Vol 56, No 1—February 2022

ANALOG DEVICES
想像を超える可能性を
AHEAD OF WHAT'S POSSIBLE™

AnalogDialogue

ワイヤレス・バッテリ管理システムの新時代、注目すべきはセキュリティのレベル

著者：Lei Poo、システム・アーキテクチャ担当ディレクタ

ワイヤレス・バッテリ管理（バッテリ・マネージメント）システムのメリットを最大限に活かすためには、1つの条件を満たす必要があります。その条件とは、製品の開発プロセスと製品そのものについて、システム・レベルのセキュリティを確実に確保できるようにするというものです。

電気自動車（EV）の分野では、バッテリ管理システム（BMS：Battery Management System）のワイヤレス化に注目が集まっています。ワイヤレス化されたBMS（wBMS：Wireless BMS）は、多くの技術的なメリットやビジネス上のメリットをもたらします。このことは、現在では明確な事実として受け止められつつあります。アナログ・デバイセズがEVのメーカー各社と初期検討を行った際には、気が遠くなるほど難易度の高い課題がいくつも見つかりました。しかし、wBMSの潜在的な能力は非常に高く、決して無視できるものではありませんでした。有線（ケーブル接続）の技術と比較すると、ワイヤレス技術は多くの本質的なメリットを備えています。このことは、携帯電話をはじめとする無数の商用アプリケーションで既に実証されています。BMSが、ワイヤレス化を図るべき次なる候補であることは明らかでした。

EV用のバッテリ・パックについては、新たな期待が寄せられるようになりました。なかでも大きなニーズは、煩わしい通信用のハーネスからバッテリ・パックを解放することです。そうすれば、更に小型で軽量なモジュール式のバッテリ・パックを実現できるからです。実際、wBMSを採用したバッテリ・パックでは、配線を最大90%、体積を15%削減できます。また、部品のコストを低減し、開発の複雑さを緩和することが可能です。加えて、手作業での取り付け／メンテナンスの労力を軽減することが可能になります。つまり、フットプリントを大幅に削減できるだけでなく、自動車全体の設計の効率化を図れるということです。

wBMSを採用すれば、自動車メーカーが開発するEVの全車種に、バッテリ関連の単一の設計を簡単に適用することができます。つまり、メーカーや車種ごとにバッテリ・パック用のハーネスを再設計する必要がなくなります。言い換えれば、大がかりでコストのかかる作業が不要になるということです。また、wBMSを採用すれば、自動車のフレームの設計を自由に変更できるようになります。バッテリ・パック内でBMSの配線をやり直すという大掛かりな作業について心配する必要がなくなるからです。

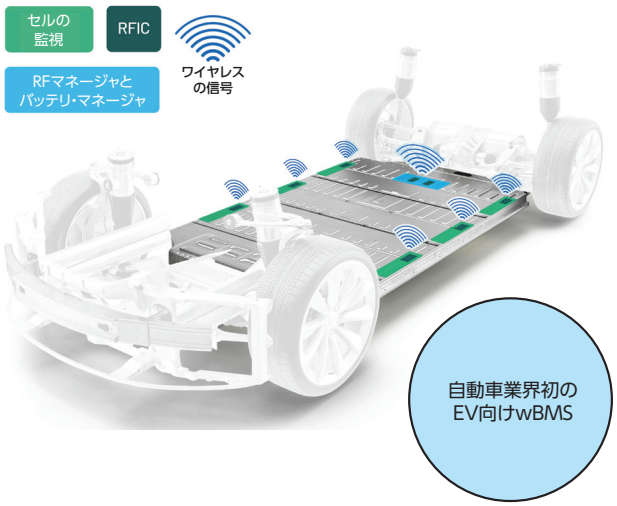

図1. wBMSを適用したEV

EVについては、車体の軽量化とバッテリ・パックのサイズの縮小を更に進めていくことが重要です。今後数年間のうちにEVの航続距離を大きく伸ばすためには、そうした改善は不可欠だと言えるでしょう。つまり、wBMSは航続距離の延伸に向けた自動車メーカーの取り組みを推し進める役割を果たします。また、EVの航続距離についてくすぶり続ける消費者の懸念の解消にも貢献します。

