AUTOCRYPT

(총괄)자동차 보안 취약점 기반 위협 분석 시스템개발

자동차 산업계에 다가오는 **사이버 보안 규정변화**에 대한 준비

규제 준수, 테스트 그리고 그 이상

사이버보안 가이드북

TABLE OF CONTENTS

개요

인류의 역사를 통틀어 보안은 사회에서 끊임없이 요구되어 왔다.

태초부터 인간은 자신의 것을 보호하는 데 집중해 왔다. 산업과 기술의 발전으로 사회가 진화하면서 자원 보호의 범위는 음식, 집, 돈과 같은 유형의 소유물뿐만 아니라 데이터, 클라우드, 심지어 블록체인과 같은 무형의 자원으로까지 확장되었다.

가상의 연결과 경로는 사람의 눈에 보이지 않기 때문에 무형의 자원을 보호하는 것이 유형의 자원을 보호하는 것보다 훨씬 더 까다로울 수 있다. 바로 이 점이 IT 보안과 애플리케이션 및 시스템 보안의 중요성이 대두되는 이유다. 개인과 기업 모두에 대한 보안 솔루션이 우선순위가 되고 나아가 보편화되었다.

그러나 사회가 계속해서 발전하는 것처럼 기술 또한 지속적으로 발전하고 있으며, 현재는 교통 및 모빌리티와 같은 복잡한 생태계에서 연결성이 구현되는 것을 볼 수 있다. 완전 자율 주행이 추진되면서 차량은 그 어느 때보다 더 많이 연결되고 있지만, 소프트웨어 기반의 차량을 연결하는 것은 완전히 새로운 차원의 과제라고 할 수 있다.

본 가이드북에서는 성장하는 사이버보안과 관련된 보안 위협, 관련 이해관계자들을 위한 규정 준수를 용이하게 하는 방법에 대해 살펴본다. 일회성 구현이 아니라 기술이 궁극적으로 완전 자율주행을 지원하기 위해 변화하고 발전함에 따라 전체 모빌리티 생태계가 안전하게 유지되도록 보장하기 위한 포괄적이고 주기적인 접근 방식이 필수적이다.

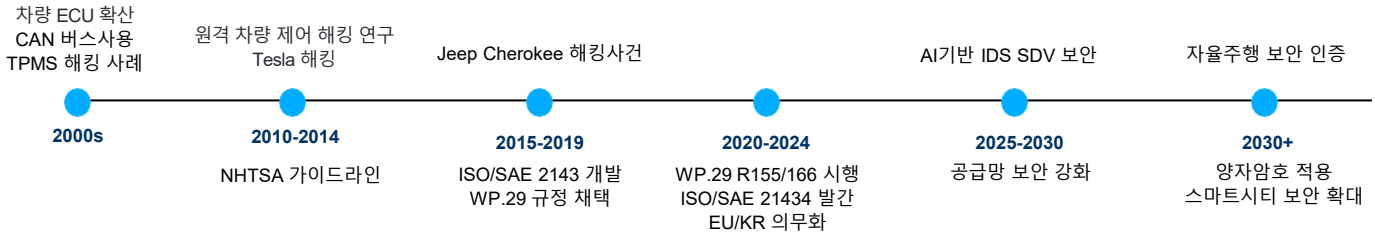
차량 사이버보안 발전

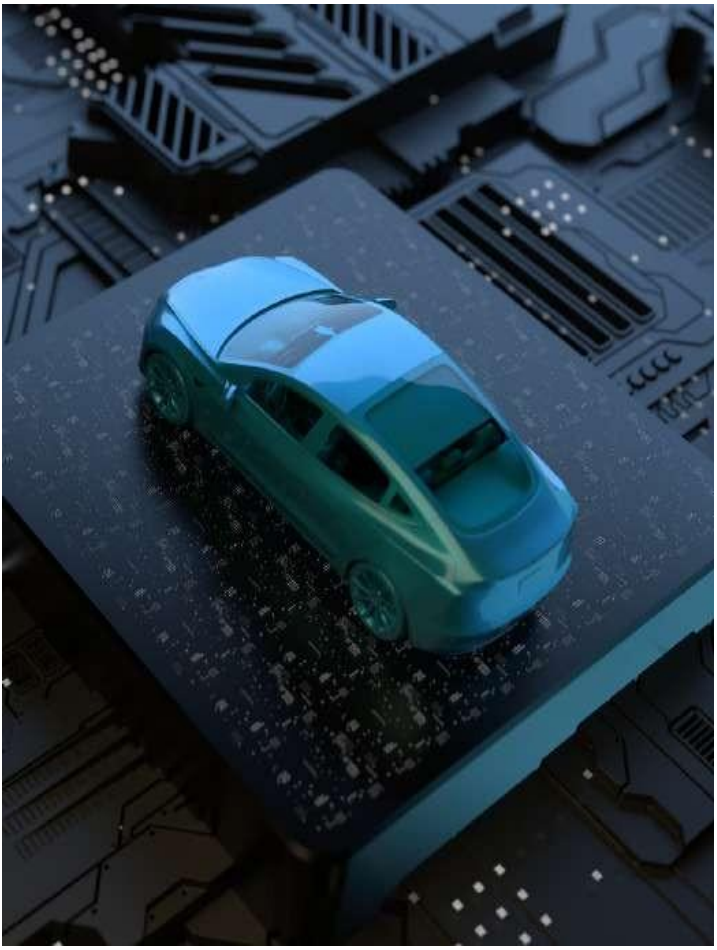
차량 기술

자동차의 역사를 통틀어 기술 발전은 빠르고 꾸준히 이루어졌다. 20세기에 들어와 많은 사람들이 자동차를 소유하는 것이 보편화되었고, 수요가 급증하면서 새로운 기능이 계속해서 추가되었다. 스마트 키, 라디오와 같은 기술적 발전과 전기차를 통한 탄소 배출 감소와 같은 혁신이 자동차 기술 역사에 큰 기여를 했다.

새로운 기술 기능은 운전자와 탑승자가 볼 수 있었지만 차량 내부에 숨겨진 기술에도 변화가 있었다. 1978년경 제너럴 모터스가 자동차에 처음으로 전자 시스템을 도입하면서 전자 제어 장치(ECU; Electronic Control Unit)의 역사가 시작되었다고 널리 알려져 있습니다.[1]

기본적으로 마이크로컨트롤러인 ECU는 차량의 전기 시스템과 하위 시스템을 제어할 수 있다. 각 ECU는 독립적인 노드로서 작동하면서, 네트워크 역할을 하기도 합니다. 이들은 더 큰 차량 네트워크 아키텍처에 기여하며 동시에 실행되는 수백만 줄의 코드를 포함한다. 따라서 자동차는 단순히 기계적인 작품에서 진정한 커넥티드의 의미를 가지는 변화를 겪고 있다.





2000년대 들어 차량에 전자제어장치(ECU)가 빠르게 확산되면서, 내부 네트워크인 CAN 버스가 본격적으로 사용되기 시작했다. 이 시기에는 타이어 공기압 모니터링 시스템(TPMS) 해킹과 같은 초기적인 공격 사례가 등장하며 차량 보안의 취약성이 드러나기 시작했다.

2010년대 초반에는 원격으로 차량을 제어할 수 있는 해킹 연구가 활발히 진행되었고, Tesla 차량 해킹 사례가 대표적인 사건으로 기록되었다. 이에 따라 미국 도로교통안전국(NHTSA)이 사이버보안 가이드라인을 발표하는 등 제도적 대응이 시작되었다.

2015년부터 2019년 사이에는 Jeep Cherokee 해킹 사건이 큰 충격을 주었다. 이 사건은 실제 도로 주행 중 원격으로 차량을 제어할 수 있었음을 보여주며, 업계와 규제 당국에 경각심을 불러일으켰다. 같은 시기 국제 표준 ISO/SAE 21434의 개발이 시작되었고, UN 산하 WP.29 규정이 채택되면서 차량 사이버보안에 대한 국제적 규범이 본격적으로 마련되기 시작했다.

2020년에서 2024년 사이에는 WP.29 R155/156 규정이 시행되었으며, ISO/SAE 21434가 공식 발간되었다. 유럽과 한국 등 주요 지역에서는 이 표준과 규정을 자동차 제조사에 의무화함으로써 법제화가 가속화되었다.

2025년부터 2030년까지는 자율주행차와 소프트웨어 정의 차량(SDV)의 확산을 고려한 보안 기술이 주목받을 전망이다. 특히 인공지능(AI) 기반 침입탐지시스템(IDS)이 도입되고, 글로벌 공급망 보안이 한층 강화될 것으로 예상된다

1. Moynahan, Nathan A., "Development of a vehicle road load model for ECU broadcast power verification in on-road emissions testing" (2005). Graduate Theses, Dissertations, and Problem Reports. 1675. https://researchrepository.wvu.edu/etd/1675.

