Journal of KIIT. Vol. 23, No. 4, pp. 203-211, Apr. 30, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.4.203

SDV 인공지능 보안 거버넌스 구현에 대한 연구

이정찬*[1], 윤철희**, 최진영*[2]

Research on Implementing Security Governance for SDV AI Security

Jungchan Lee*[1], Cheolhee Yoon**, and Jinyoung Choi*[2]

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임
(No. RS-2024-00337489, 분석 모델의 성능저하 극복을 위한 데이터 드리프트 관리 기술 개발)

요 약

본 연구는 SDV 자동차 산업의 사이버보안 위협과 그 해결 방안을 분석하였다. 기존 자동차의 디지털화에 따른 보안 위협의 특성과 영향 분석을 통해 소프트웨어로 하드웨어를 제어하고 관리하는 자동차인 SDV(Software Defined Vehicle)가 직면한 새로운 유형의 사이버 위협을 식별하고, 차량 안전성과 신뢰성에 미치는 영향을 평가하려 하였다. SDV Security and Prevention Data drift가 적용된 초거대 SDV AI 보안 플랫폼을 중심으로 SDV 자동차 산업이 직면한 사이버보안 과제들을 검토하고, 이에 대한 체계적인 대응 방안을 제시하였다. 본 논문은 최근 직면한 SDV 사이버보안 강화를 위한 통합적 접근 방식을 제안하며, 향후 발전 방향에 대한 시사점을 제공한다.

Abstract

This study analyzes cybersecurity threats and solutions in the SDV automotive industry. By analyzing the nature and impact of security threats due to the digitization of traditional automobiles, we aimed to identify new types of cyber threats faced by Software-Defined Vehicles(SDVs), which are vehicles that control and manage hardware with software, and evaluate their impact on vehicle safety and reliability. SDV Security and Prevention We reviewed the cybersecurity challenges faced by the SDV automotive industry and proposed systematic responses to them, centering on the ultra-large-scale SDV AI security platform with data drift. This paper proposes an integrated approach to strengthen SDV cybersecurity in the face of recent challenges and provides implications for future development.

Keywords
automotive cybersecurity, software defined vehicle preventing data drift, ultra-large-scale SDV AI security governance

* 연세대학교 일반대학원 기술경영협동과정 박사과정 (*[2] 교신저자)
- ORCID[1]: https://orcid.org/0009-0009-3713-6992
- ORCID[2]: https://orcid.org/0009-0006-7925-4020
** 경찰대학교 치안정책연구소 연구관
- ORCID: https://orcid.org/0000-0002-4862-4790

· Received: Mar. 07, 2025, Revised: Apr. 14, 2025, Accepted: Apr. 17, 2025
· Corresponding Author: Jinyoung Choi
Management of Technology, Yonsei University Graduates School,
50 Yonsei-ro Seodaemun-gu, Seoul, Korea
Tel.: +82-2-2123-4484, Email: gksniper@yonsei.ac.kr

Ⅰ. 서 론

1.1 연구 배경

현대 자동차 산업은 전례 없는 기술적 변화의 시기를 맞이하고 있다. 자율주행 기술의 발전, 커넥티드 카의 보편화, 전기차로의 전환 등 혁신적 변화는 자동차를 단순한 이동수단에서 첨단 모빌리티 플랫폼으로 진화시키고 있다[1]. 이러한 변화 속에서 자동차는 더 이상 독립적인 기계 장치가 아닌, 다양한 디지털 시스템과 네트워크로 연결된 복합 시스템으로 발전하고 있다. 특히 5G 통신 기술의 발전과 IoT 기기의 보급은 차량의 연결성을 획기적으로 향상시켰으며, 이는 새로운 서비스와 비즈니스 모델의 창출로 이어지고 있다[2]. 그러나 이러한 디지털 전환은 새로운 보안 위협을 동반하며, 최근 발생한 여러 차량 해킹 사례들은 자동차 사이버보안의 중요성을 명확히 보여주고 있다. [3][4] 차량 원격 제어 시스템 해킹, 차량 통신 네트워크 침투, 개인정보 유출 사고가 보고되고 있으며, 이러한 사고는 단순한 재산상의 피해를 넘어 운전자의 생명과 직결될 수 있다는 점에서 특별한 주목을 요한다.

더욱이 자동차 산업의 공급망이 복잡해지고 글로벌화됨에 따라, 보안 위협의 범위도 확대되면서, 단일 부품의 보안 취약점이 전체 차량 시스템의 위험으로 이어질 수 있으며, 이는 대규모 리콜 사태를 초래하거나 브랜드가치 하락과 같은 심각한 결과를 초래할 수 있게 되었다[5][6]. 특히, 소프트웨어 정의 차량(SDV, Software-Defined Vehicle)의 등장은 자동차 산업의 보안 패러다임을 더욱 복잡하게 만들고 있다. 기존의 차량이 하드웨어 중심의 보안 모델을 기반으로 했다면, SDV는 소프트웨어 및 네트워크 기반 보안이 핵심이 되는 새로운 체계로 전환되고 있다. 이는 자동차 공급망 내 보안 위협의 범위를 확장시키며, SDV의 보안 및 개인정보 보호 문제를 해결하기 위한 새로운 거버넌스 전략이 요구된다[7].

