Diagnostics and Security: Brave New World

Opportunity or risk?

慣れ親しんだ真実というのは、ちょっと厄介なものです。現代の車両診断も例外ではありません。これまでは、標準化されたOBDコネクタを介して車両にアクセスしていたという事実に頼ることができました。また、標準化されたプロトコルベースの通信手段にも。ちなみに、設計上重要なセキュリティ要件を満たすことができないプロトコルですが。しかし、現代の自動車はさまざまな方法で外部に開かれています。V2x（Vehicle to any environment）では、外部機器との無線通信が必要ですし、現在のすべての車両に必要なeCall機能にはSIMカードが必須です。また、修理工場に行かなくても車両のソフトウェアを更新できるようにしたいという要望（SOTA - Software over the air）から、診断環境にも無線接続が浸透してきています。

しかし、それにはリスクも伴います。無線通信経路に無断で侵入した場合、甚大な被害が発生する可能性があります;

- 人身事故：ハッカーが車両を操作した場合、人が怪我をしたり、死亡したりする可能性があります。
- 保証請求：チューナーが無線で車両データを修正し、早期に故障を誘発するため、OEMの費用で部品を交換しなければならなくなります。
- データ保護：許可されていない第三者が個人情報にアクセスする ---現在の法律では、VIN（車両識別番号）も個人情報に含まれます。罰金は1件につき50,000ユーロにもなります。

最近の報道では、被害の大きさを示す例が取り上げられています。ブリティッシュ・エアウェイズが顧客データを十分に保護していなかったのです。英国の法制度は、2億ユーロの罰金を決定しました。(2019年7月8日、シュピーゲルオンライン)

Originally published in German in the section “Measurement - Test - Diagnosis” of the technical magazine HANSER automotive 10/2019, published by Carl Hanser, Munich, Germany

Hardware and software repair

今日、自動車のライフサイクルは、診断なしでは考えられません。機能が分散した100個以上のECU（Electronic Control Unit）で構成されるネットワークを修理することは、修理工場のメカトロニクス技術者では不可能です。製造においても、車両がどの段階で正しく組み立てられているかを製造ライン担当者によって判断することは非常に難しいといえます。

また、設計・開発の現場では、製品に近いECUの多くの変数にアクセスできません。

これらのケースでは、エキスパートシステムが車両自体で生成され利用可能な情報を評価しなければなりません。さらに、診断に導入された通信メカニズムは、ECUソフトウェアの更新にも使用されます。これは、新バージョンを導入してテストを行うエンジニアリングの現場でも、製造やアフターサービスの現場でも同じことが言えます。ソフトウェアの修理は、最新バージョンのソフトウェアを使って効果的に行われます。

車両にアクセスする際のサービスには、基本的に3つのタイプがあります。

- 読み取りサービスは、車両から情報を読み取るためのものです。その情報とは、ECUが機能を制御するための物理的な値である「計測値」や、「エラーメモリエントリ」などです。エラーメモリのエントリは、セルフテストを継続的に実行する過程で異常が発生すると、ECUによって入力されます。
- ライティングサービスは、ECUの内容を変更するものです。これは、一方ではプログラミングで、もう一方ではバリアントコーディングで行われます。これにより、統一されたECUソフトウェアを、以下のような様々な動作モードに適応させることができます。例えば、国の特性（ステアリングホイールが右か左か）や、装備オプションの違い（同じエンジンで出力レベルが異なる）など。
- サービスを実行することで、ECU内でルーチンを開始することができます。これには、ワイパーモーターなどのアクチュエーターのアドレス指定やテスト機能などが含まれます。診断機能を使用すれば、例えばテストベンチなどのスイッチは必要ありません。

現在、車両へのアクセスには2つのバスシステムが使われています。1つは従来のCANによるUDS（Unified Diagnostic Services）プロトコル、もう1つはイーサネットによるDoIP（Diagnostics over IP）プロトコルです。

Gateways...

