

車載電子システムに潜むセキュリティリスク



車載システムにはフラッシュメモリに対する最新のアプローチが必要であることは明らかです。市場に出回っている従来のフラッシュメモリ技術とは異なり、暗号化されたセキュアな標準 SPI バスを介して、セキュアな領域と SoC/MCU との間でコードやデータの転送を可能にする新しい技術が必要とされています。将来的には、これらのよりセキュアなフラッシュメモリソリューションが、特にサイバー攻撃が広範かつ巧妙になってきていることから、セキュリティのガイドラインや基準を満たすための要件となる可能性が高まっています。

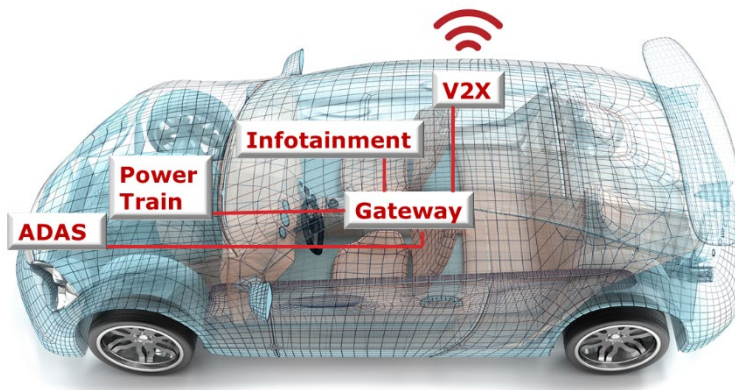
モノのインターネット（IoT）は、人々の生活、仕事、遊び方を変える新しい機会をもたらしています。しかし、日常がネットワークに接続されるようになるにつれ、あらゆる新しい IoT デバイスへのハッカーからの攻撃や、セキュリティ侵害のリスクが高まっています。携帯電話やノートパソコンなど、最も信頼を寄せるデバイスを安全に保つ必要がある理由については、ほとんどの人が熟知していますが、現在、自動車を便利にしているコネクテッドインテリジェンスについては、あまり考えたことはないのではないのでしょうか。事実として、これらのシステムはセキュリティ侵害の好対象になりやすいのです。車業界にて最もインテリジェントな車の 1 つである、テスラのモデル 3 を見ればわかります。2019 年 3 月、ハッカーたちはこの車のインフォテインメントシステムを標的として、画像描画の JIT（Just In Time）バグを利用することで、システムのコントロール権を奪取することに成功しました。これはハッキングイベントの一環として行われたものであり、実所有者に危険が及ぶことはありませんでしたが、車載電子システムのセキュリティホールを露呈するものでした。自動車が今後もインテリジェント化を進め、世界中で成長している IoT インフラストラクチャに接続していくのであれば、この弱点に対応し、解決していく必要があります。

アプリケーションがさらなるセキュリティと安全性のニーズを牽引

車載電子システムは、着実にインテリジェント化しています。下図に示すように、ADAS、ゲートウェイ、パワートレイン、インフォテインメント、V2V、V2X など、自動車の随所に高度な電子機能が追加されていきます。これらの新しい機能は、特にフラッシュメモリというシステム上重要な構成要素周辺のセキュリティと安全性の向上を求めつつあります。フラッシュメモリは数十年も前から存在していますが、今では車載業界に貢献するまでに進化を遂げています。しかし、現在の組み込みフラッシュメモリは、セキュリティと安全性の両方を保証する適切な認証を取得していないレガシー技術およびアーキテクチャをベースにしているため、重大なセキュリティリスクを抱えているという問題があります。

ISO 26262 規格で定義されているように、車載システムにおける安全性とセキュリティは基本要件となっており、許容範囲レベルのリスクを保証しています。これらのリスクは、自動車メーカーやサブシステムを提供するサプライヤーによって管理されていますが、車載エレクトロニクスの複雑化に伴い、機能的安全性は重要なコードとデータを格納するフラッシュメモリを含めた IC メーカーの責任でもあります。

車載セキュリティとは、情報を隠し、すべてを暗号化することで、サイドチャネル攻撃などの高度なテクニックによる情報漏洩を防止することです。フラッシュメモリアレイに保存されたデータは分解・混合して暗号化される必要があります。また、通信チャネルは強力に暗号化される必要があります。同様に、車載システムの安全性には、100%の可観測性、エラー検出、情報の最大開示が重要です。データを検証し、テストにて ODPDM に近い非常に高い品質レベルを保証する必要があります。さらに、不具合分析により、不良の根本原因を検出し、品質の向上に努めていく必要があります



自動車メーカーが問うべきこと

近い将来、市場で実際にセキュリティ侵害が起こるかもしれない、そうなる前のまさに今、自動車メーカーや車載電子システムのサプライヤーは大きな岐路に立たされています。自動車メーカーは、どのようなフラッシュメモリ技術を採用するかを選択することができますが、それは、そのフラッシュメモリを搭載した製品が市場に出た際、車両や搭乗者を保護できるか否かを大きく左右します。例えば、次の質問を試みてください。

