自動車クロスドメイン セキュリティフレームワーク

次世代ビークルコンピューターにおける安全性、セキュリティ、柔軟性の確保

Empowering Tomorrow's Automotive Software

www.etas.com

ETAS

概要

このホワイトペーパーでは、ETASの「自動車クロスドメインセキュリティ」フレームワークの活用（アプローチ）を提案します。このフレームワークは、厳密に分離された通信チャネルを使用するセキュリティドメインを明確に定義します。このアプローチによって、企業のネットワークを構築する拠点同士のように、ドメインの各機能が分離されていながらも相互接続された状態を維持しつつ、次世代の車載アプリケーションに必要なセキュアで柔軟なアーキテクチャを構築できます。本書では、ソフトウェアディファインドビークル（SDV）への移行過程におけるアプローチの構造について考察を深め、不正アクセスのリスク軽減効果を明らかにします。技術的な解説に加えて、実際のビークルコンピューターへの攻撃シナリオを用いて、信頼できる実行環境（TEE）とハードウェアセキュリティモジュールを組み合わせることによる具体的なメリットを示します。さらに、将来のセキュアな車載コンピューティングの実現に向け、「自動車クロスドメインセキュリティ」フレームワークをどのように活用してゼロトラストパラダイムを確立できるかを説明します。

1. はじめに

自動車業界は、大きな変革期を迎えています。近い将来、フリート（法人が所有する複数台の車両）は、ライフサイクル全体を通じてアプリやサービスのOTAアップデートが主流となることで、ソフトウェアデファインドビークル（SDV）が大半を占めると言われています。これはメーカーにとって、重要な意味を持ちます。競争が熾烈さを増す自動車業界において、すべての（サイバー）セキュリティ要件を満たし、同時に新しい機能をリリースするという大きなプレッシャーの中でイノベーションサイクルの短縮も求められるからです。SDVの主要コンポーネントであるビークルコンピューター（電子制御ユニット）のセキュリティと、イノベーションスピードとの適切なバランスを確保することはきわめて重要です。統合やプログラミングに多大な労力を費やすことなく、動的な適応と安全性の両立を実現できるシステムの開発が求められます。これを達成するための効果的な方法は、厳密に分離されながらも相互接続されたドメインをビークルコンピューター内部に設けることです。これにより、車両の安全性を損なうことなく、セーフティクリティカルな機能と非セーフティクリティカルな機能を共存させることが可能になります。

自動車業界に留まらずあらゆる分野において、増大し続ける外部からのサイバーセキュリティ脅威への対応が喫緊の課題です。世界規模でのデジタル化が加速するなか、複雑化するシステムにおける柔軟性とコネクティビティを高め、同時に機能的整合性を維持できるかが大きな焦点となっています。そのため、特定の分野に固執せず異なる分野にも視野を広げ、実証済みソリューションを適用していくことが求められます。たとえば、エンタープライズITアーキテクチャの構成要素を掘り下げて整理してみると、クロスドメインソリューション（CDS）[1]というセキュリティ原則（サイバーセキュリティ技術）が確立されていることがわかります。ETASは、この分野で積み重ねてきた知見をビークルコンピューターに実装することで、「自動車クロスドメインセキュリティ」フレームワークを開発しました。このフレームワークを活用し、厳密に分離された通信チャネルとセーフティクリティカルな機能を分離することで高いセキュリティレベルを実現することができます。

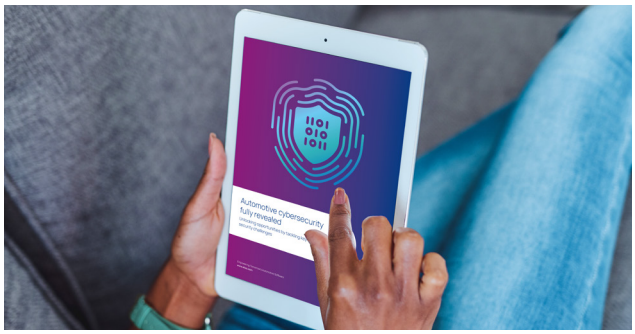
2. ビークルコンピューターセキュリティの課題

従来の車載ソフトウェア開発においては、エンジニアリングプロセスはアプリケーションの規模や複雑さにあまり左右されませんでした。一見無害なアプリでも、ドライバーの安全を脅かす誤動作やマルウェア（悪意のあるソフトウェア）の侵入経路を生み出さないよう、あらゆる車両機能の整合性や安全性をチェックするテストは不可欠です。外部からのアクセスチャネルと要求の増加に伴い、車両はより多くのリスクにさらされ、車両のセキュリティ全体を維持するために必要な労力は指数関数的に増大しています。

