Electronic Design

ALAN R. EARLS, Contributing Editor

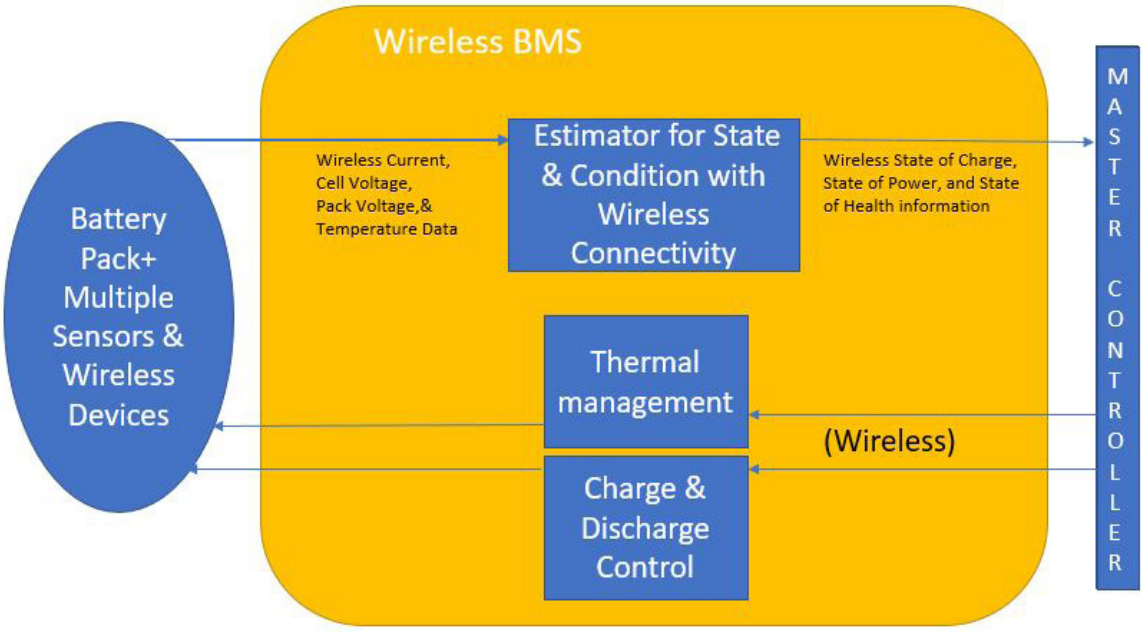
Mastering the Challenges of Wireless EV Battery Management

Flexibility is one of the advantages of a wireless EV BMS, but designers must also keep in mind cyber risks as well as the reliability and safety standards used across the automotive industry.

If EVs and hybrids are to reach their full potential, battery management must improve. That generally means successfully managing the state of health and state of charge of hundreds of individual cells. Thorough and accurate monitoring of all those cells has long implied additional wiring, which can add to a vehicle's complexity and weight, as well as potentially add failure points. A solution that's gained traction recently is wireless monitoring (e.g., through short-range RF such as Bluetooth).

A wireless approach offers simplicity and potentially better monitoring, but it also comes with complexities that need to be addressed.

Battery-management systems (BMS) have typically relied on a daisy-chain type of wiring harness. Given the need to have different wire lengths to reach each cell and route the wires safely without interfering with other systems or take up space unnecessarily, it becomes a challenge to make and install such harnesses. Going wireless can help reduce or eliminate the weight and bulk of the wire used in battery management while also eliminating many potential electro-



Shown is a functional diagram of a wireless BMS.

mechanical failure points.

Wireless BMS *(see figure)* brings instant simplification by eliminating this cumbersome feature. However, of course, it requires special on-cell monitoring technology that can accurately track temperature, voltage, etc., as well as on-cell wireless transmit and receive ability.

Though wireless transmission has become a generally robust and reliable technology, it still needs to be understood and evaluated on a case-by-case basis, especially within the confines of an EV.

Assessing a Design's Digital Signaling and Bit Errors

Safe EV operation and useful battery management requires that wireless deliver signals in two directions reliably and in real-time. EVs and battery packs present a difficult environment for transmitting and receiving RF. Therefore, a design needs to begin with a review of how to assess digital signaling and bit errors—defined as bits that have synchronization errors or are otherwise altered through electronic noise.

