セーフティとセキュリティ ―ホリスティック（全体論的）アプローチ

Safety and Security – A Holistic Approach

レベル	措置	実施事項／必要条件
1	▪ . . .	▪ . . .
2	▪ セキュア（リ）プログラミング ▪ . . .	▪ セキュアアップデート／フラッシング ▪ 完全にソフトウェアで実施 ▪ . . .
3	▪ セキュア（リ）プログラミング ▪ システム起動時の完全性チェック ▪ . . .	▪ セキュアアップデート／フラッシング およびセキュアブート ▪ ハードウェアのパッシブセキュリティ モジュールで対応（たとえばセキュアハード ウェアエクステンション（SHE）など） ▪ . . .
4	▪ セキュア（リ）プログラミング ▪ システム起動時の完全性チェック ▪ 周期的な実行時の完全性チェック ▪ . . .	▪ セキュアアップデート／フラッシング、 セキュアブート、および実行時操作検知 ▪ ハードウェアのアクティブセキュリティ モジュールで対応（たとえばハードウェア セキュリティモジュール（HSM）など） ▪ . . .
5	▪ . . .	▪ . . .

コネクテッドビークルに必要な新しいリスク認識

車載 IT システムは外界からますますアクセスされやすくなっています。これにより、新たなチャンスだけでなく、新たなリスクももたらされるため、リスクアセスメントおよびセキュリティアーキテクチャの根本的な再評価が必要になります。今後はセーフティとセキュリティを今まで以上に緊密に調和させなければならないでしょう。そこで必要となるのは、車両の全コンポーネントをライフサイクル全体にわたってカバーする全体論的なアプローチです。

朗々とした声で観光名所を案内して、歴史的背景の情報を紹介し、また時には地元のバーやお店のお得な最新情報をお知らせします。あなたは今、広告収入を資金にした、コネクテッド技術に基づくプログラムを利用して、ご自分の車でオンラインの市内観光をしているところです。センサが周囲の環境をモニタして、そのデータを車の ECU および通信設備に送り、通信設備が交通管制センタおよび近くにいる他の車との交信を維持します。

このようにデータが継続的に交換されるおかげで、交通は流れ続けます。事故や渋滞はまれな出来事です。交通信号は車両データを受信して、信号の変わるサイクルを交通量に合わせてリアルタイムに調整するので、道路交通による CO_2 の排出レベルが低減します。駐車場を探している車が交通の流れを妨げることはもうありません。ドライバーと乗客は指定された停車ゾーンで車から降り、そこからはウェブベースのシステムが、次に利用可能となる駐車スペースに車を誘導します。駐車のために必要な手順については自動駐車アシスタントが、それまでその場に駐車していた車のデータを評価することにより、事前に算出することができます。

成功しているネットワークには脆弱性の入る余地なし

この未来像は、コネクテッド輸送の可能性を示唆しているに過ぎません。これまで外界から閉ざされていた車両 IT システムが車外の大規模なネットワークの一環として接続されたとき、いったいどのようなビジネスモデルが花開くことになるのかは、誰にもわかりません。任意で提出した運転データに基づいて保険料率が低くなるのと全く同様に、「車のインターネット」(“internet on wheels”) では、エンジン性能、ナビゲーションシステムおよび支援システムがアップグレードされることが考えられます。しかし、アプリ、アップグレード、および様々な車両占有者のモバイルデバイスや Car-to-X データトラフィック向けにデータチャンネルを開放すると、開発段階で未知の危険因子をはらむ新たなリスクがもたらされます。これらのリスクを最小限に抑えるためには、リスクアセスメントおよびセキュリティアーキテクチャの根本的な再評価が必要になります。

外界に向けた開放がますます進んでいるにもかかわらず、いまだに組込みセキュリティの実現が目標とされています。どのような状況でも、モバイルデバイスを介して密かに侵入したハッカーやウイルスが車とその占有者の安全を脅かすようなことがあってはいけません。また、車は、ドライバーが何もせずに未認証プロバイダから、テストが行われていないソフトウェアを不正にインストールされるという事態に対して、自動的に保護されなければなりません。このことからも、車の IT アーキテクチャには保護が不可欠です。