커넥티드 카

바퀴 달린 슈퍼컴퓨터가 등장하면서 커넥티드 카에 연결성이 추가되는 것은 시간 문제였다. 본질적으로 커넥티드 카는 인터넷에 연결하여 차량과 연결되는 모든 엔드포인트 간에서의 데이터와 메시지를 공유한다.

Applications of V2X technology include:

- Collision avoidance
- Hazard warning
- Vulnerable road user (VRU) protection
- Emergency services support
- Intersection assistance
- Signal phase and timing (SPaT)
- Vehicle platooning
- Traffic data sharing

이로써 차량 기술은 완전히 새로운 가능성의 영역을 열었다. 이제 차량의 시스템(내장형 또는 연결형)은 스마트폰이나 컴퓨터처럼 메시지를 주고받고, 다른 장치와 연결하고, 애플리케이션을 활용할 수 있게 되었다.

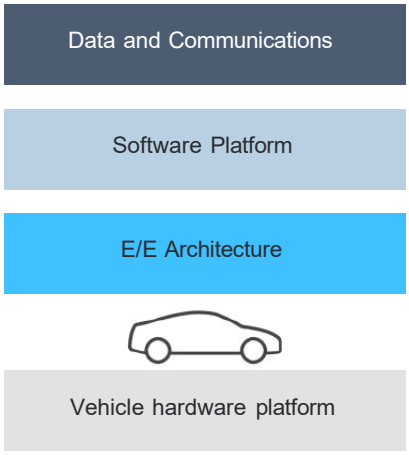
또한 연결성은 이제 자율주행의 가능성을 현실로 가져왔다. 수십 년 동안 공상 과학 소설과 미래 영화에서 묘사된 '자율주행' 차량은 이제 '만약'의 시나리오가 아닌 '언제'의 문제가 된 것처럼 보인다. 연결성이란 이제 차량이 V2X(Vehicle-to-Everything) 기술을 통해 다른 차량, 기기, 인프라 및 네트워크와 통신할 수 있다는 것을 의미한다. V2X 기술의 구현은 자율 주행, 나아가 보행자 안전을 위한 다양한 가능성을 열어준다.

V2X 기술은 실시간에 가까운 통신이 가능하기 때문에 차량은 물론 보행자나 자전거와 같은 도로 사용자도 이동 중인 차량과 직접 연결하여 서로의 위치 및 임박한 상황을 알릴 수 있다.

소프트웨어 중심 차량

많은 사람들이 자동차를 구매할 때 그 높은 가격에 대해 잘 알고 있다. 하드웨어 차량은 마력, 성능, 브랜드 가치에 따라 가격이 책정된다. 하지만 자동차 역사에서 보았듯이 자동차 기술은 끊임없이 진화하고 있다. 커넥티드 카의 다음 단계는 소프트웨어 중심 차량(SDV; Software-Defined Vehicle)이다. 이름에서 알 수 있듯이 '소프트웨어 중심 차량'은 주행 지원, 인포테인먼트 또는 주차 지원과 같은 다양한 기능을 소프트웨어로 구동하는 차량을 뜻한다.

자동차 산업과 차량 기술의 급격한 변화 속에서 소프트웨어 중심 차량은 업계의 판도를 바꾸고 있다. 그렇다면 구체적으로 어떤 차이를 가져오는 지에 대해 알아본다.



출처: Adapted version of Hyundai Motor Group "Software House", 2022.

운전자의 경우, SDV를 통해 차량을 더욱 맞춤화하고 편리하게 사용할 수 있다. 예를 들어, 차량 애플리케이션은 주문형 기능(FoD; Features on Demand)을 통해 그 자리에서 적용할 수 있으며, 정비소나 엔지니어를 방문해야 하는 번거로움 없이 '무선(OTA; Over-The-Air)'으로 업그레이드할 수 있다.

제조업체의 경우, 하드웨어 업그레이드나 값비싼 리콜 없이도 확장 가능한 배포가 가능해진다. 최적화된 사용을 위해 앞서 언급한 ECU는 이제 차량 내부에서 수집한 데이터를 활용하여 소프트웨어 제공업체와 차량 제조업체에 차량 모델의 수명 주기에 대한 정보를 제공할 수 있다.

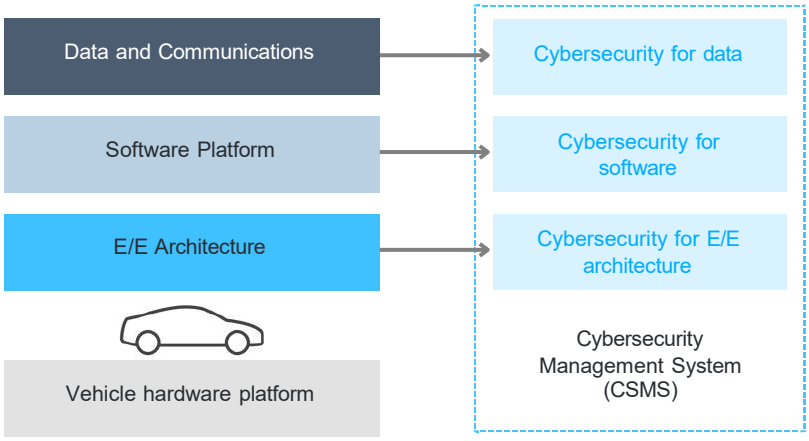
자동차 산업 전반의 경우, SDV는 본질적으로 차량의 하드웨어, E/E 아키텍처, 소프트웨어 및 데이터가 모두 함께 작동 및 최적화되고 업데이트되는 슈퍼컴퓨터로, 연결의 중심 역할을 한다.

도로에서의 소프트웨어 취약점

소프트웨어는 커넥티드 카의 기능을 더욱 깊이 있고 폭넓게 구현할 수 있게 해주지만, 동시에 차량에 보안이 필요한 영역을 확장시킨다. 이제 보안은 더 이상 하드웨어나 차량이 다른 차량과 통신하는 데 사용하는 데이터의 보안에 국한되지 않는다. 그렇다면 보안 측면에서 이는 정확히 무엇을 의미하는지에 대해 알아본다.

첫째, 많은 제조업체는 운전자가 원하는 다양한 소프트웨어 기반 플랫폼을 제공하기 위해 여러 소프트웨어 공급업체와 협력하고 있다. 이러한 다양성으로 인해 여러 공급업체와 각 공급업체의 개별 도구 및 보안 조치를 관리하기가 어려울 수 있다.

둘째, 앞서 언급한 차량의 하드웨어, E/E 아키텍처, 소프트웨어 및 데이터의 계층은 모두 전체 시스템을 보호하기 위해 함께 작동하는 서로 다른 보안을 필요로 한다.



소프트웨어 기반 운영 및 기능은 차량 환경과 관련된 연결 개체의 범위와 잠재적인 진입점을 확장하기 때문에 사이버 보안에 대한 철저한 접근 방식이 특히 중요하다. 예를 들어, SDV에서 다른 차량, 충전소, 모바일 디바이스 또는 도로변 장치로 연결할 수 있다.

커넥티드 카에서의 잠재적인 사이버 공격 진입점

- **OBD-II 포트**

  OBD(OnBoard Diagnostics)는 차량의 상태와 주행을 추적하며, 이러한 정보는 차량 운영자가 관리 및 유지보수를 하는 데에 활용된다. OBD-II 포트는 파워트레인, 배기가스 제어 시스템 및 기타 모든 종류의 주행 정보에 대한 액세스를 제공한다.

- **교통 인프라**

  소프트웨어 통신은 차량에만 국한되지 않는다. 이러한 통신은 도로변 장치와 네트워크 운영자까지 확장될 수 있으며, 이들은 데이터 분석, 자율주행 또는 모빌리티 서비스를 위해 이러한 메시지를 다른 엔드 엔티티에 전달한다.

- **헤드 유닛**

  차량의 헤드 유닛은 내부 시스템과 가장 가까운 진입점으로, 인포테인먼트 시스템에 서비스를 제공하는 메인보드 ECU와 애플리케이션 요청을 CAN 버스로 전달하는 게이트웨이 ECU가 포함되어 있는 경우가 많다. 해커가 헤드 유닛에 대한 액세스 권한을 얻는 경우, 한 단계만 거치면 차량을 장악할 수 있다.

- **스마트 키** *(모바일)*

  스마트키는 전자 신호로 차량의 잠금을 해제한다. 버튼식 키와 달리 스마트 키는 지속적으로 신호를 보내 키 없이도 차량에 탑승할 수 있다. 해커가 스마트키를 해킹하여 신호를 재설정하여 차량의 잠금을 해제하고, 시동을 거는 것 까지도 가능하다.