航続距離の延伸は、EVの更なる普及促進につながります。また、自動車メーカーは、長い航続距離を実現することで、EVの市場で主導的な地位をいち早く獲得する機会を得ることができます。今後も、航続距離はEVメーカーにとって主要な差別化要因になるでしょう。航続距離の延伸に向けた技術や市場の分析結果については、「EV業界でワイヤレス・バッテリ管理の革命が始動、潜在的なROIは莫大なレベル」[1]をご覧ください。

セキュリティ向けの新たな規格

wBMSがもたらすメリットを活かせるようにするためには、克服しなければならない課題がいくつも存在します。wBMSで使用するワイヤレス通信は、車両が走行している際に生じる干渉に対して高い堅牢性を発揮する必要があります。また、その通信用のシステムは、あらゆる条件下で安全に信号をやり取りできるものでなければなりません。実際、堅牢性が高く安全に通信を実現できる機能を設計するという方針は重要です。ただ、それだけでは、強い悪意を持った攻撃者に対しては十分ではないかもしれません。重要なのは、システム・レベルのセキュリティです。

自動車の通信機能については、都市部を走行しているのか、地方を走行しているのかといった違いによって事情が大きく異なります。また、車内で誰かが通信機能と同じ周波数帯で動作する別のワイヤレス・デバイスを使用していることもあります。このような状況の違いによって、自動車の通信機能には異なる干渉源からの影響が及ぶことになります。また、バッテリ・セルを収容するバッテリ・パックの素材によっては、パック内で生じる反射の影響で通信性能が低下するおそれもあります。wBMSで使用する信号に揺らぎが生じると、通信に乱れが発生します。その可能性は、自然な条件下においてもかなり高いと言えます。そのような状況下で、悪意のある攻撃を仕掛けられたら、ひとたまりもないということは容易に想像できるでしょう。

wBMSで使用する通信が何らかの理由で遮断された場合、どのように対処すればよいでしょうか。1つの答えは、車両の速度を落としてセーフ・モードに移行し、ドライバーが問題に対処できるようにすることです。あるいは、wBMSの通信が完全に損なわれたら車両を自動的に安全に停止させる機能を用意してもよいでしょう。常に安全を確保できるようにすることを念頭に置いて適切に設計を行えば、そうした機能を実現できるはずです。そのためには、システムで起こり得るすべての障害について十分に検討しなければなりません。また、安全を確保するためには、車両の構成要素の偶発的な故障に対応可能なエンドtoエンドのメカニズムを実装する必要があります。

しかし、安全を確保できるように設計を行いたいと思っても、悪意のあるすべての攻撃の可能性を考慮するのは容易ではありません。そうした攻撃の例としては、遠隔操作によって車両の制御を奪うというものが考えられます。攻撃の詳細はともかくとして、自らの利益のためにシステムを悪用しようとする攻撃者は後を絶たないでしょう。2016年に開催された「Black Hat」というカンファレンスでは、次のような攻撃が紹介されました。その攻撃とは、車両のゲートウェイを介したリモート・アクセスを利用し、走行中の車両の制御を奪うというものです。そのような攻撃を実現できるということが、研究者らによって実証されたというのです。ワイヤレス接続の堅牢性を高めたり、フェイルセーフを実現できるような設計を行ったりするだけでは不十分です。そうした攻撃に対応可能なセキュリティ対策が必要になります。Black Hatでは、貴重な教訓が示されました。すなわち、車両に実装する未来のワイヤレス・システムは、リモート・アクセスが可能な新たなエントリ・ポイントとして悪用できないように設計しなければならないということです。なお、従来の有線式のバッテリ・パックには、リモートからアクセスするための手段が存在しません。そのため、攻撃者がバッテリに関するデータにアクセスするには、車両内の高電圧の環境に物理的にアクセスする必要があります。

