Vol 56, No 1—February 2022

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

AnalogDialogue

In the New Era of Wireless Battery Management Systems (wBMS), Security Takes the Spotlight

Lei Poo, Director of System Architecture

The full benefits of wBMS technology can only be achieved if system security can be assured from process to product.

The challenges identified in early conversations with electric vehicle (EV) OEMs about the technological and business benefits of wireless battery management systems (wBMS) seemed daunting, but the rewards are too promising to ignore. Wireless connectivity's many inherent advantages over wired/cabled architectures have already been proven in countless commercial applications, and BMS was another clear-cut candidate for cord cutting.

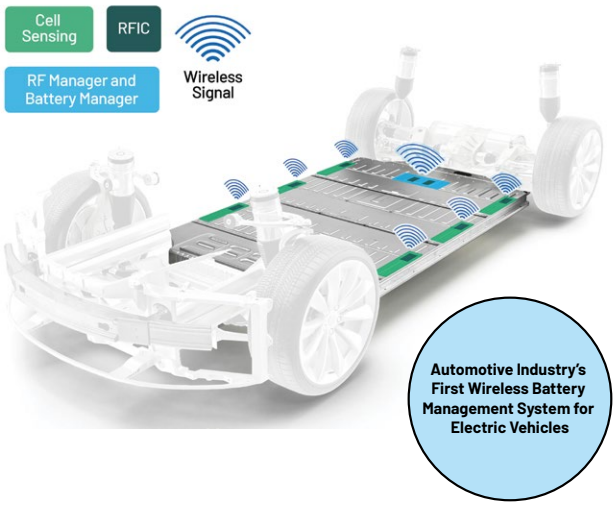

Figure 1. An electric vehicle using a wireless battery management system (wBMS).

The prospect of a more lightweight, modular, and compact EV battery pack—finally liberated from its cumbersome communication wiring harness—has been roundly embraced. By eliminating up to 90% of the pack wiring, and 15% of the pack volume, the entire vehicle's design and footprint can be streamlined significantly, as can its bill of materials (BOM) cost, development complexity, and associated manual installation/maintenance labor.

What's more, a single wireless battery design could be readily scaled across an OEM's entire EV fleet, precluding extensive and costly pack harness redesigns for each make and model. With wBMS, OEMs can freely modify their car frame designs without worrying about having to reroute extensive BMS wiring within the battery pack.

Taking a longer view, continued reductions in vehicle weight and battery pack size will be essential for extending EV driving ranges in the coming years. wBMS technology will therefore play an instrumental part in helping OEMs boost their range capabilities, and in so doing, help overcome consumers' long-lingering EV range anxiety.

This not only promises to spur greater overall EV market adoption, but also it gives OEMs the opportunity to leapfrog into EV market leadership positions on the strength of their driving range claims. This will remain a major differentiator among EV OEMs going forward. Further details about the advantages and market analysis can be found in "Electric Vehicle Wireless Battery Management Revolution Has Begun and the ROI Potential Is Huge."[1]

A New Security Standard

There are numerous challenges that need to be overcome to achieve the promises that wBMS offers. Wireless communications used in wBMS need to be sufficiently robust to interference when the car is driven, and the system must be safe under all conditions. But robust and safe design alone may not suffice against a determined attacker—this is where system security comes into play.

Sources of interference change depending on where the car is driving (for example, city vs. rural area) as well as whether someone is using another wireless device in the car that operates in the same frequency band. Reflections within the battery pack can also degrade performance depending on the material used for the pack housing the battery cells. There is a significant possibility that the

wBMS signal could fluctuate, potentially disrupting communication under natural conditions, let alone in the face of a malicious actor.

If the wBMS communication was somehow interrupted, the car can revert to a "safe mode" with reduced performance to allow the driver to act, or, with complete loss of wBMS communications, come to a safe stop. This can be accomplished by proper safety design, which takes into account all possible failure modes in the system and implements end-to-end safety mechanisms that address random failures of components.

But safety design does not consider the possibility of malicious actors who might exploit the system to their advantage, which may include taking control of the car remotely. This possibility was demonstrated by researchers on a moving vehicle during the 2016 Black Hat conference, using remote access via the vehicle's gateway. Thus, wireless robustness and fail-safe design are not sufficient; they need to be accompanied by security. The Black Hat demonstration was a valuable lesson, showing that future wireless systems in cars need to be designed in such a way that they cannot be leveraged as another remote entry point. In contrast, conventional wired battery packs offer no remote access, so to gain access to battery data, a hacker would need physical access to a high voltage environment in a vehicle.