診断がローカルで行われている限り、つまり診断テスターと診断インターフェースや車両との間をケーブルで接続している限り、診断システムは不正アクセスに関する限り基本的に安全であると考えます。しかし、インターネットを介した遠隔データ接続があると同時に、状況は一変します。：

車両とのリモート診断接続は、アプリケーションを起動し、車両を選択した後にユーザーが確立します。一般的には、トランスポート層としてインターネットが使用されます。この接続は、関連するサービス要求を車両に送信するために使用され、車両はすべての条件が同じであれば、関連するレスポンスを送信します。

要求されたデータが受信されると、テスター・アプリケーションはそれを評価し、必要に応じて情報をデータベースに保存します。

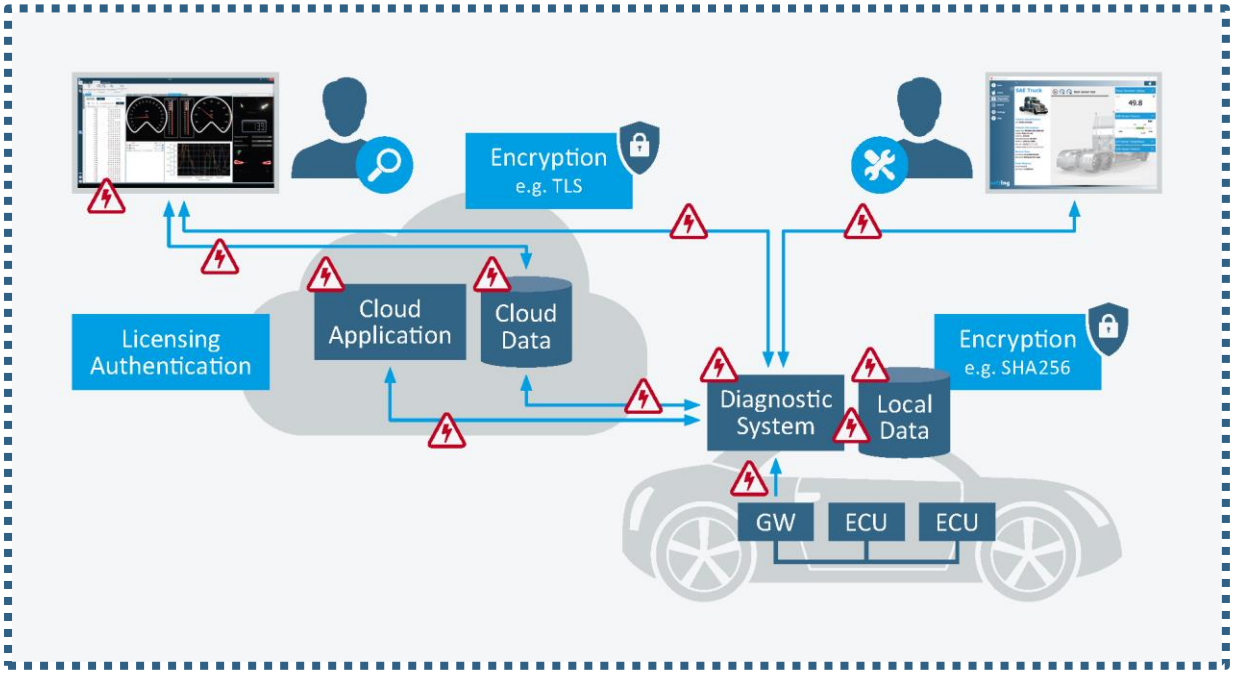

Figure 1: The Diagnostic Ecosystem
(© Softing Automotive)

Originally published in German in the section “Measurement - Test - Diagnosis” of the technical magazine HANSER automotive 10/2019, published by Carl Hanser, Munich, Germany