図2（上）に示したのは、EV用のバッテリのライフ・サイクルです。その全体を通して、セキュリティに関連する様々な課題が発生する可能性があります。製造済みのバッテリは、自動車の工場に搬入され、車両に実装されます。車両での使用期間中にはメンテナンスが適用され、最終的にはセカンド・ライフとして再利用されるか、廃棄されることになります。アナログ・デバイセズの技術者は、wBMSを設計するにあたり、そうした様々な段階について深く理解することに努めました。その上で、様々なユース・ケースに応じ、wBMSがサポートしなければならない様々な機能を定義しました。例えば、EVに配備された後のwBMSについては、不正なリモート・アクセスを防ぐ方法を検討しなければなりません。その一方で、製造段階において、より柔軟なアクセス手段を提供する必要があります。また、保守性についても検討しなければなりません。

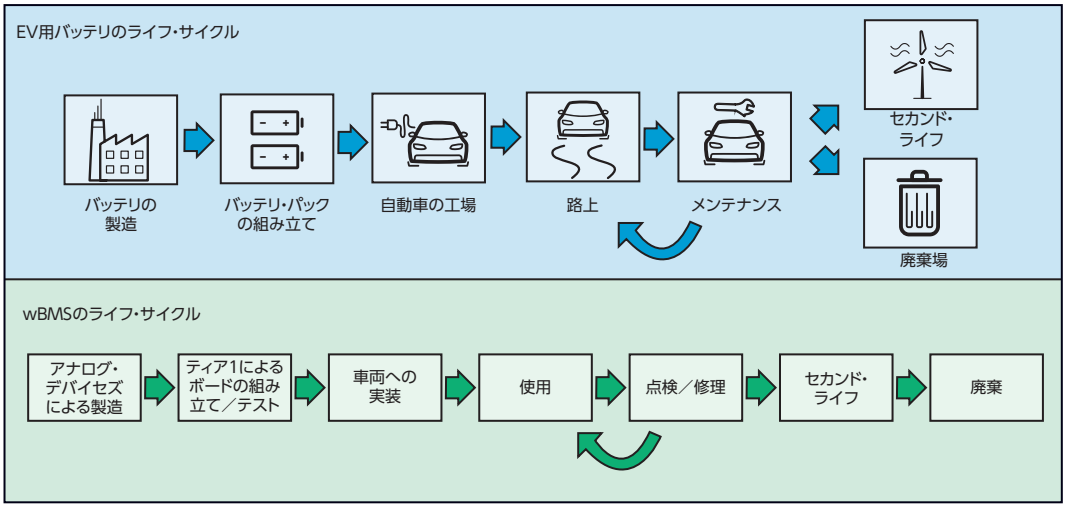

図2. EV用バッテリのライフ・サイクル、
それに付随するwBMSのライフ・サイクル

修理する権利（Right to Repair）について定めた法律により、バッテリ・セルやwBMSに起因する問題については、自動車の所有者が修復できるようにするための手段を設けることが義務づけられています。これに対応するには、wBMSのソフトウェアをアップデートするための正規の手段を用意しなければなりません。また、車両がサービス・センターを離れた後に、そのアップデートのメカニズムが車両の安全性を脅かす要因にならないようにすることも求められます。

EV用のバッテリは、使用期間が長くなればなるほど性能が低下していきます。ただ、EV用のものとしての性能を満たせなくなったとしても、即座に破棄されるとは限りません。例えば、電力業界で蓄電用のバッテリとして再利用する（セカンド・ライフ）といったケースがあるのです。その場合、バッテリの所有権を、ファースト・ライフの所有者からセカンド・ライフの所有者に安全に移さなければなりません。そのためには、バッテリのライフ・サイクルに対して最も適切なセキュリティ・ポリシーを適用する必要があります。ただ、バッテリそのものは、インテリジェンスな機能を備えていません。したがって、その役割はwBMSが担うことになります。ファースト・ライフにおける機密情報は、セカンド・ライフに移す前に確実に消去する必要があります。

