항공기술을 이용한 자동차 안전성 향상

승인된 안전 기준들의 공통점

자동차 전자 부품들이 발전하는데 있어 새로운 접근 방법이 요구되고 있다. 특히 자동차에서 전자제어 시스템 수가 증가함에 따라 다양한 기능을 하나의 칩에 통합하는 단기적 솔루션이 필요해졌다.

항공전자공학에서 제시하는 하나의 모델이 있다: 항공전자 분야에서는 파티셔닝(partitioning) 기술이 이미 10년 전부터 사용되고 있고, 기본 OS로 작동하는 마이크로커널은 다른 OS들이 동작 가능한 파티션을 생성한다. 독일 베를린에 위치한 소프트웨어 회사인 오픈시너지는 표준 소프트웨어 플랫폼에 대한 기술적 부분을 담당하고 있고, 이 기술들을 자동차 산업에 적용하기 위해 준비해왔다. 이 기고는 자동차 소프트웨어를 개발하는데 있어 안전 기준을 유지하면서 기술을 이전하는 것에 대해 설명한다.

글 | **마티아스 게를라흐** 박사 / **스테판 송크 티에보** 박사
역 | **최주희** 주임, MDS테크놀로지 〈juhee@mdstec.com〉

AirBus

Safer vehicles through aircraft technology
Comparability of safety standards confirmed

마티아스 게를라흐(Matthias Gerlach) 박사는 오픈시너지(OpenSynergy)의 소프트웨어 엔지니어로 VirtuOS 프로젝트 총책임으로 근무 중이다. 베를린 기술대학에서 박사 학위를 취득했으며 ITS 표준화 및 Car-2-Car 커뮤니케이션 컨소시엄에서 활동하고 있다.

스테판 송크 티에보(Stefaan Sonck Thiebaut) 박사는 오픈시너지 창립 멤버이자 총괄 매니저로 전체 제품 개발을 책임지고 있다. 스탠포드 대학에서 박사 학위를 받았고 20년 이상 소프트웨어를 개발해왔다.

자동차에서 볼 수 있는 많은 전자제어 시스템들은 이미 자동차의 총 무게에 큰 영향을 미치고 있으며 이는 연비 저하와도 관계되고 있다. 또 전자 부품은 상당한 추가 비용을 필요로 하기 때문에 자동차에 더 많은 전자 부품을 사용하는 것은 경제적으로도 문제가 된다. 자동차 제조사들과 부품 공급자들이 지닌 유일한 해결책은 하나의 제어장치에 여러 기능을 통합하는 것이다. 즉, 가장 안전하고 효율적인 솔루션은 마이크로커널과 가상화 기술의 결합이다.

이 기술은 마이크로커널이 소프트웨어 아키텍처의 기반을 구성하고, 추가적인 OS를 결합할 수 있는 기본 기능을 제공한다. 이것은 하나의 프로세서 위에 서로 다른 논리적인 소프트웨어 영역들을 생성한다.

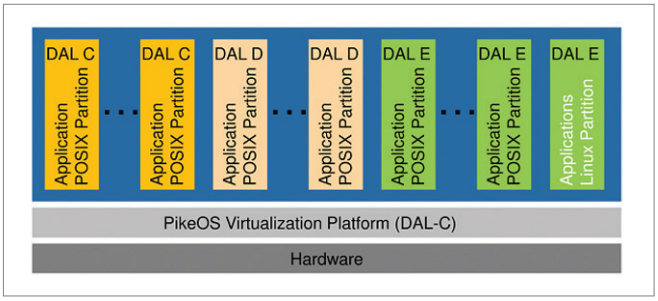
이 파티션들은 서로 독립적으로 동작하기 때문에 하드웨어적으로 요구 사항이 다른 OS들을 각각의 파티션에 결합할 수 있다. 만약 하나의 파티션에서 소프트웨어에 이상이 생기더라도, 전체 시스템은 아무 제약을 받지 않고 계속 실행된다. 이런 형태의 시스템 디자인은 OS들이 서로 영향을 미치는 것을 방지하는 동시에 악의적인 공격으로부터 보호한다.