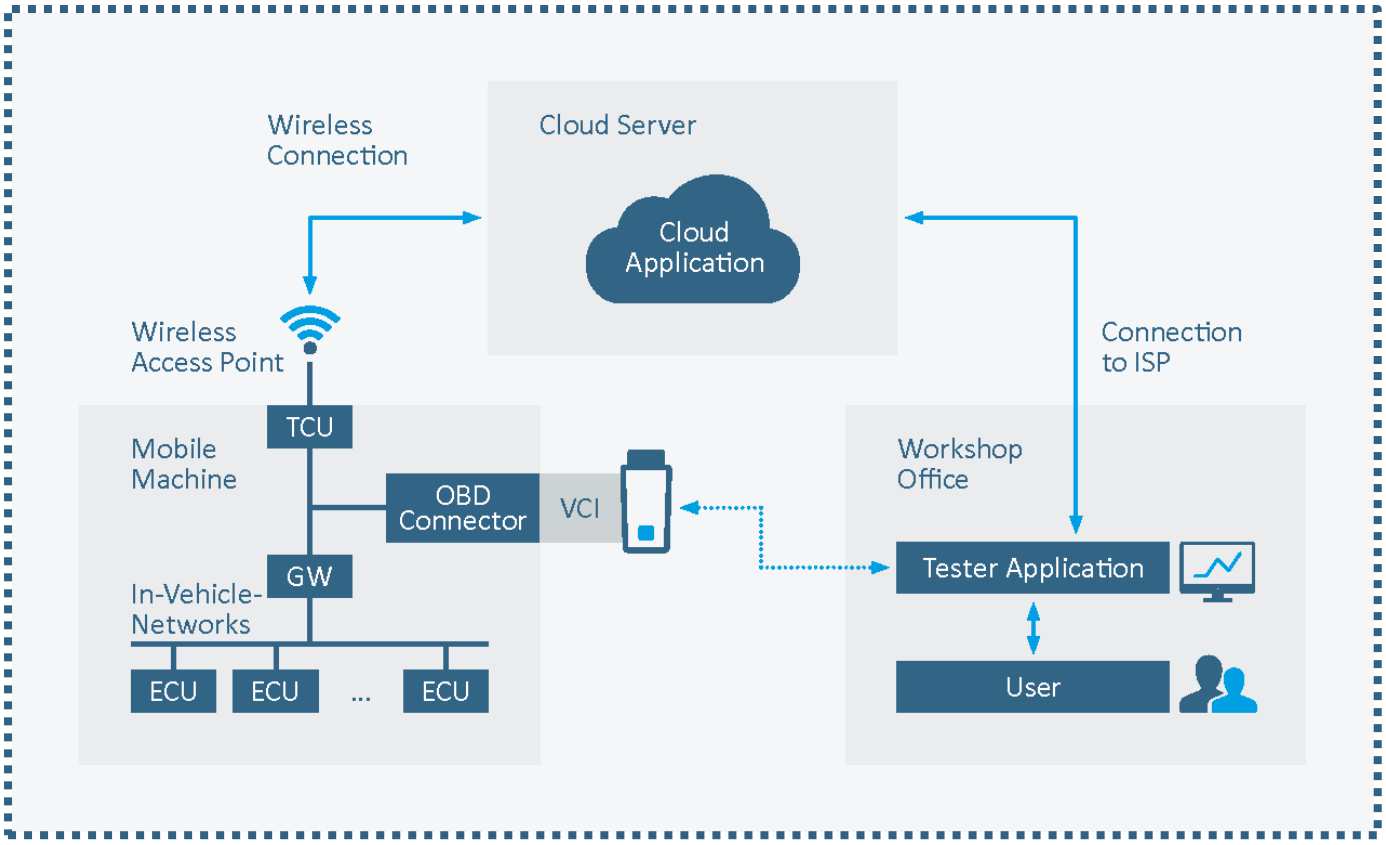

Figure 2: Gateways for Hacker Attacks from the Application to the Vehicle
(© Softing Automotive)

一見すると、現代の自動車環境における日常的なシナリオです。しかし、よく見てみるとテスター・アプリケーション側に最初の攻撃ポイントがあることがわかります。：テスターアプリケーションは、不正なアクセスやハッキングに対して十分な保護を持っているでしょうか？オフィス部門でおなじみのアクセスデータを不用意に扱うことは、非常に大きなリスクとなります。しかし、診断ソフトウェアを最大限に保護しても、関連する権利が中途半端に割り当てられていては役に立ちません。：関連するユーザーは、実際に特定のサービスを実行する権利があるのでしょうか？すべてのユーザーがECUのプログラムやコーディングを行えるわけではありません。多くの場合、最初はサービスを読むことだけに権限を限定し、状況が発生したときに、権利の延長が有用かどうか、いつまで可能かどうかを明確にすることが重要です。

