AUTOSAR 기능 안전 충족

이타스, 베이징 신에너지 자동차社의 목표 달성을 돕다

AUTOSAR는 완전한 ECU 소프트웨어 스택을 개발하기 위한 표준으로 자동차 시장에서 지속적으로 그 사용범위가 확장되고 있습니다. AUTOSAR가 빠르게 성장하는 전기차(EV)를 분야를 비롯한 임베디드 애플리케이션 개발에 있어서 보다 성숙도 높고 포괄적인 표준으로 자리매김함에 따라 고효율, 출시 기간 단축, 전체기능 커버라는 장점이 더욱 부각되고 있습니다. 베이징 신에너지 자동차社는 AUTOSAR를 ECU에 도입하기 위해 이타스를 선택했습니다.

베이징 신에너지 자동차(BJEV)는 어떤 회사인가

베이징 자동차 그룹(Beijing Automotive Group Co., Ltd.)의 자회사인 베이징 신에너지 자동차 (BJEV, Beijing New Energy Automobile Co., Ltd.)는 중국 최대의 전기자동차 제조사입니다. 2017년에 10만대 이상의 전기차를 생산했으며, 머지 않아 생산량이 23만대를 넘어설 것으로 예상됩니다. 이 회사는 중국의 국가주도 산업정책인 'Made in China 2025'를 비롯해 중국정부의 산업 전략에 있어서 핵심적인 역할을 담당하고 있습니다.

도전과제

최근 몇 년 간 자동차 산업은 몇 가지 요인으로 인해 큰 변화를 겪었습니다. 이 가운데 중요한 한 부분이 ISO 26262와 같은 승용차용 기능안전표준 및 농기계용 ISO 25119 기능안전기준의 도입입니다. 이러한 기준들은 소프트웨어 개발 프로세스 및 실행에 중대한 영향을 미쳤습니다

'베이징 신에너지 자동차'가 직면한 과제는 ISO 26262에 맞춰 ASIL-C 요구사항을 충족하는 MCU(Motor Control Unit), VCU (Vehicle Control Unit) 및 BMS(Battery Management System)등의 ECU를 개발하는 것이었습니다. AUTOSAR를 비롯해 여러 요소의 동시적 도입으로 인해 다양한 안전조치의 실행이 쉽지 않았습니다.

안전과 관련된 가장 큰 과제는 '간섭개념의 자유' (freedom of interference concept)를 가능케 하는 효율적 메커니즘의 구현이었습니다. 이 개념은 예를 들어 하나의 ECU와 같은 동일한 실행상황에서 안전과 관련된 소프트웨어 기능이나 안전과 관련없는 소프트웨어 기능들의 공존을 허용합니다. 간섭개념의 자유를 실현할 수 있는 대표적인 전략들은 다음과 같습니다.:

- 안전관련 시스템을 非 안전관련 시스템에서 분리할 수 있도록 하는 메모리 보호
- 데이터가 올바른 논리구조로 수신되었는지 여부와 데이터의 콘텐츠 유효성 여부를 탐지하는 end-to-end 방법 같은 데이터 손상 방지 기능
- 예기치 않은 실행을 탐지하기 위해 프로그램 플로우(flow) 모니터링 기능을 사용하여 순차적인 프로그램 실행

이러한 목표를 달성하려면 다양한 영역에서 명확한 조치와 세심하고 상세한 프로젝트 관리 접근방식이 필요했습니다. 이타스는 '베이징 신에너지 자동차' 가 핵심적인 혁신활동에 집중할 수 있도록 컨설팅 및 엔지니어링 서비스를 지원했습니다.

단계별 프로젝트

이 프로젝트는 세 단계로 구성됩니다. 첫째, 자동차를 제어하는 VCU 개발에 중점을 두어 베이징 신에너지 자동차에서 AUTOSAR의 기능을 구축하는 것이었습니다. 이 단계에서 이타스는 ECU를 위한 완전한 AUTOSAR 미들웨어인 RTA 기본 소프트웨어(RTA-BSW) 릴리스 패키지(release package)의 엔지니어링, 인프라 소프트웨어의 드라이버 모듈인 MCAL / CDD의 통합, 베이직 소프트웨어(BSW) 배열의 미세 조정, 현장에서 프로그램 오류를 수정할 수 있는 온 사이트 디버깅, 소프트웨어 구성(SWC) 통합에 대한 컨설팅과 같은 다양한 교육을 제공하는 것으로 고객을 도왔습니다. 이 단계는 베이징 신에너지 자동차가 최종 제품의 효율성과 품질을 개선할 수 있는 ECU가 AUTOSAR에 기반한 미래를 계획하는 데 중요한 역할을 했습니다.

둘째, 베이징 신에너지 자동차는 AUTOSAR 아키텍처를 BMS와 MCU로 마이그레이션했습니다. 여기에는 RTA-OS(운영시스템)를 TI TMS570 및 IFX TC234 마이크로 컨트롤러에 이식하는 것을 포함하여 여러가지 태스크 포함되었습니다. 셋째, 모든 ECU 소프트웨어 스택의 기능안전인증 획득을 위해 TUV, 베이징 신에너지 자동차, 이타스가 함께 ASIL-C 요구사항 충족을 위해 협업하는 것입니다. 이타스는 '베이징 신에너지 자동차'에게 기능안전인증, 안전 매뉴얼, 안전 사례, 평가 보고서 및 안전 검토와 같은 전체적인 솔루션을 제공하여 승용차용 기능안전표준인 ISO 26262의 요구사항을 충족할 수 있도록 도왔습니다.

결론

자동차에 대한 표준과 규정이 발전하고, 시장이 이전보다 제한이 많아졌으며, 복잡해지고, 표준 중심으로 변함에 따라 자동차를 수주하여 납품하는 회사는(OEM) 혁신적이면서 성공적인 자동차를 개발하는 데 어려움을 겪고 있습니다.

성공의 열쇠는 복잡성이 증가에도 불구하고, 합리적인 수준으로 비용을 유지하고 시장출시시간을 단축시키는데 있습니다. 이타스는 ISO 26262 ASIL-C 요구사항을 완벽하게 충족하는 ETAS AUTOSAR 컴포넌트를 배포함으로써 개발작업을 최소화하는 것으로 '베이징 신에너지 자동차'가 목표를 달성할 수 있도록 올바른 제품과 전문지식을 제공했습니다.

저자

탕이(Tang Yi), 이타스 중국지사, RTA 솔루션 허브 매니저.
다니엘 가로팔로(Daniele Garofalo), 이타스 주식회사 (ETAS Ltd.), RTA솔루션 제품관리 글로벌 책임자.