이타스의 RTA-BSW, ISO 26262의 요구사항 충족

이타스의 AUTOSAR 베이직 소프트웨어, ISO26262: 2018 ASIL-D 요구사항 충족

차량에 탑재되는 기능 소프트웨어가 많아질수록 기능 안전성도 더욱 중요해집니다. 한편 E/E 아키텍처가 점차 복잡해지면서 기능 안전성을 확보한 소프트웨어의 개발은 더욱 까다로워지고 있습니다. 이러한 상황을 해결하기 위해서는 오랜 기간 입증된 신뢰성 있는 소프트웨어가 필요합니다. 이에 TUV SUD는 이타스 AUTOSAR 소프트웨어 제품의 안전성 기준 충족 여부를 ISO 26262 ASIL-D 애플리케이션에서 테스트하였으며, '기준 충족'이라는 결과를 얻었습니다.

ISO 26262 등의 기능 안전성 기준은 E/E 시스템의 작동 오류로 인한 사고를 방지할 수 있도록 안전대책을 정의합니다. 이러한 안전 대책은 특정 소프트웨어 및 하드웨어가 관련 요구사항을 충족한다는 점을 공인하는 평가 지표 등이 포함되어 있습니다. 그러나 이러한 지표만으로도 차량 제조사 및 부품업체가 시스템 안전성을 충분히 입증할 수 있을까요? 그렇지 않습니다. 그 이유는 다음과 같습니다.

복잡성에 대처하기 위해서는 시간과 비용 필요

우선 현대식 프리미엄 차량을 예로 들어봅시다. 이 차량에 탑재된 소프트웨어 코드의 길이는 1억 줄을 단숨에 넘어버립니다. 이는 2013년부터 F-35 전투기에서 사용된 소프트웨어 코드의 4배를 넘는 양입니다. 주행의 전기화 및 자동화 흐름 속에서 차량 제조사들은 E/E 차량 아키텍처에 전례 없는 수준의 변화를 적용해야 했습니다. 이러한 변화 가운데, 전자 시스템의 책임 범위가 넓어지면서 기능 안전성은 그 어느 때보다 중요해졌습니다.

차량 내 시스템 전체에 걸쳐 안전성 요구사항을 충족하려면, 전략을 명확히 하고 컴포넌트가 설계 단계에서부터 안전성을 확보하도록 해야 합니다. 안전성 기준은 차량 제조사의 준수 사항을 정의할 뿐 준수 방법을 알려주지는 않습니다. 그렇기 때문에 공인된 컴포넌트를 사용해야 전체 프로세스를 더욱 원활하게 진행하면서 전체 시스템에 대한 공인 전략을 세울 수 있습니다.

한편 차량 제조사는 급격한 시장의 변화와 생산원가 절감의 압력에 직면해 있습니다. 그 중 안전성 관련 소프트웨어를 구현, 검토 및 검증하는 작업은 상당한 비용과 시간이 들지만 그렇다고 해서 결코 생략할 수 없는 과정입니다. 따라서 사전에 공인된 컴포넌트를 사용하는 것이 최적의 솔루션이라고 볼 수 있습니다.

프로젝트

이타스는 안전성 중심의 시스템을 개발하는 고객을 지원하기 위해 TUV SUD에 프로젝트를 의뢰하여 AUTOSAR 베이직 소프트웨어인 RTA-BSW의 검증을 실시하였습니다. TUV SUD는 안전성 분야에서 신뢰와 인정을 받고 있는 세계 최고 수준의 기술 서비스 공급업체입니다. TUV SUD는 TUV SUD 스마트 소프트웨어 프로그램에 기초하여 RTA-BSW이 기능 안전성 요구사항 등 관련 공인 기준을 충족하는지를 확인하였습니다. 또한 다음의 품질 및 보안 요소도 분석하였습니다.

- 일반적인 안전성 관리
- 소프트웨어 산출물 범위와 관련된 세부 소프트웨어 요구사항들
- 소프트웨어 개발 프로세스

해당 프로젝트는 승용차, 오토바이, 트럭 및 중장비 차량 등을 포괄하기 위하여 다수의 안전 기준을 참고하였습니다. 준수여부를 평가하기 위하여 적용된 안전 기준은 다음과 같습니다.

- ISO 26262:2018
- IEC 61508:2010
- ISO/DIS 19014:2018
- ISO 25119:2018

전체 평가 결과에 따르면 RTA-BSW는 기능 안전성 모듈에 포함된 요구사항 등 TUV SUD 스마트 소프트웨어 프로그램의 관련 요구사항을 충족하였습니다. 이번 결과를 통해 영국, 독일 및 이탈리아의 이타스 RTA팀은 매우 중요한 전기를 맞이하였습니다. 이타스 RTA-BSW 고객은 이제 높은 안전성 기준을 충족할 수 있는 기반을 확보하게 되었습니다.

RTA-BSW란?

RTA-BSW는 이타스의 AUTOSAR Classic 베이직 소프트웨어 그룹으로서 RTA Classic AUTOSAR 제품 포트폴리오의 핵심입니다. RTA-BSW는 지난 20년이 넘는 기간 동안 이미 도로를 달리고 있는 약 20억 대의 ECU에 적용되었으며, 생산 후 이슈가 전혀 발생하지 않은 제품입니다. AUTOSAR R4.x 기능을 지원하는 RTA-BSW는 통신, 메모리, 진단 및 안전성 등 AUTOSAR 스택 세트(모듈 집합)로 이루어져 있습니다. 베이직 소프트웨어 모듈은 일반적으로 특정 차량 기능을 개발하기 위한 공통 분모라고 알려진 중앙 ECU 통신 기능을 지원합니다.
일반적으로 베이직 소프트웨어 모듈은 특정 차량 기능을 개발하는데 공통적으로 이용되는 ECU 통신 기능을 사용 할 수 있도록 지원합니다.

RTA-BSW는 기능 안전을 포함하는 응용프로그램 개발에 고객들이 필요로 하는 모든 요구사항을 지원합니다.

요약

현재 자동차 산업은 차량 소프트웨어 개발 프로세스의 모든 단계에 영향을 미치는 여러 변화에 직면해 있습니다. 이러한 변화의 영향을 특히 크게 받는 영역은 안전성과 관련된 임베디드 소프트웨어입니다. 추가 경비 절감의 필요성이 큰 기업들은 차별화 전략에 집중하면서도 다른 부분에서는 가능한 한 AUTOSAR 플랫폼 같은 기성 컴포넌트를 사용하고 있습니다. 이타스는 공인된 AUTOSAR 베이직 소프트웨어 제품을 통해 고객들이 최고 수준의 안전성 기준을 충족하고 향후 과제에도 완벽히 대비할 수 있도록 합니다.

영문 원문으로 보기

저자

루카 벌디니(Luca Baldini)
이타스(영국 요크), RTA-BSW 프로덕트 매니저
대니얼 개러팰로(Daniele Garofalo)
이타스(영국 요크), RTA Solutions 프로덕트 관리 글로벌 부문장
조너던 맹텔로(Jonathan Manktelow)
이타스(영국 요크), Safety Certification 프로젝트 매니저