ライフサイクル全体にわたるリスクの分析と評価

明らかに、技術的変化が求められています。ネットワークに接続している車は、セキュリティ、外部からの攻撃に対する防御、およびセーフティ（緊急時にシステムの諸機能が障害を起こさないという保証）について、今まで以上に緊密に調和させなければならなくなるでしょう。セキュリティとセーフティの専門家は、ソフトウェアとハードウェアの開発が始まる前に知恵を集め、潜在するリスクを特定して評価しておく必要があります。そうすれば、潜在する障害の可能性と影響を ISO 26262 の ASIL（自動車機能安全度水準）に沿って格付けする評価手順を用いて、リスクに関する基本方針をまとめることができます。この基本的分析は全体論的アプローチに従って行い、常設のコンポーネントはもちろんのこと、間欠的に接続されるスマートフォン、サービス診断デバイス、サーバー、および無線（OTA）でデータ通信している車も考慮して行う必要があります。

システム内のリスクが評価され、セーフティとセキュリティの要件が明らかになったら、ソフトウェアアーキテクチャの設計に入ることができます。このように早い段階でも、エンジニアはどのデータがどのようにして ECU に入るのか、それぞれのデータの読取りや変更を行えるのは誰か、およびその後の機能とテストがどの仕様に従うことになるのかを明らかにする必要があります。コネクティビティが高まる中、車両システムの決め手となるのは、納品されたそのときから、外の複雑な世界とオープンに対話できることです。

ネットワーク化された世界でセキュアなシステムを実現するためには、包括的な保護が必要

執筆者

Dr. Simon Burton
ETAS GmbH
グローバルエンベデッドソフトウェアサービスディレクタ

Dr. Martin Emele
ETAS GmbH
プロダクトセキュリティグループ長

Dr. Thomas Wollinger
ESCRYPT GmbH
マネージングディレクタ

サービス工場へのリモートアクセス権を明確にすること、および受信するデータの送信者を認証することが必要です。また、暗号データも、システムの開発が始まるその瞬間からシステムが処分されるその時まで、不正アクセスから保護されなければなりません。車両の一意の暗号鍵は、不要になったら確実に削除し、セキュリティ関連情報が不適切な人物の手に渡らないようにしなければなりません。

