생산 차량에서의 가상 ECU?

저자

마이클 하우저 (Michael Hauser),
슈투트가르트 보쉬 자동차 전장 사업부 소프트웨어 개발 팀장

제임스 디키 (James Dickie)
박사,
이타스 영국 RTA 솔루션 프로덕트 매니저

나이젤 트레이시 (Nigel Tracey)
박사,
이타스 영국 사장

유연성, 효율성, 안전성을 보장하는 이타스 경량 하이퍼바이저

애자일 소프트웨어 개발은 자동차 산업에서 증가하는 추세입니다. 이는 사용자가 안전 또는 보안 문제없이 소프트웨어 제어 차량의 기능을 업그레이드하고 업데이트할 수 있어야 한다는 아이디어에서 비롯되었습니다. 이 개발은 개별 소프트웨어 기능 간의 철저한 분리를 전제로 합니다. 그러나 하드웨어의 경우 소프트웨어와는 달리 점점 더 많은 기능이 중앙 ECU에서 실행되고 있습니다. 이러한 모순을 해결하기 위해 보쉬 자동차 전장 사업부는 이타스의 새로운 경량 하이퍼바이저를 사용하고 있습니다.

3년간의 무사고 후, 레옹의 부모는 OEM 웹사이트에 로그인하여 운전 면허증을 받았을 때 활성화되었던 소프트웨어 제어 전원 리미터를 마침내 제거합니다. 또한 그들은 레옹이 원하고, 그들이 비용의 절반을 지불하는 새로운 멀티미디어 패키지를 설치합니다.

최근 진행되는 기능 업그레이드 및 지속되는 over-the-air 업데이트의 전제 조건은 변화가 다른 소프트웨어에 영향을 주지 않아야 한다는 것입니다. 그러나 요즘 조금의 중앙 ECU에 더 많은 연결 기능을 집중시키는 추세라면 이를 어떻게 보장할 수 있을까요? 또한 그런 환경에서 업그레이드 및 업데이트 후 테스트를 통해 전체 시스템의 기능적 안전성을 사전에 검증하고 확인하는 것이 가능할까요? 이 두 가지 질문은 소프트웨어 기능을 서로 안전하게 분리하는 것이 얼마나 중요한지를 보여줍니다.

파티셔닝(partitioning)의 필요성

기능적 안전성 이외의 다른 이유도 파티셔닝의 필요성을 환기합니다. 예를 들자면 파티셔닝은 각기 다른 제조업체의 소프트웨어가 단일 ECU에서 실행될 때 개발 작업과정을 간소화합니다. 이외에도 파티셔닝은 지금과 같이 사이버 범죄가 증가하는 시대에 ECU를 공격하기 어렵게 합니다. 만약 해커가 어떤 기능에 액세스하려고 한다면 하이퍼바이저는 추가적인 제재를 통해 사이버 범죄자들이

막대한 피해를 주지 못하도록 방지하기 때문입니다.
이 파티셔닝을 가능하게 만드는 방법은 다양합니다. 예를 들어 소프트웨어 기능들을 각각 자체 제어 하드웨어에 할당할 수 있습니다. 그러나 이 방법에 필요한 하드웨어와 시스템 복잡성은 굉장히 큰 비용을 필요로 합니다. 따라서 파티셔닝 및 분리 개념을 정의한 AUTOSAR 기반 아키텍처가 보다 현실적인 옵션이 될 수 있습니다. 이를 바탕으로 개별 기능을 업그레이드하는 동시에 다른 기능이 손상되지 않도록 할 수 있기 때문입니다. 이렇게 하면 한 기능을 수정해도 문제가 되는 ECU의 모든 소프트웨어를 총체적으로 재확인할 필요가 없어집니다. 그러나 AUTOSAR 개념을 구현하려면 추가 기능이 필요합니다.

하이퍼바이저는 어떤 방법으로 솔루션을 제공할까요?

하이퍼바이저는 개별 ECU를 다양한 가상머신(VM, Virtual Machine)으로 나누어 효과적인 솔루션을 제공합니다. 다양한 기능들이 실질적으로 같은 ECU에서 실행되더라도, 개별 소프트웨어의 각 기능이 할당 받은 공유 리소스 접속 시간 안에서 실행됩니다. 각 기능은 완전히 재검증하지 않고도 개별적으로 수정할 수 있도록 매우 엄격하게 분리되어 있으며 다양한 제조업체는 ECU 개발 중에도 다른 제조업체와 독립적으로 작업할 수 있습니다. 소프트웨어 오류나 악의를 지닌 해커는 단일 가상 시스템에 로컬로 포함되어 확산하지 않습니다. 또한 단일 ECU에서 최저 수준(QM)부터 최고 수준(ASIL D)까지 다양한 자동차 안전 무결성 수준(ASIL, Automotive Safety Integrity Level)을 사용하여 소프트웨어를 작동시킬 수 있습니다.

