MOBILITY INSIGHT

10
2024 VOL.33

COVER STORY

커넥티드카 사이버보안 실태 및 방향성은 어떠한가?

KATECH KOREA AUTOMOTIVE TECHNOLOGY INSTITUTE 한국자동차연구원

MOBILITY INSIGHT

10
2024 VOL.33

COVER STORY

커넥티드카 사이버보안 실태 및 방향성은 어떠한가?

모빌리티 인사이트
2024. 10. Vol.33
www.katech.re.kr

발행인 : 나승식 **발행처 : 한국자동차연구원** 충청남도 천안시 동남구 풍세면 풍세로 303
TEL_041. 559. 3114 **FAX**_041. 559. 3068 **문의처 :** mobilityinsight@katech.re.kr
편집·디자인 : 브랜드캐스트(주) TEL_02. 2661. 6786

※ 본 「모빌리티 인사이트」에 실린 보고서는 연구진이나 집필자의 개인적인 견해이므로 한국자동차연구원의 공식적인 의견이 아님을 말씀드립니다.
Copyright(c) 2024 KATECH(Korea Automotive Technology Institute) All right reserved.

스페셜 컬럼
임강빈 순천향대학교 정보보호학과 교수

정책동향
김태주 법무법인(유) 광장 파트너 변호사

트렌드 리뷰 ①
권중한 LG전자 Cyber Security Governance Unit 책임

트렌드 리뷰 ②
연원호 국립외교원 경제기술안보연구센터장

CONTENTS

임강빈 좌장
순천향대학교
정보보호학과 교수

커넥티드카 사이버보안 실태 및 방향성은 어떠한가?

SECTION 1 커넥티드카 사이버보안 시장 동향 및 이슈는 무엇인가?

SECTION 2 커넥티드카 사이버보안의 중요도는 어떠한가?

SECTION 3 커넥티드카 사이버보안 경쟁력 강화를 위한 육성 방안은?

- 일 시 : 2024년 9월 3일(화) 14:00~15:40
- 장 소 : 포포인츠 바이 쉐라톤 서울역(19층 PDR Room)
- 대 상 : 학계, 자동차업계, 관계기관 등 각 분야 전문가 총 6명

권중한 LG전자
Cyber Security Governance Unit 책임

심상규 아우토크립트(주)
부사장

송경식 (주)HL Klemove
연구원

연원호 국립외교원
경제기술안보연구 센터장

정원선 한국자동차연구원
인천사무소 센터장

커넥티드카 대중화 시대 사이버보안

오늘날 자동차의 가장 대표적인 단어 중 하나는 SDV(Software Defined Vehicle)로 정의된다. SDV(소프트웨어 정의 차량)는 소프트웨어로 하드웨어를 제어하고 관리하는 자동차를 뜻하며, 소프트웨어는 자동차의 주행 성능은 물론 편의 기능, 안전 기능, 차량의 감성 품질, 그리고 브랜드의 아이덴티티까지 규정한다. SDV는 크게 OTA(Over-The-Air) 업데이트, 통합 ECU(전자제어장치), 차량용 소프트웨어 및 클라우드로 구성된 전자 아키텍처, 모빌리티 및 연결성 서비스, 그리고 서드파티 사업자를 고려한 서비스 플랫폼으로 구성된다.

이러한 기술 발전 속에서, 자동차와 통신이 결합한 커넥티드카(Connected Car)가 빠르게 증가하고 있다. 그러나 이에 따른 사이버 공격 우려도 커지고 있다. 커넥티드카는 차량 내외부가 무선 네트워크로 연결된 차량을 말하며, 이러한 연결성은 운전자와 보행자의 안전과 생명까지 위협할 수 있는 심각한 사이버 공격의 표적이 될 수 있다. 이러한 문제를 해결하기 위해, 국내에서도 커넥티드카의 사이버보안을 확보하기 위한 법적·제도적 장치를 마련하고 있다..

한국자동차모빌리티산업협회(KAMA)에 따르면, 2023년 3월 기준 국내 커넥티드카는 708만 1,444대로, 총 자동차 등록 대수(약 2,564만 대)의 27.6%를 차지한다. 즉, 도로 위 자동차 4대 중 1대가 커넥티드카인 셈이다. 2014년에 관련 통계가 처음 공개될 당시 커넥티드카는 66만 대로, 전체 자동차 2,010만 대 중 3.3%에 불과했다. 이후 커넥티드카는 꾸준히 증가하여 2016년에는 116만 대(3.6%), 2017년 136만 대(6%), 2018년 179만 대(7.7%), 2019년 246만 대(10.4%)로 늘었다. 2020년에는 364만 대로 전체 차량의 15%를 차지하며 큰 폭의 성장을 이루었고, 2021년에는 516만 대(20.7%), 2022년에는 662만 대(26%)로 해마다 100만 대 이상씩 규모가 확대되고 있다.

이와 같은 커넥티드카 보급의 확대에 따라, 국내에서는 사이버보안 관리체계 인증제도와 소프트웨어 업데이트 관리제도 도입을 골자로 한 자동차관리법 일부개정법률안이 2024년 1월 국회 본회의를 통과했다. 사이버보안 관리체계(CSMS: Cyber Security Management System)는 자동차를 사이버 공격 및 위협으로부터 보호하기 위한 관리적, 기술적, 물리적 보호 조치를 포함한 종합적 관리체계를 의미한다. 기존에 정보통신사업자가 정보보호 관리체계(ISMS: Information Security Management System) 인증을 받았던 것처럼, 앞으로는 자동차 제작사들도 CSMS 인증을 받아야 할 것으로 전망된다.

이에 따라 모빌리티 인사이트는 커넥티드카 시장의 확대와 더불어 급부상하는 사이버보안을 주제로, '커넥티드카 사이버보안 실태 및 방향성은 어떠한가?'를 다루고자 한다. 이번 논의에서는 최근 현황과 이슈, 문제점 및 개선점을 살펴보고, 미래차 시장에서 사이버보안의 방향성과 그 의미에 대해 논의하고자 한다

소프트웨어 혁신으로 SDV 전환을 앞당기는 현대자동차그룹

SDV 개발 체제로 전환을 가속화해 모빌리티 기술 역량을 강화하고 있다.

스마트모비리티 시대 가상도
(출처: 현대자동차)

Section 01

커넥티드카 사이버보안 시장 동향 및 이슈는 무엇인가?

ADAS(Advanced Driver Assistance System)와 커넥티드 기능의 확대로 내·외부 연결성이 증가하면서 사이버보안의 중요성이 주목받고 있다. 최근 판매된 차량에 이커넥티드 기능 등이 탑재되면서, 자동차를 대상으로 한 사이버 공격이 차량 내·외부를 넘어 클라우드와 네트워크까지 확산할 수 있는 위험이 커졌다.

이에 다수의 글로벌 자동차 제조사가 사이버보안 문제를 중요시하고 있으며, 위험을 방지하기 위한 자동차 사이버보안 산업은 빠르게 성장하고 있다. 이런 변화 속에 그 중요성이 대두되고 있는 '커넥티드카 사이버보안 시장'의 현재 동향은 어떠하며, 어떻게 움직이고 있는가?

기차 중심으로 발전하고, 자율주행이나 정보통신 기술들이 접목되면서 알고리즘을 운용하는 것이 가능해지면서 자동차는 이제 소프트웨어 플랫폼화되고 있다. 또한 OTA(Over-The-Air), 무선 소프트웨어 업데이트 등의 기능이 일반화되면서 SDV(Software Defined Vehicle)라는 새로운 개념이 등장했다. 이러한 자동차 전반의 기술적 발전에서 사이버보안 영역은 제조사뿐만 아니라 소비자, 국가 간의 이슈로도 다뤄지고 있는 만큼 그 중요성이 매우 커지고 있다. 이런 관점에서 오늘 다양한 분야의 전문가분들을 모시고 함께 사이버보안에 대해 논의하는 뜻깊은 자리가 될 것으로 기대된다.

커넥티드카 시장 新영역 '사이버보안'

임강빈(좌장) 순천향대학교 정보보호학과 교수

오늘 '커넥티드카 사이버보안 실태 및 방향성은 어떠한가?'라는 좌담회 주제에서 중요한 키워드 중 하나는 바로 '커넥티드카'다. 커넥티드카의 초기 버전은 1996년 GM의 온스타로 당시 목적은 안전과 사고가 발생했을 때 차량에 대한 긴급 도움을 받는 것이었다. 운전자가 버튼을 누르면 상담원에 도움을 받을 수 있는 콜센터로 연결되는 방식이었다. 단순한 자동차 외부와의 연결 개념에서 시작된 커넥티드카는 비약적인 기술적 발전을 통해 2000년도를 넘어서면서 점차 모바일 망을 이용하게 되면서 점차 자동차 인프라와 연동하는 방향으로 발전하고 있다.

과거에는 텔레매틱스를 기반으로 긴급 지원 서비스와 같은 편의성 차원이었다면 점차 인터넷, 무선통신, 모바일 등의 IT 환경이 발전·변화하면서 자동차와의 연동 폭이 대폭 확대되었다. 이런 발전 과정에서 이제 자동차는 타고, 내리는 '이동수단'에서 사이버보안 관점에서 볼 때, '공격도구 혹은 공격대상'이 되고 있다. 특히 내연기관에서 배터리를 탑재한 전

커넥티드카 사이버보안 선택이 아닌 '필수영역'

심상규 아우토크립트(주) 부사장

개인적으로 2012년부터 자동차 보안을 연구하기 시작했다. 당시에는 많은 사람이 '자동차에 무슨 보안이 필요한가? 너무 오버 아닌가?'라고 했었다. 그러던 중 2015년 일명 '지프 체로키 해킹' 사건이 발생했다. 미국의 화이트 해커 두 명이 노트북을 이용해 체로키 차량을 해킹한 것이다. 이들은 차량과 무려 16km나 떨어진 곳에서 차량 내부 시스템에 접속해 조향 방향을 바꾸고, 가속을 마음대로 조작하기도 했다. 해킹 시연 영상을 보게 된 많은 사람은 차량 해킹으로 자동차에 대한 악의적 조작이 가능하고 이에 따라 목숨이 위협받을 수 있다는 것을 알게 되었고 전 세계에 큰 충격을 주었다. 이를 계기로 자동차 사이버보안에 관한 관심과 연구가 더욱 활발해졌으며 이후 차량에 대한 사이버보안을 위한 국제 표준들이 등장하기 시작했다. 대표적으로 UNECE WP.29, UNR.155(CSMS 인증), ISO/SAE 21434 등이 있다. 이처럼 자동차 사이버보안에 대한 국제 표준이 등장하면서부터 '왜 자동차에 사이버보안이 필요하며, 중요하냐?'는 이야기는 사라졌다.

이제는 자동차 산업에서 사이버보안은 필수영역으로 폭넓게 이해되고 있으며 시장 또한 성장하고 있다. 자동차 내 적용 범위도 텔레매틱스나 셀룰러 통신 채널 등에 적용하는 것을 넘어 자동차 내부 다양한 제어기들까지 사이버보안의 영역으로 점차 확대되고 있다. 한편 자동차 사이버보안에 대한 표준설정과 이를 위한 연구개발이 활발히 이루어지고 있으나 자동차가 빠르게 소프트웨어 중심으로 발전하면서 적용해야 할 범위와 기준, 검증, 신뢰성 확보 등에 대한 우려와 풀어야 할 숙제가 많은 상황이다. 또한 '커넥티드카'에 대한 용어도 확실한 개념과 정의가 필요하다. 커넥티드라는 단어에서 IT, 통신, 스마트폰, 클라우드와 같은 개념으로 많이 연상하는 것 같다. 그러나 자동차에서 커넥티드라는 개념은 단순한 통신 연결 그 이상으로 범위가 넓다. 자동차 내

출처 : 현대자동차 홈페이지

블루투스 통신, NFC 통신, UWB 통신뿐만 아니라 전기차 충전, 자동차 진단, 차량제어 등에 필요한 통신영역까지 커넥티드카 사이버보안의 개념은 폭넓다는 것을 지적하고 싶다.

자동차 사이버보안 표준과 규제 극복해야 할 '당면 과제'

송경식 (주)HL Klemove 연구원

오늘 자동차 사이버보안에 대한 주제를 논의하기에 앞서 기술적, 개념적 시장 동향에 대해 짚어주셨다면 이 영역에 있어 중요 포인트 중 하나가 국제적 혹은 국가 차원의 엄격한 '표준과 규제' 준수 여부가 OEM사 및 부품사가 당면한 과제로 대두되고 있다. 앞으로 자동차는 점차 커넥티드 형태로 발전할 것이고, 각종 표준과 규제를 통과해야 하는 당면 과제를 마주하는 현재 상황에서 국내도 자동차의 안정성 및 사이버보안 품질 향상을 위해 자동차 사이버보안에 대한 표준과 규제가 필요하다.

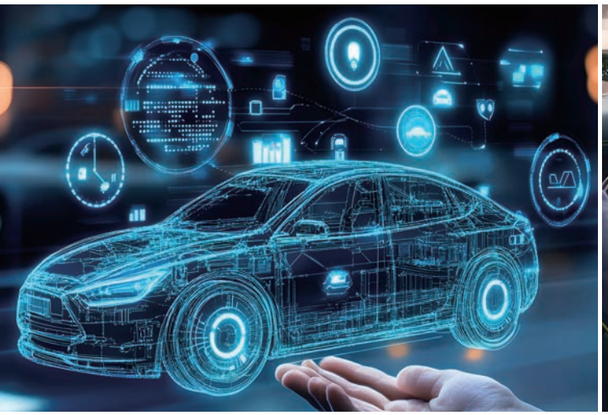
현재 자동차 생산 현업에서 자동차의 공격 지점으로 활용될 수 있는 외부 통신 컴포넌트들에 대한 보안대책을 지속해서 추진하고 있는데, 이는 앞서 언급한 바와 같이 자동차 사이버보안이 결국 고객의 안전과 재산과도 연결되기 때문이다. 이미 많은 OEM사들이 외부 컴포넌트에 대한 강력한 보안 메커니즘을 적용하기 위해 노력하는 이유도 여기에 있으며 완성차의 품질과도 직결되어 있다. 이러한 이유로 생산된 자동차의 품질 보증을 위해 엄격한 표준과 규제가 도입되어야 한다고 생각하며 사이버보안 프로세스를 준수하는 차량이 생산될 수 있도록 OEM사 및 부품사들이 함께 극복해야 할 부분이다.

이처럼 자동차에 있어 사이버보안은 자동차 전체 품질을 결정하는 중요한 결정요소로 작용하고 있으며 엄격한 표준과 규제 준수 그리고 사이버보안 관리체계 CSMS(Cyber Security Management System)에 입각한 부품 과 자동차 개발 여부가 기술력과 경쟁력을 증명하는 수단으로 사용된다. 결국 어느 때보다도 사이버보안에 대한 기술력과 경쟁력을 갖춰야 하는 시점에 도달했다고 볼 수 있다. 오늘 커넥티드카 사이버보안의 중요성과 경쟁력 강화에 대한 부분을 CSMS 관리체계와 프로세스 중심으로 말씀드리고자 한다.

커넥티드카 사이버보안 정확한 '품질목표·기준설정' 필요

권중한 LG전자 Cyber Security Governance Unit 책임

우리는 2020년부터 CSMS 관리체계를 준비하고 있다. 점차 자동차 사이버보안에 대한 표준과 규제 등이 확대되면서 그 중요성이 점차 커지는 가운데 많은 자동차 OEM사와 형식승인 등을 진행했다. 이런 과정을 겪으면서 OEM사의 사이버보안에 대한 요구사항이 점점 증가하고 있다. 자동차가 점차 소프트웨어, 커넥티드 중심으로 발전함에 따라 많은 OEM사나 부품사들은 여러 가지 V2X(Vehicle-to-X) 기능들이 탑재



현대자동차 제너시스 (출처 현대자동차 홈페이지)

되는 형태로 개발·생산하고 있다. 이는 그간 자동차를 구성하고 품질을 결정하는 주요 부분이 하드웨어나 장치 부품들에 있었다면 앞으로는 다양한 소프트웨어와 통신 간의 복잡도를 어떻게 관리하느냐가 중요한 경쟁 요소로 작용하고 있다는 것이다. 이는 단순한 변화를 넘어 자동차 산업 전반의 패러다임이 바뀌고 있다는 것이다.

이러한 변화 속에서 많은 보안 솔루션 개발업체와 기술업체들이 당사와 함께 협업을 하고자 많은 제안이 오는 것을 보면서 지금의 변화를 실감하고 있다. 많은 OEM사와 부품사들이 자동차 각 부분의 품질목표를 두고 개발·생산함에 있어 소프트웨어의 비중이 점차 커지고 있다. 이렇게 탑재된 소프트웨어들이 출시 이후 오류나 취약점 발생 가능성까지 고려해 개발해야 하는 어려움이 있다. 여기에 사이버보안이라는 주제가 추가되면서 그간 명확한 정의와 수치로 품질목표를 관리할 수 있었던 것에서 경우에 따라 획일적으로 적용할 수 없는 사이버보안 품질목표를 어떻게 설정하느냐는 자동차 업계 전반에 걸쳐 매우 어려운 숙제로 대두되고 있다.

커지는 사이버보안 시장 더 빠른 '기술, 정책 대응' 필요

정원선 한국자동차연구원 인천사무소 센터장

우선 커넥티드카의 기본적인 기술적 정의는 '양방향 무선통신'이 가능한 자동차를 말한다. 커넥티드카를 이러한 '양방향 무선통신'이란 기준으로 볼 때, 국내뿐만 아니라 전 세계적으로 신차 발매 기준 약 90% 이상이 커넥티드카에 해당한다. CSMS를 적용하는 제품과 부품을 볼 때 CAL(Cybersecurity Assurance Level) 레벨 3, 4까지 인증받는 데에는 좀 더 노력해야 하는 상황이며 나머지 부품들에 대해서는 아직은 괜찮은 상황이다. 다만 우리와 같이 자동차 사이버보안 쪽에서 일하는 실무자들 관점에서 그간 다양한 표준과 규제들이 등장하면서 이것이 우려 상황이 아닌 실제상황으로 변화하면서 사이버보안에 대한 경각심이 높아졌다.

이런 측면에서 외국과 비교하면 국내에서는 다소 사이버보안에 대한 인지와 준비가 좀 늦어진 감이 없지 않다. 외국의 경우 10여 년 넘게 사이버보안 분야에 상당한 관심과 투자, 연구가 진행되고 있었으며 이를 바탕으로 한 다양한 정책도 마련되고 있다는 점에서 시사하는 바가 크다. 따라서 지금이라도 사이버보안에 대한 기준과 대책 및 정책들이 정부와 기업 차원에서 추진되어야 할 것이다.

이에 정확하게 커넥티드카를 분류하고 사이버보안 레벨을 분류해서 보안이 취약한 부분부터 우선 해결해 나가는 노력이 필요한 시점이다. 또한, 단순한 통신 부분을 넘어 자동차 제어장치에까지 사이버보안의 범위가 넓게 적용되고 있는 현실을 고려한 적극적인 대응이 절실하다. 여기서 짚어봐야 할 또 하나의 포인트는 앞으로 자동차는 SDV로 발전할 것이고, 이에 따라 OTA가 점차 확대, 적용될 것이라는 점이다. 게이트웨이나 일부 통신 모듈에 국한해서 사이버보안을 적용하는 수준을 넘어 현대차는 CCU(Central Communication Unit)에 사이버보안을 적극적으로 적용하는 방안을 세우고 있다. 그러나 이것도 전체 사이버보안 시장에서 보면 작은 부분이고 더 넓은 범위에서 더 빠른 대응이 필요하다.

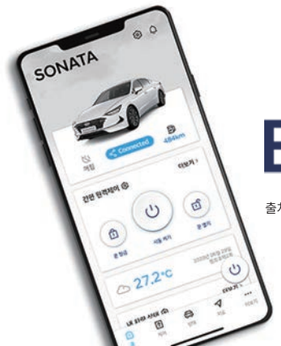
사이버보안 이슈 기술관점을 넘어 '외교관점'에서도 중요

연원호 국립외교원 경제기술안보연구 센터장

저는 업무 특성상 국가 간 외교, 무역 측면에서 말씀드리고자 한다. 특히 미·중 관계의 틀에서 커넥티드카 이슈에서 특정 국가 제품을 활용하는 부분에도 사이버보안을 고려해야 한다는 포인트를 지적하고 싶다. 올해 초 미국 바이든 대통령이 중국 등 우려 국가에서 생산된 일정 품목들을 활용한 커넥티드카의 위험성을 조사하여 필요한 조치를 하라는 뉴스가 나왔다. 그 당시 국내 많은 언론은 중국의 전기차 이슈에 초점을 맞췄다. 그러나 전체적인 미·중 간의 무역 대립이란 흐름에서 볼 때 이는 단순한 전기차 이슈보다 정보통신 서비스 이슈라고 생각한다.

미국은 2018년 수출통제개혁법(ECRA: Export Control Reform Act)을 제정하여 신흥 및 기반 기술(EFT: Emerging and Fundamental Technologies)을 지정하여 본격적으로 신기술 수출통제 정책을 추진하고 있다. 특히, ICT(Information & Communications Technology)와 관련된 중국 특정 기업들의 제품에 대한 제재를 강화하고 있다. 대표적으로 화웨이나 ZTE는 5G 기업이고, 하이크비전이나 다후아테크놀로지는 CCTV 기업이고, 하이테라는 무선통신 기업인데 이런 다섯 기업을 명시하면서 이들 기업의 제품을 사용하지 않도록 경고하고 있다. 이후 2019년에는 틱톡이나 위챗까지 언급하게 이르렀다. 또한, 2023년 12월 미 상무부 산하의 국가안보 및 첨단기술이 관련된 문제를 다루는 기관인 BIS(Bureau of Industry and Security)가 생겼으며, 여기서 최초로 나온 규정이 바로 올해 2월에 있었던 커넥티드카 이슈다. ICT 정보통신 서비스를 다루는 부서에서 처음으로 다룬 것이 커넥티드카를 이슈화했다는 점이 주목할 만하다.

이런 전체적인 흐름과 맥락으로 볼 때, 단순한 전기차 이슈가 아닌 정보통신 서비스 이슈임이 분명하다. 앞으로 이 이슈는 미·중 관계가 개선될 가능성이 크지 않다는 전제하에서 보면 점차 중국산 부품을 완전히 배제하는 방향으로 갈 것이다. 이것이 미국의 궁극적인 목표이며 이런 상황에서 우리나라도 자유로울 수 없다는 것이 크게 우려되는 점이다.



Bluelink

출처 : 현대자동차 홈페이지

Section 02

커넥티드카 사이버보안의 중요도는 어떠한가?

지금까지 자동차는 출력, 연비, 가속력 등 하드웨어 퍼포먼스를 중심으로 개발되어 왔다. 그러나 전동화, 전장화가 진행되면서 자동차는 하드웨어보다 소프트웨어 중심으로 개편되고 있다.

소프트웨어의 중요성이 높아지면서 자동차 연결성이 확장됨에 따라 자연스럽게 사이버보안에 관심이 높은 상황에서 사이버보안은 얼마나 중요한 요소인가?

사이버보안의 중요성 자동차 '시장 전반'에 작용

임강빈(좌장) 순천향대학교 정보보호학과 교수

앞서 사이버보안 산업 동향 및 기술적인 부분에 대해 논의했다. 또한, 사이버보안의 관점을 어떤 특정 영역이 아닌 전반적인 기술 요소 모든 부분으로 초점을 다각적으로 봐야 한다는 의견도 있었다. 새로운 관심 시장이나 신산업 영역에서 무엇보다 중요한 것은 순발력 있는 대응력이라고 생각한다. 이미 오래전부터 사이버보안 관점에서 자동차 내 기능 안전 부분을 시작으로 이후 IT 기반의 특수한 보조 기능들이 추가되면서 사이버보안에 관한 관심과 시장은 커졌다. 그러면서 다양한 국제 표준과 규제들이 만들어지고 있다. 그리고 이에 대응하기 위해 관련 유관 주체들이 사이버보안에 대한 지금의 현실과 우려 사항들에 대해 선제적으로 대응책을 마련하는 노력이 필요했다. 그러나 지금 우리의 현실은 외부로부터의 압력이나 제재가 있어야만 움직이는 다소 수동적인 부분이 많다. 지금이라도 사이버보안에 대한 중요성을 인식하고 이에 대한 빠른 대응과 대책이 시급한 상황이다. 보다 구체적으로 말하면 지금의 표준과 규제 수준에 맞춰 대응하기보다 그 이상의 기준에서 더 깊고, 더 세부적인 고민에서 이를 준비하는 방향으로 발전해

야 한다고 생각한다. 또한, 자동차 공급망 보안 측면에서도 중요한 사안들이 많다. 자동차 생산, 판매, 소비에 있어 사이버보안의 중요성에 대해 논하고자 한다.

커넥티드카 사이버보안 국가간 '보안이슈'로 확대

연원호 국립외교원 경제기술안보연구 센터장

커넥티드카와 사이버보안의 주요 이슈를 간략하게 세 가지로 정리해 보고자 한다. 첫째, 자동차 차체에 대한 내·외부 공격으로 탑승자의 안전을 위협할 수 있다는 점이다. 만약 차량 내 국가적으로 중요한 인물이 탑승하고 있다면 이는 국가적, 국제적 안보 이슈에까지 이를 수 있다는 것이다. 둘째, 자동차를 하나의 매개로 주변 교통 및 시설 인프라를 교란, 마비시킬 수 있다는 것이다. 셋째, 차량 정보 및 데이터 보안 측면에서 작게는 개인정보에서부터 차량 위치정보 등 다양한 차량 정보 데이터를 수집하여 적국에 넘어갈 수 있다는 우려 등이 주요 이슈다.

이러한 세 가지 측면에서 앞으로 자동차 사이버보안의 중요성은 매우 높다. 또한, 외교통상무역 측면에서도 미국의 규제 조치 내용이 광범위하며 강력하기에 우선하여 그 범위를 제한해야 한다는 현장의 목소리가 높다. 예를 들어 ICT 부분에 한정해서 중국산 부품을 배제한다든가, 자동차에 필요한 카메라나 센서에까지 전방위적으로 중국산을 배제하는 것은 현실적으로 문제가 많다는 의견이 많다. 물론 향후 미국의 움직임을 자세히 주시해야겠으나, 미국의 큰 방향성은 특히 사이버보안에 있어 중국산을 배제하라는 것이 분명하다. 이에 정부나 국내 기업들은 이러한 현실에 입각한 현명한 접근과 대책 마련이 필요하다. 본 자동차 사이버보안과는 다른 영역의 예를 들면, 우리나라 국방부가 최전방 감시카메라를 중국산으로 도입해 사용했는데 이때 중요 군사정보가 중국으로 넘어가는 것이 아니냐는 이슈가 있기도 했었다. 결국, 미·중 간의 외교무역 대립에 있어 각국의 안보 이슈가 크게 작용하고 있는 것이며, 이제 자동차 사이버보안 영역도 이런 관점에서 볼 때, 그 중요성은 앞으로 더 커질 것으로 예상한다.

어느 때보다 중요한 사이버보안 기업뿐만 아니라 '정부의 역할' 중요

정원선 한국자동차연구원 인천사무소 센터장

자동차 업계에서 일하고 있더라도 사이버보안 관련 업무를 하지 않는다면 지금의 이슈를 정확하게 이해하기는 어려울 것이다. 20여 년 전 처음 업계에 ERP 시스템을 전사적으로 적용할 때도 상당한 혼란과 시행착오가 있었다. 아마도 지금의 상황은 그 당시보다도 더 복잡하고 혼란스러울 것이다. 왜냐하면, 사이버보안 이슈가 단순히 어느 부품에 한정된 것이 아니라 전사적인 시스템을 새롭게 구축해야 하는 사안이기 때문이다. 따라서 지금 ERP 시스템이 대기업뿐만 아니라 중소, 중견기업까지 넓게 적용되는데 거의 10여 년의 시간이 필요했던 것처럼 사이버보안 시스템을 전방위적으로 구축하는데 그만한 시간과 노력이 필요할 것으로 본다. 과연 그 시간 동안 얼마만큼의 시행착오가 있을지, 또한 그러한 준비를 정부나 기업이 얼마나 빠르게 대처하고 대응할 수 있을지가 가장 큰 관건이다.

오늘 참석하신 분들은 그나마 사이버보안에 대한 이해도나 업무 진척이 있으시지만, 기업 규모는 큰데도 사이버보안에 대한 전문가가 없는 기업도 많고, 일반 제조업체들은 아예 사이버보안에 대한 이해나 인지 수준이 매우 떨어진 경우도 많다. 이런 기업들을 만나서 도움을 주고 싶어도 현실적으로 어려운 부분이 많다. 이런 가운데 사이버보안에 대한 인식을 환기하고 공론화하기 위해 힘들지만 노력하고 있다. 또한, 미국의 규제, 법규 이전에 유럽이 먼저 규제, 법규 제정을 시작했다. 이미 많은 국내 자동차, 부품 기업이 유럽 등에 수출을 하면서 사이버보안에 대한 중요성을 인지했음에도 대응이 다소 안일하지 않았나 싶다. 미국의 강력한 제재가 현실화하는 상황에서 CSMS의 중요성은 더욱 커질 것이며, 여기에 기술, 부품의 원산지까지 따지기 시작하고 있다. 따라서 지금의 사이버보안에 대한 이슈는 단순히 기업 차원을 넘어 정부도 함께 자동차 산업 전반을 재편하는 중대사임을 인식하고 현실적인 대응 전략을 면밀하게 준비해야 한다.

강화되는 규제법규 대응 정부와 기업 '지원·협력 관계' 절실

권중한 LG전자 Cyber Security Governance Unit 책임

현재 사이버보안의 중요성은 이미 미국과 유럽 중심으로 본격화되고 있는 다양한 규제와 법규들이 등장하고 있다는 것만 보아도 잘 알 수 있다. UNR 155뿐만 아니라 RED(Radio Equipment Directive)까지 보안 관련 내용을 추가하여 내년 8월부터 규제를 시행한다는 상황이다. 이에 업계 입장에서는 이러한 규제와 법규를 지키면서 극복하기 위해 노력하고 있으나 각종 규제와 법규 시행 시점이 빠르게 도래할 것이므로 긴장도가 높은 상황이다. 현재 시행 예정인 규제들에 대해 중복규제 등의 이슈도 거론되나 일단 시행을 하면서 차차 조정하는 방향으로 진행되고 있다. 주로 EU 중심으로 규제는 계속 강화될 것이다. 특히 UNR 155의 경우 자동차 제조부터 폐기에 이르기까지 전체 과정을 아우르고 있으며, 각종 증거자료를 증빙해야 하는 상당히 큰 규모의 규제

내용을 담고 있기에 이에 대한 대응을 위해 기업들이 노력하고 있다. 또한, 완성차 제조사에서는 Tier1을 비롯한 하위 부품사들에까지 사이버보안 역량 확인이나 그 산출물에 대한 사이버보안 평가까지 요구하고 있다. 어느 한 기업이 CSMS 관리체계를 잘 구축하고 운영하느냐보다 복잡한 공급망 안에서 사이버보안 관련 위험까지 포괄적으로 관리해야 한다는 측면이 현실적으로 어려운 부분이며 동시에 중요한 부분이다. 우리도 사이버보안 관련 협력업체들과 다양한 방법으로 소통하며 사이버보안 대응력 강화 방안을 다각적으로 논의하고 있다. 그러나 자사에서 사이버보안의 중요성에 대해 협력업체 인식을 개선하고자 노력하고 있으나, 아직도 많은 협력업체의 인식수준이 낮은 것이 사실이다. 중대 문제임에도 불구하고 사이버보안에 대한 경각심과 대응 방안이 미흡한 기업이 많다. 이런 취약 기업들을 대상으로 정부 차원에서 적극적으로 지원하고 인식을 개선할 수 있는 제도나 프로그램을 만들어 활용한다면, 우리 같은 기업 입장에서 협력업체들과 더 원활한 의사소통이 될 것이고, 이를 통해 더 현실적이고 효과적인 사이버보안 대응책을 만들 수 있을 것이다.

사이버보안의 중요성 자동차 품질의 '새로운 척도'

송경식 (주)HL Klemove 연구원

앞으로 차량의 사이버보안 품질은 곧 차량 전체 품질과도 연결된다는 측면에서 그 중요성은 더욱 높아질 것이다. 이와 관련하여 지난 2021년 미국 시장에서는 보안 기능 문제로 특정 브랜드 차량이 집중적으로 도난 당하는 사건이 발생하였다. 당시 관련 조사를 한 결과, 전체 도난 차량의 50% 정도가 해당 브랜드 차량으로 밝혀졌다. 뉴욕을 비롯한 일부 주에서는 해당 차량에 대해 도난에 노출되었다는 이유로 소송까지 진행되기도 했다.

사이버보안의 품질 저하는 결국 브랜드 이미지에도 나쁜 영향을 미치고, 이는 곧 판매 저하라는 악순환을 피할 수 없기에 기능 안전뿐만 아니라 사이버보안에 대한 중요성은 더욱 커지고 있다. 소비자 권리 차원에서도 사이버보안의 중요성은 커지고 있다. 소비자에게 가장 중요한 요소가 차량 안전 부분인데 사이버보안에 관련된 보안 매커니즘을 세심하게 살펴보고 구매를 결정해야 한다는 인식이 확산하고 있다. 앞에서도 체로키 해킹 사건을 말씀하셨듯이 가능성이 작기는 하지만 외부로부터의 공격을 통해 임의적인 조작이 가능하게 된다면, 이는 차량과 탑승자에게 아주 치명적일 수 있다.