すべてのコンポーネントの概要

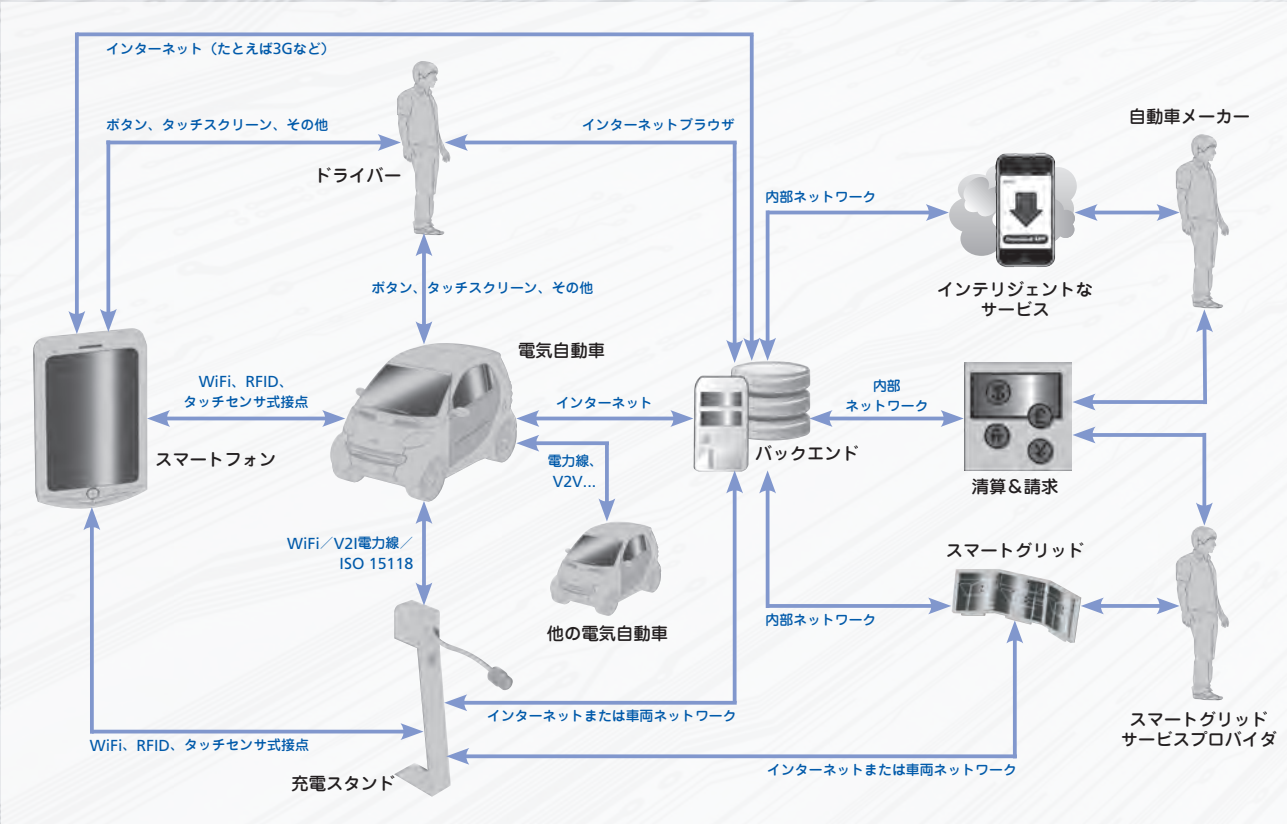
リスクの原因としては他にも、ファームウェアおよびソフトウェアの無線によるアップグレード（FOTA/SOTA）と、車両ソフトウェアに介入するアプリなどがあります。これらがコントローラ、センサ、およびアクチュエータとの強化連携が、全体のネットワークに脅威を与えます。この脅威の重大さは、開発者が外界から車両の機能への侵入を依頼された実験で証明されています。

たとえば、2015 年に米国のチームは、苦労を重ねた末ではありましたが、走行中のテスト車両のブレーキを作動させてエンジンを止めることに成功しました。メーカーはこのような攻撃に対して、たとえば、ファイアウォール、ゲートウェイ、および固有の暗号鍵により保護された通信を利用して車両を保護するなどの予防策を取る必要があります。セキュアな鍵管理には三重の効果があります。各車両が固有の暗号鍵で保護されていれば、ハッカー攻撃は非常に難しくなり、最悪の場合でも、影響は 1 台の車両にしか及びません。しかも、認証を行わなければならないことが、未知のソフトウェアとその送信者に対する門番の役割を果たします。

認証されたパートナーとだけデータを交換

今後は、適切な資格を持つスタッフが配属されているセキュアなデータセンタによって裏付けされたセキュリティソリューションを専門的に導入することは、Vehicle-to-X 通信への参加の決め手となるでしょう。データが受信者に届けられるのは、信頼できる署名を送信者が提供できる場合だけです。メーカー間および部門間にまたがる鍵管理ソリューションは、車両が大量のデータから関連する情報だけを取り出すのにも役立ちます。

