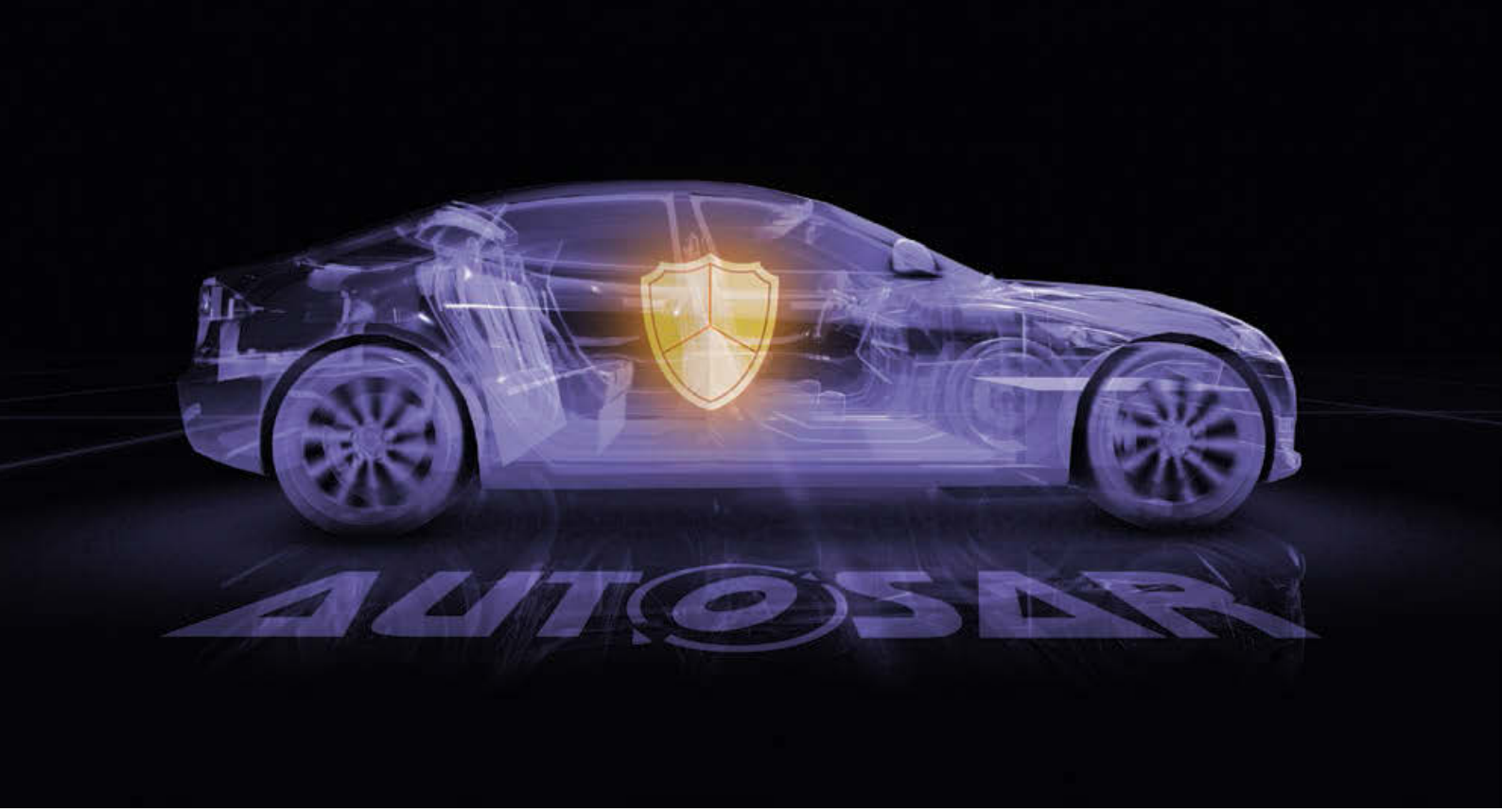

AUTOSAR 보안

어댑티브 플랫폼, 차량 보호를 위한 전체론적인 접근 방식이 필수적

차량의 자동화된 주행 기능과 증가된 연결성은 보다 유연한 소프트웨어 아키텍처와 높은 수준의 보안이 요구되고 있습니다. AUTOSAR는 adaptive 플랫폼과 보안 컴포넌트를 통해 이러한 요구사항을 충족시키고 있습니다.

대부분의 차량 플랫폼에서 표준 미들웨어로 사용되고 있는 AUTOSAR Classic은 일반적인 요구사항을 충족시키는 플랫폼으로서 여전히 의미가 있습니다. 그러나 미래에는 vehicle computer가 차량의 핵심 애플리케이션으로서 E/E 아키텍처의 모습을 만들어 갈 것이며, 그 결과 차량은 소프트웨어 중심 시스템으로 발전할 것입니다. 이에 따라 AUTOSAR Adaptive는 미래 지향적 규칙 세트로서 AUTOSAR Classic을 상당 부문 대체하고 차량 보안에 관한 새로운 표준을 제시하고 있습니다.