차량은 점차 커넥티드화 될 것이 분명하며 이런 커넥티드카에 있어 사이버보안의 중요성은 아무리 강조해도 부족하지 않을 것이다. 그렇기에 미국을 비롯한 유럽 국가들이 앞다투어 관련 규제와 법규를 만들고 있으며 다른 많은 국가도 자국의 이익과 안전을 위해 사이버보안에 대한 규제와 강도를 높일 것으로 본다. 결국, 그간 자동차 안전에 대한 부분이 기계적인 부분에 집중했었다면 앞으로는 사이버보안 등과 같은 영역의 중요성이 더욱 부각 될 것이다.

사이버보안 미래차 '가치와 안전'의 핵심

심상규 아우토크립트(주) 부사장

자동차 사이버보안을 논함에 있어 다소 자동차 제조 입장에서만 생각하는 경향이 있다. 그러나 자동차를 구매하는 소비자 입장에서 사이

포티투닷 자율주행 셔틀. (출처 : 포티투닷)

Section 03

커넥티드카 사이버보안 경쟁력 강화를 위한 육성 방안은?

앞으로 자동차는 더욱 정교하고 첨단화된 소프트웨어 중심으로 발전할 것이라는 예상이 지배적이다. 이는 기존에 경험하지 못한 새로운 보안에 대한 숙제까지 늘어날 것이다. 당면하고 있는 사이버보안에 대한 규제와 법규를 통과해야 한다는 측면을 넘어 궁극적인 브랜드 가치를 높이는 차원에서도 사이버보안의 중요성은 어느 때보다도 높다. 이런 상황에서 국내 OEM사들과 많은 부품사가 사이버보안의 신뢰성을 높이기 위한 노력은 어떻게 해야 하며 더 나아가 글로벌 경쟁력 확보를 위한 도전과 극복 과제, 육성 방안은 무엇인가?

버보안의 중요성을 생각해 볼 필요가 있다. 자동차는 다른 제품과 달리 상당한 고가이며, 생명과 직결된다는 측면에서 안전에 대한 대안은 필수적이다. 결국, 소비자들은 안전하고 믿을 수 있는 자동차를 원한다. 따라서 기계적 안전뿐만 아니라 사이버보안에 대한 안전을 요구하는 것은 당연하다. 자동차는 점점 첨단화, 기능화되고 있으며 이런 기술적 발전이 다양한 장치를 추가로 탑재할 수밖에 없다. 새롭게 추가되는 장치들에 대한 검증과 신뢰도를 확보하는 문제는 그래서 힘들고 어려운 것이다.

따라서 단순하게 규제나 법규를 통과해야 한다는 시각을 넘어 인간과 생명에 대한 소중함을 이해하는 근본적인 인식 전환이 필요하다. 법적 기준을 통과했다는 사실이 중요한 것이 아니라 소비자의 근본적인 안전을 위한 확실한 대안을 기술적으로 마련해야 한다는 사명감으로 사이버보안의 중요성을 이해할 필요가 있다. 이런 노력으로 자동차에 대한 신뢰를 쌓아야만 경쟁력도 생기고 판매도 증가할 수 있다. 사이버보안에 대한 신뢰도를 높이려면 무엇보다도 이 부분에 대한 과감한 투자와 연구개발이 선행되어야 한다. 그리고 사이버보안을 이야기하면 SDV 내 소프트웨어에 들어간 부품의 보안이라는 협소한 시각들이 있는 것 같다. 현업에서 많은 해외 OEM사들을 만나보면 그들의 요구범위는 제어기 안에 들어간 메모리 모듈 형태, 그리고 메모리를 제어하는 펌웨어 레벨까지 포함하여 매우 넓다.

국내·외 OEM사의 사이버보안에 대한 요구사항을 만족시키지 못한다면 아마도 산업 내에서 빠르게 도태될 것이다. 또한, 전기차를 비롯한 새로운 형태의 OEM사들이 늘어날 것이고 이들의 사이버보안에 대한 요구사항 또한 많아지고 그 수준 또한 높아질 것이다. 그만큼 자동차에 있어 사이버보안의 중요성은 더욱 커질 수밖에 없다.

사이버보안 경쟁력 강화 '국가산업 차원'의 시각 필요

임강빈(좌장) 순천향대학교 정보보호학과 교수

지금까지 커넥티드카 사이버보안이란 주제를 놓고 시장 동향과 그 중요성 등에 대해 심도 있게 논의했다. 결국, 자동차에 있어 사이버보안은 단순히 부품과 통신만의 영역을 넘어 자동차 전반의 품질을 결정하는 새로운 '중요요소'라는 점에 대해서는 이견이 없다고 본다. 이는 자동차 신뢰성 확보 차원에서 사이버보안은 보안 안전 관점에서 각 부품과 기능들의 가용성이란 관점에 이르기까지 광범위하게 적용된다. 또한, 자동차 자체의 안전이란 관점을 넘어 국가 간의 안보 이슈까지 등장하면서 사이버보안에 관한 연구와 개발의 필요성은 중요한 과제로 대두되고 있다. 여기에 글로벌 표준과 규제, 법규들까지 등장하면서 자동차 산업뿐만 아니라 국가산업이란 넓은 범위에서도 이를 극복하고 경쟁력을 높이려는 노력은 필수적이다. 그리고 구상만이 아닌 실질적인 대응 방안이 필요한 시점이다. 이제 사이버보안의 중요성과 경쟁력 강화, 글로벌 규제, 법규를 극복하기 위해 어떠한 노력과 준비가 필요한가에 대해 논하고자 한다.


테슬라 모델Y (출처 : 테슬라)

사이버보안 이슈를 새로운 기회로 정부, 기업, 관련 단체 '긴밀한 협력' 절실

연원호 국립외교원 경제기술안보연구 센터장

미국의 자료 가운데 소프트웨어 관련 리콜이 평균 5% 정도 수준이었으나 작년은 약 15% 정도까지 높아졌다는 내용이 있다. 물론 모든 소프트웨어 리콜이 사이버보안 이슈는 아니겠으나 사이버보안에 대한 중요성을 이 부분에서도 유추할 수 있다. 사이버보안 이슈가 이제는 외교통상 무역 측면에까지 영향을 미치고 있다. 각종 규제와 법규를 통해 특정 국가의 품목을 배제해야 한다든지 하는 수출입 장벽으로 작용하고 있다는 점은 그 중요성과 심각성이 매우 높다. 이런 국가 간 무역에 있어, 특히 미·중 간 무역경쟁에서 사이버보안이 크게 대두되고 있다는 점은 앞으로 관련 기업이나 정부 부처가 어느 때보다도 빠르게 움직여야 한다는 경각심과 시급성을 공유하는데 주요 포인트로 작용할 수 있다고 본다.

미·중 간의 무역경쟁에서 대중국 견제로 사이버보안을 활용하고 있다는 점에서 우리에겐 위기이기도 하지만 새로운 기회가 될 수도 있을 것이다. 이는 미국이 중국산 부품을 배제하겠다는 방침을 고수한다면, 이 부분을 우리 업체들이 파고 들어갈 수 있다면 또 다른 기회로 작용할 수도 있다는 것이다. 물론 완성차 제조사 입장에서는 중국산 부품을 배제한 공급망을 재편해야 한다는 점에서 비용상승 등의 악재들이 있을 수 있으나 국내 제조사들의 기술 수준이 상당히 높은 것을 잘 활용한다면 극복하지 못할 난제는 아니라고 본다. 물론 지금의 국제무역 관점에서 기업만의 노력으로는 이를 극복하기 쉽지 않을 것이다. 따라서 정부 차원에서도 지금의 사이버보안에 대한 국제적 흐름과 각국의 규제, 법규를 면밀하게 검토하고, 업계와의 긴밀한 협력이 매우 중요하다. 이를 위해 구체적인 로드맵과 제도 및 프로세스 개선, 교육과 공론화 등을 통한 효과적인 극복 방안을 마련해야 할 것이다. 산업부를 비롯한 정부 관련 기관들이 제조사뿐만 아니라 부품업체, 한국자동차연구원과 같은 협력 기관 등과 긴밀한 소통을 통해 국가 차원에서 적극적인 대응 방안을 마련해야 할 것이다.

사이버보안 글로벌 경쟁력 강화 보다 넓고 높은 '관점의 변화'에서부터

정원선 한국자동차연구원 인천사무소 센터장

사이버보안의 이슈는 우리 자동차 산업에 어느 정도의 타격은 불가피할 것으로 본다. 이런 측면에서 어떻게 하면 그 피해 규모를 줄이고, 이를 전화위복으로 만들 것인가가 관건이다. 단기적인 방안으로 현재 사이버보안 관련 인력과 시설이 절대적으로 부족한 상태다. 이를 각 기업이 단시간에 끌어올리기에는 현실적으로 무리가 있다. 따라서 사이버보안에 대한 연구개발을 하나의 공공재 성격으로 키우는 방안을 생각해 볼 수 있다.

미국의 경우 마이터(MITRE)란 비영리단체를 만들어 항공, 방위, 의료, 국토안보, 사이버보안 분야 등의 다양한 미국 정부 기관을 지원하는 임무를 수행하고 있다. 이들의 모든 연구성과를 업체들이 함께 공유, 활용하고 있으며 국내에도 이러한 사이버보안 관련 전문단체를 만들면 단기적으로 큰 효과가 있을 것으로 본다. 중장기적 방안으로 해외 주요 기관들과 얼라이언스 및 협력 관계를 구축하여 이를 극복하는 방안을 검토할 수 있다. 미국에서는 자동차 사이버 보안 문제와 관련해 자동차, 부품 제조사 등이 정보를 공유하여 공동대응하기 위한 AUTO-ISAC이라는 민간 협의체가 운영되고 있다. 일본은 미국의 AUTO-ISAC 단체의 동향을 살펴보면서, AUTO-ISAC이 생기자마자 AUTO-ISAC JAPAN을 만들어 이들의 내용을 교류, 공유하는 방안을 만들었다. 이렇듯 지

금의 사이버보안 이슈는 정부나 기업만으로 극복하기 어려운 글로벌 이슈임에 국제적인 단체나 기관과의 긴밀한 교류와 협력을 통한 방안도 고려해 볼만 하다. 앞서 지금의 사이버보안 이슈가 우리에게 기회가 될 수도 있다는 말씀이 있었는데 우리나라의 IT기술과 보안 솔루션의 기술은 우수하나 이것이 자동차와 연계되는 부분에서는 여전히 취약하다는 이미지가 팽배하다.

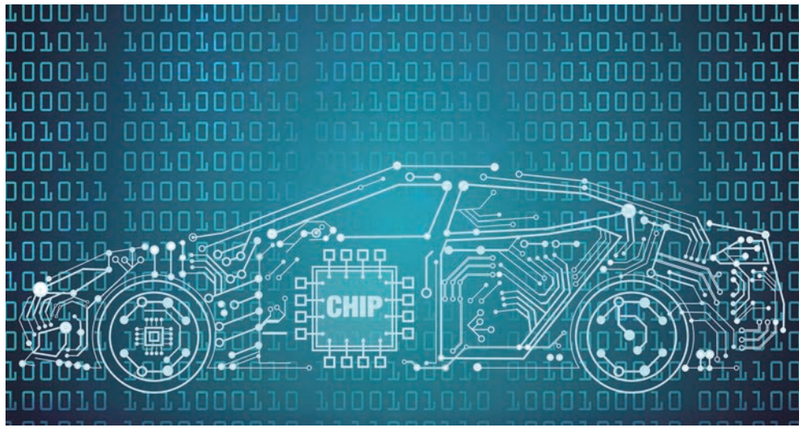
따라서 국내 제조사 및 부품사들이 중국산 기술, 제품을 대체할 수 있으려면 기술 발전뿐만 아니라 국가적 이미지도 상당히 중요하다. 또한, 단편적으로 규제, 법규를 통과했다는 점을 어필하는 수준을 넘어서 이를 검증하는 대표성을 갖는 사이버보안 품질지수를 만드는 것도 방안이라고 본다. 미국의 JD파워, 유럽의 NCAP와 같은 품질지수를 기준으로 브랜드 및 차량에 대한 신뢰도를 확보하고 있다. 이와 같이 우리의 사이버보안 품질지수를 개발, 강화하고 대표성을 확보하여 우리 기업의 사이버보안 품질지수가 높다는 인식을 심어 경쟁력을 강화하는 것이다. 하나의 아이디어로 인텔이 'Intel Inside'라는 캠페인으로 브랜드 가치를 높였듯이, 사이버보안 영역 또한 하나의 한류 브랜드 'K-Security Inside'라는 캠페인을 적극적으로 벌여 국가적인 브랜드 가치를 높이는 방안도 생각해 본다. 결국, 사이버보안의 글로벌 경쟁력을 강화하고 이를 극복하기 위해서는 기업만의 노력과 우리나라 안에서만 해법을 찾기보다는 글로벌 협력과 트랜드를 리드하는 구체적인 실행 방안들을 정부와 업계가 협력하여 마련해야 할 것이다.

사이버보안 경쟁력 강화 '적극적이고 긍정적인 자세'에서 시작

권중한 LG전자 Cyber Security Governance Unit 책임

지금까지 사이버보안과 관련하여 규제 대응 측면에서 기술적인 부분, 환경변화, 업계 흐름에 대해 말씀하셨는데 기술적 관점에서 볼 때, 지금 자동차에 적용하는 사이버보안 기술은 완전히 새로운 것은 아니라고 본다. 기존에 있던 IT 보안의 테두리에서 개발된 솔루션들을 자동차의 분산된 아키텍처와 임베디드 환경, 리얼타임 환경에 어떻게 적용할 것인가? 즉, 커스터마이징을 얼마나 효율적으로 잘 하고 있느냐의 관점으로 볼 필요가 있다. 기술 판매와 솔루션 공급업체 입장에서 최근 중요한 변화는 자동차 아키텍처 자체가 급변하고 있다는 점이다.

이런 변화 속에 자동차 제조사 입장에서는 각각의 환경에 맞는 솔루션을 요구하고 있으며 이러한 다양한 아키텍처의 장단점을 분석하여 최적화된 해법을 제공해야 하는 것이 우리들의 핵심과제다. 그리고 또 하나 중요한 부분이 출시 이후의 대응 영역이다. 소프트웨어의 취약점은 제



품 출시 이후에도 계속 발생할 수밖에 없기에 부품사에서도 일정 기간 사이버보안 모니터링, 위협 식별, 대응 조치를 할 수 있는 체계를 구축해야 한다. 이를 위한 이를 위한 사이버보안 전문 인력 수급도 현실적인 어려움 중 하나다. 업계에서 당면한 여러 이슈를 극복하고, 글로벌 사이버보안 경쟁력 강화를 위해서는 한국자동차연구원과 같은 전문기관 등에서 관련 기업들을 지원하고 정부, 기업, 학계의 협력 방안을 만드는 것도 중요하다고 본다. 이를 통해 국내 자동차 관련 기업의 사이버보안 경쟁력을 강화한다면, 규제를 발판으로 삼아 중국산 부품을 국산으로 대체하는 새로운 기회로 활용할 수 있을 것이다.

사이버보안 경쟁력 제도개선만큼 '인식개선' 중요

송경식 (주)HL Klemove 연구원

오늘 사이버보안과 관련하여 기술적, 규제, 법규, 외교통상 등 다양한 부분에 걸쳐 논의했다. 실무자로서 OEM사를 비롯한 관련 업체 임직원들의 사이버보안에 대한 인식과 태도 변화도 중요하다고 본다. 관련 법규 통과를 위한 기술개발이나 이를 극복할 방안이 결국은 관련된 사람들로부터 시작하기 때문이다. 자동차 제조사, 부품사, 협력사 임직원들의 인식개선이 필요하며 이를 위해 정부 차원의 사이버보안 교육 등을 제도화하여 사이버보안에 대한 중요성을 정확하게 인식할 필요가 있다. 인식변화를 통해 사이버보안에 대한 적극적인 관심과 투자를 높여서 전문인력을 양성, 채용 부분이 해결되어야만 더욱 경쟁력 있은 연구개발에 집중할 수 있으며 이는 곧 전체 자동차 품질향상과 직결되기 때문이다. 결국, 지금의 사이버보안 이슈를 극복하고 경쟁력을 강화하기 위해서는 정확한 상황인식, 제도개선, 중장기적 교육, 우수인력양성 등 다각적인 부분에서 노력이 필요하다. 또한, 사이버보안의 해법은 단순한 제조사, 부품사 등의 분절적인 부분이 아닌 전체적인 연장선에 있다는 점에서 정부, 제조사, 부품사, 관련 기관 등이 각 영역에서 사이버보안의 경쟁력을 높이기 위한 노력을 함께해야 한다.

특히 무엇보다도 정부 차원에서 과감한 지원은 필수 불가결한 요소라고 본다, 여기에는 교육지원도 필요하나 기술개발에 직접 필요한 자금지원 등의 파격적인 지원제도를 전면적으로 개선하는 노력도 필요하다. 기술력은 있지만, 자본과 인력이 부족한 기업들을 적극적으로 지원함으로써 기존 대형 업체들뿐만 아니라 소규모 업체들도 함께 육성하는 것이 탄탄한 산업기반을 만드는 데 크게 도움이 될 것이다.

사이버보안 경쟁력 '정부의 역할'에서 기회를 찾는다.

심상규 아우토크립트(주) 부사장

지금 자동차 사이버보안에 관한 관심과 중요성을 논의하는 것이 어쩔 수 없이 글로벌 규제 및 법규의 영향에서 시작한다고 본다. UNR 155를 중심으로 관련 규제와 법규는 글로벌 차원으로 시작된 상황에서 국내 관련법의 개정 및 시행령들도 하루빨리 마련되어야 그 기반 위에 실질적인 체계를 갖출 수 있을 것으로 본다. 사이버보안을 적용하더라도 결국 평가 부분이 중요한데 아직은 초기 단계에 있는 것이 사실이다. 또한, 사이버보안 교육 관련하여 단발적인 지원이 아닌 지속적인 관리운영 차원에서 기업의 자생력을 갖출 수 있는 방향으로 개선되어야 할 필요성이 있다. 사이버보안 적용 이후 유지, 운영 측면에서 개별 기업들이 이것을 모두 감당하기에는 비용적으로 무리가 있다, 앞서 말씀하신 공공재 개념으로 상호공유하자는 의견은 이런 면에서 타당한 방안이라고 생각한다.

지금도 국내 정부 주도하에 산학연 협력 등의 프로그램은 있으나 유럽과 같이 사이버보안에 대해 집중적으로 연구·개발하는 프로그램은 부족한 것 같다. 지금이라도 우리나라도 사이버보안에 대한 전문적인 기관을 통한 산업지원책을 마련하는 부분도 함께 더욱 적극적으로 논의할 필요가 있다. 그런 탄탄한 기반을 갖춰야만 방대한 사이버보안 이슈를 효과적으로 극복할 수 있을 것이다. 현재 우리나라가 사이버보안에 대한 부분이 해외보다 다소 뒤처져 있는 것이 사실이지만 이런 상황에서도 우리나라가 경쟁력을 가질 수 있는 데이터, 서비스 부분에 특화하여 집중하는 방안도 생각해 본다. 결국, 사이버보안 이슈를 극복하기 위해서는 정부 역할이 무엇보다도 중요하다. 이는 사이버보안의 성격상 기술적인 부분뿐만 아니라 제도와 정책이 함께 발전해야 한다는 측면에서 사이버보안의 중요성을 정부에서부터 그 심각성을 인식하고 관

련 제도개선과 기업지원, 협력 프로세스를 갖추는 것이 우리가 지금의 위기를 기회로 바꿀 수 있는 계기가 될 것이다.

사이버보안 이슈 공론화 해법을 찾는 '중요한 시작'

임강빈(좌장) 순천향대학교 정보보호학과 교수

오늘, 다양한 분야의 전문가들과 함께 긴 시간에 걸쳐 자동차 사이버보안에 대해 열띤 논의를 나눌 수 있어 매우 보람 있었다. 순수 연구를 수행하는 대학의 입장, 현장에서 활동하는 업계의 관점, 외교무역과 국가안보에 중점을 둔 기관의 입장 등 각 분야에서 소중한 의견을 공유해 주신 모든 분들께 감사하다. 특히, 대학, 업계, 연구기관, 외교부 등 다양한 입장이 존재함에도 불구하고, 오늘과 같은 자리에서 공통된 주제인 사이버보안에 대해 의견을 모으고 인식을 공유하는 과정이 앞으로도 필수적이라는 점을 다시 한번 느꼈다.

우리나라가 현재는 사이버보안 분야에서 선진국을 따라잡는 과정에 있지만, 이는 결코 극복할 수 없는 문제는 아니다. 정부는 근본적인 로드맵 수립과 프로세스 개선에 힘쓰고, 업계는 기술 연구에 집중하며, 이러한 성과를 서로 공유하고 개선해 나가는 노력이 지속된다면, 우리나라의 기술 수준은 한층 더 발전할 수 있을 것이다. 이는 궁극적으로 자동차 산업 전반에 활력을 불어넣고, 자동차 품질 향상에도 기여할 것이라고 확신한다.

끝으로, 오늘 좌담회에 참여해 주신 모든 패널 여러분께 감사의 말씀을 드리며, 이번 자리를 마련해 주신 한국자동차연구원과 모빌리티 인사이트 관계자분들께도 진심으로 감사의 말을 전한다.

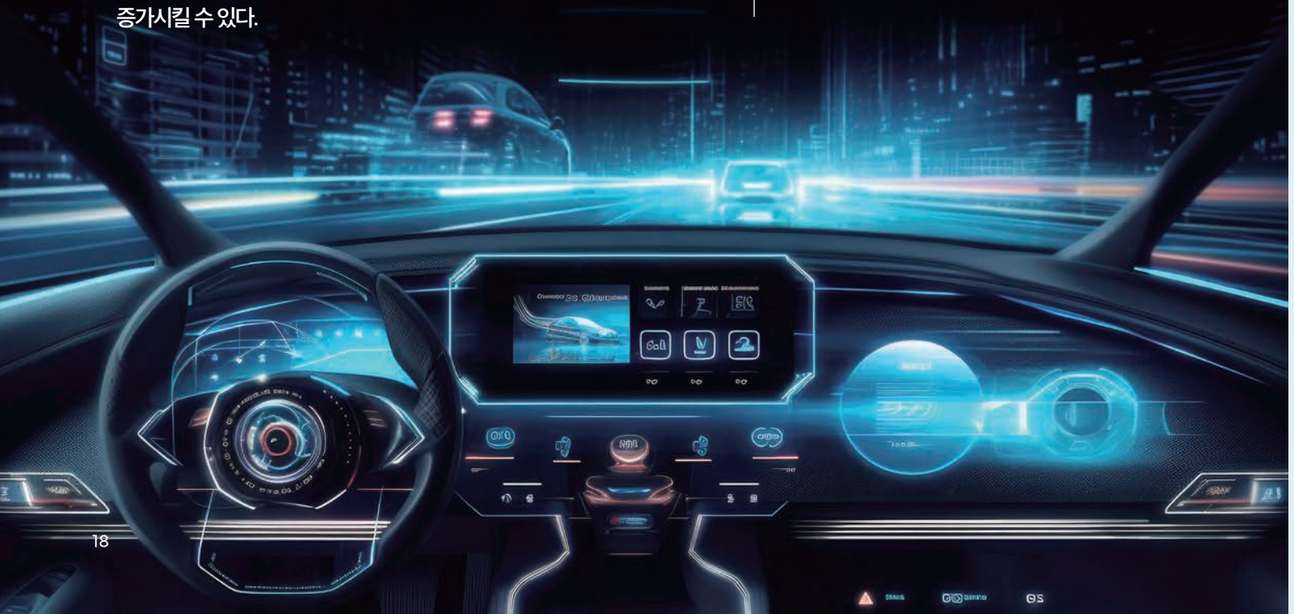
커넥티드카 사이버보안 현황과 미래 평가검증의 중요성

커넥티드카와 사이버보안의 중요성

커넥티드카는 차량과 외부 네트워크가 실시간으로 연결되어 데이터 전송 및 다양한 서비스가 가능해진 차량을 의미한다. 차량이 외부 네트워크에 연결됨으로써 차량의 운행 상태에 대한 원격 모니터링 및 진단을 포함하여 인프라와의 소통을 통한 협력 주행 기능 등이 가능하며 차량용 인포테인먼트 시스템의 운영체제와 서비스 소프트웨어를 비롯한 전자제어장치의 펌웨어까지도 원격 업데이트가 이루어지는 시대가 되었다.

일찍이 2015년 지프 체로키에 대한 해킹 시연으로 커넥티드카에 대한 사이버보안 위협이 얼마나 치명적일 수 있는지를 확인한 바 있다. 차량에 대한 외부 연결성 확장은 차량 관리와 기능개선의 유연성을 포함하여 운전자의 편의성과 안전성을 증대시키는 등 다양한 장점을 제공하지만 차량 내부의 많은 구성요소가 외부로부터의 다양한 악의적 시도에 노출될 수 있는 위험도 증가시킬 수 있다.

임강빈
순천향대학교
정보보호학과 교수
yim@sch.ac.kr



이러한 우려에 대응하기 위한 시장의 움직임은 이미 수년 전부터 시작되어 최근에는 유엔유럽경제위원회(UNECE)의 WP.29를 통한 UNR No.155 사이버보안 관리체계(CSMS: Cyber Security Management System), No.156 소프트웨어업데이트 관리체계(SUMS: Software Update Management System) 등의 규제가 2021년 1월에 발효되었다. 이에 따라 2024년 7월부로 사이버보안 관리체계 인증을 받은 조직으로부터 생산되어 사이버보안에 관한 차량형식승인(VTA: Vehicle Type Approval)을 확보한 차량만이 유럽 시장에 수출이 가능한 상황에 이르고 있다. 또한 2021년 8월에 차량용 사이버보안 국제표준 ISO21434가 완성됨으로써 차량의 사이버보안 관련 형식승인을 획득하기 위한 구체적인 위협분석 및 위험평가 (TARA) 방법의 모범적 지침이 마련되었다.

이런 상황에서 최근 몇 년은 우리 차량 제조사들도 글로벌 시장 진출에 대한 새로운 장벽으로서의 CSMS 및 VTA라는 강제적 규정의 발효에 대응하기 위하여 내외부적으로 매우 분주했던 것으로 알고 있다. 물론 현대자동차를 비롯하여 KG모빌리티 등 주요 완성차사들이 재빠르게 준비하여 인증을 획득하고 있으나 그렇지 못한 기업들도 많은 것으로 보인다. 특히 이러한 규제의 대상에는 완성차사뿐만 아니라 부품 제조사까지도 암묵적으로 포함되고 있으므로 해당 규제가 우리의 글로벌 자동차 시장에 미치는 영향이 미미하지는 않을 것으로 예상된다. 규제로서의 사이버보안 관리체계는 시스템 최초 인증에 필요한 투자부담이 크다. 그러나 일단 인증을 획득하고 나면 인증의 유지에 큰 문제는 없을 수 있다. 다만 사이버보안에 관한 VTA는 새로운 차량 모델에 대하여 반복적으로 수행되어야 하고 시험평가 검증에 대한 환경변화 우려도 크기 때문에 기업으로서 꽤 큰 부담이 될 수 있다. 그동안 자동차 산업은 기술적 폐쇄성이 가장 큰 분야의 하나였으나 앞으로의 사이버보안 위협 대응을 위한 부담을 줄이기 위해서는 조금 더 개방적으로 다양한 사이버보안 관련 주체와 협업할 시기가 되었다고 판단된다.

커넥티드카 사이버보안 위협 요소

전형적인 자동차 시스템은 대부분의 요소 기능이 자동차 내부 네트워크를 중심으로 연결된 다수의 분산 전자제어장치에 의하여 협업적으로 수행되도록 설계된다. 그럼에도 불구하고 자동차 내부 네트워크에서 패킷을 송수신하는 제어장치들은 송수신 당사자 간에 서로의 신원을 검증하는 기능을 가지고 있지 않다. 이는 임의의 패킷이 자동차 내부 네트워크에 주입되는 경우 이를 수신하는 제어장치는 패킷의 송신자에 대한 검증 없이 해당 패킷에 부여된 기능을 수행함을 의미한다. 그러므로 자동차 내부 네트워크에 악의적 패킷을 고의로 주입하는 경우 매우 심각한 사고를 초래할 수 있다. 따라서 자동차 시스템 내의 모든 구성요소를 대상으로 내부 네트워크에 악의적 패킷 주입이 가능한 경로를 탐색하고 이를 봉쇄하는 것이 매우 중요하다. 자동차 내부 네트워크로의 패킷 주입을 공식적으로 허가하고 있는 대표적인 경로는 자동차 진단 포트이다. 진단 포트는 미리 정의되어 있는 메시지를 수신함으로써 자동차의 주행 및 상태와 관련한 다양한 정보를 출력하기도 하지만 자동차의 특정 요소기능과 관련된 메시지 주입에 이용될 수도 있으며 네트워크에 참여하는 제어기의 펌웨어 업데이트에 이용되기도 한다.

제어기 펌웨어 업데이트는 매우 민감한 부분이다. 펌웨어 업데이트를 위하여 과거 WP2000 프로토콜을 비롯하여 현재의 UDS 프로토콜 등이 간단한 보안 프로토콜을 기반으로 운영되는데 2015년 순천향대학교 연구실에서는 자동차 진단 포트에 연결되는 진단기 하드웨어와 펌웨어 업데이트 소프트웨어 도구를 분석함으로써 제어기 펌웨어 업데이트를 위한 보안 프로토콜이 쉽게 무력화될 수 있음을 검증한 바 있다[1].

차량용 인포테인먼트 시스템은 기존 자동차 구성에서 가장 성능이 뛰어나고 가장 많은 외부 접점을 가진 제어기로서 범용컴퓨터 수준의 운영체제를 탑재하고 있고 이를 기반으로 자동차 내부 및 외부 양쪽 네트워크와 동시에 연동되므로 자동차에서 매우 치명적인 사이버보안

위협 요소가 될 수 있다. 인포테인먼트 시스템이 모바일 네트워크, 협력 주행 통신채널(V2X: Vehicle to Everything) 등 외부 네트워크로부터의 사이버보안 위협이나 블루투스, USB, SD-CARD 등 외부 접점으로부터의 취약점에 노출되어 악의적 사용자에게 제어권을 빼앗기는 경우 차량 내부 네트워크로 임의의 패킷 주입이 가능하게 되므로 차문개폐, 엔진제어 등 자동차 내부의 다양한 기능 조작이 원격으로 이루어질 수 있다.

인포테인먼트 시스템의 외부 접점을 통한 제어권 탈취는 인포테인먼트 시스템의 운영체제를 포함하여 외부 접점의 하드웨어, 소프트웨어 및 프로토콜 등을 로컬에서 분석하여 관련 취약점을 찾아내고 이를 활용하는 로컬 환경을 구현함으로써 이루어진다. 순천향대학교에서는 SD-CARD 내 펌웨어 배치구조, 설치 시의 펌웨어 인증구조를 파악하여 SD-CARD를 통한 펌웨어 업데이트 인증 과정을 우회함으로써 변조된 펌웨어가 쉽게 설치될 수 있음을 확인하였다.[2] [3] 그러나 취약점을 찾아낸다고 하더라도 이를 활용하는 로컬 환경을 구현하는 일은 자동차에 물리적인 근접 접근해야 하므로 일반적으로 치명적인 사고로 이어질 가능성은 낮은 편이다. 그러나 인포테인먼트 시스템의 소프트웨어 설치 인증구조, USB 파일 등 자원관리 구조, 암호화 구조 등을 파악함으로써 이러한 정보를 향후 외부 네트워크 채널을 통한 사이버보안 위협과 연동함으로써 심각한 공격을 유도할 수 있다.

인포테인먼트 시스템의 무선 네트워크 연동은 자동차의 사이버보안 관점에서 핵심 주제이다. 이미 인포테인먼트 시스템 운영체제의 커널, 시스템 앱, 사용자 앱 등이 무선채널(OTA: Over The Air)을 통하여 원격으로 업데이트되고 있으므로 이를 위한 보안 메커니즘에 허점이 발생할 때 자동차가 심각한 사이버보안 위협에 노출될 수 있다. 무선채널을 통하여 펌웨어를 안전하게 업데이트하기 위해서는 펌웨어에 대하여 배포 측에서 서명하고 설치 측에서 이를 검증함으로써 펌웨어에 대한 무결성을 확보하는 것이 필수이다. 이를 위하여 대개의 인포테인먼트 시스템이 관련 메커니즘을 도입하고 있으나 구현상의 실수 등으로 인하여 원격 업데이트 과정에서 악의적으로 변조된 펌웨어가 설치될 수 있는 취약점이 발견된다.

대개의 인포테인먼트 시스템은 무선채널을 통한 원격 펌웨어 업데이트를 위하여 오픈 모바일 동맹의 디바이스관리 프레임워크(OMA-DM)를 기반으로 구성된 솔루션을 도입하고 있다. 펌웨어 무결성 보장을 위한 서명 및 검증 기술에서 펌웨어 배포 측은 펌웨어에 서명 즉 암호화하기 위한 개인키를 생성하여 비밀리에 관리하며 펌웨어 설치 측에서 펌웨어에 대한 서명값을 복호화하여 무결성을 검증할 수 있도록 자신의 개인키로부터 공개키를 생성하여 설치 측에 공유한다. 이때 공개키 및 펌웨어에 대한 서명값 등이 포함된 인증서가 펌웨어와 함께 배포 측으로부터 설치 측에 전달된다.