こうした状況に対処するには、ソフトウェアの開発、デプロイメント、運用を簡略化しながら、同時にユーザーの安全性とシステムの信頼性を高いレベルで維持できる新しいソフトウェアアーキテクチャが必要です。ビークルコンピューターは、車両のさまざまな機能を中央で制御し、ソフトウェアデファインドビークルの未来を切り拓きます。しかし、課題もあります。自動車メーカーは、最適なパフォーマンスを達成すると同時に、増加するサイバーセキュリティに対して適切な対策を採り、高い柔軟性を確保しなければなりません。自動車業界の多くの企業が、この課題の解決に踏み出しています。既存の枠にとらわれる必要はありません。すでに成功しているアプローチを検討してみる価値が十分にあります。

自動車サイバーセキュリティの全貌解明ガイド

自動車業界のサイバーセキュリティについて、さらに詳しく知りたいと思いませんか？ ETASのホワイトペーパー『自動車サイバーセキュリティの全貌』は、自動車メーカーが直面している主要な課題とビジネス機会をさらに深く掘り下げ、変化の激しい自動車サイバーセキュリティの世界を把握し展望を開くための包括的なガイドです。



3.　安全性に関わる機能

車両の安全関連機能といえば、まず思い浮かぶのはブレーキ機能、エンジン制御、エアバッグなどが挙げられます。SDVへの移行に伴い車両アーキテクチャの変化が進んでいるとはいえ、こうした安全性に関わる重要なコンポーネントは、今でも多くの場合、ビークルコンピューターの一部（ドメイン）としてではなく、個別のECUによって独立して制御されています。しかし、これらの安全性に関連するコンポーネントに直接影響を与えるさまざまな機能や信号は、必然的にビークルコンピューターに移管されることになります。センサーテクノロジーの制御と処理から、障害物検知（またはADAS全般）や横滑り防止装置（ESC）のような運転に影響を及ぼす高度な機能を含め、さまざまな機能がビークルコンピューターに統合されることになります。このホワイトペーパーでは、「安全性に関わる機能」について言及する場合は、快適性を高める機能やエンタテインメント系の機能、さらにはコネクティビティ機能と共にビークルコンピューターで稼働する、こうした新しい機能を含む幅広いカテゴリを指します。

4.　エンタープライズITセキュリティから得られる知見

複雑で高度に接続されたシステム内で柔軟性とセキュリティを両立させるという課題に取り組むのは、自動車業界が初めてではありません。エネルギー、金融、医療といった主要な業界でも、セキュリティレベルの異なるIT環境が広がっています。エネルギー企業を例に取ると、電力網の運用を制御する社内ネットワーク（機密データ）と顧客サービス向けの外部ネットワーク（機密性が低いデータ）が存在しています。こうした業界のクロスドメインアプローチでは、仮想化の仕組みを使用して複雑なシステムを独立したユニットに分離し、機能の管理、リアルタイムの検知と防止を担うセキュリティドメインを設定します（図1）。

クロスドメインアプローチを採用することで、異なるドメイン間のセキュアなアクセスとデータ転送を管理することができます。これにより、運用データを確実に保護しながら、インターネット経由でさまざまなソースと双方向でデータを送受信するといった外部とのコミュニケーションが可能になります。こうした業界の企業は、すでに取り組みを始め、拡大するサイバー脅威に対抗する手段を確立しています。

1台の車両を、企業のネットワークに匹敵する複雑なITネットワークとして捉える視点が必要です。車両のネットワークは、多数のドメインが存在し、ドメイン間であるいは外部のソースと接続しているか、接続が可能です。そのため、前述したクロスドメインの仕組みは、車両のソフトウェアにも適用可能です。ただし、忘れてならないのは、どれだけデジタル化が進んでも、自動車は人を運ぶための機械であるという事実です。したがって、すべての道路利用者の安全を常に最優先で考える必要があります。

