10차시. 자율주행차와 사이버 보안

01. 자율주행차의 이해

- 과거 드라마로 인기를 끌었던 전격 Z 작전에서 키트는 우리에게 운전자 없이 스스로 움직이는 자동차라는 환상을 심어주었다. 즉, 자율주행 자동차가 이제는 꿈이 아닌 현실로 다가오고 있다. 자율주행 자동차는 교통사고를 줄이고 교통 효율성을 높이며 연료를 절감하고 운전을 대신해줌으로써, 편의를 증대시킬 수 있는 미래의 보편적 교통수단이 될 것으로 기대한다. 이번 차시에서는 자율주행차의 개념 파악을 시작으로 핵심 기술 요소에 대한 이해, 자율주행차의 혜택과 과제와 함께 자율주행차에 핵심인 보안에 대해서 학습한다.

자율주행차의 개념

- 자율 주행차란 운전자의 개입 없이 자동차 스스로 주변 환경을 인식하고, 주행 상황을 판단하여, 차량을 제어함으로써 스스로 주어진 목적지까지 주행하는 자동차를 의미한다. 즉 운전자는 목적지 입력만 하면 자율주행차가 스스로 길을 찾아 목적지까지 안전하게 운전하고 주차까지 수행하는 것을 의미한다.

※ 출처 : (산업부) 자율주행자동차 산업생태계 활성화를 위한 국가차원의 통합지원 활용방안, 2014

잠깐!

- **커넥티트카(Connected Car)? 스마트카(Smart Car)?**

커넥티드카는 안전과 편의성 향상을 목적으로 자동차에 통신기능 탑재하여 자동차와 모든 인프라 간 양방향 연결을 목표하는 차를 의미하였다. 주로 스마트폰과 차량을 연결하는 서비스가 주된 형태로 인포테인먼트 구현을 중심으로 개발되었다.

잠깐!

- **커넥티트카(Connected Car)? 스마트카(Smart Car)?**

스마트카는 간단히 말해서 커넥티드카에서 자율주행차로 발전하면서 생긴 용어로 이해하면 된다. 초기의 스마트카는 실시간으로 주행정보 제공이나 엔터테인먼트 등에 치중한 커넥티드카 형태이었지만 현재의 스마트카는 주변환경 인식, 판단, 차량제어 등을 통해 사람의 개입 없이 목적지까지 갈수 있는 자율주행차까지를 포함한다.

- **운전자 보조(Driver Assistance) 기술?**

운전자 보조 기술이란 종방향이나 횡방향 중 하나에 대해 운전자에게 경고하거나 제어를 지원하는 기술을 의미한다. 예를 들어

스마트 크루즈 제어(SCC: Smart Cruise Control) 기술은 종방향의 속도는 시스템이 제어하고 횡방향의 조향은 운전자가 담당하는 형태를 말한다.

자동 주차의 경우에는 조향은 시스템에서 자동으로 진행하고 속도 조절만 운전자가 하는 시스템을 말한다.

- **자동주행(Automated Driving) 기술?**

자동 주행 기술은 종횡 방향 모두에 대해 제어를 지원하는 기술을 의미하는데 한가지 전제 조건으로는 운전자가 모니터링하고 있다가, 언제든지 운전에 다시 개입하는 형태를 말한다. 예를 들어 고속도로에서 SCC와 차선유지(LKS: Lane Keeping System)가 결합된 서비스의 경우 앞 차와의 간격을 유지하며, 현재 차선을 계속해서 추종하다가 필요에 따라서 즉, 긴급한 상황 발생 시 운전자가 언제든지 개입하는 시스템을 의미한다.

- **무인자동차(Unmanned Vehicle/Driverless car)? 자율주행(Self-driving/Autonomous Driving) 기술?**

현재는 두 가지 용어를 혼용해서 사용하고 있지만, 일반적으로

무인 자동차는 사람이 탑승하지 않고 예를 들어 국방 분야에서 무인으로 임무를 달성하는 차량을 의미하며

자율주행 자동차는 항상 사람이 탑승한 상태에서 목적지까지 주행하는 차량, 예를 들어 일반 승용차를 지칭한다.

자동주행과 자율주행은 운전자가 항상 개입을 할 수 있도록 준비해야 하는지 아닌지에 따라 구별한다. 운전자가 항상 개입해야 하는 자동 주행과 달리 자율주행 차량에서는 차내 운전자의 행위와 무관하게 차량이 자율로 주행하는 개념이다.