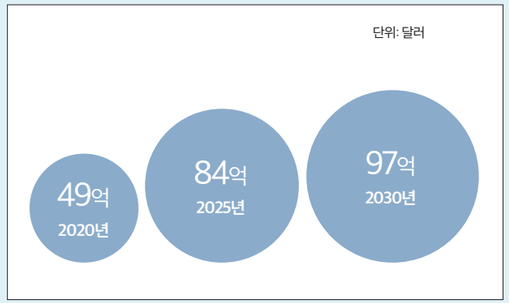
인증서를 통한 공개키 및 서명값 전달 과정에서 공개키와 서명값과의 관계, 즉 공개키와 개인키 쌍방의 유일한 관계가 깨지지 않도록 하는 것은 배포 측의 중요한 책임이다. 배포 측의 개인키가 유출될 경우 펌웨어를 변조하여 이를 해당 개인키로 서명하여 배포함으로써 설치 측에서 변조된 펌웨어가 설치될 수 있다. 이를 방지하기 위하여 언제라도 개인키와 해당 서명값을 갱신할 필요가 있으며, 따라서 인증서의 공유는 일반적으로 펌웨어 배포 시마다 매번 이루어지도록 설계하고 있다. 그러나 임의의 공격자도 자신이 스스로 개인키와 공개키 쌍을 생성하여 변조된 펌웨어에 서명할 수 있다. 만약 공격자가 자신의 공개키와 서명값을 포함하는 인증서와 함께 변조된 펌웨어를 설치 측에 배포할 수 있다면 해당 펌웨어는 설치될 수 있다.

순천향대학교에서는 특정 자동차 모델을 대상으로 무선채널을 통한 펌웨어 업데이트 과정을 분석한 결과, 설치 측의 서명검증 소프트웨어가 배포 측으로부터 내려받은 인증서에 대한 출처(URL)를 검증하지 않고 서명검증 절차를 수행하는 취약점이 있음을 발견하였으며 이에 따라 변조된 펌웨어와 임의의 키 쌍방을 기반으로 생성된 인증서를 임의의 서버에 게시한 후 이를 내려받도록 하여 변조된 소프트웨어를 설치할 수 있다는 점을 확인하였다.[2][3] 이는 자동차의 임의 제어뿐만 아니라 차량 내 도청 등의 사회적 문제도 유발할 수 있다. 공격자는 얼마든지 가짜 모바일 기지국을 구축하여 연결을 유도할 수 있고 또 공개 와이파이를 준비하는 것도 수월하므로 이러한 무선 네트워크에 연동되는 서비스는 보안기술의 안전한 구현에 더욱 신경을 써야 한다.

차량 무선 네트워크 연동에서의 악의적 공격은 자동차 원격 관리 및 제어를 위한 앱을 통해서도 이루어질 수 있다. 모바일 앱의 분석은 시스템 분석에 비하여 수월하여 취약점의 발견도 그만큼 쉬울 수 있으므로 앱의 설계와 구현에 보안 관점에서 최대한 신중히 처리해야 한다. 대개의 자동차용 모바일 앱이 사용자 인증이나 메시지 암호화 등의 보안 기능을 갖추고 있으나 이러한 보안 기능이 무력화될 수 있으며[2][3] 이럴 때 앱에 구현된 모든 원격제어 기능이 공격자에게 제공되므로 차량 사고, 도난 등의 사건으로 이어질 수 있다.

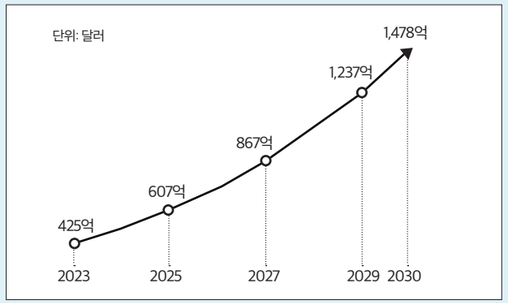
차량과 V2X 통신채널과의 연동은 차량 간 통신(V2V)과 차량과 인프라와의 통신(V2I)이라는 관점에서 모바일 네트워크를 통한 연동에 비하여 차량 내부와 외부 간의 접근 표면이 훨씬 넓다. 그러므로 잠재적 보안 위협도 더 다양할 수 있다. [4]에 의하면 시범사업을 통하여 구축되었던 V2X 환경에서 WAVE 메시지에 대한 해석과 임의 주입이 가능함으로써 자동차가 다른 차량이나 교통인프라와 통신하는 과정에서 중요한 정보를 가로채거나 변조할 가능성이 있었다. 이는 불특정 다수의 악의적 공격자에게 자동차의 내부 네트워크가 노출되는 결과를 초래할 수 있다.

[자동차 사이버 보안 관련 시장 전망]



출처 : 맥킨지

[소프트웨어 정의 차량(SDV) 글로벌 시장 전망]



출처 : 프레시던스 리서치

상기와 같은 사례는 사이버보안 위협에 안전하기 위해서 보안 요소기술의 도입도 중요하지만, 개발 및 실행에 대한 관리가 얼마나 중요한지를 보여주고 있다. 특히, 제어기에 대한 펌웨어까지 무선채널을 통한 업데이트를 추진하고 있고 소프트웨어 정의 차량(SDV: Software Defined Vehicle)을 통하여 자동차가 소프트웨어 플랫폼이 되어가는 현시점에서는 "외부 네트워크-네트워크 모뎀-인포테인먼트 시스템-게이트웨이-도메인(또는 Zone) 제어기-말단 제어기-센서 및 액추에이터"라는 계층구조를 포함하여 새로이 등장하는 구조 전반에서의 펌웨어, 소프트웨어 및 이들의 업데이트 수행에 대한 시험평가 및 검증의 중요성이 더욱 커지고 있다. 특히나, 개별 자동차로부터 수집되는 모든 이종 데이터를 클라우드에 집화하여 도시 수준의 글로벌 데이터 클라우드를 구축하고 이를 기반으로 차종 및 차량의 물리적 구성과 독립적인 총체적 상황인지 기반의 서비스를 구축하기 시작하는 시점에서 사이버보안 위협에 대한 대책이 없으면 향후 큰 낭패를 볼 여지가 크다.

커넥티드카 사이버보안 위협분석 및 평가

서두에서 언급한 바와 같이 자동차 산업에서 기업이 사이버보안 관리체계(CSMS) 및 차량 형식승인(VTA) 관련 규제에 대한 대응 역량을 확보하는 것은 필수가 되었다. 이는 규제에 대한 인증을 획득하는 것뿐만 아니라 더 나아가 자동차를 위한 기술적 환경변화에 따라 증가하고 있는 사이버보안 위협에 대한 내성을 확보하기 위하여 관련 기업들이 지속해서 노력해야 한다는 것을 의미한다.

UNECE WP.29의 사이버보안 관리체계(CSMS) 인증은 다음의 네 가지를 요구하는 것으로 이해될 수 있다. 첫째, 자동차의 전체 수명주기에 걸쳐서 사이버보안 관리체계가 잘 적용되고 있음을 입증하라. 둘째, 사이버보안 관리체계가 포함하고 있는 모든 절차가 전반적인 보안 사항을 충분히 고려하여 개발되었음을 입증하라, 셋째, 보고된 사이버보안 위협이나 취약점에 대하여 합리적인 시간 내에 완화할 수 있는 체계를 갖추었음을 입증하라. 넷째, 사이버보안 관리체계를 통하여 지속적인 보안 모니터링을 수행함으로써 취약점 탐지뿐만 아니라 잠재적 위협에 대한 대응 신속성을 확보하라.

차량 형식승인(TVA)은 차량이 도로 주행에 필요한 법적 요구조건을 충족하는지에 대한 인증 절차로서 UNR 사이버보안 규제에 따라 사이버보안 관련 요구사항이 추가되었다. 추가된 핵심 내용은 크게 두 가지로 볼 수 있는데 첫째, 출시할 차량이 사이버보안 관리체계에 근거하여 개발되고 적절한 보안 조치가 반영되었는가, 둘째, 차량 구성요소에 대하여 사이버보안 보증 수준이 적절한 방법으로 도출되고 수준별 사이버보안 유효성 검증 방법에 따라 사이버보안 보증 수준이 테스트 되었느냐는 것이다. 첫째 내용은 CSMS 준용을 의미하며, 둘째 내용은 ISO21434 준용을 의미한다. 여기서 ISO21434의 준용은 의무적인 것은 아니지만 규제 당국과 제조업체 간에 최소 기준으로 여겨지고 있다.

사이버보안 보증 수준 즉, Cybersecurity Assurance Level(CAL)은 낮은 수준에서 높은 수준으로 CAL1~4까지의 4단계로 정의되며 차량의 각 구성요소는 위협분석 및 위험평가(TARA: Threat Analysis and Risk Assessment) 절차를 통하여 CAL 수준별로 분류된다. 유효성 검증을 위한 테스트에는 코드 리뷰, 기능 테스트, 취약점 스캐닝, 퍼징 테스트, 침투 테스트 등이 포함되며 각 CAL 수준에 따라 다른 조합으로 수행된다.

[현대자동차 커넥티드 카 핵심 운영 체제 ccOS - connected car Operating System]

국제 공인시험인증기관인 TUV라인란드(TUV Rheinland)로 부터 차량 사이버보안 관리체계(CSMS, Cyber Security Management System) 인증 받은 **LG전자 차량 인포테인먼트 시스템**

출처 : LG전자

출처 : 현대자동차

UNECE WP.29의 규정은 국내·외 자동차 기업들이 사이버보안을 바라보는 시각을 짧은 시간에 매우 크게 바꾸어 놓았다. 국내 자동차 제조업체들도 최근 5년간 사이버보안 관련한 관리체계 및 형식승인 인증을 획득하기 위해 조직까지 재편하며 국내외로 분주하게 움직였다. 그 결과로 현대자동차는 2021년 12월에 국내 최초로 사이버보안 관리체계 인증을 획득하였고 KG모빌리티가 2022년 12월에 마찬가지로 인증을 획득하였다. 또한 자동차 부품사인 LG전자도 2023년 2월에 차량용 인포테인먼트 시스템 등을 대상으로 인증을 획득하였다. 이외에도 여러 자동차 부품 기업들이 필수적으로 규제에 따른 인증을 준비하거나 이미 획득하고 있다.

자동차 사이버보안과 관련한 또 다른 주제는 '개인정보보호'다. 유럽연합(EU)에서 2018년 5월 25일부터 시행된 일반데이터보호규정(GDPR: General Data Protection Regulation)은 유럽연합 시민의 데이터를 처리하는 모든 국가의 기업과 조직에 적용된다. 일반데이터보호규정은 개인 데이터 수집, 저장, 처리하는 방식에 대해 엄격한 기준을 세우고 있으며 이름, 이메일 주소, 위치 데이터, IP 주소, 의료 정보 등 다양한 개인정보에 대한 접근, 수정, 삭제, 처리, 보관, 이동을 포함하여 동의, 책임, 처벌 등에 관한 규제를 포함하고 있다. 자동차와 관련하여 규제 대상의 개인정보는 인포테인먼트 시스템과 연동되는 통상적인 개인정보를 포함하여 차량이 생성하는 위치, 운전 습관, 차량 사용 패턴 등을 포함하여 자율주행 자동차가 수집하는 도로 촬영 영상 등으로 확장될 수 있다.

커넥티드카 사이버보안 위협에 대한 향후 대응

최근 국내 주요 자동차 제조사들이 사이버보안에 대한 대응투자를 늘리고 있지만 특정 기업을 제외하고는 글로벌 규제 준수와 인증을 위한 범위에 한정된 것이 사실이다. 그동안 사이버보안 위협에 대한 시연과 논쟁이 10여 년 지속되고 있었고 글로벌 규제에 대한 움직임도 이미 발견되고 있었음에도 그에 대한 적절하고 적시적인 대응이 없었기에 우리 기업에 규제 발효에 따른 여파는 더욱 크게 느껴진다. 상기한 바와 같이 주요 기업들이 규제 대응을 위해 짧은 기간에 집중투자를 하고 있지만 국가적 측면에서 볼 때 현재 우리 자동차 산업이 이러한 규제의 여파를 아무런 피해 없이 통과하기는 쉽지 않아 보인다.

사이버보안 관련 글로벌 규제에 흔들리지 않는 순조로운 합류를 위한 답은 우리 기업들의 상시적인 사이버보안 내재화에 있다. 특히 그동안의 자동차 산업은 하드웨어 중심이었기 때문에 시험평가 및 인증이라 하면 하드웨어 중심의 신뢰성 평가 및 인증을 말한다. 소프트웨어를 포함하여 사이버보안에 대한 인식이나 사고 체질이 아직 준비되지 않은 상황에서 이를 위한 체계적인 시험평가 및 검증 기술을 이야기하는 것이 매우 낯설다. 그러므로 관련 기술을 선제적으로 확보하고 대응하는 것은 쉽지 않다. 기존 IT 영역에서의 사이버보안 문제에서 경험했던 바와 마찬가지로 사이버보안은 부수적이고 선택적인 사항이라 여겨지는 것이 선제 대응을 더욱 어렵게 만든다. 국가가 이를 위한 지원에 나서야 하는 이유이다.

자동차 제조사들도 사이버보안 내재화를 위하여 자사 연구소뿐만 아니라 관련 전문 보안업체를 포함하여 국가 연구소 및 대학 연구실 등과의 협업을 통한 보안 위협 발굴 및 대응 기술 개발에 관심을 가져야 한다. 사이버보안 관련 국가 연구소 또는 대학 연구실은 오랫동안 사이버보안 위협 발굴 및 대응 기술 연구에서 중요한 역할을 담당해 왔다. 특히, 다양한 사이버보안 위협에 대한 공격 시나리오 설계와 분석, 이를 해결하기 위한 대응 기술의 검증 등과 관련하여 이론적 연구뿐만 아니라 현장 중심의 실질적인 사이버보안 적용 기술 관련하여 다양한 연구가 진행되고 있으므로 이러한 자원을 충분히 활용할 필요가 있다. 다만, 자동차 분야에서는 기술 수요자로서의 자동차 제조사들만이 오랜 기간에 걸쳐 확보한 지식과 경험이 있고 이는 사이버보안 연구자들도 마찬가지여서 따로는 서로 겹치지 않는 영역이 있으므로 서로 만나서 상호 자원을 공유하는 것이 필요하다.

자동차가 전기차로 전환되면서 점진적으로 충분한 전력이 확보됨으로써 우리는 최근 자율주행을 포함하는 다양한 정보통신기술이 자동차에 집중되는 현상을 보고 있다. 기존 정보통신 분야에서 도입되었던 기술들이 자동차 분야로 점차 이동하고 있고 이러한 기술의 수용을 원활하게 하도록 자동차의 기반 아키텍처가 크게 진화하고 있다. 과거, 기능 안전성과 유지 효율성 등의 목적으로 채택하였던 메시지 기반의 다중 분산 제어기와 분산 소프트웨어 구조를 점차 탈피하고 있다. 현재 상황으로 볼 때는 이러한 아키텍처 변화의 목적지는 SDV가 될 것으로 보인다. 기존 정보통신 분야에서 핫이슈였던 소프트웨어 정의 네트워크(SDN: Software Defined Network)의 경우와는 탄생 과정이 전혀 다르지만, 추진 동력은 같다고 할 수 있다.

조만간 자동차가 기술적으로는 대표적인 복합적 컴퓨팅 플랫폼으로서, 또한 환경 측면으로는 가장 오래 머무는 서비스 공간으로서 자리매김할 것이다. 이는 악의적 공격자 입장에서는 자동차가 갖가지 공격 도구를 갖추고 물리적으로 독립되어 은밀하게 도시 인프라를 공격할 수 있는 자신만의 요새를 가지게 되는 것을 의미한다. 이러한 이유로 자동차 사이버보안 위협은 프로그램 가능한 공격용 통합플랫폼으로서 앞으로 더욱 심각한 사회적 토론의 주제가 될 것이다. 이는 우리가 모두 자동차 사이버보안 위협과 그 대응 방안에 집중해야 하는 중요한 이유 중의 하나이다.

새로운 기술 도입의 입장에서도 머신러닝이라는 키워드는 보안 솔루션을 위한 도구 개발이라는 차원에서도 중요하지만, 취약점 발굴의 자동화나 이에 대한 지능적 공격이라는 관점에서도 인기가 지속될 것이다. 또한, 양자암호화라는 키워드에서도 이는 현재의 암호화 기술보다 훨씬 더 높은 보안성을 제공할 수 있지만 이 또한 새로운 창과 방패의 싸움이 될 가능성이 크다. 따라서 우리는 이러한 싸움에 노출될 체력 단련을 함과 동시에 새로운 기술의 도입에서도 포괄적으로 접근하기 위해 노력해야 한다. 단일 요소기술을 독립적으로 고민하는 것이 아니라 예로서 블록체인을 활용한 분산 인증 기술로 코드, 데이터뿐만 아니라 시스템이나 네트워크 구성에 대한 무결성을 검증하기 위한 기술, 차량 및 기반 시설로부터의 이종 데이터를 기반으로 제로 트러스트 패러다임으로부터 얻을 수 있는 비정상 행위 상시 모니터링 기술 등을 활용한 복합적 접근이 요구된다.

결론적으로, 자동차를 중심으로 하는 양방향 사이버보안 위협은 기술의 발전과 함께 계속해서 진화할 것이며 이와 같은 위협을 예방하거나 사후에라도 신속하게 대응하기 위해서는 기술적으로나 정책적으로나 다면적인 방안으로 무장해야 한다. 마찬가지로 한국 자동차 산업의 글로벌 경쟁력을 지속해서 유지하고 더욱 강화하기 위해서는 글로벌 규제를 넘어서서 사이버보안 위협 발굴 및 대응 기술에 대한 보다 선제적이고 다각적인 접근이 필요하며 이를 위해서는 더욱 다채로운 사회 구성원이 이에 참여하고 이바지할 수 있는 사회적 분위기와 실체적 기회를 만들어 가는 것이 '산-학-연-관-민' 모두의 역할이자 의무이다. 앞으로의 모빌리티 산업이 더욱 안정적으로 발전하기 위해서, 그리고 미래 모빌리티 환경에서 우리들이 더욱 안전하게 살아가기 위해서 사이버보안 문제에 대하여 우리는 사회 구성원 모두가 협심하여 지속해서 협업해야 할 것이다.

참고

[1] 분산 임베디드소프트웨어의 오류전파 특성분석을 통한 시스템 단위 검증체계 연구 (순천향대학교 시스템보안연구실, 2013)

[2] 스마트카 보안 취약점 연구 (순천향대학교 시스템보안연구실, 2015)

[3] 커넥티드카 침해사고 시나리오 모델 구현 및 분석방법 연구 (순천향대학교 시스템보안연구실, 한국인터넷진흥원, 2018)

[4] 커넥티드 카 외부 접점 보안위협 분석 모델 구현 및 분석방법 연구 (순천향대학교 시스템보안연구실, 한국인터넷진흥원, 2019)

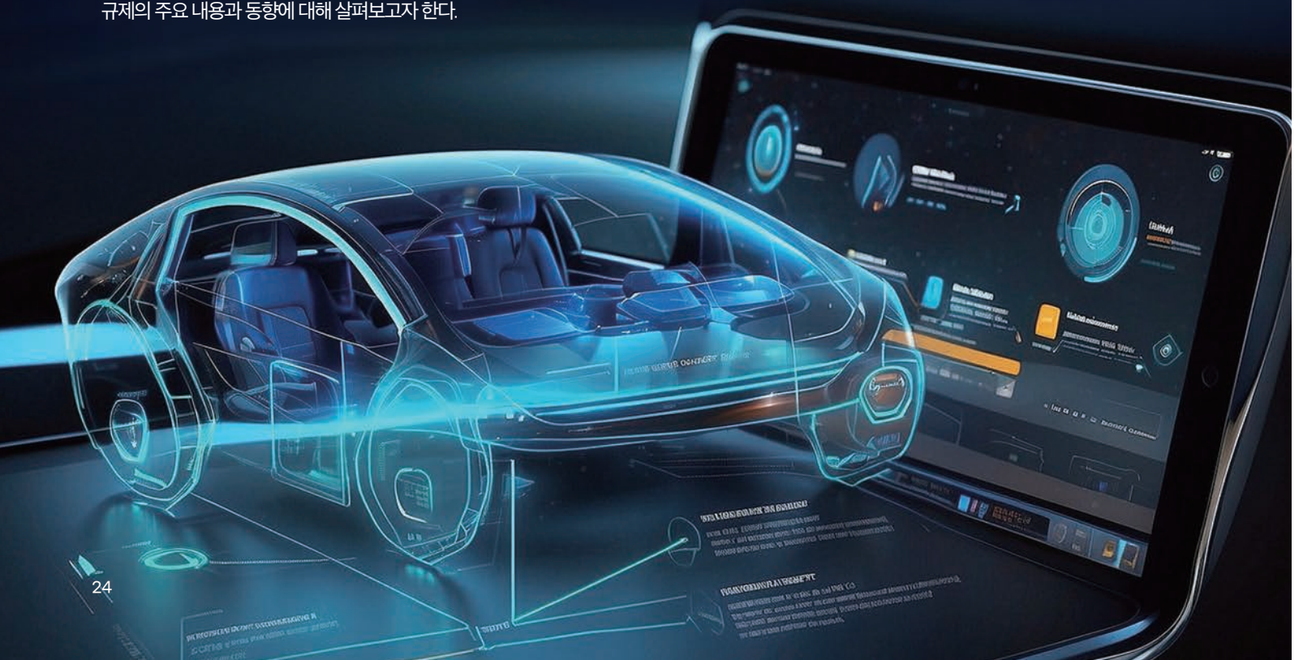
커넥티드카 **사이버보안 문제**에 대한 **국내·외 규제 동향**

커넥티드카의 시대가 도래하면서 국내·외에서 커넥티드카 사이버 보안 관련 규제도 도입 및 시행되고 있다. 일부 국가에서는 중대한 무역장벽으로도 작용할 수 있는 규제 입법화까지 논의되고 있는 상황이다.

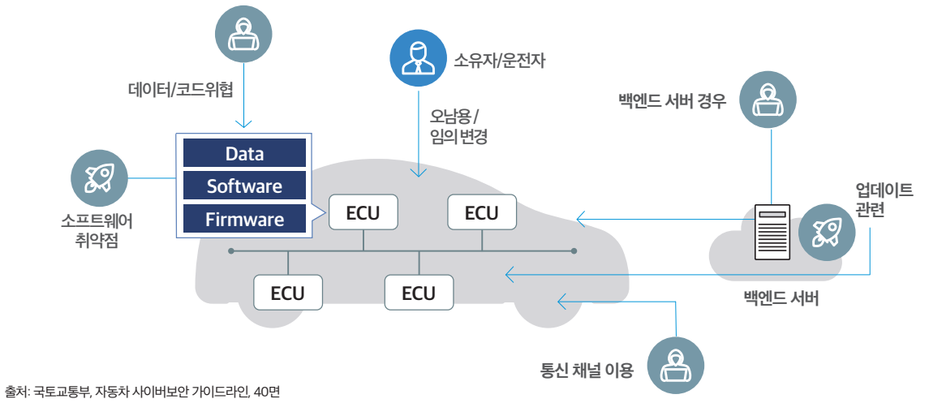
김태주
법무법인(유) 광장 파트너 변호사
taejoo.kim@leeko.com

정보통신기술이 고도로 발전하고 자동차에도 본격적으로 접목되면서 자동차가 무선통신을 통해 다른 사물과 정보를 송수신하는 커넥티드카(Connected Car)의 시대가 도래하였다. 이러한 커넥티드카의 등장은 차량 내에서 인포테인먼트 서비스를 이용할 수 있게 하는 등 자동차 이용 편의성을 크게 증대시키고 있지만, 다른 한편 통신을 통해 외부에서 자동차 내부 장치에 접근하는 것이 가능해짐으로써 자동차 탑승자 등의 안전을 위협하거나 프라이버시 침해 문제를 일으키는 해킹 등 커넥티드카를 향한 사이버공격 가능성에 대한 우려도 지속적으로 제기되고 있다.

이에 커넥티드카의 사이버보안 문제에 대한 규제 필요성이 본격적으로 대두되었고, 국내외에서 이미 규제가 도입되었거나 도입이 검토되고 있다. 이하에서는 이러한 규제의 주요 내용과 동향에 대해 살펴보고자 한다.



[사이버보안 위협의 예]



출처: 국토교통부, 자동차 사이버보안 가이드라인, 40면

국제연합 유럽경제위원회(UNECE)의 Regulation No.155, 156

UNECE 산하 국제 자동차기준 조화 회의체(WP. 29)는 2020년 6월 자동차 사이버 보안 문제에 대한 최초의 국제기준인 Regulation No. 155(UNECE R155)를 채택하였다. 이 국제기준의 주요 내용을 간략히 정리해보면 다음과 같다.

(1) 각 국가별로 자동차 사이버보안 관리를 위한 체계(Cyber Security Management System, 이하 'CSMS')의 승인을 위한 기관을 지정하도록 함

(2) CSMS 승인기관은 해당 국가의 자동차 제작사가 CSMS를 갖춘 경우 인증서를 발급하고, 차량에 대한 사이버보안 위험평가·관리가 CSMS에 따라 적절히 시행된 경우 차량에 대한 형식승인을 할 수 있도록 함

(3) CSMS 인증서 발급을 위한 요건으로 자동차 제작사는 자동차 사이버보안에 필요한 보안 위협을 식별·평가·분류·관리하기 위한 프로세스, 차량 보안성 시험을 위한 프로세스, 보안위협을 모니터링하고 탐지·대응하는 프로세스 등의 관리체계를 적절히 갖추었음을 입증해야 함

(4) 차량에 대한 형식승인 요건으로 자동차 제작사는 CSMS 인증서를 보유하고, 차량에 대한 사이버 공격의 탐지 및 예방 조치, 제작사의 모니터링 기능 지원 조치, 사이버 공격에 대한 분석을 위한 "데이터 포렌식" 지원 조치 등의 위험평가·관리·보안조치 및 충분한 검증시험 등을 수행해야 하며, 해당 차량의 부품, 애프터마켓 소프트웨어 등 제작사 외부의 공급업체·시스템에 대한 위험도 관리하여야 함

(5) 자동차 제작사는 보안 모니터링 결과를 승인기관에 보고해야 함

[자동차 해킹 관련 해외 주요 사례]

시기	내용
2022. 11.	• 인포테인먼트용 전원공급 장치의 취약점을 이용하여 혼다, 닛산, 인피니티등의 차량에 대해 원격으로 운전자 개인정보 탈취, 무단 차량 위치 파악, 도어락 잠금 해제 등을 시연
2022. 05.	• 테슬라의 저전력 블루투스(BLE) 통신의 취약점을 이용하여 차량을 훔치는 해킹 시연
2022. 03.	• 혼다의 10세대('16~'21) 원격키시스템의 취약점을 이용하여 리플레이공격등을 통해 무단으로 차량을 잠금, 잠금 해제, 원격 시동할 수 있음을 시연
2021. 08.	• 테슬라 오토파일럿의 차선 유지기능의 취약점을 이용하여 차량이 오인식하지만, 운전자는 인식하지 못하는 페이크 차선을 이용하여 공격 가능함을 시연
2021. 06.	• 차량의 ECU(전자 제어 장치)에 구현된 특정 기능을 악용하여 차량의 제동, 조향 관련 ECU의 기능을 정지시키는 공격을 시연
2021. 04.	• Wi-Fi 동글을 탑재한 드론을 사용해 차량의 인포테인먼트 시스템을 해킹하여 도어, 트렁크, 좌석변경 등을 조작할 수 있음을 시연

출처 : 제21대 국회 자동차관리법 일부 개정법률안(정당만 의원 대표발의 안) 검토보고서

현대자동차 커넥티드카에 탑재된 오비고 웹 솔루션 _ 출처 :오비고 홈페이지

삼성-하만 익스플로어_레디 Curved display(출처 : 하만 홈페이지)

(6) 본 기준을 채택한 회원국의 승인기관들은 형식승인 관련 정보 교류를 위한 DB에 승인기관이 자동차 제작사의 보안조치 적절성을 평가하기 위한 방법·기준, 이에 대한 타 승인기관의 검토의견 등의 정보를 공유하여야 함

이 UNECE Regulation No. 155(UNECE R155) 을 보면, 기본적으로 자동차의 사이버보안 문제에 대해 형식승인 제도를 채택하였다는 점을 알 수 있다. 이 기준은 2021년 1월부터 발효되었는데, EU 회원국들은 이 기준을 채택하여 2022년 7월 이후 출시된 신차와 2024년 7월 이후 운행되는 모든 차에 대해 이 기준을 적용하고 있다. 그리고 일본의 경우도 위 국제기준을 도로운송차량법(道路運送車両法)의 하위 법령인 도로운송차량의 보안기준 등에 반영하는 방식으로 관련 법령을 정비하였으며, 현재 운행되는 모든 차에 대하여 해당 기준이 적용되고 있다. 다만, OTA(Over The Air) 무선 소프트웨어 업데이트 기능이 없는 2022년 5월 이전 출시된 기존 차량은 2026년 5월 이후 해당 기준이 적용될 예정이다.

한편, WP. 29는 2020년 6월 자동차 소프트웨어 업데이트에 관한 국제기준인 UN Regulation No. 156(UNECE R156) 도 함께 채택하였는데, 이 국제기준은 자동차 소프트웨어 업데이트 관련 보안 요구사항과 규제당국의 소프트웨어 업데이트 관리시스템 관련 적정성 조사 권한 등을 정하고 있어 커넥티드카의 사이버보안 문제를 일부 규율하고 있는 것으로 볼 수 있다.

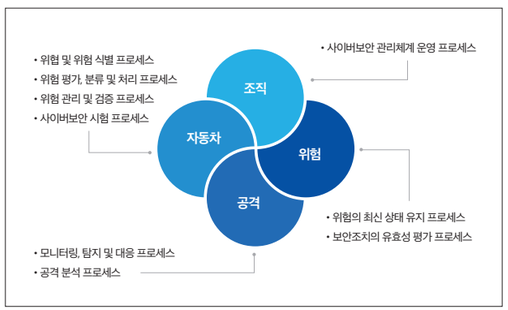
우리나라의 개정 자동차관리법

(2025년 8월 14일 시행 예정)

한-EU FTA에서는 우리나라로 하여금 UNECE Regulation 중 일부와 우리나라의 규제를 조화시킬 것을 의무화하고 있으나 커넥티드카 사이버보안 관련 규제는 이러한 기준 조화 의무의 대상에 포함되어 있지 않다. 즉, 우리나라가 UNECE Regulation No. 155 및 No. 156을 채택하여야 하는 FTA상의 의무를 부담하는 것은 아니나, 우리나라도 자동차 사이버보안과 관련한 기준 조화의 관점에서 UNECE Regulation No. 155 및 No. 156의 내용과 유사한 규제내용을 담아 자동차관리법을 개정하였으며, 해당 개정 자동차관리법은 2025년 8월 14일부터 시행될 예정이다. 법 시행 당시 이미 제작·조립 또는 수입되고 있는 자동차에 대해서는 충분한 준비기간을 확보할 수 있도록 2년의 추가 유예기간이 부여된다. 개정된 자동차관리법의 주요 내용은 다음과 같다.

(1) 자동차 제작사는 자동차 제작에 앞서 사이버보안 관리체계를 구축하여 국토교통부 인증을 획득하여야 함[사이버보안 관리체계는 자동차 생애주기에 걸쳐 사이버 위협요소를 상시 모니터링하고 위협 발생 시에는 이에 신속히 대응하기 위한 조직·수단·절차 일체를 포함함(사이버보안 관리체계의 세부 요건·기준 등은 국토교통부 고시를 통해 구체화될 예정)]

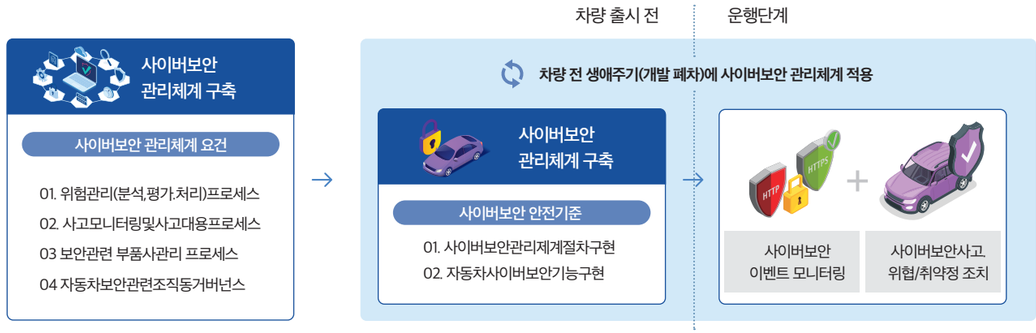
[사이버보안 관리체계의 프로세스]



출처 : 국토교통부 자동차 사이버보안 가이드라인 18 면

(2) 자동차 제작사의 사이버보안 관리체계가 적절하게 수립되었는지를 확인·인증하고, 인증 후에도 관리체계의 안전성·신뢰성을 확인하기 위해 관련 자료 제출을 요구할 수 있는 권한을 국토교통부에 부여함

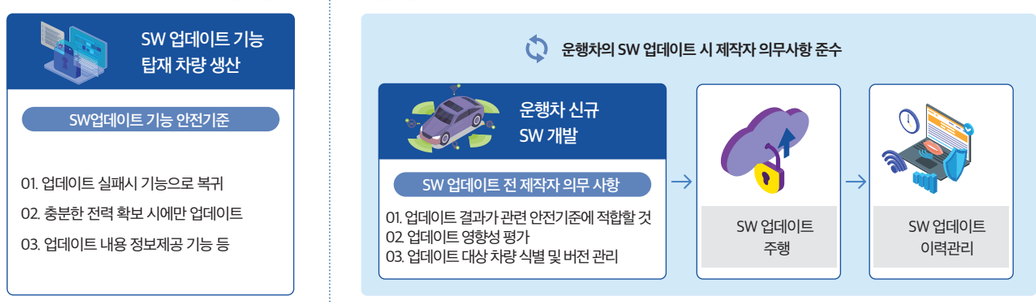
[자동차 사이버보안 제도 체계]



출처 : 국토교통부 보도참고자료 (2024. 1. 25.)

