ANALOG DEVICES 超越一切可能™ | ADI AnalogDialogue

在无线电池管理系统(wBMS)的新时代，安全成为焦点

Lei Poo，系统架构总监

只有从流程到产品确保系统安全性，wBMS技术的全部优势才能实现。

在与电动汽车(EV)车厂的早期对话中，就无线电池管理系统(wBMS)的技术和商务方面的挑战似乎令人生畏，但回报却非常丰厚，不容忽视。无线连接相对于有线/电缆架构的许多固有优势已经在无数商业应用中得到证明，BMS是又一个明确要抛弃线缆的候选领域。

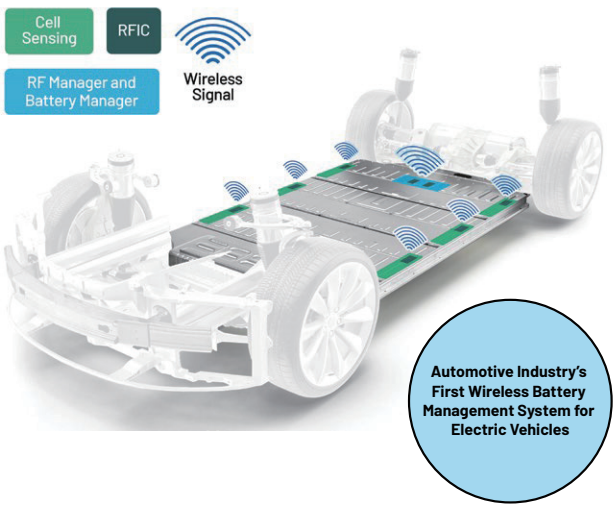

图1. 使用无线电池管理系统(wBMS)的电动汽车

更轻巧、模块化、紧凑型电动汽车电池组的前景——最终摆脱繁琐的通信线束——已被广泛接受。通过消除高达90%的电池组布线和15%的电池组体积，整车的设计和尺寸得以显著简化，物料清单(BOM)成本、开发复杂性和相关的人工安装/维护工作也大幅减少。

更重要的是，单一无线电池设计可以很容易在车厂的整个EV车队中进行扩展，而无需针对每个品牌和型号进行广泛且成本高昂的电池组线束重新设计。借助wBMS，车厂可以自由修改其车架设计，而不用担心需要重新布置电池组内的大量BMS布线。

从长远来看，车辆重量和电池组尺寸的持续减小对于未来几年延长电动汽车的续航里程至关重要。因此，wBMS技术将在帮助车厂提升续航能力方面发挥重要作用，进而帮助克服消费者长期挥之不去的电动汽车里程焦虑。

这不仅有望刺激电动汽车整体的市场采用率的提升，而且还使车厂有机会凭借其实现长续航的实力跃入电动汽车市场领导地位。展望未来，这仍将是电动汽车车厂的一个主要差异化因素。关于优势的更多详细说明和市场分析，请参阅“电动汽车无线电池管理革命已经开始，投资回报潜力巨大”[1]。

新安全标准

要兑现wBMS的承诺，需要克服许多挑战。当汽车行驶时，wBMS中使用的无线通信需要对干扰具有足够的鲁棒性，系统必须在所有情况下都是安全的。但是，仅靠鲁棒和安全的设计可能不足以对抗顽固的攻击者——这就是系统安全性发挥作用的地方。

汽车行驶的地点（例如是城市还是农村地区），是否有人在车内使用另一个同频段的无线设备，都会导致干扰源发生变化。电池组内的反射也会降低性能，具体取决于用于封装电池的电池组的材料。wBMS信号很可能会波动，在自然条件下通信可能会被破坏，更不用说面对恶意攻击者了。

如果wBMS通信因为某种原因被中断，汽车可以回到“安全模式”，降低性能以允许驾驶员采取行动，或者当wBMS通信完全丢失时，汽车能够安全停车。这可以通过适当的安全设计来实现，考虑系统中所有可能的故障模式，并实现端到端安全机制以应对组件随机故障。

但是，安全设计并未考虑恶意行为者利用该系统达到某种目的的可能性，包括远程控制车辆。在2016年黑帽会议期间，研究人员对一辆运动中的汽车展示了这种可能性，通过车辆网关实现了远程接入。因此，只有无线鲁棒性和故障安全设计是不够的，还需要抵御攻击的安全性。黑帽演示是一个有价值的教训，表明汽车中的未来无线系统需要以某种方式进行设计，使其不能作为另一个远程入口点被利用。相比之下，常规有线电池组不提供远程接入，要获得对电池数据的访问权，黑客需要以物理手段接入车辆中的高电压环境。