그러나 이런 장점들로 인해 하이퍼바이저 솔루션의 성공 여부는 구현방식에 따라 달라집니다. 솔루션을 차량의 특정 환경에 맞게 조정하지 않으면 문제가 발생할 수 있습니다. 예를 들어 하이퍼바이저는 대개 자체 메모리 관리는 물론 액세스 권한을 제어하는 하이퍼바이저 관리자 모드가 필요합니다. 클래식 버전에는 하이퍼바이저 자체, 기본 소프트웨어 그리고 캘리브레이션 기능의 3단계가 있습니다. 그러나 오늘날 많이 쓰이지만, 지금까지 차량의 하이퍼바이저 기술 확산을 지연시킨 차량용 마이크로 컨트롤러는 해당 메모리 관리 및 3단계 권한 모드를 지원하지 않습니다.

대형 OEM의 프로젝트에서 보쉬 AE-BE(Bosch Automotive Electronics - Body Electronics)는 이제 이타스 경량 하이퍼바이저(ETAS RTA-LWHVR)로 이러한 까다로운 문제를 해결할 수 있습니다. 최적화된 자동차 하이퍼바이저의 메모리 용량 요구량을 5킬로바이트(kB)로 줄이는 것뿐만 아니라 액세스 시간도 4배에서 5배까지 향상되었습니다. 이 새로운 솔루션은 가상머신 간에 영향이 없도록 합니다. 특정 프로젝트에서 중앙 ECU는 11개의 가상머신으로 분할되었으며, 각 가상머신은 모두 다른 공급 업체의 소프트웨어용으로 마련되었습니다. ASIL 등급은 QM에서 B까지 다양합니다.

AUTOSAR를 능가하는 경량 하이퍼바이저

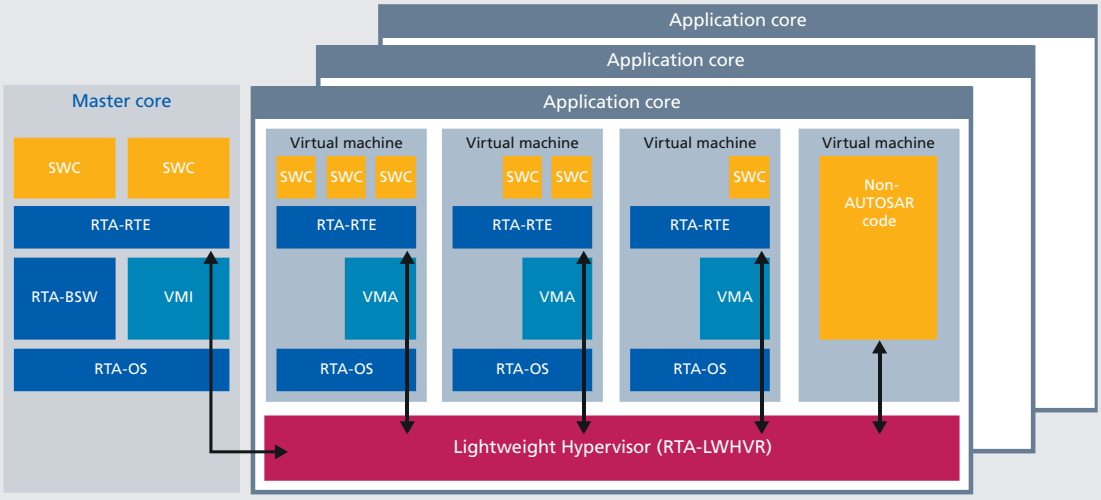
소프트웨어 기능의 양과 이질성에도 불구하고 가상머신에 탑재된 소프트웨어들은 경량 하이퍼바이저로 캡슐화될 때 아무 문제없이 작동했습니다. 이 성공은 가상머신이 공유 메모리에 액세스하더라도 액세스 및 런타임이 코어에서 명확하게 제어되기 때문에 가능했습니다.

이 솔루션의 높은 성능은 컴퓨터 코어를 마스터 코어 및 다양한 애플리케이션 코어로 나누었기 때문에 가능합니다. 마스터 코어가 하드웨어 관리, 중앙 집중화된 BSW의 운영 및 일부 소프트웨어 애플리케이션의 작업을 담당한다면, 애플리케이션 코어는 엄밀히 분리된 가상 시스템(그림1 참조)을 포함합니다. 이때 애플리케이션 코어는 선택적으로 AUTOSAR 당 파티션된 런타임 환경(RTE) 또는 AUTOSAR 비 호환 소프트웨어를 갖춥니다. 그리고 이 모든 것은 단일 ECU에서 이루어집니다. 이 방법을 사용할 시 보쉬 AE-BE가 개발한 해당 코어 간 통신(Inter-Core Communication, ICC)이 중요한 요소가 됩니다. 모든 상황에서 보장되는 실행시간 외에도 기능들은 다른 기능의 실행을 줄이지 않고도 추후 추가적인 시간 분배를 필요로 할 수 있습니다(그림2 참조). 따라서 실시간 요구 사항은 항상 보장됩니다.