1.2 연구 목적

본 연구는 최근 자동차 산업이 직면한 SDV의 사이버보안 문제의 복잡성과 그 해결 방안을 종합적으로 분석하는 것을 목적으로, SDV 거버넌스 플랫폼을 통한 Preventing Data Drift, SDV 사이버보안 관리를 위한 체계적 접근 방안을 제시하고자 한다. 본 연구는 우선적으로 자동차의 디지털화에 따른 보안 위협의 특성과 영향 분석을 통해 SDV가 직면한 새로운 유형의 사이버 위협을 식별하고, 이들이 차량 안전성과 신뢰성에 미치는 영향을 평가하려 하였다. 이는 자동차 산업의 디지털 전환 과정에서 SDV가 고려해야 할 핵심적인 보안 요소들을 이해하는 데 기여할 것이다. 그 해결을 위해 방법으로 자동차 사이버보안 관련 규제, 표준의 발전 동향 분석, UNECE R155/156, ISO/SAE 21434와 같은 국제 표준의 요구사항, 규제 환경 변화에 대응하기 위한 전략적 거버넌스를 모색하였다. 더불어, 글로벌 선도기업의 사례 분석 및 라 SDV 개발 프로세스에서 품질, 안전, 보안을 확보하는 선행연구 결과를 통해 통합 보안 관리 플랫폼의 구현 방안을 제시하였다. 본 논문을 통해 위협 분석, 보안 테스트, 모니터링, 업데이트 관리 등 SDV 사이버보안의 핵심 요소들을 어떻게 효과적으로 통합하고 운영할 수 있는지에 대한 실질적인 지침을 제공하였다.

Ⅱ. SDV 사이버보안 환경

2.1 자동차의 상호연결성 증가

현대 자동차 산업에서 가장 주목할 만한 변화는 차량의 상호연결성 증가이다. 차량 간 통신(V2V)을 통해 실시간으로 교통 정보와 안전 경고를 주고받을 수 있게 되었으며, 도로 인프라와의 통신(V2I)을 통해 더욱 효율적인 교통 관리가 가능해졌다. 또한 클라우드 서비스와의 연결(V2C)을 통해 차량의 원격 진단과 소프트웨어 업데이트가 실시간으로 이루어지고 있다. 보행자와의 통신(V2P)은 도로 안전성을 크게 향상시켰으며, 전력망과의 연결(V2G)은 전기차의 효율적인 충전 관리를 가능케 했다.

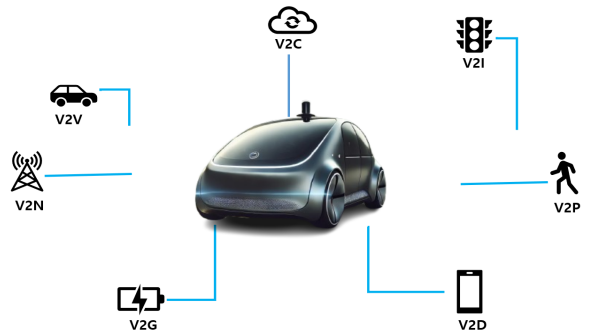

그림 1. 현대 자동차의 상호 연결 아키텍처
Fig. 1. Interconnectivity architecture of modern automotive

그림 1과 같이 자동차의 상호성의 증가는 차량의 기능과 서비스를 획기적으로 확장시켰다. 일례로, 실시간 내비게이션 서비스는 교통 상황에 따른 최적 경로를 제공할 뿐만 아니라 주변 차량과의 정보 공유를 통해 사고 위험을 사전에 감지하고 예방할 수 있게 되었고 스마트폰과의 연동(V2D)을 통해 차량의 원격 제어와 상태 모니터링이 가능해졌다. 그리고 5G 네트워크의 도입(V2N)은 이러한 연결성을 한층 강화하여, 자율주행과 같은 고도의 기술 구현을 가능하게 했다[8]. 그러나 이러한 다차원적 연결성은 새로운 서비스와 가치를 창출하는 동시에, 사이버 공격의 잠재적 경로도 함께 증가시키는 결과를 가져왔다. 각각의 연결 지점이 잠재적인 보안 취약점이 될 수 있으며, 이는 차량 시스템 전반의 보안 위협으로 이어질 수 있다. 따라서 이러한 연결성의 확대는 포괄적이고 체계적인 사이버보안 대책의 필요성을 더욱 부각시키고 있다.

