FuSa in a Nutshell: BMS application with AURIX™ TC4xx

About this document

Scope and purpose

Meeting the functional safety (FuSa) standards in automotive, industrial, and other fields is a challenging subject. This document intends to provide a first set of guidelines for users who are unfamiliar using the AURIX™ TC4xx and PSOC™ 4 HVPA SPM 1.0 microcontroller units (MCU) with focus to functional safety aspects for battery management systems (BMS). This application note is part of a series of documents named “FuSa in a nutshell”, as listed in [1].

Intended audience

This document is intended for all those evaluating the AURIX™ TC4xx and PSOC™ 4 HVPA SPM 1.0 MCUs, including functional safety engineers and application engineers on the customer’s side. This includes designers of safety-related systems who are new to functional safety, want to know more about its applications, understand on how functional safety can be implemented with the support of hardware or looking for details beyond the MCU user manual.

Structure of the document

This document wants to provide a first guidance on the following safety-related arguments, focusing on BMS system and their safety considerations, chip sets for ASIL C or D use cases, and new trends in the field.

Disclaimer

Information provided in this document is for training purposes only and is not to be taken as a blueprint for productive development.

Keypoints

- HV-LV BMS
- BDU
- Battery SoH and SoC

About this product family

Product family

- AURIX™ TC4xx
- PSOC™ 4 HVPA SPM 1.0

Target applications

- Edge AI for batteries SoH, BMS

Table of contents

Table of contents

1 Introduction

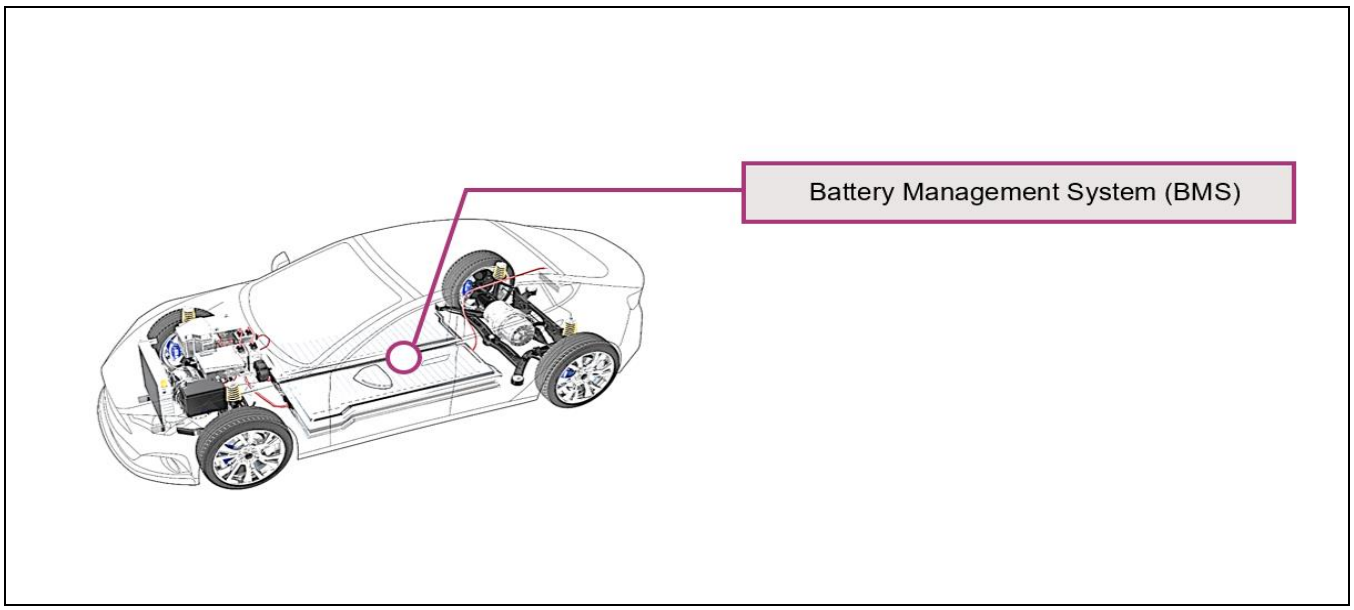

Figure 1 BMS typical position in a modern car

The powertrain system in an electric vehicle (EV) consists of several crucial system-level blocks, including the electric motor, traction inverter drive, DC/DC converter, high-voltage traction battery with its management system (BMS), and the on-board charger (OBC).

The Battery Management System (**BMS**), described in detail in the subsequent sections, is a vital electronics system that provides information about the battery's state, such as temperature, state of health (SoH), and state of charge (SoC).

This system can also manage and control the cells within the battery, using the measured data to avoid malfunctioning of the battery and improve efficiency.

BMS is a key feature in modern cars to ensure:

- Safe battery use
- Highest possible longevity
- Highly efficient energy storage
- Fast charging capabilities

New electric and hybrid cars heavily rely on power supply coming from battery system to implement functional and safety features.

In other words, the BMS operates to optimize and extend the lifetime of the battery. When critical conditions are reached, the control operation becomes a safety operation. There are many ways to implement a **BMS**. For instance, in this document, Infineon provides a high-voltage solution (up to 1000 V) using a cell monitoring and balancing unit (CMU), current sensing unit (PMU), battery management unit (BMU), and battery disconnect unit (BDU). This solution includes a description of all necessary safety features, such as isolated communication and emergency disconnect.

Introduction

The system is able to measure the current, voltage, and temperature of the cells and can deduce the **SoH** and **SoC** of the cell. Sensors transmit the data read on the high-voltage side via an isolated communication. To prevent thermal runaway, a battery-disconnect-unit (**BDU**) can disconnect the battery cell from the supply. To provide these safety features, the **BMS** needs to fulfill the ASIL C or ASIL D requirements, depending on the safety category of the cells used.

To control and balance the single cells, the CMU unit is used. It measures the voltage and the temperature of the cells and operates the balancing between the cells, so that the voltage difference is compensated. The CMU can also undertake diagnostics of cells and their surrounding circuits.

High-voltage batteries are built out of many single cells in series, which inevitably have production variances, such as differences in battery capacity. If cell balancing is not present, the two most unbalanced cells define how much of the battery pack can be utilized in terms of working range. The cell with the highest state of charge (Figure 2 (b) - green cell) will limit the total charge of the whole series, whilst the cell with the lowest state of charge (Figure 2 (b) - red cell) will limit the operating time.

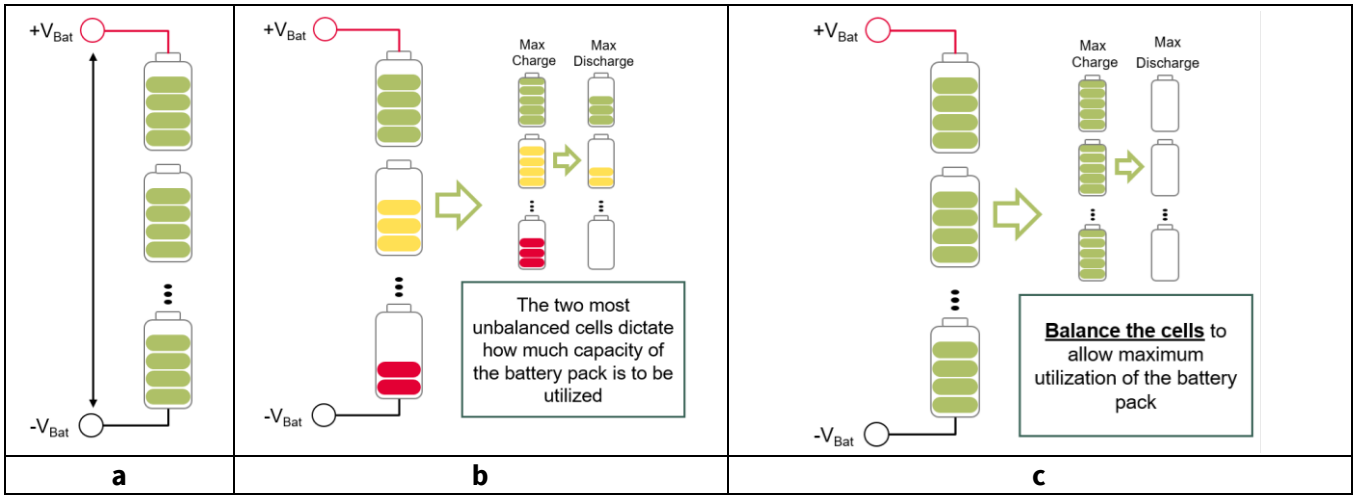

Figure 2 Charging and discharging behavior of (a) cells in series when (b) unbalanced and (c) balanced.

A Li-ion cell must never be operated beyond its safe operating area (SOA) in terms of both temperature and voltage, represented by the green region in Figure 3. However, if the cell is properly managed, it is possible to achieve extending the operating window (the yellow region), thus utilizing a battery cell to its maximum potential.

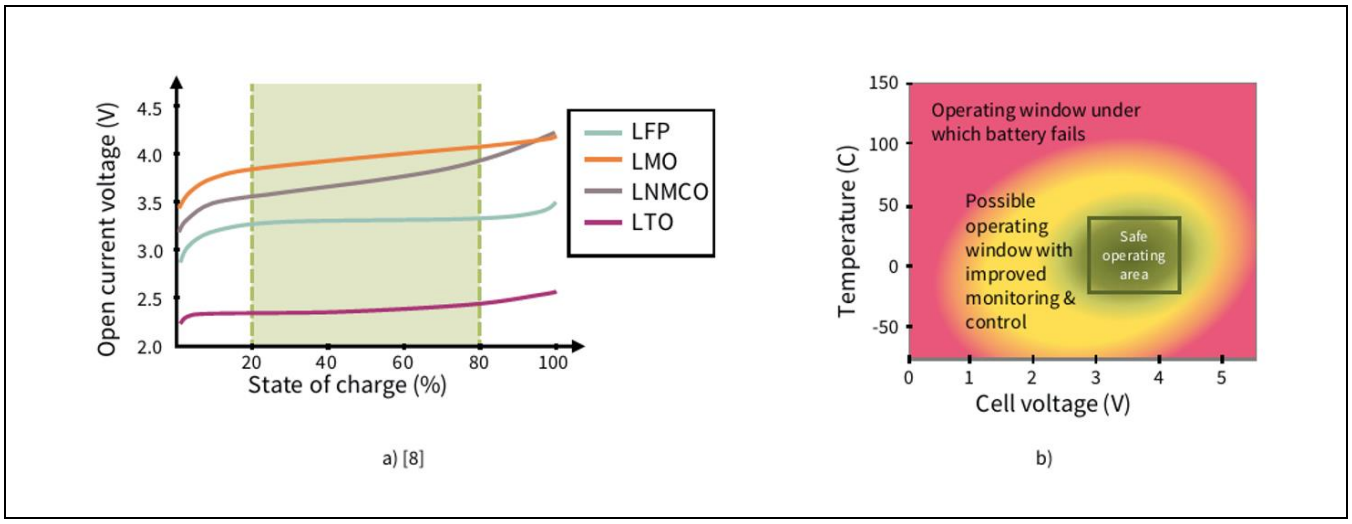

Figure 3 State of charge characteristic (a) and safe operating window of Li-ion battery cell (b)

Introduction

BMS includes the following key functionalities:

- Monitoring the pack and cells parameters (including voltages, currents, and temperature)
- Calculate and estimate the battery and cell states (SoX: states of charge, health, power, safety, and more)
- Optimize the battery performance/operation (including balance cells, request for cooling/heating battery pack)
- Protect the battery from being operated outside the safe operating regions (for example, during events like overcurrent, over/under charge

1.1 Initial technical assumptions

Assumed BMS key characteristics:

- 1000 V battery pack voltage
- 500 A max. charge/discharge current

Cooling control is applied either by water cooling or air cooling and in both scenarios requires e-motors, such as BLDC for active cooling purpose.

Security

- Battery pack manipulation protection (QM – no ASIL)
- Might be achieved by Cyber Security Module from AURIX™ TC4xx (with QM assumption)

2 Hazards of BMS/ Energy Storage System

A preliminary hazard analysis can be performed to identify different situations and assign the corresponding ASIL.

The main hazards associated with BMS/ESS can be categorized into several areas:

- Thermal overheating of cell array due to any kind of undetected cell shorts, overcurrent, or any kind of inadequate charging due to external grid chargers or recuperation from traction inverter(s). This may lead to fire or toxic fumes and endanger the lives of passengers
- Isolation defects between high voltage elements and the chassis. This can lead to electric shocks.
- Mechanical stress on the cell modules resulting from various factors, including accidents, nail penetration into the cell modules, vibration, and structural fatigue

Vibrations, mechanical stresses or nail shaped object (that could penetrate the battery shield cell) could cause internal short circuit that is one of the thermal runaway triggers. The system should be designed using other technologies with respect to E/E for risk prevention (i.e. robust mechanical box).

At present, the current scope of ISO 26262 primarily considers hazards caused only by malfunctioning behavior of safety-related E/E systems.

3 Safety goals and ASIL

Based on the identified hazards, the safety goals and their Automotive Safety Integrity Level (ASIL) ratings are formulated to describe what the system shall prevent. These safety goals shall be specific, measurable, and achievable.

Table 1 Safety goal definition

ID	Description	SG ASIL	FTTI (pessimistic values at MCU level)
SG1	Prevent thermal run-away of the battery cells due to OV, UV, OC, OT	ASIL D	≤ 800 ms
SG2	Avoid of electric shock because of crash or HV insulation loss	ASIL B	≤ 30 ms

Each safety goal inherits an ASIL rating based on the hazard risk classification by considering factors such as exposure, controllability, and severity. This ASIL rating determines the level of safety required for the system.

In BMS system, an E/E system could supervise hazards not always directly caused by E/E, like thermal runaway and electric shock. In general, ISO 26262 2010 edition would not directly cover this kind of hazards, as stated in the scope, but it is common use to apply automotive functional safety standard also for this aim, even because there is always a grey area when determining what is the initial source of a hazard.

To summarize, this document wants to detail possible solution to cove the following two safety goals:

- **SG1:** Prevent thermal run-away of the battery cells due to OV, UV, OC, OT. In general, Faut Tolerant Time Interval (FTTI) is <= 800ms and safety rating assigned is ASIL D
- **SG2**: Avoid of electric shock because of crash or HV insulation loss. In general, FTTI is <=30ms and safety rating assigned is ASIL B

3.1 SG1 Thermal runaway

The primary precondition for thermal runaway (TRA) of the battery system is, when:

- Any cell experiences a thermal runaway
- Thermal energy propagates through spreading the thermal runaway from one cell to another

The cell thermal runaway can be triggered by various factors, including overvoltage (OV), undervoltage (UV), overcurrent (OC), or overtemperature (OT). To mitigate this, a monitoring function of voltage, current, and temperature in the BMS has to be implemented and, where possible, each cell voltage shall be measured correctly, continuously, and in a timely manner.

If cell OV, UV, OC or OT is detected, the system shall go to a safe state by interrupting the HV circuit within FTTI (i.e., disconnecting the HV battery from any source of charge).

Concerning **current measurement**, it is not feasible to accurately measure the current through each cell but the total current of the battery pack can be measured.

If all the logical cells in the battery pack are connected in series, then the current through all cells is the same as the battery pack current. This is the assumed battery configuration in this application note use case, since it enables a proper current monitoring and OC detection for all cells with the minimum complexity.

Safety goals and ASIL

Concerning **temperature measurement**, given the current state-of-the-art for battery system design, it is normally not convenient to put a temperature sensor on every battery cell. Therefore, only a few temperature sensors are placed on a battery module, which contains many battery cells. By studying the thermal behavior and characteristics of the battery module, the single-cell temperature can be derived. This relationship is used to monitor cell temperatures based on the measured module temperatures.

Note: *To be precise, **undervoltage** itself is not dangerous, but the re-charging after an under-voltage event is. When a lithium-ion battery is discharged below its safe voltage threshold, it can trigger a series of chemical reactions that can compromise the integrity of the cell.*

One of the primary concerns with over-discharging is the dissolution of copper in the anode. The anode, which is typically made of a copper-based material, plays a critical role in the battery's electrochemical reactions. When the battery is discharged too deeply, the copper can begin to dissolve, weakening the cell structure and creating an environment that is conducive to the formation of metallic deposits. These metallic deposits, which are often composed of copper, can reform inside the battery when it is recharged. This can create unintended conductive pathways within the battery, which can lead to an internal short circuit when the battery is used again. An internal short circuit can cause a range of problems, including overheating, electrical fires, and even explosions.

3.2 SG2 Loss of insulation

The insulation of HV+ and HV- could be damaged or destroyed due to a crash or other factor. In such cases, there is a high risk that the human body is exposed to both HV+ and HV- causing an electric shock.

The precondition for an electric shock of the battery system due to HV insulation fault are:

- HV+ insulation failure
- HV- insulation failure
- Human body or a part of the human body is in contact with the HV circuit

For this, both HV+ insulation and HV- insulation shall be measured correctly, continuously, and in a timely manner, as per ISO 6469-3:2021. A logic element shall process the measured insulation resistance to detect insulation failure. The principles of this measure are shown in Figure 4.

If an insulation failure is detected, the system shall go to a safe state by interrupting the HV circuit within SG2 FTTI (i.e., disconnecting the HV battery from the other systems in the vehicle and from any potential contact points for the human body).

Even after receiving a crash signal (e.g., via dedicated signal line or via CAN message) from another ECU (e.g., airbag system, VCU), the BMS should provide an immediate disconnection.