在电动汽车电池的全寿命周期中，还可能出现其他安全挑战，如图2所示。ADI公司的wBMS设计方法注重了解电动汽车电池经历的不同阶段——从出厂到部署和维护，最后到下一次寿命或寿命终结。这些使用场景定义了wBMS必须支持的各种功能。例如，防止未经授权的远程访问是在电动汽车部署期间的一个考虑事项，但在制造过程中需要更灵活的访问。另一个例子是在维修期间，修理权法律要求提供一种方式以便车主解决电池或相关wBMS的故障。这意味着必须支持wBMS中的软件以合法方式更新，并且当汽车离开维修站时，更新机制不应损害汽车的安全性。

此外，当电动汽车电池不再符合电动汽车性能标准时，这些电池有时会被重新部署到能源部门。这需要将电动汽车电池的所有权安全转移到下一生命阶段。电池是没有内置智能的设备，因此与之相伴的wBMS的责任在于，实施适当的安全策略以最好地为电动汽车电池寿命周期服务。过渡到第二生命（梯次利用）之前，必须安全擦除第一生命的所有秘密。

ADI公司预见了这些问题并按照我们自己的核心设计原则（即特别注重维护和增强从流程到产品的安全完整性并进行详尽审查）加以解决。与此同时，ISO/SAE 21434[2]标准“道路车辆：网络安全工程”经过过去三年的开发，已于2021年8月正式发布。它定义了类似的穷举式端到端过程框架，网络安全保证分为四级。车厂和供应商的在1到4的尺度上评分，4表示最高级别的符合性（参见图3）。