(3) 자동차 제작사는 소프트웨어 업데이트에 앞서 관련 장치·기능의 정상적인 작동 및 안전기준 적합성 여부를 확인하는 한편, 업데이트 시에는 관련 정보를 사용자에게 공지하고 보안 및 안전성을 확보하여야 함. 아울러, 국토교통부는 제작사의 소프트웨어 업데이트 준수사항 이행 여부를 성능시험대행자(한국교통안전공단)를 통해 조사하고, 부적정한 업데이트에 대해서는 시정조치를 명할 수 있음

[자동차 SW 업데이트 제도 체계]



출처 : 국토교통부 보도참고자료 (2024. 1. 25.)

시행령 규정을 통해 사이버보안 관련 장치나 부품이 형식인증의 대상이 될 가능성은 있다고 하겠다.

한편, 참고로 지난 2020년 국토교통부가 자동차 사이버보안 가이드라인을 마련한 바 있으나 이 가이드라인은 법적 구속력이 있는 것이 아니며, 개정 자동차관리법의 시행으로 비로소 자동차 사이버보안과 관련한 법적 구속력 있는 규제가 시행되게 된다. 그리고 관련 규제의 세부사항들은 (비록 EU의 경우와 유사한 내용으로 정해질 가능성이 높다고 예상되지만) 시행령, 시행규칙 및 국토교통부 고시 등 하위법령을 통해 구체화될 예정이므로, 관련 사업자들은 향후 하위법령 입법 상황을 지속적으로 모니터링 할 필요가 있을 것이다.

위 내용을 보면, 주요 내용이 UNECE Regulation No. 155 및 No. 156의 내용과 조화되어 있다는 점을 알 수 있으나, 한 가지 중대한 차이점은 자동차에 대한 형식승인 관련 내용이 명시되어 있지 않다는 점이다. 우리나라의 자동차관리법은 기본적으로 자동차와 관련하여 자기인증 제도를 채택하고 있고, 이러한 자기인증 체계가 사이버보안과 관련하여서도 유지된 결과로 볼 수 있을 것이다. 다만, 2025년 2월 17일부터 시행될 예정인 개정 자동차관리법 제30조의7은 이러한 자기인증 제도에도 불구하고 구동축전지 등 신기술 등이 적용되는 핵심 장치 또는 부품으로서 대통령령으로 정하는 핵심 장치 또는 부품의 경우에는 국토교통부장관으로부터 안전성인증을 받도록 규정하고 있으므로 향후

미국의 자동차 사이버 보안 규제

미국의 경우 현재까지는 UNECE Regulation No. 155 및 No. 156을 채택하거나 자동차 사이버보안과 관련된 법령을 별도로 제정하지 않고, 법적 구속력이 없는 NHTSA의 자동차 사이버보안 관련 가이드라인

(Cybersecurity Best Practices for the Safety of Modern Vehicles)만을 운영 중에 있다.

현재 미국은 자동차 안전이나 프라이버시 침해 가능성 등의 관점보다는 국가안보의 관점에서 커넥티드카 사이버보안 문제를 접근하고 있는 것으로 보인다. 즉, 바이든 미국 대통령은 2024년 2월 중국, 러시아 등 일부 국가가 미국 내 커넥티드카를 통한 데이터 수집 및 인프라 교란 등의 활동으로 국가안보에 위협을 초래할 수 있을 것으로 보고 상무부에 커넥티드카 산업 현황을 조사하고 관련 조치를 취하도록 하였고, 이에 따라 미 상무부 산업안보국은 2024년 3월 1일 커넥티드카에 필수적인 정보통신기술서비스를 설계, 개발, 제조, 공급하는 자 중 특정 외국정부가 소유, 통제하거나 그 외국정부의 관할, 지시 하에 있는 자와의 정보통신기술서비스 거래를 금지하는 규정의 도입을 위해 이해관계자의 의견을 구하는 사전 입법예고(Advance Notice of Proposed Rulemaking)를 발표하였다. 그리고 지난 9월 23일 미 상무부는 특히 중국과 러시아로부터 특정 기술이 포함된 커넥티드카의 수입 또는 판매나 특정 부품의 수입을 금지하는 입법예고를 발표하였다.

이번 입법예고안의 내용은 지난 3월에 사전 입법 예고되었던 규제안과 비교할 때 특히 중국 및 러시아와 관련한 규제에 집중하고 있다는 점이 그 특징이라고 볼 수 있다. 구체적으로 해당 규제안은 중국 또는 러시아의 소유, 통제 또는 관할권이나 지시를 받는 자가 설계, 개발, 제조 또는 공급하는 VCS 하드웨어(Vehicle Connectivity System Hardware) 또는 VCS 및 ADS 소프트웨어(이하 VCS 및 ADS 소프트웨어를 통칭하여 "Covered Software")와 관련하여, 일반 허가(General authorizations) 또는 특별 허가(Specific authorizations)를 받지 아니한 상태에서, (1)VCS 하드웨어 수입업자가 VCS 하드웨어를 고의로 미국으로 수입하는 것을 금지하고, (2) 커넥티드카 제조업체가 Covered Software를 통합한 완성된 커넥티드카를 고의로 미국으로 수입하는 것을 금지하며, (3) 커넥티드카 제조업체가 Covered Software가 통합된 커넥티드카를 고의로 미국 내에서 판매하는 것을 금지하고, (4) 중국 또는 러시아의 소유, 통제 또는 관할권 또는 지시를 받는 커넥티드카 제조업체가 VCS 하드웨어 또는 Covered Software가 통합된 커넥티드카를 고의로 미국에서 판매하는 것을 금지함을 주요 내용으로 하고 있다. 아울러 VCS 하드웨어 수입업체, 커넥티드카 제조업체로 하여금 VCS 하드웨어 또는 완성된 커넥티드카의 수입이나 판매를 위해 미 상무부 산업안보국에 적합성 선언(Declaration of Conformity)을 제출하도록 하는 것도 주요한 내용 중 하나이다.

이와 같이 미국 정부가 국가안보 관련 이유로 커넥티드카를 규제하는 것은 기존의 수출통제나 경제제재의 경우와 유사한 측면이 있으나, 기존의 수출통제와 경제제재가 미국의 부품이나 기술이 외부의 적대국가 등에서 사용되는 것을 막기 위한 조치라면 이번 커넥티드카 관련 규제는 외부의 적대국가로부터 미국의 커넥티드카 관련 개발이나 운영 등을 보호하려는 목적을 지닌다는 점에서 그 성격이 다소 다른 측면도 있다. 따라서 기존에 미국 정부가 운용해온 수출통제와 경제제재 관련 체제 내지 방식이 그대로 적용될지 여부는 추가로 지켜볼 필요가 있다고 생각된다. 아울러 위 입법예고에 따르면, (지난 3월의 사전 입법 예고되었던 내용보다는 보다 명확해진 측면이 있으나) 커넥티드카나 VCS 하드웨어, Covered Software 등과 관련된 규정의 적용범위가 넓게 해석될 여지가 있어 위 규제의 적용범위를 구체적으로 예상하기도 어려운 상황이다.

즉, 전체적으로 미국의 커넥티드카 관련 사이버보안 규제의 구체적인 적용범위나 방식 등을 현재 시점에서 구체적으로 예상하기가 쉽지는 않은 상황이다. 나아가 만약 규제의 적용범위가 넓게 설정된다면 각 자동차 제작사들은 관련 부품 및 기술 개발이나 공급망 변경 등을 위해 막대한 비용을 추가적으로 부담하게 될 가능성이 높고, 이는 결과적으로 중대한 무역장벽으로도 작용할 가능성이 높아, 위 규제와 관련한 우려가 적지 않은 상황이다. 미국의 관련 규제에 대한 입법화가 신속하게 진행되고 상황이므로 해당 입법 상황에 대해 예의주시할 필요가 있을 것이다. 참고로 위 규제안은 의견수렴절차를 거쳐 최종적인 규제 내용이 연방 관보에 게시되고 60일 후에 발효될 예정이다.

향후 국내외 규제 변화 예상 및 대응 방향

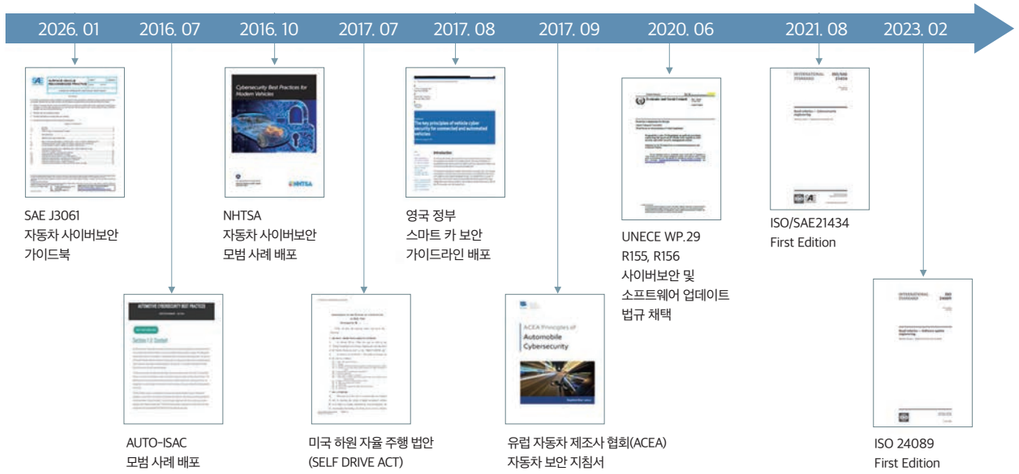
커넥티드카 사이버보안에 관한 규제는 주로 차량 및 운전자 등의 안전과 프라이버시 보호의 관점에서 검토 및 도입되고 있으며, 커넥티드카 사이버보안 규제 필요성이 논의된 배경 내지 이유를 고려하면 향후에도 기본적으로 이와 같은 관점에서 규제가 개선 내지 발전될 것으로 예상된다. 그리고 국경의 제약이 적은 정보통신의 특성상 향후에도 각국의 규제가 조화되는 방향으로 전개될 가능성이 높다고 예상된다. 다만, 위에서 살펴본 미국의 경우와 같이 국가안보의 관점에서도 커넥티드카 사이버보안 규제를 시행하는 국가가 등장할 경우 다른 국가들도 같은 취지의 규제를 추가로 도입할 가능성이 있으며, 이는 커넥티드카와 관련하여 중대한 무역장벽으로 작용할 가능성이 높다. 우리나라는 주요 자동차 수출국 중 하나로서 이러한 규제의 영향을 크게 받을 수밖에 없으므로 이러한 규제 도입의 움직임이 있을 경우 통상의 측면에서 적극적이고 선제적인 대응이 필요할 것이다.

커넥티드카 사이버보안, 또 하나의 차별화 포인트

커넥티드카 사이버보안 규제 동향

미래 자동차 시장을 선점하기 위한 각국의 움직임이 가속화되고 있다. 커넥티드카 시장에서 유리한 고지를 점령하기 위해 기술 개발뿐만 아니라 새로운 법과 규제를 도입하면서 기업에 혁신을 요구하고 있다. 이러한 움직임은 궁극적으로 미래 자동차 시장에서 우위를 점함으로써 국가 경쟁력을 강화하기 위한 것이다. 커넥티드카의 다양한 기능 구현을 위해 자동차는 기계장치 중심에서 소프트웨어 중심의 장치로 변모하고 있다. 이에 따라 차량 사이버보안 사고에 대한 우려가 커지면서 자동차 사이버보안 산업은 빠르게 성장하고 있다. SDV(Software Defined Vehicle), 즉 소프트웨어로 자동차를 정의한다는 의미는 수만 개의 기계 부품을 관리하여 완성차 경쟁력을 강화하던 것에서, 수억 라인의 소스 코드를 관리해야 하는 더욱 복합하고 비용이 많이 투입되는 산업으로 경쟁의 패러다임이 바뀌는 것이다. 관리해야 할 소스 코드가 늘어나는 것은 기존에 없던 새로운 안전에 대한 위협, 즉 사이버보안 위협이 증가함을 의미한다. 이에 따라 자동차 업계는 사이버보안 품질을 확보하기 위해 고정된 품질 목표가 아닌 언제든 새로운 사이버보안 위협에 노출될 수 있는 새로운 환경에 직면하고 있다.

[자동차 사이버보안 규제 동향]



UNECE R155에서는 자동차 제조, 생산, 생산 후 관리 및 폐기 시까지 차량 사이버보안 관리 체계 운영을 요구하고 있다. 이는 과거와는 달라진 자동차 제품의 특성을 반영한 것이다. 기존의 자동차는 차량 출시 이후 기능 업그레이드가 거의 없었으며, 소모품만 교환해 가면서 생명주기를 다했다. 그러나 현재, 그리고 미래 자동차는 출시된 차량 하드웨어(HW)를 기반으로 정기 또는 비정기적인 소프트웨어 업데이트를 통해 차량의 기능을 추가, 변경할 수 있는 구조다.

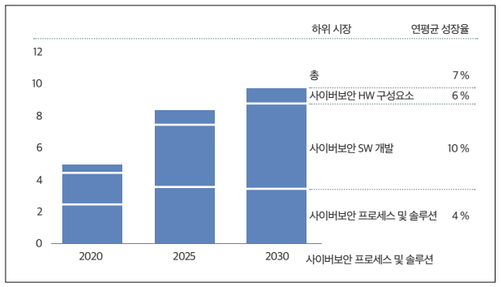
따라서, 소프트웨어는 단순한 차량 제어기 관리 차원을 넘어 차량의 기능을 새롭게 정의하는 중요 부품이 되었다. 소프트웨어로 기능을 추가하고 업그레이드까지 할 수 있는 유연성은 또 다른 시장을 창출하고, 기업에 새로운 사업 기회를 제공하고 있다. 그러나, 이러한 유연성으로 인해 차량 제조 과정에서부터 폐기 시까지 차량 소프트웨어는 지속해서 변경될 수밖에 없다. 이러한 변경점의 연속은 또 다른 문제를 초래하게 된다. 바로 차량 소프트웨어에 가해질 수 있는 사이버보안 위협이 무빙 타겟으로 변모하게 된 것이다. 차량 제조 및 생산 시까지 달성한 사이버보안 품질 목표가 차량 폐기 시까지 유지될 수 없다는 얘기다. 차량 제조 과정에서 사이버보안 강화 활동을 진행하고, 생산 과정에서는 차량에 남아 있는 백도어를 모두 제거한다고 해도 안심할 수 없다. 제품 출시 이후 지속적인 사이버보안 모니터링을 통해 새롭게 발견된 위협을 제거해야만 무빙 타겟을 추적 관리할 수 있다. 자동차 소비자는 차량을 선택할 때 출고 시점의 디자인과 기능뿐만 아니라, 소프트웨어 유지보수 정책과 출고 후 사이버보안 대응 체계도 함께 고려해야 더욱 안전하게 자동차를 운용할 수 있을 것이다.

커넥티드카 사이버보안의 중요도가 커짐으로 인해 관련 산업이 성장하고, 기술 발전에도 가속도가 붙고 있다. 이러한 변화는 자동차 안전에 새로운 위협 요소로 부각되면서, 각국 규제 기관은 자동차 안전을 확보, 유지하기 위한 새로운 규제를 도입하고 있다. UNECE 회원국에서는 이미 2024년 7월부터 모든 자동차에 대한 CSMS

권중한
LG전자
Cyber Security Governance Unit
책임
junghan.kwon@lge.com

인증 및 VTA를 의무화하고 있고, 한국에서도 2025년 8월 신차를 시작으로 2027년 8월까지 모든 차량에 대한 한국 자동차 사이버보안 관리 체계 준수를 요구하고 있다. 차량 단위의 규제뿐만 아니라 부품 단위 규제도 곧 시행을 앞두고 있어 티어(Tier) 부품사들도 사이버보안 규제의 직접적인 영향을 받고 있다. 이에 따라 국내외 주요 완성차 업체에서는 티어(Tier) 부품사들의 사이버보안 대응 역량을 협력사 선정의 주요 평가 기준으로 활용하기 위해 준비하고 있으며, 티어(Tier)1 또한 티어(Tier)2, 티어(Tier)3 업체의 사이버보안 대응 역량 강화를 위해 노력하고 있다.

[자동차 사이버보안 산업규모 및 구성]

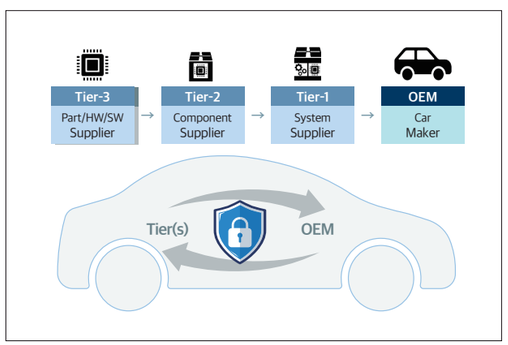


출처 : McKinsey

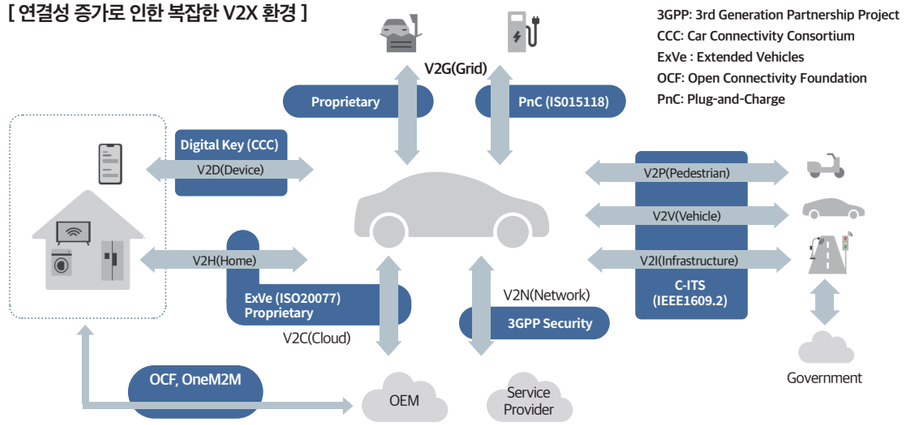
소프트웨어 규모가 커지고 연결성이 강화되면 몇 가지 중요한 체크 포인트가 생긴다. 첫째, 커넥티드카의 연결성은 사이버보안 관점에서 보면, 공격 표면의 무한 확장으로 볼 수 있다. 기존에는 차량에 대한 물리적 또는 근거리 접근을 통해서만 사이버보안 공격이 가능했다면, 커넥티드카는 거대한 인터넷망에 연결됨으로써 불특정 다수에 의한 원거리 사이버보안 공격에 노출되고 있기에 이에 대한 대비가 필요하다.

둘째, 연결성 증가는 다양한 서비스 이용을 가능하게 하며, 이런 서비스 이용을 위해서는 운전자의 여러 가지 개인정보를 수집, 저장, 전송할 필요가 있다. 이 과정에서 사이버보안 사고가 발생하면 개인정보 유출 문제가 발생할 수 있고, 수집된 데이터가 위변조되면 잘못된 정보 제공으로 인해 심각한 안전 문제가 발생할 수 있다. 이에 연결성 증가에 따른 자동차나 사용자 데이터 보호도 반드시 고려되어야 한다. 셋째, 완성차는 수많은 티어(Tier)에서 공급한 부품으로 구성된다. 부품 중에는 서드파티(3rd Party) 소프트웨어, 하드웨어+소프트웨어 통합 부품, 소프트웨어 라이브러리 등이 있을 수 있다. 소프트웨어 또는 소프트웨어를 포함하는 부품 중 보안이 취약하거나 악성 코드가 포함된 부품이 차량에 설치되면 그 파급 효과는 매우 클 것이다. 최근 증가하고 있는 공급망을 이용한 공격 위협은 사전에 인지하고 차단하기가 복잡하고 까다로워서 철저한 공급망 보안 관리 체계 구축이 필요하다. 마지막으로, IT 및 OT 보안 영역도 점점 중요한 점검 포인트가 되고 있다. 제품 보안 관리를 아무리 철저하게 하더라도 제품을 개발하고 유지보수하는데 필요한 IT 환경과 생산에 투입되는 장비의 OT 보안까지 챙기지 않으면, 제품이 고객에게 전달되기 전 예상치 못한 사이버보안 위협에 노출될 수 있다. 최근 CSMS VTA 심사에서는 IT, OT 보안 영역까지 중요하게 점검하는 추세로 변화하고 있다. TISAX와 같이 IT 보안 중심으로 심사하던 인증에서도 제품 사이버보안 영역에 대한 점검을 비중 있게 다루는 양상을 보이고 있기에 IT / OT 보안에 대한 고려도 충분히 해야 한다.

[자동차산업 공급망구성 및 협업관계]



[연결성 증가로 인한 복잡한 V2X 환경]



사이버보안 경쟁력 강화를 위해

완성차 업체의 자동차 사이버보안 규제 대응은 이제 사업의 영속성을 결정짓는 중요한 변수가 되었다. 이는 완성차 업체의 부품사 선정 기준에도 영향을 미치고 있어, 부품사 또한 사이버보안 대응 체계가 회사 경쟁력의 주요한 요소가 되고 있다. 그뿐만 아니라 연결성을 기반으로 한 다양한 V2X 서비스도 증가하면서 사이버보안 위협은 피할 수 없는 현실이 되었다. 이러한 위협의 증가는 위협 대응에 필요한 여러 가지 사이버보안 솔루션 및 기술이 필요하다. 기존 IT 보안 및 모바일 기기에 적용되던 보안 기술들은 자동차 환경에 최적화되어 통합되고 있고, 다양한 보안 솔루션들이 자동차 사이버보안 특성을 반영하여 개발되고 있다. 그런데, 큰 틀에서 보면 새로운 기술이나 솔루션은 많지 않고, 기존 보안 환경에서 알려진 기술과 솔루션들이 주를 이룬다. 연결성이 증가하고 전동화가 진행됨에 따라 자동차 소프트웨어의 규모는 커지고, 이에 최적화된 자동차 아키텍처와 네트워크 구조는 날로 진화하고 있다. 각 단계의 아키텍처는 장단점이 존재하므로, 이를 사이버보안 솔루션 및 보안 기술 개발에 반영하여 차별화 포인트로 활용할 수 있어야 한다.

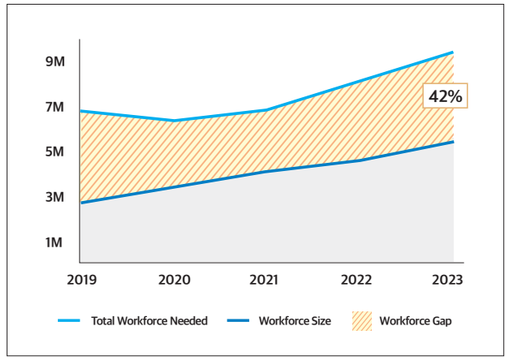
오늘 내 자동차가 사이버보안 관점에서 안전하다고 해서 내일도 안전하다고 보장할 수 없는 시대가 도래했다. 이는 소프트웨어 보안이 갖는 특성 때문이다. 특정 시점에 필요한 사이버보안 조치를 모두 완료한 소프트웨어를 릴리즈하고, 단 한 줄의 소프트웨어도 수정하지 않았다고 가정해 보자. 그렇다면, 이 소프트웨어는 계속 사이버보안 관점에서 안전한 상태에 있을까? 소프트웨어는 언젠가 새롭게 발견된 취약점에 노출될 수 있으며, 그로 인해 더 이상 안전하지 않은 상태로 변할 수 있다. 아무런 변경이 없었지만, 자동차의 안전성은 외부 변수에 의해 지속해서 바뀌는 것이다. 따라서, 또 하나 중요하게 다루어야 할 부분은 지속적인 위협 모니터링과 대응, 그리고 소프트웨어 업데이트이다. 소프트웨어 업데이트는 차량 출시 후 기능을 업그레이드 할 수 있는 SDV(Software Defined Vehicle) 환경에 없어서는 안 될 중요한 기능이자, 사이버보안 관점에서는 출시 후 빠른 사고대응을 위한 필수 사항으로 차량 소프트웨어를 안전한 상태로 유지하는데 가장 중요한 요소라 할 수 있다. 쉽고 안전한 업데이트 체계 구축은 무빙 타겟으로 변한 사이버보안 품질 목표 달성을 위한 거의 유일한 수단이므로 자동차 생명주기 전반에 걸쳐 고려해야 하겠다.

사이버보안을 넘어 안보까지 챙겨야 하는 자동차 업계

2024년 2월 미국의 중국산 커넥티드카 사이버보안 규제 발표는 자동차 사이버보안을 대하는 우리의 자세 전환을 요구하는 중요한 시그널이라고 생각된다. 기존에 발표되었던 자동차 사이버보안 규제는 주로 차량과 차량 사용자 안전에 초점을 맞추었다면, 미국의 규제 방침은 보안을 넘어 국가안보 차원의 의사결정이기 때문이다. 커넥티드카가 국가안보를 위협할 수 있는 사이버 공격 도구로 사용될 수 있다는 점은, 사이버보안 대응이 더 이상 최소 비용 최대 효과의 경제 논리로만 접근할 수 없음을 시사한다. 더 이상 사이버보안 대응을 위한 투자를 미루면 시장에서의 입지는 점점 좁아질 수밖에 없다는 위기의식을 가져야 하겠다.

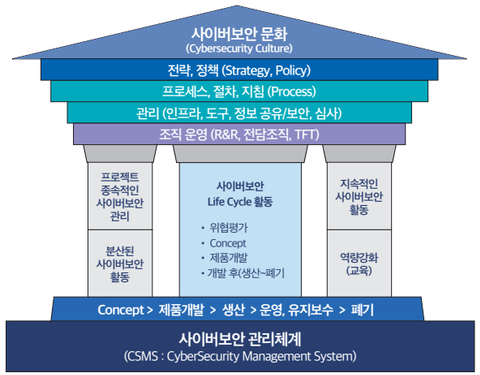
이제 정부, 업계, 학계가 힘을 모아 자동차 산업 경쟁력의 한 축으로 사이버보안 대응력의 중요성을 인지하고 장기적 관점의 로드맵 수립이

[사이버보안 인력수요와 공급]



출처 : ISC2 Cybersecurity Workforce Study, 2019-2023

[자동차 사이버보안 관리체계]



필요하다. UNECE R155 및 미국의 중국산 커넥티드카 사이버보안 규제 대응 지원을 위해 정부에서도 각 규제 별로 지원방안 마련을 위해 움직이고 있다. 이러한 노력이 큰 틀의 방향성에 따라 전략적이고 집중적으로 수행 되도록 하기 위해 우선 해결되어야 할 과제를 몇 가지 제안하고자 한다.

첫째, 사이버보안 규제 대응 컨트롤 타워가 필요하다. 산발적으로 이루어지고 있는 사이버보안 규제 대응을 위한 노력을 통합하고 중복되지 않도록 조율하여 시너지를 내도록 만들어야 하겠다. 정부, 업계, 학계가 모두 참여하여 장기 전략을 수립하고 로드맵을 구체화할 필요가 있다.

둘째, 사이버보안 전문 인력 육성이 필요하다. 자동차에서 소프트웨어 비중이 커짐에 따라 개발 및 유지보수 복잡도가 증가하고 있어, 이를 관리하기 위한 우수 소프트웨어 인력뿐 아니라 사이버보안 전문 인력에 대한 수요도 증가하고 있다. 전 세계적으로 사이버보안 인력에 대한 수요가 급증하고 있지만, 임베디드 소프트웨어 개발 경험을 보유한 사이버보안 전문가를 채용하는 것은 쉽지 않은 것이 현실이다. 사이버보안 전문가 육성은 자동차 산업 사이버보안 경쟁력 강화를 위한 초석임을 공감하고 각 분야의 공동 대응이 필요한 시점이다.

셋째, 교육 및 사이버보안 검증 환경 지원 등 단순히 사이버보안 기술 개발 관점이 아니라 체계를 구축할 수 있도록 다방면의 지원이 필요하다. 앞에서도 언급한 바와 같이 사이버보안 목표는 무빙 타겟이기에 특정 보안 기술을 개발하고 제품에 적용하는 것만으로 충분조건이 될 수 없다. 자동차 산업을 영위하기 위해, 필요한 모든 기업 활동에 사이버보안 관리 체계를 구축하고 적용해야 하므로, 최고경영자를 포함한 전 임직원의 인식 개선 교육과 개발자 대상 기술 교육은 매우 중요한 활동이다. 더불어, 무빙 타겟 문제를 해결하기 위해서는 자동화된 주기적, 지속적 모니터링과 검증 체계가 필요하다. 각 분야 전문가가 머리를 맞대고 공동 대응할 수 있는 시스템을 구축하여 이러한 투자가 어려운 업체를 지원하고, 중복 투자를 방지해야 한다.

넷째, 중복규제 최소화를 위한 공동 대응이 필요하다. UNECE R155/R156을 필두로 한 EU의 NIS Directive(Directive on security of network and information systems), CRA(Cyber Resilience Act) 규제, RED(Radio Equipment Directive) 3.3 인터넷 연결 기기에 대한 사이버보안 규제, 중국의 GB·GB/T 사이버보안 규제, 브라질/싱가포르의 통신기기 사이버보안 규제와 더불어 미국의 중국산 커넥티드카 사이버보안 규제도 시행을 앞두고 있다. 사이버보안의 중요성을 인지하고 안전한 모빌리티 환경을 만들고자 하는 각국의 노력은 바람직하나 분명히 중복된 부분이 있기에 중복규제를 제거하고, 필요한 경우 국가 간 상호인증을 추진하여 기업의 규제 대응에 대한 짐을 덜어줄 필요가 있다.

사이버보안 규제는 일종의 무역장벽이나 자동차 산업의 또 다른 진입장벽이 될 수 있지만, 규제 동향을 면밀하게 파악하고 예측함으로써 국내 자동차 산업 경쟁력 강화를 위한 수단이 될 수도 있다. 최근 각 분야에서 사이버보안의 중요성을 인식하고 제대로 준비하고자 하는 움직임은 매우 긍정적인 신호라고 생각된다. 모쪼록 이러한 노력이 시너지를 내어 사이버보안이 대한민국 자동차 산업 경쟁력의 새로운 해자가 되고, 미래 모빌리티 시장을 우리 기업들이 주도하는 희망찬 미래를 기대해 본다.

한국자율주행산업협회는 급변하는 미래 모빌리티 산업에서
우리나라가 자율주행 관련 기술 우위를 확보하고,
산업 생태계를 선도할 수 있도록 다양한 민간기업, 대학, 유관기관 사이의
소통과 협업을 주도하고 있습니다.

또한, 협회는 자율주행 산업 생태계 활성화와 경쟁력 제고를 위해
정책기획, 기반구축, 산업진흥, 국제협력 등 산·학·연·관과 연계하여
주도적 역할을 수행함으로써 효율적인 사업 방향을 모색해 나가겠습니다.

KAAMI
KAAMI 한국자율주행산업협회
Korea Association of Autonomous Mobility Industry
www.kaami.or.kr
kaami@kaami.or.kr

미·중 전략 경쟁의 맥락에서 본 커넥티드카 규제

BYD전기차 (출처 : BYD 홈페이지)

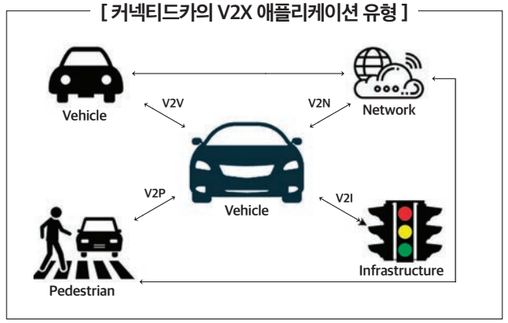
2024년 5월 6일 토니 블링컨 미국 국무부 장관은 샌프란시스코에서 열린 세계 최대 정보보안박람회 'RSA 콘퍼런스'의 기조연설자로 나서 '미국 국제사이버 공간 및 디지털 정책전략(US International Cyberspace and Digital Policy Strategy)'의 일부를 공개했다. 블링컨 국무장관은 "미국과 동맹국들의 기술 경쟁력을 확보하면서 민주주의적 가치를 안전하게 지키고 신기술로 인한 위험 요인들을 최소화하는 데 그 목적이 있다"라고 강조했다. 블링컨 국무장관이 명시한 6대 핵심 기반기술 분야는 반도체, 고급 컴퓨팅 및 양자 기술, AI, 생명공학, 청정에너지 기술, 그리고 첨단 통신 분야다.

그간 미국의 대중국 견제는 첨단반도체, 슈퍼컴퓨팅, 양자 정보기술을 중심으로 특정 품목 및 장비에 대한 수출통제로 이뤄져 왔다. 그러나 2024년 2월 미국 정부가 두 개의 새로운 규제를 발표하며, 미국의 대중국 견제 양상도 변화하고 있다. 하나는 데이터 이전 금지에 대한 대통령 행정명령(E.O. 14117)[1]이며, 다른 하나는 커넥티드카 규제 제정 사전 예고(ANPRM: Advance Notice of Proposed Rule Making)이다. 미국은 이제 상품을 넘어서 데이터 및 정보통신 네트워크로 그 견제의 초점을 확대해 나가고 있다. 그리고 그 중심에 커넥티드카(connected car) 이슈가 있다.

국내에서는 커넥티드카 이슈를 전기차 이슈로 단순화해서 보는 경향이 지배적이지만 이것은 큰 착각이다. 커넥티드카를 다루는 미국의 시각은 사이버안보와 정보통신 서비스상 국가안보의 확보에 있다. 이번 커넥티드카 규제를 위해 제안된 규칙은 2019년 5월 15일 트럼프 1기 대통령 행정명령 "정보통신 기술 및 서비스 공급망 보안(E.O. 13873, Securing the Information and Communications Technology and Services Supply Chain)"에 근거하고 있다. 특히 본 행정명령에 따라 2023년 12월 설립된 상무부 산업안보국(BIS) 정보통신기술 서비스 사무소(OICTS)의 첫 번째 안건이 바로 커넥티드카 규제 이슈다.

