Virtual ECUs in Production Vehicles?

量産車に仮想 ECU を搭載？

執筆者

Michael Hauser 氏
Bosch Automotive Electronics
（シュトゥットガルト）
ソフトウェア開発チーム リーダー

Dr. James Dickie
ETAS Ltd
（英国、ヨーク）
RTA ソリューションズプロダクトマネージャ

Dr. Nigel Tracey
ETAS Ltd
（英国、ヨーク）
統括マネージャ

ETAS Lightweight Hypervisor による柔軟性、高効率性、セキュリティ対策の実現

「アジャイルソフトウェア開発」は、自動車産業界において採用が増えている開発手法です。この手法は「安全性やセキュリティ対策を気にせずに、ユーザーがソフトウェア制御式の車両ファンクションのアップグレードや更新を行える」という発想に基づきますが、これはソフトウェアファンクション同士が厳重に分離されていることが前提となります。しかしハードウェアの傾向はこれに反し、中心的な複数の ECU においてますます多くのファンクションが実行されるようになってきています。このギャップを解決するため、Bosch Automotive Electronics は ETAS の新しい軽量ハイパーバイザを採用しました。

免許取得から 3 年、無事故で安全運転を続けた Leon に、ついにその日がやってきました。両親は彼の車のメーカーのウェブサイトにログオンし、免許取得時にオンに設定してあったソフトウェア制御式パワーリミッタをオフにします。同時に、Leon が欲しがっていた新しいマルチメディアパッケージのインストールも行います。この費用は彼も半分負担します。

車両の納品後にこのようなファンクションアップグレードを行い、無線通信経由（OTA: over-the-air）で継続的な更新が行えるようにするには、その影響が他のソフトウェアに及ばないことが前提条件となりますが、これまで以上にコネクテッド化された多くのファンクションが複数の中心的 ECU に集中する傾向にある今日、それを保証する手段はあるでしょうか。さらに、アップグレードや更新を行った後にシステム全体の機能安全を走行前に検証することはできるのでしょうか。この 2 つの質問は、ソフトウェアファンクション間の確実な分離が非常に重要であることを示しています。

実質的なパーティショニングが必要

このような「分離」が支持される理由は、機能安全以外にもあります。厳密に分割されていれば、たとえば複数のメーカーのソフトウェアが同一 ECU 上で実行される場合に、開発時のワークフローを単純化することができます。またファンクションの分離によって ECU への攻撃が難しくなるため、サイバー犯罪が増加している現代では重要なファクタであると言えます。あるファンクションにハッカーがアクセスすると、その行く手にハイパーバイザが高いハードルを配置し、

最大の損害を与えようとするサイバー犯罪者の意欲を強力に抑止します。「分離」はさまざまな手法で実現することができます。まずはソフトウェアファンクションをそれぞれ専用の制御ハードウェアに厳密に割り振ることが考えられますが、それではハードウェアのコストとシステムの複雑性が桁違いに増大してしまいます。より現実的な手法として、「パーティショニング」と「分離」のコンセプトが定義されている AUTOSAR ベースのアーキテクチャがあります。これにより、他のファンクションに影響を与えずに個々のファンクションをアップグレードすることが可能になります。この手法では、1 つのファンクションが修正されるたびに同じ ECU 上のソフトウェア全体を包括的に再検証する必要がなくなります。ただしこの AUTOSAR のコンセプトを実装するにはアドオンが必要です。

ハイパーバイザが提供する解決策

ここでハイパーバイザによる効果的な解決策をご紹介します。ハイパーバイザは 1 つの ECU を複数の仮想マシン（VM: Virtual Machine）に分割します。実際には複数のファンクションが同じ ECU 上で実行されるのですが、ソフトウェアは各ファンクションに専用のハードウェアが割り振られていることを認識しています。ファンクション同士は非常に厳密に分離されているので、個別に修正でき、修正後にシステム全体を再検証する必要はありません。またソフトウェアサプライヤは、ECU の開発時において他のどのサプライヤとも無関係に作業することができます。ソフトウェアエラーや悪質な侵入者が出現しても、1 つの仮想マシン上に局所的に封じ込めるため、拡散することはありません。また、最低レベル（QM）から最高レベル（ASIL D）までのさまざまな ASIL（Automotive Safety Integrity Level: 安全性要求レベル）のソフトウェアを 1 つの ECU 上で動作させることが可能になります。
ただし、ハイパーバイザソリューションのすべての長所をうまく生かせるかどうかは、その実装方法に依存します。このソリューションを実際の車載環境に適合させないと、不具合が生じる可能性があります。たとえば、アクセス許可を制御するには、通常はハイパーバイザ専用のメモリ管理とハイパーバイザ特権モードが必要です。従来のバージョンでは 3 段階の特権モード（ハイパーバイザ自身、基本ソフトウェア、適合ファンクション）があります。しかし一般的な車載マイクロコントローラはこれらのメモリ管理や 3 段階の特権モードに対応していないため、今日までハイパーバイザテクノロジーが車載システムで幅広く使用されることはありませんでした。