자율주행차의 기술 수준 및 기술 요소

- 미국의 도로교통안전국(NHTSA: National Highway Traffic Safety Administration)는 자율주행 차량의 기술적 발전 수준을 기반으로 자율주행 정도를 0~4레벨의 5단계로 구분하고 있다. 0단계는 자동제어 장치가 없이 일반적으로 사람이 운전하는 자동차를 의미한다. 1단계에는 자동긴급제동장치(AEB)와 스마트 크루즈 컨트롤(SCC) 등의 자동 보조 시스템의 도움을 받아 사람이 운전하는 차, 2단계는 핸들조작 일부의 자동화와 고속도로 내 차선유지 등의 기능이 추가됐음에도 사람의 개입이 필요한 자동차를 의미한다. 3단계부터 자율주행차로 정의할 수 있는데, 이 단계에서는 가속, 주행, 제동이 모두 자동으로 수행될 수 있는 시스템을 의미하고, 운전자는 자동운전 여부만을 결정하면 되는 단계다. 4단계는 완벽한 자율주행의 수준으로 운전자가 목적지를 입력하면 자동차가 목적지까지 사람의 개입없이 이동이 가능한 수준이다.

	Level 0	Level 1	Level 2	Level 3	Level 4
	No Automation (비자동) 운전자에 의해 완벽하게 제어	Function Specific Auto (기능특화자동) 1개 이상 특정 제어 기능을 보유한 자동화 시스템	Combined Function Auto (조합기능 자동) 2개 이상 특정 제어 기능을 보유한 자동화 시스템	Limited Self-driving Auto (제한된 자율주행) 가속, 주행, 제동 모두 자동으로 수행, 필요 시 운전자 개입	Full Self-driving Auto (완전자율주행) 100% 자율주행
운전자 역할	직접 운전	정상적인 주행이나 충돌 임박 상황에서의 일부 기능을 제외한 자동차 제어권 소유	운전자가 여전히 모니터링 및 안전에 책임을 지고 자동차 제어권 소유	자동차가 모니터링 권한 보유, 특정 교통 환경에서 자동차가 모든 안전 기능을 제어	운전자는 목적지만 입력하면 자율주행시스템이 안전 운행에 대해 책임
대표 기능		스마트크루즈컨트롤, 차량 자세제어, 자동브레이킹	스마트크루즈컨트롤, 차선 중앙 유지, 핸들과 페달 제어	교통혼잡 시 자동차 스스로 저속 주행, 운전자 조작 없이 고속도로 주행, 자동 차선 변경 등	
	Now			2020+	2025+

출처 | NHTSA 참고, KT 경제경영연구소 재구성

- 자율주행차를 구성하는 핵심 기술은 주변환경 인식, 위치인식 및 맵핑, 판단, 제어, 상호작용 분야로 구분하여 볼 수 있다.

  - 주변 환경 인식은 정적장애물, 동적장애물(차량/보행자 등), 도로표식(차선, 정지선, 횡단보도 등), 신호등의 신호 등을 인식하는 기술로 레이다, 라이다, (스테레오) 카메라 등의 센서가 활용된다.

  - 위치인식 및 맵핑을 위해서는 자차의 절대적 상대적 위치의 추정이 필요한데 이를 수행하기 위하여 3차원 고정밀 디지털지도와 GPS, 센서정보 등을 융합해야 한다. 글로벌 항법 위성 시스템(GNSS: Global Navigation Satellite System)과 기타 맵핑을 위한 센서를 사용한다.

  - 자동차가 주변 환경에 대한 정보를 기반으로 판단을 하기 위해서는 차량의 위치에 대한 정보와 인공지능과 같은 소프트웨어의 도움이 필수적이다. 목적지까지의 경로 계획이나 장애물 회피 경로 계획과 같은 포괄적 판단은 물론 주행 상황별 필요한 행동,

- 자율주행차를 구성하는 핵심 기술은 주변환경 인식, 위치인식 및 맵핑, 판단, 제어, 상호작용 분야로 구분하여 볼 수 있다.

  - 예를 들어, 차선유지, 차선변경, 좌우회전, 저속차량 추월, 유턴, 비상정지, 갓길정차, 주차 등에 세부적인 주변 환경에 대한 판단을 수행한다.

  - 제어는 차량간 또는 인프라와의 주행 정보 교환을 근거로 운전자에게 경고 및 정보를 제공하여 핸들조절, 가속, 감속, 급제동 등의 차량을 제어하며 주어진 경로 추종을 위해 조향, 가감속, 기어등 액츄에이터를 제어하는 것을 말한다.

  - 상호작용은 차량과 운전자 및 외부환경과의 정보를 교환하는 기술로 V2X(Vehicle to Everything) 통신을 통해 인프라 및 주변차량과 주행정보를 교환하여 보이지 않는 전방의 교통상황, 위급상황, 사고 등의 정보를 획득하고 HVI를 통해 운전자에게 경고 및 정보제공하고 운전자의 명령을 입력하도록 기능한다.