현재 미국이 준비하고 있는 조치로 인해 글로벌 자동차업계는 자동차의 사이버보안뿐만 아니라 지정학적 위험을 고려하여 차량에 들어가는 정보통신 부품의 특정국 의존도까지 탈피해야 하는 상황에 부닥쳤다.

[커넥티드카의 V2X 애플리케이션 유형]



1) 바이든 대통령은 2024년 2월 28일 국가안보를 이유로 '우려 국가'로의 특정 민감한 데이터 전송을 제한하거나 금지하는 E.O. 14117을 발표.

미국의 커넥티드카 규제

미국 바이든 대통령은 2024년 2월 29일 상무장관에게 중국 등 우려 국가[2]의 정보통신기술을 활용한 자동차(커넥티드카)의 안보 위험을 조사하고 필요한 조치를 하라고 지시했다. 이에 따라 미국 상무부 산업안보국(BIS)은 2024년 2월 29일에 규칙 제정 사전 예고(ANPRM: Advance Notice of Proposed Rule Making)를 발표하여 커넥티드카 규제에 대한 공개 의견을 구했다. 특히 ANPRM에서는 2024년 4월 30일까지 다음과 같은 사항에 대한 이해당사자들의 의견을 구했다.

(1) 커넥티드카의 정의

(2) 커넥티드카에 필수적인 ICTS 거래가 초래할 수 있는 미국 안보에 대한 리스크

(3) 상기 위험에 대응하기 위한 실행 가능한 메커니즘

(4) 미국의 안보 위험이 완화되었음을 증명하여 금지된 거래에 대한 참여를 승인하는 절차를 마련할 것인지 여부

이후 제출된 의견들을 취합하였으며, 후속 조치로서 2024년 9월 23일에 미국 상무부 산업안보국(BIS)은 중국 및 러시아와 관련된 업체가 설계, 개발, 제조 또는 공급하는 커넥티드카와 차량 시스템 및 부품의 수입 또는 판매를 금지하는 규칙 제정 제안 공고(NPRM: Notice of Proposed Rule Making)를 발표했다. 제안된 규칙은 중국 및 러시아와 관련 있는 특정 차량 연결 시스템(VCS: Vehicle Connectivity Systems)과 자동 운전 시스템(ADS: Automated Driving Systems) 하드웨어 또는 소프트웨어가 장착된 차량의 미국 내 수입 또는 판매를 금지한다.

Bluetooth, 5G, 위성 및 Wi-Fi 모듈과 같은 VCS를 사용하면 차량이 외부와 통신할 수 있고, ADS는 자율 주행 차량이 운전자 없이 운행할 수 있도록 하는 구성 요소와 시스템을 다룬다. 소프트웨

2) 조사의 근거가 되는 대통령에 근거한 최종 규칙에서는 '외국 적대자(foreign adversary)'가 관련된 ICTS 거래를 금지 조치 등의 대상으로 삼고 있다. '외국의 적대자'는 상무장관에 의해 홍콩을 포함한 중국, 쿠바, 이란, 북한, 러시아, 베네수엘라 등 6개 국가가 지정되어 있으므로 이번 조사 대상은 반드시 중국만 해당하는 것은 아니지만, ANPRM에서는 주로 중국을 대상으로 하고 있음.

연원호
국립외교원
경제기술안보연구센터장
whyeon24@mofa.go.kr

지나 러몬도 미국 상무장관_출처 : 연합뉴스

출처 : 아시아경제

어에 대한 금지 조치는 2027년 모델부터, 하드웨어에 대한 금지 조치는 2030년 모델부터 적용할 것을 제안하고 있다. BIS는 2024년 11월 12일까지 NPRM에 대한 이해관계자들의 의견을 수렴하고 2024년 내로 최종 규정을 발표할 가능성이 크다.

안보위협론 말말말

"中 당국에수집정보 넘어갈것"

바이든 미국 대통령

中 커넥티드카 조사, 위험 조치 지시

러몬드 미국 상무 장관

中 전기·자율주행차 정보 수집 우려

피터 부티지지 미국 교통장관

中 교통 기술 안보 우려 있다

출처 : The JoongAng

배경 및 목적

2024년 2월 바이든 대통령은 이번 조치가 중국을 포함한 우려 국가의 커넥티드 차량이 초래하는 국가안보 위험으로부터 미국인을 보호하기 위함이라고 설명했다. 상무부는 구체적으로 차량의 네트워크 연결성이 증가함에 따라 민감한 정보를 수집하고 악용할 기회가 발생한다고 지적했다.

커넥티드카가 제기하는 리스크는 크게 세 가지로 볼 수 있다. 첫째는 운전자 또는 커넥티드카 주변 정보에 대한 데이터 탈취, 둘째는 운행 중인 자동차에 대한 사이버 공격, 셋째는 자동차를 매개로 한 주변 인프라에 대한 사이버 공격이다. 특히 미국의 이번 조치는 미·중 전략 경쟁의 맥락에서 중국이 제기하는 '특히 심각하고 지속적인 위협'에 주의를 기울이고 있다.

바이든 대통령은 2월 성명에서 "중국의 커넥티드카는 미국 국민과 인프라에 대한 기밀 데이터를 수집해 중국으로 보낼 수 있다"라고 언급했다. 9월 NPRM을 발표하는 자리에서 제이크 설리번 국가안보 보좌관도 "중국 등은 커넥티드 차량을 통해 운전자와 승객의 민감한 개인 데이터, 지리적 위치 데이터, 오디오 또는 비디오 녹화, 기타 생활 방식 분석 등을 수집하려고 하고 있다"라며 "이는 미국인들의 개인 보안에 지대한 위협이 될 수 있다"라고 강조했다. 미국 정부는 2024년 2월 28일 우려 국가들이 미국인의 민감한 개인 데이터 및 미국 정부 관련 데이터에 대한 접근하는 것을 방지하는 행정명령(E.O. 14117)을 이미 발표한 바 있다.

또한, 바이든 대통령은 통신 성능을 갖춘 커넥티드카를 '달리는 스마트폰'이라고도 불렀다. 그러면서 커넥티드카가 스마트폰, 주변 차량, 교통 인프라와도 지속적인 통신이 가능하며, 원격으로 차량을 제어할 수도 있다는 점에서 사이버 공격을 받으면 큰 피해가 발생할 수 있다는 점을 지적했다. 러몬도 상무장관은 2024년 5월 로이터통신과의 인터뷰에서 "도로에 차량 수백만 대가 있는데 소프트웨어가 작동을 멈추면 극도로 재앙적인 상황이 초래될 것"이라며 중국산 동영상 앱인 틱톡(TikTok)이 제기하는 위협과 크게 다르지 않다고 강조했다.

미국 정부 내에서는 인공지능(AI) 등의 보급에 따라 정보 조작과 사이버 공격에 대한 우려가 커지고 있다. NPRM 브리핑에서 제이크 설리번 국가안보 보좌관은 "이미 중국이 교란 및 방해 행위를 목적으로 미국의 주요 인프라에 악성 코드를 심고 있다는 충분한 증거를 발견했다"라고 밝혔으며, 특히 전기차 충전소, 스마트 도로 등 주요 인프라에 커넥티드 차량이 점점 더 많이 통합됨에 따라, 사이버 해킹 등을 통한 중국의 교란 위험이 극적으로 증가하고 있다고 우려했다.

[커넥티드카의 진화와 주요 키워드]

출처 : KAMA웹진

커넥티드카 규제의 의미와 시사점

현 단계에서는 우려할 만한 중국산 장비를 탑재한 차량이 미국 내에는 많지 않기 때문에, 올해 발표된 미국의 커넥티드카 규제 조치들은 커넥티드카 본격 보급에 따른 위험에 사전 대비 성격이 크다고 할 수 있다. 9월 NPRM을 발표하는 자리에서 러몬도 장관도 "미국의 도로가 중국 자동차로 가득 차고 위험이 극도로 커질 때까지 기다리지 않고 지금 선제적으로 조치를 취해 미국 국민을 보호하고 국가안보 위협을 억제할 것"이라고 언급했다.

업계는 당장 공급망에 미칠 영향을 우려한다. 존 보젤라(John Bozella) 미국 자동차 혁신협회(Alliance for Automotive Innovation) CEO는 BBC와의 최근 인터뷰에서 "세계에서 가장 복잡한 공급망을 하룻밤 사이에 마치 스위치를 켜는 것처럼 바꿀 수는 없다"라고 말하며, "규제안에 포함된 리드 타임은 일부 자동차 제조업체에는 필요한 전환을 완료하기에 충분할 수 있지만, 다른 제조업체에는 너무 짧을 수 있다."라고 우려를 표했다.

그러나 미국 정부가 커넥티드카 산업을 반도체, 양자 컴퓨팅, AI 분야와 함께 국가의 핵심 기술 인프라의 일부로 간주하고 있음을 자동차 업계는 인식할 필요가 있다. 미국 정부가 이번에 제안한 규정이 본격 도입될 것으로 보이는 2030년까지는 아직 시간이 남았지만, 자동차 업계는 미·중 전략 경쟁이 지속하는 한 미국 정부의 규제 방향성은 일관될 수밖에 없다는 점을 이해해야 한다. 따라서 자동차업계는 당장 지금부터 NPRM이 자사에 미치는 영향과 그 정도를 파악해야 할 것이다. 특히 신차 개발 및 출시에 오랜 시간이 걸리는 점을 고려한다면 자동차 제조업계는 빠른 시일 내에 자체 공급망을 재평가하고 공급망 재편에 나서야 할 것으로 보인다.

더욱이 기술이 발전하고 잠재적인 국가안보 취약성이 확인되면 미국 정부는 이 분야 및 관련 분야에 대한 규제를 더욱 강화하거나 새로운 규제를 추가로 도입할 가능성도 크다. 이번 NPRM은 외국 기업과 관련된 ICTS 거래로 인해 제기되는 국가안보 우려를 해결하기 위한 미국 정부의 지속적인 노력의 첫 단계에 불과하다. 미국 정부가 공급망의 취약성을 인지할 경우, 예를 들어 잠재적인 적국의 커넥티드카 접근, 데이터 유출 및 조작이 일어나면 특정 시장 참여자를 주저하지 않고 퇴출할 수 있음을 시사한다는 점에 주목해야 한다.

자동차가 발명된 지 260여 년 동안 자동차 기술은 달리고, 돌고, 멈추는 이동수단으로서의 기술을 중심으로 발전해왔지만, 최근 20년은 무선통신기술의 발전과 함께 '연결'이 새로운 기술로 추가되었다. 초기에는 통신(Telecommunication)과 정보과학(Informatics)을 합친 조어로 텔레매틱스(Telematics)라고 주로 불렀으며, 자동차에 주로 이동통신망을 통한 무선통신 시스템을 이용하여 각종 서비스를 제공하는 것을 말했다. 최근에는 이 시스템을 탑재한 자동차를 커넥티드카, 그 시스템을 활용하여 제공하는 서비스를 커넥티드 서비스라고 부르며, 정보통신기술(ICT)의 발전과 함께 자동차 산업의 기술 및 서비스 혁신을 지속하고 있다.

문제는 기술의 변화에 미·중 전략 경쟁이 더해져 새로운 보안 이슈를 낳고 있다는 점이다. 자동차업계는 새로운 보안위험을 예측하기 위해 항상 준비해야 하며, 커넥티드카에 있어서 데이터가 자동차뿐만 아니라 관련 생태계 전반을 통해 흐르고 있다는 점에서 자동차를 넘어선 정보통신 인프라 전반에까지 관심을 가져야 하는 시대를 맞이했다.

심상규

아우토크립트㈜ 부사장

Interview

자동차 사이버보안 인증평가의 기준을 만든다.

AUTOCRYPT

아우토크립트(주)

자동차가 점차 소프트웨어 중심으로 변화하면서 기술 발전의 패러다임이 급격히 전환되고 있다. 소프트웨어 정의 차량(SDV)은 전기차와 커넥티드카를 중심으로 발전하고 있으며, 이러한 기술적 변화는 새로운 과제를 제시한다. 그중에서도 사이버보안 이슈는 자동차 산업에서 해결해야 할 중요한 과제이며, 동시에 신흥 시장으로 주목받고 있다.

커넥티드카의 증가와 함께 글로벌 규제 및 법규가 강화되면서, 사이버보안을 해결하기 위한 노력이 활발히 진행되고 있다. 이 과정에서 국내의 대표적인 자동차 사이버보안 인증평가 전문기업인 아우토크립트(AutoCrypt)가 시장의 주목을 받고 있다. 아우토크립트는 17년 동안 자동차 보안 솔루션을 개발하며, 글로벌 자동차 보안 표준인 ISO/SAE 21434와 같은 국제적 기준을 충족하는 인증 시스템을 구축해 왔다. 이를 통해 세계 각국의 자동차 제조사들이 요구하는 규제에 부합하는 보안 체계를 제공하고 있다. 특히 2024년 5월, 아우토크립트는 아시아 태평양 지역 최초로 유럽차 소프트웨어 보안 인증평가기관에 선정되었으며, 이를 계기로 해외 평가기관에서도 아우토크립트의 기술력과 가능성을 높이 평가하고 있다. 이러한 성과는 아우토크립트의 기술력이 전 세계적으로 인정받고 있음을 보여주며, 향후 글로벌 자동차 보안 시장에서의 성장이 기대된다.

모빌리티 인사이트는 아우토크립트의 심상규 부사장과의 인터뷰를 통해, 자동차 사이버보안 분야에서의 최신 동향과 도전 과제, 그리고 아우토크립트가 글로벌 시장에서 어떻게 경쟁력을 갖추고 있는지에 대한 생생한 목소리를 담았다.

새로운 기회의 시장, 사이버보안 시작부터 '남다른 출발'

이번 10월호 주제인 '커넥티드카 사이버보안 실태 및 방향성'에 적합한 국내 기업을 찾는 것은 결코 쉽지 않았다. 그만큼 이 분야는 아직 생소하고, 높은 전문성을 요구하는 영역이다. 이에, 국내 자동차 사이버보안 인증평가 전문기업인 '아우토크립트'의 심상규 부사장을 만나, 아우토크립트의 사업 전반과 자동차 사이버보안 산업과의 연관성 및 중요성에 대해 등에 대해 구체적인 내용을 요약하여 담아본다.

아우토크립트의 자동차 사이버보안 사업은 어떻게 시작되었으며, 심부사장의 개인적인 경력에 대해 물어봤다.

"저는 석박사 과정에서 정보보안을 전공했습니다. 그중에서도 암호알고리즘의 안전한 구현 방법을 연구하였고, 박사 취득 후에 사이버보안 전문기업 펜타시큐리티에서 잠시 근무하고, 삼성전자로 이직하여 콘텐츠 저작권 보호를 위한 기술을 연구·개발하였습니다. 선배들과 창업을 하기도 하였고, 2012년에 펜타시큐리티에 재입사를 하였습니다. 재입사 후에 펜타시큐리티의 신사업을 위한 기술개발을 맡았는데, 자동차 사이버보안과 사물인터넷(IoT; Internet of Thing) 보안이 주된 연구분야였습니다. 2012년에 자동차 사이버보안을 이야기하면, '자동차에 사이버보안이 왜 필요한 것이냐?"는 반문이 대부분이었습니다. 그렇지만, 저는 자동차 사이버보안의 미래에 핵심 기술이 될 것이라는 확신이 있었고, 자동차 제조사와 부품사들이 요청하는 기술을 개발하여 공급하면서 조금씩 자동차 사이버보안을 더 깊이 연구하게 되었습니다."

정보보안 분야가 방대한데, 특별히 자동차 사이버보안에 대해 관심을 갖게된 특별한 계기가 있었는지 궁금하다.

"2015년은 자동차 사이버보안에서 기념비적인 사건이 있었던 시기입니다. 두 명의 해커가 달리는 지프 체로키 차량을 원격지에서 통신을 통해 해킹할 수 있음을 시연했던 사건입니다. 이 사건으로 자동차 제조사를 포함한 자동차 관련 기업들뿐만 아니라 해외의 국가 기관들이 자동차 사이버보안의 필요성을 절실히 인지하게 되었습니다. 두 해커 덕택에 '자동차에 사이버보안이 왜 필요한 것이냐?"는 질문의 답을 쉽게 제시할 수 있었습니다. 또한, 공교롭게도 2015년은 펜타시큐리티가 자동차 사이버보안을 전문적으로 연구하는 기업부설 연구소를 개소한 해이기도 합니다. 연구소가 집중적으로 연구했던 기술은 자동차의 외부 통신을 안전하게 보호하는 기술이었습니다. 자동차가 주변의 다른 자동차와 통신(V2V; Vehicle-to-Vehicle)하거나, 자동차가 도로와 통신(V2I; Vehicle-to-Infrastructure)하는데 필요한 보안 기술을 국내 최초로 개발하였고, 개발된 기술을 국내의 C-ITS(Cooperative Intelligent Transport System) 사업에 적용하였습니다. 2015년 두 해커가 선보인 기법은 자동차가 갖는 외부 통신 채널을 통해 자동차에 침입하는 것이었습니다. 자동차의 외부 통신 채널을 안전하게 만드는 것은 자동차의 해킹을 방어하는데 가장 먼저 확인되어야 합니다.

아시아 최초로 자동차 사이버보안 솔루션을 출시한 펜타시큐리티는 2019년 8월에 관련 조직을 분사하여 아우토크립트가 출범하게 되었습니다. 2012년에 시작했던 펜타시큐리티의 신사업이, 2015년에는 자동차 사이버보안 전문 연구소를 만들고, 2019년에는 자동차 사이버보안 전문기업을 만들어 내었습니다."

심상규 부사장을 통해 들은 그의 이력만큼이나 아우토크립트 탄생의 뒷이야기는 사뭇 흥미로웠다. 또한 사업 진척과 맞물려 자동차 시장 내 사이버보안의 중요성이 커지던 시점에 이를 본격적인 사업 아이템으로 선정하고, 이를 위해 매진했다는 점에서 지금의 아우토크립트가 이만큼 성장한 데에는 분명한 이유가 있었다는 확신이 들었다.

사이버보안 글로벌 규제·법규 단순한 통과를 넘어 '실질적인 솔루션' 필요

오늘의 핵심 주제인 자동차 시장에서 사이버보안의 중요성에 대한 그의 생각을 들어봤다.

"간단하게 말하자면, '법제화를 통해 의무화되었으니 중요하다'라고 하겠으나, 이것은 너무나도 소극적이고 수동적인 의견입니다. UNECE(유엔 유럽경제위원회)의 Regulation 155(UNR 155)와 Regulation156(UNR 156)가 제정된 이후, 여러 나라에서 UNR 155와 UNR 156에 대응하는 법제화가 이루어졌고, 우리나라에서도 자동차관리법이 개정되었습니다. 법을 준수하자면, 자동차 제조사가 사이버보안 관리체계를 갖추고, 생산하는 자동차에도 사이버보안이 적용되어야 합니다.

많은 사람이 자동차가 바퀴 달린 스마트폰으로 변하고 있다고 이야기합니다. 컴퓨터에 인터넷이 본격적으로 보급되던 시기에 다양한 해킹 사건들이 있었습니다. 스마트폰이 확산하는 시기에도 다양한 해킹 사건들이 있었습니다. 현재에도 컴퓨터와 스마트폰에서 피싱(phishing), 개인정보 유출, 시스템 침해 등의 다양한 보안 사고들이 발생하고 있습니다. 이런 일들이 앞으로 자동차에서도 일어날 수 있다는 것은 자명한 일입니다.

컴퓨터 혹은 스마트폰에서 발생하는 보안 사고는 개인의 피해에 그치지만, 자동차에서 보안 사고가 발생한다면 탑승자뿐만 아니라 보행자의 인명 피해로 이어질 수 있고, 국가적인 교통 대란으로까지 확산할 수 있습니다. 최근, 자동차 급발진 추정 사건들과 전기차의 화재 사고들이 발생하여 큰 인명 손실과 재산 피해가 있었습니다. 자동차의 외부 통신을 통해 해커가 자동차를 장악한다면, 자동차 급발진 및 화재 등의 조작도 충분히 가능합니다. 자동차가 바퀴 달린 스마트폰으로서 더욱 많은 통신 기능을 갖게 되면, 해커가 침입할 수 있는 경로도 그만큼 많아집니다. 자동차의 사이버보안은 자동차의 외부 통신을 안전하게 해주고, 자동차의 내부 시스템을 안전하게 지켜줍니다. 법을 준수하기 위해 자동차에 사이버보안을 적용하는 소극적인 적용이 아니라, 자동차의 보안 사고로 인한 인명 피해나 재산 피해가 발생하지 않도록 사이버보안의 적극적인 적용이 필요합니다."

자동차 시장 내 사이버보안의 중요성에서 글로벌 규제와 법규가 핵심이라는 부분에 대해 보다 구체적인 설명을 들어봤다.

"미국 상무부(Department of Commerce)는 2024년 2월에 ANPRM(Advanced Notice of Proposed Rulemaking)을 발표했고, 9월 23일에는 NPRM(Notice of Proposed Rulemaking)을 공시했습니다. 이 두 규제는 '미국의 국가안보 확보를 위해 자동차 사이버보안이 필요하다'는 전제를 바탕으로 하고 있습니다. 여기서 중요한 것은 사이버보안이 적용되지 않은 부품이나 자동차가 미국 시장에 수입되는 것을 금지한다는 점입니다. 이는 자동차 사이버보안이 단순히 탑승자나 보행자의 안전을 위해서만 필요한 것이 아니라, 국가 안보를 위한 필수 요소임을 의미합니다. 따라서 자동차 사이버보안은 법적 기준을 충족하는 것 이상의 의미를 지니며, 안전과 더불어 국가 안보를 위한 국제적인 요구로 자리잡고 있습니다."

자동차 사이버보안 구축 자동차 산업의 '특수성 고려해야'

커넥티드카로 발전하는 미래 자동차 시장에서 사이버보안의 중요성은 더욱 커지고 있다. 그만큼 기술 개발에도 현실적인 어려움이 많을텐데, 현업에서 느끼는 자동차 사이버보안 솔루션 개발의 어려운 점은 무엇인지 궁금하다.

"사이버보안을 자동차에 적용하거나, IT 환경이나 IoT 환경에 적용하는

것은 생각하는 것보다 어려운 일입니다. 사이버보안이 다른 기술들과는 다른 특성이 있기 때문입니다. 다른 기술들은 일정 수준의 목표를 설정할 수 있고, 그 목표를 달성하면 기술 수준이 유지됩니다. 운전자가 방향을 바꾸거나 가속 또는 제동하는 조작에 맞춰 차량이 동작하는 기술은 일정 수준의 목표를 설정할 수 있습니다. 어떤 수준의 민감도를 가지며, 어떤 수준의 정확도와 반응 속도를 갖느냐가 목표가 될 수 있고, 목표를 달성한 기술을 자동차에 적용하면 해당 기술의 수준이 저하되는 일은 거의 발생하지 않습니다. 자율주행을 위해 자동차가 주변을 인지하는 기술도 일정 수준의 인식률과 정확도를 설정할 수 있습니다.

그러나 사이버보안은 기술 수준을 정량적으로 설정하는 것이 거의 불가능합니다. 몇 점짜리 사이버보안이냐, 혹은 몇 %의 공격을 차단할 수 있냐를 설정할 수가 없습니다. 현재에 최고 수준의 사이버보안 기술을 적용했다고 하더라도, 새로운 보안 취약점이나 공격법이 발견되면 적용된 사이버보안 기술의 수준이 상대적으로 저하될 수밖에 없습니다. 새로운 보안 취약점이나 공격법이 있는지 지속해서 살펴보고, 이에 대응할 수 있도록 기존에 적용한 사이버보안 기술을 조정하거나 갱신해야 합니다. 가정이나 회사에서 사용하는 컴퓨터에 바이러스 백신 프로그램을 설치하고, 지속해서 백신 업데이트를 해줘야 하는 것과 같은 이유입니다."

자동차가 하드웨어 중심에서 소프트웨어 중심으로 발전하면서, 커넥티드카에서 사이버보안의 중요성에 대한 설명을 들어봤다.

"자동차에서도 사이버보안을 적용한 후에 새로운 취약점과 공격법에 대응할 수 있도록 지속적인 운영과 관리가 필요합니다. 자동차 내 전자제어장치의 소프트웨어나 사이버보안 기술의 갱신이 필요할 때는 업데이트를 시행해야 하고, 이는 차량의 OTA(Over The Air) update 체계를 이용하여 진행할 수 있습니다. 하지만, 전자제어장치의 소프트웨어나 사이버보안 기술의 수정을 통해서 대응하는 것에 한계가 있을 수 있습니다. 자동차의 전자제어장치는 수행해야 하는 고유 기능에 적합하도록 하드웨어를 설계하고, 해당 하드웨어에 특화된 소프트웨어 개발을 해야 하는 경우가 대다수입니다. 이런 경우, 새롭게 발견된 사이버보안 문제를 해결하기 위해 하드웨어 시스템의 한계나 소프트웨어의 큰 수정이 허용되지 않을 수 있습니다.

자동차 환경이 IT 환경이나 IoT 환경에 비해 가장 큰 특징은 자동차의 생명주기가 길다는 것입니다. 자동차 제조 기술의 발전으로 자동차가 제조된 이후 폐차되기까지의 생명주기를 최소 15년 이상으로 보고 있습니다. UNR 155와 UNR 156등의 사이버보안 규제는 자동차가 생산된 이후 운영기간 동안 사이버보안의 운영과 관리를 요구하고 있습니다. 2024년에 생산하여 출고된 자동차가 10년, 15년 후에도 운영될 수 있도록 하려면 사이버보안의 운영과 관리를 제공해야 합니다. 10년 후나 15년 후에는 현재와는 전혀 다른 수준의 새로운 공격법이 출현할 수 있고, 그러한 상황에서도 2024년에 생산된 자동차에 사이버보안을 확보해야 합니다. 뒤집어서 생각해 보면, 10년 전 혹은 15년 전에 사용하던 컴퓨터에 최신 보안 기술을 적용해야 하는 것과 유사한 상황입니다.

이에 반해, 첨단 운전자 보조시스템(ADAS; Advanced Driver Assistance System), 자율주행을 비롯한 첨단 편의 기능이 자동차에 적용되고 있기에, 자동차에 탑재되는 소프트웨어의 비중과 통신의 역할이 늘어나고 있습니다. 소프트웨어의 비중이 늘어나고, 통신의 역할이 확대되는 것은 사이버보안의 위협이 증가하는 것을 의미합니다. 이러한 이유로, 자동차에서 사이버보안이 더욱 중요한 기술로 인식되고 있습니다.

하지만, 자동차의 전자제어장치는 환경 측면에서 여러 가지를 제약하고 있습니다. 전자제어장치의 제한된 자원을 일부만 사용하여 전자제어장치의 고유 기능에 지장을 주지 않지만, 사이버보안의 기술 수준을 높여 적용하여야 하는 문제는 쉽지 않습니다. 이 문제를 해결하려면, 자동차와 전자제어장치의 환경과 속성을 잘 이해하고, 사이버보안 기술의 적용과 응용을 위한 전문 기술팀의 역할이 필수적입니다. 아우토크립트는 사이버보안의 전문 지식과 오랜 경험으로 자동차와 전자제어장치에 사이버보안 기술을 최적화하여 적용할 수 있도록 돕고 있습니다."

복잡한 공급망에서의 사이버보안, 자동차 산업의 새로운 도전

자동차가 커넥티드카로 발전하고, 다양한 소프트웨어들이 직간접적으로 결합되면서 사이버보안의 중요성은 더욱 커지고 있다. 특히, 자동차 산업은 다른 산업과 달리 방대한 부품과 복잡한 공급망이라는 특수성을 가지고 있는데, 이 부분에 대해 물어봤다.

"자동차에서 사이버보안을 확보하는데 또 다른 어려움은 자동차의 공급망이 방대하고 복잡하다는 점입니다. 2024년 9월, 레바논에서 무선호출기가 원격 기폭 제어를 통해 폭파되어 수십 명이 사망하고 수백 명이 다치는 큰 사건이 있었습니다. 해당 무선호출기는 부품 공급 과정에서 원격 제어 기폭 장치가 포함되었을 것으로 추정되고 있습니다. 무선호출기 생산 공급망에서 큰 보안 문제가 발생하여 수많은 인명 피해가 났습니다. 자동차 생산 공급망은 무선호출기 생산 공급망보다 몇십 배 이상 복잡합니다. 자동차 한 대를 생산하기 위해 수백 개 기업이 부품 공급에 참여하고 있으며 이 과정에서 고의, 혹은 실수로 인해 보안 위협 요소가 발생한다면, 무선호출기 폭파 사고보다 더 위험한 사고가 발생할 수 있습니다.

자동차 사이버보안 현재-미래차를 아우르는 'Hot Issue'

커넥티드카에서 사이버보안의 중요성에 대해선 이견이 없다. 그렇다면, 전기차 중심으로 발전하고 있는 현재 상황에서 사이버보안의 역할은 무엇인지 궁금하다.

"2024년 8월 초, 국내에서 전기차 대형 화재가 발생하여 사회적으로 큰 쟁점이 되었습니다. 충전 중이 아닌, 주차 중에 발생한 화재로 알려져 있고, 사이버보안과의 연관성은 밝혀진 바가 없습니다. 하지만, 우리가 생각해 볼 점이 있습니다. 전기차는 앞으로도 늘어날 것이고, 충전을 위해 충전기와 연결된 상태이거나, 자동차의 원격관리를 위해 원격의 관리서버와 연결되는 경우도 늘어날 것입니다. 이런 환경에서 공격자가 침투하여 충전기를 임의로 제어하거나 자동차 내부의 배터리 관리시스템을 임의 조작한다면 더욱 큰 사고가 광범위하게 발생할 가능성이 존재합니다. 충전기들도 원격관리와 충전 서비스 제공을 위해 백엔드 서버와의 통신 기능을 갖습니다. 공격자가 충전기를 1차 공격 대상으로 삼고, 충전기를 통해 자동차에 진입한다면 방어하기 어려운 공격 경로가 완성됩니다. 충전기 대부분은 자동차와 유선 전력망 통신으로 연결되지만, 무선 통신을 사용하여 자동차와 연결되는 다른 기기들도 유사한 문제가 발생할 수 있습니다. 자동차의 사이버보안을 자동차에만 국한할 것이 아니라, 자동차와 연결된 모든 것에 사이버보안을 적용해야 하는 것이 이런 이유입니다."

설계 단계에서 출시 이후까지 철저한 '사이버보안을 책임지다'

자동차 시장에서 사이버보안의 중요성은 이제 당연한 주제로 자리잡고 있다. 특히, 글로벌 규제와 법규가 발효되면서 그 역할은 더욱 강조되고 있다. 이런 환경변화 속에서 아우토크립트의 주요 사업과 솔루션은 어떤 역할을 하고 있는지를 물어봤다.

"아우토크립트의 기술은 크게 두 가지로 구분됩니다. 첫째, 자동차의 외부 통신(V2X)을 안전하게 하기 위한 보안 기술과 자동차 내부 시스템(In Vehicle System)을 안전하게 하기 위한 보안 기술입니다. 자동차 외부 통신(V2X) 보안은 전기차와 충전기 사이의 충전을 위한 통신 보안, C-ITS 사업의 V2V 통신 및 V2I 통신의 통신 보안을 제공하고 있습니다. 둘째, 자동차 내부 시스템 보안은 차량 내부 전자제어장치의 펌웨어, 미들웨어, 소프트웨어를 사이버보안 측면에서 안전하게 만드는 기술을 제공하며, 차량 내부 네트워크에서 발생할 수 있는 공격을 탐지하고 대응할 수 있는 기술을 제공하고 있습니다.

자동차에 이러한 솔루션을 적용하기 위해서는 자동차나 전자제어장치의 설계 단계에서부터 사이버보안을 고려하여야 합니다. "Security by Design"의 개념은, 제품의 설계 단계에서부터 보안을 고려하여 제품에 내재화하는 것을 의미합니다. 아우토크립트는 자동차 제조사나 부품사들이 제품에 사이버보안을 적용할 수 있도록 전문적인 컨설팅 서비스를 제공하여 "Security by Design"을 확보할 수 있도록 도와드리고 있습니다.

보안 기술을 적용하여 제품의 구현이 완료된 후에는 사이버보안의 수

준이 설계와 계획에 부합하는지에 대하여 검증 및 타당성 확인(V&V; Verification and Validation)을 전문가 서비스로 제공합니다. V&V 전문가 서비스에는 사이버보안 수준 평가를 포함하여, 세부적으로는 ISO21434 표준이 정의하는 기능 테스트(Functional Test), 취약점 검토(Vulnerability Scan), 퍼징 테스트(Fuzzing Test), 침투 테스트(Penetration Test)를 제공하고 있습니다.

신규 개발된 차량에 대해 형식승인 제도(VTA; Vehicle Type Approval)를 시행하는 유럽 등의 국가에 자동차를 수출하기 위해서는, 사이버보안 V&V가 완료된 차량에 대해서도 사이버보안 형식승인을 인증기관(Approval Authority)으로부터 획득하여야 합니다. 아우토크립트는 유럽의 사이버보안 형식승인 인증기관들 중의 하나인 RDW가 인증한 평가기관(Technical Service, TS)으로 지정되었습니다. 이는 아시아-태평양에서 최초 사례입니다. 아우토크립트는 RDW의 공인 TS 기관으로서 자동차의 형식승인을 위한 사이버보안 심사를 제공하고 있습니다."

전 세계가 인정하는 사이버보안 '유니콘 기업을 꿈꾼다.'

오늘 '커넥티드카 사이버보안'이라는 주제로 진행된 아우토크립트와의 인터뷰는 매우 흥미로웠다. 끝으로, 아우토크립트의 경쟁력, 성과, 그리고 향후 계획에 대해 물어봤다.

