AutoCrypt E2E Cybersecurity for ADS Safety

아우토크립트가 제시하는 자율주행 사이버보안 전략

"아우토크립트의 E2E(End-to-End) Cybersecurity는 자율주행 시스템의 안전성을 위해 자동차제작사, 자율주행 기업, 운송플랫폼사, 보험사 등 자율주행 생태계 전 계층에 걸친 구조적 체계로 사이버보안을 정의한 통합적 접근 방식을 제안한다."

서론

자율주행 시스템(ADS: Autonomous Driving System)은 차량이 운전자의 개입 없이 주변 환경을 인지하고 판단하여 스스로 주행하는 기술로, 인공지능(AI), 센서 융합, 고성능 컴퓨팅, 통신 기술이 결합된 대표적인 융합 산업이다. 자율주행 차량은 카메라, 레이더(Radar), 라이다(LiDAR) 등 다양한 센서를 통해 도로 상황과 객체를 실시간으로 인식하고, 이를 기반으로 경로를 계획하며 차량을 제어한다. 이러한 기술은 교통사고 감소, 교통 효율성 향상, 이동 약자 지원 등 다양한 사회 경제적 가치를 창출할 것으로 기대되며, 자동차 산업을 단순한 이동 수단에서 지능형 모빌리티 서비스로 전환시키는 핵심 동력으로 평가된다.

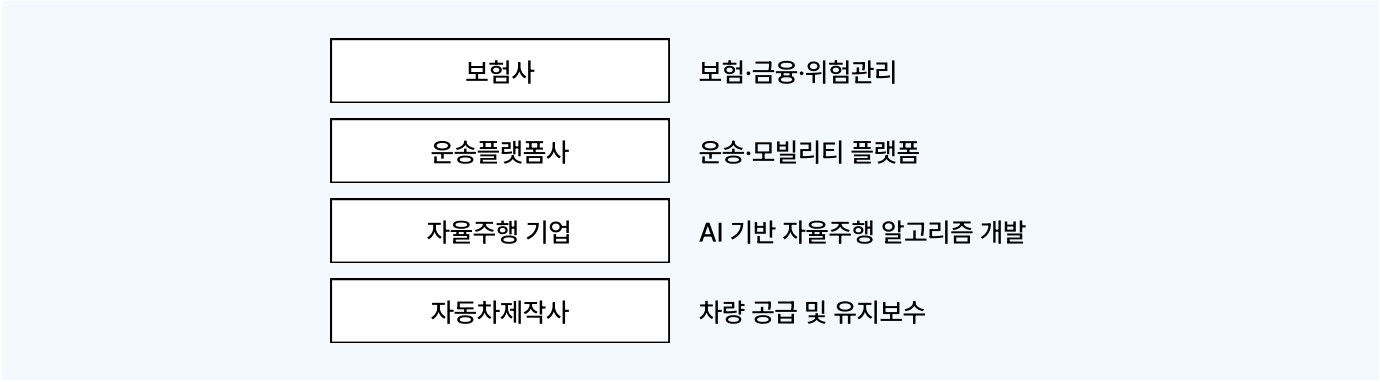
자율주행 기술의 발전은 차량의 전동화(Electrification)와 소프트웨어 정의 차량(SDV: Software Defined Vehicle)으로의 진화를 동반한다. 이에 따라 차량 내부 네트워크와 외부 인프라 간의 연결성이 급격히 증가하고 있으며, 차량은 더 이상 폐쇄된 시스템이 아닌 외부와 지속적으로 데이터를 주고받는 개방형 CPS(Cyber-Physical System) 플랫폼으로 변화하고 있다. 확장된 연결성은 자율주행의 핵심 요소이지만 동시에 새로운 사이버 위협의 공격 표면을 확대시키는 요인이 된다.