厳密な分離：
専用の仮想マシンがデフォルトで分離を確保し、ネットワーク内での脅威の水平/横展開（ラテラルムーブメント）を防止します。

永続的な制御：
ネットワークとシステム構成、ソフトウェアの更新、アクセスポリシー、キーのローテーション、その他すべての非機能要件（システムの機能以外の要件）に対する制御は、分離されたセキュリティドメインに移管されます。柔軟性が向上し、機能ドメインからの攻撃にさらされることなく、これらの制御を動的に実行できます。

リアルタイムの脅威検知と防止：
セキュリティドメインを導入することで、機能ドメインの動作を妨げることなく、（仮想）ネットワーク通信とホストプロセスの両方に侵入検知システムのようなセキュリティソリューションをデプロイするための水平基盤が実現されます。これにより、攻撃を封じ込めるローカルなセキュリティ対応を実行できます。

図1：IT業界が外部のサイバーセキュリティ脅威に対処し、ITを簡略化するために採用しているクロスドメインアプローチの原則

5. ビークルコンピューターへの知見の適用

クロスドメインアプローチを自動車業界に適応するため、ETASはその基本的なパターンと、管理や接続の目的で追加のドメインを使用するというコンセプトの両方を取り入れています。その結果が、仮想マシン(VM)[2]とアプリケーション間で仮想ネットワークチャネルを利用して、領域に応じてセキュリティ対応を変える「自動車クロスドメインセキュリティ」フレームワークです。この仮想ネットワークチャネルにより、異なるドメインをシームレスに接続し、SDVのソフトウェアアーキテクチャ内でソフトウェアを柔軟に配置することが可能になります。

ドメインを分離し、それぞれの要件に合わせて防御戦略を変えることで、リスクを効果的に軽減することができます。図2の自動車に特化したアプローチは、4つのドメインで構成されています。

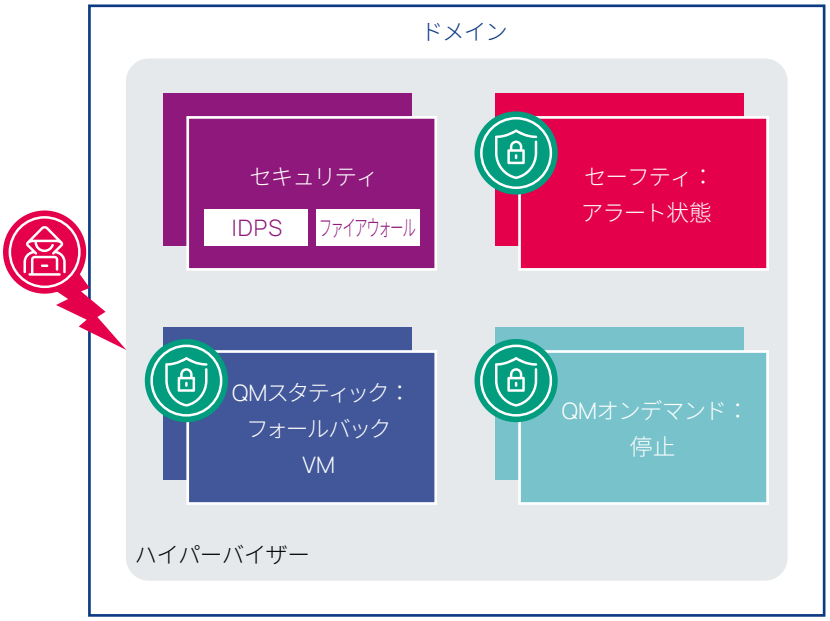


図2：仮想マシン内の自動車クロスドメインセキュリティフレームワークのドメイン(仮想マシンのカテゴリ)

セキュリティドメインは、すべての通信のゲートウェイとして機能します。セキュリティドメインには、専用のVM、ハードウェアセキュリティモジュール、TEE(Trusted Execution Environments)を含む、堅牢なセキュリティ対策が組み込まれています。さらにこのドメイン内の通信は、ファイアウォールシステムと侵入検知メカニズムによる厳密な分析を受けます。セキュリティドメインは、システム構成とポリシーに対して排他的な権限が与えられ、TEEのようなテクノロジーを活用して、通常の操作から確実に分離されています。この構成によって、積極的な防御メカニズムをビークルコンピューターに実装できます。その結果、外部のセキュリティオペレーションセンターへの依存を減らし、修正が利用可能になるまで攻撃を封じ込めることができます。

