

Functional Safety Considerations in Battery Management for Vehicle Electrification



David Tatman
Systems Engineer
Battery Management Systems
Texas Instruments

TI POWER

Li-ion batteries in electric vehicles need to operate within a limited range of temperatures and operating voltages for the best performance and safest operation.

At a glance

This paper examines battery monitor considerations to meet functional safety standards in electric vehicles.



1 EV requirements for battery management systems

Changing market conditions are driving higher standards for safety requirements.



2 Monitoring battery cell voltage and temperature

High-accuracy battery monitors help ensure the most rigorous functional safety standards are met.



3 Designing for redundancy

Redundant communication protocols provide fault tolerance and ensure the state of health and safety of the battery pack.

EV requirements for battery management systems

The world is in the midst of a transportation revolution. Advances in lithium-ion (Li-ion) battery technology in the past two decades have made it possible to envision a future where electricity is stored in battery packs that power cars, motorcycles, trucks and buses.

In parallel, de-carbonization of the energy economy is a high priority in many parts of the world. It is much easier to reduce emissions a vehicle's energy source at the power grid generation level than at the vehicle level. Achieving

de-carbonization targets requires the electrification of the majority of transportation systems. Spreading the costs of electric vehicle (EV) development and production over the increasing numbers of EVs planned means that EV prices are falling fast and approaching internal combustion engine (ICE) vehicle prices.

Safety considerations for a battery system in a passenger vehicle are multifaceted. There are important traditional electrical safety considerations for keeping production workers, owners, mechanics and vehicle recyclers safe from high-voltage exposure and shock. There are mechanical considerations for protecting battery cells from puncture and impact damage and for containing liquids and gases that could leak or vent from the cells. There are thermal safety considerations in the battery pack design, since Li-ion batteries operate safely and most efficiently in a more restricted temperature range than temperatures present in an ICE vehicle. There are functional safety considerations for the electrical system that maintains the battery in a safe operating range while the vehicle is in use or charging.

Monitoring battery cell voltage and temperature

Li-ion batteries (as shown in **Figure 1**) need to operate within a limited range of temperatures and operating voltages for the best performance and safest operation. This range is unique for each type of Li-ion battery chemistry. Outside of this range, undesirable side reactions may occur within the battery that can lead to excessive self-heating and perhaps longer-term, internal electrical shorts. Excessive self-heating and internal shorts can be a first step to cascading thermal runaway and an eventual safety hazard. In order to maintain battery packs in that safe operating range, battery monitoring application-specific integrated circuits (ASICs) measure and transmit information about voltage, temperature and current flow to a battery control unit.

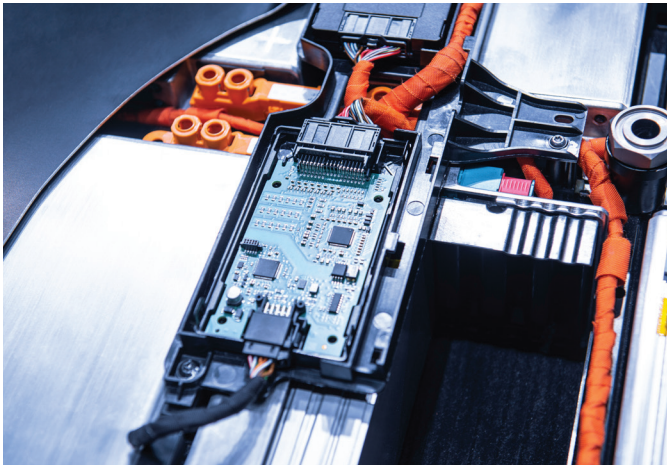


Figure 1. A battery pack in an EV.

In an electrified passenger vehicle, there may be 16, 96 or 128 battery cells or more to measure. In a commercial vehicle, the total cells may be double those amounts. Such large systems have many printed circuit board (PCB) connections, where faults can occur between the battery and the monitoring ASIC, or in the communication connections between ASICs. The sensor input may open or communication may be lost. Without the necessary measurements and communications, the battery control system is “blind” and can no longer manage the state of the batteries in the pack.