Additional security challenges can arise throughout the EV battery life cycle, as shown in Figure 2. At Analog Devices, Inc. (ADI), our approach to designing wBMS focuses on understanding the different stages an EV battery goes through from birth to factory, to deployment and maintenance, and finally to either the next life or end-of-life. These use cases define the various functions a wBMS must support. For example, preventing unauthorized remote access is one consideration during EV deployment, but more flexible access is needed during manufacturing. Another example is in serviceability, where right-to-repair laws require a way for car owners to fix issues that stem from the battery cells or the associated wBMS. This means that a legitimate way of updating software in the wBMS must be supported and that the update mechanism should not compromise the safety of the vehicle when it leaves the service center.

Also, EV batteries are sometimes redeployed to the energy sector when they no longer meet EV performance standards. This requires secure ownership transfer of the EV battery from its first life to the next life. Since the batteries are devices without built-in intelligence, it falls upon the accompanying wBMS to enforce the proper security policies that best serve the EV battery life cycle. Secure erasure of first life secrets is needed before transitioning to a second life.

ADI anticipated these concerns and addressed them in accordance with our own core design principles that place a premium value—and exhaustive scrutiny—on maintaining and enhancing security integrities from process to product. In parallel, the ISO/SAE 21434[2] standard on "Road Vehicles: Cybersecurity Engineering" that has been in development over the last three years was officially released in August 2021. It defines a similar exhaustive, end-to-end process framework, with four levels of Cybersecurity Assurance. Automotive OEMs and suppliers are rated on a scale from 1 to 4, with 4 denoting the highest level of conformance (see Figure 3).

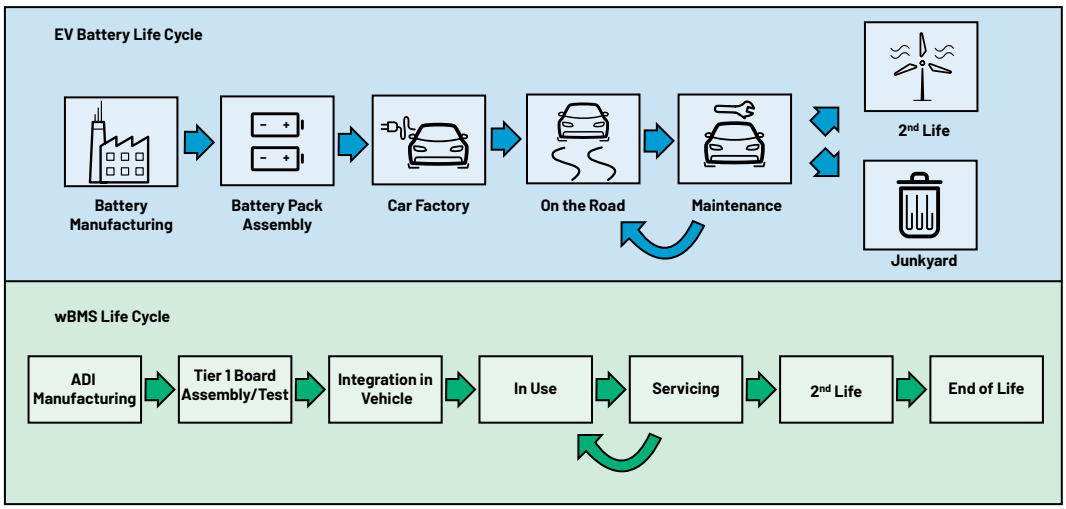

Figure 2. EV battery life cycle and its associated wBMS life cycle.