セーフティドメインは、第3章で説明したように安全性に関連するすべての機能を含みます。セーフティドメインは常に稼働しているため、アクティブな通信チャネルの数を減らすことを除いて、仮想マシンに対して直接介入する機能を持っていません。

品質管理(QM)スタティックドメインは、安全性には関連しないものの重要な機能に対応しています。QMドメインで不正な操作が検知されると、VMが停止され、フォールバックVMが起動されます。攻撃を封じ込めるために、実行中のサービスのデータはフォールバックVMに転送されず、サービスはリセットされた状態になります。さらに、攻撃の容易な再現を防ぎながら、インフォテインメントシステム関連などの基本的なQM機能を維持するために、接続を制限したフォールバックVMを構築することも可能です。

QMオンデマンドドメインは、可用性を必要としない残りのサービスのほか、エッジコンピューティングや実際のオンデマンド機能など高度な機能をサポートします。QMオンデマンドドメインは一時停止が可能で、その場合はすべてのサービスが停止されます。一時停止によってユーザーエクスペリエンスに影響が出るのは避けられませんが、不正な操作が検知された場合のやむを得ない措置として機能します。

6. 探求：セキュリティドメイン

セキュリティドメインは、重要なセキュリティコンポーネントをホストするため、クロスドメインアプローチにおいてきわめて重要な役割を負っています。アクセスやアップデートに関連するポリシーを管理するほか、プラットフォーム全体の監視を担うこともあります。各ドメインは図3のように仮想ネットワークを介して、セキュリティドメインを中心とするスター型トポロジで接続されます。この構成により、QMデバイスからセーフティドメインへのデータフロー（またはその逆方向のデータフロー）は、必ずこの「仮想ゲートウェイ」を通過することになります。このトラフィックには、シンプルなファイアウォールからディープパケットインスペクション、完全なプロトコルブレイク（システム間の通信を脅威から保護する機能）まで、幅広いセキュリティメカニズムを適用できます。すべてのセキュリティメカニズムは、中央のホスト上にある侵入検知システムに結果を報告します。

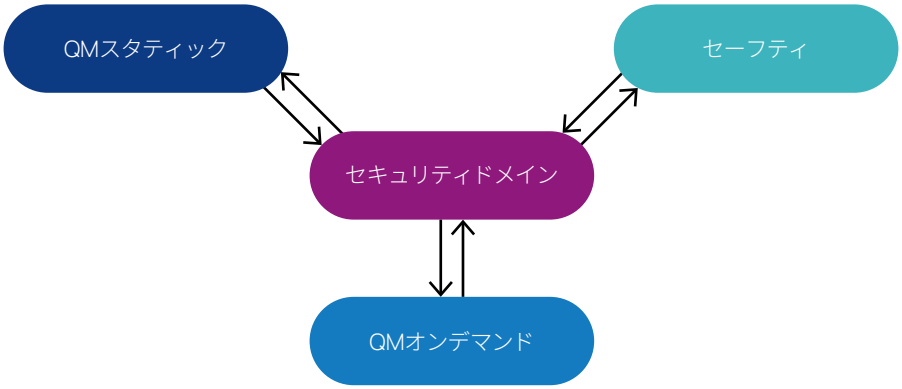


図3：ドメイン間の通信フロー（スター型ネットワーク）およびセキュリティ機能とパフォーマンスの提供に使用されるテクノロジー

このアプローチによって、セーフティドメインを保護するために十分なレベルのセキュリティが確保されます。ただし、必要な計算処理の負荷は大きくなる可能性があります。セーフティドメインでは、低遅延で高速の応答（CANバス上での処理など）が求められることが多く、通常は10 ～ 20マイクロ秒のリアルタイム処理が必要です。セキュリティ処理でこのレベルのサービス品質を保証するために、ハードウェアセキュリティモジュール（HSM）がセーフティドメイン専用で関連付けられることがあります。HSMは論理的にはセキュリティドメインの管理下にあり、セキュリティドメインがHSMに格納されるキーの配布と更新を担います。

