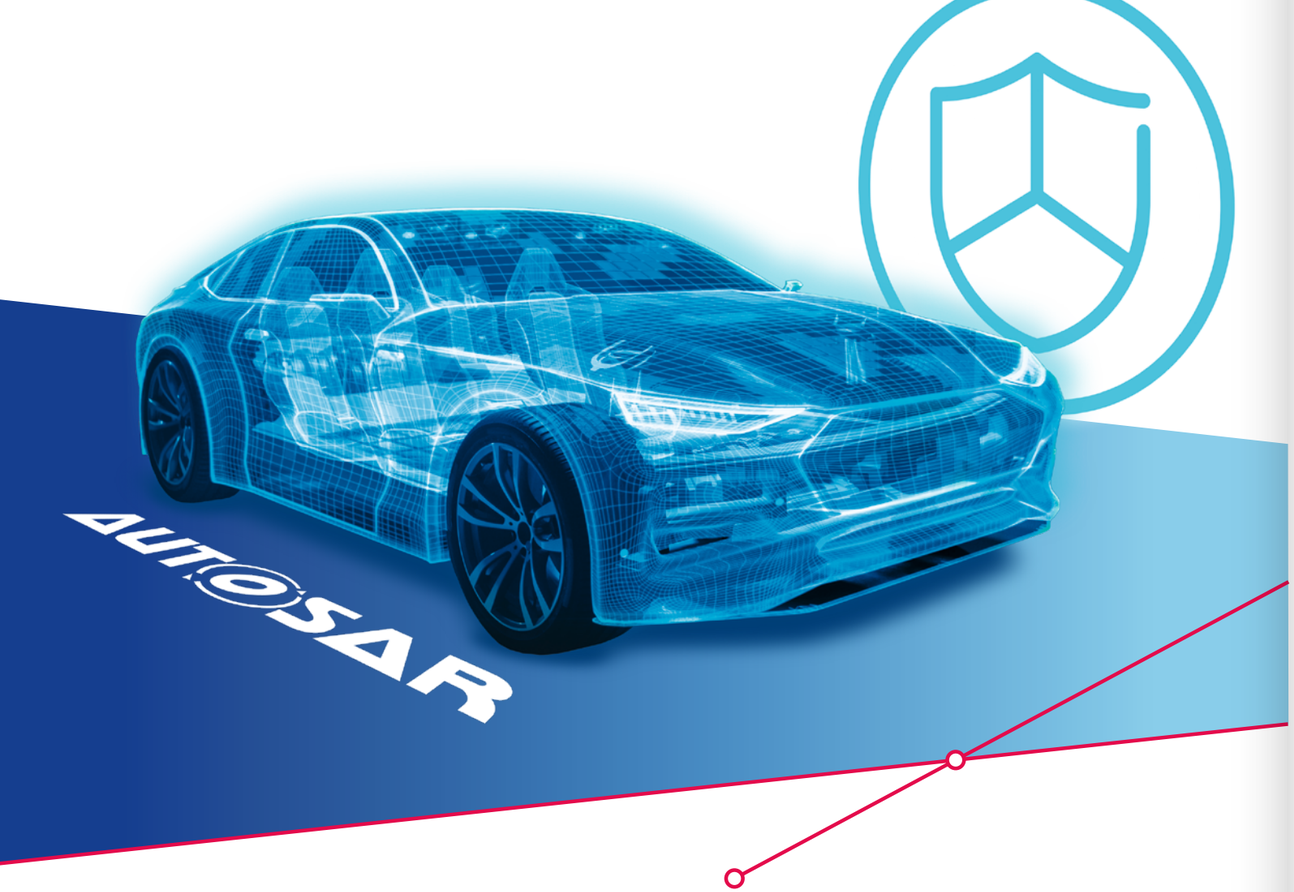


サイバーセキュリティ対策も万全

AUTOSAR Adaptive アーキテクチャのセキュリティ

AUTOSAR Adaptive はインテリジェントなコネクテッドカーの実現を可能にします。この規格のひとつに、サイバー攻撃を確実に防ぐことを目的としたセキュリティ機能があります。この機能を今から組み入れることで、未来の E/E アーキテクチャを実現することができるのです。

