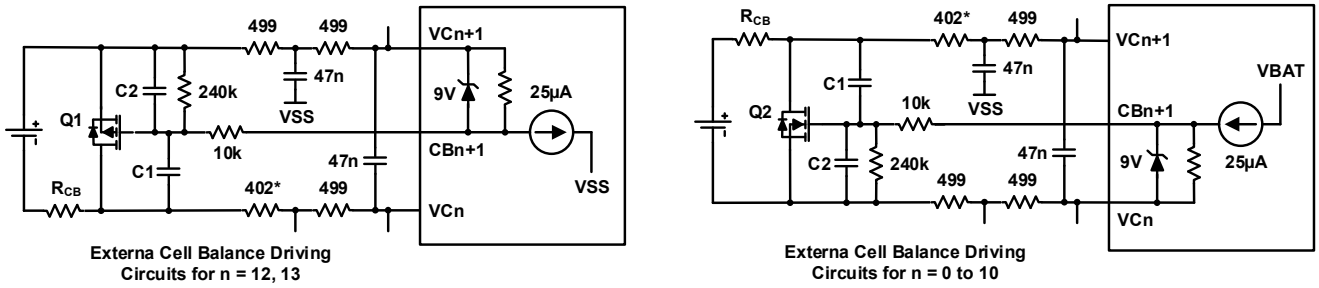

Figure 5. External Cell Balancing Circuitry Facilitating Diagnostics

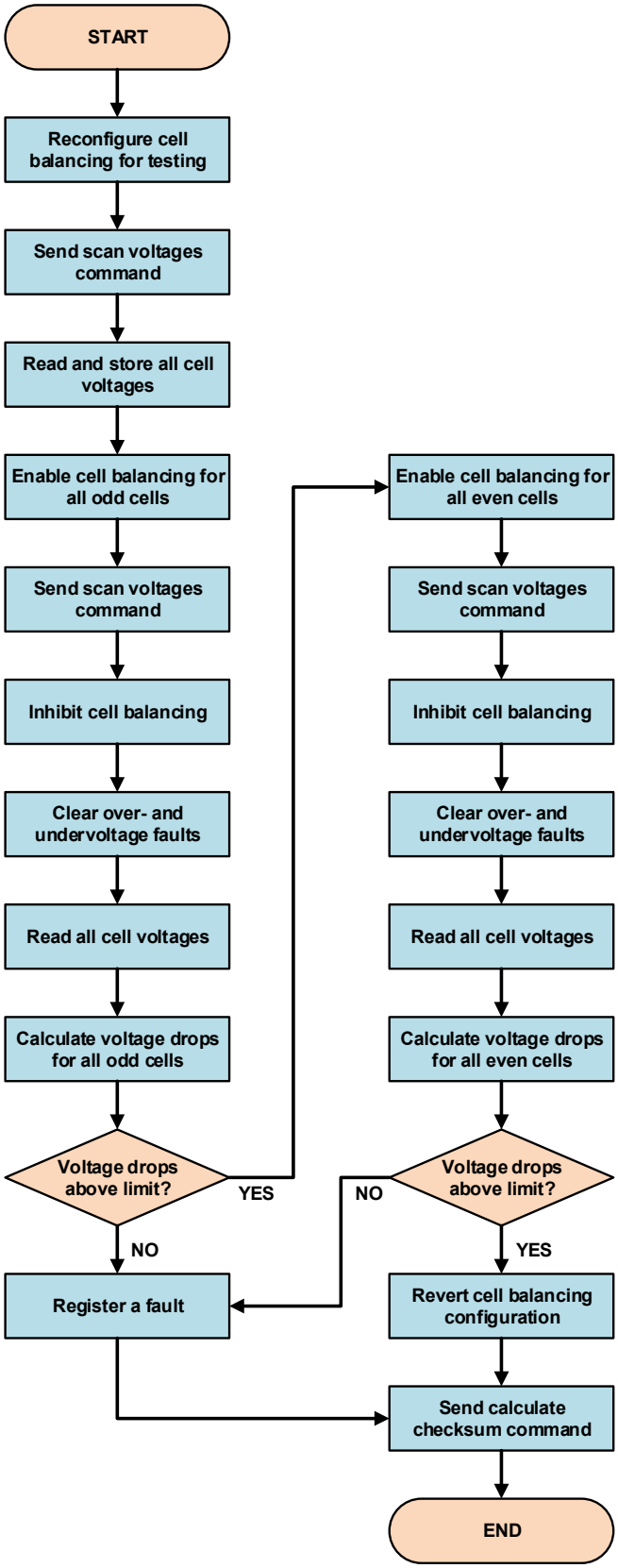

Figure 6. External Balancing Circuitry Test Flowchart

3.2.3 Open-Wire Check Procedure

The complete open-wire check procedure on all measurement inputs is shown in Figure 7. The dedicated Scan Wires Command is sent to test the cells and pack voltage measurement inputs, followed by a Fault Status register read to check if bit 9'h080.7 OW is set. Keep in mind that you must provide the necessary time interval for the scan action to finish before checking the result. The external