未来のコネクテッドビークルネットワークには非常に多くのインターフェースがある



このため、セキュリティソリューションを確立することは、コネクテッドトラフィックのすべての利害関係者に義務付けられることでしょう。また一方で、緊急時にはセーフティソリューションも実施されなければなりません。
ISO 26262 などの規格に適合するシステマチックエンジニアリングは、攻撃を受けた場合や軽微なウイルス汚染が発生した場合にも車両のすべての重要機能が使用可能なままであることを保証します。
そのため、セキュリティ関連の領域は、後からインストールされるソフトウェアによる影響からも確実に保護されることが重要になります。ETAS の Hypervisor RTA-HVR などの市販のソリューションは、1 つの ECU を互いに厳密に分離された複数個のバーチャル ECU に分割することにより、ECU の機能を外的影響から完全に保護することができます。この方法を使用するためには、保護を必要とする中核機能を前もって定義しておく必要があります。それを行うためには、同一車上の ECU 間の強化連携を前提として、膨大な経験、十分に試行された手順、および効率的なツールが要求されます。具体的には Software--in-the-Loop および Hardware-in-the-Loop のテスト設備、機能するセキュリティプロトコル、または、メモリアクセス、計算時間、転送速度のリアルタイム監視を行うために必要な機器などが考えられます。そして最後に一番大切なこととして、このプロセスにはこの開発環境で快適に作業でき、要求される（システムの）基準と AUTOSAR などの業界基準について完全に理解している熟練のスタッフが必要です。

既存の知識を活用

ETAS にはこれらがすべて揃っています。弊社のモジュール式の製品とサービスのポートフォリオは、セキュアな組込みソフトウェアの計画、実装およびテストに関する専門知識および長年にわたる経験に端を発し、AUTOSAR 準拠のオペレーティングシステムおよびセキュア通信用プロトコルにこだわり続け、弊社のハードウェアセキュリティモジュール(HSM) または上述の Hypervisor RTA-HVR などのように、単なるツールという枠を超える存在として展開されています。
まもなくメーカーは自身のアップデートおよびアップグレード向けに後者を利用して、選択された ECU 領域を予約できるようになります。これは、将来のコネクティビティ市場において現在よりさらに高度なセーフティとセキュリティを保証する、また別の方法です。そしてまた、ETAS の子会社 ESCRYPT が提供するモジュール式のセキュリティソリューションも販売されています。このソリューションはすべての新車のライフサイクル全体を対象に、暗号ソフトウェアのライセンスから完全な鍵管理に至るまで、トップセキュリティのデータセンタでの処理を含めてカバーしています。

ノウハウを応用して手ごろな価格でリスクを最小化

コネクテッドビークル内のすべての ECU を完全に区分化できないのは、ひとえにコストがかかるからです。実現のためには妥協が必要ですが、それはリスクを分析し評価して初めて可能になります。リスクの分析と評価では、すべての車両システムの安全コンセプトについて、あらゆるものを含めて把握することが不可欠です。それを行うことにより、ある機能のセキュリティとセーフティが万が一脅かされたとしても状況に応じて対応し、システムをうまくシャットダウンできるようにするルーチンを実装することができます。

セキュリティとセーフティのアプローチをシステマチックに連結させることが非常に重要です。なぜなら、未来の脅威はまだわからないからです。そのような未知のリスクに立ち向かうべくコネクテッドビークルを効果的に装備するためには、適切な鍵管理をセキュアなビークルシステム設計と結び付けるしかありません。脅威が姿を現すたびにただそれに反応するだけでは不十分です。セキュリティアーキテクチャの根本的欠陥をアップデートで修正することはできませんし、データの転送レートが制限されていることを考えると、面倒なセキュリティアップデートをとにかく最小限に抑える必要があります。

まとめ：リスク認識の調整 – 対策のパッケージをまとめる

コネクテッドビークルのネットワークには、新しいリスク認識が必要です。膨大な数の車とそれらの使用頻度および外部のデータストリームへの接続が、障害の可能性を高めています。その結果として起こる損害を最小限に抑えるために、普通はそれぞれ別個に実行されていたセーフティソリューションとセキュリティソリューションをこれまでよりはるかに緊密に連結させることが必要になります。開発に先だってリスクの総合評価を全体論的に行うことは、コネクテッドビークルを現在と未来のリスクから確実に守るために欠かせない前提条件です。製品のライフサイクル全体を通じて、「セーフティとセキュリティを計画的に実現すること」をモットーにしなければなりません。