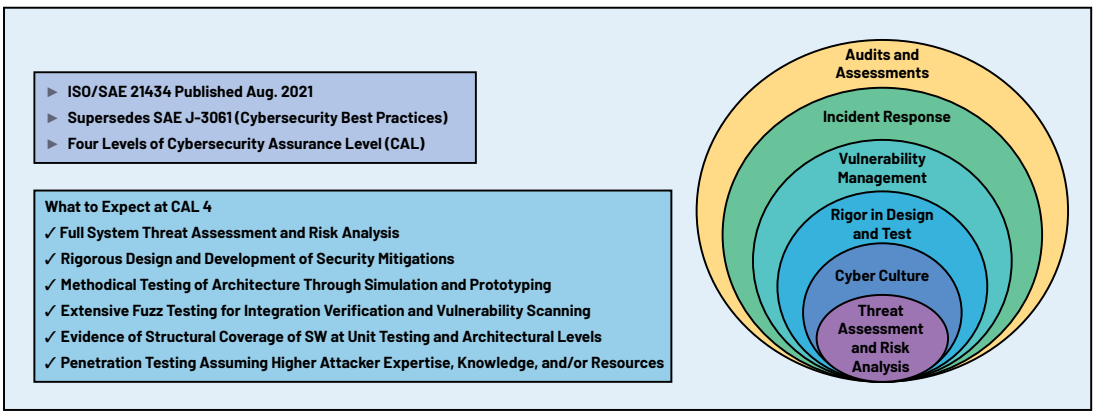

Figure 3. ISO/SAE 21434 framework and CAL 4 expectations.

ADI's approach for wBMS resonates with ISO/SAE 21434 for the highest level of examination and rigor that is needed for secure product development in the automotive industry. To this end, ADI engaged with TÜV-Nord, a well-known trusted certification lab, to assess our internal development policies and processes. This resulted in our policies and processes being vetted to fully comply with the new standard ISO 21434, as shown in Figure 4.

TÜV NORD

ZERTIFIKAT
CERTIFICATE

Hiermit wird bescheinigt, dass die Firma / *This is to certify, that the company*

Analog Devices Inc.
One Analog Way
Wilmington, MA 01887
USA

ein Managementsystem konform zu den Anforderungen der ISO/SAE 21434 betreibt und innerhalb der Laufzeit des Zertifikats von 3 Jahren auf Konformität überwacht wird.
operates a management system conforming to the requirements of ISO / SAE 21434 and within the the duration of the certificate of 3 years is monitored for conformity.

Road vehicles – Cybersecurity engineering
gemäß / *according to* ISO/SAE 21434:2021-08

Geltungsbereich: *Scope of application:* **ADI1381 Development Process for Product Security**
Automotive Business Unit (all locations)

Geprüft nach: *Compliant in accordance with:* **ISO/SAE 21434:2021-08**

Registrier-Nr. / *Registration No.* 44 331 13082139
Prüfbericht Nr. / Test Report No. TNM_8118984937-D06-CSA-R_V1.1
Aktenzeichen / *File reference* 8003030776

Gültigkeit / *Validity*
von / *from* 2021-10-30
bis / *until* 2024-10-29

Zertifizierungsstelle
der TÜV NORD CERT GmbH

Essen, 2021-10-30

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de

Figure 4. Certificate from TÜV-Nord.

Rigorous Scrutiny from Device to Network

Following our systematic process in the product design of wBMS, a threat assessment and risk analysis (TARA) was conducted to map out the threat landscape based on how the customer intends to use the product. By understanding what the system does, and the various ways it will be used over its lifetime, we can determine what key assets need protection and from what potential threats.

There are several choices of TARA techniques, including the well-known Microsoft STRIDE method, which attempts to model threats by considering the six threats abbreviated by the word STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. We can then apply this to the different interfaces of the components that make up the wBMS system, as shown in Figure 5. These interfaces are natural stops along the data and control flow paths where a potential attacker may gain unauthorized access to the assets of the system. Here, by role playing the attacker and asking ourselves how applicable each threat is on each interface and why, we can map out possible attack paths and determine how likely the threat is to happen and how severe the consequences may be if it succeeds. We then repeat this thought process across the different life cycle stages as the threat likelihood and impact may vary depending on the environment the product is in (for example, warehouse vs. deployment). This information will point to the need for certain countermeasures.

Take for example the wireless channel between the wireless cell monitors and wBMS manager during deployment, as shown in Figure 5. If the asset is the data from the wireless cell monitors, and the concern is the leakage of the data values to an eavesdropper, then we may want to encrypt the data when it passes through the wireless channel. If our concern is about the data being tampered with as it passes through the channel, then we may want to protect the data with a data integrity mechanism, such as a message integrity code. If the concern is about identifying where the data came from, then we will need a method for authenticating the wireless cell monitors to the wBMS manager.

Going through this exercise allows us to identify the key security objectives of a wBMS system, as shown in Figure 6. These goals will require some mechanisms to be implemented.

Very often, the question of "how far do we go in selecting the mechanisms to achieve a particular security goal?" is asked. If more countermeasures are added, it would almost certainly improve the overall security posture of the product, but at great cost, and possibly add unnecessary inconvenience to the end consumer using the product. A common strategy is to mitigate the most likely threats that are the easiest to deploy. More sophisticated attacks that tend to target assets of higher value will likely require stronger security countermeasures, but these may be extremely unlikely to occur and hence yield low returns if implemented.