Safety goals and ASIL

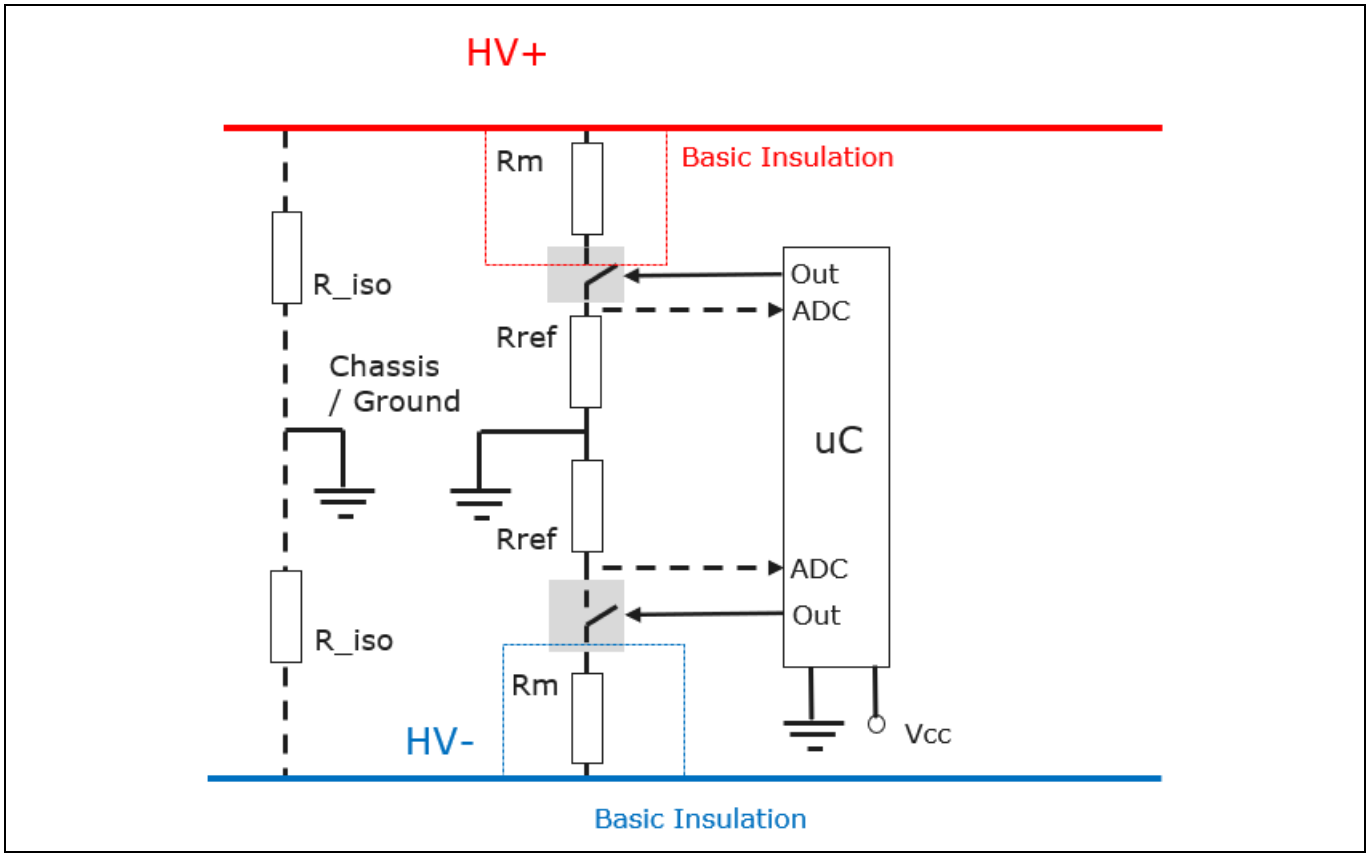

Figure 4 Insulation monitor principle

4 Description of the functional safety concept

The HV BMS could be considered composed by the following four main blocks:

- CMU
- PMU
- BMU
- BDU

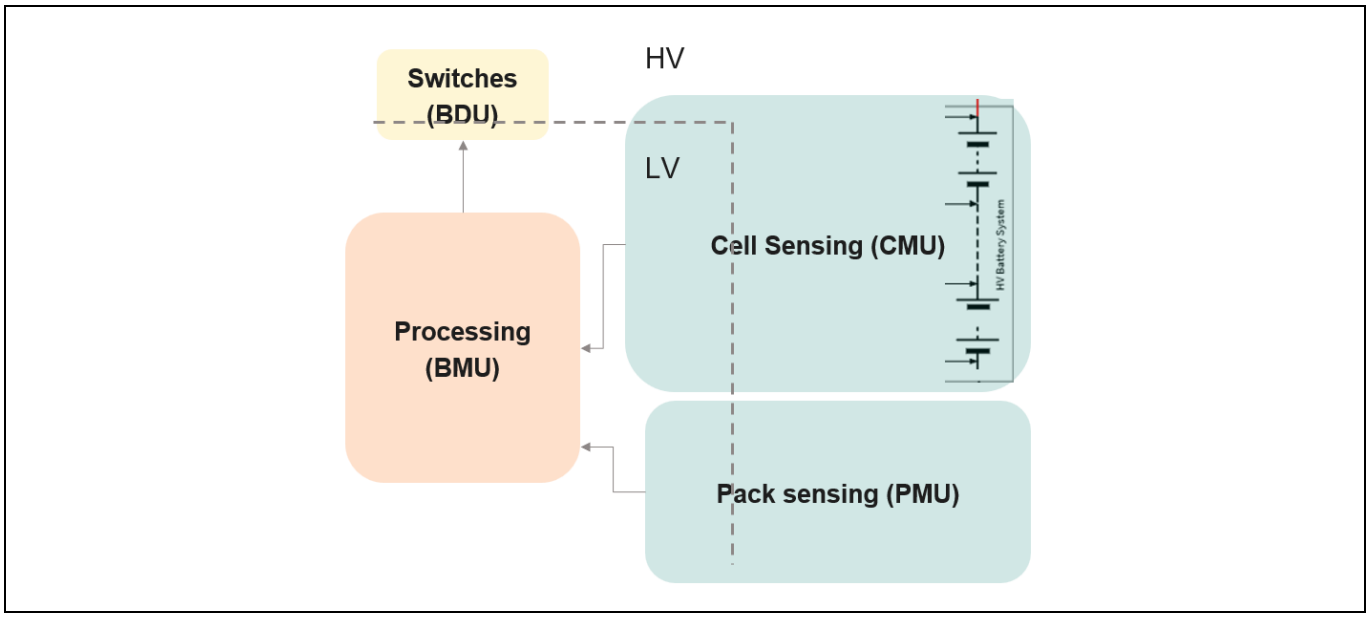

Figure 5 BMS functional safety concept block diagram

A short desciption of each block is reported in the following four sections.

The following description has no intention to be exhaustive in summarizing the functional safety concept but rather focussed towards assigning specific safety task to the various blocks.

To be noted that in BMS, all the fuctionalities listed below are also safety relevant and require ISO 26262 compliant components, where possible.

4.1 Cell monitoring unit (CMU)

The CMU implements the cell monitoring function based on the sensors acquisition. Task of CMU modules are the following:

Inputs measurement function:

- CMU measures the cell voltage of each battery cell and the temperature of the battery module by using a temperature sensor (NTC)

Data processing:

- Performs periodic A/D conversion to determine the digital cell voltage measurement value
- Performs limited data processing, such as collection of multiple voltage measurements, debouncing to eliminate invalid measurement data, and conservative high/low voltage estimation

Output / communication:

- Transmission of voltage measurement data to BMU via UART interface (daisy-chain of all cell monitoring units)
- Passive cell balancing

4.1.1 About cell temperature measurement

Several temperature sensors are used to measure the temperature of each battery module. Even though not all cells are measured individually, the temperature measurement in a few places in the battery module is sufficient to estimate the temperature of all cells. This approach is according to a worst-case analysis performed for the battery modules.

However, it must be ensured that any local heat-up (e.g., due to internal short in only one cell) can be detected.

These multiple temperature sensors do not constitute redundancy (in the sense of ISO 26262). Instead, these multiple sensors are necessary to achieve an accurate temperature measurement for the complete battery module.

If more temperature sensors are implemented than required to fulfill the above concepts and guidelines, then it must be specified whether these additional sensors are used for safety/redundancy, or for availability purposes (to enable continued operation without restrictions in case of a single sensor failure).

The temperature sensors provide an analog output signal with sufficient resolution for the required measurement accuracy. The analog signals are routed to the CMU Sensor IC and converted into digital data (via internal ADC) for further processing.

The temperature sensors must provide an accurate measurement in the expected temperature range (-45°C to 85°C). For lower temperatures, a reduced measurement accuracy or even low saturation is acceptable, because no further differentiation of the required actions is needed at these low temperatures. However, the sensors must reliably deliver a “very-low-temperature” readout. Similarly, for higher temperatures, a reduced accuracy or high-saturation is acceptable, as long as a “very-high-temperature” readout is ensured.

The highest accuracy is required in the range of overtemperature alarm and pre-warning (40°C to 70°C).

4.2 Pack monitoring unit (PMU)

The PMU implements the cell monitoring function based on the sensors acquisition. Task of PMU modules are the following:

Input/measurement function:

- Battery pack current measurement via Hall-sensor (medium accuracy)
- Battery pack current measurement via shunt resistor (high accuracy)

Data processing:

- Periodic A/D conversion of Hall-sensor to determine the digital current measurement value
- Periodic A/D conversion of analog data from Shunt resistance in PMU local microcontroller to determine digital current measurement value
- Insulation resistance measurement

Output / communication:

- Transmission of current measurement data from Hall sensor to BMU via a digital communication interface
- Transmission of current measurement data from shunt resistor and local microcontroller to BMU via digital communication interface
- Alarm transmission to BMU module

4.3 Battery management unit (BMU)

BMU is the central processing unit.

Input/measurement/communication function:

The module receives:

- Battery pack current data as a necessary input to over-current detection (OV),
- Temperature data as a necessary input to cell over-temperature detection (OT),
- Cell voltages as necessary input for all safety calculations
- Pack overall voltage

Data processing:

- Processing of pack current measurement data from shunt and Hall sensor, and temperature measurement data
- Detection of overcurrent (limit is mainly dependent on the cell itself, temperature, charge/discharge, etc.,), overtemperature
- Initiation of fault reaction mechanisms according to the battery fault detected

Output/Communication:

- Generation of “HV shut off” command to Battery Disconnection Unit (BDU) in case of a detected battery pack overcurrent, overtemperature, HV insulation failure or any other critical fault detected.

4.3.1 About battery pack overcurrent detection

The BMU receives the overall current measured by the pack monitoring module (PMU).

Measurement of the pack current is done twice by using both Hall sensor and a shunt resistor. Aim is to achieve the required ASIL and at the same time take advantages from diversity.

Typically, shunt resistor and Hall sensor support a limited current range, and they may not be able to do an exact current measurement across the full range of possible charge or discharge currents, especially in case of overcurrent.
The shunt resistor typically covers the full current range up to the maximum possible overcurrent threshold (e.g. ±500 A continuous or ±3000 A peak<10 s). The shunt current is required for high-accuracy current measurement across the full range of charge or discharge current during normal operation (including for non-safety related functions such as State of Charge (SoC) estimation), as well as a reliable overcurrent threshold detection.

The Hall sensor covers an even larger current range, far beyond to the overcurrent threshold (e.g., ±3000 A). In case of overcurrent, when the shunt resistor measurement goes out-of-range, the Hall sensor is the only sensor providing (medium-accuracy) current measurement data. This overcurrent measurement is needed to decide the proper procedure for HV interruption.

4.3.2 About cell overtemperature detection

Considering that not all the cells are monitored individually (see 4.1.1), a worst-case estimation analysis is performed to supervise all the cells of the battery module. A thermal simulation and/or tests should be performed to confirm that the placement of the temperature sensors does not leave any undetectable local hot-spot development.

4.3.3 About HV insulation measurement and failure detection

Insulation measurement could be performed inside the switch box (BDU) using a local logic and a set of known resistors to support the measurement. Same could also be realized in the PMU using microcontroller special features. In our use case we suppose that the BMU implements the insulation failure detection function by comparing the insulation resistance values with the critical limits according to ISO 6469 or other equivalent standards.

4.4 BDU – Battery Disconnect Unit

Tasks of Battery disconnect unit (BDU) are the following:

- Connect the battery pack to the vehicle's electrical system when the vehicle is started or when the battery pack is being charged
- Disconnect the battery pack from the vehicle's electrical system in the event of a fault or emergency, such as a crash event, a short circuit, overcharge, or overheating of the battery cells

Trying to distinguish between Inputs, core and actuator we can list the following main functionalities:

Input/measurement/communication function:

- Crash signal from another ECU (e.g., airbag system)
- Control signals for the switches sourced by the BMU processing unit

Data processing:

- Independent triggering of switch opening by Battery Disconnect Unit in case of a crash or short circuit

Actuator functions/reactions:

- Opening of contactors
- Fire Pyro-Fuse
- Driving Battery Disconnect switches (BDS)
- E-FUSE functionality

4.4.1 Type of disconnecting devices and their use

The BDU includes switches connecting or disconnecting the HV battery from the vehicle board supply network. The BMS system safe state “HV battery disconnected” is reached by opening the switches under the control of BMS system or another ECU, such as the airbag system in case of a crash.

The current magnitude must be considered when attempting to open the switches. Opening the switches under no or a small current load is not critical, but a high or excessive current (overcurrent) may pose a serious challenge for the disconnection units to successfully interrupt that current flow without damaging and permanently welding the switches (e.g., contactors).

Description of the functional safety concept

Since mechanical contactors are not suitable for interrupting large currents, there is a need for other disconnect devices like melting fuses, pyro-fuses or semiconductor-based battery disconnect switches.

Battery Disconnect Switch based on semiconductors, relay and pyro-fuse have separate control signals arriving from BMU.

If the HV battery is going to be disconnected in normal operation (e.g., after vehicle is turned off), the current is first reduced to < 5 A before starting to open the switches. This results in minimum stress for all switch types.

However, in a **safety critical situation,** such as when BMU issues a “HV shut off” command to enter a safe state, it may not be possible to reduce the current flow and the switch opening must be initiated immediately.

If the switches are opened under no, low or high current load, the following procedure is used:

- BDS unit is “opened”
- Contactor is opened after a predefined delay (current dependent)
- Pyro-fuse[1] is not opened/triggered

In case of a **crash**, or if a very high overcurrent is detected, then the pyro-fuse could be used in addition to BDS and contactors, to achieve a fast and reliable – even though destructive – HV disconnection.

In this case the following procedure is applied:

- BDS and pyro-fuse[1] are opened/triggered at the same time
- Relay is opened after a very short, predefined delay

[1] Pyro-fuse could NOT be used anymore in conjunction with semiconductor-based BDS.

5 BMS technical safety concept and requirements overview

To control the BMS, Infineon's automotive MCU family implements advanced features for signal acquisition with the highest safety level, such as multicore and lockstep architecture, DS-ADC-enabled direct resolver-to-MCU interface, ethernet interface, and so on.

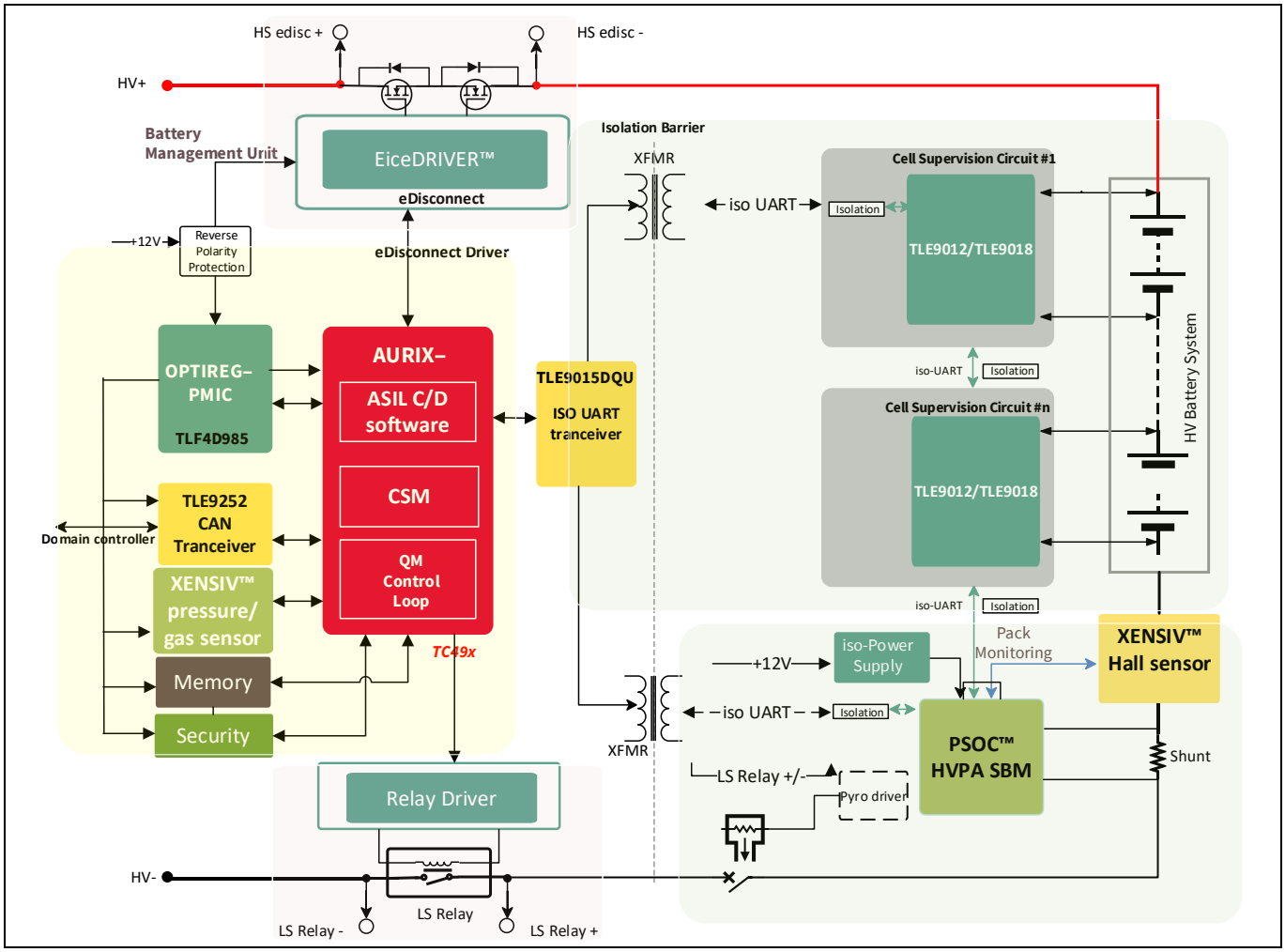

Figure 6 Simplified block diagram of the BMS system

To understand the safety features implemented by Infineon components together for the high voltage BMS scope, we will go through the following functional blocks of the BMS:

CMU +PMU

- Cell monitoring and balancing (TLE9012/TLE9018),
- Isolated UART communication between the CMU and BMU microcontroller (TLE9015)
- PSOC™ 4 HVPA SPM 1.0
- Hall current sensing TLE497x

BMU

- Battery control unit (BCU) (TC4xx)
- Power management unit TLF4Dxx
- Absolute Pressure Sensor KP467

BMS technical safety concept and requirements overview

BDU

- Contactor (and pyro-fuse)
- BDS Battery disconnect switches (eFuses)
- SPI for communication with microcontroller and current sensors or can transceiver

Note: *Digital insulation preserves communication between AURIX™ and PSOC™. The PSOC™ MCU is powered though an isolated PMIC.*

5.1 CMU and PMU

The CMU and PMU blocks are located on the high-voltage side, close to the battery pack.