- **충전소**

  전기차가 도로에서 지속적으로 보급되고 있으며 충전소의 수도 계속 증가하고 있다. 충전소는 충전과 관련된 데이터를 수신하고 운영자 서버로 전송하므로 데이터에 대한 사이버 공격의 위험이 있다.

- **V2X 메시지**

  C-ITS 환경에서는 차량, 인프라, 보행자 등 도로 참여자 간에 V2X 메시지가 실시간으로 전송된다. 공격자는 이러한 메시지에 대해 스푸핑 공격을 시도하여 잘못된 판단을 유도하고 심지어 차량의 제어권을 넘기게 할 수도 있다.

규정 준수

더 많은 SDV가 도로에 등장함에 따라 소프트웨어 유형과 소프트웨어가 지원하는 연결은 계속 증가할 것이며, 이는 공급업체, 판매업체 등의 네트워크가 기하급수적으로 확장될 것임을 의미한다. 이는 차량이 시장에 출시되기 전에 제조업체와 공급업체가 숙지해야 하는 위험이다.

다른 유형의 보안 및 사이버 보안과 마찬가지로 이러한 종류의 취약점으로부터 보호하려면 여러 가지 접근 방식이 필요하지만, 모두가 일관된 보안 철학을 따라야 한다. 다행히도 입법자와 규제 당국은 차량 사이버 보안의 중요성을 인식하기 시작했으며 전 세계적으로 사이버 보안 규정과 표준을 도입하고 있다.

많은 사람들이 규정 준수를 초기에 제품 제조업체에 부여하는 인증서인 승인 표시를 일회성 거래로 생각하는 데 익숙해져 있다. 실제로 이러한 유형의 인증서는 존재하며, 전통적으로 차량은 시장에 출시되기 전에 형식 승인을 받는다. 규정은 어떤 차량이 시장에서 판매되고 도로에서 주행하기에 적합한지를 명시하며, 이 규정은 유엔 유럽 경제 위원회(UNECE; United Nations Economic Commission for Europe)에서 제정한다.

사이버 보안과 관련하여 국가마다 커넥티드 카의 보안 여부를 검증하는 규정과 표준이 다르다. 그러나 차량이 더욱 연결되고 소프트웨어 중심으로 변함에 따라 규정을 준수하는 것이 간단하지만은 않다. 실제로 많은 제조업체와 공급업체가 규정의 세부 사항을 파악하는 데 어려움을 겪고 있으며, 지역이나 솔루션에 따라 규정이 다를 경우 더욱 복잡해지는 경향이 있다.

우선, 한 번의 버튼 클릭으로 소프트웨어를 완전히 변경하여 무선(OTA; Over-The-Air) 업데이트를 실행할 수 있는 것이 SDV의 특징이다. 그러나 이 업데이트는 실제로 차량의 여러 기능에 영향을 미칠 수 있으므로 한 시점의 유효성 검사가 다른 시점의 차량에는 적용되지 않을 수 있다.

다음으로, 업계가 발전함에 따라 끊임없이 진화하는 보안 위협으로부터 차량을 안전하게 보호해야 하는 근본적인 문제가 항상 존재한다.

UNECE WP.29

이러한 우려를 해결하기 위해 2021년 UNECE 산하의 차량규정의 일치화를 위한 세계포럼(WP.29; The World Forum for Harmonization of Vehicle Regulations)은 형식 승인에 사이버 보안 요소를 추가하는 두 가지 새로운 규정을 발표했다.[2] 이는 국제적으로 차량에 대한 사이버 보안 규정이 처음으로 제정된 것으로, 업계에 있어 중요하고 역사적인 움직임으로 평가받았다.

R155와 R156이라는 두 가지 규정을 통해 1958년 차량에 관한 협정에 가입한 54개국은 2022년까지 이 규정을 이행하도록 의무화되었다. 원래 협정에 참여하지 않은 주요 국가도 있지만, 업계의 국제적 특성으로 인해 운영을 계속하려면 규정을 준수하지 않을 수 없게 되었다.

2. UNECE. (2020, June 24). UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles . UNECE. Retrieved December 5, 2022, from https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll.

Autocrypt는 현재 포괄적인 WP.29 규정 준수 프로그램을 제공하며, 이 프로그램은 컨설팅, 차량 내 시스템 보안 솔루션 구현, 그리고 각 단계가 올바르게 완료되었는지 확인하기 위한 공격 및 방어 테스트로 이루어진 3단계 프로세스로 구성되어 있다.

> Both the standard and regulation look at securing the entire lifecycle of the vehicle – from vehicle production to post-production.

ISO/SAE 21434

WP.29의 규정과 별도로 ISO/SAE 21434는 국제 표준화 기구(ISO)와 국제 자동차 기술자 협회(SAE)가 공동으로 개발하였다. 이 표준은 오랜 작업 끝에 "Road Vehicles – Cyber Security Engineering" [3] 이라는 제목으로 2021년 8월에 공식 발표되었다.

WP.29 규정과 ISO/SAE 21434 표준은 크게 다르지 않다. 표준과 규정 모두 차량 생산부터 생산 후까지 차량의 전체 수명 주기에 대한 보안을 확보하는 데 중점을 두고 있다. 이러한 지침은 보안을 일회성 해결책이 아닌 프로세스로 간주하여 전반적인 보안을 다루게 된다.

WP.29 규정과 ISO/SAE 21434 표준의 차이점

WP.29 규정은 원래 협약에 서명한 54개국에 대해 법적 구속력이 있는 반면, ISO/SAE 21434는 각각의 기업이 준수 여부를 직접 정할 수 있는 국제 표준이다. 그러나 표준을 준수하고 공식적인 규정 준수 인증을 받으면 해당 제조업체 또는 공급업체가 고객과 파트너를 보호하는 데 주력하고 있다는 사실을 강조할 수 있다.

이 둘은 상호 배타적인 것이 아니며 상호 보완적으로 사용하는 것이 이상적이다. 그러나 WP.29 규정과 마찬가지로 제조업체와 공급업체, 특히 사이버 보안 아키텍처와 차량 내 하드웨어 및 소프트웨어의 보안을 보장하기 위한 접근 방식에 익숙하지 않은 경우 표준을 파악하기 어려울 수 있다.

3. International Organization for Standardization. (2021). Road vehicles—Cybersecurity engineering (ISO Standard No. 21434:2021). https://www.iso.org/standard/70918.html

규정 준수를 위한 체크리스트

UNECE WP.29 워킹 파티에 따르면, 제조업자들과 공급망과 관련된 업체들은 다음의 규정들을 준수하는 것을 보장해야 한다.

CYBER SECURITYMANAGEMENT SYSTEMS (CSMS)

자동자 산업/부문

- ☑ 차량의 설계 단계에서 사이버 보안 위협을 식별하고 관리
- ☑ 시험을 포함하여, 리스크가 관리되고 있음을 검증
- ☑ 리스크 평가를 최신으로 유지
- ☑ 사이버 공격을 감시하고 효과적으로 공격에 대응
- ☑ 성공한 또는 시도된 공격의 분석을 지원
- ☑ 새로운 위협과 취약점에 대해 사이버 보안 조치가 여전히 유효한지 평가

제조업체

- ☑ CSMS가 구축되어 있으며, 이를 도로 위의 차량에 적용가능
- ☑ 리스크 평가 분석을 제공하고 무엇이 치명적인지 식별

  식별된 리스크를 감소하기위한 완화 조치
- ☑ 완화 조치가 의도한대로 작동하는지 근거 제시
- ☑ 사이버 공격을 탐지 및 예방하고 데이터 포렌식을 지원하기 위한 조치 마련 확인
- ☑ 차량 종류 별 활동 모니터링
- ☑ 모니터링 활동에 대한 보고서를 관련 승인 기관에 전송

SOFTWARE UPDATE MANAGEMENT SYSTEMS (SUMS)

자동자 산업/부문

- ☑ 차종 별 하드웨어/소프트웨어 버전 기록
- ☑ 차종 승인과 관련한 소프트웨어 식별
- ☑ 컴포넌트에서 동작하는 소프트웨어 검증
- ☑ 특히, 소프트웨어 업데이트와 관련한 상호의존성 식별
- ☑ 목표 차량을 식별하고 업데이트와 호완성을 검증
- ☑ 소프트웨어 업데이트가 차종 승인 또는 법적으로 정의된 매개 변수에 영향을 미치는지 평가(기능 추가/제어 포함)
- ☑ 업데이트가 안전 또는 운전에 영향을 끼치는지 평가하고 업데이트한 차량의 소유주에게 알림

제조업체

- ☑ SUMS가 구축되어 있고 이를 도로 위 차량에 적용 가능
- ☑ 소프트웨어 업데이트 전달 메커니즘을 보호하고 무결성과 인증을 보장
- ☑ 소프트웨어 식별 숫자 보호
- ☑ 소프트웨어 식별 숫자가 차량이 읽을 수 있음을 보장

OVER- THE - AIR (OTA) SOFTWARE UPDATES

- ☑ 업데이트 실패시의 복구기능
- ☑ 공급될 때만 업데이트 실행
- ☑ 안전한 실행 보장
- ☑ 각 업데이트와 그들의 완료에 대해서 사용자에게 알림
- ☑ 차량이 업데이트를 수행할 수 있음을 보장
- ☑ 정비공이 필요할 때 사용자에게 알림

포괄적인 사이버 보안 관리

소프트웨어 기반의 차량은 독특하다.