アナログ・デバイセズは、上記のような課題にいち早く注目しました。そして、設計に関する当社の中核的な原則に従って対応を図っています。その原則では、開発プロセスの段階から製造済みの製品までセキュリティの完全性を維持／強化することに高い価値があると位置づけています。この目標を達成するために、徹底的な精査を行います。一方、業界全体としては、ISO/SAE 21434[2]（Road vehicles－Cybersecurity engineering）という規格が3年間にわたる策定期間を経て2021年8月に正式にリリースされました。この規格では、サイバーセキュリティに関する4つの保証レベル（CAL：Cybersecurity Assurance Level）が定められています。また、それに対応する開発プロセスのフレームワークも提示されています。この包括的かつエンドtoエンドのフレームワークは、当社の設計上の原則とよく似ています。自動車のメーカーやサプライヤは、4段階のCALで評価されます。CAL 4が最も高い準拠レベルにあたります（図3）。

自動車の業界では、安全性の高い製品開発を実現するために最高レベルの検査と厳密さが求められます。wBMSの設計に対するアナログ・デバイセズのアプローチは、その点でISO/SAE 21434の理念と一致しています。当社はそのことを証明するために、認証機関として高い信頼を得ているTÜV-Nordに、当社の開発ポリシー／プロセスの審査を依頼しました。その結果、当社の開発ポリシー／プロセスは、ISO 21434に完全に準拠しているという認定を取得することができました（図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

Zeichnungsberechtigte/r TÜV NORD CERT GmbH

Essen, 2021-10-30

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

図4. TÜV-Nordから取得した認証書

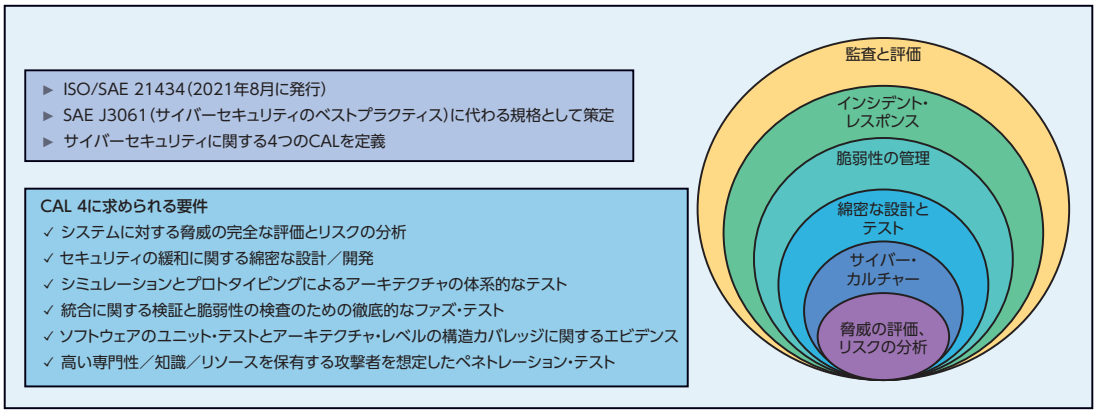

図3. ISO/SAE 21434のフレームワークとCAL 4の要件

デバイスからネットワークに至るまでの厳密な検査

アナログ・デバイセズはwBMS製品を設計するにあたり、自社の体系的なプロセスに従って脅威の評価とリスクの分析（TARA：Threat Assessment and Risk Analysis）を実施しました。それにより、お客様がwBMS製品をどのように使用するのかという観点から、脅威が生じる状況（threat landscape）を洗い出しました。重要なのは、システムの動作と、そのライフ・サイクルを通した様々な使用方法を理解することです。それにより、どのようなアセット（設備）をどのような潜在的な脅威から保護する必要があるのかということを把握できます。