The two blocks acquire voltage and temperature of the cells (CMU) plus battery pack current with two different methodologies (PMU) in order to let the core of BMS (BMU) to perform accurate calculations and decisions.

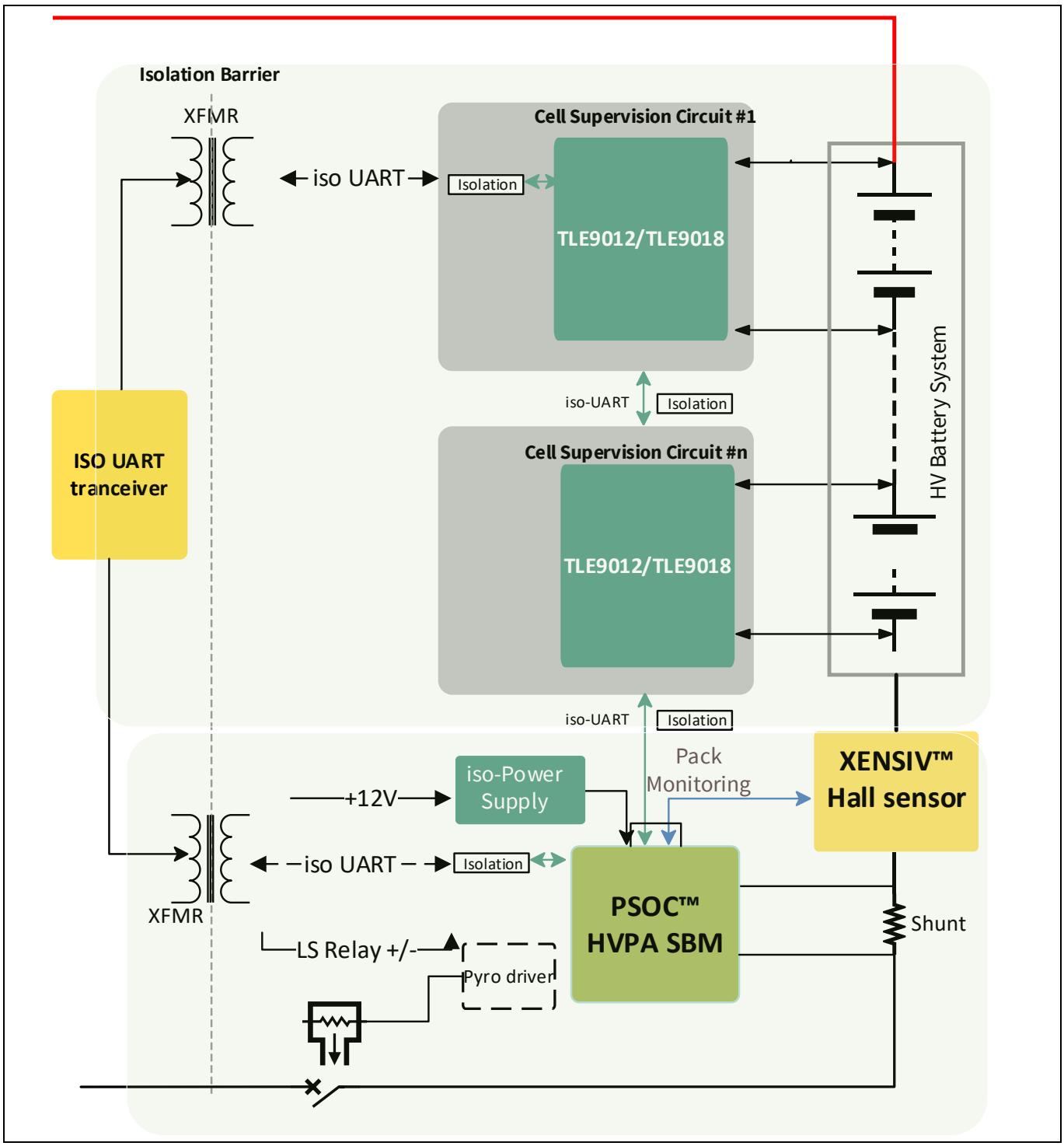

Figure 7 CMU + PMU schematic representation

5.1.1 TLE9012/TLE9018 cell monitoring and balancing IC

TLE9012 and TLE9018 are multi-cell battery monitoring and balancing system IC designed for Li-ion battery packs used in hybrid electric vehicles (HEV), plug-in hybrid electric vehicles (PHEV), battery electric vehicles (BEV) as well as in 12 V/48 V Li-ion batteries and energy storage systems (ESS).

The main difference between TLE9012 and TLE9018 is that the first is able to monitor up to 12 battery cells connected in series whilst TLE9018 can monitor up to 18 battery cells.

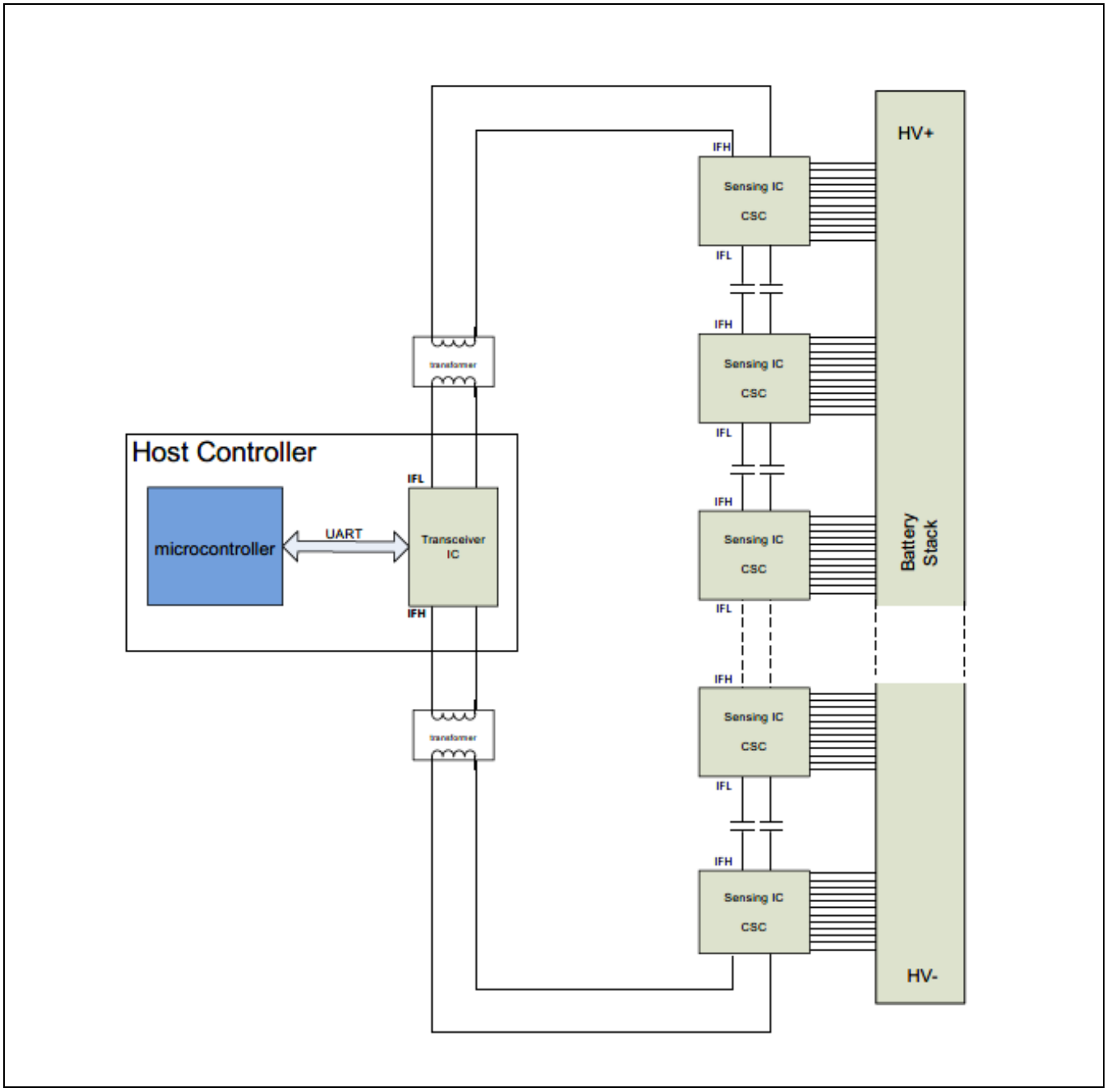

Figure 8 Example of usage of TLE9012/TLE9018 in daisy chain and communication with host controller (RING mode)

The required number of TLE9012 or TLE9018 chips depends on the battery configuration.

Both types of monitoring sensors can communicate in daisy chain (see Figure 8), with the possibility to include in the daisy chain also PSOC™ 4 HVPA SPM 1.0, that works as the Pack Monitoring Unit (PMU) and measures the current of the battery pack. PSOC™ 4 HVPA SPM 1.0, as the last element of the daisy chain, transmits data to the transceiver (**TLE9015DQU**).

The whole set of components that constitutes CMU and PMU blocks, contribute to satisfy Safety Goal 1 and 2 (described in Section 3) performing the following safety task:

- Measure in a safe manner the **voltage of each cell** and calculate the state of charge (**SoC**) via Coulomb counting. This data is then used to estimate the state of health (**SoH**) thanks to special algorithms running in the BMU block, that receive parameters by the CMU and PMU blocks.
- Measure safely the **cells temperatures** for the battery pack thermal management. As described in the Functional safety concept (Section 4.1.1), temperature sensors number and positioning depend on considerations made in the cell pack project phase and on the verification results
- Check if the cells are always operating within their safe operating area (**SOA**)
- Equalize the cell's state of charge
- Safely Transmit data via UART Isolated communication

The TLE9012 or TLE9018 IC are directly connected to the battery cells and can take care of overtemperature check, overvoltage, and undervoltage check and open load check on the sense line.
In case of any error detection, a message is sent to the core MCU in BMU block, in order to open the battery main switches.

5.1.2 TLE9015 UART communication

The TLE9015 is a safe transceiver designed to be used in conjunction with TLE9012/TLE9018 multi-cell monitoring and balancing integrated circuits. By means of its two UARTs and iso UART interface pairs, it can support ring communication, improving the availability of the system. It is designed for Li-ion battery packs used in hybrid electric vehicles (HEV), plug-in hybrid electric vehicles (PHEV), battery electric vehicles (BEV) as well as in stationary Lithium-Ion batteries.

UART is a communication protocol which consists of transmitting or receiving a group of 8 bit called "frame". It can be used to send a simple information in one frame but there are diverse types of frame which can be used to create a safety communication.

Both the transceiver and the cell monitoring sensor use the frame sequence described below, contributing to satisfy Safety Goal 1 and 2 (described in Section 3).

- Identification frame (to determine the type of command)
- Synchronization frame
- Reply frame (in case of broadcast write)
- Data frame (contain the message)
- Address frame (determine the register affected by the read or write command)
- CRC frame

The usual way to communicate is to send those frames in this order:

Sync frame <- ID frame <- Address frame <- Data frame <- CRC frame <- reply frame (for broadcast)

The TLE9012 or TLE9018 sensors are not linked directly to AURIX™ TC4xx, instead TLE9015 transceiver will do the link between the microcontroller and TLE9012/TLE9018 ICs. The transceiver and the cell monitoring and balancing IC are linked with an isolated communication UART protocol to communicate the data. The Iso UART

is more resistant than the UART itself and allows to transmit and receive data in a high voltages environment (up to 1000 V depending on the system).

In addition to the isolated UART, a transformer is applied between the transceiver and the sensor to create a galvanic isolation.

The AURIX™ TC4xx checks each incoming communication for CRC correctness. In the case of CRC fails, the affected messages shall be discarded by the AURIX™.

The AURIX™ TC4xx verifies the correctness of all reply message(s) after each command. Moreover, the MCU would implement a time-out detection and reacts accordingly if the selected BMS CMU section does not respond after a request . A reaction that brings system into safe state is expected only if the same error is detected multiple consecutive times, as the fault reaction time on system level is usually much longer than the data repetition time at device level.

In order to be able to check for possible errors within the defined timeframe and thresholds by avoiding false triggers, the AURIX™ TC4xx should set the parameters according to the actual system architecture (number of cells connected to the device, number of NTCs connected to the device, cell type, balancing current, timing, external circuitry, and so on).

5.2 PSOC™ 4 HVPA-SPM 1.0

PSOC™ 4 HVPA Smart Battery pack Monitor (SPM) provides the following safe main functionalities, contributing to satisfy Safety Goal 1 and 2 (detailed in Section 3) :

- Pack voltage monitoring
- Overcurrent monitoring and battery pack current measurement
- Fire the pyro-fuse in case of crash or another fault detected

The high-voltage battery must be insulated from the rest of the car, so constant monitoring of the pack insulation is necessary to guarantee that a safety action takes place in case of fault. This monitoring is performed by using high-impedance-faulty shunts to sense the variation in impedance between the different poles of the pack.

A critical point to consider when selecting a pack monitoring device is the speed of overcurrent detection (OCD) and reaction: In the event of a short circuit, the DC bus bar current can spike to a few thousand amps in just a few hundred microseconds. Since the disconnect might need time to switch off (less than some microseconds for solid state disconnects and a few milliseconds for relays), the pack monitoring must have a very fast OCD and trigger the disconnect to switch off.

PSOC™ 4 HVPA SPM 1.0 presents:

- High resolution 16-20+ bit ADCs with best-in class gain error (±0.16%)
- ASIL D process according to ISO 26262
- Embedded intelligence including reduced power consumption features and embedded memory

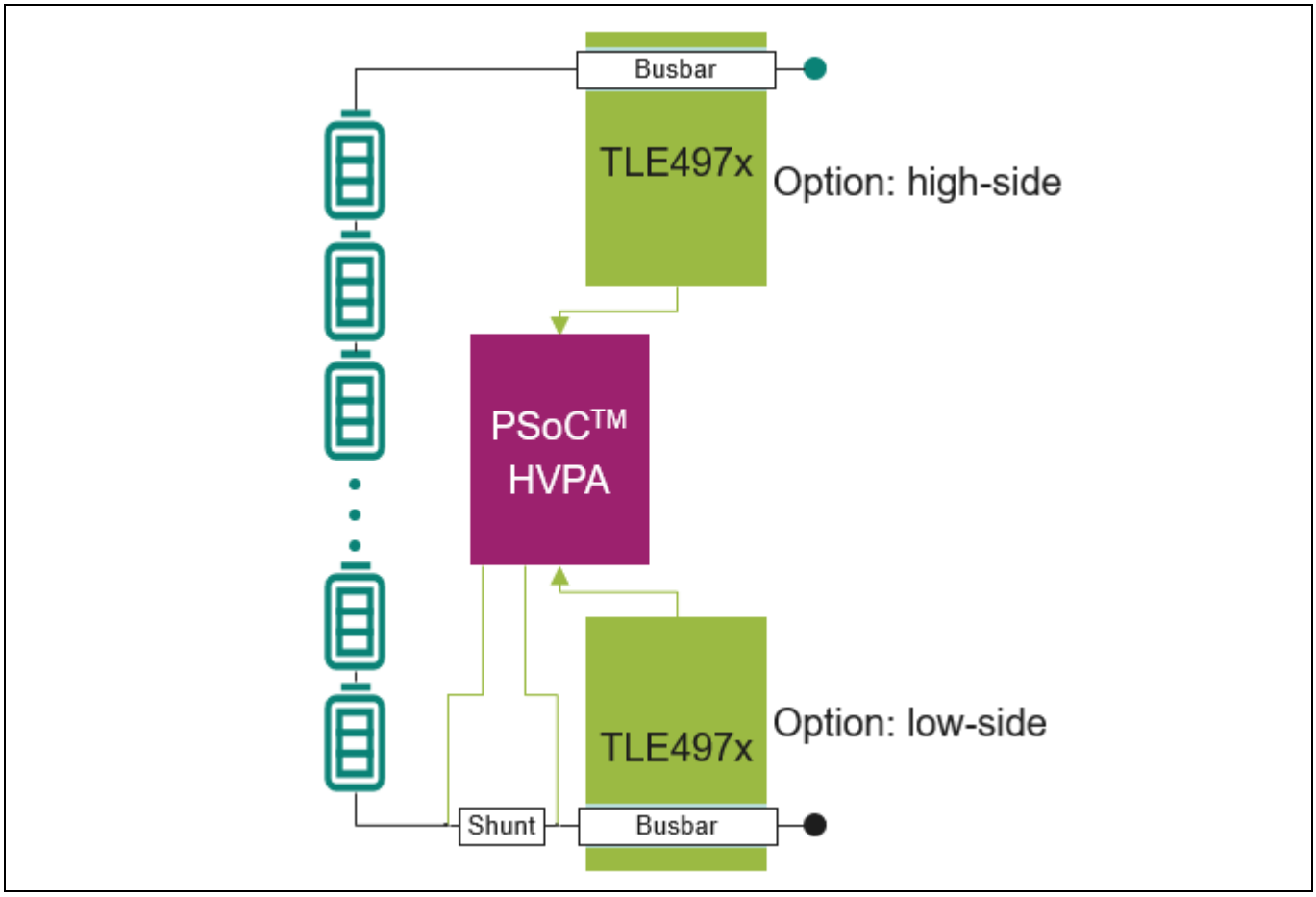

Figure 9 Hybrid hall and shunt-based current sensing

The most important safety features that are enabled for this MCU are:

- Pack current-sensing connection both to shunt (high accuracy) and Hall (fast, redundant sensor)
- Overcurrent detection and pyro-fuse trigger : Fast-detection (µs) of overcurrent event and Trigger capability of pyro-fuse to disconnect the battery, avoid thermal runaway
- Pack voltage and contactor monitoring: Pack voltage measure through external dividers, Contactor switches and link voltage
- Isolation-resistance / leakage monitoring : Leakage current between HV and LV (chassis) domain
- Charge monitoring and charge measurement, SOC of the battery using coulomb counting
- Daisy chain and isolated communication with cell-monitors and sync V/I monitoring for EIS Isolated comm with host ECU
- Sensor hub and fusion: sensor interfaces: Shunt, Hall, pressure, TMR etc.,
- BMS gateway because of standardized CAN interface to the zonal ECU and Isolated daisy chain communication to the cell-monitors
- Ability to manage diagnostics of battery pack parameters: cell-voltages, current, temp
- Secure communication with the zonal ECU: Secure authentication and Secure key storage

5.2.1 TLE4973 Current sensor

This system uses a TLE4973 coreless current sensors from Infineon as a highly reliable and functionally safe solution designed for accurate current measurement without the need for bulky magnetic cores. It offers a range of features to ensure safe and precise operation.