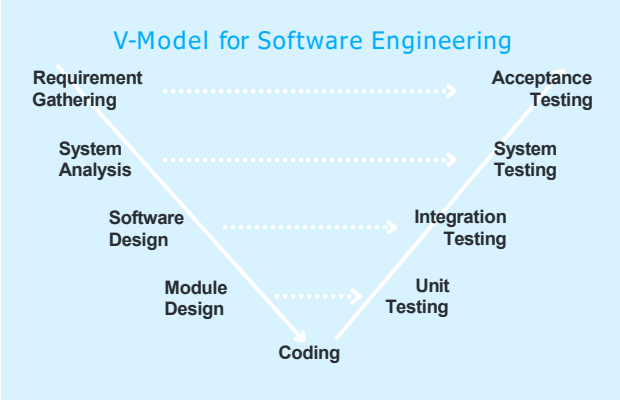
특히 서로 다른 표준과 요구사항으로 작동하는 여러 공급업체의 소프트웨어가 포함될 가능성이 높다는 점에서 그렇다고 할 수 있다. 이러한 환경을 파악하고 보호하려면 종합적인 솔루션이 필요하다.

기술 및 산업 전반의 발전적인 특성으로 인해 제조업체와 공급업체는 차량 보안의 기본뿐만 아니라 의무 규정 및 업계에서 인정하는 표준을 준수하고 입증된 방어 및 공격 방법을 사용한 테스트를 통해 차량의 보안을 유지할 수 있는 포괄적인 사이버 보안 솔루션을 찾도록 권장되고 있다.

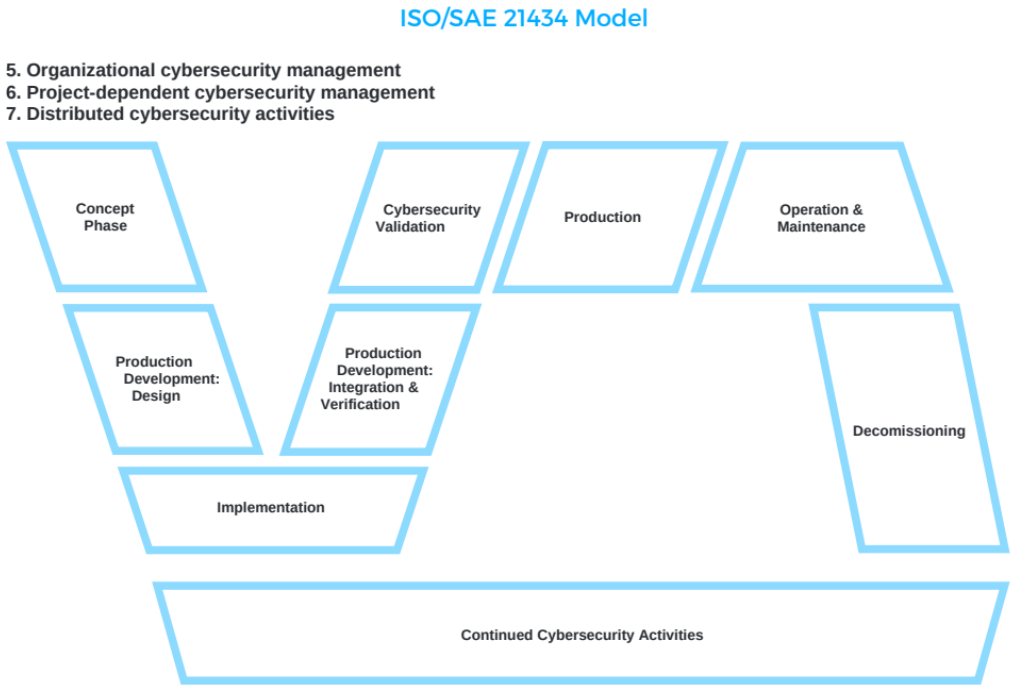
V Model

V 모델은 전통적으로 개발된 소프트웨어 엔지니어링 모델이다. "검증 및 유효성 검사 모델"이라고도 하는 이 표준은 1980년대에 Paul Rook에 의해 개발되었으며[4], 선형적이지 않은 일련의 프로세스를 따르며, 관련 테스트 단계에 중점을 두고 있다.

반복적으로 위험을 감소시키는 특성으로 인해 ISO/SAE 21434 표준은 차량 사이버 보안의 기초로 V 모델을 사용하고 있다.



ISO/SAE 21434는 표준의 요구 사항을 정의하는 조항으로 구성되어 있다. 5장부터 7장까지는 일반적인 사이버 보안 관리 방법을 다루고, 8장부터는 차량 보안을 위한 구체적인 접근 방식에 대해 설명하고 있다.



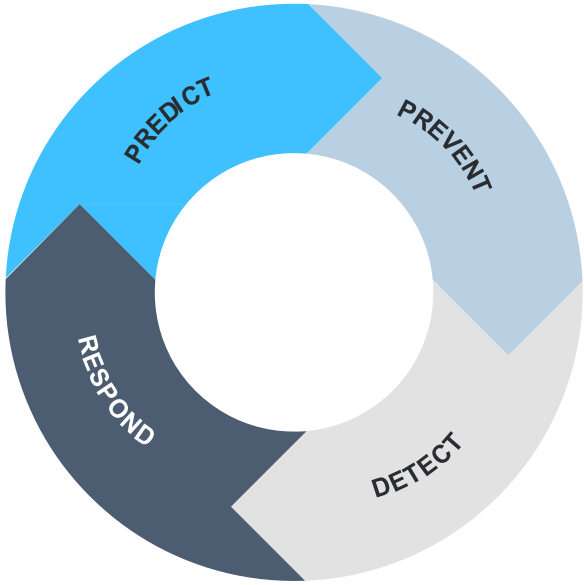
4. Rook, P. (1986). Controlling software projects. Software Engineering Journal, 1(1), 7–16. https://doi.org/10.1049/sej.1986.0003

자동차 사이버 보안에서 가장 어려운 부분 중 하나가 바로 차량이 통합 운영 체제에서 실행되지 않는다는 것이기 때문에 이 모델은 복잡한 성격을 가진다. 대신 차량은 수백 개의 고유한 ECU로 구성되어 있으며 CAN(Controller Area Network) 버스를 통해 상호 운용되므로 프로세스에 대한 전체적인 개요를 파악하면 보안에 대한 요구 사항을 훨씬 쉽게 이해할 수 있다.

이를 좀 더 간단히 이해하기 위해 차량의 전체 수명 주기를 네 가지 반복되는 단계로 나누어 살펴볼 수 있다.

1. 위험 예측
2. 솔루션을 통한 위험 방지
3. 솔루션, 기타 검증 및 유효성 검사를 통한 위험 감지
4. 위험 및 사고 대응

이러한 단계들은 반복적으로 진행되기 때문에 순환적인 성격을 가지며, 따라서 4단계가 완료되면 프로세스가 다시 반복된다.



네 단계에 해당하는 사이버 보안을 구현하기 위해 제조업체와 공급업체가 취할 수 있는 조치의 범주는 다음과 같다:

- 컨설팅 및 TARA
- 차량 내 시스템 보안 구현
- 검증 및 유효성 검사
- 사고 보고

다음은 각각의 카테고리에 대한 자세하게 살펴본다.

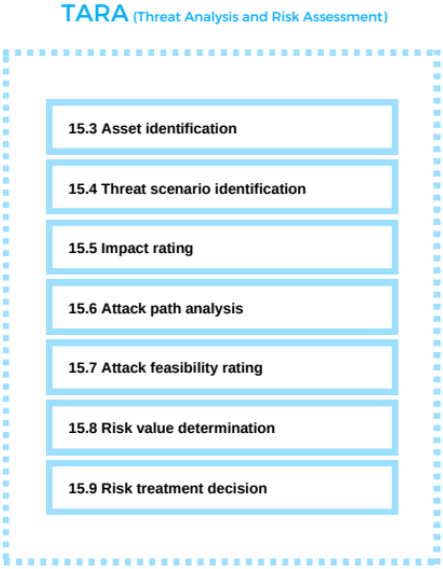


그림: TARA methods for ISO/SAE 21434

컨설팅 및 TARA

1967년형 쉐보레 임팔라 같은 클래식카를 떠올려 보자. 자동차 애호가라면 엔진, 부품의 종류, 차량의 상태를 먼저 파악하지 않고는 기계에 손을 대지 못할 것이다.