TARAの手法には、いくつかの選択肢があります。その1つが、よく知られているMicrosoftのSTRIDEです。STRIDEという名称は、Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報の漏えい）、Denial of Service（サービスの拒否）、Elevation of Privilege（権限の昇格）の頭文字から来ています。STRIDEでは、これら6つの脅威について検討することで、脅威のモデル化を実施します。この手法は、wBMSの各構成要素に対応する様々なインターフェースに適用することができます（図5）。それらのインターフェースでは、制御用のものを含むデータがやり取りされます。その経路は、アセットに対する不正アクセスを試みる攻撃者が必ず目を付ける個所にあたります。ここで必要になるのは、攻撃者の視点を持つことです。各インターフェースに対してどのようにすれば攻撃を仕掛けられるのか、なぜそれが可能になるのかということを自問自答します。それにより、攻撃の対象になり得る潜在的な経路を洗い出し、脅威が発生する可能性と、攻撃が成功した場合に生じる影響の度合いを判断します。そして、ライフ・サイクルの各段階について、そのような思考のプロセスを繰り返します。脅威が発生する可能性と影響の度合いは、製品が置かれる環境（倉庫なのか、車内なのか）によって異なる可能性があるからです。このようなプロセスによって得た情報に基づくことで、必要になる具体的な対策が明確になります。

ここでは、図5を基に具体的な例を示すことにします。ご覧のように、車両にはwBMSを適用したワイヤレスのセル・モニタとwBMSマネージャが搭載されます。両者の間には通信用のワイヤレス・チャンネルが構成されます。アセットに相当するのは、ワイヤレスのセル・モニタからのデータです。ここでの懸念事項は、盗聴によるデータの漏洩であると仮定しましょう。その場合、ワイヤレス・チャンネルでやり取りされるデータの暗号化が必要になる可能性があります。では、チャンネル間でやり取りするデータの改ざんが懸念事項である場合にはどうなるでしょうか。その場合に必要なのは、データを保護するための仕組みです。つまり、メッセージの完全性を保つためのコードなど、データの完全性を実現するためのメカニズムが必要だということです。場合によっては、データの送信元の身元確認が懸念事項になることもあるでしょう。その場合に必要なのは、wBMSマネージャによってワイヤレスのセル・モニタを認証する手段です。

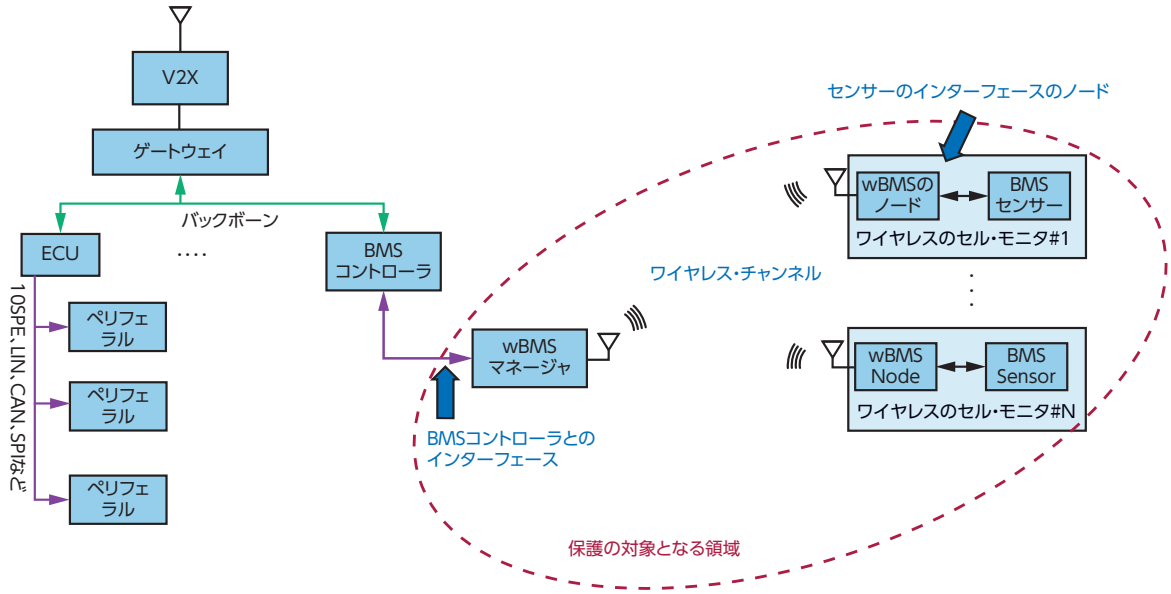

図5. wBMSを適用する場合のシステム構成。
脅威に対する保護を実現すべき領域を示しています。

このような検討を行うことによって、wBMSにおけるセキュリティ関連の主要な目標を特定することができます（図6）。これらの目標を達成するには、何らかのメカニズムを実装しなければなりません。