It contributes to satisfy Safety Goal 1 (detailed in Section 3) measuring the battery pack current.

TLE4973 current sensor offers a sensitivity from 53 to 254 mV/mT, sustaining up to +/-132 A when mounted on the PCB (internal current rail) and up to +/-2000 A on when present on the busbar (external current rail).

The sensor is equipped with an overcurrent detection (OCD) pin, enabling efficient monitoring and protection against excessive current levels. This pin provides an additional layer of safety by allowing the system to quickly respond and mitigate potential risks associated with overcurrent conditions. The sensors can be configured by the customer for specific thresholds and deglitch timings.

The OCD pin is designed as open-drain output and can be connected to the logic input pins of the MCU and/or the pre-driver to quickly react to overcurrent events.

All user-programmable parameters, such as OCD threshold blanking times and sensitivity, are stored in an embedded EEPROM memory. Device configuration can be performed in-situ through a UART-based bus compatible with one-wire interface called Digital Control Diagnostic Interface (DCDI).

The DCDI provides read/write access to internal registers of the device and allows to trigger the diagnostic mode and to read temperature, OCD, and safety status. It has an auto-addressing functionality that enables the address resolution and hence the handling of up to 8 slaves on one bus; multiple current sensors can be connected to the same microcontroller pin.

The device can trigger a diagnostic mode when the corresponding command is received through DCDI in regular operating mode (after the start-up time). The diagnostic mode functionality can be used by the system integrator to support safety analysis at system level. Using this diagnostic mode, the system integrator can verify the functionality of the main analog path and of the internal/external overcurrent detection at system level.

Another notable feature is the configurable analog output operational mode. It offers flexibility in selecting the operational mode, whether fully differential or single-ended. This adaptability enables seamless integration into different system architectures, catering to specific application requirements and optimizing overall performance.

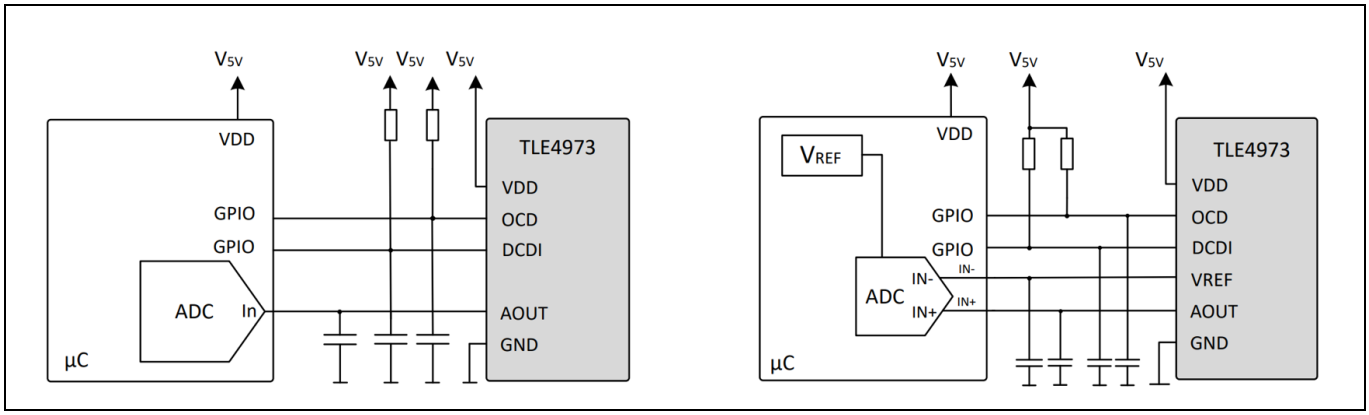

Figure 10 Application circuit for Infineon TLE4973 current sensor, single-ended (left) and fully differential (right)

The current sensor combines precise current measurement, independent overcurrent detection pins, configurable operational modes, and a robust design compliant to functional safety compliance (ISO 26262 ASIL B).

Current measurement of the battery system is performed using a Hall-based principle and a battery pack monitor realized with a microcontroller incuding high precision ADC module (see Section 5.2). The combination of these two sensors is used to achieve ASIL-C/D requirements.
PSOC™ 4 HVPA SPM 1.0 can realize the high-precision measuring sensor and safely monitor the current flowing through a shunt resistor.
On the other side, the **TLE4973** is a less accurate sensor that is typically used only to detect overcurrent.

TLE4973 is equipped with two independent fast overcurrent detection (OCD) pins, enabling efficient monitoring and protection against excessive current levels.

The advantage of the additional OCD pin is the low latency in the detection of positive and negative overcurrents. Depending on the primary current slope and the programmed threshold, detection latencies of about 1us can be implemented with the Infineon current sensor. This enables fast hardware protection.

The current sensor combines precise current measurement, independent overcurrent detection pins, configurable operational modes, and a robust design compliant to functional safety rating (ISO 26262 ASIL B).

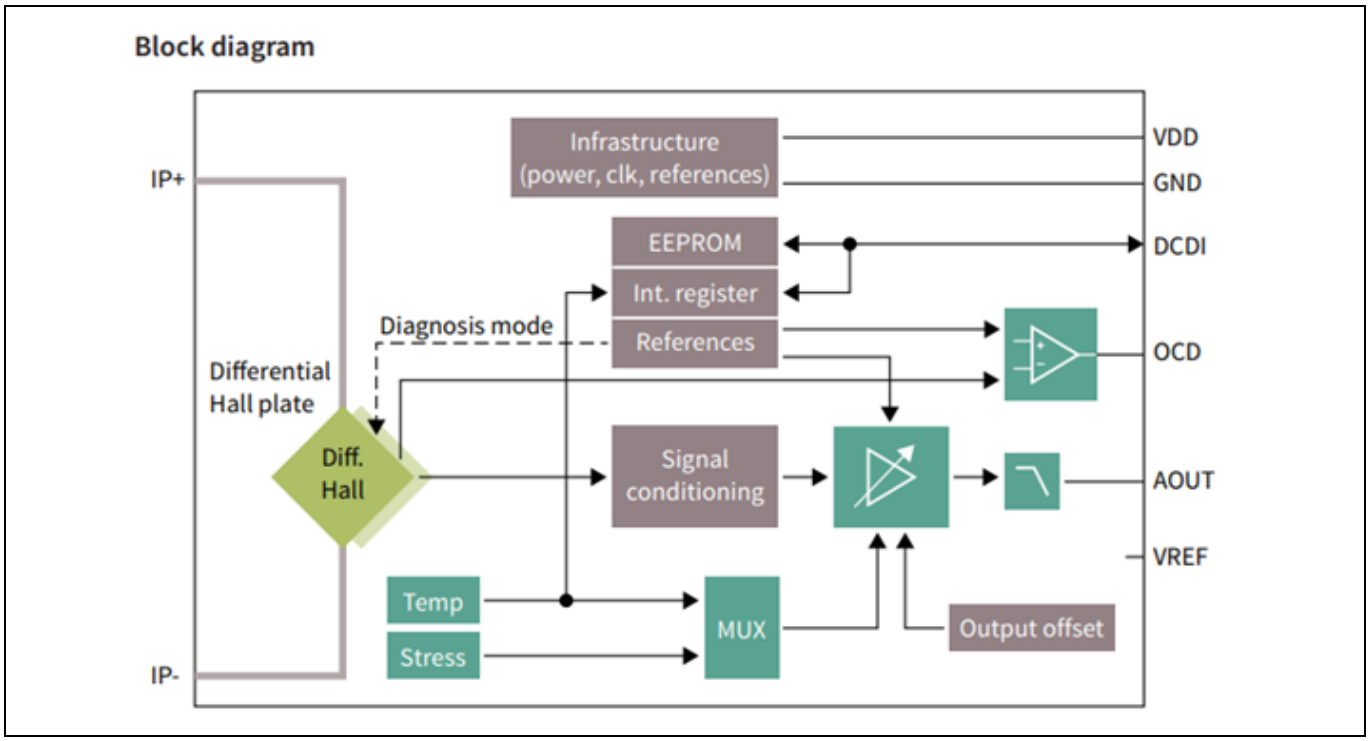

Figure 11 TLE4973 Hall sensor block diagram

In TLE4973, a safety communication protocol called digital control diagnostics interface (DCDI) is implemented. The DCDI is a single-master, multi- slave interface. It is based on UART communication, and it is possible to connect up to 8 sensors to the microcontroller. This interface is designed to be operative in harsh electronic environments such as voltage spikes.

To reduce errors during the transmission and to correctly interpret the sensor response, the DCDI protocol implements a majority vote principle. For instance, if each bit is sampled 3 times with the outcome of two have the same value, that value is chosen to be the correct one.

For example, the 3 bits are S1, S2, and S3, if S1 = 0, S2 = 1, S3 = 0, bit value is ‘0’.

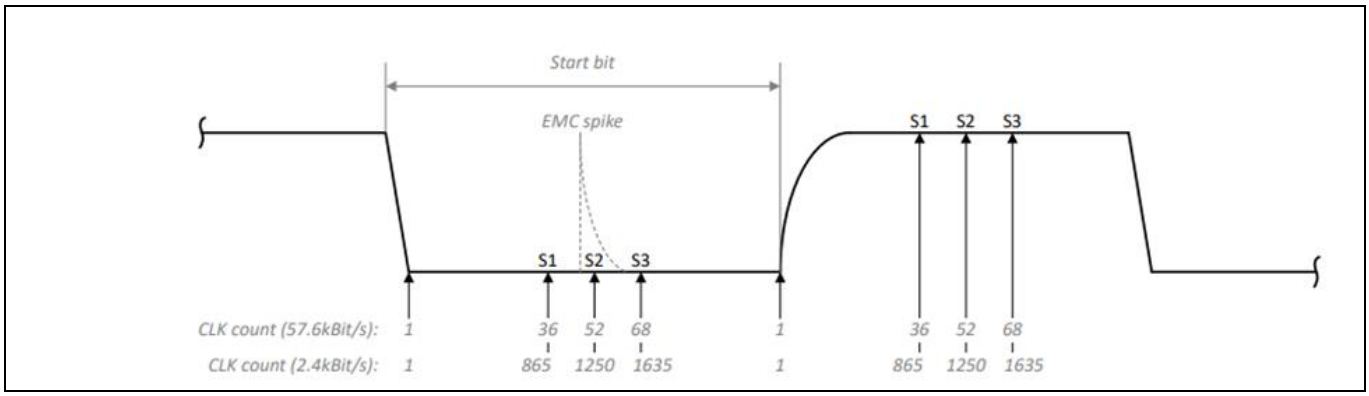

Figure 12 DCDI protocol with majority vote

When the DCDI transmit data, it transmits a frame composed of 4 types of byte fields:

- Command byte (CMD), it contains the sensor address and the CRC (3 bits)
- Address byte, it contains the address of the target sensor internal register
- Data byte, it contains the data information
- Safety byte, it contains a rolling counter, a safety bit status and a CRC (5 bits)

Rolling counter (RC): Counter which is increment depending on mode command (by 3 for a read command and by 1 for a write command), the RC is part of the CRC calculation.

Note: Cyclic redundancy check (CRC): Error detecting code that use polynomial algorithm code base on the cyclic codes.

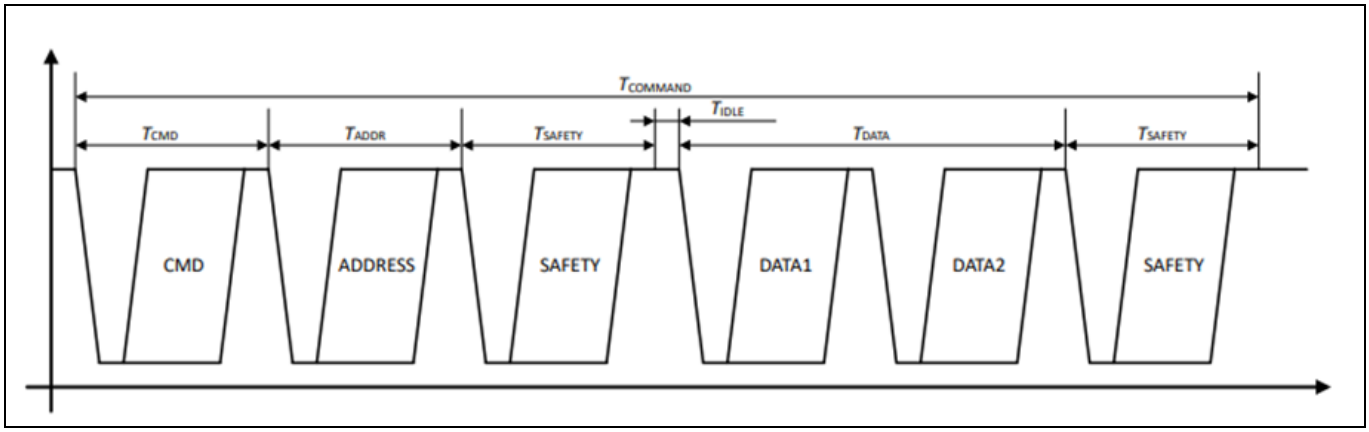

Figure 13 DCDI transmit frame

To ensure a safe transmission between the AURIX™ TC4xx and the sensor, the communication should be isolated. To choose the most suitable solution, refer to Infineon’s existing products, such as transceiver and smart switch.

5.3 BMU block

BMU is the main logic block of our high-voltage BMS use case. In the following section a list of its main components and their features is presented.

5.3.1 AURIX™ TC4xx MCU

As the main processor of the HV BMS and core of “Battery Management Unit”, AURIX™ TC4xx contributes to satisfy Safety Goal 1 and 2 (detailed in Section 3)for monitoring the battery pack.

Infineon’s AURIX™ TC4xx MCU family offers:

- Up to hexa-core with lockstep
- PPU suitable for battery-models acceleration
- SAR ADC or DSADC for signal acquisition for analog measurements (battery current and pack voltage)
- Complex, multiple and independent PWM pattern generation, e.g. needed, for example, for DAB-based active balancing system”
- Safe and secure connectivity to cloud with high throughput
- Functional safety: ASIL-D compliance to ISO 26262
- ISO 21434 Security features are also available, such as future-proof battery passport protection

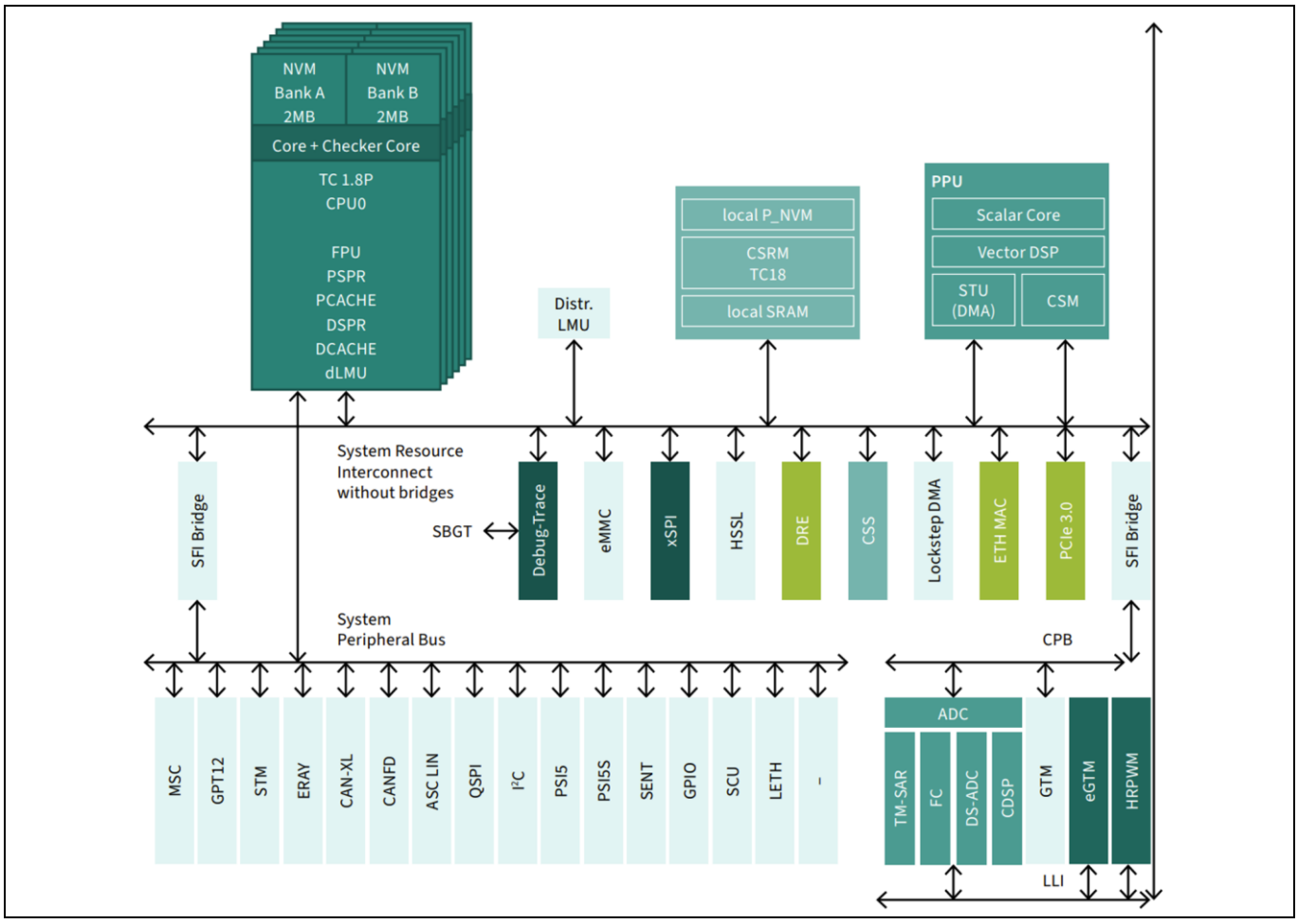

Figure 14 AURIX™ TC4xx Architecture scheme

BMS technical safety concept and requirements overview

The AURIX™ family is engineered to meet functional safety ASIL D rating as defined by ISO 26262.