이와 마찬가지로 보안을 구현하기 전에 기존 시스템에 대한 손상을 방지하기 위해 철저한 검토와 평가가 필요하다. 커넥티드 차량에서 보안 구현 프로세스의 이 단계는 TARA(Threat Analysis and Risk Assessment)라고 하는 방법론이다.

ISO/SAE 21434와 같은 표준의 핵심 구성 요소인 TARA는 차량 아키텍처에 대한 심층 분석을 기반으로 사이버 보안 위험을 평가하는 데 업계에서 널리 사용되고 있다. 위험을 철저히 평가한 후 보안 엔지니어는 위험을 완화하기 위해 필요한 대응 조치의 목록과 순서를 선택할 수 있다.

분석가는 시간, 접근성, 장비와 같은 위험 요소뿐만 아니라 취약점 목록을 사용하여 알려진 취약점과 알려지지 않은 취약점을 찾고 위험의 예상 실현 가능성을 도출한다. 이를 통해 보안팀은 '위험 처리 결정(Risk Treatment Decision)'을 내리거나 해당 차량에 필요한 보안 시스템을 설정하기 위한 일종의 지침 역할을 하는 충분한 정보를 얻을 수 있다.

차량 내 시스템 보안 구현

차량의 내부 시스템은 60~100개의 ECU로 구성되며, 각 ECU는 해당 SDV의 다양한 하위 시스템과 기능을 제어한다.

ECU는 일반적으로 사용되는 네트워크 프로토콜인 CAN 버스를 통해 서로 통신한다. CAN 네트워크는 이러한 ECU가 단일 호스트 서버 없이 통신할 수 있도록 설계되었지만, 구축 당시 통신 메시지의 출처를 추적하려는 목적이 없었기 때문에 차량 내 시스템은 외부 위협 및 공격자로부터 취약할 수 있다.

메시지 위조, 무작위 악성 CAN 패킷, 데이터 유출 등은 보안 조치가 충분하지 않은 차량에서 발생할 수 있는 위험 요소 중 일부에 불과할 정도이므로 차량 내 시스템 보안은 필수적이다.

그러나 특히 SDV의 경우 보안 적용은 바이러스 백신 설치만큼 간단하지 않다. 솔루션 제공업체와 제조업체는 외부 네트워크에서 내부 네트워크에 이르기까지 차량의 각 계층과 시스템을 보호하기 위해 협력해야 하며, 이를 위해 여러 가지 요소를 고려해야 한다.

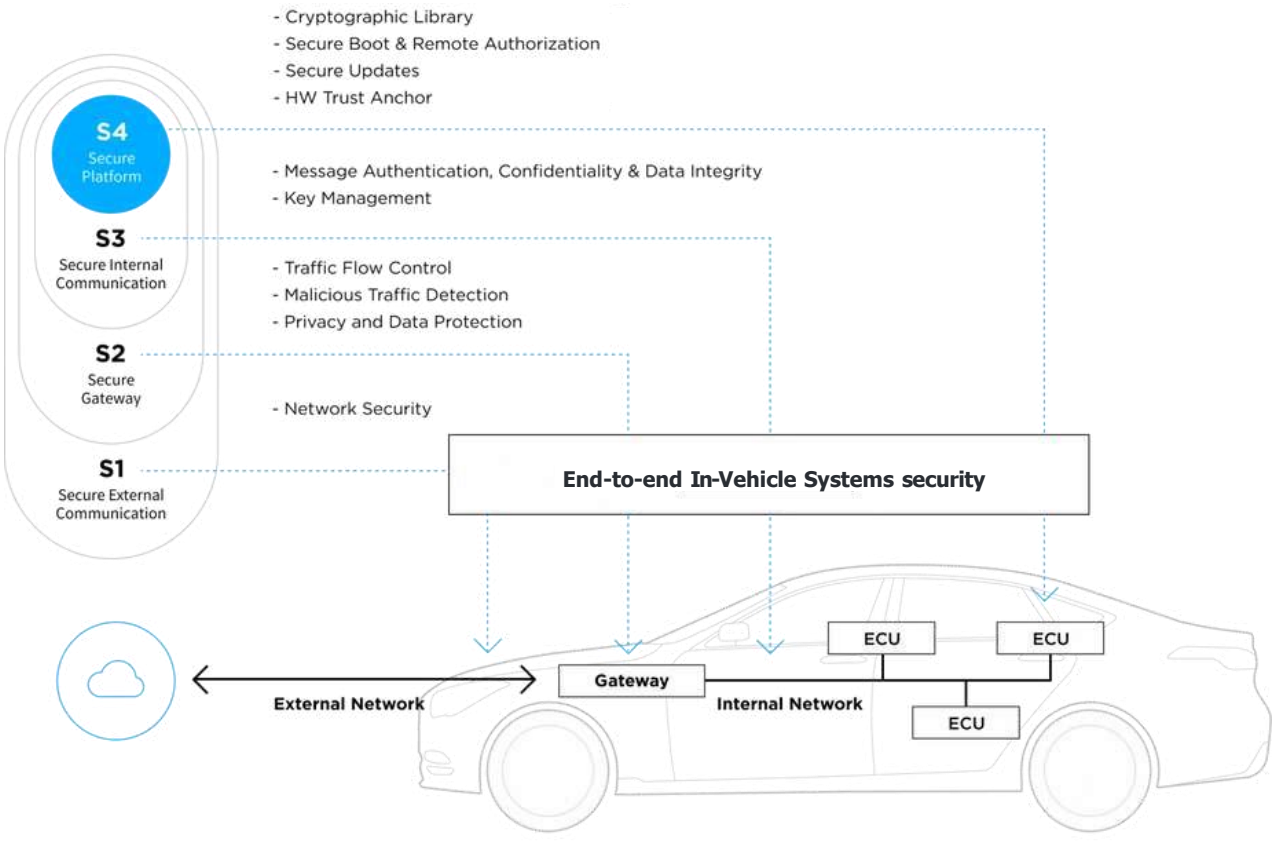


그림: Layers of security and related offerings by Autocrypt

검증 및 유효성 검사

구현은 사이버 보안의 필수적이고 중요한 부분이지만, 여러 차례 검증되고 확인되지 않는 한 보안은 완성되지 않는다.

> Verification and validation are both vital to ensuring that the solution at hand is working properly

Verification vs. Validation

검증(Verification)은 소프트웨어 또는 하드웨어가 문제없이 의도한 바를 달성하는지 확인하는 과정을 뜻한다. 제품이 고객의 요구 사항을 충족하는지 여부를 확인하는 것으로, 코드를 실행하지 않기 때문에 정적 테스트(static testing)로 간주된다.

반면에 유효성 검사(Validation)는 제품의 품질과 높은 수준의 요구 사항을 충족하는지 여부를 확인하는 것으로, 코드 실행을 포함하며 동적 테스트(dynamic testing)로 간주된다.

검증(Verification)과 유효성 검사(Validation)는 현재의 솔루션이 제대로 작동하는지 보장하는 데 중요한 역할을 한다.

Types of Testing

Vulnerability Scanning	• **Software static testing**: 초기 개발 단계에서 누수, 버퍼 오버플로우 및 표준 편차와 같은 주요 문제를 찾아내어 개발 시간을 단축한다. • **Software dynamic testing**: 런타임 환경에서 코드를 실행하여 동적 변수의 동작 및 보안 취약점을 테스트한다.
Fuzz Testing	• 유효하지 않거나 임의의 데이터(fuzz)에 대한 테스트를 통해 충돌, 메모리 누수 및 실패한 코드를 모니터링한다. 퍼징은 정의되지 않은 동작을 활용하여 예기치 못한 숨겨진 버그를 발견하므로 비용 대비 효과가 높다.
Penetration Testing	• 알려진 취약점과 사이버 공격 방법을 활용하여 하드웨어, 소프트웨어 및 서비스의 조합에 대한 공격을 시뮬레이션하고, 위협 데이터베이스를 통해 다양한 수준의 취약점을 활용하여 공격 테스트를 진행한다.