2.2 사이버보안 위협의 현실화

자동차 산업의 SDV 디지털 전환은 원격 진단, 예측 정비, 맞춤형 운전 서비스 등 데이터 기반의 새로운 서비스를 만들어내고 있지만, 그 이면에는 심각한 보안 위협이 존재한다. 차량 제어 시스템 해킹, 개인정보 유출, 서비스 거부 공격 등 다양한 형태의 사이버 위협이 현실화되고 있으며, 최근에는 랜섬웨어를 통한 차량 시스템 장악, 차량 위치 추적을 통한 프라이버시 침해, 차량 통신 시스템을 통한 대규모 네트워크 공격 등 위협의 형태가 더욱 지능화, 고도화되고 있다[9]. 더욱 우려스러운 점은 이러한 사이버 공격이 단순한 금전적 손실을 넘어 운전자의 생명과 직결된다는 점이다. 주행 중인 차량의 제동 시스템이나 조향 장치가 해킹될 경우 대형 사고로 이어질 수 있으며, SDV 관리시스템에 대한 공격은 다수의 차량에 동시다발적 영향을 미칠 수 있어, 그 피해 규모가 매우 클 것으로 예상된다. 이러한 위험성은 자동차 산업에서 사이버보안이 선택이 아닌 필수 요소임을 명확히 보여주고 있다.

2.3 SDV Data-Drift 사이버보안 위협

차량 내부의 통합 네트워크와 전자제어 장치(ECU) 간 통신을 담당하는 CAN Bus 해킹과 원격 제어 침입 등의 경우 통신 패킷의 data 침입을 통해 CAN Bus를 해킹이 가능하다. SDV 차량의 주요 시스템이 제동장치 조향 장치, 엔진 제어 시스템에 접근할 수 있게 되며, 이러한 해킹 공격은 차량을 원격으로 제어할 수 있게 하여 큰 위험을 초래한다[10]. 텔레매틱스 시스템을 통한 data drifting 원격 제어 공격으로 차량의 위치 추적, 원격 잠금 해제, 엔진 제어 등이 가능하며, 차량에 탑재된 인포시스템(Infotainment system)의 취약점을 통해 Unit의 차량제어 권한을 탈취하는 악성코드를 주입하여 원격으로 차량 브레이크 해제 및 운전자 조종을 무력화하는 가속제어 조작 수행이 가능하다. 또한, APE 업데이트 프로그램에 존재하는 취약점을 악용한 root 권한 획득으로 원격 차량을 강제 조작이 가능하고, 리모트 키 암호화 시스템 취약점 및 원격시동 앱 해킹을 통한 해킹의 우려가 존재한다[11]. 2017년 현대자동차 블루링크 애플리케이션에 해커가 보안되지 않은 와이파이를 통해 침입, 사용자의 정보를 탈취하고 원격으로 시동을 걸 수 있는 취약성이 포함된 것으로 발표된 적도 있다[12].

III. SDV 사이버보안 규제 환경 분석

3.1 SDV 사이버보안 국제 규제

SDV 사이버보안 규제는 전 세계적으로 강화되는 추세로 UN 산하 자동차 기준 조화 세계 포럼

(UN/ECE/WP.29)은 자동차 사이버보안 관리 시스템에 대한 국제 규정인 UNECE R155/R156을 제정하였다. 이는 모든 신규 차량에 대한 사이버보안 인증을 의무화하는 첫 번째 국제 규정으로서, 자동차 산업의 사이버보안 관리 체계를 근본적으로 변화시키고 있다. UNECE R155는 차량 제조사가 적절한 사이버보안 관리 시스템을 구축하고 운영할 것을 요구하고 있으며, 설계 단계부터 생산, 운영, 폐기에 이르는 전체 수명주기에 걸친 보안 관리를 의무화하고 있다. 주요 사항은 차량 제조사는 사이버 위협을 평가하고 그에 따른 보안 대책을 마련해야 한다는 '사이버보안 위험 평가'를 규정하고 있으며, 차량의 보안관리 프로세스를 명확하게 정의하고 이를 일관되게 관리해야 한다는 '사이버보안 관리 체계 구축'도 명시하고 있다. 아울러 사고 발생 시 신속하게 대응할 수 있는 절차와 계획을 마련해야 한다는 '사이버보안 사고 대응 계획'도 요구하고 있다.