The architecture features multiple TriCore™ CPUs, including cores in a lockstep configuration.
This provides redundancy and allows for immediate detection of processing errors, which is a fundamental requirement for safety-critical systems. The multicore concept allows for the integration of multiple applications onto a single device while using encapsulation to prevent interference between them.

Built-hardware safety features are also present in most of the blocks so that claiming ASIL D metrics is also an easy job when following the safety documentation provided.

The AURIX™ TC4xx can communicate with several units in the system, such as BDU, pack monitoring, cell balancing, and management unit, and with the vehicle control unit (VCU), the main controller of the car responsible for triggering the actuators. Each of these units must communicate in the safest way with the microcontroller (transceiver, isolated communication, and smart switch).

A key safety and security feature of the AURIX™ family is the embedded Hardware Security Module (HSM), which acts as a secure anchor of trust within the microcontroller.

- **Trusted Execution Environment:** The HSM is a self-contained computing platform with its own 32-bit CPU, access-protected memory for cryptographic keys, and dedicated hardware accelerators. It is separated from the main microcontroller cores by a security firewall, creating a trusted and isolated environment for security-critical tasks
- **Cryptographic Capabilities:** The HSM includes hardware accelerators for symmetric (AES-128) and asymmetric (ECC-256, SHA-2) cryptography, along with a true random number generator (TRNG). This enables secure on-board communication, which is critical for protecting sensitive data within a BMS.
- **Secure Functions:** It supports essential security applications such as secure boot, secure key storage, and integrity monitoring to protect the system's software and data from unauthorized access or modification. For a BMS, the HSM can be used to ensure the integrity of software updates at the ECU level
- **Standards Compliance:** The HSM is designed to fulfill automotive security standards such as ISO 21434 and support full EVITA level

Note: *E-safety Vehicle Intrusion Protected Applications (EVITA) is an EU-based research project that proposed security classifications for ECUs*

In this BMS use case, it is possible to find various functional blocks connected and coordinated by AURIX™ TC4xx. A non-exhaustive list includes the following ones:

- Communicating through TLE9015 with cell monitoring unit (CMU) and pack monitoring unit (PMU) and processing data received by these two modules
- Driving battery disconnect unit (BDU)
- Providing safe access to memory and vehicle control unit with CAN transceiver
- Monitoring pressure sensor
- Monitoring temperature sensors to detect temperature rise before thermal runaway

In summary, the AURIX™ TC4xx family provides robust safety for HV BMS applications through its integrated Hardware Security Module for cybersecurity, a multicore lockstep architecture for functional safety up to ASIL-D, and seamless integration with companion safety ICs to ensure system-level integrity.

5.3.2 Infineon TLF4D985 Power Management IC

Power Management Integrated Circuits (PMICs) are key components in modern BMS as these devices ensure reliable power delivery, monitoring, and protection for complex MCU architectures.

TLF4D985 is a PMIC tailored for the high range AURIX™ TC4xx. In addition to offering power delivery, the TLF4D985 PMIC actively monitors the system health, manages fault conditions, and supports safe-state transitions independently of the MCU when necessary, contributing to satisfy Safety Goal 1 and 2 as detailed in Section 3.

Furthermore, the secondary safety shutdown path, combined with advanced supervision functions, enables the system to react quickly and effectively during critical fault scenarios, ensuring both user and system safety.

The TLF4D985 is also meant to trigger the so called “secondary safety shutdown path”, which ensures system reliability when the primary safety path, managed by the MCU, becomes unresponsive or unreliable. This is achieved through a couple of Safe State Output signals:

- **Safe State Output 1 (SSO1)**: This pin is dedicated to power disconnection. If the MCU fails to initiate the required safety actions, the PMIC takes over, sending a signal via the SSO1 pin to the safety actuators. This action ensures the power flow to critical components is interrupted, effectively safeguarding the overall system
- **Safe State Output 2 (SSO2)**: This pin is used for communication disconnection. In scenarios where the MCU cannot reliably manage communication interfaces, the PMIC uses SSO2 to deactivate the communication channel, such as CAN, to prevent the propagation of erroneous or unsafe signals to other connected systems

5.3.2.1 TLF4D985 Safety features enabling functional safety at the system level

To support system-level functional safety, the TLF4D985 integrates multiple safety features that monitor and protect various aspects of the power supply, system operation, and environmental conditions.

Voltage monitoring

The PMIC actively monitors various supply rails to ensure proper power delivery. The main supplies to AURIX™ TC4xx that are also monitored are:

- Standby Supply ($V_{DDEVRSB}$ in AURIX™)
- Pre-regulator output ($V_{DDEXTDC}$ in AURIX™)
- Core regulator supply (V_{DD} in AURIX™)
- Interface supply (V_{DDHSIF} in AURIX™)
- Boost voltage supplies (V_{DDEXT}, V_{DDM}, V_{DDFLEX} in AURIX™)

These voltage monitoring functions detect overvoltage and undervoltage conditions, ensuring that the system operates within defined safety margins and avoids damage to connected components.

Supervision function monitoring

The TLF4D985 includes advanced supervision functions designed to monitor and address system malfunctions:

- **Error monitoring:** Tracks critical MCU errors and reports anomalies to ensure timely corrective actions

- **Window watchdog:** Monitors the MCU activity within a predefined time window. If the MCU does not perform a specific task or send a signal within the allowed timeframe, the PMIC triggers a reset to restore proper operation
- **Functional watchdog:** Continuously monitors the overall health and responsiveness of the MCU by assessing its ability to execute expected tasks. If the MCU fails, the PMIC initiates a reset or safe-state transition

Combined with Infineon's AURIX TC4xx , these supervision functions form a robust monitoring framework to detect and react to system malfunctions effectively.

Overcurrent and overtemperature monitoring

The TLF4D985 monitors several key parameters related to current and temperature, ensuring the system operates within safe limits. Specific monitored parameters include:

- Overcurrent conditions in the power supply lines
- Overtemperature conditions within the PMIC itself
- Excessive power dissipation scenarios

These monitoring capabilities prevent damage to both the PMIC and connected components, enhancing system reliability in demanding environments.

Analog Built-In Self-Test (ABIST)

The PMIC features an Analog Built-In Self-Test (ABIST) mechanism to verify the functionality of internal safety mechanisms, such as voltage and current monitoring systems. This feature helps to detect potential internal faults, ensuring the device maintains its safety functions throughout operation.

Reverse polarity protection and safety switch

The TLF4D985 is capable to manage a reverse polarity protection circuit to prevent damage to the device or system caused by incorrect battery connections. This function ensures that power is only delivered when the correct polarity is applied, safeguarding the PMIC and downstream components.

Additionally, the safety switch provides a mechanism for isolating critical power rails during fault conditions. This feature enhances system-level safety by enabling a controlled and reliable shutdown of power delivery to specific components, thereby preventing further damage or unsafe system behavior.

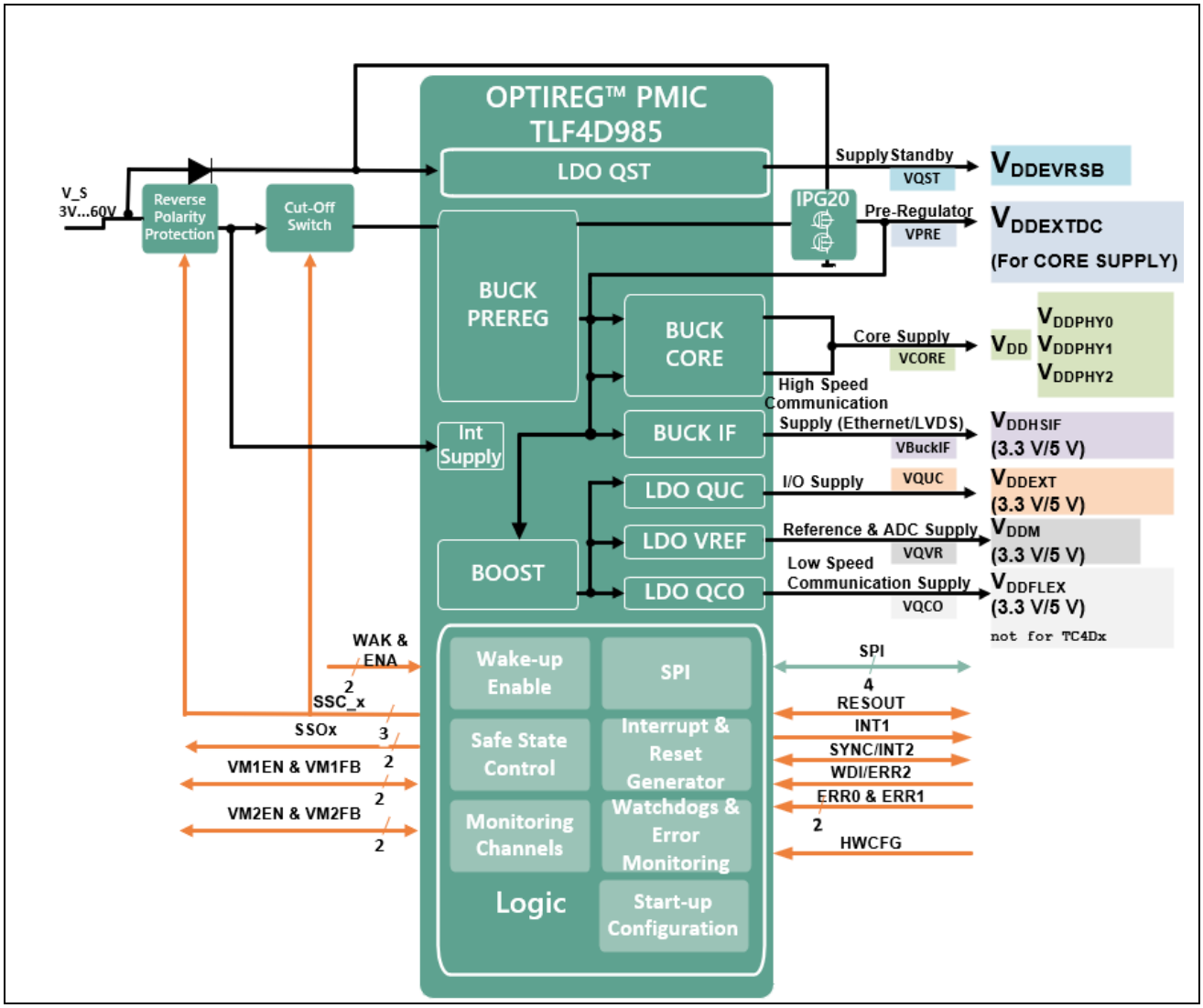

Figure 15 Supply rails and logic of TLF4D985

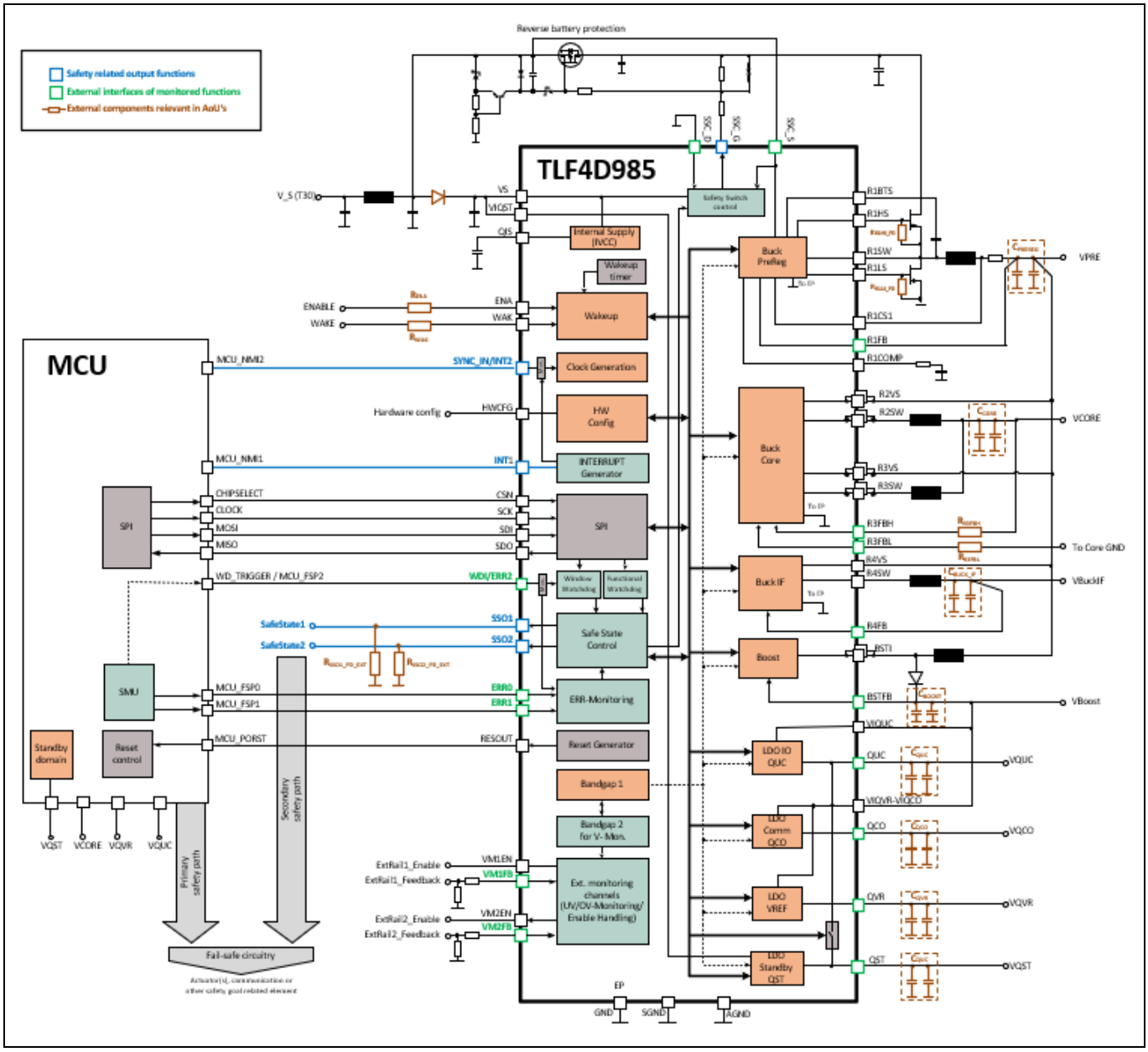

Figure 16 Infineon TLF4D985 logic connections of the power module

Table 2 provides an example of connections needed for functional and safety purposes when using the TLF4D985 PMIC as a power supply chip. As Infineon is continuously expanding its portfolio with dedicated chips and solutions, it is recommended to check the company website or the regional support for the latest information on the newest chipset.

Besides the power supply of the AURIX™, the power supply IC also has a supervision function for the microcontroller. During operation, the MCU and the power supply IC are exchanging signal patterns to check if the MCU is still in the right operation and is trustworthy. If the power supply IC receives the wrong pattern several times, an MCU power removal can be forced as a safe reaction.

Table 2 AURIX™ TC3xx-TLF4D985 logic blocks connections

Pin nr.	AURIX™	PMIC	Description
1-4	SPI- pins	SPI- Pins	SPI data transmission for configuration and data readout in a bidirectional way
5	FSP0	ERR0	Diagnostic output signal from AURIX™ TC4xx to TLF to activate an independent safety path
6	FSP1	ERR1	Diagnostic output signal from AURIX™ TC4xx to TLF to activate an independent safety path
7	NMI1	INT1	Safety output from PMIC to AURIX™
8	NMI2	INT2	Safety output from PMIC to AURIX™
9	PORTX.Y/FSP2	WDI/ERR2	Watchdog input signal from AURIX™
10	PORST	RESOUT	Reset to AURIX™
11	PORTA.B	SS1	For the startup test of SS1 output effectiveness (optional)
12	PORTC.D	SS2	For the startup test of SS2 output effectiveness (optional)

5.3.3 Absolute pressure sensor KP467

A pressure sensor can be added to the HV BMS to measure the ambient pressure. This allows to detect the small temperature variation or smoke appearance before an overtemperature detection occurs.

KP467 is the first pressure sensor for battery management systems that monitors and provides a warning in case of a thermal runaway event with highest efficient, immediate response, and very cost-effective.