사고 보고

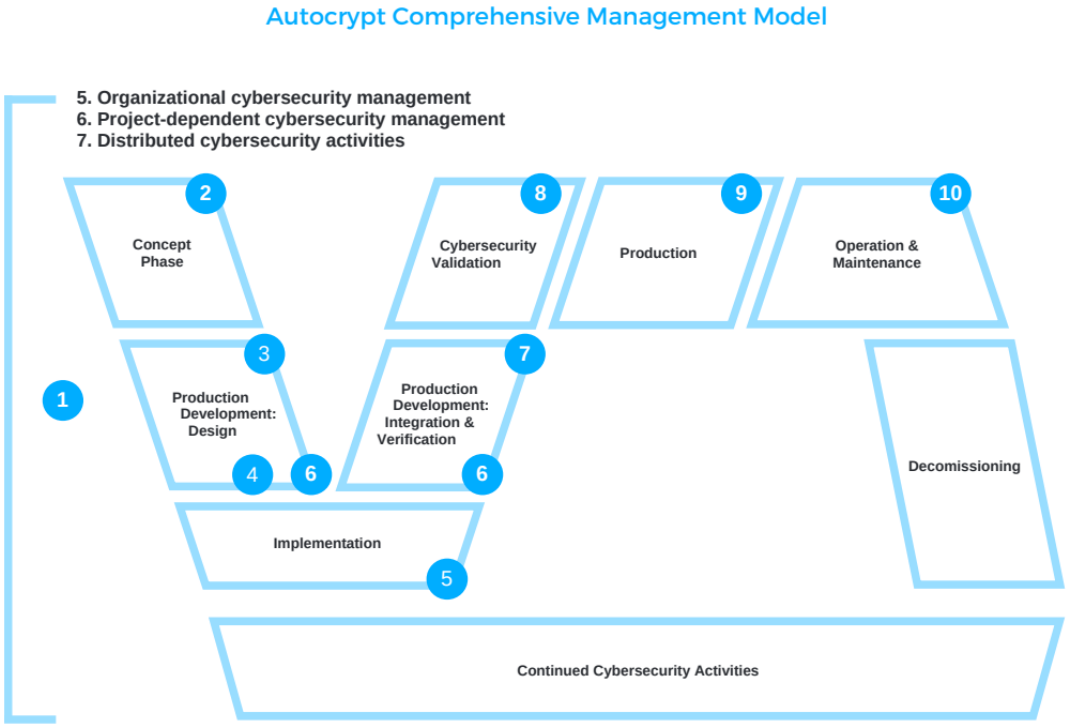
사이버 공격을 예방하는 과정에서 사고가 발생했을 때 대응책을 마련하고, 문제를 개선 및 수정하고, 사고의 원인을 분석하고, 보안 취약점과 위협을 지속적으로 검토해야 한다.

많은 제조업체는 24시간 내내 사고를 모니터링하는 차량 보안 운영 센터를 운영한다. 이 센터는 자체 또는 외부 아웃소싱 팀으로 구성될 수 있으며, 연중무휴로 차량 시스템을 모니터링하기 위해 맞춤형 플랫폼을 활용한다.

AUTOCRYPT 제공 서비스

앞서 언급했듯이 여러 공급업체와 협업하는 경우 보안을 위한 솔루션 구현 프로세스가 매우 세분화되어 관리가 어려워질 수 있다. 이러한 문제를 해결하기 위해 Autocrypt는 제조업체와 공급업체를 지원하기 위한 V 모델의 시작부터 마지막까지의 맞춤형 지원과 구현을 제공하여 규정 준수를 보장하는 대안을 제공한다. 이를 통해 제조업체와 공급업체는 생산 전 단계부터 출시 후까지의 투명성을 강화할 수 있다.

Autocrypt는 ISO/SAE 21434의 각 단계 및 WP.29 규정에 대응하여 해당 서비스 및 컨설팅 서비스를 제공한다.



Autocrypt Solutions Offerings

1. CSMS / ISO 21434 consulting
2. TARA (Threat Analysis and Risk Assessment)
3. OEM requirement analysis
4. Security design & engineering
5. Security solution implementation (porting, customizing)
6. Vulnerability analysis and management
7. Fuzzing test
8. Penetration test
9. Incident response
10. Production-line integration

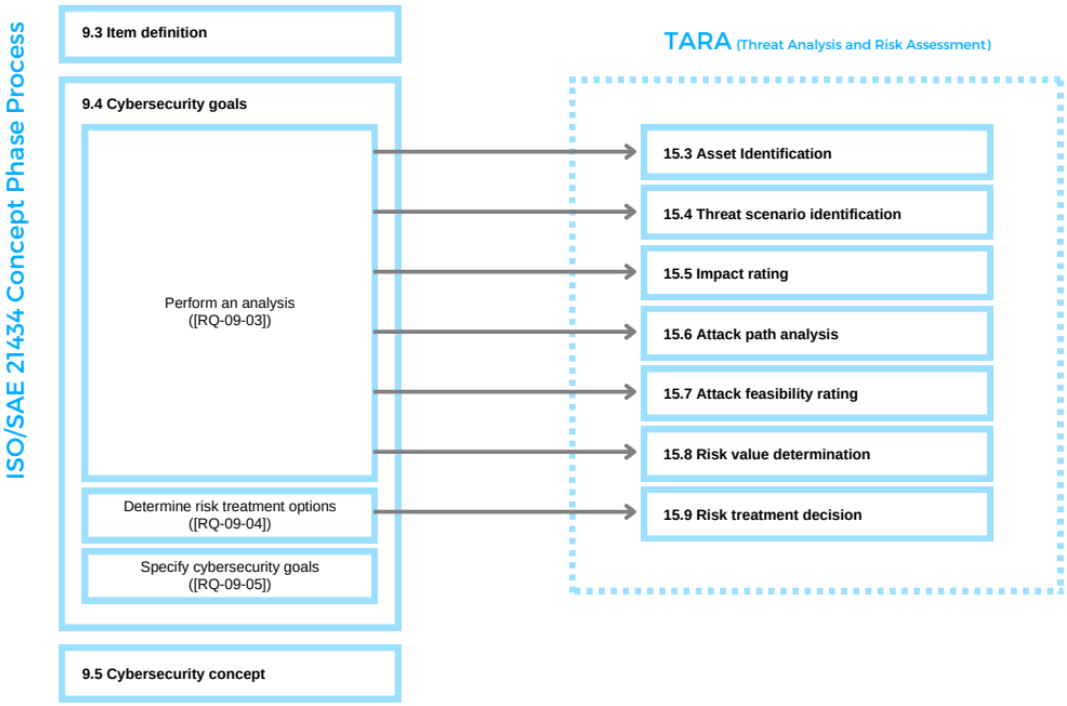
규정 준수 프로세스에는 많은 구성 요소가 있지만, Autocrypt는 각 파트너와 협력하여 모든 단계를 포괄적으로 진행하고 제조업체의 특정 요구에 따라 솔루션을 맞춤화한다. 백서의 다음 부분에서는 Autocrypt의 제품에 대해 자세히 살펴본다.

1 CSMS / ISO 21434 consulting

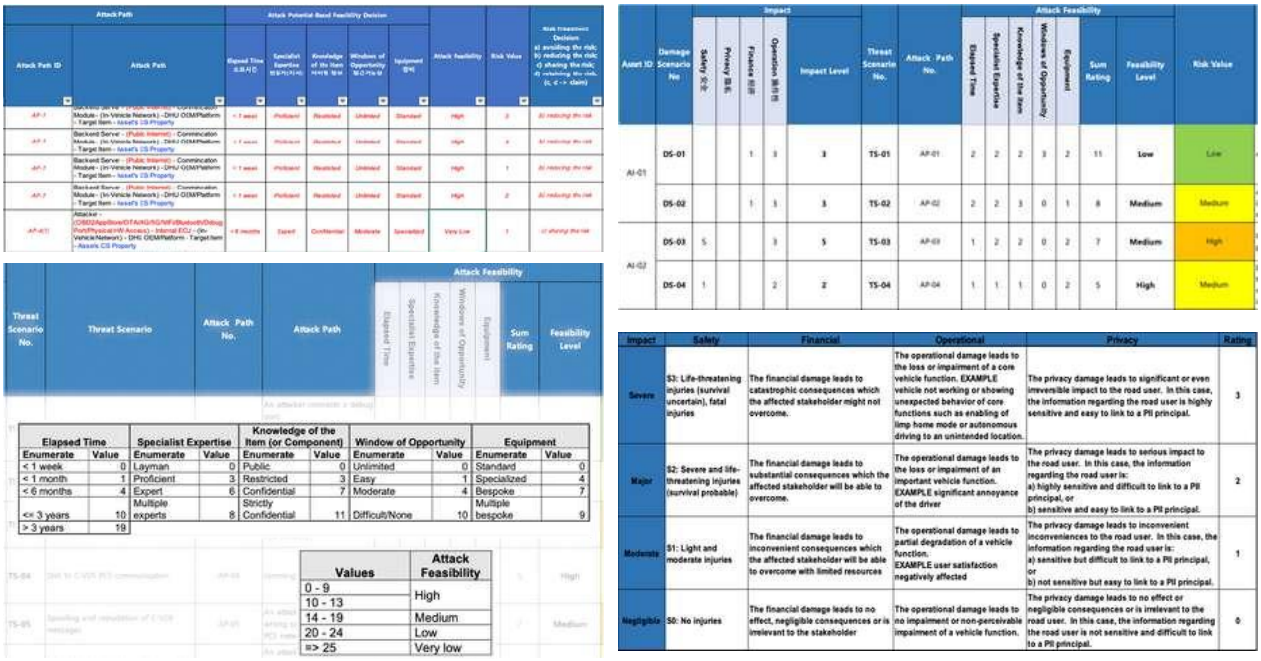
Autocrypt는 사이버 보안 관리 체계(CSMS) 구축과 WP.29의 R155, R156 규정 및 ISO/SAE 21434 표준 준수를 위한 전문 컨설팅 서비스를 제공한다.