セキュリティドメインそのものは通常のVMですが、補助的なテクノロジーを利用することがあります。HSMコアは、自動車業界でよく知られており、安全認証を受けた堅牢な暗号化機能を提供します。TEE[3]も、同様の暗号化機能を提供できます。しかし、TEEの強みはその柔軟性にあります。HSMコアはシステムオンチップ（SoC）設計に組み込まれたハードウェアコアです。一方、TEEはソフトウェアのオペレーティングシステムと、近年のCPUに搭載されているハードウェアセキュリティ機能を組み合わせたものです。そのため、TEEは、高性能なマルチコア、広大なアドレス空間、周辺機器へのアクセスといったCPUの機能をすべて活用できます。TEEは、多くの点で別のVMと見なすことができますが、プロセッサの状態とレジスタが独立しているほか、CPU内およびバス経由の両方でメモリが分離され、ハードウェアレベルで隔離されています。

ETASは、セキュリティコアが多くの機能をTEEで実行するようになると予想しています。たとえば、ソフトウェアの更新やドメイン間通信に関連するポリシーの評価をTEE内で完結させることで、攻撃者のアクセスを制限できます。同様にTEEは大量のデータを保存することができるため、複雑なキーのローテーションとアクセス制御ポリシーの管理を可能にし、さらに監査ログやクラッシュ時のデータを安全に保管しておく領域も提供できます。このアーキテクチャには高い柔軟性があり、HSMとTEEの間で、機密性の高いセキュリティ関連タスクを分配することもできます。QMスタティックドメインまたはQMオンデマンドドメインで実行されるアプリケーションは、TEEで実行される特定のアプリケーションへのアクセスを許可されることで、DRMで保護された動画の復号化など、自身のセキュリティ関連機能に直接アクセスできるようになります。

ここまで見てきたようなドメインの分割やセキュリティテクノロジー（HSM、TEE、ハイパーバイザー）を利用することで、ゼロトラストプラットフォームを構築し、以下のような機能を実現できます。

... 特に仮想ネットワークチャネルを活用し、
サービス単位で真正性、機密性、完全性を保護します。

... HSMを利用してセキュリティ上重要な資産を保護し、
アクセスを必要な範囲に制限します。

... TEEとハイパーバイザーを利用して、
アクセス権と管理権限を保護します。

... IDSでトラフィックとシステム全体のステータスを
監視します。

7. 実際のシナリオに基づくユースケース

このフレームワークの効果をわかりやすく説明するために、このアプローチがIT業界に由来することがよくわかる例を取り上げます。サービス妨害(DoS)攻撃は、ネットワーク機器に大量のトラフィックを送りつけて利用不能にし、機能を停止させる、よく知られたサイバー脅威の1つです。ITスペシャリストから小規模なWebサイトの運営者に至るまで、ネットワークに関わる人にはよく知られた攻撃ですが、この攻撃が自動車業界でも深刻な懸念になりつつあります。