Features of KP467:

- Dedicated low power monitoring (LPM) mode for battery monitoring applications (delta pressure threshold accuracy +-4%)
- High accuracy pressure sensing (+-3.0 kPa), pressure range 45 to 200 kPa
- Operating ambient temperature range -40°C to 105°C
- Best in class low power consumption
- 10-, 12- or 14-bit resolution pressure and temperature values via SPI Interface
- Integrated diagnosis features for signal path and signal processing
- **ISO 26262 Safety Element out of Context for safety requirements up to ASIL B**

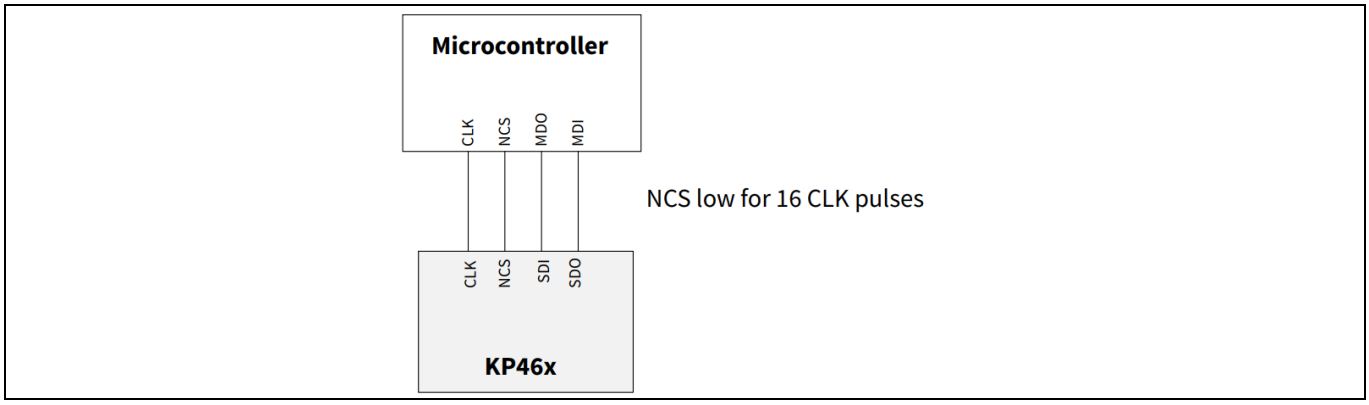

Figure 17 How to connect a single device KP46x to a microcontroller

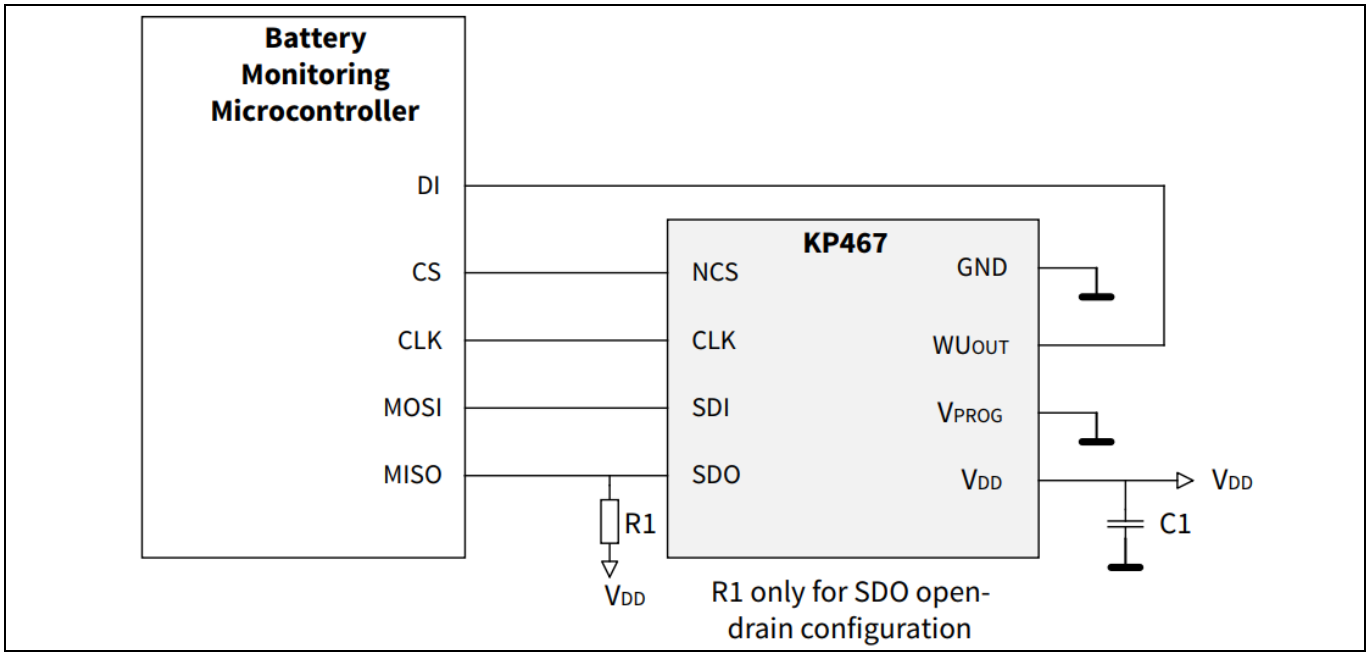

Figure 18 Application circuit example for battery monitoring (full-duplex use case)

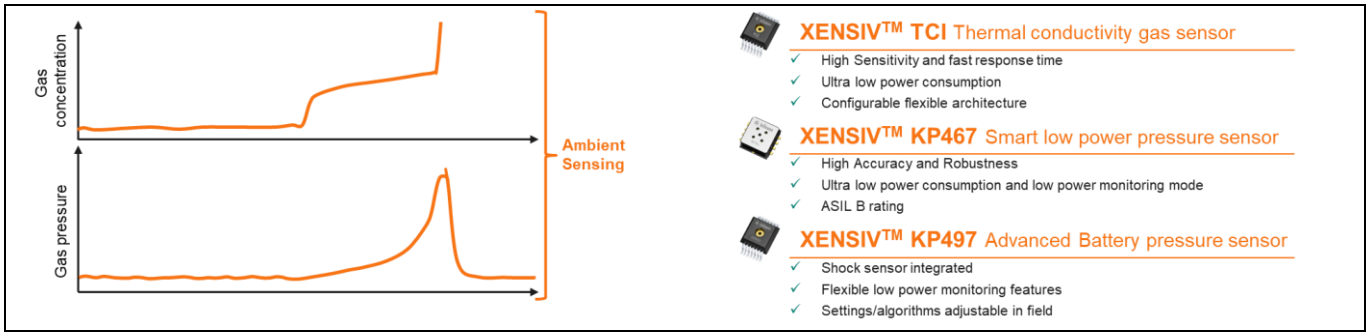

Figure 19 Infineon offer of various gas and pressure sensors

5.3.4 CAN transceiver TLE9252V

TLE9252V is a feature-rich system basis chip that integrates advanced power management, wake-up functionality, and diagnostic capabilities suitable for more complex automotive ECUs.

The Iso-CAN transceiver are used to create an isolated communication between the BMU microcontroller and the VCU or other external boards. To integarte BMS within the entire car system, an integrated circuit that accomplishes CAN communication is needed. For this reason, a CAN transceiver must be selected to enable the AURIX™ TC4xx MCU to communicate using that specific bus protocol.

Some of the key features of a good CAN module are:

- Fail-safe features such as TxD time-out, RxD recessive clamping, and overtemperature shut-down, that allow the system to perform in a predictable manner in a safety-critical situation. Other safety measures also report the CAN short circuit proof to ground, battery and VCC, as well as undervoltage detection on the supply voltages
- Local failure diagnostics should also be implemented by specifically designed output pins

BMS technical safety concept and requirements overview

Keeping into account the earlier mentioned characteristics of a CAN transceiver, the Infineon TLE9252V CAN transceiver is taken as a reference to understand how the CAN functionality can be integrated into the safe system itself.

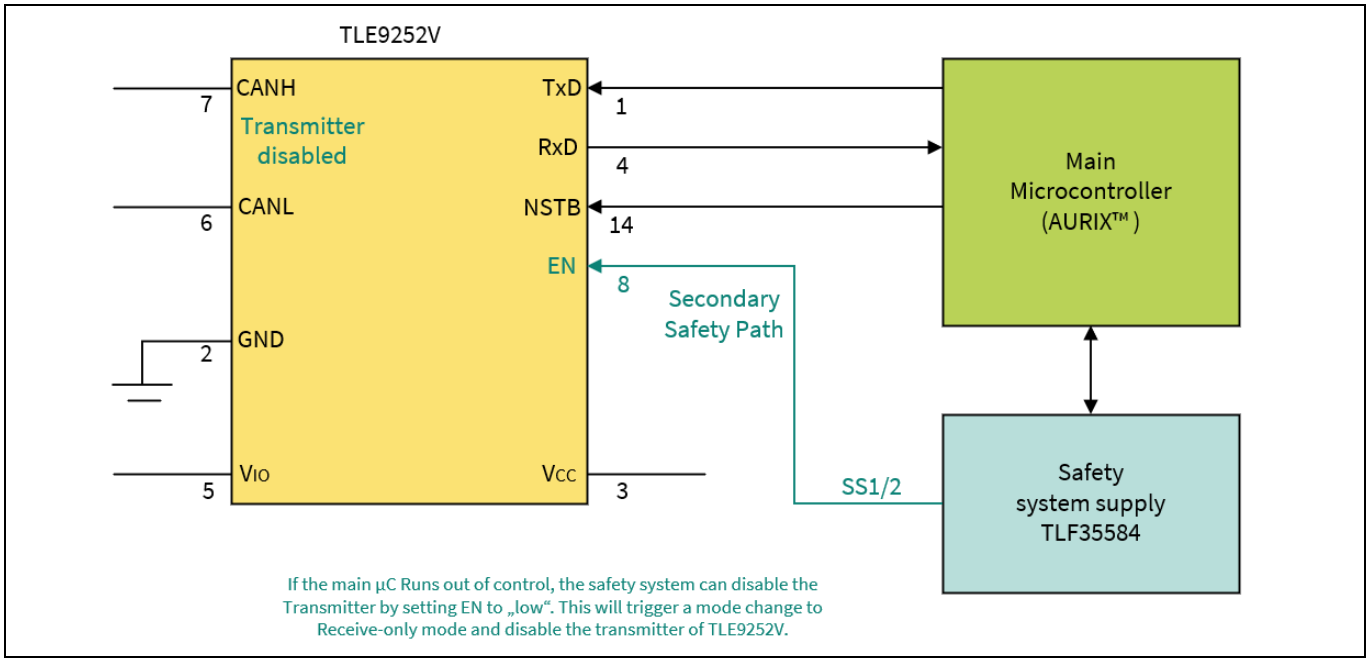

Figure 20 TLE9252V CAN transceiver connections with MCU and power supply

Referring to Figure 20, the connection required with the MCU is reported in Table 3.

Table 3 AURIX™ TC4xx-TLE9252V connections

S.No	AURIX™	CAN TR.	Description
1	CAN	TxD	Transmit data input from the MCU
2	CAN	RxD	Receive data output to the MCU
3	GPIO	NSTB	Stand-by control input (for the transceiver)

5.3.4.1 CAN Transceiver TLE9371VSJ as alternative to TLE9252V

Instead of TLE9252V, the TLE9371VSJ CAN transceiver could also be used. The choice depends on the features needed for the specific project.

The TLE9252V and TLE9371VSJ are both high-speed CAN transceivers designed for automotive applications, but they serve different performance tiers and incorporate distinct core technologies.
The primary distinction is that the TLE9371VSJ features CAN FD Signal Improvement (SIC) technology, enabling higher data rates and enhanced signal integrity compared to the standard CAN FD capabilities of the TLE9252V. This feature actively improves the signal on the bus to reduce ringing, which allows for more complex network topologies and supports a higher maximum transmission rate of up to 8 MBit/s.

Table 4 AURIX™ TC4xx-TLE9252V connections

Feature	TLE9252V	TLE9371VSJ
Core technology	Standard High-Speed CAN FD	CAN FD with Signal Improvement (SIC) ,
Max. data rate	5 MBit/s ,	8 MBit/s ,
Operating Modes	Normal, Receive-only, Stand-by, Sleep, Go-to-Sleep	Normal, Standby ,
Mode control pins	EN, NSTB	STB
Low power current	Max 26 µA in Sleep Mode	Typ. < 10 µA on VIO in Standby Mode
Wake-up sources	Bus Wake-up (WUP) and Local WAKE pin	Bus Wake-up
Diagnostic output	Dedicated NERR pin for local failures ,	No dedicated diagnostic pin mentioned
Inhibit pin (INH)	Yes, for controlling external regulators	No
Package	PG-DSO-14, PG-TSON-14 (variants)	PG-DSO-8

While the TLE9252V and TLE9371VSJ are not listed as fully ISO 26262 compliant, they can still be used in an ISO 26262-compliant system. According to the standard's guidelines (part 8, clause 13), it is possible to use QM parts in safety-relevant applications provided that the system integrator provides "evidence of the suitability of hardware components and parts".

5.4 Battery disconnect unit (BDU)

The switch box/battery disconnection unit is the unit that contains at least the elements used to disconnect HV sides (plus and minus) of the supply when fault information arrives from the battery pack or the vehicle control unit, or a crash signal or loss of insulation happens. BDU block is essential to satisfy the Safety Goal 1 and 2, as detailed in Section 3).

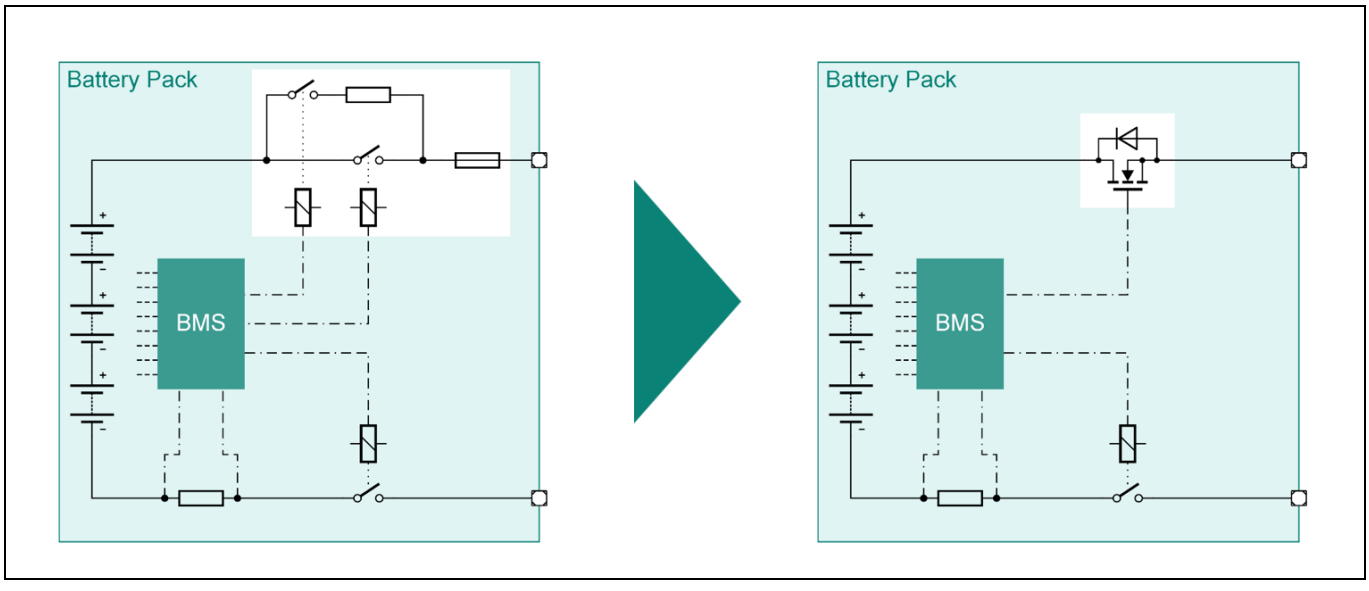

Figure 21 Battery disconnection unit evolution

BMS technical safety concept and requirements overview

Main elements of the switch box, also called BDU are:

- eFuse or High-side relay
- Pyro-fuse
- Low-side relay

These protective circuits are required to prevent critical event like overvoltage, short circuit, load inrush, and reverse polarity.

In traditional BDU, the disconnection unit is composed of a low-side relay, a high-side relay, and a high side preload.

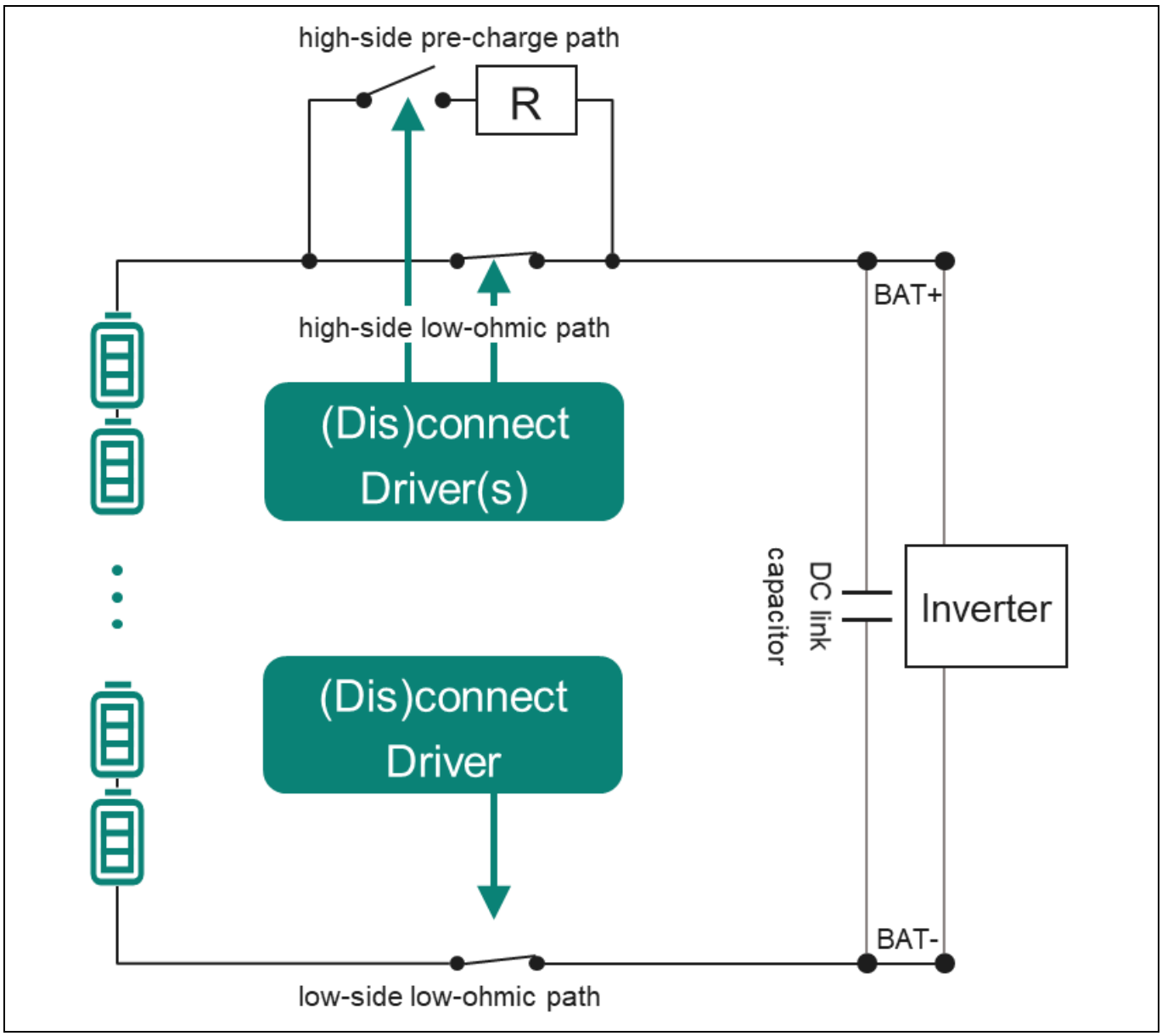

Figure 22 Switch box basic diagram

5.4.1 HV+ disconnection or eFuse

The high side of the HV connection normally host the fast-acting switch that is composed of a gate driver and two MOSFETs. It often also presents a “pre-charge” feature to load the inverter capacitors without destroying them.