2 TARA (Threat Analysis and Risk Assessment) & 3 OEM requirement analysis

컨셉 단계의 일부인 TARA 프로세스는 보안 전문가와 제조업체 모두에게 보안 관리 시스템 구현에 대한 명확한 방향을 제시한다.



각 OEM에는 고유한 아키텍처 설계와 해당 요구 사항이 있으며, Autocrypt는 각 고객과 협력하여 철저한 분석을 수행한 후 결과에 대한 맞춤형 종합 보고서를 제공한다.



Elapsed Time		Specialist Expertise		Knowledge of the Item (or Component)		Window of Opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
< 1 week	0	Layman	0	Public	0	Unlimited	0	Standard	0
< 1 month	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
< 6 months	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
<= 3 years	10	Strictly Multiple experts	8	Strictly Confidential	11	Difficult/None	10	Multiple bespoke	9
> 3 years	19								

Values	Attack Feasibility
0 - 9	High
10 - 13	
14 - 19	Medium
20 - 24	Low
=> 25	Very low

Impact	Safety	Financial	Operational	Privacy	Rating
Severe	S3: Life-threatening injuries (survival uncertain), fatal injuries	The financial damage leads to catastrophic consequences which the affected stakeholder might not overcome.	The operational damage leads to the loss or impairment of a core vehicle function. EXAMPLE vehicle not working or showing unexpected behavior of core functions such as enabling of limp home mode or autonomous driving to an unintended location.	The privacy damage leads to significant or even irreversible impact to the road user. In this case, the information regarding the road user is highly sensitive and easy to link to a PII principal.	3
Major	S2: Severe and life-threatening injuries (survival probable)	The financial damage leads to substantial consequences which the affected stakeholder will be able to overcome.	The operational damage leads to the loss or impairment of an important vehicle function. EXAMPLE significant annoyance of the driver	The privacy damage leads to serious impact to the road user. In this case, the information regarding the road user is: a) highly sensitive and difficult to link to a PII principal, or b) sensitive and easy to link to a PII principal.	2
Moderate	S1: Light and moderate injuries	The financial damage leads to inconvenient consequences which the affected stakeholder will be able to overcome with limited resources	The operational damage leads to partial degradation of a vehicle function. EXAMPLE user satisfaction negatively affected	The privacy damage leads to inconvenient inconveniences to the road user. In this case, the information regarding the road user is: a) sensitive but difficult to link to a PII principal, or b) not sensitive but easy to link to a PII principal.	1
Negligible	S0: No injuries	The financial damage leads to no effect, negligible consequences or is irrelevant to the stakeholder	The operational damage leads to no impairment or non-perceivable impairment of a vehicle function.	The privacy damage leads to no effect or negligible consequences or is irrelevant to the road user. In this case, the information regarding the road user is not sensitive and difficult to link to a PII principal.	0

Figures: Post-TARA analyses reports (sample only)

4 Security design & engineering

컨설팅 및 평가 단계 이후에는 시스템 설계, 구현 및 검증 절차가 진행되는 프로세스의 주요 부분이 진행된다.

Autocrypt는 보안 부팅, 액세스 제어, 파일 시스템 암호화는 물론 호스트 IDPS, 방화벽, CAN-IDS/Ethernet-IDS 등 포괄적인 사이버 보안 시스템을 구현할 수 있는 제품군을 개발하였다.

하지만 앞서 언급했듯이 사용자 정의가 핵심으로, Autocrypt는 각 파트너 및 고객과 협력하여 특정 요구 사항을 충족하는 적절한 제품 조합을 설계하는 데 도움을 제공한다.

	Category	OEM requirements	HSM	TrustZone API	ASK API	Firewall	SMACK	dm-crypt	App Security	OS hardening	Pen/Fuzz Test	Static/ dynamic test
1	MCU	Secure Flash	✓		✓						✓	
2		ASK			✓							
3		HSM	✓									
4		HW	✓	✓								
5		SW		✓								✓
6		Secure Flash		✓								
7		HSM(TrustZone)	✓	✓								
8		OS								✓		
9	CPU (AP)	Secure Algorithm	✓	✓								
10		Firewall				✓	✓					
12		Communications				✓						
13		Personal Data Protection	✓	✓				✓				
14		File System Encryption		✓				✓				
16		OS security								✓		
17		Mobile app security							✓			
18		SMACK					✓					
19	Non Functional	TARA										
20		Security evaluation										✓
21		Pen testing									✓	
22		OSS vulnerability analysis										✓
23		Fuzz testing									✓	

Figure: Security design & engineering items (sample only)

5 Security solution implementation

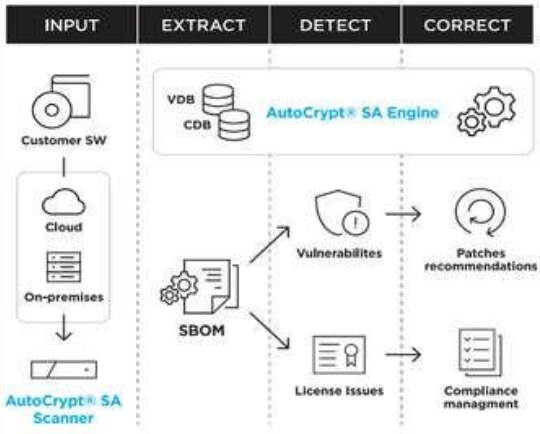
AutoCrypt IVS는 ECU에 대한 강화된 보안 및 모니터링을 제공하며, 내부 및 외부 통신에서 이상행동과 공격 시도를 탐지한다.

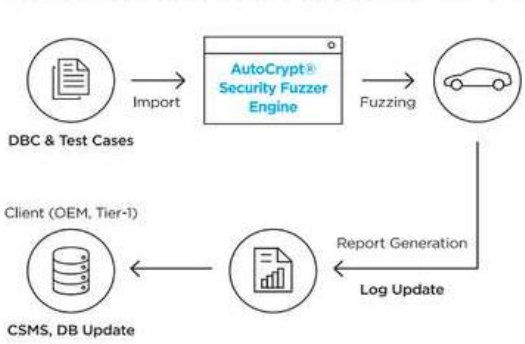
Autocrypt는 파트너와 협력하여 차량 내 시스템을 포괄할 수 있는 적절한 솔루션 조합을 구현한다.

	Autocrypt Solutions	AP	MCU+HSM	MCU	GW/CCU
1	Secure Boot	O	O	O	O
2	Secure Flashing (OTA Client)	O	O	O	O
3	HW-based Crypto Lib.	O	O	-	O
4	SW-based Crypto Lib.	-	O	O	-
5	Access Control	O	-	-	-
6	File System Encryption	O	-	-	-
7	Host IDPS & Firewall	O	-	-	O
8	CAN-IDS / Ethernet-IDS	-	-	-	O
9	Etc. (customizing tool)	O	O	O	O

6 Vulnerability analysis and management

Autocrypt는 취약점을 철저히 검사하기 위해 차량용 오픈 소스 소프트웨어(OSS; Open-Source Software)의 취약점을 탐지하고 관리하는 AutoCrypt Security Analyzer를 개발하였다. 이 도구는 소프트웨어 개발 수명 주기(SDLC; Software Development Life Cycle)의 모든 단계에서 구현할 수 있는 소프트웨어 구성요소 명세서(SBOM; Software Bill Of Materials)에 구성 요소를 정확하게 식별, 분류 및 나열한다.