高度に自動化された自動運転コネクテッドカーの時代に突入した現在、シグナルベースの通信と機能ごとに分割した ECU とで構成される E/E アーキテクチャは、限界を迎えようとしています。自律性とコネクティビティが強く求められる中、E/E アーキテクチャは機能が集約された高性能ビークルコンピュータ（VC）およびドメインコントローラ（DCU）に制御を行わせ、センサ／アクチュエータ用 ECU が単にコマンドを実行するという形にシフトしています。

この新しい E/E アーキテクチャにフレームワークを提供するのが、AUTOSAR Adaptive のプラットフォームです。このフレームワークではアプリケーションソフトウェアを動的に実行することができ、AUTOSAR Runtime for Adaptive Applications（ARA）を利用して、Linux などの POSIX オペレーティングシステムにインターフェースすることが可能になります（図 1）。さまざまなベンダーによる、ASIL カテゴリーが異なるソフトウェアを安全に VC 上で稼動させるための手段として、事前に構成が設定されたハイパーバイザによるパーティショニングが行われます。

サイバーセキュリティ管理

最新鋭のコネクテッドカーは個別のセキュリティ対策では守ることができません。必要なのは、車両アーキテクチャ全体のリスク分析に基づいた「統合されたセキュリティ」という考え方です。この概念は、各コンポーネントのセキュリティ要件、ECU のセキュリティ要件、および ECU の論理パーティションのセキュリティ要件の 3 つに分けて考えなくてはなりません。そこで AUTOSAR Adaptive には、さまざまなセキュリティ機能を統合した 1 つの基本セットが記述されています。開発者はこの基本セットを用いることで、自動運転コネクテッドカーシステムの、絶えず変化する量的・質的な保護要件に対応することができるのです。分散型のソフトウェアベースの E/E アーキテクチャの場合、リアルタイム条件下でのデータ負荷が非常に大きくなるため、セキュリティ対策においても、より高いパフォーマンスが要求されます。そのため、AUTOSAR Adaptive には以下に挙げるようなセキュリティ機能が組み込まれています（図 2）。

「重要コンポーネント」としての暗号化機能

セキュリティの使用事例の多くは暗号プリミティブに依存しています。例えば重要データを暗号化する、ソフトウェア更新時に署名を検証するといった場面が考えられます。その際に必要な暗号鍵と証明書は安全な場所に保管し、権限のあるアプリケーションで管理しておかなくてはならず、場合によっては複数の ECU 間で同期させておく必要もあります。AUTOSAR Adaptive では、これらのプリミティブは暗号化ファンクションクラスタ（暗号 API ともいう）を通して提供されます。これには提供されたインターフェースを抽象化する機能があるため、ソフトウェア全体としての移植性が高くなります。

データのやりとりを安全に行えるよう、AUTOSAR Adaptive はイーサネットを介した TCP/IP 通信などの最新規格に準拠しています。また、TLS と IPSec という、IT の世界で実績のあるプロトコルを採用することにより、不正な操作や窃取をシャットアウトする安全な通信チャンネルを、車両内部の通信や外部インスタンスとの通信用に確立することができます。

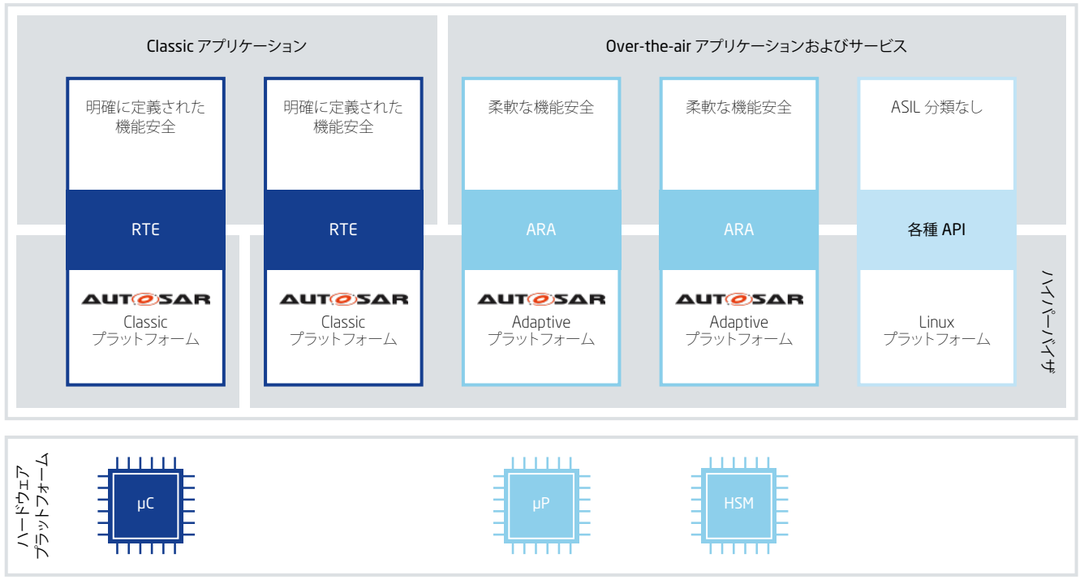
AUTOSAR Adaptive は不揮発性メモリ、通信チャンネル、暗号鍵などのシステムリソースへのアクセスを管理します。AUTOSAR Identity & Access Management モジュールは、明示的に権限を許可されたアプリケーションだけに各リソースへのアクセスを許す、いわば門番の働きをします。アクセス権を必要に応じて設定でき、随時更新することもできます。