그리고 UNECE R156은 소프트웨어 업데이트와 관련된 요구사항을 다루고 있는데 특히, 차량의 소프트웨어가 원격으로 업데이트될 경우의 보안 위험을 중요한 요소로 보고 있다. SDV 경우 소프트웨어 업데이트가 암호화를 통해 인증된 경로에서만 실행될 수 있어야 하며, 이를 통해 악성코드나 불법 업데이트를 금지하는 '원격 소프트웨어 업데이트 보안'을 명시하고 있다. 제조사는 소프트웨어 업데이트가 차량에 적용되기 전에 위험 평가와 검증 절차를 거쳐야한다는 '소프트웨어 변경 관리'와 업데이트가 이루어진 모든 소프트웨어 변경 사항은 기록되고 추적 가능해야 하고 이를 통해 문제 발생 시 신속하게 원인 분석을 할 수 있어야 한다는 '소프트웨어 이력관리'도 명시하고 있다. EU를 포함한 대다수 국가에서 이 규정을 법적으로 적용하고 있으며, 규정 미준수 시 법적 제재가 부과될 수 있다[13][14].

ISO/SAE 21434 표준은 SDV 사이버보안 엔지니어링의 기술적 기준을 제시하고 있으며, 이는 업계 표준으로 자리잡고 있다[15]. 이 표준은 위험 평가 방법론, 보안 통제 구현 지침, 보안 테스트 요구사항 등 상세한 기술적 가이드라인을 제공하며, 공급망 보안 관리에 대한 요구사항을 포함하고 있다. SDV 산업의 복잡한 공급망 구조에서 발생할 수 있는 보안 위험을 체계적으로 관리할 수 있는 프레임워크를 제공하고 UNECE 규정보다 더 구체적인 기술적 요구사항을 포함하고 있다. 미국의 경우는 NHTSA(국립고속도로교통안전국)가 2016년부터 자동차 사이버보안 가이드라인(Cybersecurity best practices for the safety of modern vehicles)을 통해 SDV 차량 사이버보안 위협을 체계적으로 평가하고, 사고 발생 시 신속하게 대응할 수 있는 보안사고 대응계획을 마련하는 '위험 평가 및 대응 계획'을 선 보이고 있다[16]. 앞서 언급한 CAN Bus와 같은 차량 내부 네트워크에 대한 보호를 강화하여 해커가 차량 시스템에 접근을 막는 '내부 네트워크 보호'와 소프트웨어 업데이트를 통해 취약점을 지속적으로 수정할 수 있도록 하며, 원격 업데이트 시스템의 보안을 강화하는 방안을 제시하는 '소프트웨어 업데이트 및 패치 관리'와 차량의 소프트웨어와 하드웨어가 보안요구 사항을 충족하는지 확인하기 위해 정기적인 보안 검사와 인증 절차를 마련하도록 권하는 '보안검사와 인증'도 명시되어 있다.

아울러 차량 내 통신 및 원격 접근을 암호화하여, 외부에서의 불법적인 해킹 시도를 방지하고, 차량에 침입 탐지 시스템을 설치하여 비정상적인 네트워크 활동을 실시간으로 감지하고 대응할 수 있도록 해야한다고 강조하는 등 구체적인 보안 조치도 제시하고 있다[17]. 현재 NHTSA의 사이버보안 가이드라인은 권고사항이나 2021년부터 규제 법제화가 필요하다는 목소리가 커지고 있으며, 미국 의회 일부 의원들은 자동차 제조사들이 사이버보안에 대한 책임을 강화하고 사고 발생 시 법적 책임을 지도록 하는 법안을 제안하는 등 향후 이를 의무 규정으로 강화하려는 움직임을 보이고 있다.

한국 경우 역시 UNECE WP.29 R155/156을 기반으로 자동차 사이버보안 규제를 수립해가고 있으며, 차량 개발 단계부터 보안 리스크를 분석하여 전체 수명주기 동안 사이버보안을 유지할 수 있는 시스템 구축 및 위험 평가와 대응 절차 마련에 고심하고 있다. 표 1에 제시된 국가별 사이버보안 법규 비교를 통해 세계 주요국의 자동차 사이버보안에 대한 고민을 고찰해 볼 수가 있다.

표 1. 국가별 사이버보안 규제 비교
Table 1. Compare cybersecurity legislation by country

Country	Legal /Regulatory	Highlights	Coverage
Korea	Automotive cybersecurity act	Putting cybersecurity stewardship in the hands of automakers, risk assessment and incident response	Vehicle manufacturers and automotive technology companies
EU	UNECE WP.29 regulations (R155/R156)	Fleet cybersecurity and software update management regulatory	EU member states and vehicle manufacturers
USA	Cybersecurity regulations by state	State-by-state regulation of vehicle security systems, increasing autonomous security	Major automakers by state and country
China	China cybersecurity law	Managing cybersecurity and increasing safety regulations for vehicles	Domestic manufacturers and vehicle-related technology companies