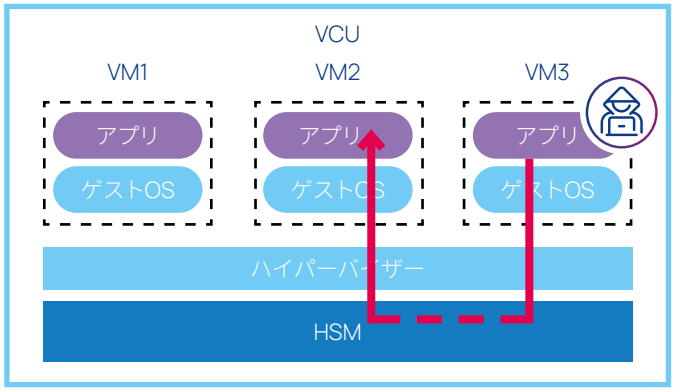
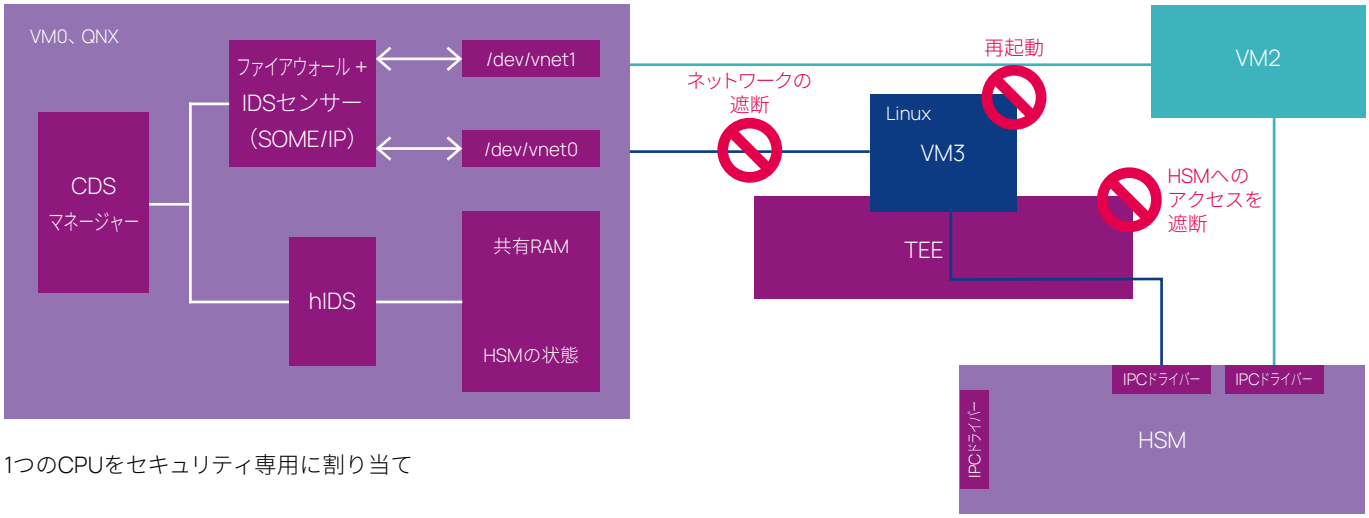


図4：VM3上のアプリから他のVMに影響を及ぼすサイバー攻撃

この例では図4に示すように、攻撃者がVM3内のアプリケーション(テレマティクスサービスなど)の乗っ取りに成功した後、実際の標的であるVM2の機能を攻撃しようとしていることを想定しています。つまり、攻撃者はVM3からVM2に攻撃を拡大する必要があります。ポイントは、この攻撃を成功させるために、これ以上の脆弱性が不要であるということです。この攻撃は、VM2とVM3のどちらもHSMに対する正当なアクセス権を持っているという状況を利用します。この例では、VM2の機能は安全なオンボード通信(イモビライザー機能や運転機能に影響するその他の信号など)のためにHSMを利用します。VM3にはHSMに対する正当なアクセス権があるため、大量のリクエストをHSMに送信するだけで、VM2は安全なオンボード通信を実行できなくなり、他の車載ECUから実質的に孤立します。

クロスドメインのセキュリティシステムを構築するために、図5の設定を使用します。この例では、QNXハイパーバイザーが、マスター仮想マシン(VM0)を使用しています。VM0はゲストVMを完全に管理できるため、セキュリティドメインとして使用されます。すべてのトラフィックをセキュリティソリューションでルーティングし、検査できるように、VM0には専用のCPUコアが1つ割り当てられています。テレマティクスサービスを実行するQM VM(VM3)とイモビライザーサービスを実行するセーフティVM(VM2)は、それぞれ専用の仮想Host2Guestネットワークインターフェースを使用して、セキュリティドメインに接続されています。



1つのCPUをセキュリティ専用に割り当て

■セキュリティドメイン ■QMドメイン ■セーフティドメイン

図5：多層防御でセーフティー VMへのサイバー攻撃を回避するシナリオ

VM2とVM3のどちらもHSMへのアクセス権があります。VM3とHSMの間にTEEを導入することで、HSMに対するすべてのアクセス要求をVM0の中央IDSに報告することが可能になり、DoS攻撃を容易に検知できます。さらにTEEは、アクセス頻度の制限やアクセスの完全な禁止といったアクセスポリシーを適用できます。つまり、この構成では、サービスレベルで攻撃に対処できることになります。この構成が優れている点は、全体的な機能への影響を抑えながら、精度の高い防御が可能になることです。しかし、考えられる攻撃シナリオをすべて理解し、設定する必要があるため、現実的ではありません。