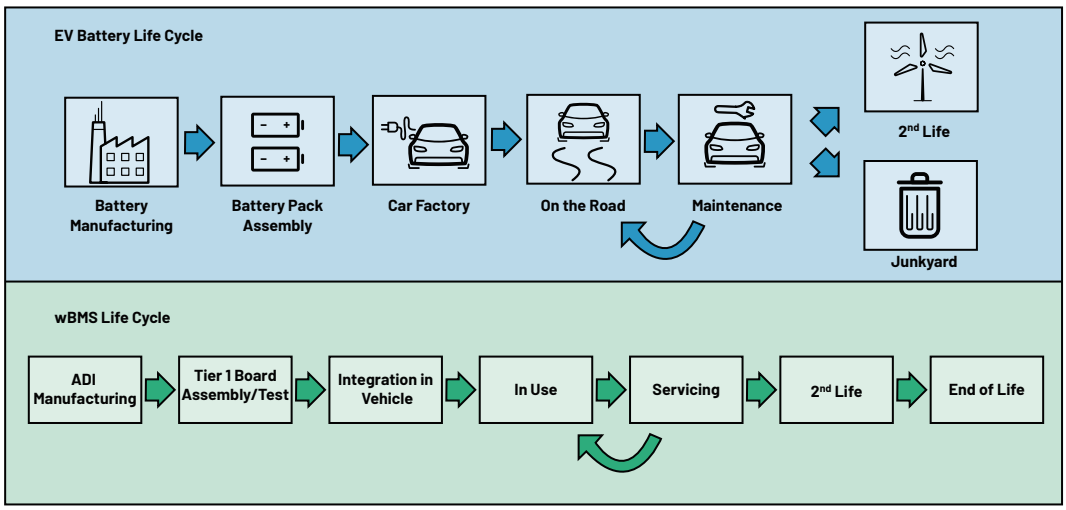

图2. 电动汽车电池生命周期及其相关的wBMS生命周期

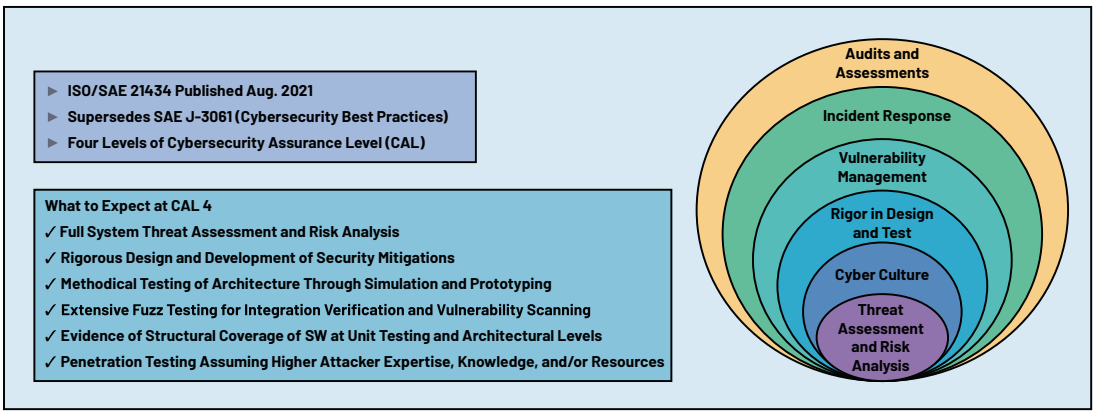

图3. ISO/SAE 21434框架与CAL 4期望

ADI公司的wBMS方法响应了ISO/SAE 21434要求，实施了汽车行业安全产品开发所需的最高水平的检查和严谨性。为此目的，ADI公司聘请了著名的可信认证实验室TÜV-NORD来评估我们内部的开发策略和流程。我们的策略和流程经过审查，完全符合新标准ISO 21434，如图4所示。


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_811898493 7-D06-CSA-R_V1.1
Aktenzeichen / *File reference* 8003030776

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

Zertifizierstelle / *the* TÜV NORD CERT GmbH

Essen, 2021-10-30

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

图4. TÜV-Nord证书

从器件到网络的严格审查

在wBMS产品设计的系统化流程之后，我们执行威胁评估和风险分析(TARA)，以根据客户意图使用该产品的方式来明确威胁概况。通过了解系统的用途，以及在寿命期间它的各种使用方式，我们可以确定哪些关键资产需要防范哪些潜在的威胁。

TARA技术有多种选择，包括众所周知的Microsoft STRIDE方法，即通过考虑缩写词STRIDE所表示的六大威胁来对威胁建模：欺骗(S)、篡改(T)、否认(R)、信息披露(I)、拒绝服务(D)和权限提升(E)。然后，我们可以将其应用于构成wBMS系统的组件的不同接口，如图5所示。这些接口是数据和控制流路径上的自然暂停点，潜在攻击者可能会藉此对系统资产进行未经授权的访问。在这种情况下，通过扮演攻击者并询问自己，每个威胁与每个接口的相关程度有多高以及为什么，我们可以找出可能的攻击路径，并确定威胁发生的可能性，以及如果攻击得逞，后果可能有多严重。然后，我们在生命周期的不同阶段重复这个思维过程，因为可能的威胁和影响因产品所处的环境（例如仓库与部署）而有所不同。此信息将指出需要某些对策。

以部署期间的无线蜂窝监视器与wBMS管理器之间的无线通道为例，如图5所示。如果资产是来自无线蜂窝监视器的数据，担心将数据值泄漏给窃听者，那么我们可能需要在数据通过无线通道时加密数据。如果我们担心数据通过通道被篡改，那么可能需要利用数据完整性机制（例如消息完整性代码）保护数据。如果担心有人识别出数据来自何处，那么我们需要一种方法来对与wBMS管理器通信的无线蜂窝监视器进行身份验证。

通过此练习，我们就能明确wBMS系统的关键安全目标，如图6所示。这些目标将要求实施一些机制。

很多时候，我们要回答这样一个问题：“为了实现特定安全目标而选择某些机制时，我们愿意付出多大代价？”如果增加更多应对措施，则几乎肯定会改善产品的整体安全态势，但代价会很大，而且可能给使用产品的最终消费者带来不必要的不便。一个常见策略是减轻可能性最大且最容易部署的威胁。更复杂的攻击往往针对较高价值的资产，可能需要更强的安全对策，但这种情况极不可能发生，因此如果实施的话，回报并不划算。