이러한 맥락에서 사이버보안은 자율주행의 신뢰성과 안전성을 확보하기 위한 필수 요소로 부각된다. 전통적인 자동차에서의 사이버보안 위협이 비교적 제한적이었다면, 자율주행 차량에서는 해킹을 통한 원격 제어, 센서 데이터 위·변조, 통신 채널 공격, 소프트웨어 취약점 악용 등이 실제 물리적 안전사고로 이어질 수 있다. 특히 Physical AI 개념이 적용된 자율주행 시스템은 AI가 센서와 액추에이터를 통해 현실 세계와 직접 상호작용하기 때문에, 사이버 공격이 곧바로 차량의 물리적 동작으로 연결된다는 점에서 위험성이 크다. 예를 들어, 공격자가 차량 제어 시스템에 침입해 가속, 제동, 조향을 조작하거나 센서 데이터를 교란하면, 자율주행 AI는 잘못된 판단을 내리고 사고로 이어질 수 있다.

자율주행 기술의 성공적인 상용화와 대중적 수용을 위해서는 운행 기술의 완성도뿐 아니라 사이버보안에 대한 신뢰 확보가 선행되어야 한다. 사이버보안은 선택적 요소가 아닌 자율주행 시스템의 안전성과 직결된 핵심 기반이며, 이를 간과할 경우 단일 사고가 산업 전체에 대한 신뢰 붕괴로 이어질 수 있다. 따라서 자율주행 생태계 전반에서 보안을 핵심 설계 원칙으로 반영하고, 기술적 대응과 제도적 대응을 병행하는 것이 필수적이다.

자율주행 생태계

자율주행 산업은 차량, 소프트웨어, 서비스, 제도 등 다양한 요소가 결합된 복합 생태계로, 개별 기업의 기술력만으로는 완전한 구현이 어려운 특징을 가진다. 이러한 한계를 극복하기 위해 최근에는 자동차제작사, 자율주행기업, 운송플랫폼사, 보험사가 유기적으로 협력하는 통합형 자율주행 생태계가 중요하게 부각되고 있다. 특히 자율주행 실증도시 사업을 추진하고 있는 국토교통부는 자동차제작사, 보험사, 운송플랫폼사로 구성된 "K-자율주행 협력모델"을 통해 차량 공급, 전용 보험, 서비스 운영을 하나의 체계로 묶어 자율주행 기업이 기술 개발에 집중할 수 있는 체계를 제시하고 있다.



자율주행 기업은 AI 기반 자율주행 알고리즘을 개발하는 핵심 주체로 실제 주행 데이터를 기반으로 시스템을 고도화하고 자율주행 성능을 지속적으로 개선하는 역할을 수행한다. 그러나 자율주행 기술은 차량 제어, 안전성 확보, 서비스 운영 등 다양한 요소와 밀접하게 연결되어 있기 때문에, 자율주행 기업 단독으로는 개발과 실증에 구조적인 한계가 존재한다.

이러한 문제를 해결하기 위해 자동차제작사는 자율주행 기술 실증에 최적화된 차량을 공급하고 표준화된 차량 제어 인터페이스를 제공한다. 또한, 차량에서 발생하는 데이터를 실시간으로 전달하는 데이터 파이프라인을 구축하고, 차량 상태 모니터링 및 유지보수까지 지원함으로써 자율주행 기업이 핵심 자율주행 SW 개발에 집중할 수 있는 환경을 조성한다.

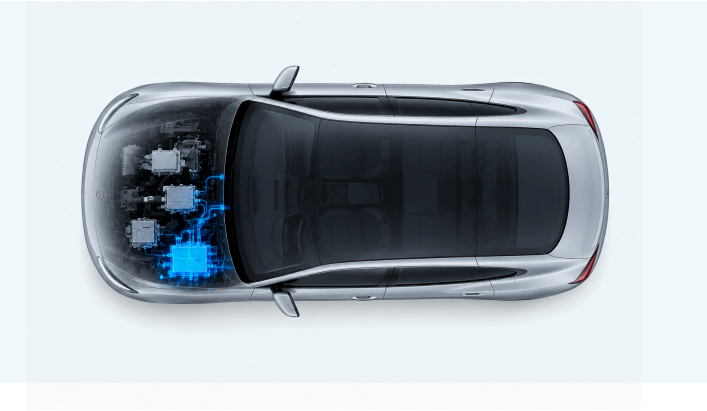
운송플랫폼사는 자율주행 서비스 운영 및 데이터 활용을 담당한다. 차량 관제, 배차 관리, 운행 데이터 분석 등 자율주행 서비스 운영에 필요한 플랫폼을 제공하며, 차량과 플랫폼 간 연동을 통해 실제 서비스 환경에서의 운영 효율성과 안정성을 검증한다.