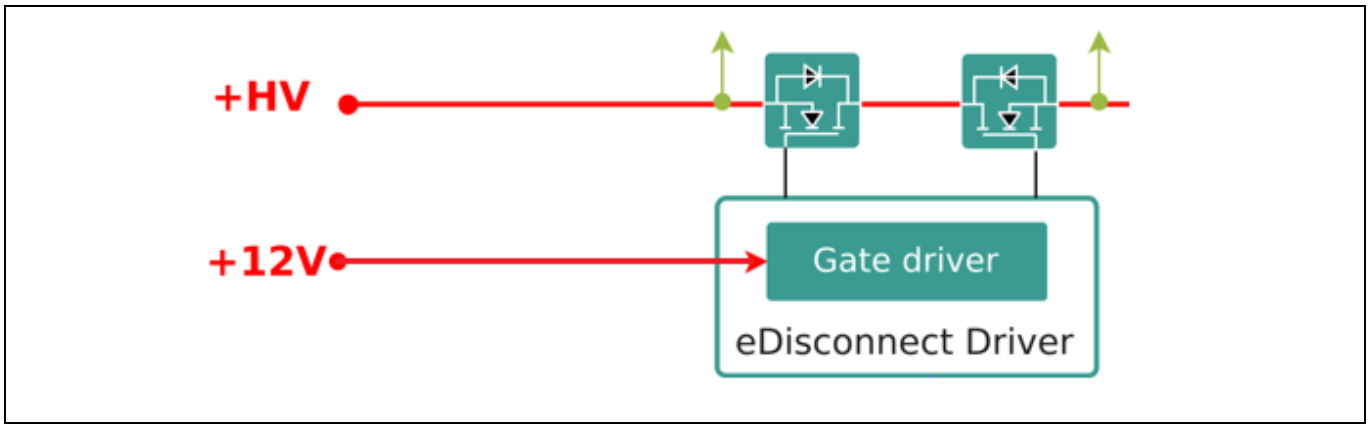

Figure 23 HV+ E-disconnect

5.4.1.1 Gate driver

A possible gate driver that could fit to this application is EiceDRIVER™ 1EDI3033AS. The device is a high-voltage SiC gate driver designed for automotive motor drives above 5 kW. The device is based on Infineon’s Coreless Transformer (CLT) technology, providing galvanic isolation between low-voltage and high-voltage domains. The device has been designed to support SiC MOSFETs up to 1200 V.

The device can be connected on the low-voltage side (“primary” side) to 5 V and 3.3 V logic. On the-high voltage side (“secondary” side), the device is dimensioned to drive an external booster stage or directly SiC MOSFETs. Short propagation delays and controlled internal tolerances lead to minimal distortion of the PWM signal.

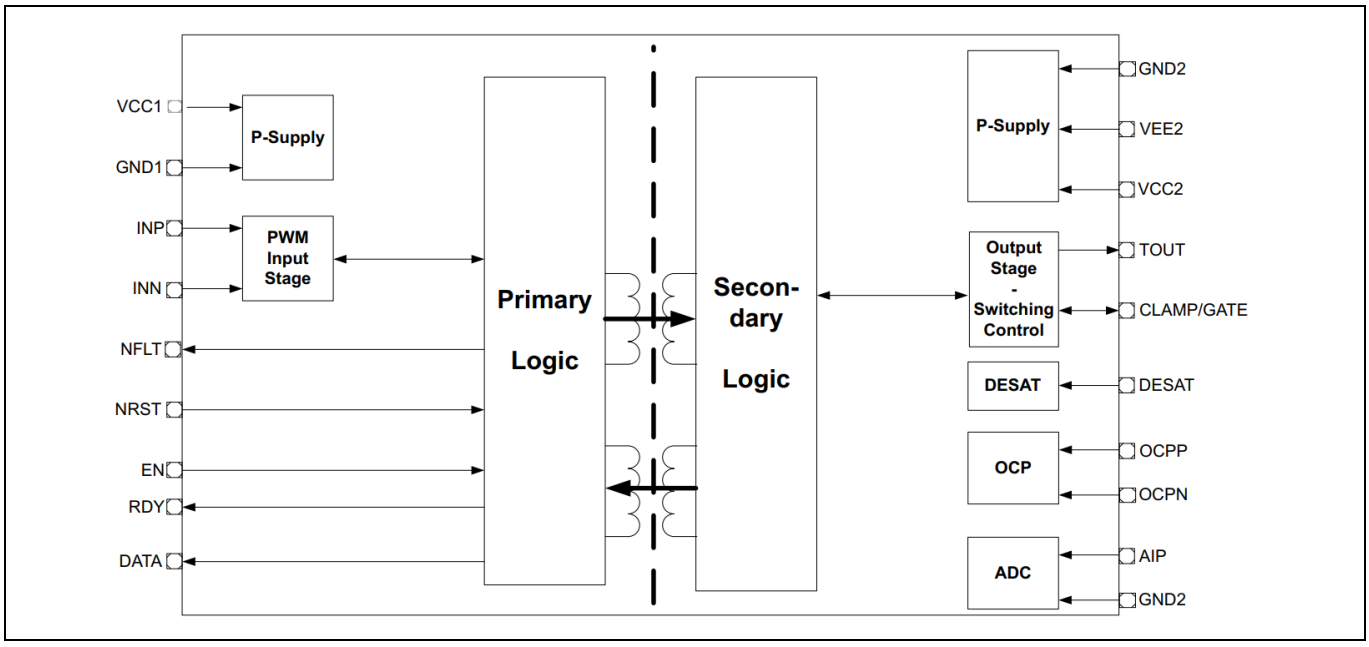

Figure 24 Block diagram of EiceDRIVER™ 1EDI3033AS

EiceDriver™ gate driver IC 1EDI302x/3xAS family offer, depending on the specific need is presented in the following table:

Table 5 EiceDriver™ product variant and its features

Product variant	Driver support	Additional functionality
1EDI3020AS, Diode	IGBT	ADC for Temperature
1EDI3021AS	IGBT	Active Short Circuit
1EDI3023AS	IGBT	ADC for NTC & DC-Link
1EDI3030AS	SiC	ADC for Temperature Diode
1EDI3031AS	SiC	Active Short Circuit
1EDI3033AS	SiC	ADC for NTC & DC-Link

5.4.1.2 E-switches (IPDQ60R010S7A)

IPQC60R010S7A combines the experience of the leading SJ MOSFET supplier with high class innovation enabling low R in QDPAK package. The S7A series is optimized for low-frequency switching and high-current application like circuit breakers.

Potential applications are circuit breakers (HV Battery disconnect switch, DC and AC low frequency switch, HV E-fuse) and diode paralleling/replacement for high power/performance applications.

Infineon's CoolMOS™ S7 SJ MOSFET makes it economically convenient to see superjunction technology as an effective way to replace electromechanical relays and circuit breakers or to improve existing solid-state designs.

Infineon's CoolMOS™ S7 compared to electromechanical devices:

- Switches faster
- Does not have contact arcing, bouncing, or degradation of on-resistance over a lifetime
- Ensures system reliability and considerably longer system lifetime
- Resistant to shock and vibrations and is not sensitive to mounting position

5.4.2 HV- disconnection

On the HV- side, the contactor circuit is described in Figure 25. The low-side switch is between the relay and the negative power of relay-driver-PMIC and the high-side switch between the relay and the contactor-drive-PMIC positive power. High-side switch is made of P-MOS (PROFET) and low-side is made of N-MOS (HIFET).

This units provides overvoltage, overcurrent, and overtemperature protection. OPTIREG™ is used as a regulator to drive the PROFET™ and the HIFET™.

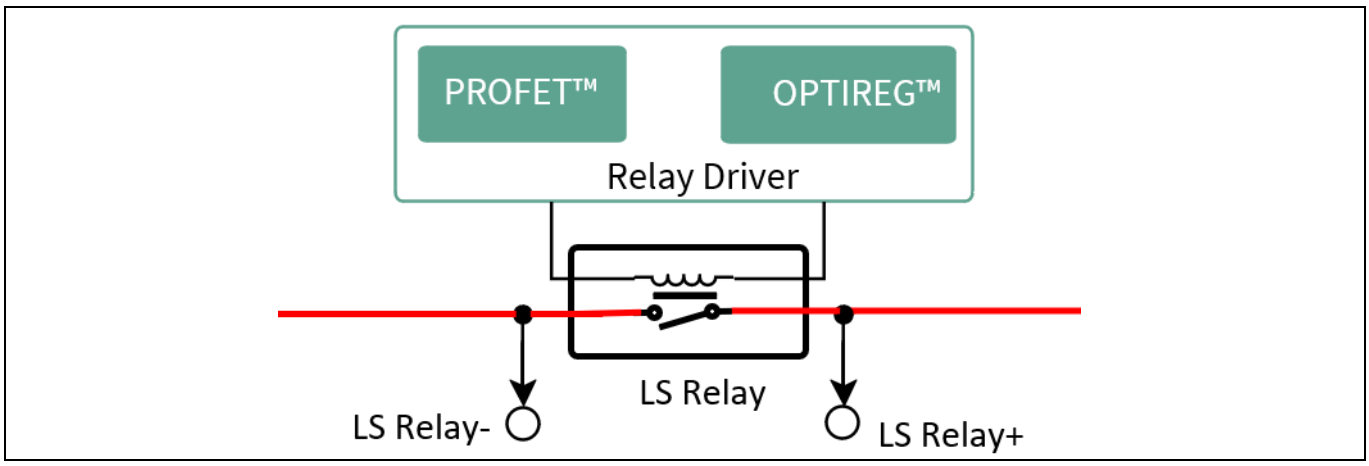

Figure 25 HV- relay

The low-side disconnect unit is composed of the following elements:

- Low-side power switch (HIFET™)
- High-side power switch (PROFET™)

5.4.2.1 Low-side power switch (HIFET™)

A smart low-side power switch provides overvoltage protection, over-temperature protection, and current limitation. Infineon has developed its own smart switches, such as **BTS3125EJ** , which provides an auto-restart thermal shut-down function.

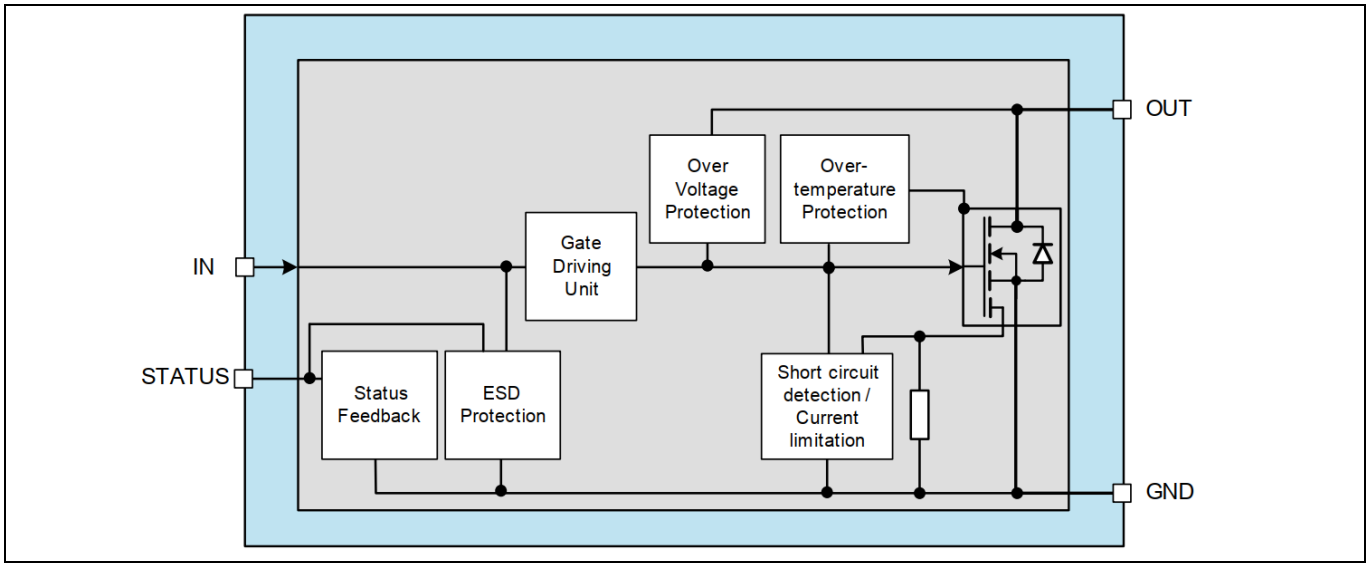

Figure 26 Block diagram for the BTS3125EJ

5.4.2.2 High-side power switch (PROFET™)

A smart high-side power switch provides overcurrent protection, overvoltage protection, and undervoltage shutdown. It can detect open load, short circuit, and can sense load current.

Infineon's high-side smart switches, such as **BTT6020-1ERA**, is protected against overtemperature, overload, reverse battery and overvoltage.

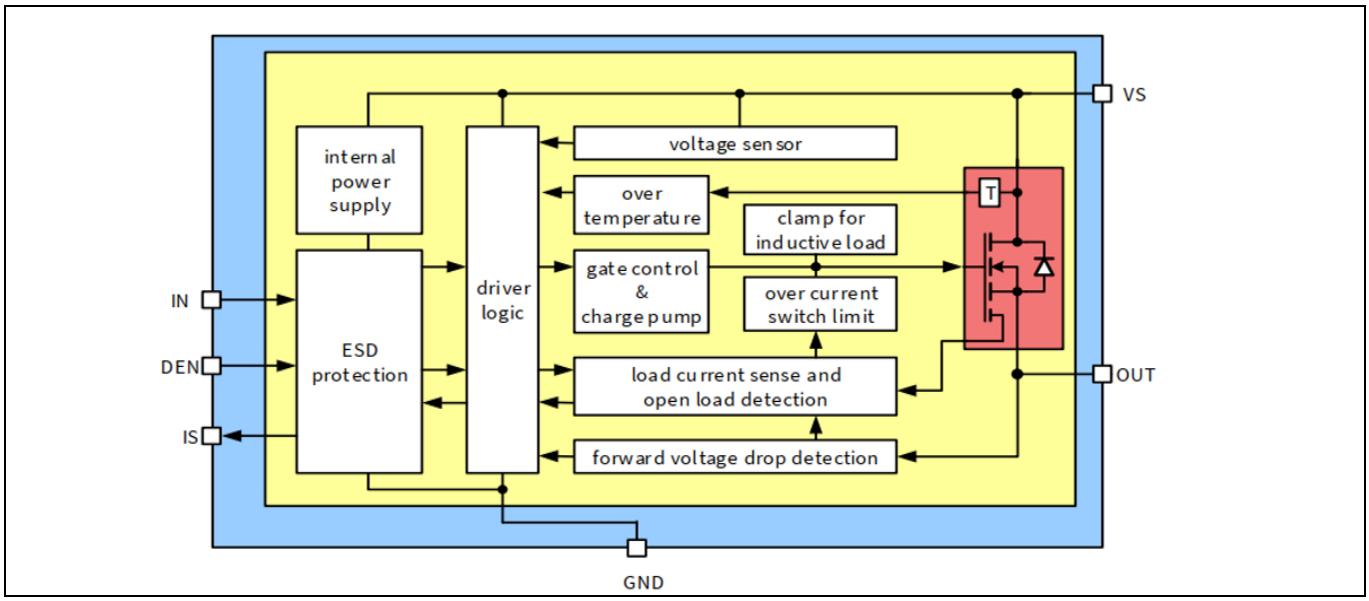

Figure 27 Block diagram for the BTT6020-1ERA

6 New trends – Highly available systems

6.1 Redundant power supply

In the near future, the HV battery could be divided into two HV battery blocks, splitting the DC-DC converter as well, to provide two low-voltage outputs each. This would allow the DC-DC converter to not only charge the low-voltage battery but also power critical systems such as brake-by-wire and steer-by-wire systems.

Having the two HV batteries will allow the system to keep running, even if one of the batteries fails, providing limited functionality in such cases.

In Figure 28, a traditional fail-safe supply system is represented. In this system, the presence of any redundancy is not intended to support fail-operational system like steer-by wire, but rather to maintain supply for the minimum time, allowing the system to send an alarm indication or a remote help request in case of a HV battery fault.