次に考察すべきことは、「セキュリティの面で特定の目標を達成するためには、どれだけのメカニズムを盛り込む必要があるのか」というものです。より多くの対策を講じれば、製品の全体的なセキュリティ・レベルはほぼ確実に高まります。しかし、それには莫大なコストがかかります。それだけでなく、現実的には不必要な対策によって、ユーザにとっての利便性が損なわれてしまうかもしれません。したがって、一般的な戦略は「最も簡単に仕掛けられる、最もよくある脅威を緩和する」というものになります。ただ、より価値の高いアセットには、より高度な攻撃が仕掛けられる傾向があります。そのような攻撃に対しては、より強力なセキュリティ対策が必要になる可能性があります。とはいえ、そうした攻撃を仕掛けられる可能性は非常に低いので、対策を講じたことによるメリットは小さいかもしれません。

極端な例を挙げると、次のような攻撃も想定できます。すなわち、wBMSを適用した車両が路上を走行しているときに、ICが物理的に改ざんされてバッテリに関する測定データに対する不正アクセスが行われるといったものです。しかし、このような攻撃が現実に行われるとは考えられません。EV用のバッテリに関する深い知識を持つ熟練の機械工でなければ、走行中の車両のコンポーネントに細工を施すことはできないからです。現実の攻撃者は、より簡単な方法があるなら、そちらを試そうとするでしょう。ネットワークに接続されたシステムに対する一般的な攻撃としては、ユーザが製品を使用することを妨げるDoS（Denial of Service）攻撃が挙げられます。より高度なDoS攻撃としては、可搬性を備えるワイヤレスの妨害機（ジャマー）を構築し、wBMSの機能に干渉を加えるというものが考えられます。ちなみに、悪意を持ってタイヤの空気を抜くという行為もDoS攻撃の一種です。

上記のように、一連の適切な緩和策を適用しつつリスクを管理する作業のことをリスク分析と呼びます。必要なのは、特定の脅威について、適切な対策を講じる前後の影響と発生の可能性を比較検討することです。それにより、満足できる程度まで残存リスクを抑えられるかどうかを判断することができます。最終的な結果として、必要かつユーザが許容できるコストで導入できるセキュリティ機能だけを実装することが可能になります。

アナログ・デバイセズは、wBMSに関するTARAを実施しました。その結果、wBMSのセキュリティには2つの重要な側面があることが判明しました。デバイス・レベルのセキュリティとワイヤレス・ネットワークのセキュリティの2つです。

あらゆるシステムを安全なものにするためには、遵守すべき1つの規則があります。それは「鍵は秘密にしておく」というものです。この規則は、アナログ・デバイセズが製造するデバイスと世界規模で行われている当社の製造業務の両方に適用しなければなりません。当社の場合、wBMS製品のセキュリティを確保するために、ハードウェア、IC、IC上の低レベルのソフトウェアについて考慮します。それにより、変更が不可能なメモリを使ってシステムを安全にブートし、コードを実行するための信頼できるプラットフォーム上で起動させられるということを保証します。ソフトウェアを構成するコードは、すべて実行前に認証されます。フィールドでソフトウェアをアップデートする場合には、事前にインストールした情報を使用して認証を行わなければなりません。また、システムを車両に配備した後でソフトウェアを古いバージョンに戻すことは禁止されます。古いバージョンには脆弱性が未修正のまま残っている可能性があるからです。更に、システムを車両に配備したら、デバッグ用のポートはロックされます。それにより、バックドアへの不正なアクセスによってシステムに侵入される可能性を排除します。