7 Fuzzing

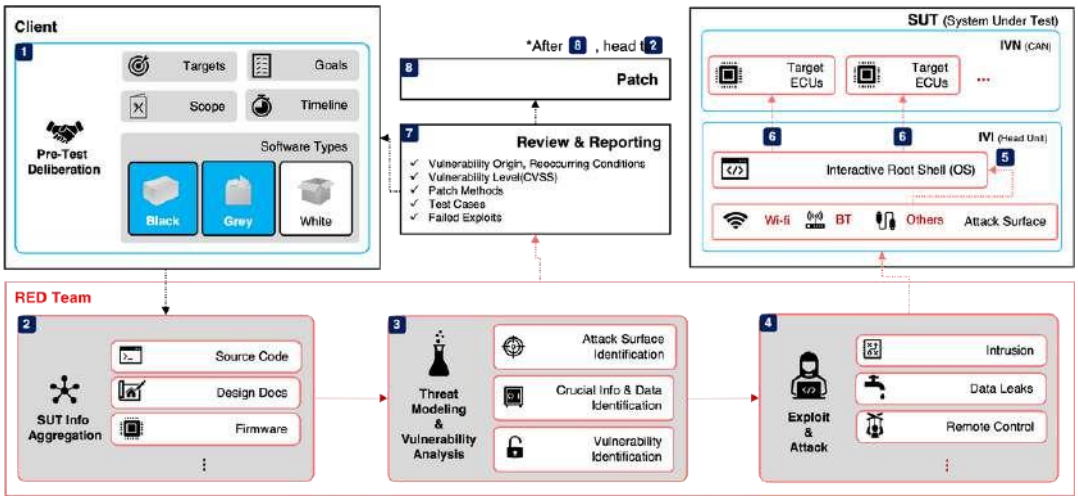
Fuzz 테스트는 대상 프로그램에 무작위/준무작위(random/semi-random) 입력 데이터를 주입하여 숨겨진 코딩 오류를 찾아내는 자동화된 소프트웨어 테스트 기법이다. AutoCrypt Security Fuzzer는 이 프로세스를 빠르고 효율적으로 수행하여 최소한의 시간으로 최대의 결과를 얻을 수 있다.

8 Penetration test

Autocrypt의 침투 테스트(penetration testing) 또는 "pentesting"은 수상 경력을 가진 사내 레드 팀에 의해 지원된다. 레드 팀은 숙련된 전문 해커들로 구성되어 있으며, 공격 시나리오를 설계하고 시스템의 약점과 취약점을 발견하기 위해 공격 시나리오를 수행한다.

그림 (오른쪽): Autocrypt Red Team comes in first place in 2021 Cyber Security Challenge, hosted by the Ministry of ICT, Seoul, Korea.

(아래): Autocrypt Red Team cycle process for pen-testing with client.



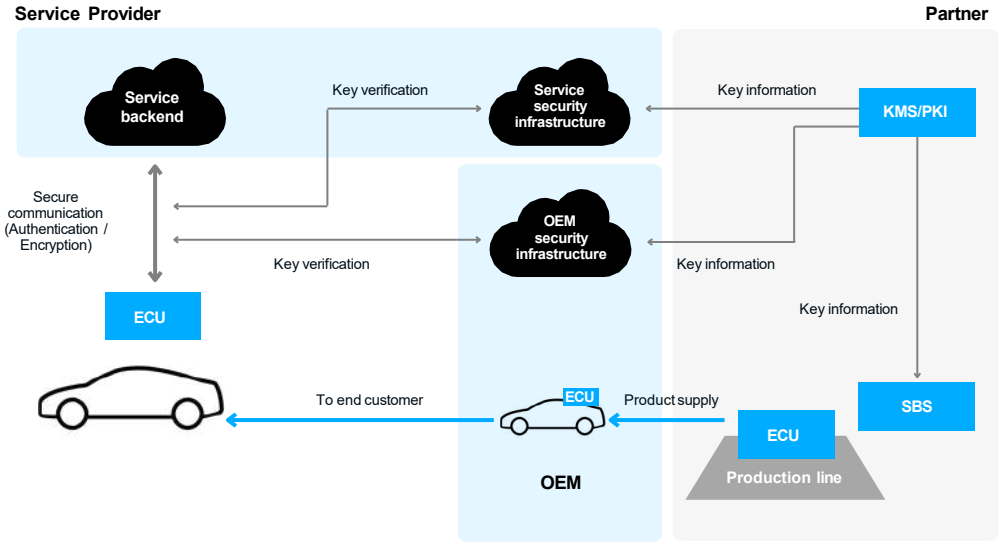
9 Incident response

AutoCrypt vSOC는 차량 생산 후 관리를 위해 다른 차량 내 시스템 보안 솔루션과 함께 제공된다. 이 플랫폼은 직관적이고 탐색하기 쉬운 사용자 인터페이스를 제공하며, 제조업체는 실시간으로 위협 인텔리전스에 대한 정보를 얻을 수 있다.

그림: vSOC user interface (sample)

10 Production-line integration

생산 단계에서, Autocrypt는 키 관리 시스템과 공개 키 인프라(PKI; Public Key Infrastructure), 보안 부트스트랩(SBS; Secure BootStrapping)을 포함한 서버 솔루션을 제공한다.



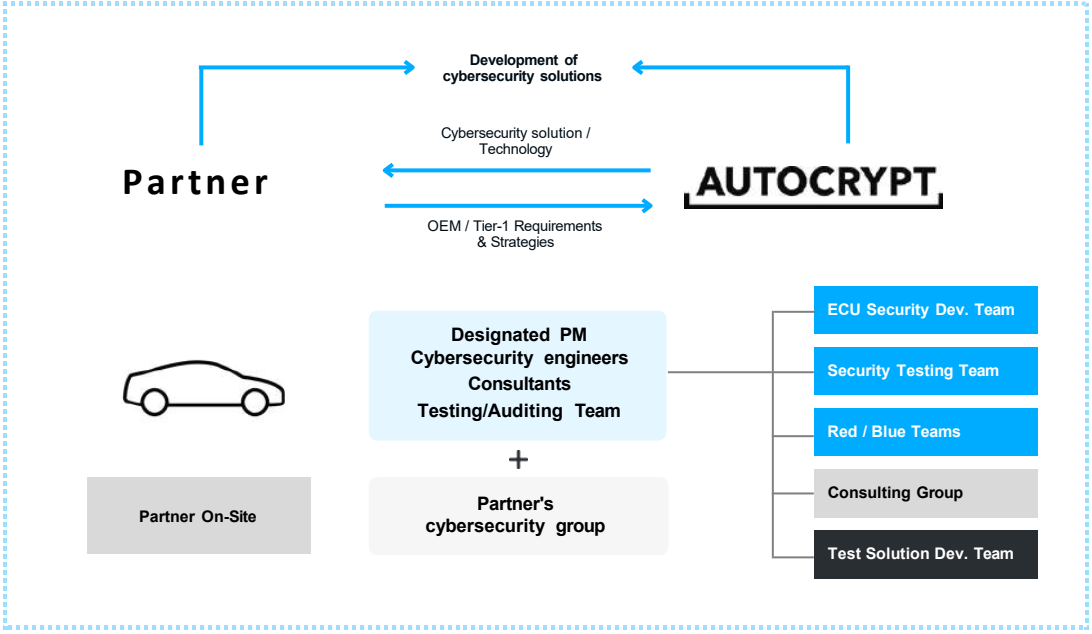
보안 구축 시 고려사항

자동차 산업이 하드웨어보다는 소프트웨어 중심으로 변화함에 따라 자동차가 사이버 공격과 데이터 유출의 더 큰 표적이 될 것이라는 전망이 나오고 있다.

또한, 다양한 소프트웨어와 각 차량 모델에 관련된 다수의 소프트웨어 제공업체의 특성으로 인해 차량 보안과 관련하여 더 많은 복잡성이 발생할 수 있다.

그렇기 때문에 차세대 SDV의 보안을 위해서는 종합적이고 포괄적인 사이버 보안이 필수적이라고 할 수 있다. 차량이 도로를 달리기 전에 안전을 보장하기 위해서는 다양한 솔루션과 접근 방식이 협력해야 한다. 그러나 일반적인 생각과는 달리 전체적이고 포괄적인 것이 반드시 어려운 것은 아니다.

Autocrypt는 협력적인 사이버 보안을 지원하며 팀워크, 기술 및 테스트의 조직적 모델을 활용하여 최고 수준의 안전한 경험을 제공한다.



커넥티드 시대를 위한 사이버 보안 기술 분야에서 수십 년간 쌓아온 Autocrypt의 경험은 업계가 변화하고, 차량 기술이 발전함에 따라 계속 변화할 것임을 이해하는 제조업체와 공급업체에게 큰 자산이 될 수 있다. 보안은 결코 획일화된 모델이 아니라고 믿으며, 각 파트너와 파트너의 아키텍처 및 구조적 요구 사항에 맞게 맞춤화하는 데 자부심을 가지고 있다.

For more information about Autocrypt's comprehensive cybersecurity offerings for SDVs, CAVs, and EVs, visit www.autocrypt.io or contact global@autocrypt.io