3.2 규제 대응의 시급성

2022년 7월부터 시행된 UNECE WP.29 TF-CS/OTA 요구사항은 신규 차종에 대한 사이버보안 인증을 의무화하였으며, 2024년부터는 이 규정이 모든 신규 차량으로 확대 되고 있다. 이러한 규제 요구사항을 충족하기 위해서는 조직 전반의 포괄적인 변화가 필요하기 때문에, 개발 단계에서의 보안 설계(Security by design) 원칙 도입, 공급망 전반의 보안 관리 체계 구축, 실시간 위협 모니터링 시스템 구축, 보안 업데이트 관리 체계 수립 등 광범위한 영역에서의 변화가 요구되고 있다. 그리고 이러한 변화는 단순한 기술적 대응을 넘어, 조직 문화와 업무 프로세스의 근본적인 변화를 수반해야 하기 때문에 본 논문에서 제시하는 사이버 보안 안전성 확보에 대한 거버넌스 수립이 매우 중요한 사항으로 부각되었다. 특히, 주목할 점은 이러한 규제가 단순한 기술적 요구사항을 넘어, 조직 전반의 사이버보안 관리 체계 구축을 요구한다는 것으로 기업은 보안 위험 평가, 위협 모니터링, 취약점 관리, 인시던트 대응 등 포괄적인 보안 관리 프로세스를 구축하고 이를 지속적으로 개선해야 한다. 또한, 이러한 프로세스의 효과성을 입증할 수 있는 객관적인 증거를 제시해야 하며, 이는 정기적인 심사와 인증을 통해 검증을 받는 선순환을 수행해야 한다는 점이다. 국내 자동차 업계도 역시 UNECE WP.29의 사이버보안 규제에 대응하기 위해 다양한 노력을 기울이고 있으며, 차량 개발 단계부터 생산, 판매, 사후 관리에 이르는 전 과정에서 사이버보안 체계를 구축하고 운영하려 노력 중으로 차량의 전자제어장치(ECU)와 통신 네트워크의 보안 강화를 위해 정보보호 국제표준인 ISO27001 준수, 자동차 사이버보안 관리체계(CSMS)인증 획득, 보안 취약점 점검, 그룹사 보안협의체 운영 등을 통해 정보보호를 강화 등의 노력을 하고 있다. 즉, SDV 거버넌스 체계를 통해 차량 개발 단계부터 보안 강화부터, 사용자 개인 데이터를 암호화하여 보호하는 보안 프로토콜을 적용까지, SDV 차량 주기 전반에 걸쳐 보안 위험을 식별하고 관리하는 프로세스를 운영하려는 노력을 수행하고 있다.

Ⅳ. SDV 인공지능 보안 거버넌스를 통한 플랫폼 구현

4.1 SDV 인공지능 보안 거버넌스 구성

SDV 산업의 복잡한 사이버보안 요구사항을 충족시키기 위해 통합 거버넌스 플랫폼은 그림 2의 거버넌스 플랫폼을 통해 포괄적인 보안 관리 사항을 제시할 수 있다. 플랫폼의 핵심 요소인 컴플라이언스 대응을 통해 국제 표준과 규제 요구사항의 준수를 자동화와 문서화 그리고 ISO/SAE 21434와 UNECE R155/R156와 같은 핵심 규제에 대한 체계적인 대응이 가능하다. 이는 복잡한 규제 요구사항을 체계적으로 관리하고, 필요한 증거 자료를 효율적으로 생성할 수 있게 한다. 또한, 보안 위협 관리를 위한 위험대응 분야는 위협 분석 및 위험 평가를 자동화 후 시스템 모델링 기반의 접근 방식을 통해 잠재적 위협을 식별하고, 위험도를 평가하며, 적절한 대응 방안을 수립하는 과정을 수행할 수 있다.