ある大規模 OEM 向けのプロジェクトにおいて Bosch Automotive Electronics – Body Electronics（AE-BE）は、ETAS の軽量ハイパーバイザ（ETAS RTA-LWHVR）と共にようやくこの問題を解消することができました。最適化により、自動車用ハイパーバイザのメモリ使用量が 5 キロバイト（kB）に抑えられただけでなく、アクセスタイムも 4 ～ 5 倍改善されました。そしてこの新しいソリューションは、仮想マシン間の影響をなくしました。このプロジェクトでは、中心的なボディ ECU が 11 個の仮想マシンに分割され、各仮想マシンがそれぞれ異なるサプライヤのソフトウェア用に確保されました。ASIL の等級範囲は QM ～ B です。

AUTOSAR を超える軽量ハイパーバイザ

システムには多種多様なソフトウェアファンクションが数多く存在していましたが、軽量ハイパーバイザがそれらをカプセル化し、すべて問題なく機能しています。仮想マシンが共有メモリにアクセスしても、そのアクセスとランタイムがコア上で明確に制御されるのです。

このソリューションでは、コンピュータコアを 1 つのマスタコアと複数のアプリケーションコアに分割することで高性能を実現しています。マスタコアに与えられるジョブとしては、ハードウェア管理や、中央の基本ソフトウェアと各種のソフトウェアアプリケーションの実行があり、各アプリケーションコアには厳密に分離された複数の仮想マシンが展開されます（図 1 参照）。各仮想マシンは、パーティション化された AUTOSAR ランタイム環境（RTE）または AUTOSAR 非準拠のソフトウェアで構成され、これらすべてが 1 つの ECU 上で実行されます。このアプローチにおいては Bosch AE-BE が開発したコア間通信（ICC）が重要な役割を果たします。どのような状況においても実行時間が保証されるだけでなく、各ファンクションは、他のファンクションの実行を抑制することなくタイムバジェットを追加要求することができ（図 2 を参照）、リアルタイム要件は常に保証されます。
高度なランタイム要件により仮想マシンの能力を超える負荷が発生する恐れが生じると、仮想マシンはハイパーバイザに対して、予備のランタイムウィンドウに一時的にアクセスしてよいかを尋ねる場合があります。するとハイパーバイザは、予備のランタイムウィンドウが利用可能になるのを待つためのキューにその仮想マシンを追加します。そしてランタイムウィンドウが解放されると、ハイパーバイザはキューに最初に入れた仮想マシンにそのウィンドウの使用を許可し、システムの高負荷による影響を最小限に抑えます。ただし、不正な仮想マシンがシステムの支配権を得ようとするのを防ぐため、各仮想マシンは 1 つの予備ウィンドウの使用しか要求できません。

今日から使える未来型ソリューション

標準的なハイパーバイザに比べて、メモリオーバーヘッドはわずか 5 kB に低減し、電力消費もコアの使用可能容量の 5 パーセントに抑えられました。このような改良により、RTA-LWHVR は車載組み込みシステムの境界条件に難なく適合することができます。柔軟性に富んでいるため、広範なアプリケーションに対応でき、数多くのマイクロコントローラに実装することができます。また高性能かつ高信頼性のパーティショニング技術で ECU を分割するので、今後は、さまざまなメーカーやさまざまな安全等級のソフトウェアを同一の ECU 上で稼働させ