가상화 기술은 OS가 물리적인 하드웨어가 아닌 가상의 하드웨어를 사용하는 각 파티션에 설치되는 것을 의미한다. 이것은 매우 복잡한 OS도 파티션 안에서 실행되도록 설계돼 있다.

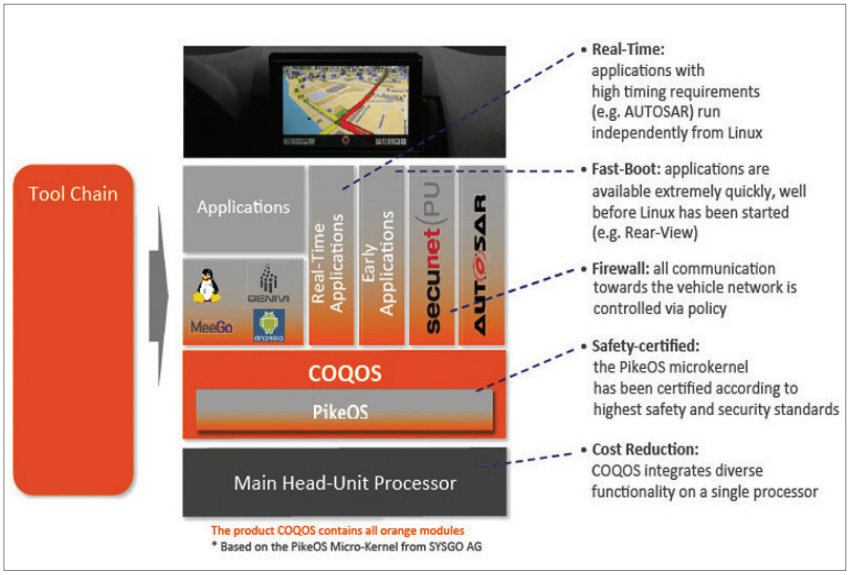
항공기에서 이미 사용 중인 파티셔닝 기술

마이크로커널을 이용한 파티셔닝 기술은 이미 10년 넘게 항공기술에서 사용돼 왔다. 이는 IMA(Integrated Modular Avionics) 아키텍처의 일부로 사용되고 있다(**그림 1**).

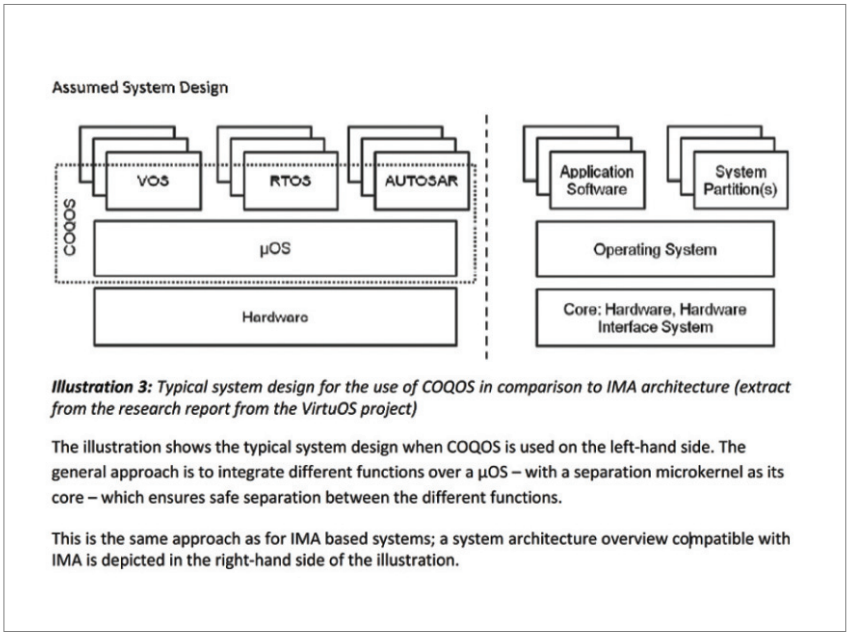
수년 전 엔지니어들은 필요한 소프트웨어 시스템의 수가 지속적으로 증가하는 상황에서도 제어장치의 수를 줄일 수 있었다. 예를 들어, 에어버스(Airbus)의 경우 시스고(SYSGO)의 마이크로커널 PikeOS가 화물 수송기인 에어버스 A400M 뿐 아니라 장거리용 에어버스 A350 항공기에도 탑재됐으며 이는 안전 표준