- 이러한 핵심적인 기술의 진보를 위한 요소 기술들인 1) 센서, 2) V2X통신, 3) 고정밀 디지털지도, 4) 인공지능 5) 고정밀 위치측위, 6) HVI기술에 대해서 학습한다.

- **라이다(LiDAR: Light Detection And Ranging)**

  라이다는 자율주행차의 핵심 센서로 자율주행차의 눈에 해당하는 역할을 한다. 레이저 펄스를 목표물에 비춤으로써 발사한 레이저 펄스와 반사된 레이저 펄스 사이의 시간, 펄스가 발사된 각도, 센서의 절대 위치 등을 사용해 사물까지의 거리, 방향, 속도 그리고 물체의 온도 특성까지 감지를 한다. 라이다는 현재 높은 가격이 단점이지만 자율 주행차의 상용화의 핵심이기 때문에 기술적 진보로 단가가 인하될 전망이다.

- **레이다(RADAR)**

  레이다는 라이다와는 다르게 전자기파를 발사하여 반사된 신호를 분석하는 일명 도플러 효과 이용하는 센서이다. 레이다는 움직이는 물체와 거리, 높이, 방향, 속도 등 주변 정보를 획득하는 센서로 단거리, 중거리, 장거리 특성을 모두 갖추고 날씨에 무관하게 동작하는 장점이 있다. 따라서 레이더는 적응형 순항제어 장치에 활용되어 차량의 200m 전방을 주시하며, 차량을 추적하면서 차량의 가감속을 지령해 차량 사이의 간격을 유지하거나 사각지대와 차선이탈을 감지하여 경보를 울리는 기능을 제공하기도 한다. 레이다는 정지 물체를 추적할 수 없고 금속이 아닌 다른 재질의 물체를 감지하기 힘들기 때문에 라이다와 그 역할을 나누어 활용된다.

- **카메라**

  카메라는 다른 센서에 비해 높은 해상도로 대상 물체에 대한 형태인식 정보를 제공한다. 즉 정확한 배경과 물체 인식이 가능하다. 하지만 빛의 반사를 이용하므로 주변 환경에 크게 영향을 받는 단점도 있다. 카메라는 차선, 표지만, 신호등 등의 정보를 판독하는데 기여한다. 예를 들어 고정된 도로 표지판의 경우에는 GPS와 도로 지도의 정보를 바탕으로 인식 가능하지만 긴급 도로공사 현장에서의 임시표지판 경우에는 카메라를 활용하여 그 내용을 인식한다. 또한 색상을 인식할 수 있어 신호등이나 브레이크 등을 판단하기에 적합하다. 3D 카메라의 경우에는 렌즈를 두 개 사용하거나 다른 센서의 도움을 받아 일반 카메라가 인식하지 못하는 깊이를 인식한다.

- **초음파(Ultrassonic) 센서**

  초음파 센서는 음파(50 KHz 주변 초음파)를 보내 되돌아오는 반향을 듣는 장비로 음파가 미치는 주변 지역에 위치하는 물체를 감지한다. 잡음과 반사파 반향으로 인해 정밀하지는 않지만 보조적인 수단으로 활용된다. 예를 들어 일반 차량에서는 주로 후방 감지 센서와 측면 감지 센서로 사용되고 자율주행차의 경우에는 저속에서 벌어지는 근접 이벤트 즉, 병렬주차와 저속충돌회피를 감지하기 위해 사용된다. 하지만 차량이 사람이 걷는 속력보다 빠르게 움직일 경우 탑재된 초음파 센서는 제대로 동작하지 않는다.