セキュアアップデート（安全な更新）とトラステッドプラットフォーム（信頼できるプラットフォーム）

AUTOSAR Adaptive のセキュアアップデート機能は、例えば IDS（Intrusion Detection System：侵入検知システム）などによって検出された脆弱性を修正するために役立つもので、個々のアプリケーションや、時にはプラットフォーム全体のセキュリティに関わる更新データを受信し、処理します。1 つ 1 つの更新用データ（Blob）にはバックエンドによる署名が付されているため、信頼する配信元から送られてきた更新データのみが実行されます。

更新データだけでなく、ECU 用および VC 用のアプリケーションの検証も定期的に行わなければなりません。そのために AUTOSAR Adaptive ではセキュアブート、あるいはトラステッドプラットフォーム機能というものが使われます。トラステッドプラットフォームはトラストアンカーとして、すべてのアプリ

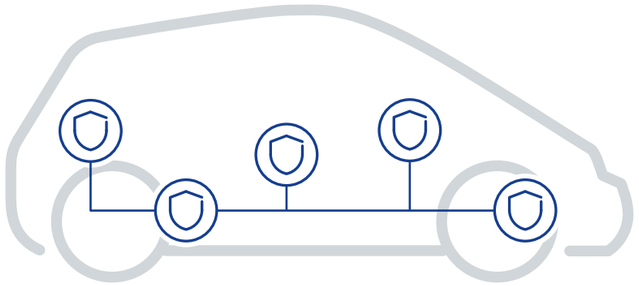
図 1：AUTOSAR Classic が静的なリアルタイム要件のシステムを対象とするのに対し、AUTOSAR Adaptive は動的アプリケーションを扱うという点で区別されます。



RTE = ランタイム環境
µC = マイクロコントローラ

ARA = AUTOSAR Runtime for Adaptive Applications
µP = マイクロプロセッサ

API = Application Programming Interface
HSM = Hardware Security Module



AUTOSAR Adaptive のセキュリティコンポーネント

- **暗号スタック**（キーマテリアル管理、暗号プリミティブへのアクセス管理）
- 実績ある TLS ／ IPSec プロトコルを介した**セキュアな通信**
- 重要リソースに対する**アクセス保護**（例：Identity and Access Management モジュールによる鍵の保護）
- 個々のアプリケーションからプラットフォーム全体まで、すべてを対象とする**セキュアアップデート**
- 「トラステッドプラットフォーム」の一部であるセキュアブートの連続したトラストチェーンで**認証されたアプリケーション**

図 2：AUTOSAR Adaptive のセントラルセキュリティコンポーネント

ケーションを検証し、プラットフォーム自体の検証までも行います。起動からプラットフォーム、アプリケーションまでを含めたトラストチェーンが維持されることで、信頼できるソフトウェアだけが実行されます。