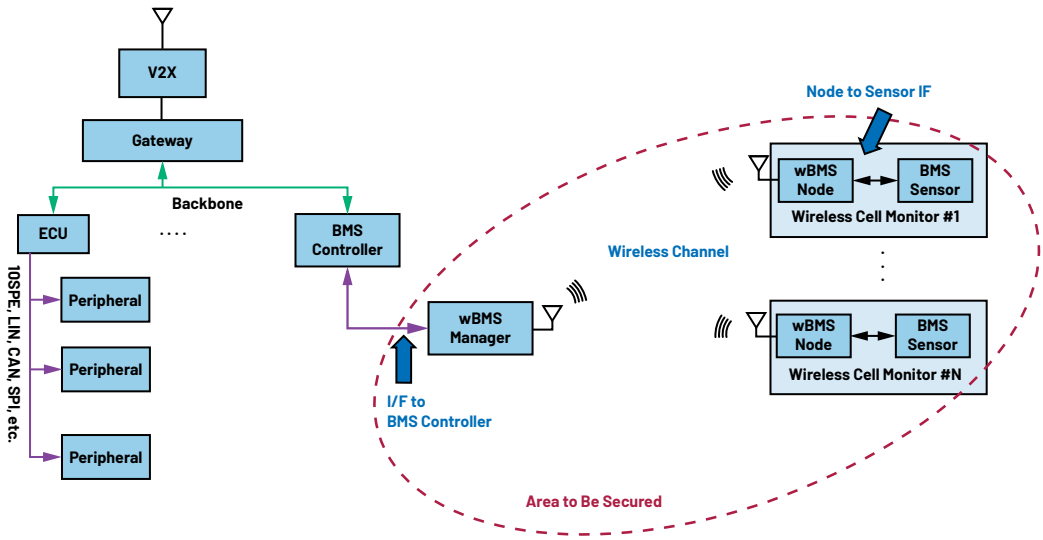

Figure 5. Threat surface considerations for wBMS.

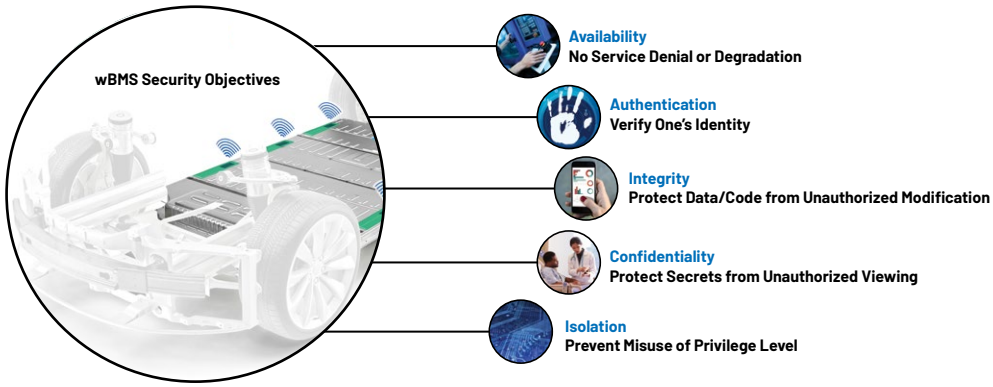

Figure 6. Security objectives of wBMS.

For example, in wBMS, physical tampering of the IC components to gain access to battery data measurements while the vehicle is driving down the road is extremely unlikely, since one would need a well-trained mechanic with deep EV battery knowledge to do gymnastics on the car parts while the car is in motion. An attacker in real life would likely attempt an easier path if one exists. A common type of attack on networked systems is a denial of service (DoS) attack—depriving the user of product utility. You could create a portable wireless jammer to try to interfere with wBMS function (hard), but you can also let the air out of the tires (easy).

This step of reconciling the risks with a set of appropriate mitigations is known as risk analysis. By weighing the impact and likelihood of the relevant threats before and after suitable countermeasures have been introduced, we can determine if the residual risks have been reasonably minimized. The end result is one where security features are incorporated only because they are needed and at a cost level acceptable to the customer.

The TARA for wBMS points to two important aspects of wBMS security: device-level security and wireless network security.