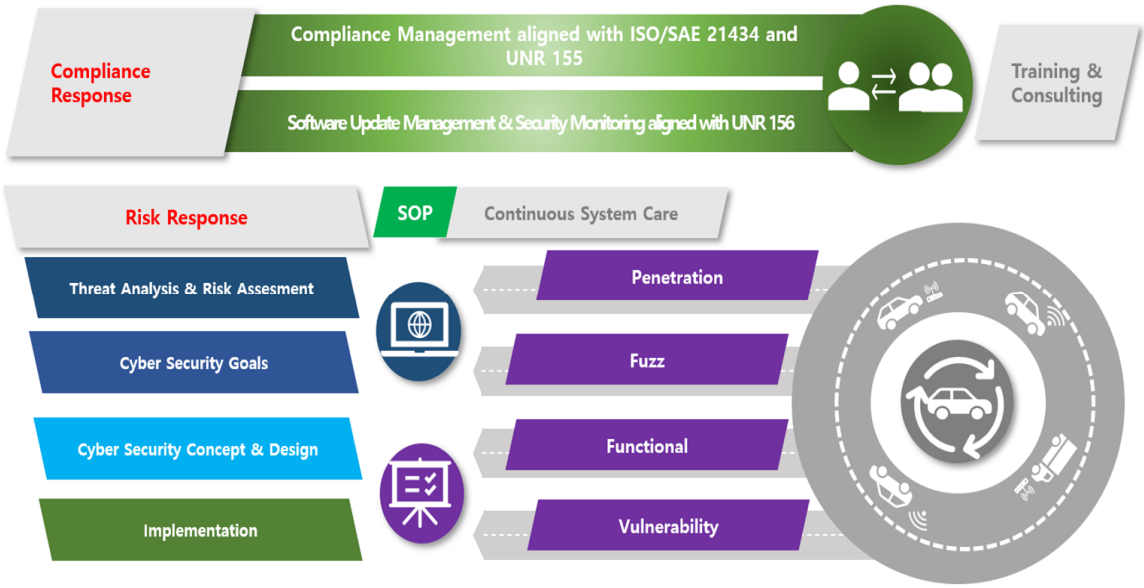

그림 2. SDV 인공지능 보안 거버넌스 플랫폼
Fig. 2. SDV AI security governance platforms

특히 Preventing Data drift을 통해 데이터 위변조에 의한 예방과 자동화된 위협 시나리오 생성으로 공격 관련 예방의 효율성과 정확성이 크게 향상된다. 그리고, 보안 검증을 위해 포괄적인 보안 테스트 자동화를 통해 기능 테스트, 퍼징 테스트, 침투 테스트 등 다양한 테스트를 자동화하여, SDV 통신 프로토콜(CAN, AutoSAR 등)에 대한 전문적인 테스트를 수행해서, 효율적인 취약점 관리를 수행할 수 있다. SDV 소프트웨어 업데이트 관리는 보안 모니터링 에 핵심으로 SDV 차량의 전체 수명주기에 걸친 소프트웨어 업데이트를 안전하게 관리하고, 실시간으로 보안 위협을 모니터링하는 기능을 적용하여 SDV 거버넌스 플랫폼을 운영하여야 한다. SDV 거버넌스 관리의 주안점은 자동차의 전체 생명주기에 걸친 통합적 보안 관리 접근방식으로 개발 단계에서의 보안 요구사항 분석과 위협 모델링을 통한 잠재적 위험 식별, 이에 대한 대응, 'Security Compliance' 원칙 적용을 통해 초기 설계 단계부터 보안이 핵심 요소로 고려하게 하고, 모델 기반 위협 분석을 통해 보안 취약점을 조기 발견 후 제거할 수 있도록 하는 점이다. 이후 구현 단계에서는 자동화된 보안 테스트와 취약점 분석을 통해 설계된 보안 대책의 효과성을 검증하고, 자동화된 테스트 도구를 통해 품질 보증과 인증 과정을 효율화하도록 한다. 퍼즈 테스트(Fuzz test)를 통한 예상치 못한 취약점 발견과 침투 테스트를 통한 실제 공격 시나리오 검증이 수행되고, 운영 단계에서는 지속적인 모니터링과 실시간 위협 탐지를 통해 새롭게 발견되는 보안 위협에 대응한다. 즉, 차량 네트워크의 이상 행동을 실시간으로 감지하고, 필요한 경우 즉각적인 대응 조치를 취할 수 있고, 소프트웨어 업데이트 관리의 경우 보안 패치의 신속한 배포와 적용을 가능하게 함으로써, 차량의 보안 수준을 지속적으로 유지할 수 있게 한다. 그리고 부가적으로 공급망 보안 관리를 통해 부품 공급업체의 보안 관리 현황 및 모니터링을 통해 공급망 전반의 보안 수준을 일관되게 유지할 수 있게 관리 해야 한다.

4.2 SDV 보안 거버넌스 기술적 특징

SDV 보안 거버넌스 기술적 특징 중 주목받는 요소는 차량 내의 데이터 보호를 위해 인공지능과 클라우드 기반의 보안 요소를 활용하는 방안이다. 기존의 스마트폰 보안 기술을 기반으로 SDV에서도 데이터 보호와 침입 탐지, 보안성 강화 방식이 가능해지고, 차량 내 센서 및 네트워크 발생 데이터를 실시간으로 분석 후 위협 감지 및 자동 보안 조치가 인공지능 기반기술로 가능하다.