Detecting and addressing malfunctions like a communication fault or battery cell to sensor connection faults avoiding hazardous events is a part of functional safety.

Functional safety is the part of comprehensive safety related to the prevention and mitigation of potential hazardous events caused by the malfunctioning behavior of electronic systems. In the automotive industry, the International Organization for Standardization (ISO) 26262 series of standards for road vehicle functional safety defines the current state of the art and functional safety best practices

for the development of safety-related systems for passenger vehicles, trucks, buses and motorcycles.

In some automotive systems, a loss of functionality cannot lead to a hazard. In the case of a malfunction within the system, the safe state for the system is for the electronics to switch off and the driver to be alerted through a dashboard light or other indicator. However, in some systems a malfunction or the loss of functionality can potentially lead to a hazardous event. For systems that cannot simply switch off, safety goals may include specifying a “safety-related availability” requirement. In that case, a tolerance for some types of faults in the system for a period of time may be required to avoid hazardous events.

Safety-related availability in this context is the system’s ability to provide safety functionality for some specified period of time even in the presence of defined fault conditions. In other words, the safety system has to tolerate a fault for a period of time. This fault tolerance enables the system to continue functioning longer with an acceptable level of safety. Part 10, Section 12 of ISO 26262 provides guidance for system developers regarding safety-related availability requirements.

Returning to the battery monitoring subsystem, battery cell voltage and temperature sense locations connect to the battery-monitoring ASIC. The measurement information is frequently read by the control processor to calculate the current state of the battery and to help ensure that operation remains within a safe range. For high-voltage battery packs, the monitoring ASICs are arranged in a stacked configuration, with each ASIC measuring multiple cells in parallel. Commands and data are streamed from ASIC to ASIC using an isolated communication interface, as shown in **Figure 2**.