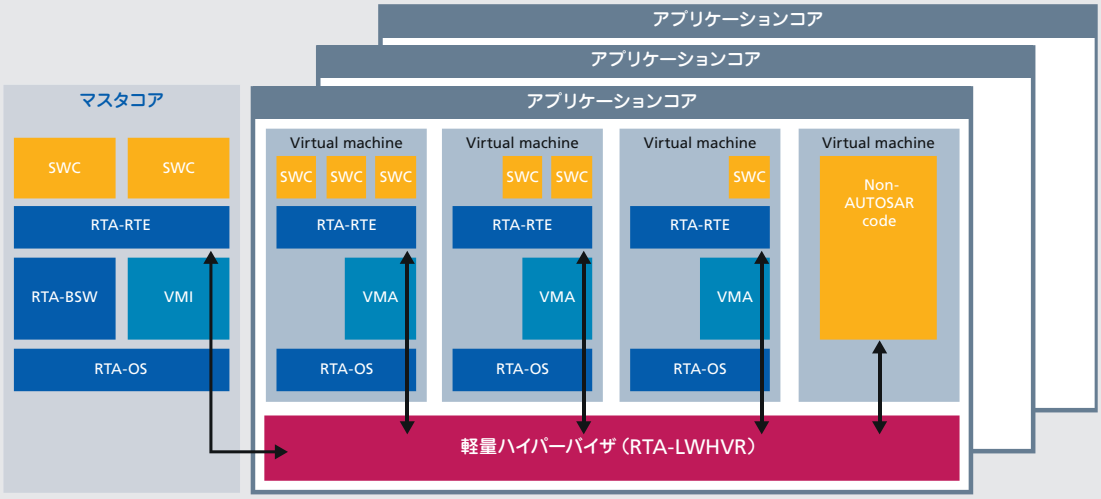
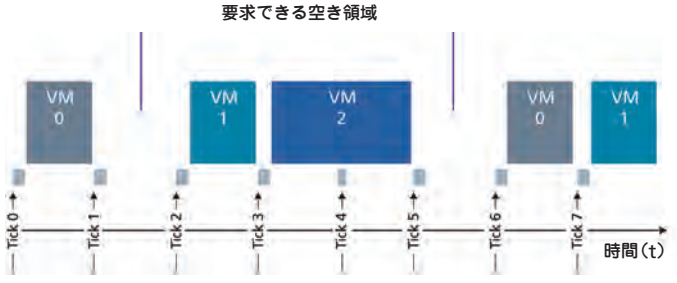


図 1:
軽量ハイパーバイザ RTA-LWHVR が展開された ECU の図

RTA-BSW AUTOSAR基本ソフトウェア
RTA-OS オペレーティングシステム
RTA-RTE ランタイム環境
SWC セキュアアプリケーションのソフトウェアコンポーネント
VMA 仮想マシンアダプタ
VMI 仮想マシンインターフェース
→ コア間通信（ICC）

VM 仮想マシン



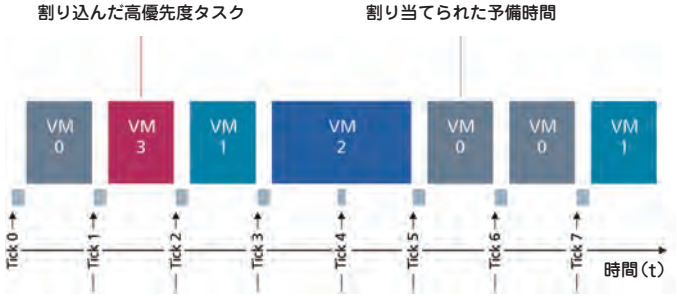


図 2:
アプリケーションコア内の時間管理

ることができるようになります。

インテリジェントなコア間通信と厳密なカプセル化により、ソフトウェアで制御する複数のファンクションを互いに影響されずに開発することができます。既存車両のファンクションも含めた修正も容易に行え、時間のかかるシステム全体の再検証を行う必要がなくなります。このように軽量ハイパーバイザは、自動車産業界においてソフトウェアとファンクションのアジャイル開発を行うためのセキュアな基礎を構築するので、定期的なセキュリティ更新を行う動的セキュリティシステムも容易に実現できます。そして、Leon と彼の両親が利用したような車両の設定変更やアップグレードを実現すること阻むあらゆる障害を取り除くことも可能になるのです。