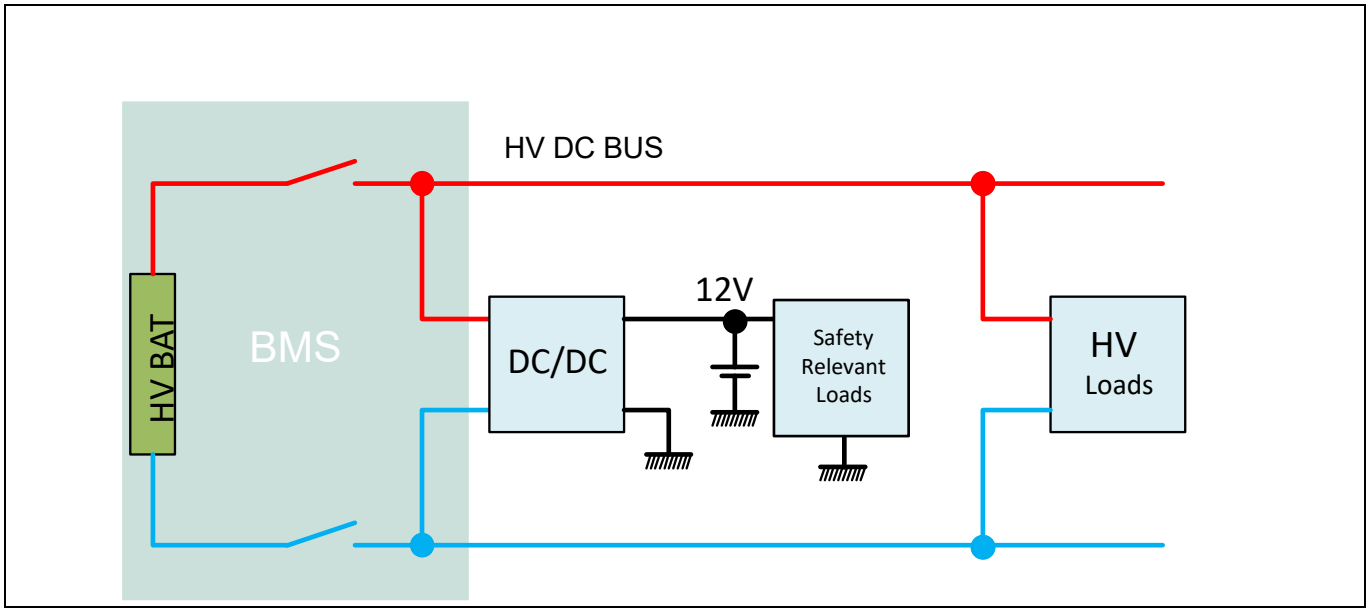

Figure 28 Fail safe supply – state of the art

In the automotive scenario, ADAS and x-by-wire requirements are driving the need for higher and ASIL-rated energy availability with:

- Redundant high voltage availability for ASIL-rated functions
- ASIL-rated battery State-of-Function for x-by-wire
- Redundant low voltage power distribution for x-by-wire requirements

Due to functional safety and other legal requirements, the safe state has to be empowered by the availability of the energy supply. This could also bring a cost reduction due to the removal of 12 V batteries, receiving supply directly from traction energy storage system.

The way these new requirements will be satisfied implies replacing the high-voltage mechanical disconnects with a solid-state relay. The availability is achieved by using solid state disconnect switches and ASIL rated redundant HV/12 V DC-DCs and micro-DC-DCs.

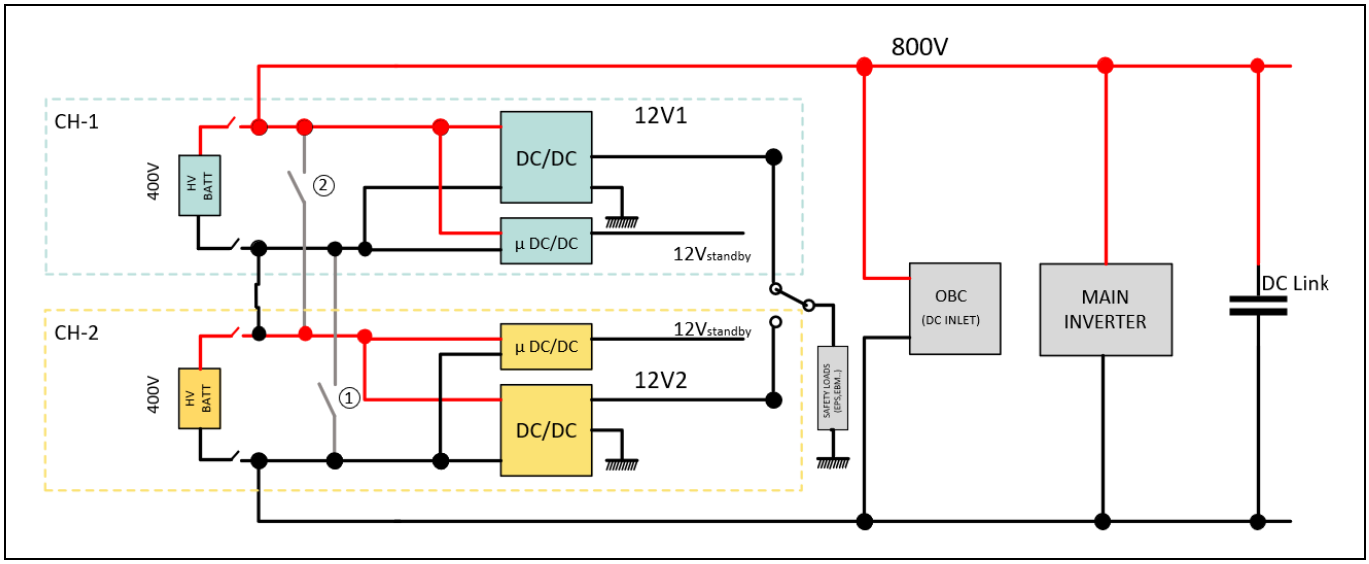

Figure 29 Example of fault tolerant system

6.1.1 TLE90xx, cell monitoring and balancing, and EIS

The complex impedance of lithium-ion batteries holds significant insights into their state of charge (SOC) and state of health (SOH). This is why many recent studies are focused on Electrochemical Impedance Spectroscopy (EIS) and the benefits it would bring.

EIS is a technique used to **measure the electrical properties of a battery**. It involves applying a small electrical signal to the battery and then measuring the response of the battery over a range of frequencies. EIS is particularly relevant for a BMS because it provides a way to monitor the health of the battery and ensure that it is performing optimally.

Traditionally, electrochemical impedance spectroscopy is conducted when the battery cells are in a relaxed state. However, today new solutions have enabled the performance of EIS during actual battery operation, made possible by the use of switching power converters.

By analyzing the impedance of the battery over time, the BMS can detect changes in the battery's behavior that may indicate that it is degrading or approaching the end of its useful life.

This information can be used to help in optimizing the performances and lifespan of the battery.

Coupling Infineon TLE90XX Cell Monitoring and Balancing ICs and PSOC™ 4 HVPA SPM 1.0 permits to explore this new methodology during the working phase of BMS.

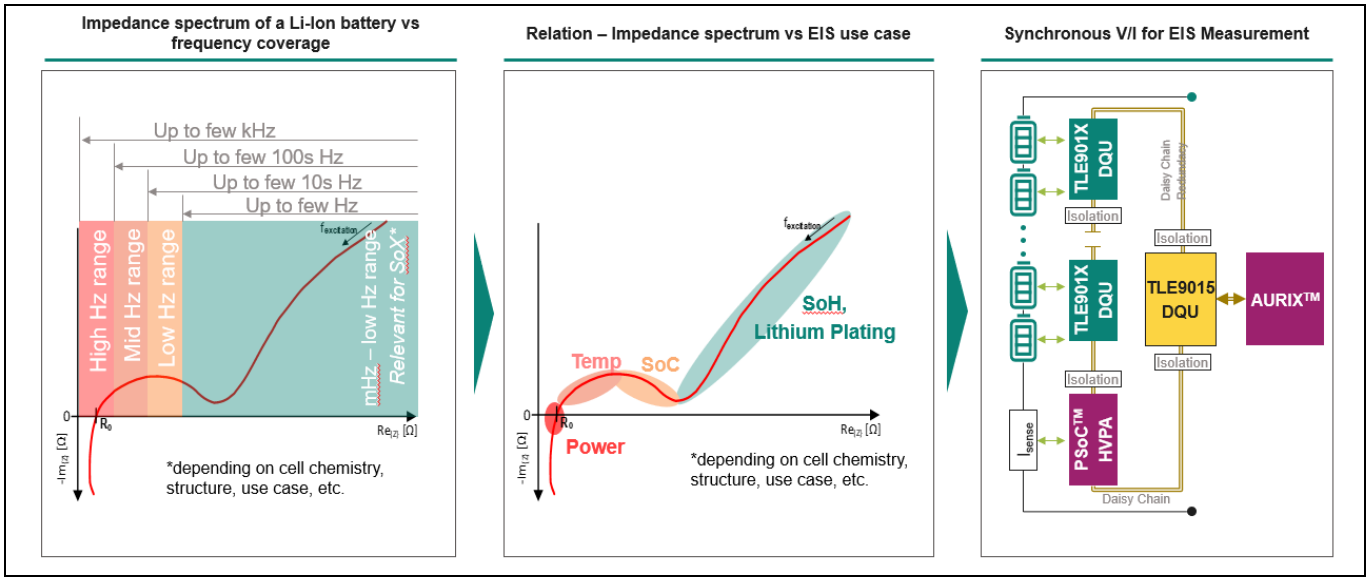

Figure 30 Inherent EIS with synchronous V/I measurement between TLE90xx and PSOC™ 4 HVPA

Enhanced EIS might require a lot of data (measured, stored and calculated). If, for example, sophisticated electrochemical models or digital twins were used, then a faster data transmission would be required (Iso UART2.0) and more calculation power would be beneficial. For this purpose, TLE90xx products and TC4xx PPU would be the perfect solution to enable EIS technique.

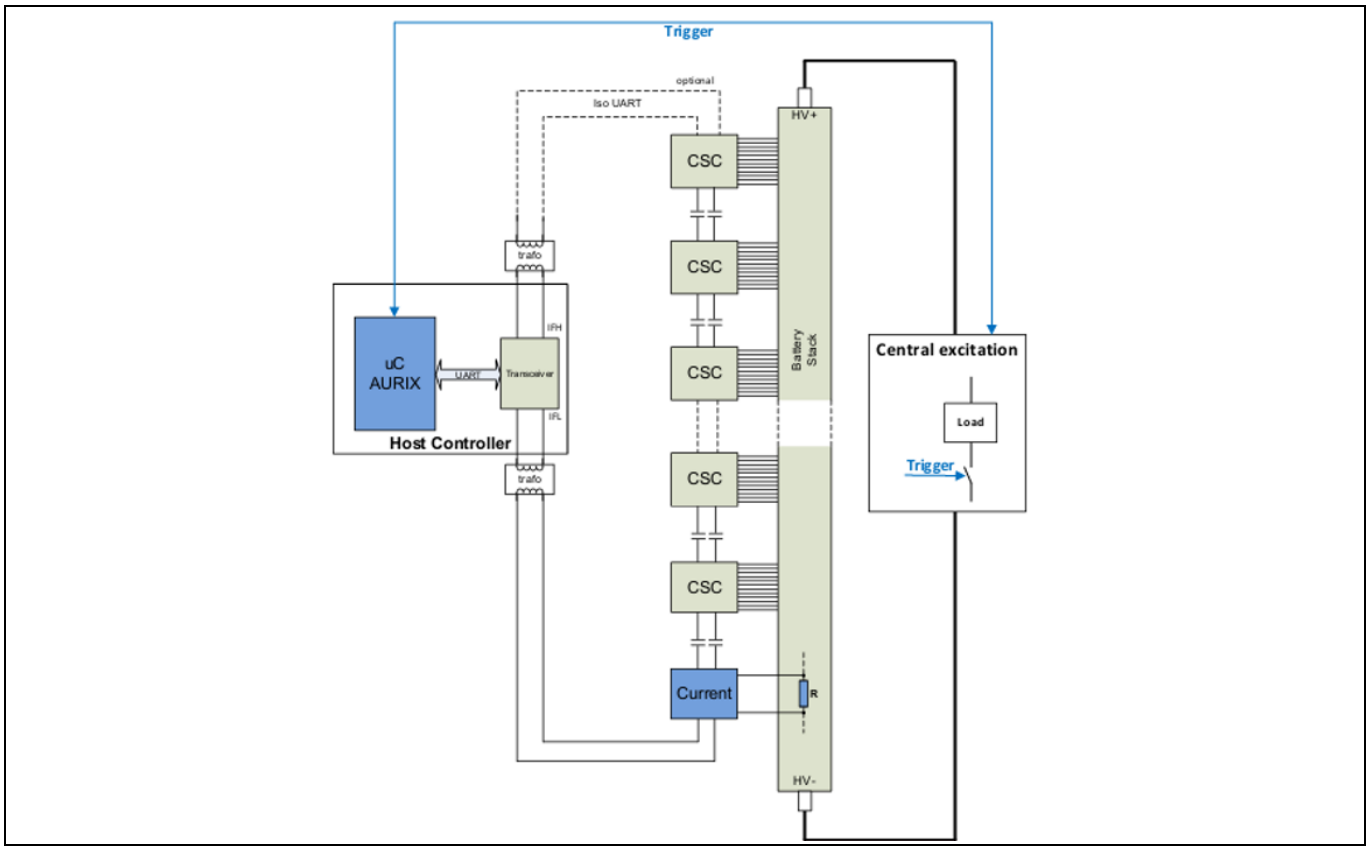

Figure 31 Example of usage of TLE9018, TLE9012, PSOC™, and AURIX™ in EIS use case

New trends – Highly available systems

The required number of TLE09018 chips (see Section 5.1.1) accomplishes the cell monitoring and the cell balancing needs of the battery cells and send the data to the local microcontroller (PSOC™ 4 HVPA SPM 1.0 in our example). Cell monitoring sensors communicate in daisy chain, including also PSOC™. PSOC™, as last element of the daisy chain, transmits data to the transceiver (**TLE9015DQU**) that then will forward them to the core MCU AURIX™ TC4xx.

7 Related resources

- 32-bit TriCore™ AURIX™ – TC4x webpage
- PSOC™ 4 HVPA-SPM 1.0
- High Voltage BMS application
- AURIX™ digital documentation
- Knowledge base articles

References

[1] ISO 26262:*2018 Road vehicles- Functional safety*

[2] Infineon Technologies AG: *AN1000 - FuSa in a Nutshell - release note*; Available online

Glossary

Table 6 Glossary

Definition	Description
ASIL	Automotive Safety Integrity Level; refer to ISO 26262-1:2018, 3.6
BDU	Battery Disconnect Unit
BEV	Battery-powered Electric Vehicle
BMS	Battery Management System
BMU	Battery Management Unit
CMB	Cell Monitoring and Balancing
CMU	Cell Monitoring Unit
EIS	Electrochemical Impedance Spectroscopy
ESS	Energy Storage System
HARA	Hazard Analysis and Risk Assessment; Refer to ISO 26262-1:2018, 3.76
HW	Hardware
IC	Integrated Circuit
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PMIC	Power Management ICs (PMICs)
PMU	Pack Monitoring Unit
Safety Measure	Activity or technical solution to prevent, detect, control or mitigate systematic and random failures
SM	Safety Mechanism: for the definition refer to ISO 26262-1:2018, 3.142
SW	Software
VCU	Vehicle Control Unit

Revision history

Document revision	Date	Description of changes
V 1.0	2025-10-24	Initial release

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

PSOC™, formerly known as PSoC™, is a trademark of Infineon Technologies. Any references to PSoC™ in this document or others shall be deemed to refer to PSOC™.

Edition 2025-10-24

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

AN1104

Important Notice

Products which may also include samples and may be comprised of hardware or software or both ("Product(s)") are sold or provided and delivered by Infineon Technologies AG and its affiliates ("Infineon") subject to the terms and conditions of the frame supply contract or other written agreement(s) executed by a customer and Infineon or, in the absence of the foregoing, the applicable Sales Conditions of Infineon. General terms and conditions of a customer or deviations from applicable Sales Conditions of Infineon shall only be binding for Infineon if and to the extent Infineon has given its express written consent.

For the avoidance of doubt, Infineon disclaims all warranties of non-infringement of third-party rights and implied warranties such as warranties of fitness for a specific use/purpose or merchantability.

Infineon shall not be responsible for any information with respect to samples, the application or customer's specific use of any Product or for any examples or typical values given in this document.

The data contained in this document is exclusively intended for technically qualified and skilled customer representatives. It is the responsibility of the customer to evaluate the suitability of the Product for the intended application and the customer's specific use and to verify all relevant technical data contained in this document in the intended application and the customer's specific use. The customer is responsible for properly designing, programming, and testing the functionality and safety of the intended application, as well as complying with any legal requirements related to its use.

Unless otherwise explicitly approved by Infineon, Products may not be used in any application where a failure of the Products or any consequences of the use thereof can reasonably be expected to result in personal injury. However, the foregoing shall not prevent the customer from using any Product in such fields of use that Infineon has explicitly designed and sold it for, provided that the overall responsibility for the application lies with the customer.

Infineon expressly reserves the right to use its content for commercial text and data mining (TDM) according to applicable laws, e.g. Section 44b of the German Copyright Act (UrhG).

If the Product includes security features:

Because no computing device can be absolutely secure, and despite security measures implemented in the Product, Infineon does not guarantee that the Product will be free from intrusion, data theft or loss, or other breaches ("Security Breaches"), and Infineon shall have no liability arising out of any Security Breaches.

If this document includes or references software:

The software is owned by Infineon under the intellectual property laws and treaties of the United States, Germany, and other countries worldwide. All rights reserved. Therefore, you may use the software only as provided in the software license agreement accompanying the software.

If no software license agreement applies, Infineon hereby grants you a personal, non-exclusive, non-transferable license (without the right to sublicense) under its intellectual property rights in the software (a) for software provided in source code form, to modify and reproduce the software solely for use with Infineon hardware products, only internally within your organization, and (b) to distribute the software in binary code form externally to end users, solely for use on Infineon hardware products. Any other use, reproduction, modification, translation, or compilation of the software is prohibited. For further information on the Product, technology, delivery terms and conditions, and prices, please contact your nearest Infineon office or visit https://www.infineon.com