자율주행 환경에서는 예측 불가능한 도로 상황, 시스템 오류, 사이버 공격 등의 요인으로 인해 사고가 발생할 수 있는데, 보험사는 이러한 위험을 제도적으로 완화하며 사고 데이터 분석, 사고 예방 컨설팅 등을 제공하여 자율주행 시스템의 안전성과 신뢰성을 향상시키는 데 기여한다. 이는 자율주행 기술의 상용화를 가로막는 요소 중 하나인 책임 리스크를 완화하는 기능으로 작용한다.

자율주행 사이버보안: 단일 계층 보안

자율주행 시스템은 차량 내부 제어 시스템, 자율주행 소프트웨어, 클라우드 및 플랫폼, 보험 및 데이터 인프라까지 다층적으로 구성되어 있다. 이러한 구조적 특성으로 인해 자율주행 사이버보안은 특정 계층만을 보호하는 방식, 즉 단일 계층 보안 (Single-Layer Security)으로는 근본적인 안전성과 신뢰성을 확보하기 어렵다. 오히려 단일 계층 중심의 보안 접근은 전체 시스템의 취약성을 은폐하거나 특정 지점에 집중시키는 결과를 초래할 수 있다.

단일 계층 보안이 실패하는 가장 근본적인 이유는 공격자의 전략이 항상 가장 약한 고리를 선택한다는 점에 있다. 자율주행 시스템이 여러 계층으로 구성되어 있는 이상, 공격자는 보안이 강한 차량 내부 시스템을 직접 공격하기보다 상대적으로 취약한 외부 플랫폼, 클라우드 API, 모바일 애플리케이션 등 우회 경로를 선택한다.
예를 들어 차량 ECU와 내부 네트워크가 강력하게 보호되어 있더라도, 운송플랫폼 서버가 취약하다면 공격자는 해당 서버를 침해하여 원격으로 차량 제어 명령을 주입할 수 있다. 이는 단일 계층 보안이 전체 공격 경로를 차단하지 못한다는 것을 보여주는 대표적인 사례다.



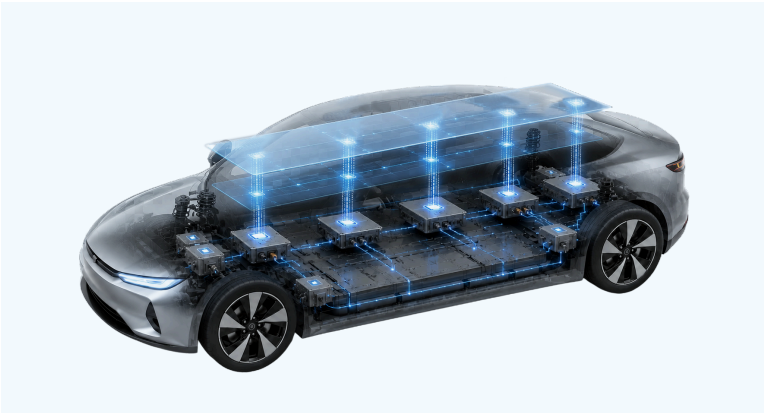
또한 자율주행 환경에서는 계층 간 인터페이스가 핵심 공격 지점으로 작용한다. 데이터는 차량, 클라우드, 플랫폼, 외부 서비스 간을 지속적으로 이동하며, 이 과정에서 인증, 암호화, 무결성 검증이 적절히 적용되지 않을 경우 공격자는 데이터 위·변조 또는 세션 탈취를 통해 시스템을 교란할 수 있다. 단일 계층 보안은 해당 계층 내부의 보호에는 효과적일 수 있으나, 데이터가 이동하는 경계 영역까지 보호하지 못하기 때문에 실제 공격 시나리오를 방어하는데 한계가 존재한다.