Bit error rate and bit error probability are ultimately reflected in the packet error ratio (PER), which is the ratio of incorrect data packets received compared to the total number of packets received. One bit of error in a packet is enough to invalidate that packet, hardly an unusual occurrence in many data streams. The frequency of such errors is the packet error probability. Without getting further into the details, suffice to say that designers aim for "five nines"—99.999% successful packet transmission.

This matters in wireless BMS operation due to the cluttered, conductive, and potentially electronically noisy space inside an EV. Fortunately, the data that must be moved in both directions is comparatively modest in volume and at least on a moment-to-moment basis.

Lost or missing data is mostly survivable: Tweaking of cell and battery operations typically undergoes more substantial forces (charge and discharge, in particular) than those a BMS might implement. On the other hand, batteries are packed with energy, and mismanagement can quickly lead to failure or worse. So, getting BMS communication right is vital.

Ensuring Optimal BMS Performance in EVs

A benchmark for thinking about reliability is the Automotive Safety Integrity Level (ASIL). It's a risk classification based on the ISO 26262 - Functional Safety for Road Vehicles standard and the Severity, Exposure and Controllability of vehicle operations scenario.

Assessing a hazard using ASIL involves considering relative impact of potential hazards on a system compared with relative likelihoods of the hazard actually happening. It also considers judgements about the severity and controllability of the occurrence. These are likely comparatively easy tests to pass for a BMS, whether wired or wireless.

Those considerations are all pure engineering. But in today's world, the ability of any system to be secure from access by unauthorized parties and against misuse or attack must also be top of mind. That's particularly true where wireless is involved and signals can be acquired, interrupted, or potentially altered.

Addressing Cybersecurity Threats in Wireless BMS

Risks can come from many sources. Electronic components are sourced globally and may inadvertently or deliberately include problematic hardware features. Some of these may simply be insecure and exploitable, while others could actually be trojans.

Hardware Trojans can be created by the designer of a computer chip, using a pre-existing ASIC core from a questionable source. Trojans could also be added deliberately by a vendor, or a vendor on behalf of a state entity or some other rogue group. Trojans may be activated externally (e.g., through a wireless signal) or internally. The possible risks they pose can range from interrupting or changing a function to exfiltrating data. Since the BMS contributes to the performance and safety of an EV, anything that could upset this operation must be avoided.

Of equal or perhaps greater concern is the security of the wireless element in a wireless BMS.

For all of these issues, we're inevitably talking about tradeoffs between absolute security at any price and low or no security with little or no cost. Various thought tools have been developed to help navigate these tradeoffs, one of the best-known being STRIDE. STRIDE, a model for identifying computer security threats, was originally developed at Microsoft. The *table* lists these threats.

Bluetooth, in particular, has been shown to have a significant number risks and hacks in circulation. But these can be addressed by implementing up-to-date versions of Bluetooth and ensuring best practices are in use. For instance:

- *Encryption:* Widely used encryption such as AES (Advanced Encryption Standard) can protect data sent via Bluetooth.
- *Authentication and Access Control:* Implementing device certificates, two-factor authentication, and secure key exchange protocols can ensure that Bluetooth devices don't communicate without using robust authentication mechanisms to verify their legitimacy.
- *Intrusion Detection and Prevention:* Implementing intrusion detection and prevention systems (IDPS) can identify unauthorized communication attempts and prevent such connections from succeeding.

While the list of wireless BMS concerns is a long one, most can be handled through implementation of standard electronic and cybersecurity tools and standards. Since the security picture will always continue to evolve, it's important to keep security issues in mind in the design process, with a consideration of future needs.

The flexibility of wireless, which can be extended across multiple EV models and modified easily to adapt to changes in vehicle design, can make a wireless BMS a compelling option now and in the future.

References

"In the New Era of Wireless Battery Management Systems (wBMS), Security Takes the Spotlight," Analog Devices Inc. (https://www.analog.com/en/resources/analog-dialogue/articles/in-the-new-era-of-wireless-battery-management-systems-wbms-security-takes-the-spotlight.html)

"A Survey of Wireless Battery Management System: Topology, Emerging Trends, and Challenges"