The first rule of any secure system is "keep your keys secret!" This means both on the devices and in our worldwide manufacturing operations. ADI's wBMS device security takes into account the hardware, ICs, and low level software on the ICs, and ensures that the system is able to boot securely from immutable memory into a trusted platform for code to run. All software code is authenticated prior to execution, and any in-field software update requires authorization by pre-installed credentials. Rollback to a previous (and possibly vulnerable) version of the software is prohibited after the system is deployed in the vehicle. Additionally, debug ports are locked once the system is deployed, thereby eliminating the possibility of unauthorized backdoor access into the system.

Network security is targeted at protecting the over-the-air communication between a wBMS cell monitor node and the network manager within a battery pack enclosure. Security starts at network joining where membership is checked for all of the participating nodes. This prevents random nodes from joining the network even if they happen to be physically close by. Mutual authentication of the nodes to the network manager at the application layer will further secure the wireless communication channel, making it impossible for a man-in-the-middle attacker to masquerade as a legitimate node to the manager or vice versa. Furthermore, to ensure that only the intended recipient can access the data, AES-based encryption is used to scramble the data cryptographically, preventing information leakage to any potential eavesdroppers.

Securing the Keys

As with all secure systems, the heart of security is a set of cryptographic algorithms and keys. ADI's wBMS follow NIST-approved guidelines, which means choosing algorithms and key sizes that align to a minimum security strength of 128 bits that are suitable for data-at-rest protection (for example, AES-128, SHA-256, EC-256) and uses algorithms found in well-tested wireless communications standards such as IEEE 802.15.4.

The keys used in device security are typically installed during ADI's manufacturing process and never leave the IC devices. These keys, which are used to ensure system security, are in turn protected physically by the IC devices both in use and at rest from unauthorized access. A hierarchical key framework then protects all application-level keys by saving them as encrypted blobs in nonvolatile memory, including the ones used in network security.

To facilitate mutual authentication of the nodes in the network, ADI's wBMS has provisioned a unique public-private key pair and a signed public-key certificate into each wBMS node during manufacturing. The signed certificate allows a node to verify that it is talking to another legitimate ADI node and valid network member, while the unique public-private key pair is used by the node in a key agreement scheme to establish a secure communication channel with another node or with the BMS controller. One benefit of this approach is easier wBMS installation without needing a secure installation environment, as the nodes are programmed to automatically handle network security after deployment.

In contrast, past schemes that use pre-shared keys to establish secure channels often required a secure installation environment and an installer to manually program the key value for the communication end points. To simplify and lower the cost of handling the key distribution problem, assigning a default common network key for all nodes in the network was often the shortcut many took. This often resulted in a hard lesson learned when a break-one, break-all disaster occurred.

As the OEM production scales, having the ability to leverage the same wBMS with varying number of wireless nodes across different EV platforms and to install at

different manufacturing or servicing sites that are necessarily secure, we lean in favor of the distributed key methodology that simplifies the overall key management complexity.

Conclusion

The full benefits of wBMS technology can only be achieved if security can be assured from device to network, and over the lifetime of the EV battery. Security, in this light, requires a system-level design philosophy, encompassing both process and product.

ADI anticipated the core cybersecurity concerns addressed by the ISO/SAE 21434 standard during its draft period and embraced them within our own wBMS design and development ethos. We are proud to be one of the first technology vendors to achieve ISO/SAE 21434 compliance on our policies and processes, and are currently undergoing certification for wBMS technology to the highest Cybersecurity Assurance Level.

Reference

[1]Shane O'Mahony. "Electric Vehicle Wireless Battery Management Revolution Has Begun and the ROI Potential Is Huge." Analog Devices, Inc., November 2021.

[2]ISO/SAE 21434:2021 - Road Vehicles. ISO, 2021.

About the Author

Lei Poo is director of system architecture in the E-Mobility Group within the Automotive Business Unit at Analog Devices and currently manages the Systems Architecture Team, which is responsible for designing wireless battery management systems (wBMS). She previously led ADI's Security Architecture and Platforms Team to establish the internal, secure product development process and now builds HW embedded security into ADI's emerging silicon products for Industrial Ethernet and wBMS. Prior to joining ADI, Lei was with NXP, Broadcom, and Marvell, where she was an embedded systems and security architect who designed secure chip/controller solutions for smartcards/smartphones, set-top boxes, and secure disk drives. Lei received a Ph.D. in electrical engineering from Stanford University in 2005 and holds 20 U.S. patents in the areas of HW embedded security, systems, and algorithms. She can be reached at lei.poo@analog.com.