バッテリ・パックの筐体内には、wBMSのセル・モニタのノードがあります。このモニタは、ネットワーク・マネージャとの間でOTA（Over-the-Air）の通信を行います。ネットワークのセキュリティは、この通信を保護することを目的としたものです。すべてのノードに対しては、ネットワークに接続される際にメンバーシップの確認が行われます。これがセキュリティのメカニズムの始点になります。メンバーシップの確認は、たまたま物理的に近い場所にあったノードが、無作為にネットワークに接続されてしまうことを防ぐ役割を果たします。また、アプリケーション層におけるネットワーク・マネージャとノードの相互認証は、ワイヤレス・チャンネルの更なる保護につながります。具体的には、正当なノードになりすましてマネージャを欺く（またはその逆）中間者攻撃を不可能にします。更に、意図した受信者だけがデータにアクセスできるようにするためには、暗号化方式としてAES（Advanced Encryption Standard）を利用するとよいでしょう。暗号論に基づいてデータをスクランブルすれば、潜在的な盗聴者に対して情報が漏れることを防ぐことが可能です。

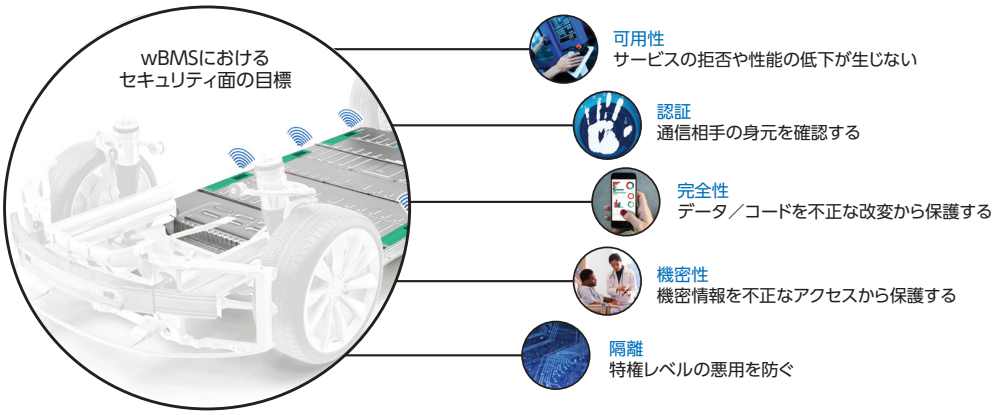

図6. wBMSにおける
セキュリティ面の目標

鍵の保護

あらゆるシステムに言えることですが、セキュリティを確保する上では、暗号化用のアルゴリズムと鍵のセットが中核になります。アナログ・デバイセズのwBMSは、NIST（アメリカ国立標準技術研究所）が承認したガイドラインに従っています。すなわち、アルゴリズムとしては、IEEE 802.15.4のような実績のあるワイヤレス通信規格で使われているものを選択しています。また、保存データの保護（例えば、AES-128、SHA-256、EC-256など）に使用する鍵長としては、128ビットという最小セキュリティ強度に適合したサイズを採用しています。

アナログ・デバイセズの場合、ICのセキュリティに使用する鍵は、通常、ICの製造プロセスにおいて実装します。つまり、個々のICから鍵が切り離されることは決してありません。それらの鍵は、システムのセキュリティを確保するために使用されます。また、それらは、ICによって、使用時も保管時も不正なアクセスから物理的に保護されていることになります。鍵の管理には、階層的な構造を利用しています。ネットワークのセキュリティに使われるものを含めて、アプリケーション・レベルのすべての鍵は、暗号化されたブロブとして不揮発性メモリに保存することで保護されます。