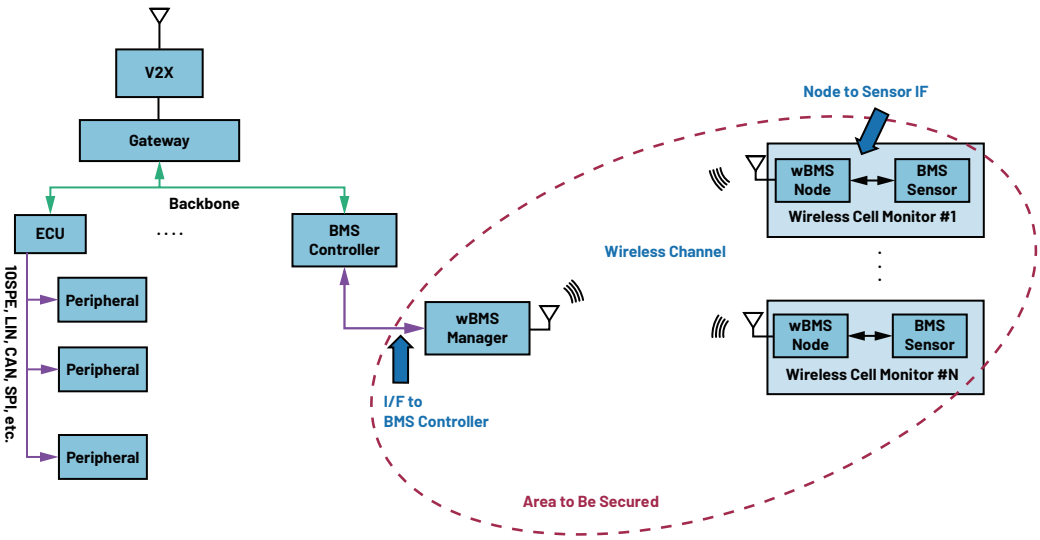

图5. wBMS的威胁面考虑

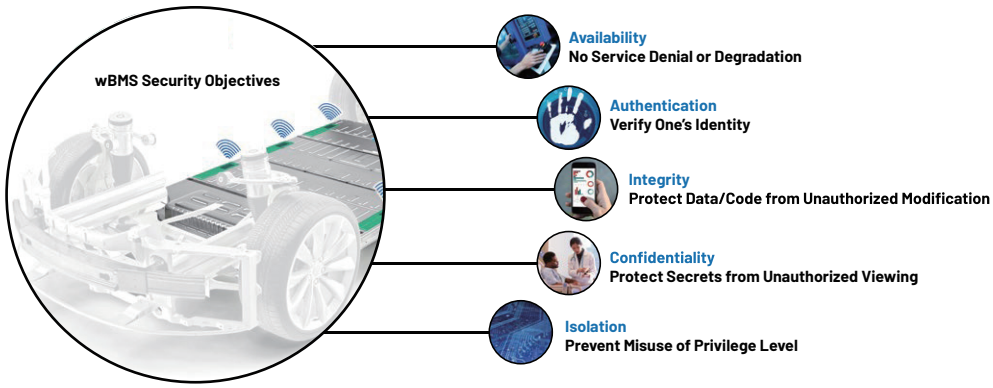

图6. wBMS的安全目标

例如，在wBMS中，当车辆正在道路上行驶时，对IC器件进行物理篡改以获得对电池数据测量的访问权是极不可能发生的，因为要对行驶中的汽车的部件动手脚，需要一个训练有素且对电动汽车电池有深厚了解的机修工。如果存在更容易的途径，现实生活中的攻击者很可能会尝试这样的路径。对网络系统的常见攻击类型是拒绝服务(DOS)攻击——使用户无法使用产品。您可以创建便携式无线干扰器来尝试干扰wBMS功能（很难），但您也可以给车胎放气（容易）。

利用一组适当的缓解措施应对风险的步骤称为风险分析。通过衡量相关威胁在引入适当对策前后的影响和可能性，我们可以确定残留风险是否已被合理地最小化。最终结果是，之所以纳入安全特性，是因为这些安全特性是必须的，并且其成本是客户可以接受的。

wBMS的TARA指向wBMS安全性的两个重要方面：器件级安全性和无线网络安全性。

任何安全系统的第一规则都是“维护密钥安全！”这意味着，在器件上和我们的全球制造业务中都要如此。ADI公司的wBMS器件安全性考虑了硬件、IC和IC上的低级软件，并确保系统能够从无法改变的存储器安全引导到可信平台以供运行代码。所有软件代码在执行之前都要进行身份验证，任何现场软件更新都需要预先安装的凭据提供授权。系统部署到车辆中之后，禁止回滚到先前（且可能易受攻击）的软件版本。此外，系统部署后便要锁定调试端口，从而消除通过未经授权的后门访问系统的可能性。

