Technical White Paper

Functional Safety-Relevant Wireless Communication in Automotive Battery Management Systems

Tomas Urban *Automotive Powertrain Systems*

1 Introduction

Battery manufacturers want to achieve the highest possible density of energy. This applies especially to electric or hybrid vehicles (EV/HEV) where achieving the maximum drive range attracts customers. With increasing energy density, the importance of battery management and monitoring is essential to avoid any kind of hazards related to overvoltage or overtemperature.

Batteries in EV/HEV reach nominal voltages of 400 V or 800 V. The batteries are typically organized in modules – groups of cells – that are managed by a dedicated battery management integrated circuit (BMIC). Typically one BMIC can monitor up to 16 cells connected in series.

Apart from other features that are not in the scope of this paper, the main role of the BMIC is to periodically measure the cell voltages and temperatures. These quantities are converted into digital form and conveyed towards a host BMS control microcontroller (MCU). The information from the BMIC is vital for calculating the state of charge and state of health. In the context of BMS, BMICs are also functional safety-relevant.

The requirements for communication in any BMS implementation include:

- Provide the host MCU with a refreshed cell data when requested
- Enable the host by verifying the overall correctness of the data

As illustrated in Figure 1-1, typical BMICs exchange data with the host MCU over a wired connected in daisy-chain topology.

Since the system cost and battery configuration flexibility are high priorities for car manufacturers, a trend can be seen that the safety-relevant battery data are transferred over a dedicated wireless link within the HEV/EV battery.

Using wireless data transfer brings significant savings on cabling, connectors, and isolation components as well as on the assembly time of the complete battery.

A requirement on ASIL D on the system level remains from the wired systems and it translates into an ASIL D-compliant communication error detection in wireless implementations. The following text considers such data exchange in the light of automotive functional safety.