즉, 차량 내부에서 발생하는 이상 행동을 탐지하고, 이 정보를 클라우드 서버로 전송하여 인공지능을 이용한 추가적인 분석을 수행하는 구조로 운영하고 또한, 데이터 암호화 및 무결성 보호 기능을 강화하여 외부 해킹 시도가 이루어질 경우 공격자가 데이터를 변조하거나 탈취하는 것을 방지할 수도 있다. 이는 SDV 보안 거버넌스의 기술적 특징에서 중요한 요소로 작용하며, 차량 간 통신(V2V) 및 차량-클라우드 통신(V2C)에서 발생하는 보안 위협을 줄이는 데 효과적이다. 그리고 다층적 보안 시스템을 구축으로 차량 내 다양한 보안 위협 방어, 네트워크 보호, 공급망 보안(Supply chain security)까지 고려한 보안 전략이 가능해진다. 인공지능과 클라우드 기반의 기술이 적용된IPS(Intrusion Prevention System)와 IDS(Intrusion Detection System)를 결합한 하이브리드 모델을 적용 후 차량 내외부에서 발생하는 보안 위협을 실시간 탐지, 대응하며 CAN Bus와 같은 내부 네트워크와 차량이 연결되는 외부 네트워크를 포함하여 클라우드로 보호하는 다층 방어가 가능해지기 때문이다. 또한, OTA 경우에도 보안 업데이트 시각화(Security update visualization) 시스템을 적용하여 OTA 업데이트가 진행될 때 보안 상태를 실시간으로 모니터링하고, 이상 징후가 발생하면 업데이트를 중지하거나 롤백(Rollback) 기능을 수행할 수 있도록 하여SDV에 새로운 보안 취약점이 발견될 경우 클라우드 기반의 원격시스템으로 보안 업데이트를 받을 수 있다.

위의 표 2와 같은 인공지능보안이 적용된 SDV 기술목록표를 통해 SDV 보안 예방 기능을 확인할 수 있다. 눈에 띄는 점은 인공지능기반 SDV 보안 플랫폼은 기술 생태계를 기반으로 침입 탐지 시스템, 소프트웨어 OTA 업데이트 체계로 구성되고 있다는 점이다. 앞서 설명했듯이 이상 감지, 운전자 인증 분석, 비정상적인 원격 접근 탐지 기능 등을 수행하며, 새로운 공격 패턴을 학습하면서 지속적으로 대응한다. 또한, 외부에서 차량 내부 시스템에 접근할 수 있는 취약점을 최소화하기 위해 강제적인 다단계 인증과 내부 보안 키를 활용한 접근 통제 시스템을 적용하고, 원격 공격을 실시간으로 탐지하기 때문에 보안 취약점이 발견되었을 때, 보안 위협을 사전에 감지하고 차단하여 CAN Bus와 같은 차량의 주요 제어 시스템을 보호하고 위협을 미리 예방할 수 있다. 결론적으로 SDV 보안의 기술적 특징은 SDV 모든 분야가 거대 인공지능 보안 거버넌스에 초점이 맞춰져야 한다는 점이다.

표 2. 인공지능보안이 적용된 SDV 기술목록표
Table 2. List of SDV technologies applied with AI security

Item	Functions	
Security approach	AI-Powered cybersecurity & OTA updates	Real-time threat detection & intrusion prevention
Real-time threat detection	Anomaly detection with AI	Automated response utilizing AI and machine learning
Intrusion Detection Systems (IDS)	Limited (mainly network traffic surveillance)	Full IDS coverage (automotive network protection)
Data protection and encryption	Enforcement of advanced encryption + security protocols	Enhanced network security + integrated security solutions
Security updates	Vulnerability patching via OTA updates	Integrated manufacturer update management
Coverage	Dedicated to Tesla vehicles	Applicable to various automobile manufacturers
Attack defense capabilities	Focused on remote hacking defense	Detect and block threats inside and outside the vehicle

Ⅴ. 결론 및 제언

SDV 기반의 자동차 디지털 전환이 가져온 사이버보안에 대한 도전과 그 해결 방안을 본 논문에서는 SDV 인공지능 사이버보안 거버넌스로 접근하였다. SDV 보안 예방은 단순한 기술적 문제를 넘어, SDV 생태계 전반의 체계적인 연구로 전환되는 기로에 서 있으며, SDV차량의 다중 연결성 증가, 보안 위협의 복잡화, 공급망 보안, 체계적인 위험 평가, 포괄적 보안 테스트, 지속적 모니터링 등은 SDV

안전 생태계구축, SDV신뢰성, 지능형 위협 탐지, 자동차 공급망 관리, 인공지능 대응모델 생성으로 발전할 것이다. 향후 연구에서는 보안과 혁신이라는 두 가지 목표를 동시에 달성하면서, 지속 가능한 발전을 이루기 위한 방안이 모색되기를 기대한다.

References

[1] M. D. Vincenzi, G. Costantino, I. Matteucci, F. Fenzl, C. Plappert, R. Rieke, and D. Zelle, "A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet", ACM Computing Surveys, Vol. 56, No. 6, pp. 1-38, Jan. 2024. https://doi.org/10.1145/3637059.

[2] J. P. Mohan, N. Sugunaraj, and R. Prakash, "Cyber Security Threats for 5G Networks", IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, May 2022. https://doi.org/10.1109/eIT53891.2022.9813965.