【그림 1】 AirBus A350의 통합된 항공 모듈 ASFC



【그림 2】 COQOS 아키텍처



【그림 3】 COQOS를 사용해 생성할 수 있는 일반적인 시스템 구조

인 DO-178B의 인증을 받았다.

마이크로커널 기술이 국방/항공분야에서는 오래 전부터 사용돼 왔는데 왜 자동차 산업분야에서는 아직 확실히 자리잡지 못했는지에 대한 질문이 있을 수 있다. 이에 대한 가장 적절한 답은, 항공기와는 달리 최근에 들어서야 자동차에 전자제어 기기 수가 급증하고 있고, 마이크로커널 솔루션에 대한 관심이 높아져 시험대에 올랐다는 것이다. 게다가, 새로운 기술은 ISO 26262와 같은 자동차에서 사용되는 소프트웨어의 안전성 요구사항을 충족시켜야만 한다.

오픈시너지는 마이크로커널 기술을 사용해 자동차에서 사용하는 소프트웨어를 통합하는 아이디어를 2007년부터 추진해 왔고, 이는 현재 시장성 있는 솔루션이 됐다. 이를 위해 표준 소프트웨어 플랫폼인 COQOS에 마이크로커널인 PikeOS를 통합했다. 이 마이크로커널 덕분에 COQOS는 다른 timing을 요구하는 소프트웨어 시스템 및 Safety Level이 다른 시스템이 서로 간의 간섭 없이 동작할 수 있는 독립적인 파티션을 제공한다. 이 말은 자동차 시스템이 어떤 파티션 위에서 동작하는 동안 리눅스 기반의 인포테인먼트 소프트웨어를 다른 파티션에서 실행할 수 있다는 의미다. 또한 COQOS는 AUTOSAR가 호환되는 프로그램을 쉽게 통합할 수 있도록 하기 위해 자동차용 소프트웨어의 통합을 위한 AUTOSAR 인터페이스를 지닌다.

COQOS 내의 마이크로커널은 국방/항공분야의 DO-178B 안전 표준 인증을 받았다. 하지만 항공전자 기기를 자동차 전자 부품에 적용하는 것은 흔하지 않기 때문에 항공전자 기기의 소프트웨어가 자동차 표준의 요구사항에 충족한 예는 없었다. 이 질문은 특히 ISO 26262가 발표됐기 때문에 더욱 중요하다.

VirtuOS 연구 프로젝트

이러한 배경 하에 베를린 연구 프로젝트 VirtuOS가 탄생했다. 이 프로젝트에서 베를린 기술대학(Technical University)과 프라운호퍼연구소(Fraunhofer Institute FIRST), 그리고 오픈시너지는 국방/항공분야의 안전 표준(DO-178B)이 근본적으로 차량용 소프트웨어 개발을 위한 안전 표준(ISO 26262)과 비슷하다는 것을 알게 됐다. 이 유사성은 항공 소프트웨어가 적용될 수 있도록 하고, 공인된 항공전자 기기 컴포넌트가 자동차 산업에서 사용될 수 있다는 보증을 제공하는 것이다. 2012년 4월 출간된 프로젝트 최종 보고서의 중요 메시지는 아래와 같다:

항공분야에서 소프트웨어 시스템의 인증을 위한 DO-178B 표준은 인증기관의 프로세스 결과, 상호작용에 결함이 없는 소프트웨어 사

용을 위해 필수적이다. ISO 26262 표준 또한 자동차에서 기능안전성을 확신하기 위한 필수 안전 시스템 개발 목적의 표준이다.