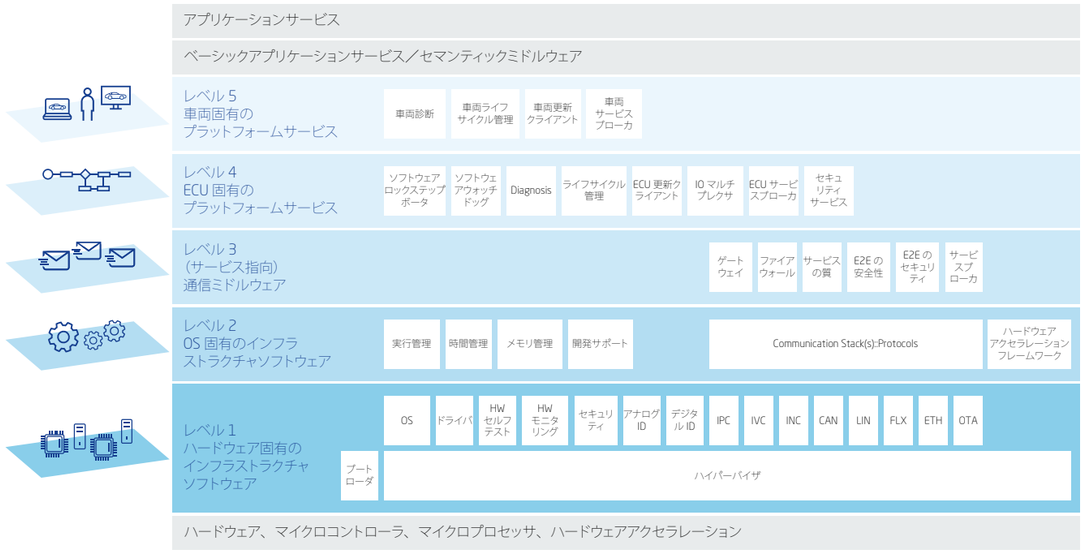
RTA-VRTE：AUTOSAR Adaptive のためのプラットフォームソフトウェアフレームワーク

未来の AUTOSAR Adaptive ユーザーにとって、今日の新しいアーキテクチャに精通しているかどうかは非常に重要な意味を持ちます。Vehicle Runtime Environment（RTA-VRTE）のプラットフォームソフトウェアフレームワークは、セキュリティ機能の統合・実装をはじめとする、ありとあらゆる AUTOSAR Adaptive 準拠プロセスの理想的な基盤となります。

RTA-VRTE には、マイクロプロセッサベースのビークルコンピュータを実現するための重要なミドルウェア要素のすべてが揃っています。このプラットフォームソフトウェアフレームワークを使用すれば、仮想 ECU の機能を普通のデスクトップパソコン上でシミュレートし、イーサネットを介してネットワークに送信することが可能になります。RTA-VRTE は、4 層の基本のソフトウェアアーキテクチャからなる仮想マシンを作成します。そして 5 層目には車両固有のプラットフォームサービスが搭載されます（図 3）。

レベル 1 とレベル 2 には、使用するハードウェアのためのインフラストラクチャソフトウェア（デバイスドライバなど）と POSIX 互換のオペレーティングシステムがあります。レベル 2 には、AUTOSAR Adaptive 規格に由来するプラットフォーム固有の要素もあります ー その筆頭が実行管理（execution management）で、これは動的に割り当てられたアプリケーションが適切に起動・終了するよう管理し、リソースの割り当てと実行時間が守られているかを監視します。つまり実行管理は信頼できるプラットフォームを提供し、Adaptive アプリケーションの完全性と真正性を検証するという意味で、IT セキュリティにおける重要機能の 1 つです。これによって不正な操作や損