攻撃シナリオを詳細に理解することなく、広範な防御機能を獲得するために、ETASはハイパーバイザーとそのネットワーク構成(ファイアウォールも含む)を制御できる、クロスドメインセキュリティマネージャー(CDS)を導入しています。CDSは、攻撃が発生した場合に、VM3を再起動できます。攻撃者がそれ以上攻撃を続けられない場合(つまりセキュアブートをバイパスできない場合)、攻撃者を排除できます。同じ攻撃が簡単に繰り返されるのを防ぐため、VMの再起動後にテレマティクスサービスを無効にできます。これにより、ハイパーバイザーレベルで攻撃に対処できるようになります。

さらに、CDSはテレマティクスサービスの外部向けのネットワークポートもブロックできます。攻撃を受けたサービスがわかっている場合は、この設定によってネットワークレベルで攻撃に対応できます。

このシナリオでは、VM3上の任意のアプリから攻撃が実行されたと想定しています。図4に示されているように、適切なセキュリティ対策が取られていない場合、この攻撃によって大量のリクエストがHSMに殺到し、システム全体が機能不全に陥って隣接するVM上の車両機能にも影響が及ぶ可能性があります。このフレームワークでは、IDSが侵入を検知し、セキュリティドメインが多層的に対処するため、ビークルコンピューターの機能が維持されます。理想的なケースでは、ドライバーは攻撃にまったく気付かないか、わずかな影響を感じる程度です。

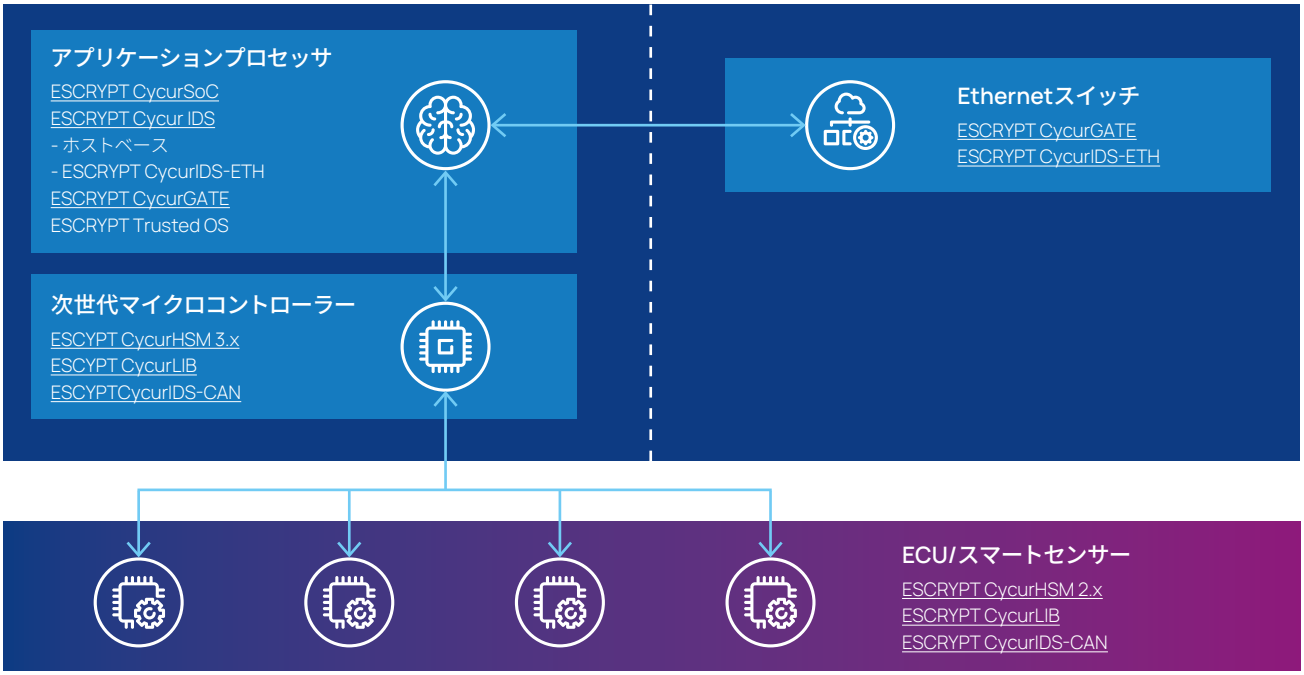
図5のとおり、攻撃の最中もセーフティ VMは影響を受けずに、車両の機能を維持できます。このようにドメインを分離したフレームワークは、攻撃時に多層的な防御が可能になります。さらに安全性に関する機能を中心に、可能な限り多くの機能を維持できるように設計されています。1つのドメインしかないシステムとは対照的に、攻撃を受けたアプリケーションを切り離したり、フォールバックによって機能を回復させたりすることができます。