AUTOSAR 보안 모듈

AUTOSAR는 이미 차량 내 통신 보안 및 기밀 데이터 보호 등을 위한 다양한 보안 모듈을 포함하고 있습니다. 그러나 AUTOSAR Classic과 AUTOSAR Adaptive는 서로 다른 아키텍처에 기초하고 있기 때문에, 일부 보안 모듈에 차이가 있습니다. (그림 1)

- **Crypto Stack**: Crypto Stack은 소프트웨어 라이브러리 또는 하드웨어 모듈을 기반으로 하며, 통일된 인터페이스를 통해 애플리케이션 및 시스템에 암호 서비스를 제공합니다. 애플리케이션은 추상화된 인터페이스를 통해서 암호 서비스에 접근하므로 다른 ECU로의 포팅이 용이합니다. 또한 Crypto Stack은 암호 연산이 병렬로 실행될 수 있도록 지원합니다.
- **SecOC, TLS, IPsec**: AUTOSAR Classic 전용 프로토콜인 SecOC는 CAN 통신을 보호합니다. SecOC는 메시지 인증과 메시지 최신성을 보장하지만 메시지 기밀성은 보장하지 않습니다. 또한 SecOC를 통해 자동차 제조사는 자신만의 고유한 보안 수준을 상세하게 설정할 수 있습니다. 반면 차량 내부 네트워크에 이더넷이 탑재되면서 TLS와 IPSec의 중요성도 커지고 있습니다. 두 보안 프로토콜 모두 통신의 기밀성과 인증을 지원합니다. TLS는 차량 외부 통신에도 적합합니다.
- **신원 및 접근 관리**: AUTOSAR의 신원 및 접근 관리 모듈은 오직 인가된 애플리케이션만이 특정 리소스에 접근할 수 있도록 합니다. 이러한 접근 권한은 AUTOSAR에서 자유롭게 설정하고 언제든지 업데이트할 수 있습니다.
- **안전한 진단**: AUTOSAR는 보안 이벤트를 안전한 메모리에 기록할 수 있도록 지원합니다. 또한 0x27(SecurityAccess), 0x29(Authentication)와 같은 UDS 서비스를 이용하여 보안 이벤트 데이터에 접근하는 것을 모니터링합니다. 예를 들어 진단 테스트 장비는 시도-응답 통신 또는 인증서를 통해 인증된 경우에만 보안 이벤트 기록에 접근할 수 있습니다.

보안 엔지니어링 프로세스

보안 엔지니어링 프로세스의 핵심 요소는 AUTOSAR의 보안 모듈을 차량 플랫폼이 요구하는 보안 요구사항에 맞게 조정하는 것입니다. 다시 말해 AUTOSAR는 보안 엔지니어링 프로세스 전체에 통합되어야 합니다. 보안 엔지니어링 프로세스는 위험 분석, 설정, 테스트와 같은 핵심 단계를 포함합니다. SecOC를 예로 들면 다음과 같습니다. (그림 2).

- **위험 분석:** 이 단계에서는 모든 메시지에 대한 위험 분석을 수행하여 SecOC가 보호해야 하는 메시지를 파악합니다. 그리고 메시지에 적합한 프로파일을 지정합니다.
- **설정:** 위험 평가와 보안 프로파일에 따라 모든 통신 대상 ECU의 SecOC와 crypto stack을 설정합니다. 이 단계에서 특히 주의해야 할 점은 하나의 ECU에서 설정 오류가 발생하면 보안 메시지가 검증되지 않아 폐기될 수 있다는 점입니다.
- **테스트:** ECU 양산 이전에 코드 리뷰 SecOC 모듈의 기능 테스트, 침투 테스트 등의 보안 테스트를 실시해야 합니다

AUTOSAR Adaptive, 통합적인 보안 접근방식이 필수적

커넥티비티 서비스와 자율주행 기능의 증가에 따라 안전과 관련된 차량 기능 또한 증가하고 있습니다. 이는 차량 플랫폼에 맞는 정교한 보안 조치와 높은 보안 수준을 갖추는 것이 그 어느 때보다 중요해지고 있다는 것을 의미합니다. 향후 자동차 제조사들도 점차 증가되는 연결성에 기초하여 새로운 사업 모델을 개발할 것이며, 이러한 사업 모델은 보안을 필수적으로 요구할 것입니다. 따라서 추후 AUTOSAR Adaptive를 개발할 때에는 보안 기능을 반드시 통합해야 합니다.

AUTOSAR Adaptive의 핵심 원칙은 차량 보안에 대한 통합적인 접근방식이 되어야 합니다. 따라서 향후 AUTOSAR Adaptive 개발 과정에서는 하드웨어 보안 모듈 및 침입 탐지·방지 솔루션 구현 가능성 등의 추가적인 보안 컴포넌트를 반드시 고려해야 할 것입니다. ■

보안 요구사항에 따른 AUTOSAR 설정

예: 안전한 ECU 통신

- 보안 관련 메시지 식별
- SecOC에서 메시지 설정
- Crypto Stack에서 키 및 알고리즘 선택
- 차량 전체적으로 설정 통일
- 핵심 보안 컴포넌트의 코드 리뷰
- SecOC 모듈의 기능 테스트
- ECU 침투 테스트

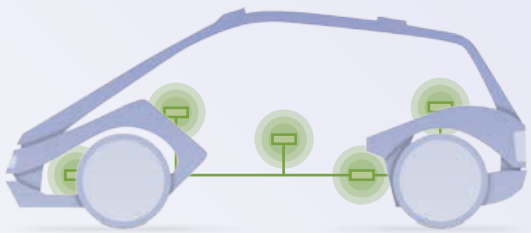

그림 2: 보안 요구사항에 따른 AUTOSAR 설정 (SecOC 예시)

저자

알렉산더 베르톨트(Alexandre Berthold) 박사: 에스크립트, 컨설팅 및 엔지니어링 팀장
미첼 피터 슈나이더(Michael Peter Schneider) 박사: 에스크립트, AUTOSAR 보안 프로젝트 매니저

영문 원문으로 보기

	Crypto Stack	SecOC	TLS	IPSec	안전한 진단	신원 및 접근 관리
AUTOSAR Classic 4.4	✓	✓	✓	✗	✓	✗
AUTOSAR Adaptive R19-03	✓	✗	✓	✓	✗	✓

그림 1: AUTOSAR Classic 및 Adaptive의 보안 모듈 (2019년 8월 현재)