さらに重要なことは、収集したデータの保存です。：意図しないアクセスからデータを最大限に保護することが絶対に必要です。ビッグデータの時代には、このデータはハッカーにとって最も重要なターゲットの一つです。あとは、インターネット上のデータ接続だけです。：考えられる攻撃の形態は多岐にわたります。データ操作による通信の盗聴、通信回線の乗っ取りなど、事実上、すべての攻撃が考えられます。このような中間者攻撃を避けるためには、データ接続の安全性を確保することが非常に重要です。

...and How to Close Them

最大限のセキュリティを実現するためには、End2Endの暗号化が絶対に必要であり、これは車両の最初のインターフェイスで完結します。診断システムは、車両内の通信に影響を与えません。この分野の暗号化は、OEMの責任範囲です。

適切なアクセス権、持続可能なライセンス、そして診断アプリケーション側と保存データ側の最新の暗号化手法を使用することで、高度なセキュリティを実現することができます。診断に必要なODXやOTXのデータも暗号化がキーワードとなります。さらに、権限のない人によるアクセスを防ぐための適切なプロセスとツールが必要です。

データ接続を保護するための暗号化方式には、対称型と非対称型があります。どちらの方式にもメリットとデメリットがあるため、どちらの方式を採用するかは個別に判断する必要があります。プロトコルレベルでの暗号化を追加することで、セキュリティレベルを向上させることができます。自動車業界で最も広く使用されている診断プロトコルの一つであるUDSの場合は、標準規格が定められているため不可能ですが、診断プロトコルの中でも最も新しいプロトコルである「DoIP」の場合は、TLSによる暗号化が標準規格として準備されています。

しかし、このようなセキュリティ対策の中でも、例えば性能や操作性など、診断にとって重要な側面を無視することはできません。

Originally published in German in the section “Measurement - Test - Diagnosis” of the technical magazine HANSER automotive 10/2019, published by Carl Hanser, Munich, Germany

Remote Diagnostics with Softing SDE

テスターに必要なアプリケーションの数が多いため、診断方法を統一的に実装し、簡単に統合できる高性能な診断ミドルウェアが必然的に必要になります。その一例がSofting SDE (Smart Diagnostic Engine)です。これは、標準化された診断データ(ODXおよびOTX - ISO 22901およびISO 13209)を処理するために、業界でテストされた診断コンポーネントと、理解しやすいAPIを組み合わせたものです。これにより、エラーメモリの読み出しやECUのプログラミングなど、最も重要な診断方法を機能として利用することができます。サービス指向のアプローチは、ベースとなっている規格とは異なり、完全なリモート対応が可能であり、通信リンクは標準的なメカニズムで比較的容易に保護されています。お客様は、エンジニアリング・テスターとテストベンチで同じ診断機能を使用できるようにするために導入されますが、現在では別々のサイトで運用されています。このようにして、世界中に分散しているエンジニアリングの利点は、さらなる効率化の基準となります。

New Diagnostic Possibilities – For Sure!

将来的には、自動車業界において車両内および車両周辺の診断と通信は、開発、製造、テスト、アフターセールスのいずれにおいても、これまで以上に重要な役割を果たすことになるでしょう。

これらに加えて、セキュリティに対する要求も常に高まっています。将来的には、自動車の安全な運転と診断を確保するために、この2つの分野のバランスをとることが必要です。

これは、自動走行などのテーマを考えると特に顕著になります。

だからこそ、将来的には、現在の技術水準に基づいてセキュリティの側面を考慮し、実際の機能性を便利に利用できるソリューションを提供することがより重要になるのだと思います。

セキュリティはアドオンではなく、ソリューションに不可欠な要素でなければなりません。

>> automotive.softing.com

Markus Steffelbauer heads up Product Management and Marketing at Softing Automotive and is a committed member ofstandardization bodies.

Günter Fahböck is a Project Manager at Softing Automotive. He specializes in cybersecurity in the diagnostic environment.

Originally published in German in the section “Measurement - Test - Diagnosis” of the technical magazine HANSER automotive 10/2019, published by Carl Hanser, Munich, Germany