図 3：RTA-VRTE の 5 層モデルは VC 用ソフトウェアの重要な機能と要件を支援します。



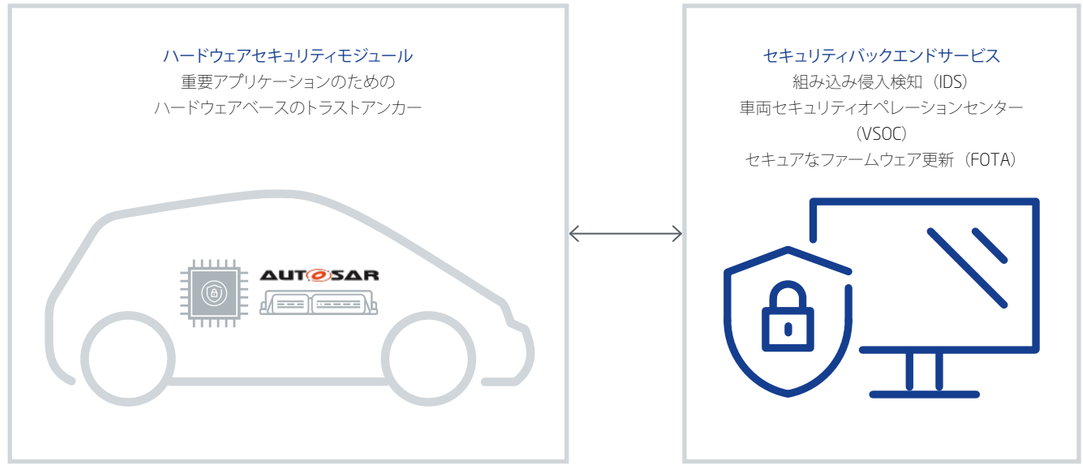


図 4：自動車の組み込みサイバーセキュリティ：マイクロコントローラにおけるトラストアンカーとしてのハードウェアセキュリティモジュールと、車両のライフサイクル全体にわたるセキュリティ監視

傷を事前に検知することができます。

さらに、レベル 3 の通信ミドルウェアは、動的で柔軟な Adaptive アプリケーションやその他のソフトウェアアプリケーションのシステムへの統合を保証します。
通信管理（communication management）は RTA-VRTE の中核的なコンポーネントとして、レベル間のインタラクションを管理／制御するものであり、レベル 4、5 の ECU および車両に依存するプラットフォームサービスを含む、カプセル化されたソフトウェアのスムーズな動作を保証します。この機能はまた、認証済みアプリケーションが提供するサービス間のエンドツーエンド通信を保護する、サイバーセキュリティ上重要な役割を担っています。

RTA-VRTE の通信管理はレベル 4 の ECU 固有サービス群とともに、車載アプリケーション用の汎用フレームワークをアプリケーション開発者に提供します。レベル 4 にはセキュリティ保護のための更新／構成マネージャ（update and configuration manager：UCM）もあり、各アプリケーションの認証済みアップデートの実行を支援し、プラットフォーム全体にわたってアップデートの調整を行います。RTA-VRTE のレベル 5 では、AUTOSAR++ のアスペクトによって車両全体、さらにはフリート全体の機能が統合され、堅牢な無線通信（over-the-air：OTA）による RTA-VRTE AUTOSAR Adaptive アプリケーションセットのアップデートが可能になります。

展望：AUTOSAR Adaptive の先にある包括的セキュリティ

2020 年には世界中で、AUTOSAR Adaptive 車載プラットフォームを採用することを目指すプロジェクトに、RTA-VRTE が使われ始めています。また、ETAS と ESCRYPT が提供する Early Access Program（EAP）により、自動車メーカーやサプライヤによる次世代のハイブリッド E/E アーキテクチャの開発手法を確立することが可能になり、すでに AUTOSAR Adaptive を通じて利用可能なセキュリティコンポーネントをも実装できるようになりました。

それらのセキュリティモジュールを備えた上で、さらに必要とされているのは、真に包括的な自動運転コネクテッドカー向けサイバーセキュリティの概念です。まず、トラストアンカーとしてのハードウェアセキュリティモジュール（HSM）による暗号鍵マテリアルのカプセル化を、VC マイクロコントローラまたは ECU 上で物理的に可能にします。次に、それをフリート全体に拡大して全ライフサイクルにわたって車両を保護するとともに、車載型の攻撃検知、バックエンドの車両セキュリティオペレーションセンター（VSOC）、無線通信によるファームウェア（Firmware Over-The-Air：FOTA）セキュリティ更新を実装します。

開発者は RTA-VRTE のプラットフォームソフトウェアフレームワークを用いて、AUTOSAR Adaptive ベースの E/E アーキテクチャに仮想環境で生命を吹き込むことが可能になります。そうすることで、サイバー攻撃に対する包括的な防御の基盤が拡張されます。未来の車両においては、防御の基盤をマイクロコントローラから車載ネットワークへ、そしてライフサイクル全体にわたるフリート単位のモニタリングへと拡大していかなければなりません。

執筆者

Dr. Michael Peter Schneider、ESCRYPT
AUTOSAR Security プロジェクトマネージャ
Dr. Stuart Mitchell、ETAS GmbH
RTA-VRTE 担当シニアプロダクトマネージャ