"아우토크립트는 2015년에 국내 최초로 자동차 사이버보안 기술을 연구개발하는 전문 연구소를 설립하고, 국내 최초로 자동차 사이버보안 솔루션을 출시했던 기술력을 토대로, 2019년 8월 분사하였습니다. 그리고, 5년의 세월이 흘렀습니다. 아우토크립트는 현재 약 300명의 인력이 자동차 사이버보안 기술을 연구개발하여 제품과 솔루션을 고객사에 제공할 뿐만 아니라, 사이버보안 전문가 서비스를 제공하고 있습니다.

아우토크립트는 2020년부터 자동차 V2X 사이버보안 분야의 "Global Top 5" 기업으로 인정받고 있습니다. UNR 155와 UNR 156이 2020년에 공표된 이후에, 전 세계 자동차 제조사를 중심으로 사이버보안 대응 준비가 시작되었습니다. 아우토크립트는 국내뿐만 아니라 해외의 자동차 제조사와 부품사의 사이버보안 대응을 지원하고 관련 솔루션을 제공해 오고 있습니다. 현재는 자동차 사이버보안 분야의 "Global Top 5"로 인정받고 있습니다.

아우토크립트는 자동차 사이버보안을 넘어 교통과 모빌리티 전반에서 국제 사회에 이바지하고자 합니다. 이를 위해 2021년에 OECD의 ITF(International Transport Forum)에 가입하였고, ITF의 CPB(Corporate Partnership Board) 멤버로서 국내의 현대자동차, 카카오모빌리티와 함께 활동하고 있습니다. 아우토크립트는 자동차 사이버보안 전문기업으로서는 최초로 ITF의 CPB에 가입하였으며, 국제 사회의 교통 현안을 함께 해결해 나가는 한편, 한국기업의 위상을 높이기 위해 노력하고 있습니다. 이 활동을 통해서 글로벌 자동차 기업들과 많은 협력을 추진하고 있습니다.

자동차 분야는 자동차 제조사와 부품사들이 국경에 연연하지 않고 협업하며 새로운 기술들을 계속 내놓고 있습니다. 아우토크립트도 사이버보안을 중심으로 국내뿐만 아니라 해외의 자동차 제조사나 부품사들과 협력하고 있습니다. 2023년 6월에, 아우토크립트는 중소벤처기업부가 선정한 '예비 유니콘 기업'이 되었습니다. 앞으로 글로벌 협력을 통해, '예비 유니콘'이 아니라, 진정한 '유니콘 기업'이 되는 것이 향후 목표입니다."

오늘 인터뷰가 진행된 여의도 아우토크립트 본사 1층은 단순한 미팅 장소가 아니라, 간단하게 솔루션을 체험할 수 있는 독특한 공간으로 꾸며져 있었다. 이런 내부 분위기에서 아우토크립트의 자신감과 기술력에 대한 확신을 느낄 수 있었다. 뉴스기사 등을 통해 알게 된 아우토크립트를 직접 만나보니 그들의 열정과 실력을 실감할 수 있었던 귀중한 시간이었다.

앞으로 자동차 사이버보안 시장 내 진정한 '유니콘 기업'을 꿈꾸는 심상규 부사장과 아우토크립트의 원대한 꿈, 그리고 목표가 꼭 이루어지길 기원하며, 바쁜 일정 중에도 인터뷰에 응해준 아우토크립트 심상규 부사장께 감사의 말씀을 전한다.

방혁준
쿤텍(주) 대표이사

Interview

자동차를 넘어 모빌리티 융합보안을 책임진다.

COONTEC 쿤텍(주)

자동차뿐만 아니라 디지털 전환의 가속화로 다양한 산업 분야에서 소프트웨어가 담당하는 비중이 커지면서 소프트웨어 공급망 보안의 중요성 역시 강조되고 있다. 하지만 오픈소스 소프트웨어 도입의 확대 및 소프트웨어 구성요소 공급 분업화로 인한 책임 부재, 고도화되고 있는 공급망 보안 위협 등으로 인한 다양한 문제점도 함께 발생하고 있다.

이제 소프트웨어의 영역은 자동차를 비롯한 다양한 사업군에서 사용되고 있으며 특히, 공급망 보안의 중요성이 점차 강조되고 있다. 국내외 지침에 따라 소프트웨어 보안을 관리하는 것이 필수적이나 기업이 자체적으로 SBOM(Software Bill Of Materials)을 분석하고 이를 토대로 공급망 보안을 관리하는 것은 현실적으로 한계가 있다. SBOM 분석을 기반으로 보안 구성요소에 대한 가시성을 확보하고 취약점까지 통합적으로 관리할 수 있는 솔루션을 개발·공급하고 있는 국내 대표 '사이버 융합보안 솔루션 전문기업' 쿤텍(주)이 주목받고 있다.

모빌리티 인사이트에서는 '융합보안 솔루션 전문기업'인 쿤텍(주) 방혁준 대표이사와의 인터뷰를 통해 현장의 생생한 목소리를 담아봤다.

커넥티드카 사이버보안 그 중심은 결국 '소프트웨어'

이번 10월호의 주제인 '커넥티드카 사이버보안 실태 및 방향성'에서 가장 중요한 핵심은 바로 커넥티드카다. 이는 당연한 말일 수 있지만, 커넥티드카를 지배하는 요소를 소프트웨어 중심으로 바라보면 이야기는 달라진다. '자동차 중심에서 소프트웨어를 볼 것인가, 소프트웨어 중심에서 자동차를 볼 것인가?'라는 시각 차이에 따라 그 내용과 관점이 달라질 수 있기 때문이다.

이번 인터뷰에서는 국내 대표 사이버 융합보안 솔루션 전문기업 쿤텍의 방혁준 대표를 만나, 소프트웨어 중심의 사이버보안 산업과 커넥티드카 사이버보안의 중요성에 대해 이야기를 나눠봤다.

현재 쿤텍이 진행하는 소프트웨어 융합보안 사업의 관점에서, 커넥티드카 사이버보안에 대한 기본적인 생각과 의견을 물어봤다.

"최근 자동차 산업은 하드웨어에서 소프트웨어 중심의 환경으로 급격하게 전환되고 있습니다. 과거에는 차량 성능과 안정성이 주로 하드웨어에 의해 결정되었으나, 이제는 소프트웨어가 차량의 핵심 기능을 결정 짓는 중요한 요소가 되었습니다. 이 같은 변화는 SDV(Software-Defined Vehicle)라는 개념으로 대표되며, 차량 내 기능 대부분이 소프트웨어에 의해 정의되고 제어되고 있습니다.

이러한 변화는 자동차 산업이 스마트폰 산업과 유사한 패턴을 보이게 만들고 있습니다. 스마트폰의 경우, 하드웨어가 출시되면 그 이후의 기능 개선이나 버그 수정은 주로 소프트웨어 업데이트를 통해 이루어집니다. 이는 고객 피드백을 빠르게 반영하고, 사용자의 요구에 따라 새로운 기능을 신속히 도입할 수 있는 유연성을 제공합니다. 자동차 역시 마찬가지로, 소프트웨어 업데이트를 통해 새로운 기능을 추가하거나, 보안 취약점을 해결할 수 있는 시스템으로 변화하고 있습니다. 특히, 커넥티드카는 외부 네트워크와 연결되어 지속적인 소프트웨어 업데이트가 가능하기에, 자동차 제조사들은 빠르게 변화하는 시장 요구와 고객 피드백에 발맞춰야 합니다. 소프트웨어 중심 차량에서는 고객의 피드백을 신속하게 반영하는 것이 경쟁력의 핵심 요소가 되고 있습니다. 자동차가 단순한 운송 수단에서 벗어나 '이동하는 컴퓨터'로 진화하면서, 소프트웨어의 역할은 더욱 중요해지고 있으며, 이를 통해 차량의 성능을 개선하고, 사용자의 경험을 혁신하는 것이 가능해졌습니다."

커넥티드카 사이버보안에 대해 이야기를 나누는 동안, 방혁준 대표는 소프트웨어 정보보안 전반과 그와 연관된 자동차 사이버보안의 중요성을 강조했다. 이에 자동차 산업 내에서 보안의 중요성에 대해 보다 구체적인 설명을 부탁했다.

"자동차 산업에서의 사이버보안은 과거와 비교해 큰 변화를 겪고 있습니다. 과거에는 차량 보안이 주로 물리적 요소와 하드웨어 결함에 대한 문제 해결에 집중되었지만, 최근에는 SDV(소프트웨어 정의 차량)과 커넥티드카 기술의 발전으로 인해 보안 위협의 양상도 변화하고 있습니다. 이처럼 소프트웨어의 의존도가 높아진 만큼, 하나의 보안 취약점이 전체 시스템에 영향을 미칠 수 있고, 원격 해킹이나 악성 소프트웨어가 차량을 마비시킬 가능성이 커졌습니다. 커넥티드카의 확산 역시 보안에 중요한 변화를 불러왔습니다. 커넥티드카의 연결성은 편리함을 제공하는 동시에 해커들이 접근할 수 있는 공격 표면을 확장할 수 있다는 점에서 위험요소도 안고 있습니다. 차량 내부의 소프트웨어와 하드웨어가 외부 클라우드나 스마트폰, 인프라와 연동되면서, 네트워크를 통한 원격 해킹이나 데이터 탈취와 같은 위협에 실시간으로 노출될 수 있기 때문입니다. 커넥티드카는 이러한 이유로 이전보다 훨씬 더 복잡하고 광범위한 보안 체계가 있어야 하는 상황입니다. 또한, 실시간 소프트웨어 업데이트는 SDV와 커넥티드카의 중요한 기능 중 하나로 자리 잡았습니다. 소프트웨어 업데이트를 통해 차량의 성능을 개선하고 새로운 기능을 추가할 수 있지만, 동시에 잘못된 업데이트로 인해 보안 취약점이 생기거나 악성 코드가 포함될 위험도 함께 존재하는 것이 사실입니다. 따라서, 실시간 보안 패치와 모니터링이 필수적이라고 볼 수 있습니다".

앞으로 자동차 사이버보안의 방향성은 어떻게 될 것으로 생각하는지 물어봤다.

"오늘날의 자동차 보안은 과거와 달리 훨씬 복잡한 네트워크와 소프트웨어 생태계를 다루고 있습니다. 이제는 자동차 제조사뿐만 아니라 부품 공급업체와 소프트웨어 제공업체까지 모두 보안 위협에 대응해야 합니다. SDV와 커넥티드카 시대에는 물리적 시스템뿐만 아니라 소프트웨어와 네트워크까지 포함하는 종합적인 보안 체계를 구축하는 것이 필수적입니다. 자동차 사이버보안은 이제 그 어느 때보다 중요한 과제가 되었습니다."

방혁준 대표는 커넥티드카 사이버보안을 소프트웨어 중심으로 바라보면서, 앞으로 자동차 산업 전반에서 사이버보안의 중요성은 더욱 커질 것이라고 강조했다.

쿤텍의 대표 솔루션 AEGIS(이지스) & FastVLabs(패스트브이랩스)

지금까지 소프트웨어 정보보안과 커넥티드카 사이버보안에 대해 많은 이야기를 나눴다. 이러한 시장 상황 속에서 쿤텍의 핵심 솔루션인 AEGIS(이지스)와 FastVLabs(패스트브이랩스)에 대한 구체적인 내용이 궁금하다.

AEGIS (SBOM 공급망 보안의 핵심 기술)

"SBOM(Software Bill of Materials)은 차량의 소프트웨어 구성요소를 추적하고 관리하는 데 필수적인 역할을 한다고 말씀드렸습니다. 차량의 소프트웨어가 점점 더 복잡해지고 제3자 소프트웨어와 오픈소스 소프트웨어의 사용이 증가함에 따라, 소프트웨어의 보안 상태를 지속해서 관리하고, 취약점을 파악하는 것이 매우 중요해지고 있기 때문입니다. 특히, 공급망 보안 측면에서 SBOM은 차량의 전체 소프트웨어 생태계를 투명하게 관리할 수 있는 중요한 도구입니다. SBOM 관리의 필요성을 충족시키기 위해 쿤텍에서 자체 개발한 솔루션인 AEGIS(이지스)는 SBOM 추출, 취약점 분석, 그리고 실시간 CVE(Critical Vulnerability Exposure) 모니터링을 제공하고 있습니다. ISO 21434에서는 소프트웨어 보안 검증 기준을 최종 산출물에 맞춰 요구하고 있는데, 소프트웨어의 최종 산출물이 바로 바이너리이기 때문에, 바이너리 분석을 통한 SBOM 관리는 매우 중요한 요소입니다. 또한, AEGIS는 차량에 최종적으로 탑재될 소프트웨어의 바이너리 파일 분석을 통해 SBOM을 자동으로 추출하여 생성하고 체계적으로 관리할 수 있습니다. 이를 통해 소프트웨어의 출처, 버전, 라이선스 상태를 명확하게 파악할 수 있으며, 보안 취약점이 발생했을 때 신속하게 대응할 수 있도록 지원하고 있습니다. 또한, AEGIS는 SBOM 생성 및 관리, 취약점 분석, 실시간 모니터링을 통해 공급망 보안을 강화하는 강력한 도구입니다. 특히 커넥티드카와 자율주행차와 같은 복잡한 소프트웨어 환경에서도 효과적으로 작동하며, 자동차 제조사와 부품 공급업체가 신속하게 보안 위협에 대응할 수 있도록 지원하고 있습니다. AEGIS는 자동차 산업의 요구에 맞는 보안 관리 솔루션으로, 차량 시스템의 안전성을 강화하는 데 중요한 역할을 하고 있다고 자부합니다."

FastVLabs (전가상화를 통한 SW 개발 가속화 및 지속적 보안 검증)

"쿤텍의 FastVLabs(패스트브이랩스)는 HW 전가상화(Full Virtualization) 기술을 기반으로 한 에뮬레이터로, 실제 하드웨어와 같은 환경을 가상으로 제공하여 소프트웨어 검증 환경을 구축하는 데 중점을 둔 솔루션입니다. Level 4 가상화 기술을 적용한 FastVLabs는 차량 소프트웨어

샤오미 전기차 (출처: 샤오미 홈페이지)

와 하드웨어의 상호작용을 완벽하게 가상화하여 물리적 하드웨어 없이도 차량 시스템에서 발생할 수 있는 잠재적인 보안 취약점을 테스트할 수 있는 환경을 제공합니다. 특히, FastVLabs는 국내 최초로 상용화된 Level 4 전가상화 제품이라는 점에서, 자동차 보안 시장에서 선도적인 기술력을 자랑하고 있습니다. ISO 21434에서는 보안 요구사항으로 Penetration 테스트, Fault Injection 등의 다양한 보안 테스트 방법론을 제시하고 있는데, 가상화된 하드웨어 환경에서는 하드웨어 내부의 레지스터와 메모리에 쉽게 접근하여 이러한 보안 테스트를 쉽게 수행할 수 있고 또한, 대량의 테스트 케이스 Script를 통해 자동화할 수 있어 빠른 테스트도 가능합니다. 2024년 초 일본에서 열린 AOC 2024에서는 하드웨어 가상화를 통한 검증과 개발 방법론에 대해 논의가 이루어졌으며, 여기서 Level 3 이상의 가상화가 효과적이라는 의견이 제시되기도 했습니다.

FastVLabs는 차량의 ECU(전자 제어 장치)와 같은 주요 하드웨어 구성요소를 가상화 하여, 실제 하드웨어 환경 없이 다양한 방식의 SW 테스트를 빠르고 손쉽게 수행할 수 있도록 합니다. 특히, SDV에서는 고객 피드백을 신속하게 반영하는 것이 경쟁력의 핵심이지만, 기존 개발 방법으로는 빠른 SW 개발과 대응이 어렵습니다. 가상화는 SW 개발자들이 하드웨어에 쉽게 접근할 수 있게 하여 SW 개발의 효율성을 높일 수 있으며, FastVLabs는 이러한 환경을 제공하여 SW 개발의 속도를 크게 향상할 수 있습니다.

보안 테스트의 중요성은 차량 소프트웨어의 지속적인 업데이트와 관련이 깊은데 소프트웨어가 배포된 이후에도 새로운 기능이 추가되거나 보안 패치가 적용되면서, 이 과정에서 새로운 보안 취약점이 발생할 가능성이 큽니다.

FastVLabs는 이러한 업데이트가 진행되기 전, 가상화된 환경에서 소프트웨어의 보안성을 검증할 수 있는 환경을 제공하여, 실제 배포 전에 잠재적인 보안 문제를 사전에 차단할 수 있도록 해줍니다. 또한, SW 보안 이슈는 기능 안전과 달리 지속해서 새로운 문제들이 발생하기에, 지속적인 테스트와 선제적인 대응이 필수적입니다. FastVLabs는 가상화 환경을 통해 24시간 365일 보안 테스트를 수행할 수 있으며, 이를 통해 SW 개발의 효율성과 보안성을 동시에 높일 수 있다는 장점이 있습니다.

FastVLabs는 보안 전문가들이 차량 시스템에 대한 다양한 보안 시나리오를 가상 환경에서 검증할 수 있도록 돕고 있으며, 자동차 사이버보안을 위한 핵심 도구로 자리 잡고 있습니다. 이를 통해 차량 제조사들은 커넥티드카와 자율주행차 시대에서 증가하는 보안 위협에 사전에 대응할 수 있게 될 것으로 기대합니다."

쿤텍의 핵심 솔루션인 AEGIS(이지스)와 FastVLabs(패스트브이랩스)에 관한 기본적인 내용은 충분히 들어봤다. 그렇다면 현재 개발 현황과 서비스는 어떻게 진행되고 있는지를 물어봤다.

"쿤텍의 AEGIS와 FastVLabs는 이미 상용화되어 자동차, 철도, 항공 우주 등 다양한 산업에서 활발히 사용되고 있습니다. 두 솔루션 모두 시장에서의 성공적인 적용을 통해 레퍼런스를 확보했으며, 특히 자동차 산업에서 그 가치를 입증하고 있습니다.

AEGIS는 현대자동차에서 사용되고 있으며, SBOM(Software Bill of Materials) 기반으로 차량 소프트웨어 구성요소의 취약점을 실시간으로 모니터링하고 관리하는 중요한 역할을 하고 있습니다. AEGIS는 소프트웨어 업데이트와 오픈소스 사용으로 인한 오픈소스 라이선스 및 보안 리스크를 줄이고, 각 구성요소의 취약점을 신속하게 파악하여 대응할 수 있도록 지원하고 있습니다. 이를 통해 현대자동차는 차량의 보안성을 지속해서 유지하고 강화할 수 있었으며, 이는 AEGIS의 실질적인 성능을 입증하는 중요한 사례로 자리 잡고 있습니다.

쿤텍은 FastVLabs에 적용된 HW가상화 기술을 통해 현대자동차의 ECU(전자 제어 장치) 가상화를 구축하였으며, 물리적 하드웨어 없이도 가상 환경에서 보안 및 성능 테스트를 수행할 수 있는 환경을 제공하고 있습니다. 이를 통해 차량 내 전자 제어 시스템의 상호작용을 안전하게 검증할 수 있었으며, 보안 취약점을 사전에 차단할 수 있는 가상화 환경을 제공함으로써 차량 제조사에 큰 신뢰를 주었다고 생각합니다. FastVLabs는 Level 4 전가상화 기술을 기반으로, 하드웨어와 같은 환경에서 실시간으로 테스트할 수 있기에, ECU를 포함한 다양한 차량 시스템에서 중요한 역할을 하고 있습니다.

이외에도 FastVLabs는 철도와 항공 우주 산업에도 성공적으로 적용되고 있는데, 이러한 적용 사례들은 FastVLabs가 단순히 자동차 산업에 국한되지 않고, 다양한 산업에서 활용 가능성이 크다는 점을 증명하고 있습니다.

쿤텍의 AEGIS와 FastVLabs는 자동차 시장을 비롯한 다양한 산업에서 지속해서 보안성과 신뢰성을 입증하며, 더 나아가 그 적용 범위를 확장하고 있습니다. 이를 통해 쿤텍은 각 산업 분야에서 중요한 파트너로 자리 잡고 있으며, 앞으로도 보안이 중요한 다양한 산업에서 그 가치를 발휘할 수 있다고 확신합니다."

자동차 사이버보안 시장 이제 쿤텍이 '중심이 된다.'

오늘 '커넥티드카 사이버보안'을 주제로 쿤텍의 방혁준 대표와의 인터뷰는 매우 흥미로웠다. 그의 열정과 쿤텍의 목표를 향한 노력이 눈앞에 그려지는 듯했다. 마지막으로, 쿤텍의 경쟁력, 성과, 그리고 향후 계획에 대해 물어봤다.

"쿤텍은 국내 시장 점유율을 확대하고, 기술 고도화를 통해 해외 시장 진출을 목표로 하고 있습니다. AEGIS와 FastVLabs는 이미 자동차, 철도, 항공 우주 산업에서 성능과 신뢰성을 입증했으며, 이를 기반으로 국내 시장에서의 영향력을 더욱 강화할 계획입니다. 특히, 자동차 사이버보안이 점점 더 중요한 화두로 떠오르면서, 쿤텍은 다양한 산업의 보안 요구를 충족하는 데 집중하고 있습니다.

쿤텍은 주요 자동차 제조사 및 부품 공급업체와의 협력을 더욱 강화하여 시장 점유율을 높이는 한편, 철도와 항공 우주 같은 기존 레퍼런스를 활용해 다양한 산업에 솔루션을 제공함으로써 국내 시장에서의 리더십을 강화할 것입니다.

또한, 기술 고도화를 통해 더 정교하고 효율적인 보안 솔루션을 제공할 예정입니다. AEGIS는 더 빠르고 정밀한 취약점 분석 기능을, FastVLabs는 가상화 성능 최적화를 통해 더 많은 시스템에서 활용될 수 있도록 발

전시킬 계획입니다. 이를 통해 쿤텍은 보안 솔루션의 기술 지배력을 지속해서 강화하고, 고객들에게 최고의 가치를 제공하고자 노력하고 있습니다. 국내 시장에서 쌓은 경험과 레퍼런스를 바탕으로, 쿤텍은 글로벌 시장으로의 진출도 계획하고 있습니다. 특히, 자동차 산업에서의 글로벌 사이버보안 요구가 높아짐에 따라, 쿤텍은 SBOM 기반 보안 솔루션과 전가상화 기술을 앞세워 해외 자동차 제조사 및 관련 산업에 진출할 예정입니다. 이를 위해 현지 파트너와의 협력과 기술 맞춤화를 통해 글로벌 시장에서의 경쟁력을 강화할 계획입니다.

쿤텍은 ISO 21434와 같은 글로벌 보안 및 안전성 표준을 꾸준히 준수하며, 산업별 보안 요구에 맞는 솔루션을 제공할 것입니다. 이를 통해 고객들이 다양한 규제와 요구사항을 충족하도록 돕는 동시에, 쿤텍은 혁신적인 보안 기술을 개발하여 미래의 사이버 위협에 선제적으로 대응할 역량을 강화할 것입니다.

현재 자동차, 철도, 항공 우주 산업에서 성공적인 레퍼런스를 보유한 쿤텍은 에너지, 스마트시티, 의료 기기와 같은 새로운 산업 분야로 솔루션을 확장할 계획입니다. IoT와 클라우드 기술의 발전에 따라 보안 위협이 다양해지고 있는 만큼, 쿤텍은 신흥 산업에서의 보안 문제 해결에도 이바지할 수 있는 솔루션을 제공할 것입니다."

이번 인터뷰를 통해 만난 쿤텍은 자동차뿐만 아니라 다양한 산업에서 보안 솔루션을 제공하는 기업이라는 점에서 남다른 인상을 준다. 자동차 사이버보안 시장에서 국내뿐만 아니라 세계를 향해 도전하는 그의 열정과 쿤텍의 미래 목표가 꼭 달성하길 기원하며, 바쁜 일정 중에도 인터뷰에 응해주신 방혁준 대표께 감사의 말씀을 전한다.

미국의 중국산 커넥티드카 사이버보안 규제 영향

장홍창 한국자동차연구원 정책전략실 선임연구원

중국자동차연구개발유한공사(CATARC)
지능형 커넥티드카와 자율주행차량 테스트 트랙
출처 : CATARC

KATECH INSIGHT

◆ 미국은 중국산 커넥티드카 기술 사용을 규제하는 사전규제 도입안을 공고하였으며, 향후 규제 대상 범위를 확대 해석 시 공급망 변경이 필요하여 자동차 업계에 혼란을 유발할 가능성 제기

◆ 동시에 UNR 155(車 사이버보안 UN 규제)를 통한 글로벌 사이버보안 요구사항이 확대 중이나, 국내 중소 부품기업의 준비가 부족한 상황으로 적극적인 인력양성·컨설팅·평가 장비 등 지원 필요

현재의 車는 ADAS·커넥티드 기능의 구현을 위해 지속해서 내외부 연결성이 확대되고 있으며, 이에 따라 주요 브랜드 차량 보안 문제 증가와 동시에 車 사이버보안 산업이 고성장 중

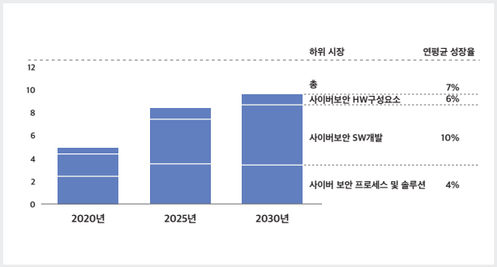
• 최근 판매 차량의 ADAS·커넥티드 기능 탑재로 차량 내외부 통신 범위가 확대되어, 車 사이버 공격은 차량 내에만 국한되지 않고 통신 기능이 연결된 클라우드·네트워크 전체에 피해 확산 가능

• 이미 대다수 글로벌 자동차 OEM社에서 사이버보안 문제가 발생하고 있으며, 이를 방지하기 위한 車 사이버보안 산업이 36.6억달러(2023년)→97~118억달러(2030년) 규모로 고성장 전망

- 테슬라·폭스바겐·BMW·닛산·미쓰비시 등 주요 OEM社 다수에서 해킹 혹은 보안 취약 사례가 보도되었고, 백도어(인증되지 않은 사용자가 몰래 설치한 통신 연결 기능) 문제의 경우 검출이 매우 어려운 상황

- Precedence Research社는 車 사이버보안 산업이 36.6억$(2023년)→118억$(2030년)로 성장할 것으로 추정하였으며, McKinsey社는 49억$(2020년)→97억$(2030년)로 시장이 성장하고 특히 보안 SW의 비중 증가 예상

[자동차 사이버보안 산업 규모 및 구성]



출처: McKinsey

미국은 中 커넥티드카 기술이 국가안보를 위협할 것으로 보고 사전규제 도입안을 공고하였고, 향후 규제 범위에 따라 車 산업 전체의 공급망 변경 조치 필요성 제기

• 美 상무부는 우려국 커넥티드카 기술 사용을 규제하는 잠정규정을 알리고 적용 범위를 결정하기 위한 규칙제정 사전통지(ANPRM)를 개시하여 우방국 및 관련 업계 의견을 수렴

- 바이든 美 대통령은 우려국*이 미국 내 커넥티드카를 통한 데이터 수집 및 인프라 교란 등의 활동이 국가안보에 위협이 될 것으로 보고, 상무부에 커넥티드카 산업 현황을 조사하고 조치 요청(2024. 2. 29)

* 우려국에 중국, 러시아, 이란, 쿠바, 북한, 베네수엘라(니콜라스 마두로 정부)를 포함

- 미국 상무부는 커넥티드카에 필수적인 정보통신 부품 관련 설계·개발·제조·공급하는 기업 중 우려 국가의 소유·통제·관할에 있는 기업의 기술 사용을 규정하는 사전규제 도입안 공고(ANPRM) 개시(2024. 3. 1)

- 현재 ANPRM 기술 정의에서의 커넥티드카는 사실상 현재 판매되는 차량 대부분을 지칭하고 있고, 기술의 범위 또한 불특정하여 향후 데이터를 생성하는 센서·소재·기타 부분품까지 포함할 가능성 존재

- ANPRM에는 커넥티드카 정의, 공급망, 데이터 수집 등의 보안 위협 요인과 관련된 질의가 포함되어 있으며, 배경과 질의 내용을 분석해 볼 때 과거 중국 화웨이 제재 형식과 일부 유사하게 진행 예상

- 美 상무부는 중국산 커넥티드카 SW 및 통신 모듈 사용 제한 방안을 '24.8월에 발표할 것으로 공개

• 美 상무부의 커넥티드카 사전규제 도입안 공고에 대한 총 57개 공개의견이 등록되었으며, 미국 기관들은 규제의 취지에 동의하는 반면 車 업계에서는 제재 대상 부품 범위 확대에 대한 우려 표명

* 전체 의견 중 공개의견 57개(비영리기관 30개, 부품·관련 기업 13개, 익명·개인 7개, 완성차社 기업 4개, 정부 3개)가 등록되었고, 이 중 美 기관 의견이 가장 많으며 한국을 포함한 EU·독일·네덜란드·호주 등 우방국 의견 등재

- 포드는 규제의 취지에 강한 동의를 하였으나 규제 범위 제품의 공급망 변경에 따른 비용 문제를 지적하였고, 폭스바겐은 공급망 변경 비용 문제 우려 및 규제 관련 업계 지원 프로그램 제안

- NXP는 사이버보안 문제를 기존 국제 표준을 통해 해소할 수 있음을 지적하고 규제 범위를 부품에 확장 시 개발 비용 상승을 우려하였으며, 웨이모는 업계에서 적응할 시간과 혼란을 방지할 임시 규칙제정 권장

글로벌 주요국은 UNR 155를 중심으로 완성차·부품기업에 사이버보안 요구사항을 확대 중

• 해외 주요 국가들은 UNR 155*를 채택하여 車·부품 기업에 대한 최소 요구사항을 확대하고, 글로벌 車 기업은 ISO/SAE 21434에 기반하여 확장한 범위에서 사이버보안 강화 노력 중

* UNECE(유럽경제위원회) 산하 자동차 기준 국제조화 회의 WP.29는 자동차 사이버보안 관련 법규인 UNR(UNECE Regulation) 155를 제정하여 사이버보안 관리체계(CSMS) 및 형식승인 의무화

- UNECE WP.29 회원·채택 국가 약 60개국은 신차 판매 시 CSMS 인증을 의무화 및 보안대책을 요구하고 있으며, 국내에서는 국토교통부가 車 사이버보안 가이드라인 및 자동차관리법을 개정하여 사이버보안 강화 중

* EU는 2024년 7월부터 유럽 지역 내 출시되는 모든 차량에 대하여 CSMS 인증을 취득하고 형식승인 요구

국제적 車 사이버보안 요구사항 급증에 더하여 미국은 중국산 커넥티드카 규제로 자국 중심의 車 산업으로 재편하고자 하지만, 국내 중소 車 부품기업의 대응에 보완 필요

• 미국은 커넥티드카 사이버보안을 계기로 차량용 이차전지 산업과 유사하게 자국 산업을 보호하고 중국 기업을 견제하여 글로벌 헤게모니를 가져오려는 전략으로 해석

• 국내 주요 OEM·Tier1 기업은 글로벌 사이버보안 규제 대응이 가능하지만, 이외 중소 Tier1·2 이하 기업 및 미래차 부품 전환 기업은 사이버보안의 중요성 인지 부족과 동시에 대응 여건 부족

- 글로벌 사이버보안 요구사항 증가에 따라 국내 Tier1 이하 부품기업에도 CSMS 인증을 위한 보안 목표 도출 방법론(TARA), 프로세스 정립, SW 문서화 체계(SBOM) 등 다양한 방법론 도입이 요구

- 주요 OEM·Tier1 기업은 글로벌 규제 대응하기 위한 역량을 갖추고 있으나, 대다수 중소 Tier1·2 이하 기업은 글로벌 기준의 최소 요구사항만을 충족하거나 대응 역량이 충분하지 않은 상황

* 완성차 기업 중 독일 3社가 높은 사이버보안 기술 수준과 규제 대응 역량을 보유한 것으로 평가되고 있으며, 글로벌 차량용 반도체 사이버보안 기술은 NXP, 인피니언, 마이크론 등이 사이버보안에 적극 대응 중

미국의 중국산 사이버보안 기술 규제를 국내 자동차 부품 수출 기회로 연결하고, 국내 車 부품기업의 사이버보안 대응 역량 강화를 위해 적극적 기술 컨설팅 및 인력양성 요구

• 중국의 車 부품기업 외에도 중국의 기술 및 부품 등을 활용하는 글로벌 자동차 부품기업이 영향을 받을 것으로 예상이며, 금번 제재 대상이 되는 제품을 중심으로 우리나라 기업의 확장 필요

* 일례로 車 반도체 등을 판매하는 대만 팹리스 기업은 중국 내 공장에서 위탁생산하여 제재 대상에 포함 추정

• 국내에 車 사이버보안 기술이 부족함에 따라 전주기 대상 사이버보안 기술 개발이 요구되고, 자체 대응이 어려운 자동차 부품 중소기업을 대상으로 보안 컨설팅 및 평가 장비 지원 요구

- 글로벌 자동차 사이버보안 요구사항에 맞춰 국내 기술 공백을 진단하고 기술 고도화를 추진해야 하며, 부품기업은 UNR 155·ISO21434 기반 사이버보안 관리체계(CSMS) 및 보안 강화 방안 마련 필요

- 내수 비중이 높은 국내 대다수 부품社은 사이버보안에 대한 중요성과 경각심을 가지지 못하고 있어 공공부문에서 미래차 부품을 양산하거나 사업화를 진행 중인 기업을 대상으로 컨설팅, 교육, 평가 장비 지원 요구

• 현재 국내 사이버보안 인력은 주요 OEM·Tier1 기업을 중심으로 집중되어 있어, 부족한 사이버보안 SW 개발 인력을 중심으로 중소 Tier2 이하 기업까지 인력이 공급될 수 있도록 인력양성 필요

- 국내 사이버보안 기술은 IT 산업을 중심으로 경쟁력을 갖추고 있으나 車 산업으로 확산되지 못하는 상황

- 현재 국내 車 사이버보안 전문인력은 주요 OEM·Tier1 기업을 중심으로 집중되어 있고 전체가 대략 천명 이상*으로 추산됨에 따라 Tier2 이하로도 인력이 공급될 수 있도록 추가 인력양성 요구