网络安全性旨在保护wBMS单元监视节点与电池包外壳内的网络管理器之间的无线通信。安全性从加入网络开始，所有参与节点的成员资格都要进行检查。这样可以防止随机节点加入网络，哪怕它们碰巧是附近的节点。在应用层对与网络管理器通信的节点进行相互认证，将能进一步保护无线通信通道，使得中间人攻击者无法充当合法节点来与管理器通信，反之亦然。

此外，为了确保只有目标接收者可以访问数据，使用基于AES的加密来扰乱数据，防止信息泄漏给任何潜在的窃听者。

保护密钥

同所有安全系统一样，安全性的核心是一组加密算法和密钥。ADI公司的wBMS遵循NIST批准的指导方针，这意味着所选的算法和密钥大小应与适合静态数据保护的最低安全强度128位一致（例如AES-128、SHA-256、EC-256），并使用经过充分测试的无线通信标准（例如IEEE 802.15.4）中的算法。

保障器件安全所用的密钥通常是在ADI制造过程中安装的，并且永远不会离开IC器件。确保系统安全性的这些密钥则由IC器件在物理上加以保护，无论在使用时还是未使用时，未经授权的访问均会被阻止。然后，分层密钥框架将所有应用层密钥作为加密二进制大对象(blob)保存在非易失性存储器中保护起来，包括网络安全中使用的密钥。

为了便于网络中节点的相互认证，ADI的wBMS在制造期间将一个唯一公钥密钥对和一个签名的公钥证书置入了每个wBMS节点。通过签名证书，节点可以验证与之通信的是另一个合法ADI节点和有效网络成员，而唯一公钥密钥对由该节点用在密钥协议方案中，以与另一个节点或BMS控制器建立安全通信通道。这种方法的一个好处是wBMS安装更容易，不需要安全安装环境，因为节点被设定为在部署后自动处理网络安全性。

相比之下，过去使用预共享密钥建立安全通道的方案通常需要一个安全的安装环境和安装程序来手动写入通信端点的密钥值。为了简化和降低处理密钥分布问题的成本，为网络中的所有节点分配一个默认公共网络密钥通常是许多人采用的捷径。这常常导致“一处崩溃，满盘崩溃”的灾难发生，必须引以为戒。

随着生产规模的扩大，车厂需要能够将具有不同数量无线节点的相同wBMS用于不同的电动汽车平台，并安装在不同的安全制造或维修场所，我们倾向使用分布式密钥方法来降低整体密钥管理的复杂性。

结论

只有在电动汽车电池的全寿命周期内确保从器件到网络的安全性，才能实现wBMS技术的全部优势。考虑到这一点，安全性要求采取系统级设计理念，涵盖过程和产品。

ADI公司预料到了ISO/SAE 21434标准在草案期间解决的核心网络安全问题，并在我们自己的wBMS设计和开发过程中采纳了相关应对措施。我们自豪地成为首批在政策和流程方面实现ISO/SAE 21434合规性的技术供应商，目前我们的wBMS技术正在接受最高网络安全保障等级认证。

参考资料

[1] Shane O'Mahony。“电动汽车无线电池管理革命已经开始，投资回报潜力巨大”。ADI公司，2021年11月。

[2] ISO/SAE 21434:2021 - 道路车辆。ISO，2021年。

作者简介

Lei Poo是ADI公司汽车事业部电动交通部门的系统架构总监，目前管理系统架构团队，该团队负责设计无线电池管理系统(wBMS)。她以前曾领导ADI安全架构和平台团队建立内部安全产品开发流程，现在则将硬件嵌入式安全性内建到ADI针对工业以太网和wBMS的新兴硅片产品中。加入ADI公司之前，Lei曾就职于NXP、Broadcom和Marvell，担任嵌入式系统和安全架构师，负责为智能卡/智能电话、机顶盒、安全磁盘驱动器设计安全芯片/控制器。Lei于2005年获斯坦福大学电气工程博士学位，并拥有硬件嵌入式安全、系统和算法领域的20项美国专利。联系方式：lei.poo@analog.com。

ANALOG DEVICES
超越一切可能™

如需了解区域总部、销售和分销商，或联系客户服务和技术支持，请访问analog.com/cn/contact。

向我们的ADI技术专家提出棘手问题、浏览常见问题解答，或参与EngineerZone在线支持社区讨论。
请访问ez.analog.com/cn。

©2022 Analog Devices, Inc. 保留所有权利。
商标和注册商标属各自所有人所有。

“超越一切可能”是ADI公司的商标。

请访问analog.com/cn