● そのフラッシュメモリ技術は CC EAL 認証を受けているのか？ またそのレベルは？

セキュアなソリューションは、認証を受けていなければ本当の意味でセキュアであり、信頼できるとは言えません。CC EAL5+ 認証の取得は、V2V や V2X を含むあらゆる車載アプリケーションにおける、最高のセキュリティ要件を満たすことを示します。このタイプのセキュリティがあれば、そのアーキテクチャは非常にわずかなデータの不正変更さえも検出し、直ちにホストに報告します。格納されたデータは、いかなる不正変更、あるいは故意やエラーによる書換変更からも保護されます。このような変更は直ちにホストに報告され、報告システムを遮断することは不可能です。またフラッシュメモリアレイは、CRC によるビットエラー検出コードの追加レイヤーにより保護すべきであり、メモリ内には、誤った状態を検出するための高度なロジックが組み込まれています。さらに SPI インターフェイスのプロトコルが暗号化とエラー検出の両方のレイヤーを追加し、エラーに対するセキュリティと安全性を両立させています。

● フラッシュメモリを製造する工場は、安全性に関する ISO 26262 を取得しているのか？

2011 年に打ち出された機能安全規格 ISO 26262 は、車載電子機器のサプライヤーが ASIL (Automotive Safety Integrity Level) の要件を満たしているか否かを検証するための認証指標です。ISO 26262 自動車安全認証には、製品のライフサイクル全体における機能的安全性、コンセプトフェーズ、システムレベル、ハードウェアレベル、ソフトウェアレベルの設計と検証、製造、運用、保守、廃棄サービスの管理が含まれます。ISO 26262 の ASIL-D は、最高レベルのリスクマネジメントを表し、ASIL-D 向けに開発されたコンポーネントやシステムは、最も厳しい安全性要件に沿っています。自動車の重要な機能のコードを格納するフラッシュメモリデバイスは高い安全性要件を満たし、信頼性の高いコード格納を提供することで、安全性のリスクを低減する必要があります。

● セキュリティの実装はアップグレード可能でプログラマブルか？ RoT (信頼の基点) の実装は？ ソリューションはプラットフォームレジリエンシー (回復力) を備えているか？

セキュアなソリューションには、システムを侵害から守るため時間の経過とともに進化・適応できる、一定レベルのプラットフォームレジリエンシー (回復力) が不可欠です。MCU や SoC が使っている従来の ROM やフラッシュ内蔵型のアプローチには、ソフトウェアによる実装が用いられており、RoT のコードは ROM

に格納されています。これらのシステムはアップグレードができず、将来の攻撃に対する適応力がありません。一方で最新のアプローチは、MCU/SoCとプログラマブルなセキュアフラッシュメモリをベースにしています。これらのソリューションは、ソフトウェアと強化型ハードウェアをベースにした実装を用いているため、プログラマブルでアップグレード可能です。このようなプログラマブルなハードウェアベースの RoT は、増え続けるさまざまな脅威に対処するために、継続的なアップデートが可能であり、かつプラットフォームレジリエンスを提供します。

上述の理由などから、車載システムにはフラッシュメモリに対する最新のアプローチが必要であることは明らかです。市場に出回っている従来のフラッシュメモリ技術とは異なり、暗号化されたセキュアな標準 SPI バスを介して、セキュアな領域と SoC/MCU との間でコードやデータの転送を可能にする新しい技術が必要とされています。将来的には、これらのよりセキュアなフラッシュメモリソリューションが、特にサイバー攻撃が広範かつ巧妙になってきていることから、セキュリティのガイドラインや基準を満たすための要件となる可能性が高まっています。また、規制がより厳しくなることが予想され、車載アプリケーションにおけるセキュリティと機能的安全性の重要性がさらに高まるが見込まれます。

未来の車

エレクトロニクスは、ボディ、パワートレイン、インフォテインメントシステムなど、今日の自動車におけるほぼすべての部分で、極めて重要な役割を果たしています。消費者が高度な安全性、セキュリティ、インフォテインメント、快適性、利便性などのイノベーションを求めるようになり、各国政府の燃費基準が上がり続けている中、次世代の自動車にはより多くの電子部品が搭載されることになります。これにより、フラッシュメモリのようなコアテクノロジーが、最高レベルのセキュリティと安全性の基準を満たすことがますます重要になります。ハッカーからの脅威は巧妙さを増しており、半導体メーカーはこれらの攻撃を迅速かつ効果的に阻止できる、最新のアプローチを開発する必要があります。もしご自身の車を考えた時、安全性とセキュリティは、絶対に譲ることができないのではないのでしょうか。



お問い合わせ先

ウィンボンド・エレクトロニクス株式会社 マーケティング & FAE 部
mkt_online.jp@winbond.com
<http://www.winbond.com>