DO-178B와 ISO 26262는 적절한 오류 예방 단계를 통해 기능안전성을 보장할 수 있다고 간주한다. 이 두 가지 표준의 유사점과 차이점은 다음과 같다.

- 프로세스와 라이프사이클: 예상되는 수명주기는 어떠하며 이 수명주기에서 어떤 프로세스에 따라 실행될 것인가? 이 프로세스를 충족시키기 위해 어떤 요구사항이 필요한가?
- 작업 결과물: 프로세스의 결과물로 각종 문서가 산출되고 최종 소프트웨어 제품이 출시된다. 일반적으로 이러한 결과물들은 표준들을 만족시키는 기준 확인(Confirmation measure)과 제품 출시의 토대가 된다.
- ISO 26262 확인 방안: 누가 의사 결정을 수행하고 어느 선까지 권한의 자율성을 보장받을 것인가? 어떤 형태의 기준을 적용할 것인가?

이러한 비교 결과에 대한 결론은 항공기술과 자동차 산업에서 개발 프로세스는 근본적으로 동일하다는 것이다.

항공기술이 차량용 SW를 위한 이점 제공

ISO 26262는 현장 작동(Field Operation)에 대한 방안을 요구하고 있으나, ISO 26262를 위한 인증기관이 없는 것과 같은 몇몇 차이점에도 불구하고, 추정되는 소프트웨어의 생명주기와 대부분의 작업 결과를 대신할 수 있어서 항공 표준에 부합해 받은 이전 인증은 ISO 26262에 부합하는 자동차 소프트웨어 개발에 도움이 될 것이다. 결국 안전 표준의 공통점에 대해 근본적인 장애물은 없다. 이와는 대조적으로 VIrtuOS에서 수행된 연구는 DO-178B을 통한 대부분의 산출물이 ISO 26262에 따른 개발을 위해 재사용될 수 있다는 결과를 보여줬다.

안전 표준의 공통점을 찾는 것은 한 분야에서 사용된 컴포넌트들이 다른 분야를 위해 사용될 수 있는 기회를 제공한다. 이 연구에서 찾아낸 것은 두 세계가 멀리 있는 것처럼 보이지만 부분적으로 수렴할 수 있다는 것이다. 또한 VirtuOS 연구는 항공과 자동차 산업 사이의 더 큰 시너지를 이끌어낼 수 있다는 결과를 나타낸다.

이미 언급한 바 있는 하나의 예는, 표준 기반 소프트웨어 플랫폼인 COQOS이다. 오픈시너지는 항공분야에서 사용된 마이크로커널 기술을 자동차 산업을 위해 사용이 가능하도록 개발했다.

항공기술에서 마이크로커널을 자동차 소프트웨어 플랫폼에 통합하기 위한 오픈시너지의 접근은 완벽히 새로운 시도다. 또한 COQOS는 항공 컴포넌트를 자동차의 소프트웨어 시스템으로 이동시킨 대표적인 예이자 선구자다. 이 재사용성은 자동차 제조사들이 상당한 개발 비용을 절약하고, 기능안전성을 향상시키며, 타당한 가격에 안전한 자동차 기술을 가능하게 한다.

그림 3의 왼쪽 부분은 COQOS를 사용해 생성할 수 있는 일반적인 시스템 구조를 나타낸다. 이것은 여러 개의 서로 다른 기능들이 하나의 µOS를 통해 통합될 수 있다는 것을 명백히 보여준다. µOS는 마이크로커널을 기반으로 한다. 이는 다양한 기능의 안전한 분리를 보장한다.

그림의 오른쪽은 같은 원리를 이용한 IMA 기반의 시스템용 아키텍처를 나타낸다.

참고문헌

[1] Lotzke, M.: Experiences from Recent Avionics Projects. Talk given at the first symposium of the VirtuOS project partners on 15 June 2011. Berlin.

[2] www.autosar.org

[3] Gerlach, M.; Weißleder, S.; Hilbrich, R.: Can Cars Fly: From Avionics to Automotive: comparability of domain-specific standards. Embedded World 2011.