* 직접적으로 자동차 사이버보안 기술을 구현할 수 있는 인력 기준으로 자체 추정

- 글로벌 요구수준을 만족하는 사이버보안 적용을 위해서 기존 개발 자원 대비 120~130% 투입이 필요하며, 다양한 역할의 사이버보안 인력*이 필요하고 특히 사이버보안 SW 전문인력이 수요가 높은 상황

* 차량 사이버보안 관련 직무는 제어기 보안 기능 설계, 차량 보안 시스템·인프라 개발, 프로세스 엔지니어링, 보안 취약점 분석, 보안 평가·심사 등이 필요(출처: 현대모비스)

- 인력양성 시 단발성 교육이 아닌 부품기업에서 실질적인 보안 전문가를 분야별로 양성할 수 있도록 전문가 교육과 기업 컨설팅 지원을 병행하여 실무 전문가 양성과 글로벌 사이버보안 규제 대응 지원 필요

[글로벌 차량 사이버보안 규정 및 표준 비교]

기업명	구분	협력 내용
UNR 155	약 60개국 (미국, EU, 영국, 한국, 일본 등)	• 사이버보안 형식승인 및 CSMS 인증 의무 규정(2022년 7월) • 조직 및 차량 수준 요구사항을 정의
GB & GB/T	중국	• 차량 사이버보안 관련 기술적 요구사항 규정 • 중국은 100개 이상의 커넥티드카 관련 표준을 적용 예정
ISO/SAE 21434	(국제 표준)	• 차량 엔지니어링 관련 첨단 사이버보안 국제 표준 • 사이버보안 관리 입증을 위한 가이드라인 및 결과물 생성 방법 제공 * UNR 155, GB & GB/T는 해당 표준을 참고하여 구성
NHTSA	미국	• 법적 구속력이 없는 자발적 자동차 산업 사이버보안 모범 실무 지침 • 차량 제조사 및 부품사가 해당 지침을 검토하여 적용하도록 권장

출처: Argus 자료 참고하여 저자 재작성

日 완성차 업계의 협력관계 변화

이호 한국자동차연구원 산업분석실 책임연구원

KATECH INSIGHT

◆ 과거 日 완성차 업계는 빠르게 성장하는 中 자동차 시장에서 확대 전략을 전개하며 성과를 창출한 바 있으나, 최근 수년간은 미래차 트렌드 대응 지연 등의 원인으로 점유율이 급속도로 하락하고 있음

◆ Honda·Nissan·Mitsubishi는 연합 형성을 통해 재도약을 시도하고 있는데, 연합 형성이 현실화되면 日 국내 경쟁 구도에는 상당 영향이 전망되나 글로벌 경쟁 구도에의 파급력은 불확실한 것으로 판단

2024년 3월 Honda·Nissan이 연합 형성 및 포괄적 협력 계획을 발표한 것에 이어, 2024년 8월 Mitsubishi가 동 연합에 합류할 계획임을 발표

• Honda·Nissan이 연합을 형성할 당시 Nissan이 대주주로 있는 Mitsubishi의 참여는 명시된 바 없었으나 이번 발표로 3社의 연합 형성 추진이 공식화되었음

- Mitsubishi는 2016년 Renault·Nissan 연합에 합류했으나 협력이 크게 활성화되지 못한 상태에서 2026년 이후 Nissan과의 지분 및 협력관계의 변화 가능성이 제기되면서 Honda·Nissan 연합에의 참여가 불투명한 상황이었음

* FY23년말 현재 Nissan(日産自動車株式会社)은 Mitsubishi(三菱自動車)의 지분 34.01%를 보유. 해당 지분은 2026년까지 매매 금지(ロックアップ) 조항이 걸려있는 것으로 알려져 있음

• 2024년 3월 연합 형성을 발표한 Honda·Nissan은 차세대 SDV 플랫폼 개발 등으로 협력 내용을 구체화했으며, 새롭게 연합에 참여하는 Mitsubishi는 Honda에 PHEV, 픽업트럭 등을 주문자상표부착생산(OEM) 방식으로 공급하는 방안 등을 고려하는 것으로 알려졌으나 구체적인 협력 내용은 미정

* 2024년 8월 Honda·Nissan 양사가 공식적으로 발표한 내용과 별개로 2024년 7월 Nikkei는 Honda·Nissan이 비용 절감을 위해 차량의 운영 시스템 등 SW 공용화 및 전기차 충전 인프라 부문에서의 협력을 논의 중임을 보도한 바 있음

과거 Honda·Nissan·Mitsubishi를 비롯한 일본계 완성차社는 성장하는 중국 시장에서 확장 전략을 전개하여 성과를 낸 바 있으나 최근 수년간은 미래차 트렌드 대응이 늦어지며 위상 약화

• 일본계 완성차社의 점유율은 `20년 정점을 형성한 이후 지속적으로 하락하는 추세를 보이고 있음

- 업체별로는 Nissan-Mitsubishi가 가장 이른 시기인 2020년부터 점유율이 하락하였으며, Honda는 2021년, Toyota계 완성차社 점유율은 2023년부터 빠르게 하락 중으로 각 사는 판매 부진에 따라 중국 내 생산을 축소하는 등 구조조정을 진행하고 있음

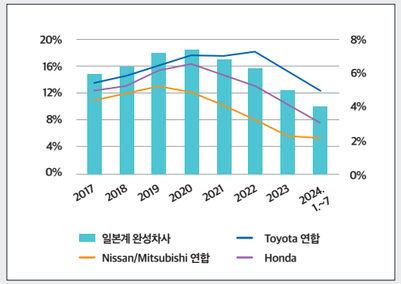
* Honda, Nissan은 판매 부진의 영향으로 현지 합작 공장의 생산량을 축소하였으며, Mitsubishi는 2023년 3월 중국 내 공장 운영을 중단하고, 2023년 10월 中 GAC(广汽集团)와의 합작투자에서 철수할 계획임을 발표

[Honda·Nissan의 전략적 파트너십 심화에 대한 양해각서 주요 내용]

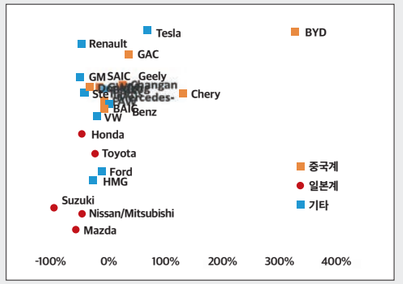
협력 분야	협력 내용
차세대 SDV 플랫폼	• 기초 요소기술 공동연구에 합의하여 연구를 시작했으며, 우선 1년간 기초연구를 완료하고 성과에 따라 양산 가능성도 검토
배터리	• 양사 간 규격 공통화, 상호 공급 등 협력 범위를 검토하며, 양사가 각각 공급 계획 중인 배터리를 상호 탑재할 수 있도록 셀·모듈 사양에 대한 중장기 공통화에 기본 합의 • Honda-LGES의 합작사 L-H Battery에서 생산되는 배터리를 `28년부터 북미서 Nissan에 탑재하는 방안 검토
전기구동시스템 (e-Axle)	• 차세대 전기차에 탑재되는 e-Axle의 사양을 중장기적으로 공통화하고, 이의 첫 단계로 모터 및 인버터를 공유하는 것에 합의
상호 보완	• 가솔린 및 전기차에서 지역별 판매 모델을 중장기적 관점에서 상호보완하도록 조정 검토
에너지·자원순환 (日 국내)	• 전기차 충전, 배터리 등을 활용한 서비스 및 자원순환 영역에서 협력 가능성 검토

출처: Honda·Nissan 발표(2024년 8월)

[일본계 완성차社의 중국 점유율 변화]



[NEV 판매비중과 중국 내 점유율 변화]



주1) 좌, 우 그래프 모두 중국 기업과의 합작사 판매량은 非중국 업체 판매량에 합산하여 산출함

주2) 우측 그래프의 가로축은 각 사의 중국 내 시장점유율 변화 비율(2021년 → 2024. 1~7월)을 표기한 것이며, 세로축은 2021년~2024. 7월까지 중국 내에서 판매한 자동차 중 NEV 비중(%)을 로그 단위로 표기한 것임

* 자료: MarkLines

• 원인으로는 中 업체 역량 강화, 애국소비 외에도 COVID-19 이후 중국 시장이 NEV(BEV, PHEV, FCEV) 중심으로 빠르게 재편되는 과정을 따라가지 못한 결과라는 관점이 설득력을 가지는 것으로 판단

- 일본계 완성차社의 위상 하락이 시작된 2021년부터 살펴보면, 일본 업체 외에도 NEV 판매량 비중이 일정 이하인 업체들을 중심으로 점유율 하락 다시 말해 위상이 떨어지는 경향성이 존재

3社 간 협력은 中 시장에서의 위축으로 촉발된 전기차, SW 등의 위기감이 반영된 결과로 해석

• Honda의 경우 그간 완성차社와의 관계에서 자체적인 노력을 기울이는 기조가 우세하였으나 협력을 강화하는 노선으로 선회

* Honda는 전기차 분야에서 2022년 GM과 저가형 전기차 개발 협력 계획을 발표하였으나 2023년 이를 포기한 바 있으며, 2024년 CES에서는 독자적인 플랫폼인 0 Series 중심으로 사업을 전개할 계획임을 발표한 바 있음

* 연료전지 분야에서는 2013년부터 GM과 협력하였으며 JV인 FCSM에서 2024년 1월 연료전지 상업 생산을 시작하기도 하였으나, 초기 수준의 시장 규모 등으로 인해 의미 있는 성과 창출이 이뤄지지 못하고 있다는 평가가 있었음

- Honda의 판매량 중 30% 이상을 차지하는 中 시장에서 영향력을 빠르게 상실한 것에 따른 위기감과 독자적으로는 미래차 전환에 성공하기 위한 임계 규모의 투자를 확보하기 어렵다는 판단 등이 변화의 배경인 것으로 추정됨

• Nissan과 Mitsubishi는 2016년부터 협력을 해왔으나 실질적인 협력 성과가 부족하고 Nissan이 보유한 Mitsubishi 지분 34.01%의 매매 금지가 2026년 해제되면 양사 간 관계가 변화할 것이라는 전망이 있었으나 이번 발표로 지속적인 협력 가능성이 높아진 것으로 평가됨

- 다만, 그간 장기적으로 연합을 구성해왔음에도 괄목할 성과가 부족하였고 Mitsubishi가 연합에 참여하면서 어떠한 시너지를 창출할 수 있을지 대해서 부정적인 견해도 존재하여 향후 협력 내용의 구체화 과정 확인 필요

3社 연합은 日 국내에는 상당 파급력을 가질 것으로 전망되나 글로벌 영향은 불투명 평가

• 연합이 성립되면 日 국내 경쟁 구도가 2개 연합으로 재편되어 큰 파급력을 가질 것으로 전망

- 日 완성차 시장은 3강(Toyota, Honda, Nissan), 4약(Mitsubishi, Suzuki, Subaru, Mazda)이 90% 이상의 점유율을 차지하고 있는데, 이번 3社 간 연합을 통해 Toyota 연합과의 격차를 좁히고 일본 국내 경쟁 구도에도 영향을 줄 수 있을 것으로 예상됨

* FY23년말 기준 Toyota(トヨタ自動車株式会社)는 Suzuki 4.98%, Subaru 20.42%, Mazda 5.07% 지분 보유

* 日 국내 점유율(2024. 1~7월): Toyota 연합 62.6%(Toyota 39.9%, Suzuki 17.2%, Subaru 2.3%, Mazda 3.2%), 3社 연합 31.3%(Honda 17.2%, Nissan 11.4%, Mitsubishi 2.7%)

• 미래차 트렌드 대응 비용 저감 및 개발 기간 단축 등을 통해 경쟁력 확보에 기여할 것으로 예상되나, 글로벌 경쟁 구도에 큰 파급력을 가질지는 미지수

- SW, 부품 공유 확대 및 공동연구 등이 원활하게 진행된다면 전기차, SDV 등의 트렌드 대응을 위한 비용을 절감하고 미래차 사업 전략 목표를 기간 내에 달성하는데 기여할 수 있을 것으로 예상되나, 각 사가 HW, SW 등을 공유하면서 제품 차별성을 확보해야 하는 것은 과제로 남음

* 제품의 차별성을 확보하는 것 외에도 3社가 Segment 및 판매 지역 등에서 높은 차별성을 가지지 못하는 상태로 진단하며 연합을 통해 상호보완성을 확보하기 어려울 것으로 보는 시각도 존재

- 한편, 협력 내용 중 하나인 공통 OS 개발과 관련하여 약 800만 대 수준의 3社의 글로벌 합산 판매량이 응용프로그램 개발자에게 참여 유인을 제공하기에는 역부족이라는 시각*이 존재하는 등 연합 형성을 통해 미래차 부문의 명확한 경쟁우위를 확보하고 글로벌 경쟁 구도 변화를 유발할 수 있을지 의문이 남는 상태

* 차량용 OS 생태계 활성화를 위해서는 다양한 응용프로그램 개발자의 참여가 필수적인데, Google의 Android, Huawei의 HarmonyOS, Xiaomi의 HyperOS 등은 스마트폰, 가전제품과 연계가 가능하여 수억 개 이상의 기기로 구성된 잠재 시장이 존재하는 반면, 3社의 OS는 차량에만 적용되어 시장성에 차이가 있을 것이라 보는 관점임

[Honda, Nissan·Mitsubishi의 전기차 사업전략]

업체명	전략 개요
Honda	• BEV 시장 둔화에도 2040년 ZEV(Zero Emission Vehicle) 100% 목표 유지 • 이를 위해 2025년부터 BEV 글로벌 시장 진출을 본격화하고, 2026년 이후 북미에서 차세대 글로벌 전략 BEV 모델인 Zero 라인업을 확대하고, 2024년 2세대 FCEV를 일본 및 미국에서 출시 • 차세대 BEV에서 Tesla의 기가캐스팅 방식을 도입하고 배터리 공급망 구축에도 집중
Nissan Mitsubishi	• 지역별로 전기차 전환이 차등화됨을 고려하여 ICE부터 BEV, HEV, PHEV 등 균형 잡힌 라인업 구성 • 다양한 차종 및 파워트레인 개발을 위해 Honda, Mitsubishi 등 연합과의 협력을 강화 (Mitsubishi) PHEV 개발 주도, (Nissan) BEV 기술 공유, (3社 간) 부품 공용화 확대 등 • 2027년까지 기가캐스팅을 도입하고, 전고체 배터리를 포함한 저비용·고성능 배터리 개발 등 추진

출처: Fourin 세계자동차기술조사월보 2024년 8월호

전기차 캐즘 극복을 위한 과제

임현진 한국자동차연구원 산업분석실 선임연구원

KATECH INSIGHT

◆ 국내 승용전기차 보급 관련 분석 결과, 전기차 신규 보급 확대를 위해서는 충전인프라의 확충이 효과적이며, 또한 전기차 및 충전 인프라 관련 소비자 만족도를 높이기 위한 노력도 중요한 요소

◆ 한편 초기시장과는 달리 앞으로 전기차 시장의 캐즘(Chasm)을 극복하고 대중 소비자의 구매를 유도하기 위해서는 전기차 가격의 중요도가 확대될 전망

우리나라 승용전기차(BEV)의 보급은 전반적으로 확대 추이를 보이고 있으나, 시도 단위의 각 지역은 전체 시장의 흐름과는 다른 차별적인 양상을 보여주고 있음

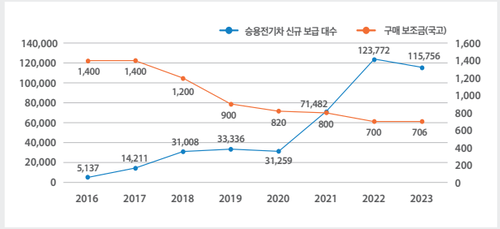
• 전기차 구매보조금의 축소 기조에도 불구하고, 국내 승용전기차 신규 보급대수 및 보급비율은 모두 증가 추세를 보이고 있음

* (전기차 신규 보급비율) = (전기차 신규 보급대수) ÷ (전체 자동차 신규 보급대수)

- 승용전기차 신규 보급대수는 증가 추세를 보이며 2022년 이후 10만대 이상을 기록하고 있으나, 2023년에는 다소 감소하여 11.6만대(보급비율 7.8%)를 기록

* 2023년 국내 전체(승용·승합·화물·특수차량을 모두 포함) 전기차 신규 보급대수(비율)은 16.3만대(9.3%)를 기록

[국내 승용전기차 신규 보급 대수 및 구매보조금] (단위: 대/백만원)



• 한편 승용전기차의 신규 보급대수 및 그 증가율을 살펴보면, 전반적으로 증가하는 흐름 속에서 시점 및 지역의 상황 등에 따라 서로 다른 변화 추이를 나타내고 있음 <☞ 참고>

- 전국 기준으로는 전기차 보급 정책 등에 힘입어 2018년까지는 높은 신규 보급 증가율을 기록하던 중 Covid-19 및 공급망 이슈 등으로 인해 2019~2020년 성장세가 한차례 꺾인 뒤, 2021~v22년 높은 증가율 및 역대 최대 신규 보급 대수(2022년 12.4만대)를 기록하였으나 2023년 다시 역성장 추세를 보임

- 그러나 전국 기준 역성장률을 보였던 2023년 전북·전남 등은 높은 증가율을 나타냈던 반면 그간 계속해서 보급 대수가 증가해왔던 대전의 신규 보급 감소율이 가장 높게 나타남

- 반대로 전국 기준 높은 성장률을 보였던 2016년, 2021년 각각 광주 및 울산은 역성장률을 기록하기도 하였음

• 이에 본고는 신규 승용 전기차 보급대수에 영향을 미치는 요인을 분석*하고, 최근 성장세가 둔화하고 있는 전기차 시장의 활성화 방안에 대해 논의해 보고자 함

* 2016~2022년까지의 17개 광역시도별 신규 전기차 보급대수, 누적 전기차 등록대수 및 충전기수, 전기차의 상대가격, 구매보조금, 1인당 지역내 총생산, 경제활동인구 자료 및 고정효과(FE) 모형을 이용하여 회귀분석을 실시함

승용전기차 신규 보급대수에는 충전인프라, 소득, 인구구조 등이 영향을 미치는 것으로 분석되나, 전기차 가격 및 구매보조금 효과는 통계적으로 확인되지 않음

• (충전인프라) 전기차 충전인프라 지표*가 1% 증가하면 승용전기차의 보급은 1.8% 증가

* (충전인프라 지표) = (전년말 지역 내 충전기 수) ÷ (전년말 전기차 등록대수)

- 전년도 지역내 전기차 등록대수 대비 충전기 수의 증가는 해당 지역의 전기차 신규 보급에 긍정적인 영향을 미치는 것으로 분석됨

- 한편 충전기의 절대적인 수는 전기차 신규 보급대수에 통계적으로 유의한 영향을 미치지 않는 것으로 나타남

• (소득/인구) 지역내 1인당 총소득 및 경제활동인구가 1% 증가하면 승용전기차의 보급은 각각 4.0%, 3.0% 증가

- 전기차 가격을 낮추기 위한 노력이 다방면에서 이루어지고 있지만 전기차는 구매보조금 적용시에도 여전히 내연차보다 판매가격이 높아, 필수재보다는 사치재에 더 가까운 특성을 가질 수 있음

* 2018년 코나 EV 모델의 국매 판매가격은 세제혜택 적용시에도 4,750만원으로 가솔린 모델(2,160만원) 대비 약 120%가 높았으며, 전기차의 상대적 가격의 하락에도 불구하고 2023년 코나 EV 모델의 국내 판매가격은 5,075만원으로 가솔린 모델(2,850만원)에 비해 약 78% 높은 가격에 판매되고 있음(보조금 미적용시 가격 기준)

- 사치재의 특성상 소득이 증가하는 폭에 비해 소비가 더 크게 증가하므로(소득탄력성〉 1), 소득수준 및 경제활동인구의 증가는 전기차 신규 구매 확률을 더욱 큰 폭으로 증가시킬 수 있음

- 그러나 향후 전기차 가격이 내연차 가격과 비슷한 수준으로 내려간다면, 전기차의 사치재 특성이 완화되고 전기차 구매의사에 대한 소득 및 경제력의 영향 또한 감소할 것으로 예상

• (준거집단 영향) 전년말 전기차 등록대수가 1% 증가하면 승용전기차 신규 보급은 약 0.5% 증가

- 전기차 도입에는 관련 인프라, 소득수준 등의 특성도 중요하지만, 지역내 전기차 보급 확대에 따른 이웃효과(neighborhood effect)*의 영향이 존재할 가능성

* 이웃효과는 이웃이 소비 등 개인 의사결정에 직간접적인 영향을 미친다는 것을 가정하는 경제 및 사회 과학 개념

- 우리나라 전기차 이용자를 대상으로 조사한 결과, 응답자의 약 97%가 향후 차량 추가 구입 또는 교체시 전기차 재구매 의사를 밝혔으며, 전기차를 주변인들에게 추천할 의향이 73.3%로 높게 조사되는 등 전반적으로 전기차 이용에 대한 만족도가 높은 것으로 나타남(한국교통연구원·한국환경공단)

- 따라서 전기차 이용에 만족하는 旣 구매자가 지리적으로 인접한 지역*에 많이 분포할수록 신제품에 대한 심리적 장벽이 낮아지고, 이에 따라 전기차 신규 구매의사가 확산될 가능성이 높아질 수 있음

* 본 분석에서는 전년말 기준 해당 지역내 전기차 등록대수를 이웃효과 변수로 사용함

• (가격/보조금) 한편 본 분석에서는 내연차 대비 전기차의 상대가격 및 구매보조금의 승용전기차 신규 보급에 대한 통계적 영향은 확인되지 않음

- 본고에서 분석한 국내 전기차 시장은 초기 성장 단계에 해당되므로 가격적인 측면보다는 기술의 혁신성, 성능·디자인 등을 중시하는 소비자 (얼리어답터 등)의 비중이 높을 것으로 추정

분석 결과, 전기차 보급 확대를 위해서는 충전인프라의 확충이 효과적이며, 이외에도 전기차 및 충전 인프라 관련 소비자 만족도를 높이기 위한 노력 또한 중요한 요소

• (충전인프라 확대) 현재 전기차 등록대수 대비 충전인프라가 적은 편은 아니지만, 국내 거주환경 특성 및 향후 전기차 수요 증가 전망 등을 고려하여 공공 충전인프라의 설치를 확대할 필요

- 2023년 기준 국내 충전기-누적 전기차 등록대수 비율(0.64)은 중국(0.16), EU(0.09), 미국(0.05) 대비 높은 편이나, 아파트 등 공동주택 거주 비율이 높은 우리나라는 공공 충전인프라의 중요성이 더욱 크게 작용할 가능성

• (준거집단 영향 확대) 운행 및 충전에 대한 기존 전기차 이용자의 긍정적인 경험을 확대하고 전기차에 대한 소비자 신뢰성·수용성을 제고함으로써, 전기차의 신규 보급 확대에 기여할 수 있을 것으로 기대

- (충전) 정부의 공공 충전기 보급 전략을 중심으로 한 충전인프라의 양적 확대와 더불어 충전기 신뢰성 및 충전 서비스의 개선·혁신이 수반된다면, 기존 전기차 이용자의 만족도가 증가하고 나아가 전기차 신규 구매 유인으로 확대될 것으로 예상

* Consumer Insight·서울시의회 등의 조사에 따르면 전기차 사용자들은 전기차 충전인프라 부족 외에도 충전소 위치정보 불충분, 긴 충전시간, 충전기 고장, 비용 결제 방식 등에서 불편함을 느끼고 있는 것으로 분석됨

- (전기차 기술) 낮은 외부기온 및 난방·공조 시스템 가동에 따른 배터리 성능·주행거리 감소 등은 전기차에 대한 소비자 수용성을 저해할 수 있으므로, 전기차 배터리 및 통합열관리 등 전기차 기술 관련 연구개발에 대한 지속적인 투자와 지원이 필요

* 전기차 사용자는 전기차 주행 성능 및 사양, 디자인 등에 만족도가 높은 편인 것과 달리 배터리 성능·주행가능거리 및 충전 편리성 등과 관련해서는 상대적으로 불만족하는 경향을 나타냄(한국환경공단·Consumer Report)

- (정비·수리) 정비 비용 부담 및 정비업체 부족 등에 대한 소비자 우려를 해소하기 위해 전기차 보급확대 속도에 맞춰 전기차 정비·수리 관련 교육 및 전문장비 확보 등에 대한 정부·기업의 지속적 지원이 필요

* 2023년 6월 기준 전기차 정비가 가능한 정비소 대비 전기차 수는 306.5대(전체 정비소 대비 내연차 수는 527.4대)로 차량 대비 정비업체의 수가 적은 편은 아니지만, 전기차 전문 정비업체가 1,517개소(전체 4.5만개소)에 불과하여 낮은 지리적 접근성 및 전기차 이용자의 불만족을 야기할 수 있음

- (안전) 전기차 및 배터리 안전성에 대한 소비자 경험 또한 전기차 확산에 주요하게 작용할 수 있으므로 차량 및 충전시설에 대한 안전성 인증 및 검사의 확대·강화가 필요

한편 초기시장과는 달리 앞으로 전기차 시장의 캐즘(Chasm)을 극복하고 대중 소비자의 신규구매를 유도하기 위해서는 전기차 가격의 중요도가 확대될 전망

• 국내에 비해 높은 전기차 신규 보급 비율을 나타내고 있는 중국 및 유럽 국가들은 전기차 가격 프리미엄*이 더 낮은 것으로 분석됨

* (전기차 가격 프리미엄) = {(전기차 판매가격)-(내연차 판매가격)} ÷ (내연차 판매가격)

- 2023년 기준 국내 전체 전기차 신규 보급 비율(9.3%) 대비 높은 보급률을 갖는 중국(25%), 독일(18%), 프랑스(17%), 영국(17%) 등은 전기차의 상대가격이 우리나라보다 더 저렴한 것으로 분석됨(IEA·ACEA)

* 2023년 코나 EV 모델이 가솔린 모델에 비해 약 78% 높은 가격에 판매된 반면, 2022년 중국에서 판매된 전기차의 가격은 보조금을 제외하고도 내연차 대비 14% 낮았으며, 독일, 프랑스, 영국의 경우 각각 전기차의 가격이 내연차 대비 14%, 39%, 44% 높게 나타남 (IEA)

• 국내 시장도 초기 단계를 넘어 전기차의 대중화를 이루기 위해서는 충전인프라 확대 및 소비자 신뢰성·수용성 제고뿐만 아니라 전기차-내연차간 가격차이를 줄이기 위한 지속적인 노력이 필요

- 일반적으로 초기 소비자의 경우 제품의 혁신성, 성능·디자인 등이 구매 동기로 작용하는 반면, 대중소비자의 수요는 가격적인 측면에 더 민감하게 반응

- 따라서 전기차 시장이 점차 성숙됨에 따라 초기 구매 수요가 완결되고, 향후 대중소비자의 수요를 유도하기 위해서는 가격의 중요성이 높아질 전망

[참고 : 지역별 승용전기차 신규 보급 대수및 증가율]

(단위: 대 / %)

지역	2015	2016	2017	2018	2019	2020	2021	2022	2023
강원	34	67 (97.1)	284 (323.9)	913 (221.5)	1,066 (16.8)	898 (-15.8)	2,526 (181.3)	3,671 (45.3)	2,781 (-24.2)
경기	100	285 (185.0)	1,480 (419.3)	3,750 (153.4)	4,716 (25.8)	5,759 (22.1)	12,423 (115.7)	28,153 (126.6)	24,165 (-14.2)
경남	137	138 (0.7)	444 (221.7)	1,079 (143.0)	1,397 (29.5)	1,626 (16.4)	4,391 (170.0)	7,523 (71.3)	10,127 (34.6)
경북	38	118 (210.5)	443 (275.4)	1,160 (161.9)	1,895 (63.4)	1,285 (-32.2)	2,226 (73.2)	4,779 (114.7)	4,587 (-4.0)
광주	79	53 (-32.9)	319 (501.9)	914 (186.5)	1,029 (12.6)	565 (-45.1)	1,316 (132.9)	2,868 (117.9)	2,653 (-7.5)
대구	62	254 (309.7)	1,656 (552.0)	4,674 (182.2)	4,515 (-3.4)	997 (-77.9)	3,427 (243.7)	7,125 (107.9)	5,053 (-29.1)
대전	6	42 (600.0)	213 (407.1)	1,024 (380.8)	1,298 (26.8)	1,359 (4.7)	2,987 (119.8)	5,887 (97.1)	3,055 (-48.1)
부산	113	124 (9.7)	421 (239.5)	717 (70.3)	1,560 (117.6)	1,209 (-22.5)	5,863 (384.9)	8,160 (39.2)	9,321 (14.2)
서울	409	467 (14.2)	3,618 (674.7)	5,057 (39.8)	5,010 (-0.9)	7,326 (46.2)	16,702 (128.0)	18,193 (8.9)	13,299 (-26.9)
세종	5	13 (160.0)	50 (284.6)	278 (456.0)	383 (37.8)	113 (-70.5)	458 (305.3)	883 (92.8)	941 (6.6)
울산	34	47 (38.2)	323 (421.0)	713 (120.7)	1,258 (76.4)	2,345 (86.4)	5,309 (126.4)	11,973 (125.5)	12,195 (1.9)
인천	34	62 (82.4)	323 (421.0)	713 (120.7)	1,258 (76.4)	2,345 (86.4)	5,309 (126.4)	11,973 (125.5)	12,195 (1.9)
전남	133	147 (10.5)	490 (233.3)	994 (102.9)	1,322 (33.0)	1,491 (12.8)	2,506 (68.1)	4,567 (82.2)	6,693 (46.6)
전북	14	18 (28.6)	261 (1350.0)	646 (147.5)	798 (23.5)	955 (19.7)	2,036 (113.2)	3,268 (60.5)	4,574 (40.0)
제주	1,703	3,243 (90.4)	3,611 (11.3)	6,946 (92.4)	3,711 (-46.6)	1,906 (-48.6)	3,271 (71.6)	5,440 (66.3)	6,127 (12.6)
충남	19	34 (78.9)	145 (326.5)	762 (425.5)	1,635 (114.6)	1,886 (15.4)	2,830 (50.1)	4,739 (67.5)	4,817 (1.6)
충북	12	25 (108.3)	207 (728.0)	880 (325.1)	1,129 (28.3)	879 (-22.1)	2,629 (199.1)	4,929 (87.5)	3,657 (-25.8)
전국	2,932	5,137 (75.2)	14,211 (176.6)	31,008 (118.2)	33,336 (7.5)	31,259 (-6.2)	71,482 (128.7)	123,772 (73.2)	115,756 (-6.5)

한국자동차산업의 경쟁력,
한국자동차연구원이 함께 합니다!

한국자동차연구원 기술이전

한국자동차연구원은
핵심기술인 소재기술, 시스템기술, 부품기술과
보완기술인 평가환경구축기술, 검증 기술, 신뢰성 기술을
개발 및 전수하고 있습니다.

한국자동차연구원 기술이전 홈페이지 통해
더 많은 정보를 확인할 수 있으며,
기술이전 상담신청이나 기술이전 설명회 참가 신청 등
기술이전과 관련된 다양한 서비스를 제공하고 있습니다.

https://tlo.katech.re.kr

한국자동차연구원
우수기술 이전문의

담당자 : 문환식 책임 Tel_ 041-559-3055 hsmun@katech.re.kr
강효진 연구원 Tel_041-559-3247 hjkang1@katech.re.kr

기술이전이란 _ 기업이 기존 사업확장 및 신사업 창출 등을 위해 필요한 기술을 KATECH으로부터 제공받아 자체 실시할 수 있도록 전수 받는 것입니다.

CAN 실시간 통신 보안기술

차량 내부통신으로 널리 사용되는 CAN 통신의 보안을 위한 기술로, CAN 통신에는 실시간 보안적용이 어렵다라는 관념을 깨는 기술이 적용되어있으며 0.1ms 이내의 실시간 메시지 차단이 가능함.

개발상태

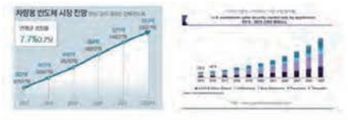
- 연구실 환경에서의 Working Model 개발

우수성

- 매우 작은 FPGA를 이용하여 구현가능하며 추후 CAN 트랜시버 및 CAN 통신 IP를 개발할 수 있음. 각 ECU의 보안 칩으로 사용되면 매우 큰 파급효과가 있으리라 사료됨.
- 기술성을 인정받아 미국 등의 국가에 국제 출원 완료함.

국제특허출원완료

시장동향	활용분야
• 차량용 반도체는 급성장중에 있음. • 차량용 보안 산업 역시 급성장중에 있음.	• 자동차내부 통신 반도체 CHIP, 또는 FPGA



기술성숙도

1 기초연구 단계 | 2 개념정립 단계 | 3 실험 단계 (기본성능 검증) | **4 실험 단계 (부품/시스템 성능 검증)** | 5 시작품 단계 (시제품 제작) | 6 시작품 단계 (성능 평가) | 7 실용화 단계 (신뢰성 평가) | 8 실용화 단계 (시제품 인증) | 9 양산 단계 (사업화)

지식재산권 현황

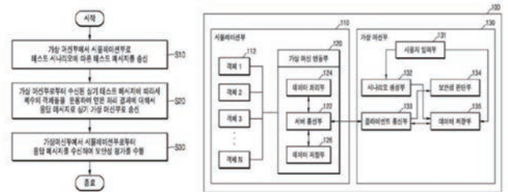
NO.	특허명	출원일	출원번호	등록번호
1	차량용 CAN 통신 보안 장치 및 방법	2020-11-18	10-2020-0154744	10-2471960
2	차량용 CAN 통신 보안 장치 및 방법	2021-09-27	17/486,284	-
3	비트 스트림 프로세서 및 이를 포함하는 CAN 컨트롤러, CAN 통신 에러 처리 방법	2021-07-12	10-2021-0090939	-

가상 머신을 이용한 보안 시뮬레이션 시스템 및 방법

가상 머신을 활용해 V2X 시뮬레이션 장비와 연동하여 보다 실제 환경에 가까운 보안 테스트 환경을 구성하는 방법임. 본 기술을 적용하면 시뮬레이션 내 노드에 일부 하드웨어 스펙을 부여할 수 있으며, 네트워크를 연결해 실제 환경에서 발생할 수 있는 다양한 사이버 보안 공격을 수행하거나 방어 기술 검증을 수행할 수 있음.

