ハイライトレポート

2024. 7. 31 Day2

【自動車サイバーセキュリティの概要と対策】
ISO/SAE 21434時代に向けたMicrochipの車載セキュリティソリューション

車載セキュリティ対応のために

ISO/SAE 21434で求められる組織としてのルール作りや開発プロセスの制定については、手法が確立されてきています。一方具体的なセキュリティ実装における習熟度はサプライヤ間のギャップが見られます。そこで本セミナーでは半導体サプライヤ視点から見た勘所となる、「ハードウェアだけが実現可能なセキュリティ要求」と部品の選定ポイントについて紹介しました。
また暗号鍵を使った実装時に見落とされがちなポイントである、「暗号鍵のライフサイクル管理」の重要性についても説明しました。

ハードウェアセキュリティの必要性

ハードウェアセキュリティ機能は、セキュリティ要求レベル応じた使い分けが重要となります。
ここでは要求を3つのレベルに分類し、どういった機能実装が求められるか、どういったハードウェアセキュリティが最適かをMicrochip社での製品例を交え解説しました。

①Firmware update要求なしの場合
②Firmware update要求ありの場合
③車外との認証を行う為の識別子の生成と保護が必要な場合

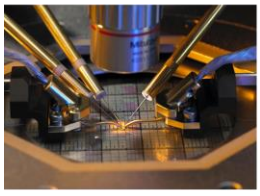
■ 本日の登壇者 ■

マイクロチップ・テクノロジー・ジャパン株式会社
松山 将之 氏　氏

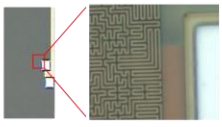
組込みシステムグループ
FAEマネージャ

ハードウェアセキュリティは信頼できる耐タンパ性がキモ

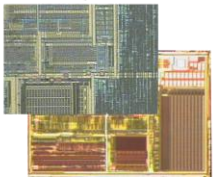
セキュリティ要求レベルによっては、耐タンパ性能も部品選定には重要な要素となります。ここでは耐タンパ性能の客観指標としての第三者認証の位置づけと、Microchip社のセキュリティICは耐タンパ性基準で最高のJIL-Highを取得対応についても説明しました。



Microchip社の
セキュリティ デバイス

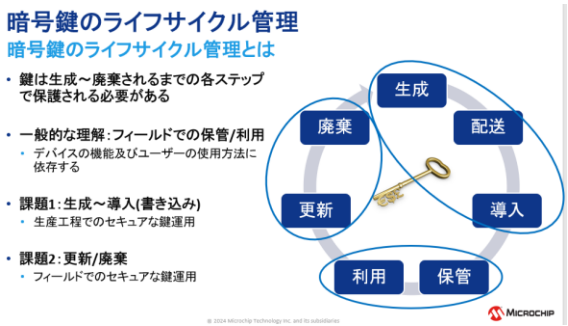


一般的なデバイス



暗号鍵のライフサイクル管理

ISO/SAE 21434でも明示的な記載がない為、暗号鍵の管理はフィールドでの保管・利用のフェイズのみが着目されがちです。しかしながら鍵は、生成から導入、また市場に出荷されてからの更新・廃棄、といったライフサイクル全体での運用を管理することが肝要です。
ここでは、鍵のライフサイクル管理において、Microchip社の提供する生産時の鍵書き込みサービスとそれに伴う鍵生成の自由度、またTrust Managerによるフィールドでのセキュアな鍵運用についてご紹介しました。



暗号鍵のライフサイクル管理
出所：投影資料より一部抜粋

他のウェビナはこちらから

リョーサンウェブサイト