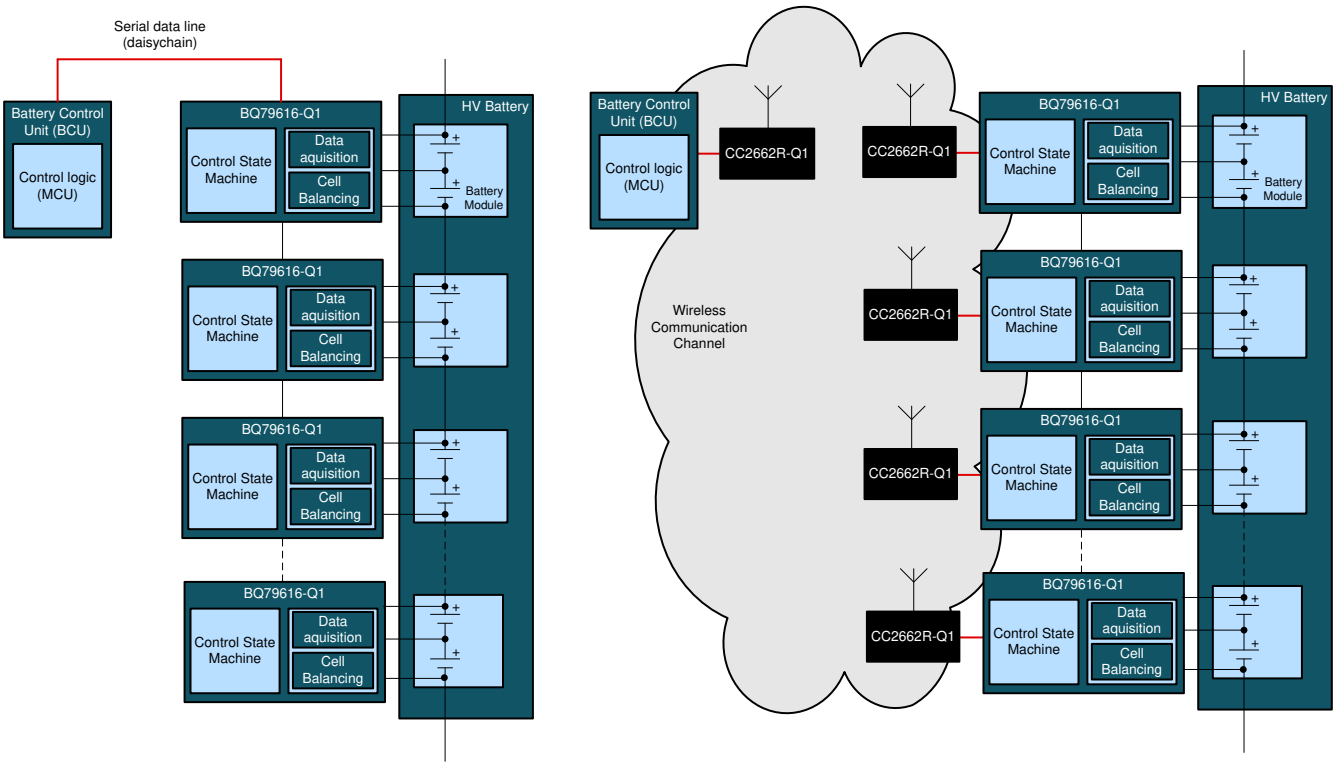

Figure 1-1. Wired vs Wireless BMS

The BMICs and the host MCU are basic components of the wired BMS whereas in a wireless BMS, the wired daisy chain is replaced with wireless controllers and appropriate communication protocol.

The wireless controllers from TI are Systems-on-Chip (SoC) that integrate a radio frequency (RF) physical layer and user-programmable MCU core that may implement communication protocol stacks and application software (SW). These wireless SoCs (WSoCs) are targeted at a wide range of applications, offering various on-chip features while keeping the cost competitive for automotive or consumer products.

The reason for mentioning this is related with a fact that the typical wireless SoCs (including those from TI) do not comply with functional safety standards from a random hardware (HW) faults diagnostic coverage standpoint.

2 Communication Architectures

Generally there are two possible architectures for safety-relevant data transmission. They are described in IEC61508-2[2] (a basic functional safety standard available from the IEC Webstore) in section 7.4.11.

- White channel – where **complete** HW, SW (including transmission protocols) are developed and validated according to functional safety standards
- Black channel – where **end** elements including HW, SW (including transmission protocol) comply with functional safety standard and part or parts of the communication channel between compliant end interfaces do not comply with any specific functional safety standard. For details, see the *Black channel* portion of the *Architectures for data communication* image (*Figure 7*) in the *IEC61508-2 Standard*[2] .

The automotive BMICs from TI are functional safety-compliant devices that offer numerous safety mechanisms to help enable system-level capability up to ASIL D according to ISO 26262[1]. Built-in communication protocol enables the host MCU to detect and report the possible communication errors and HW faults (BMICs from TI do not include any programmability or software).

The wired BMS with a functional safety compliant MCU on one end and functional safety compliant BMIC on the other end are typical examples of a white channel approach.

Conversely, the wireless controllers (as mentioned) are not functional safety compliant components thus the **Black channel approach** must be used.

3 Communication Errors in Wired Versus Wireless Data Transmission

One of the most important disciplines in safety-relevant data transmission is the ability of the HW and the SW to detect potential errors. Fortunately, the types of the errors and recommended approaches how to detect them have been standardized.

Standards IEC62280[4] and IEC61784-3[3] discuss functional safety data transmission implications and requirements which are generally unaffected by the transmission media. These standards give us a summary of types of communication errors and measures that detect them. Refer to IEC61784-3[3] for a detailed description of the communication errors.

Table 3-1 details those potential errors from the perspective of wired and wireless BMS architecture.

Table 3-1. Wired and Wireless BMS Communication Errors

Comm. Error	Wired BMS		Wireless BMS	
	Cause, Likelihood	Detection	Cause, Likelihood	Detection
Corruption	1. $P_E = 10^{-4} – 10^{-5}$ (3) 2. λ_{BMIC} (1)	Mismatch in CRC at MCU end	1. $P_E = 10^{-2} – 10^{-3}$ (3) 2. λ_{BMIC} (1) 3. λ_{WSoC} (2) 4. WSoC SW fault	Mismatch in CRC at MCU end
Unintended repetition	1. λ_{BMIC} (1)	Refresh of BMIC data monitored by on-chip safety mechanism	1. λ_{BMIC} (1) 2. λ_{WSoC} (2) 3. WSoC SW fault	Unexpected frame counter value at MCU end
Incorrect sequence	May be neglected as BMIC stores only the latest data.	N.A.	1. λ_{WSoC} (2) 2. WSoC SW fault	
Loss Unacceptable delay	1. $P_E = 10^{-4} – 10^{-5}$ (3) 2. λ_{BMIC} (1)	Timeout monitoring	1. $P_E = 10^{-2} – 10^{-3}$ (3) 2. λ_{BMIC} (1) 3. λ_{WSoC} (2) 4. WSoC SW fault	Timeout monitoring
Insertion	Highly unlikely in closed communication systems. May be neglected.	N.A.	1. λ_{WSoC} (2) 2. WSoC SW fault	Unexpected frame counter value at MCU end
Masquerade	Highly unlikely in closed communication systems. May be neglected.	N.A.	Highly unlikely in closed communication systems. May be neglected.	N.A.
Addressing	Can be neglected in wired BMS due to deterministic request-response communication scheme fully controlled by the host MCU.	N.A.	Can be neglected in wireless BMS due to deterministic request-response communication scheme fully controlled by the host MCU.	N.A.