책임 구조 측면에서도 단일 계층 보안은 구조적인 한계를 가진다. 자율주행 생태계는 자동차제작사, 자율주행 기업, 운송 플랫폼사, 보험사 등 다수의 주체로 구성되며, 각 주체는 서로 다른 시스템과 보안 정책을 운영한다. 이처럼 책임이 분산된 구조에서는 특정 계층에서 보안이 미흡할 경우 전체 시스템에 보안 공백이 발생할 수 있기 때문에 자율주행 생태계의 모든 계층에 적절한 사이버보안 기술을 적용하여야 한다.

자율주행 사이버보안: 계층별 개별 보안

자율주행 시스템은 다양한 계층으로 구성된 다계층 분산 시스템이며, 각 계층은 서로 긴밀하게 연결되어 하나의 서비스로 작동한다. 이러한 구조에서 흔히 채택되는 접근 방식은 각 계층별로 독립적인 보안 대책을 적용하는 계층별 개별 보안 (Layer-by-Layer Security)이다. 그러나 자율주행과 같은 복잡한 사이버-물리 시스템에서는 이와 같은 방식만으로는 충분한 안전성과 보안성을 확보하기 어렵다. 보안 기술을 모든 계층에 적용하는 것은 자율주행 사이버보안을 위한 "필요조건"이지 "충분조건"이 아니다.

계층별 개별 보안의 가장 중요한 한계는 보안 정책의 불일치이다. 각 계층은 서로 다른 조직에 의해 운영되기 때문에 적용되는 인증 방식, 암호화 수준, 접근통제 정책이 상이할 수 있다. 이 경우 공격자는 가장 보안 수준이 낮은 계층을 선택하여 전체 시스템을 우회한다. 예를 들어 차량 내부 시스템에서는 강력한 인증 체계를 적용하고 있더라도, 운송플랫폼이나 모바일 애플리케이션에서 상대적으로 약한 인증 메커니즘을 사용한다면, 공격자는 해당 경로를 통해 시스템 전체에 접근할 수 있다. 즉, 개별 계층이 안전하더라도 정책 간 불균형 자체가 새로운 공격 표면이 된다.