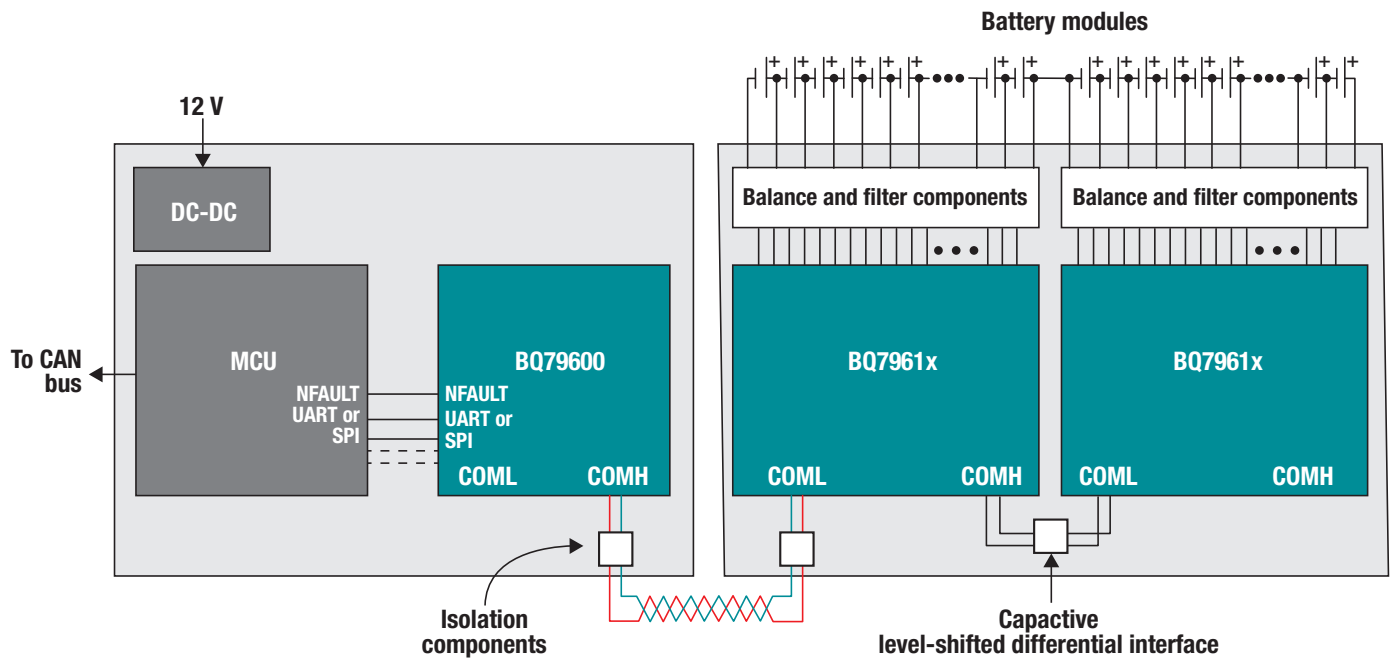


Figure 2. A battery monitoring and communication configuration.

Designing for redundancy

Should an open circuit occur between the battery cell input pin and the PCB while driving, a loss of functionality of the battery monitoring system can occur and potentially lead to a hazardous event. The Texas Instruments [BQ79606A-Q1](#) and [BQ79616-Q1](#) families of battery monitoring ASICs includes features for ring communication, as well as a

redundant battery voltage measurement path that can provide fault tolerance for these types of faults, enabling the system to continue monitoring the state of health and safety of the battery pack.

Figure 3 illustrates the BQ79616-Q1 connection using a bidirectional ring configuration. In this configuration, if there is a fault, open or short between two of the battery