アナログ・デバイセズの場合、ICの製造時に、公開鍵と秘密鍵の一意的（unique）なペアと署名済みの公開鍵証明書を各wBMSのノードに設定します。その目的は、ネットワーク内のノードにおいて相互認証を可能にすることです。署名済みの証明書を使用することによって、各ノードは、通信の相手がアナログ・デバイセズが製造した正当なノードであり、有効なネットワークのメンバーであるということを確認することができます。一方、公開鍵と秘密鍵の一意的なペアは、鍵合意方式において使用されます。その目的は、ノードが別のノードまたはBMSコントローラとの間でセキュアな通信チャンネルを確立できるようにすることです。このアプローチでは、配備済みのノードは、ネットワークのセキュリティについて自動的に処理を行うようにプログラムされます。そのため、セキュアな環境を構築することなく、wBMSを容易に配備できます。

ちなみに、以前は、事前共有鍵を使用してセキュアなチャンネルを確立するという手法が使われていました。その場合、セキュアな配備環境を構築し、通信のエンド・ポイントで実装者が鍵の値を手作業でプログラムしなければなりませんでした。つまり、鍵の配布には複雑な処理が必要になり、コストもかさんでいたということです。この問題を解消するための手っ取り早い方法として、ネットワークで共通のデフォルトの鍵をネットワーク内のすべてのノードに割り当てるということがよく行われていました。しかし、このような方法を採用すると、1つの鍵が破られたらすべての鍵が破られてしまいます。実際に被害に遭い、その危険性について身をもって学ぶという結果を招くことも少なくありませんでした。

自動車メーカーが生産規模を拡大することを受けて、アナログ・デバイセズは、鍵の管理の全体的な複雑さを軽減することが可能な分散鍵方式を採用しました。EV用の異なるプラットフォームにまたがり、様々の数のワイヤレス・ノードに対して同じwBMSを適用できるからです。また、異なる製造現場や、当然のことながらセキュアでなければならないサービスの現場で実装できることも理由の1つです。

まとめ

wBMSのメリットを最大限に活かすためには、1つの条件を満たさなければなりません。その条件とは、デバイスからネットワークまで、またEV用のバッテリの使用期間を通して、確実にセキュリティが確保されなければならないというものです。そのためには、セキュリティに関して、開発プロセスと製品の両方を網羅するシステム・レベルの設計理念が必要になります。

アナログ・デバイセズは、ISO/SAE 21434において草案の段階で取り上げられていたサイバーセキュリティに関する主要な懸念にいち早く着目していました。そして、それらの懸念を解消するための施策をwBMSの設計開発の方針に盛り込みました。ISO/SAE 21434に準拠する開発ポリシー／プロセスを、最も早い段階で構築した技術企業であることを誇りに思っています。現在は、wBMSについて最も高いCALの認定を取得すべく審査を受けている段階にあります。

参考資料

[1] Shane O'Mahony「EV業界でワイヤレス・バッテリ管理の革命が始動、潜在的なROIは莫大なレベル」Analog Devices、2021年11月

[2]「ISO/SAE 21434:2021 - Road Vehicles（自動車）」、ISO、2021年

著者について

Lei Poo (lei.poo@analog.com) は、アナログ・デバイセズのシステム・アーキテクチャ担当ディレクタです。オートモーティブ事業部門のEモビリティ・グループに所属しています。現職では、ワイヤレス・バッテリ管理システム（wBMS）の設計を担当するシステム・アーキテクチャ・チームを統括。産業用イーサネットおよびwBMSを対象とした新たなIC製品に適用する組み込みセキュリティ技術の構築に取り組んでいます。それ以前は、セキュリティ・アーキテクチャ／プラットフォームのチームを率い、社内向けのセキュアな開発プロセスの確立に携わっていました。アナログ・デバイセズに入社する前は、NXP Semiconductors、Broadcom、Marvell Technologyに在籍。組み込みシステムとセキュリティ技術を担当するアーキテクトとして、スマートカード／スマートフォン、セットトップ・ボックス、セキュアなディスク・ドライブを対象としたセキュアなIC／コントローラの設計に従事していました。2005年にスタンフォード大学で電気工学の博士号を取得。ハードウェアに組み込むセキュリティ技術、システム技術、アルゴリズムに関する20件の米国特許を保有しています。

AD5602-0-2/22