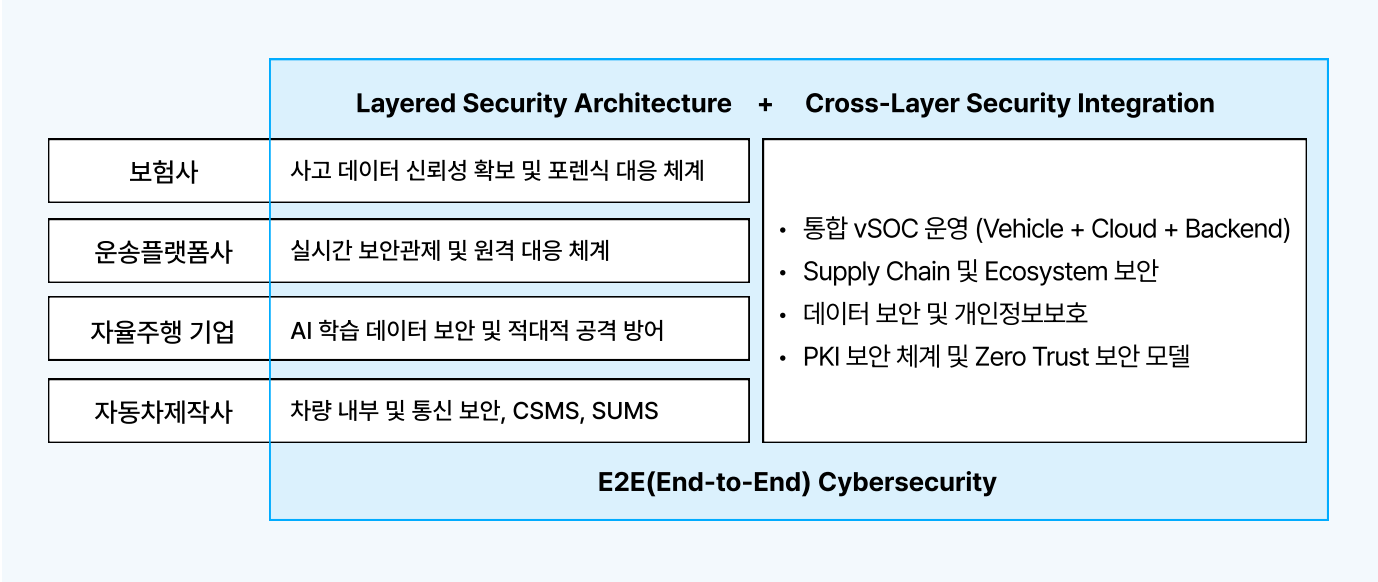


또한 자율주행 환경에서는 공격이 단일 지점에서 발생하지 않고, 여러 계층의 취약점을 결합하는 연쇄적 공격 형태로 진화한다. 각 계층에서 발견되는 취약점이 단독으로는 치명적이지 않더라도, 이를 연결하면 전체 시스템을 장악할 수 있는 공격 경로가 형성된다. 예를 들어, 모바일 앱의 취약점을 통해 인증 토큰을 탈취하고, 이를 기반으로 클라우드 API에 접근한 뒤, 최종적으로 차량 제어 명령을 전달하는 방식이 가능하다. 이처럼 계층 간 연결을 기반으로 한 공격은 개별 계층 보안만으로는 탐지하거나 차단하기 어렵다.

보안 가시성 부족 또한 중요한 문제이다. 계층별로 로그와 이벤트를 독립적으로 관리할 경우, 각 시스템에서는 정상적인 활동으로 보이는 이벤트가 실제로는 하나의 공격 시나리오를 구성하는 일부일 수 있다. 예를 들어 특정 시간대에 모바일 앱 로그인, 클라우드 API 호출, 차량 제어 요청이 각각 정상 범위 내에서 발생하더라도, 이를 통합적으로 분석하면 비정상적인 공격 흐름으로 식별될 수 있다. 따라서 계층별 개별 보안 체계에서는 전체 공격 맥락을 파악하기 어렵고, 이는 탐지 지연 및 대응 실패로 이어질 가능성이 높다.

AutoCrypt E2E Cybersecurity

자율주행 사이버보안을 위해 아우토크립트가 제시하는 E2E(End-to-End) Cybersecurity는 자율주행 시스템의 안전성을 확보하기 위해 보안을 단일 기술이 아닌 전 계층에 걸친 구조적 체계로 정의한 접근 방식이다. 이 모델은 크게 Layered Security Architecture(다층 보안 구조)와 Cross-Layer Security Integration(계층 간 통합 보안)이라는 두 축으로 구성되며, “Security for Safety”, 즉 사이버보안 사고가 곧 물리적 안전사고로 이어질 수 있다는 전제를 기반으로 한다.



Layered Security Architecture는 자율주행 생태계를 구성하는 각 계층에 대해 독립적이면서도 전문화된 보안 기술을 적용하는 아키텍처이다. 자동차 사이버보안의 풀 스택 제품을 보유하고 있는 아우토크립트의 전문 보안 기술을 바탕으로 위협 분석 프로세스를 통해 도출된 계층별 특화 보안 기술을 최적의 형태로 적용한다.

아우토크립트는 여기서 한 걸음 더 나아가, 이러한 계층별 보안이 상호 연계되지 않으면 실질적인 안전을 보장할 수 없다는 점을 강조한다. 이를 해결하기 위한 두 번째 축이 바로 Cross-Layer Security Integration이다. 이는 각 계층의 보안 시스템을 하나의 유기적 체계로 통합하여, 공격 탐지, 대응, 예방을 End-to-End 관점에서 수행하는 접근이다.