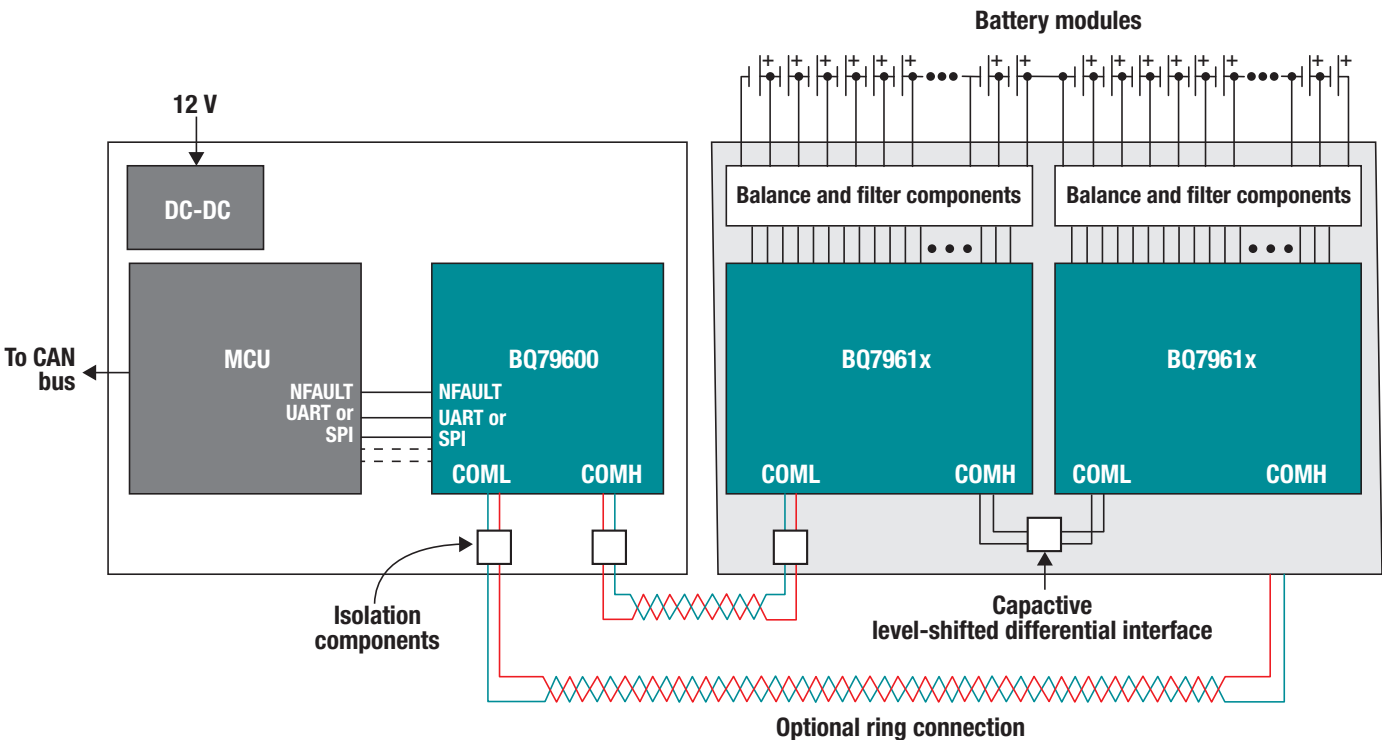


Figure 3. A bidirectional ring configuration with the BQ79616.

monitoring ASICs, the control processor will continue communicating with all of the battery monitoring ASICs switching the direction of messaging backward and forward. While normal communication is faulted, the system can maintain availability using the fault tolerance of the ring communication feature – with no loss of voltage and temperature information coming from the battery modules.

Another feature in TI's BQ79606-Q1 and BQ79616-Q1 is the redundant analog-to-digital converter (ADC) measurement path using cell balance input pins connected to the battery cell. **Figure 4** illustrates the connection from the battery cell to the VC and CB input pins. Normally, the CB pins enable a DC current load on the cell in order to balance the voltages between cells. During normal measurement operation, both the main VC ADC path and redundant CB ADC path connect to the battery cell and can measure the battery cell voltage. With this feature, if there is a fault like an open VC pin connection to the R_{CB} or an open R_{VC} resistor, the CB ADC path will continue measuring the battery cell voltage. While normal voltage measurement is faulted, the system can maintain availability using the fault tolerance of the redundant ADC path feature – with no loss of voltage information coming from the battery modules.

These ring communication and redundant path features, along with a wide range of diagnostic safety mechanisms for detecting communication and connection faults during EV battery cell voltage and temperature sensing, are included in both the TI BQ79606-Q1 and BQ79616-Q1 device family for systematic functional safety capability up to Automotive Safety Integrity Level (ASIL) D.

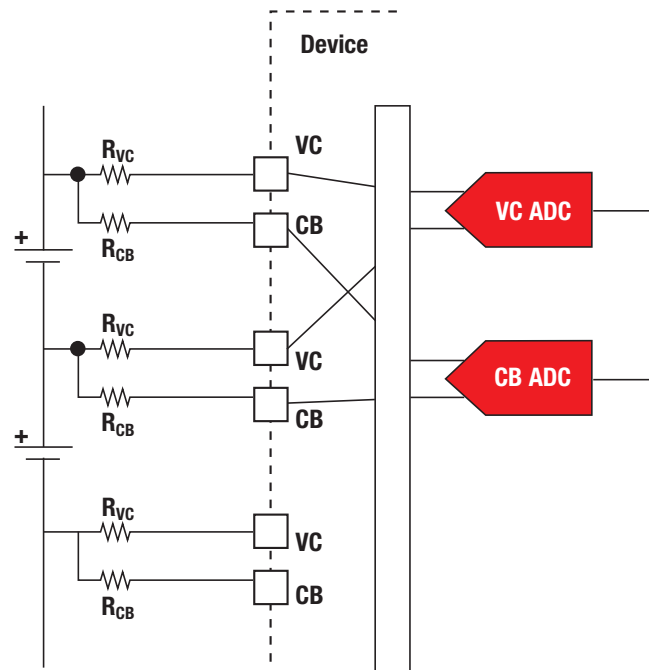


Figure 4. Connection from the battery cell to the VC and CB inputs.

Summary

Much like the beginning of the transition from animal-drawn wagons to motors in the early 20th century, today there are a wide range of vehicle solutions being developed to provide the most benefit to society. For electrified transportation systems, safety requirements are essential.

Additional resources:

- [TI's functional safety technology page](#)
- [BQ79606A-Q1 Daisy Chain Communication Timing](#)
- [BQ7961x-Q1 data sheet](#)

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.

All trademarks are the property of their respective owners.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL 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 AND 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 skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI 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. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to TI's Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2020, Texas Instruments Incorporated