temperature inputs have internal pull up resistors tied to V_{REF}. An open input results in the ADC being saturated high. This is automatically detected, so that the open-wire check for those inputs is handled by sending a Scan Temperatures Command and then checking bits 9'h084.9-12 OWTn in the Over Temperature Fault register. If any of the open-wire related fault bits is set, a fault is registered, and the system takes corresponding actions.

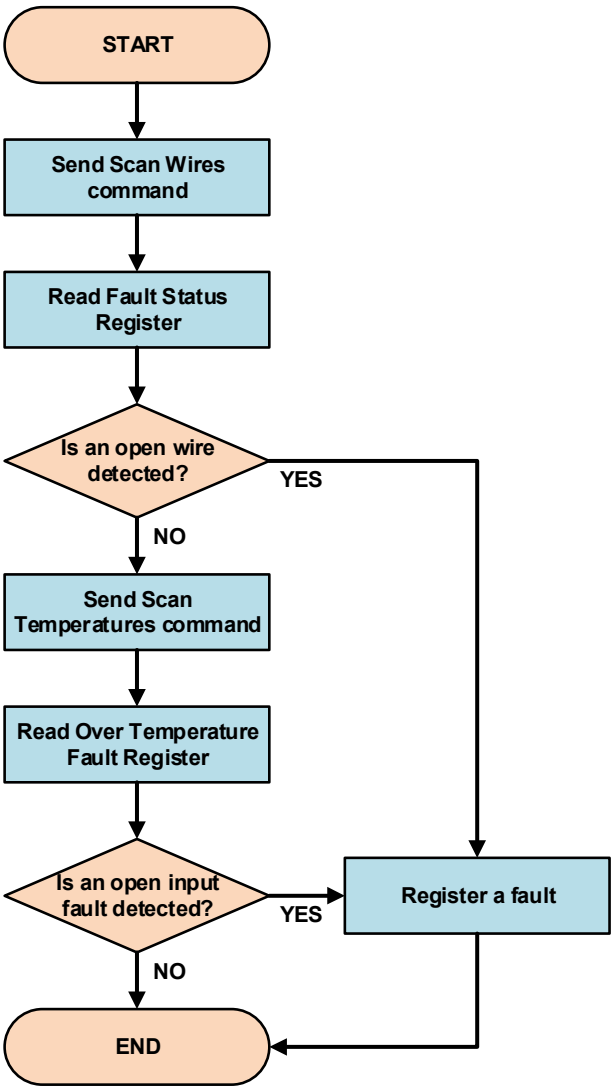

Figure 7. Open Wire Check Flowchart

All described software related diagnostic methods and safety measures are demonstrated in the RAA489204 sample code.