개발상태

- 분석과 실험을 통한 기술개념 검증



우수성

- 시뮬레이션의 한계점을 극복하고 보다 실제 환경에 가까운 테스트 환경을 구성함으로써 다양한 보안 시뮬레이션을 실험할 수 있음.
- 시뮬레이션 장비의 프로그래밍 언어에 한정되지 않기 때문에 다양한 보안 솔루션을 연동할 수 있어 유연한 테스트 환경으로 활용할 수 있음.

시장동향	활용분야
• WP.29 R155, 150 21434 등 국제 표준 및 권고 사항으로 인해 자동차 제조사들은 자동차에 대한 보안 기술 적용 및 테스트를 반드시 수행해야 함. • 제조사는 CSMS를 갖춰 인증을 받아야 차량 형식승인(VTA)을 받을 수 있으며, 이 과정을 거쳐야만 유럽시장에 차량을 판매할 수 있음.	• 차량 주행 중 V2X를 활용한 사이버 공격 및 보안 기능의 성능 테스트 • OS 및 네트워크에 존재하는 취약점 분석 및 사이버 공격의 공격 경로 분석 • 보안 시스템의 성능 보완을 위한 데이터 수집

기술성숙도

1 기초연구 단계 | 2 개념정립 단계 | **3 실험 단계 (기본성능 검증)** | 4 실험 단계 (부품/시스템 성능 검증) | 5 시작품 단계 (시제품 제작) | 6 시작품 단계 (성능 평가) | 7 실용화 단계 (신뢰성 평가) | 8 실용화 단계 (시제품 인증) | 9 양산 단계 (사업화)

지식재산권 현황

NO.	특허명	출원일	출원번호	등록번호
1	가상 머신을 이용한 보안 시뮬레이션 시스템 및 방법	2022-10-27	10-2022-0140624	-

KADaP
KOREA AUTOMOTIVE DATA PLATFORM
자동차데이터플랫폼

바로 시작하는 자동차 데이터 분석과 개발

자동차 데이터 분석과 AI 알고리즘 개발,
자동차산업클라우드로 지금 바로 시작하세요.

고사양 컴퓨팅 장비의 구입이나 구축없이
바로 자율주행 기술 개발, 자동차 데이터 분석
그리고 AI 알고리즘 개발을 시작할 수 있습니다.

KADaP CLOUD
자동차산업클라우드

https://www.bigdata-car.kr

자동차 관련 데이터를 키워드 검색과
세분화된 카테고리를 이용하여
손쉽게 찾을 수 있습니다.

KADaP PORTAL
자동차데이터포털

분석/개발에 필요한 자동차 데이터는 물론
APP, API 같은 자동차 데이터 기반의 상품과
서비스를 간편하게 구매하고 활용할 수 있습니다.

KADaP MARKET
마켓/서비스플레이스

자동차산업클라우드는

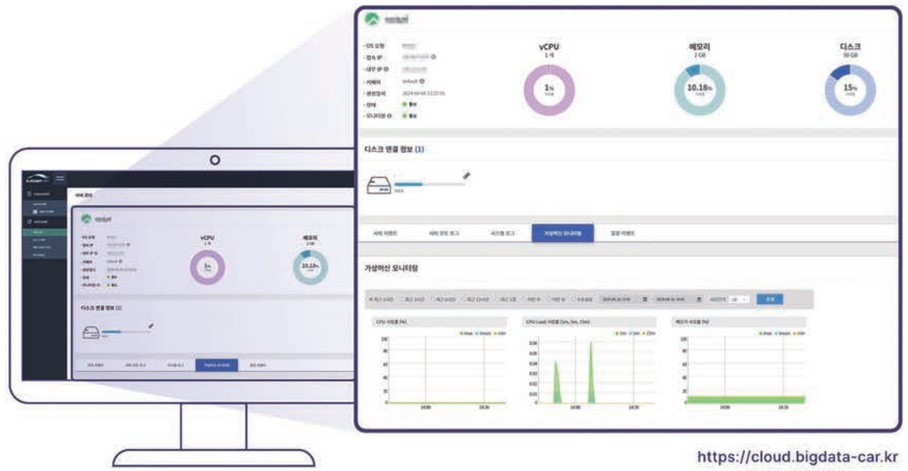
자동차 데이터 분석과 기술 개발에 필요한 IT 인프라를 가상화 기술을
활용하여 대여해 주는 서비스입니다. 사용자는 원하는 사양의 서버를 직접
생성하거나 제공되는 시뮬레이션, 분석, 개발 환경에 접속하여 바로 사용할 수 있습니다.

Cloud-Server

- 사용 목적에 맞는 사양의 가상 서버 생성 가능 (CPU, RAM, HDD)
- 다양한 OS 지원 및 지속적인 업데이트 (Ubuntu, CentOS, Rocky 등)
- 웹(Web)기반 인터페이스를 통한 가상 서버 생성-관리-반납 가능

Cloud-PC

- 자동차 기술 개발에 필요한 시뮬레이션 툴, 수치해석 툴, 분석 및 개발 환경 제공
- 제공되는 원격접속 SW및 단말기를 활용하여 설치 없이 접속 후 바로 사용 가능
- 국가 보안요구사항을 준수 하는 높은 보안성 (국가정보원 보안기능확인서 획득, 2022.6월)



https://cloud.bigdata-car.kr
(VPN접속필요)

산업통상자원부 | 대구광역시 | 한국산업기술진흥원 | 한국자동차연구원

Issue & Keyword

커넥티드카 사이버보안 주요 키워드

커넥티드카 (Connected Vehicle)

커넥티드카 (Connected Car)는 인터넷 및 다른 디지털 장치와 연결되어 데이터를 주고받을 수 있는 자동차이다. 이 차량은 V2X(Vehicle-to-Everything) 기술을 통해 외부 네트워크와 실시간으로 연결되어 운전자, 차량, 주변 환경, 인프라 간의 데이터를 공유한다. 이를 통해 차량은 교통 상황, 날씨, 도로 상태, 차량 상태 등의 정보를 실시간으로 수집하고 처리하여 운전자에게 더 나은 주행 경험을 제공한다.

커넥티드카는 자동차와 IT 기술의 융합으로 다양한 기능을 제공하고 주요 특징은 다음과 같다

1. 안전성 향상: V2V(Vehicle-to-Vehicle) 및 V2I(Vehicle-to-Infrastructure) 통신을 통해 차량 간 충돌 방지, 교통 사고 예방, 긴급 상황 시 경고 등 실시간으로 안전 기능을 제공.

2. 편의성 증대: 내비게이션 시스템을 통해 실시간 교통 정보를 반영한 경로 안내, 주차 정보, 차량 상태 모니터링 등이 가능.

3. 원격 제어: 스마트폰 앱이나 클라우드 기반 시스템을 통해 차량의 잠금 해제, 원격 시동, 공조 장치 설정 등 원격으로 차량을 제어.

4. 소프트웨어 업데이트: OTA(Over-the-Air) 업데이트를 통해 차량 소프트웨어의 보안 패치 및 기능 추가가 가능하며, 이는 차량의 유지보수와 성능 향상.

5. 엔터테인먼트 및 커뮤니케이션: 인터넷을 통한 다양한 엔터테인먼트 서비스 및 음성 인식, 차량 내 통신 기능을 제공.

커넥티드카는 운전 경험을 향상시키고, 자율주행차로 나아가기 위한 핵심 기술로 자리잡고 있으며, 이에 따라 사이버보안의 중요성도 커지고 있다. 네트워크에 연결된 차량은 해킹, 데이터 유출, 시스템 오류 등의 보안 위협에 노출될 수 있기 때문에, 이러한 차량의 보안 강화를 위한 기술이 필수적이다.

자동차 사이버보안

차량이 사이버 공격으로부터 안전하게 보호될 수 있도록 다양한 보안 기술과 절차를 적용하는 것을 의미한다. 커넥티드카와 자율주행차와 같은 차량들은 점점 더 많은 소프트웨어와 네트워크 시스템에 의존하게 되면서, 외부로부터의 해킹, 데이터 유출, 시스템 오류와 같은 사이버 위협에 노출될 가능성이 커지고 있다. 이러한 위험에 대응하기 위해 자동차 사이버보안이 필수적으로 적용된다.

자동차 사이버보안의 주요 위험 요소

1. 원격 해킹: 차량의 통신 시스템(V2X, Wi-Fi, Bluetooth 등)을 통해 원격으로 차량 시스템에 침투해 제어권을 탈취할 수 있다.

2. 데이터 유출: 차량의 센서와 시스템에서 수집된 개인 정보(위치, 주행 기록 등)가 해킹을 통해 유출될 수 있다.

3. 악성 소프트웨어: 악성 소프트웨어가 차량 시스템에 침투하여 차량 성능을 저하시키거나 중요한 기능을 중단시킬 수 있다.

4. OTA(Over-the-Air) 업데이트 취약성: 소프트웨어 업데이트 과정에서 악의적인 코드가 삽입되거나, 업데이트가 중단되어 시스템 오류가 발생할 수 있다.

5. ECU(전자제어장치) 해킹: 차량 내부의 여러 ECU(엔진, 브레이크, 조향장치 등)에 침투해 차량을 통제하거나 시스템을 손상시킬 수 있다.

자동차 사이버보안 국제 기준 (UNECE UNR 155)

UNR 155는 승용차, 상용차, 버스, 트럭, 자율주행차를 포함한 모든 유형의 도로 차량에 적용된다. 이 규정은 유럽을 비롯한 UNECE 회원국에서 새로 생산되는 차량뿐만 아니라, 해당 국가로 수출되는 차량에도 적용되기 때문에 전 세계 자동차 제조사들이 이를 준수해야 한다.

UNR 155는 UNECE(유엔 유럽 경제 위원회)에서 제정한 자동차 사이버보안에 대한 국제 규정으로, 차량의 사이버보안을 보장하기 위한 필수 요건을 제시한다. 이 규정은 2021년 1월 발효되었으며, 유럽을 포함한 여러 나라에서 자동차 형식 승인(Type Approval)을 받기 위해 반드시 준수해야 하는 기준이다. UNR 155는 특히 커넥티드카 및 자율주행차와 같은 기술이 발전하면서 사이버보안의 중요성이 커짐에 따라 차량의 안전성과 보안을 보장하기 위한 법적 프레임워크를 제공한다.

CSMS (Cybersecurity Management System)

사이버보안 관리 시스템(CSMS)은 차량에 대한 사이버위협과 관련된 위험을 처리하고 사이버 공격으로부터 차량을 보호하기 위해 조직 프로세스, 책임 및 거버넌스를 정의하는 체계적인 위험 기반 접근 방식을 의미한다.

CSMS 평가는 OEM의 사이버보안 관리시스템에 대한 심사를 말한다. 전문가 평가는 조직의 프로세스가 제품 생애주기 전체에 걸쳐 적합한 사이버보안 프레임워크를 제공하는지, UNECE 사이버보안 차량 규제의 CSMS 요구사항을 모두 충족하는지를 확인한다. 자동차가 서로 연결되고 자동화 및 자율주행 기술이 발전하는 등 복잡성이 증가함에 따라 사이버 공격의 위험성이 높아지고 있다. 자동차와 부품을 보호하기 위해 제조업체는 제품 뿐만 아니라 안전성 및 보안성을 갖춘 제품을 개발할 수 있는 조직적인 사이버보안 환경을 만들어야 한다.

UNECE 규제 도입으로 모든 신차, 시스템, 부품 및 별도의 기술 유닛에 대한 사이버보안이 의무화되고 있다. 해당 규제는 제품의 사이버보안과 조직 환경을 모두 포함하고 있다. UNECE 규제와 ISO/SAE 21434 모두 자동차 공급망 전체에 걸쳐 사이버보안을 적용할 것을 요구하고 있으며, CSMS 평가는 사이버보안 규제 요구사항을 모두 충족했다는 것을 보장하는 의미가 있다.

차량 형식승인 (Vehicle Type Approval)

차량 형식승인(Vehicle Type Approval)이란 양산된 차량, 차량 시스템, 부품 또는 구성품의 샘플이 지정된 성능 표준에 적합한지 아닌지를 평가하여 인증을 부여하는 절차를 말한다. 인증취득 여부는 제조사가 제품에 표시한 형식승인 마크, 통칭 "E-mark"(EU인증의 경우 'e', UN인증의 경우 'E' 표시)를 통해 입증할 수 있으며, EU 완성차형식승인(EU WVTA) 절차에 따라 인증된 차량의 경우 제조자가 발행한 적합 증서(Certificate of Compliance, CoC)를 통해 인증취득 여부를 입증할 수 있다. UN International Whole Vehicle Type Approval(IWVTA) 절차에 따른 완성차 인증의 경우 적합성선언서(Declaration of Compliance, DoC)를 통해 이를 입증할 수 있다.

형식승인 절차에는 샘플선정 및 시험 감독, 기술문서 검토 및 생산 적합성(Conformity of Production, CoP) 검증을 위한 제조사 품질시스템 평가 등이 포함된다. 형식승인을 위해서는 특히 제조사가 인증된 제품 형식(Type)과 완전히 동일한 사양의 양산품을 균일하게 생산할 수 있는 지속적 품질관리 능력을 갖추었는지를 우선 평가해야 하며, 이를 생산 적합성 심사(CoP audit, 초기심사의 경우 Initial Assessment라고 함) 또는 공장심사라고 한다. CoP는 형식승인의 기본 초석이며, CoP 심사를 통해 유효한 CoP 인증서(Compliance Statement)를 취득한 후에만 형식승인 절차를 진행할 수 있다.

ISMS (Information Security Management System)

정보보호 관리체계(ISMS : Information Security Management System) 인증이란 기업(조직)이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운영하는 종합적인 체계(정보보호 관리체계)의 적합성에 대해 인증을 부여하는 제도를 말한다.

*** 과학기술정보통신부 : 인증제도를 관리·감독하는 정책기관**

*** 한국인터넷진흥원 : 인증기관으로서 전체적인 인증제도를 운용**

*** 인증위원회 : 산업계/학계 등 관련 전문가 10명 이내로 구성, 인증결과심의**

*** 인증 심사원 : 심사 자격요건을 갖춘 자들로 구성, 실질적인 인증심사를 수행**

정보보호 관리체계(ISMS) 인증 기대 효과

*** 지속가능경영의 핵심인 IT 컴플라이언스 대응**

*** 기업 윤리경영, 투명경영 등 기업의 사회적 책임 강화(CSR)**

*** 정보보호 위험관리를 통한 기업 비즈니스 보호**

*** 비즈니스 연속성 확보를 통한 고객 신뢰도 향상**

*** 침해사고, 집단소송 등에 따른 사회 · 경제적 피해 최소화**

RED (Radio Equipment Directive)

무선기기지침(Radio Equipment Directive)이란 보건 및 안전, 전자파 적합성(EMC) 및 무선 스펙트럼의 효율적인 사용과 관련하여 무선 제품의 제조 표준을 확립하고자 2016년에 발효됐다. 이후 유럽연합(EU)은 유럽 시장에서 무선기기의 사이버보안을 강화하기 위해 2021년 10월, 특정 범주의 무선 장비에 대한 업데이트된 사이버보안 요구사항을 발표했다.

무선 장비 제조업체는 원활한 시장 진출을 위해 새로운 요구사항을 파악하여 미리 대응 준비를 해야 한다. 많은 제품이 응용 프로그램에서 무선 기술을 활용하고 있다. 이렇게 인터넷에 연결된 많은 장치는 보안 위험에 노출되어 잠재적인 공격과 악용에 취약할 수 있다. 이러한 위험을 완화하기 위해 유럽위원회는 특정 범주의 무선 장비에 대해 Article 3.(3) (d), (e), (f)항을 추가하는 무선 장비 지침의 위임 규정을 채택하여 사이버보안, 개인 데이터 보호 및 개인정보 보호, 금융 거래 보호 수준을 높였다.

사이버보안에 대한 제3조 3항의 (d), (e), (f) 조항

*** (d) 무선 장비는 네트워크 또는 그 기능에 해를 끼치거나 네트워크 리소스를 오용하여 허용할 수 없는 서비스 저하를 유발하지 않아야 한다.**

*** (e) 무선 장비는 사용자와 가입자의 개인 데이터와 개인정보가 보호되도록 보장하는 안전장치를 통합해야 한다.**

*** (f) 무선 장비는 사기로부터 보호를 보장하는 특정 기능을 지원해야 한다.**

MOBILITY INSIGHT Review

2024 08월호

한국자동차연구원 산업분석실

글로벌 자동차 시장 내 중국의 약진 어떻게 볼 것인가?

□ 커버스토리

미래 글로벌 자동차 시장 中國 '그 中心이 되다.'

전통적인 내연기관 중심의 자동차 시장에서 오랫동안 중국은 글로벌 브랜드들의 매력적인 소비시장으로만 인식되고 있었던 것이 사실이다. 또한, 중국은 글로벌 브랜드들의 기술력과 경쟁력을 따라가는 추종자로서 그 격차를 좁히기에는 다소 역부족이었다.

그러나 탄소중립이라는 글로벌 아젠다와 맞물리면서 기존 내연기관 중심의 자동차 시장에서 전기차를 비롯한 '친환경적 미래차 시장'으로 큰 틀의 시장 구도가 재편되는 과정에서 중국은 새로운 기회를 맞게 됐다. 지금 글로벌 자동차 시장에서 중국의 브랜드와 시장의 움직임은 심상치 않다. 한마디로 중국이 미래 글로벌 자동차 시장의 새로운 중심이 되어가고 있다.

한국자동차연구원이 주관한 이번 좌담회는 조철 좌장(산업연구원 선임연구원), 이왕휘(아주대학교 정치외교학과 교수), 유효정(지디넷코리아 중국전문 기자),차두원(소네트 대표이사), 최필수(세종대학교 중국통상학과 교수), 최재희(대외경제정책연구원 중국팀 전문연구원) 등 6명의 산학연 전문가가 모여 미래 글로벌 자동차 시장 내 중국의 입지와 역할, 의미를 토론했다.

미래차 시장의 中心은 中國 약진이 아닌 '추월, 돌파'

조철(좌장) 산업연구원 선임연구위원

지난 2024년 4월 베이징에서 개최된 '오토차이나 2024'에 직접 참관하여 중국 로컬 기업들이나 자동차 산업의 발전 양상을 보면서, 개인적으로 느낀 바가 매우 크다. 한마디로 '과연 앞으로 중국과 경쟁을 할 수 있을까?' 싶을 정도로 기대감보다는 두려움이 앞섰다. 이는 단순한 느낌의 문제가 아니라 실제 숫자적으로도 중국 내수 생산량과 수출량이 빠르게 성장하는 것을 보더라도 누구도 부정할 수 없을 것이다.

지금까지 추종자였던 중국이 '시장의 새로운 리더'로 자리매김

이왕휘 아주대학교 정치외교학과 교수

테슬라를 제외하면 중국기업과 경쟁할 수 있는 미국기업은 사실상 없는 실정이다. 현재 진행되고 있는 글로벌 전기차 동향을 볼 때, 앞으로 전기차 시장의 주도권은 미국이 아닌 중국이라고 말해도 과언이 아니다. 자동차가 발명된 이후 최근까지 중국이 미국을 따라갔다면, 앞으로는 미국이 중국을 따라가야 하는 아이러니한 상황이 도래한 것이다.

미래차 시장의 경쟁력 확보 정부의 '관심과 지원'이 우선 되어야

유효정 지디넷코리아 중국전문 기자

정보통신기술과 자동차라는 새로운 믹스매칭을 통한 경쟁력을 높이려면, 먼저 정부 차원의 튼튼한 지원과 기업들의 노력이 함께 되어야 할 것이다. 이를 통해 세계적으로 경쟁력 있는 자동차 소프트웨어 생태계가 형성될 수 있다면, 이를 바탕으로 미래차의 경쟁력 또한 높아질 수 있을 것이다.

중국차의 본격적인 국내 진출 두려워하기보다 '당당하게 맞서자'

차두원 ㈜소네트 대표이사

중국 전기차의 국내 진출은 당장은 커다란 영향을 주지는 않을 것으로 예상한다. 가성비는 높지만, 중국제품에 대한 부정적 인식이 보편화되어 있고, 국내 자동차 소비층이 보수적으로 판단되기 때문이다. 테슬라가 처음 국내에 진출했을 때는 구매 가능한 전기차 모델이 다양하지 못하기도 했고, 해외의 충성도 높은 얼리어댑터들의 구매 현상이 국내에도 연속적으로 이어진 현상은 볼 수 없을 것이다.

중국의 급성장은 우연이 아닌 치밀한 '준비와 전략'의 결과

최필수 세종대학교 중국통상학과 교수

지금의 중국 전기차 부분이 가파른 성장세를 보이는 것은 치열하고 집요한 정책의 결과라고 생각한다. 중국 정부는 오랜 기간 신에너지 자동차 부문을 집중적으로 키우려 노력했으며, 전 벨류체인에 걸쳐 거시적인 안목으로 기획해 왔다. 중국은 미래차에 대한 준비와 투자를 집중하면서 배터리 소재 확보, 모듈 조립부터 생산, 폐배터리 처리에 이르기까지 전 과정에 걸쳐 정부 차원에서 체계적으로 기획했다.

중국 자동차 시장의 키워드 '정부 주도, 빠른 전동화'

최재희 대외경제정책연구원 중국팀 전문연구원

중국 자동차 시장의 중요한 특징 중 하나는 바로 전 세계 어느 나라보다 전동화(차량의 구동 및 관련 기능을 모터와 배터리로 보조하거나 대체하는 것)가 빠르고 적극적으로 진행되고 있다'라는 것이다. 중국 자동차 시장은 세계 어느 나라보다도 적극적으로 전동화가 진행되고 있으며, 정부의 강력한 지원과 기업 간 치열한 경쟁을 바탕으로 빠르게 성장하고 있다.

□ 스페셜컬럼

중국, 세계 최대 자동차 시장이며 최대 생산국

조철 산업연구원 선임연구위원

중국은 시장 이상의 의미를 갖고 있어 우리 기업이 포기할 수 없다. 중국 시장에서 도태되는 것은 중국과의 경쟁에서 밀리는 것이고, 이는 세계 시장이나 국내 시장에서도 중국에 뒤질 수 있다는 것을 의미하기 때문이다. 현시점에서 중국은 우리 자동차 산업에 가장 큰 도전 중의 하나라고 할 수 있고, 이 도전을 이겨내야만 앞으로 생존 및 발전할 수 있는 것이다.

□ 정책동향

중국산 전기차에 대한 미국과 EU의 규제 현황 및 추가 규제 가능성

장미화 법무법인(유) 세종 전문위원

미국 바이든 행정부는 2024년 5월, 무역법 301조 검토 절차를 통해 중국산 전기차에 대한 추가 관세를 100%로 인상하였다. 이러한 조치는 중국산 전기차의 수입이 미미하여 WTO 보조금협정이 규정하고 있는 보조금 조사 요건을 충족하지 못한 상황에서 중국산 전기차의 유입을 사전에 차단하기 위한 선제 조치로 평가할 수 있다.

□ 트렌드리뷰 ①

최근 중국 자율주행 시장 및 동향 분석

차두원 ㈜소네트 대표이사

중국 자율주행 레벨4 기업들이 기술 개발을 통해 세계 최초로 수익 창출에 노력하고 있다. 첨단운전자보조시스템 시장으로의 진출 시도는 중국 현지에 한정되지만, 무인 자율주행 서비스 실현을 위한 중요한 티핑포인트가 될 것으로 예상된다. 그만큼 투자와 과감한 협력들이 진행되고 있어 향후 국내 자동차 산업에 미칠 영향과 우리의 대응도 더 적극적으로 논의되어야 할 시점이다.

□ 트렌드리뷰 ②

중국 전기차 산업의 약진, 협업의 성공 방정식을 바꾸다.

천서형 LG경영연구원 연구위원

중국 자동차 기업들의 협업 모델이 정치적, 문화적 특성에 기반하고 있어 글로벌 시장에 즉각적인 영향을 미치기는 어렵다고 생각한다. 그럼에도 불구하고, 중국 자동차 산업의 다양한 협업 모델이 향후 기술 트렌드를 주도할 가능성은 충분히 있다고 판단된다. 우리나라 기업과 정부는 이들의 활동을 면밀히 모니터링하며, 기술 혁신을 통한 경쟁력 확보 방안에 대해 지속적인 고민과 노력이 필요하다.

□ 생생 인터뷰 ①

중국을 넘어 세계를 앞서 보고 달린다. ㈜스트라드비전

김준환 ㈜스트라드비전 대표

"스트라드비전은 Vision AI 기술을 SDV 보급에 집중하고, 장기적으로는 Vision AI 기술을 활용할 수 있는 사업 분야를 확장해 나갈 계획입니다. 코스닥 상장 후 중장기적인 목표로는 스트라드비전의 핵심 기술 비전 AI를 통해 자동차뿐 아니라 다양한 일상생활에 적용되어 효율성과 생산성을 극대화할 것입니다."

□ 생생 인터뷰 ②

중국을 넘어 글로벌 시장으로 우리가 간다. 우리산업(주)

정상원 우리산업(주) 부사장

"중국 샤오미 전기차 부품납품 기사와 관련하여 우리로서는 기사 내용에 소개한 성과에 단순히 만족하지 않고, 더욱 나은 품질과 기술력으로 고객사를 만족하게 하는 것뿐만 아니라 궁극적으로 글로벌 시장으로 확대해 가는 것이 목표입니다. 이를 위해 오늘도 계속하여 노력하고 있으며 중국을 넘어 글로벌 시장에서 인정받고, 국내 부품사를 대표하는 강한 기업으로 성장하도록 최선을 다할 것입니다."

모빌리티 인사이트 **독자 후기 설문**에 참여해주세요!

격월간 <모빌리티 인사이트>는 미래 모빌리티 핵심기술 개발 이외에도 정책 연구와 기업 지원 등을 확대하여 우리 자동차산업이 급변하는 산업 패러다임의 변화에 선제적으로 대응할 수 있는 기반을 마련하기 위한 자동차산업 정보지입니다. 모빌리티인사이트는 한국자동차연구원 홈페이지(www.katech.re.kr)를 통해서도 보실 수 있습니다.

모빌리티 인사이트에서는 독자 설문 이벤트를 통해 참여해 주신 독자 20명을 선정하여 <모빌리티 인사이트>에서 준비한 소중한 선물의 드립니다. 독자 여러분의 다양하고 솔직한 의견이 발전에 큰 힘이 됩니다. 많은 참여 부탁드립니다.

○ 참여 기간 : 2024년 10월 29일 부터 ~ 11월 20일까지

○ 참여 방법 : 온라인 설문

○ 참여 대상 : 모빌리티 인사이트 독자 누구나

○ 당첨자 선정 및 발표 : 무작위 랜덤 추첨, 당첨자 개별 공지 예정 (경품은 11월 30일 일괄 발송 예정 / 관련문의 02-2661-6786)

○ 응모 방법 : 1. 우측 상단의 QR코드를 이용해 모빌리티인사이트 독자 설문 이벤트 접속 (https://url.kr/e4qbfb)

2. 간단한 개인정보 입력(경품배송정보로 활용)

3. 설문조사 문항을 읽고 설문 작성

설문 문항

1. 자동차 관련 정보나 지식을 주로 어디서 습득하십니까? (중복 선택 가능)

- 온라인 뉴스
- 자동차 전문 매거진
- 기타(카페/블로그 등)
- 컨퍼런스 세미나 등 행사 참석
- 주변 자동차 업계 지인

2. 미래 모빌리티 산업으로의 패러다임 전환에 따라 본인이 평소 가장 관심을 갖는 분야를 선택 바랍니다 (중복 선택 가능)

- 자율주행
- 도심형 항공모빌리티(UAM)
- 기타
- 친환경 차량(전기차, 수소차 등)
- 컨넥티비티 & 인포테인먼트

3. 한국자동차연구원이 출간하는 [모빌리티 인사이트]는 구독자에게 원내 R&D 기술에 대한 다양한 정보를 제공하고자 노력하고 있습니다. 내용 습득에 있어, 이해도 수준은 어떻게 생각하십니까?

- 이해가 잘 된다
- 어려운 내용이 많아 이해하기 어렵다
- 보통이다
- 기타

4. [모빌리티 인사이트]가 자동차 산업의 방향을 제시하는데 있어 유용한 정보 채널이 될 것이라고 생각하십니까?

- 매우 그렇다
- 그렇다
- 보통이다
- 아니다
- 기타

5. [모빌리티 인사이트]에 추가적으로 바라는 점을 자유롭게 작성 부탁드립니다.

모빌리티인사이트 08월호 독자의견

황인성 님
앞으로도 양질의 컨텐츠 부탁드리며 월간으로 받아 볼수 있으면 좋겠습니다.

이주한 님
당월 주제와 연관된 연구원의 최신 연구 동향 소개도 부탁드리며 모빌리티인사이트 정기적으로 구독하고 싶습니다.

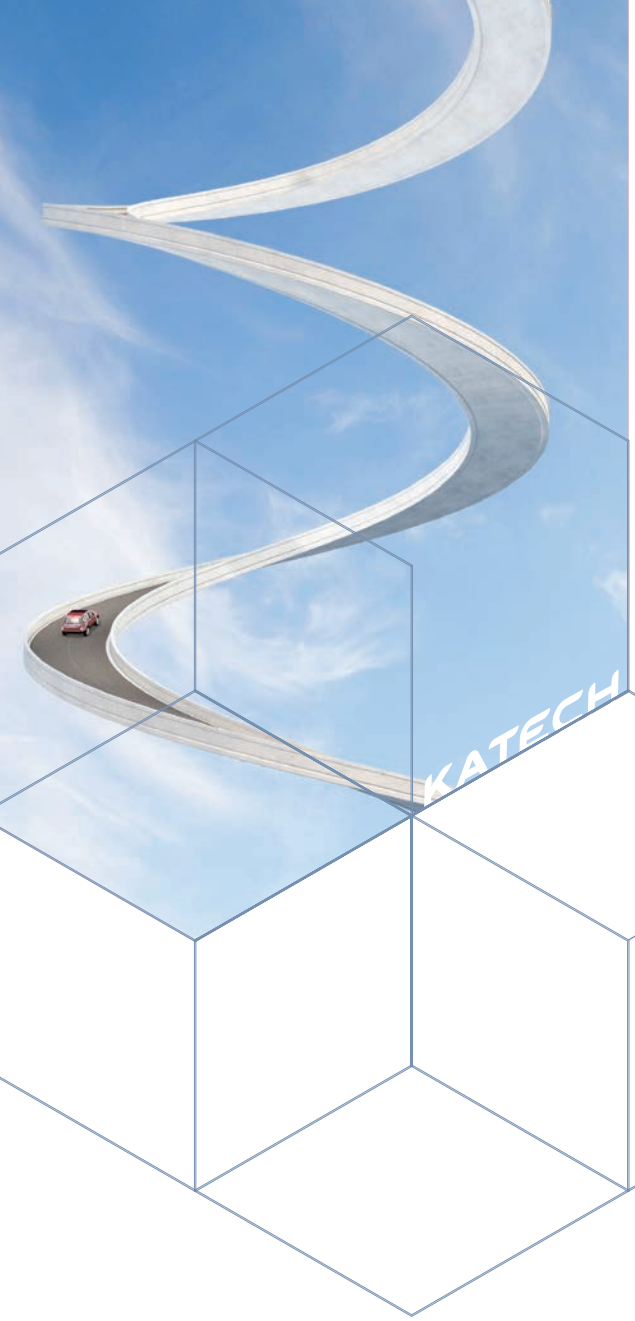
오슬기 님
영문으로 된 자료 제공도 함께해 주신다면 참 좋겠습니다

김기두 님
중국의 전기차 시장동향은 유용한 정보였습니다. 최근 전기차 배터리가 문제되고 있는데 전기차 배터리에 대한 기사도 다뤄줬으면 합니다.

이평우 님
모빌리티 인사이트 뉴스레터로도 받아 보고싶습니다. 모빌리티 인사이트 발전을 기원합니다.

모빌리티 인사이트 정기구독 신청

격월간 <모빌리티 인사이트>
정기구독을 희망하시면 QR코드를 접속하여
신청서 양식을 제출 해주세요.
무료로 보내드립니다.



국내 자동차 산업의
지속적인 혁신과
성장 동력 발굴을 위한
미래기술 개발 역량 강화에
앞장서겠습니다.

한국자동차연구원

KOREA AUTOMOTIVE TECHNOLOGY INSTITUTE
KATECH 한국자동차연구원

모빌리티 인사이트 2024. 10. Vol.33
www.katech.re.kr

발행인 : 나 승 식
발행처 : 한국자동차연구원
충청남도 천안시 동남구 풍세면 풍세로 303
TEL_041.559.3114 / FAX_041.559.3068
문의처 : mobilityinsight@katech.re.kr
편집/디자인 : 브랜드캐스트(주) TEL_02.2661.6786

※ 본 「모빌리티 인사이트」에 실린 보고서는 연구진이나 집필자의 개인적인 견해이므로 한국자동차연구원의 공식적인 의견이 아님을 말씀드립니다.

Copyright(c) 2024 KATECH(Korea Automotive Technology Institute) All right reserved.