8. まとめ

セキュリティは、急速に進化する自動車業界において最も重要な課題です。ETASが提案する「自動車クロスドメインセキュリティ」フレームワークは、さまざまな業界の知見を活用し、安全性やセキュリティを損なうことなく柔軟性を確保することで、ビークルコンピューターを保護する堅牢なアプローチを可能にします。このアプローチでは、仮想化によって複雑なシステムを複数のユニットに分離するという、エンタープライズ／クラウドネットワークで確立されたベストプラクティスを自動車システムに適用しています。このアプローチが特に優れているのは、将来的にゼロトラストプラットフォームをビークルコンピューターに実装し、自動車セキュリティを大きく進化させる可能性がある点です。これにより、自動車メーカーはあらゆる脅威に耐える安全な車両アーキテクチャを開発し、すべての道路利用者の安全を最大限に高めるという未来に向けて前進することができます。

ESCRYPTビークルコンピューターセキュリティスイート

ESCRYPTビークルコンピューターセキュリティスイートは、クロスドメインアプローチの基盤を構築できる包括的な製品です。特定のOS向けのプラグアンドプレイパッケージと、すぐに使えるセキュリティセンサーを備えており、簡単に導入できます。ETASのIDPSモジュールと任意のソースまたはネイティブアプリケーションを接続することで、カスタマイズも可能です。将来を見据えたポートフォリオの全体像をご覧ください。



参考文献

1) National Cyber Security Centre（英国国家サイバーセキュリティセンター：NCSC）、「Security principles for cross domain solutions（クロスドメインソリューションのセキュリティ原則）」、https://www.ncsc.gov.uk/collection/cross-domain-solutions（アクセス日：2025年2月7日）
2) James E. Smith、Ravi Nair、「Virtual machines – versatile platforms for systems and processes（仮想マシン – システムとプロセスのための多目的プラットフォーム）」、Elsevier社、2005年
3) Busch, Marcel、「On the Security of ARM TrustZone-Based（Arm TrustZoneベースのセキュリティについて）」、Dissertation at University Erlangen-Nürnberg（エアランゲン／ニュルンベルク大学における博士論文）、2020年

ETASについて

ETAS GmbHは、1994年にボッシュ・グループの完全子会社として設立されました。現在では欧州、北米、南米、アジアの各国に拠点を構え、グローバルに事業を展開しています。

ETASは、ソフトウェアデファインドビークル（SDV）の実現に向け、ソフトウェア開発ソリューション、車両オペレーティングシステム（OS）、自動車用クラウドサービス、データ収集・処理ソリューション、顧客向け統合ソリューション、サイバーセキュリティといった分野で包括的なソリューションを提供しています。

自動車サイバーセキュリティの分野では、業界のパイオニアとして各種オンボードおよびオフボードソフトウェア製品を取り揃えているほか、お客様がサイバーセキュリティ関連の複雑さをコントロールし、サイバーリスクを軽減し、ビジネスの可能性を最大限に引き出すためのプロフェッショナルサービスも提供しています。

ETASの自動車セキュリティソリューションは、すでに世界中の何百万台もの車両システムに導入され、ソフトウェアデファインドビークルのサイバーセキュリティ標準を確立しています。

お問い合わせ先

Tobias Klein
tobias.klein@etas.com
www.etas.com/we-secure-the-future

Dr. Max Hoffmann
max.hoffmann@etas.com
www.etas.com/we-secure-the-future

本書に記載されているすべての情報は一般的性質のものであり、特定の個人または団体の状況に対処することを意図したものではありません。当社は正確かつ最新の情報の提供に努めていますが、そのような情報を取得した時点での正確性や将来における継続的な正確性を保証することはできません。本書の情報に基づいて行動する場合は、専門家の適切な助言を受け、対象となる状況の事実を十分に調査してください。
© ETAS GmbH. All rights reserved.

最終更新：2025年2月