4. Hardware Safety Considerations

When designing a battery management system, there are hardware considerations to follow to facilitate diagnostics, increase the time between failures, and reach a certain level of safety. These considerations comprise the whole design process from circuitry and components selection to PCB routing. Specific failures associated with external components can lead to unsafe conditions in the system. A good example of this is a component that is connected between high-energy signal sources that is having a short circuit. Such a condition can easily lead to component overheating, damaging of the board and other close components. The battery can be drained to dangerous levels, resulting in chemical degradation of electrodes and a hazardous situation. The capacitors connected to the cell monitoring inputs can be considered as an external component with a potential of failure. A short in one of these capacitors would dissipate the whole charge of the battery cell when connected between two adjacent VCn measurement inputs and the charge of the whole battery pack when connected between any VCn measurement input and ground, reducing the voltage to critical levels. Renesas recommends selecting capacitors for the input filter as fail-safe or open mode types. An alternative strategy is to replace each of these capacitors with two in series, having a doubled value. A further consideration is the package sizes of capacitors used in the cell measurement circuits. Board leakage either to ground or cell to cell, which can be associated with small package sizes, can produce measurement errors when reading cell voltages. For the capacitors in the cell measurement circuits, Renesas recommends not using packages smaller than 0603. All voltage measurement inputs of RAA489204 must be protected with RC filters against transients and hot plug events. The series resistor also has a current limiting function. Keep in mind that modifying the recommended filter resistances provided in the datasheet affects the hot plug rating. All the time constants of the input filters for VCn, VBAT, and PACK monitoring inputs must be well-matched so that inputs face the same voltage drifts during transients with high magnitudes, which could damage the ESD structures and other internals. In a case of an open wire on the PACK or the VC0 pin providing a supply current path and allowing the device to operate sufficiently, additional diodes must be placed between pins VC0/VC1 and VC13/PACK. The connection is shown in Figure 8.

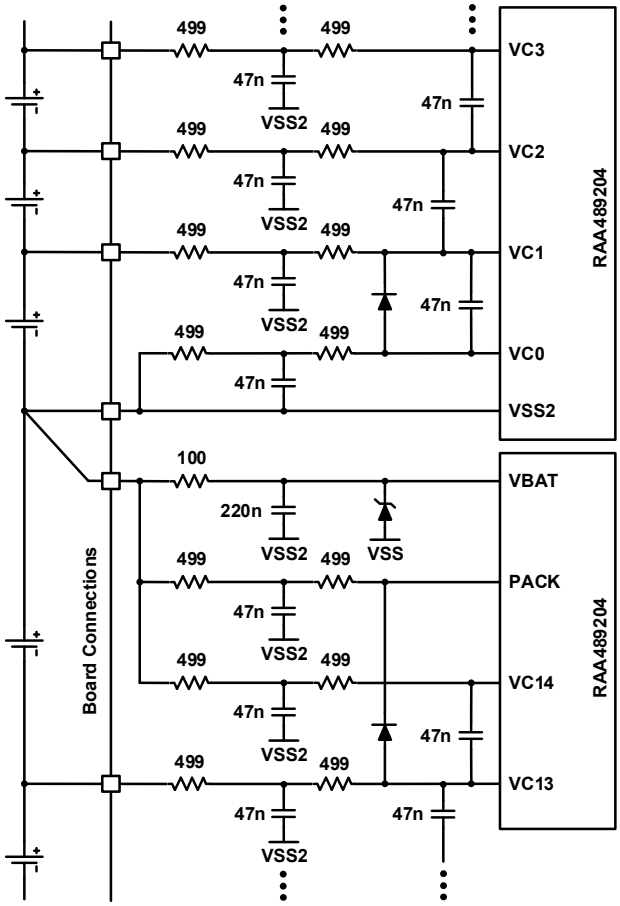

Figure 8. Typical Battery Connection Between Stacked Devices

Note: In the capacitively coupled daisy chain communication, use NPO dielectric type capacitors that maintain performance across temperature and do not jeopardize communications under a changeable operational environment.

RAA489204 provides a means for resetting the part without adding cost to BOM using the Hard Reset command. When the master device receives this command, it sends a special 32kHz signal on the daisy chain to all devices, forcing each of them to toggle the EN pin internally, resetting the analog front end, loading shadow registers from EEPROM, and configuration registers with their default values. This approach increases the safety level of the system because it can reset and restore operation but also leverages vertical daisy chain communication. However, when the master BFE is not responding and cannot generate this signal, the most reliable method remains to use external circuitry as optocouplers to pull down each EN pin.

5. Revision History

Revision	Date	Description
1.00	Mar 15, 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

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/