[3] A. A. Peralta, N. Balta-Ozkan, and S. Li, "The Road Not Taken Yet: A Review of Cyber Security Risks in Mobility-as-a-Service (MaaS) Ecosystems and a Research Agenda", Research in Transportation Business & Management, Vol. 56, pp. 101162, Oct. 2024. https://doi.org/10.1016/j.rtbm.2024.101162.

[4] Y. Shichun, et al., "Essential Technics of Cybersecurity for Intelligent Connected Vehicles: Comprehensive Review and Perspective", IEEE Internet of Things Journal, Vol. 10, No. 24, pp. 21787-21802, Dec. 2023. https://doi.org/10.1109/JIOT.2023.3299554.

[5] H. Zhang, Y. Pan, Z. Lu, J. Wang, and Z. Liu, "A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units", IEEE Access, Vol. 9, pp. 149690-149704, Nov. 2021. https://doi.org/10.1109/ACCESS.2021.3124565.

[6] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses", IEEE Access, Vol. 9, pp. 162401-162415, Dec. 2021. https://dx.doi.org/10.1109/ACCESS.2021.3130495.

[7] M. D. Vincenzi, et al, "Contextualizing Security and Privacy of Software-Defined Vehicles: State of the Art and Industry Perspectives", arXiv preprint, arXiv:2411.10612v2, Dec. 2024. https://doi.org/10.48550/arXiv.2411.10612.

[8] M. Muhammad and G. A. Safdar, "5G-based V2V Broadcast Communications: A Security Perspective", Array, Vol. 11, pp. 1-11, Aug. 2021. https://doi.org/10.1016/j.array.2021.100084.

[9] D. S. Im, "An Analysis of the Relative Importance of Security Level Check Items for Autonomous Vehicle Security Threat Response", Journal of The Korea Institute of Intelligent Transport Systems, Vol. 21, No. 4, pp. 145-156, Aug. 2022. https://doi.org/10.12815/kits.2022.21.4.145.

[10] Y. Lee, S. Kim, and S. Choi, "Anomaly Detection in Vehicles using Predictive Models based on CAN Data", Journal of KIIT, Vol. 22, No. 12, pp. 257-265, Dec. 2024. https://dx.doi.org/10.14801/jkiit.2024.22.12.257.

[11] http://www.bit.ly/4bd2ELT [accessed: Mar. 07. 2025]

[12] https://www.boannews.com/media/view.asp?idx=109385. [accessed: Mar. 07. 2025]

[13] United Nations Economic Commission for Europe (UNECE), "UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system", ECE/TRANS/WP.29/2020/79, United Nations, Mar. 2021.

[14] United Nations Economic Commission for Europe (UNECE), "UN Regulation No. 156 - Uniform provisions concerning the approval of vehicles with regards to software update and software update management system", ECE/TRANS/505/Rev.3/Add.155, United Nations, Mar. 2021.

[15] S. Ballingall, M. Sarvi, and P. Sweatman, "Standards relevant to automated driving system

safety: A systematic assessment", Transportation Engineering, Vol. 13, pp. 1-12, Sep. 2023. https://doi.org/10.1016/j.treng.2023.100202.

[16] National Highway Traffic Safety Administration (NHTSA), "Cybersecurity Best Practices for the Safety of Modern Vehicles", U.S. Department of Transportation, pp. 1-18, Sep. 2022.

[17] National Highway Traffic Safety Administration (NHTSA), "Cybersecurity Best Practices for Modern Vehicles", U.S. Department of Transportation, pp. 1-27, Oct. 2016.

저자소개

이 정 찬 (Jungchan Lee)

2006년 2월 : 동국대학교 정보통신공학(공학사)
2014년 8월 : 연세대학교 정보대학원(공학석사)
2009년 9월 ~ 현재 : 한국지능정보사회진흥원 수석연구원
관심분야 : 인공지능, 데이터분석, 데이터 품질관리

윤 철 희 (Cheolhee Yoon)

2016년 8월 : 고려대학교 디지털포렌식학과(공학석사)
2023년 2월 : 연세대학교 기술정책(공학박사)
2024년 8월 : 극동대학교 인공지능보안학과(공학박사)
2017년 6월 ~ 현재 : 경찰대 치안정책연구소 연구관
관심분야 : 인공지능, 데이터분석, 딥러닝

최 진 영 (Jinyoung Choi)

2008년 2월 : 동국대학교 정보관리학(경영학사)
2010년 2월 : 연세대학교 정보산업공학(공학석사)
2010년 2월 ~ 현재 : 한국특허전략개발원 책임연구원
2015년 9월 ~ 현재 : 연세대학교 일반대학원 기술경영학협동과정 박사과정
관심분야 : 인공지능, 빅데이터