아우토크립트의 E2E Cybersecurity는 여러 보안 기술의 단순한 나열이 아니라, 다층 방어 구조와 계층 간 통합을 결합한 최적의 자율주행 사이버보안 아키텍처이다. Layered Security Architecture가 각 계층의 전문적 방어를 담당한다면, Cross-Layer Security Integration은 이를 연결하여 전체 시스템의 일관성과 가시성을 확보한다. 이 두 요소가 결합될 때 비로소 자율주행 시스템은 복잡한 공격 시나리오와 연쇄적 위협에 대응할 수 있으며, 궁극적으로 “보안을 통한 안전(Safety through Security)”이라는 목표를 실현할 수 있다.

Layered Security Architecture + Cross-Layer Security Integration

AutoCrypt E2E Cybersecurity의 Layered Security Architecture는 자율주행 시스템을 구성하는 각 계층별로 위협 모델을 정의하고, 해당 계층에 최적화된 보안 기술을 적용한다. 자동차제작사는 차량 내의 핵심 SW 유출과 위변조를 방지하고 차량 내외부 통신 보안을 위해 암호화 및 인증 시스템을 도입하고 차량 생애주기동안 사이버보안 전반을 관리하는 CSMS(Cyber Security Management System)와 SUMS(Software Update Management System)를 구축한다. 자율주행 기업은 AI 학습 데이터의 무결성을 보장하고, SW 취약점을 관리하며, 적대적 공격(Adversarial Attack) 등으로 인한 AI의 잘못된 판단을 감시하는 AI Safety Guardrail 기술을 적용한다. 운송플랫폼사는 차량과 클라우드를 연결하는 서비스 계층에서 실시간 보안관제, 데이터 암호화, 개인정보 보호를 수행하며, 보험사는 사고 데이터의 위변조 방지와 포렌식 기반 검증 체계를 통해 책임성과 신뢰성을 확보한다. 이처럼 각 계층은 고유한 위협 모델을 기반으로 설계된 보안 체계를 갖추며, 이는 전체 시스템의 기본적인 방어선을 형성한다.

자율주행 시스템은 각 계층이 독립적으로 존재하는 것이 아니라 서로 긴밀하게 연결되어 있기 때문에 공격 역시 계층 간 경계를 넘나들며 발생한다. 이 지점에서 요구되는 개념이 바로 Cross-Layer Security Integration이다. 이는 각 계층의 보안 기능을 단순히 병렬적으로 배치하는 것이 아니라, 정책, 인증, 데이터, 모니터링을 전 계층에 걸쳐 일관되게 통합하는 접근이다. 대표적으로 통합 vSOC(Vehicle Security Operations Center)는 차량, 클라우드, 플랫폼에서 발생하는 로그와 이벤트를 통합 분석하여 개별 계층에서는 식별하기 어려운 공격 패턴을 탐지한다. 또한 PKI 기반의 통합 인증 체계를 통해 모든 통신 주체들을 상호 검증하며, Zero Trust 모델을 적용하여 "내부는 안전하다"는 가정을 제거한다.

이와 함께 공급망 보안도 중요한 요소로 포함된다. 자율주행 시스템은 다수의 협력사와 소프트웨어 구성요소로 이루어지기 때문에, 부품 및 소프트웨어 공급망에서의 취약점이 전체 시스템으로 확산될 수 있다. 따라서 개발 단계부터 운영 단계까지 전 주기에 걸친 공급망 보안 관리가 필요하며, 모바일 앱, 클라우드 인프라, 정비 시스템, 충전 인프라 등 확장된 자동차 생태계 전반을 보호 범위에 포함해야 한다. 데이터 보안 역시 통합 보안의 핵심 요소로, 센서 데이터와 AI 학습 데이터의 무결성 확보, 개인정보 보호 규제 준수 등 안전하고 신뢰할 수 있는 데이터 거버넌스 체계를 구축해야 한다.

AUTOCRYPT

For more information about AUTOCRYPT's comprehensive security solutions,
visit autocrypt.co.kr

For partnership inquiries and solution consultations,
contact global@autocrypt.io