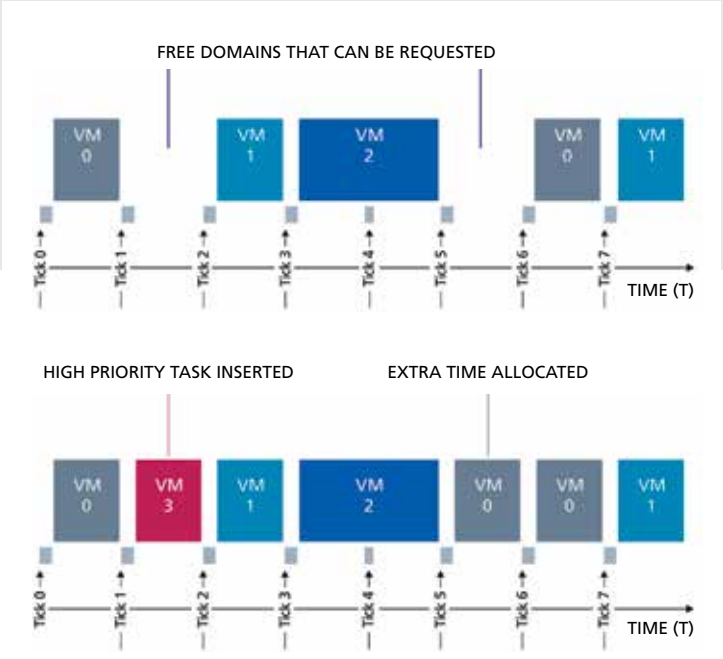
높은 런타임 요구량으로 인해 용량이 과부하 될 위험이 있는 경우 가상머신은 추가로 마련된 런타임 창으로의 일시적 액세스 가능 여부를 하이퍼바이저에 확인할 수 있습니다. 이의 경우 하이퍼바이저는 추가로 마련된 런타임 창을 사용할 수 있을 때까지 기다리며 가상머신을 대기 리스트에 추가합니다. 추가적인 런타임 창을 사용할 수 있게 되면 하이퍼바이저는 첫 번째로 대기 중인 가상머신이 사용하도록 허용하여 높은 시스템 로드의 영향을 최소화합니다. 그러나 각 가상머신이 하나의 마련된 창만 사용하도록 하여 한 가상머신이 뜻하지 않게 시스템을 제어하게 되는 상황을 막을 수 있습니다.

오늘날 사용 가능한 미래형 솔루션

고전적인 하이퍼바이저에 비해 오버헤드는 단지 5kB 메모리 용량 요구



경량 하이퍼바이저 RTA-LWHVR이 있는 ECU의 다이어그램



RTA-BSW AUTOSAR BASIC SOFTWARE
RTA-OS OPERATING SYSTEM
RTA-RTE RUNTIME ENVIRONMENT
SWC SOFTWARE COMPONENT IN SECURE APPLICATION
VMA VIRTUAL MACHINE ADAPTER
VMI VIRTUAL MACHINE INTERFACE
→ INTER-CORE COMMUNICATION (ICC)

VM VIRTUAL MACHINE

량으로 낮아졌으며 전력 소비는 사용 가능한 코어 용량의 5%로 감소하였습니다. 이러한 개선 덕분에 RTA-LWHVR은 차량의 임베디드 시스템에 대한 특정 경계 조건에 문제없이 부합합니다. 이는 광범위한 애플리케이션에 완벽한 유연성을 제공하며 수많은 마이크로 컨트롤러에서 사용 가능합니다. 한편, 이 솔루션은 향후 각각 다른 소프트웨어와 안전 등급이 실행될 수 있는 ECU의 안정적, 고성능의 파티셔닝을 보장합니다.

인텔리전트 코어 간 통신 및 엄격한 캡슐화 덕분에 서로 독립적으로 소프트웨어 제어 기능을 개발할 수 있으며 이미 고객이 소유한 차량을 포함하여 전체 시스템의 재확인에 시간을 낭비하지 않고도 언제든지 수정할 수 있습니다. 이러한 방식으로 경량 하이퍼바이저는 자동차 산업에서의 애자일 소프트웨어 및 기능 개발을 위해 안전한 기반을 구축하고, 필요에 따라 정기적인 보안 업데이트를 통해 동적 보안 시스템을 용이하게 합니다. 그 결과로 레옹과 그의 부모가 사용하는 것과 같은 개별 구성과 이에 따른 후속 차량 업그레이드에 대한 모든 장애물이 제거될 수 있습니다.