(1) λ_{BMIC} represents a HW failure rate of the BMIC
(2) λ_{WSoC} represents HW failure rate of the wireless controller
(3) P_E represents a bit error probability in the communication channel

4 Evaluation of Detection Performance

Since the WBMS targets HEV/EV, the compliance according to ISO26262[1] shall be demonstrated on the system level. However, ISO26262[1] does not provide much guidance on how to address error detection in data communication. The only mention of qualitative requirements are in the following:

- ISO26262[1] Part 5 – evaluation of data communication diagnostic coverage in Table D.6.
- ISO26262[1] Part 6 – Exchange of information between software elements in section D.2.4

Diagnostic coverage (DC) “high” can be achieved by a combination of three measures:

- Information redundancy
- Frame counter
- Timeout monitoring

Those detection mechanisms must be implemented in WBMS. However; how does one **evaluate** if they are implemented **adequately**?

4.1 Qualitative – How the Errors are Detected

This section details how the errors are detected:

- Information redundancy – see Section 5
  - Implemented as CRC16 (end-end)
  - Additionally CRC32 – in WBMS protocol
- Frame counter – end-to-end implemented (details are found in the TI WBMS functional safety concept document)
- Timeout monitoring – this is straightforward – the host monitors the timeliness of data frames against the fixed and deterministic timing scheme

4.2 Quantitative – Probability Error Versus Probability of Non-Detected Error

Claiming a high DC according to ISO6262 allows detection of 99% faulty data frames (reference: ISO26262[1] D.1). It is easy to prove that 99% is **not sufficient** to achieve ASIL D PMHF for the WBMS communication.

The minimum duration for one frame exchange between host and a single node in TI WBMS equals 2 ms. That gives 1.8×10^6 frames per hour. Worst-case bit error probability as mentioned in Table 3-1 may achieve values as high as $P_E = 10^{-2}$ (reference: IEC61784-3[3]). This translates to a frame error rate of 1.8×10^6 frames per hour. It is an identical number as the frame rate. Why is this true?

1. $P_E = 10^{-2}$ shows that statistically every hundredth bit is corrupted.
2. Frames are much longer than 100 bits

Therefore, in every frame there is nearly a 100% probability that at least one bit is corrupted.

One might state “When every single frame is corrupted, there is no communication happening at all”. And that is correct. No valid communication happens at all, nevertheless **the system must remain safe** by detecting all these errors.

Naturally, this cause of communication errors (electromagnetic interference- EMI) is by far the most probable in the complete communication chain. Therefore, the quantitative error detection performance evaluation focuses solely on EMI-caused errors.

Assuming 1FIT target of residual (undetected) faults (out of total 10FIT for ASIL D) for the communication part of the WBMS, the required diagnostic coverage or better defined as “a probability of non-detection of a communication error” may be back-calculated as:

$$\text{A probability of non-detection of a communication error} = 10^{-9}/1.8 \times 10^{6} = 5.55 \times 10^{-15} \quad (1)$$

where:

- 10^{-9} is a failure rate corresponding to 1FIT
- 1.8×10^{6} is a frame error rate per hour

This value can be achieved by a combination of multiple detection mechanisms.

5 Implementation of Communication Protocols

IEC62280[4] describes a communication error model of the black channel in Annex C. The black channel includes HW, SW, and electromagnetic interference (EMI) factor that is responsible for all non-hardware related faults in the communication channel.

This model is implemented in TI WBMS as two underlying protocols:

1. The first one called “BQ protocol” is an identical end-to-end protocol that BQ79616-Q1 uses for communication over the wired interface. This protocol is implemented in the state machine of the BQ79616-Q1 and a host safety MCU. The BQ protocol runs on both ends on a trusted HW and in IEC62280[4] nomenclature corresponds with the safety code. On this layer, the following errors are detected:
   a. Errors caused by the failure of CC2662R-Q1 at each node (in IEC62280[4] nomenclature “non-trusted HW”)
   b. EMI factor with a detection performance of implemented IBM polynomial CRC-16
2. The overlaying proprietary protocol called “WBMS protocol” runs on CC2662R-Q1 devices. This protocol corresponds to the IEC62280[4] transmission code. The WBMS protocol serves as a container for BQ protocol frames and features many mechanisms improving security, authenticity, and availability of the communication channel but in scope of functional safety are two mechanisms:
   a. CRC-32 detecting EMI-caused data corruptions
   b. Four-byte MAC (Message Authentication Code) ensures authenticity and as well integrity of the messages. It adds up to the detection performance of EMI-caused communication errors.

The TI WBMS combines CRC-16, CRC-32, and MIC to detect a sufficient amount of interference-caused communication errors. The calculated probability of error not-detection is: 3.552×10^{-17}, or better, depending on the number of wireless nodes and bit error probability of the communication channel (P_E).

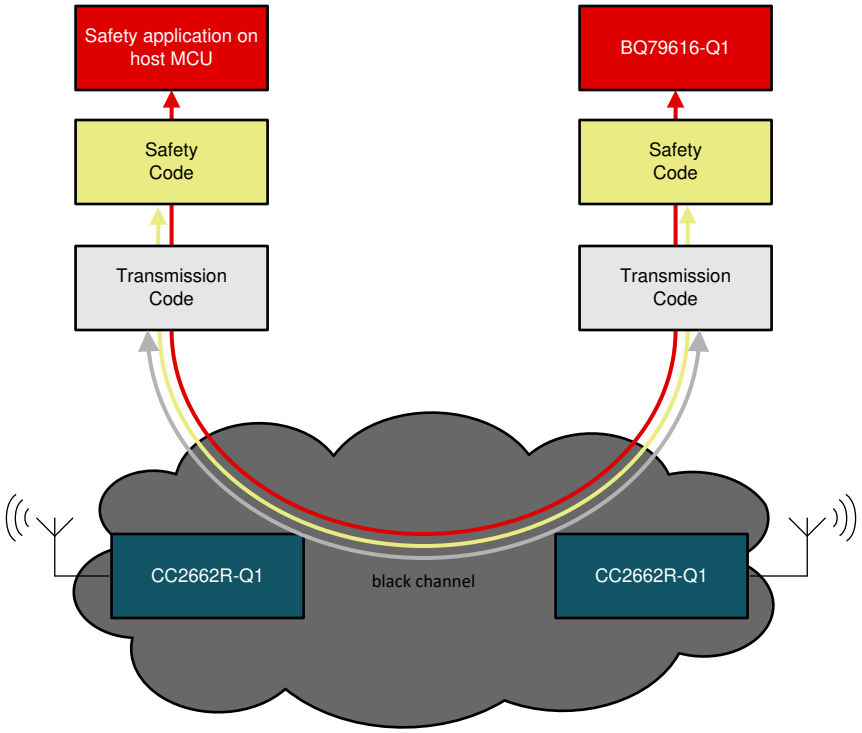

Figure 5-1. Structure of Communications Protocols in TI WBMS

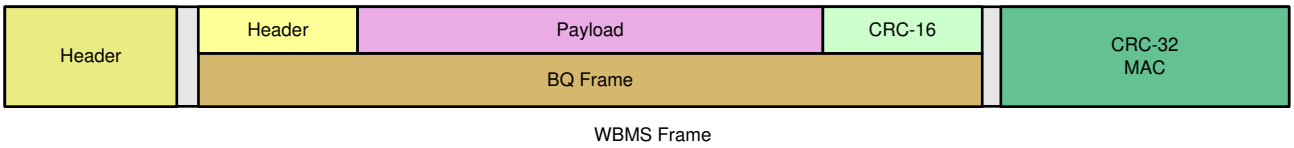

Figure 5-2. Structure of Underlying Data Frames

6 Conclusion

The TI WBMS solution using BQ79616-Q1 BMICs and CC2662R-Q1 wireless SoCs in combination with the proprietary WBMS protocol from TI shows a practical implementation of a black channel communication according to the IEC62280[4] error model used in an automotive environment. It shows both qualitative and quantitative evidence of error detection performance to help support system integrators in achieving their functional safety goals, up to ASIL D or SIL 3.

Details of the implementation of wireless communication used in accordance with ISO26262[1] and IEC61508[2] for WBMS are included in the functional safety concept document.

The ASIL D or SIL 3 systematic capability of TI WBMS is backed up with a thorough review done by TÜV SÜD and a related technical report.

Request the detailed functional safety concept document and the TÜV SÜD technical report from TI.com in the CC2662R-Q1 product folder.

7 References

1. 2018. *Road vehicles — Functional safety*. International Standardization Organization, ISO 26262.
2. 2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission, IEC 61508.
3. 2018. *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*. International Electrotechnical Commission, IEC 61784-3.
4. 2014. *Railway applications – Communication, signalling and processing systems – Safety related communication in transmission systems*. International Electrotechnical Commission, IEC 62280

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 (https: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