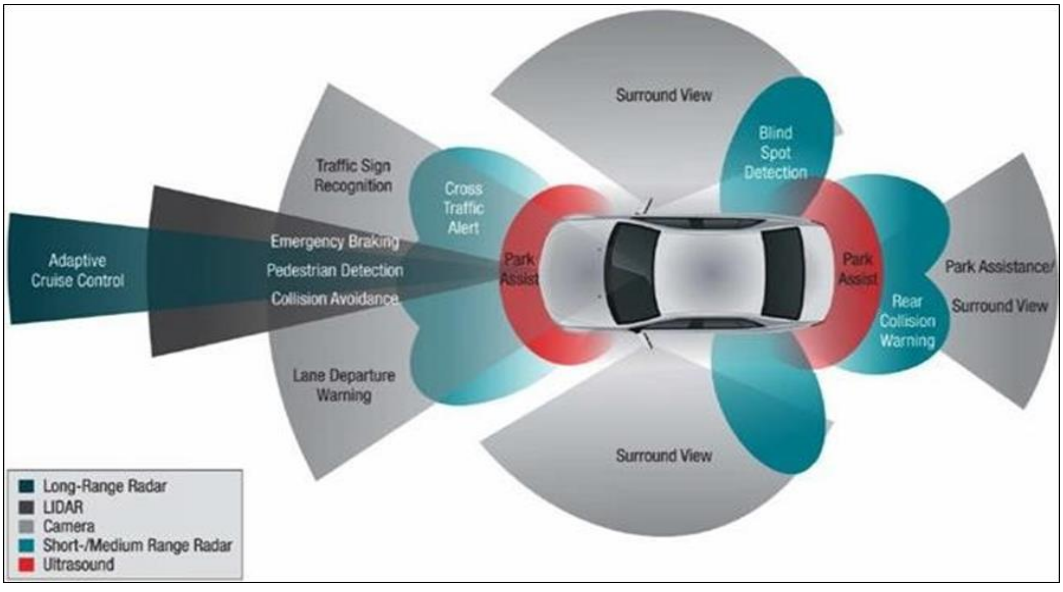
- **적외선 LED와 광센서**

  적외선 LED와 광센서는 비를 탐지하여 와이퍼를 동작시키는 것과 같은 분야에 사용된다. 또한 충돌회피를 위해 차량 외부에 장착돼 상향등의 조명 범위를 벗어난 물체를 감지하기 위해 사용되기도 한다. 아울러 에어백의 전개 속력을 조절하기 위해 탑승자의 위치를 파악하거나 운전자의 눈꺼풀을 감지해 졸음운전을 막기 위해 사용될 수도 있다.

- **고정밀 디지털지도 및 고정밀 위치측위**

  자율주행차의 원활한 주행을 위해서는 고정밀 디지털지도가 필수적이다. 고정밀 디지털지도는 자율주행차의 운행 도로에 대한 모든 정적정보를 3차원으로 표현한 지도로 도로에 위치하고 있는 물체의 위치, 형태 등의 정보를 바탕으로 자율주행차가 커브, 교차로 합류 등에 사전 대응을 할 수 있도록 한다. 기존 디지털 지도보다 10배 이상의 정확도를 갖어 실제 도로와의 차이가 10cm 수준이다.

  아래 그림은 자율주행차에서 활용되는 각종 센서의 부착위치와 그 역할을 도시한 것이다. 센서별로 거리특성, 환경 특성, 해상도, 색상 인식 등이 다르기 때문에 센서 간의 상호 보완적으로 기능 수행한다.



[자율주행차의 각종 센서의 역할]

- **V2X(Vehicle to everything)통신**

  V2X 통신은 자율자동차가 주행하는 동안 주변의 인프라 및 다른 차량과 통신을 통해 정보를 교환하고 공유하는 시스템이다. 기존 교통시스템와 연계하여 실시간으로 교통정보를 제공하고 교통 트랙픽을 관리할 수 있도록 지원한다. 또한 교통정보나 위험정보를 공유하여 전방의 도로상황을 자동차 스스로가 인지하도록 하여 전방의 위급상황과 같은 안정성 제고를 위해 필수적인 시스템이다. 따라서 차량의 고속주행 속에서도 안정적인 높은 패킷전송율과 낮은 지연율을 요구하기 때문에 차세대 이동통신인 5G 서비스가 필수적이다.

  V2X통신 기술의 종류로는 차량간 통신인 V2V(Vehicle to Vehicle), 차량과 인프라 통신 V2I(Vehicle to Infrastructure), 차량과 보행자 간의 통신인 V2P(Vehicle to Pedestrian), 차량과 네트워크와의 통신인 V2N(Vehicle to Network) 등이 있다(그림 참조).

- **사람-차량 인터페이스(HVI: Human Vehicle Interface) 기술**

  사람-차량 인터페이스 기술은 운전자에게 차량 관련 정보들을 최적화된 상태로 제공하는 이용자 인터페이스(UI: User Interface) 기술로 운전자와 자율주행차 간의 상호 작용에 활용된다. 운전자의 특성과 성향, 운전자의 상태 및 차량 내부와 외부 상황을 종합적으로 분석하고 판단하여 운전자의 성별이나 연령별로 최적화된 이용자 인터페이스를 제공하여 자율주행자동차의 주행안전성, 편의성, 수용성(불안감 해소) 등을 향상시키는 역할을 한다.

- **전방표시장치(HUD: Head Up Display)**

  전방표시장치는 운전자의 안전과 편의성을 높여 주기 위한 자동차 전자장비 기술로 차량 주행에 필요한 정보를 자동차 앞 유리에 표시한다. 고속 운전 시 운전자가 시선을 돌리지 않을 수 있도록 안전을 확보하는 역할 등을 한다.

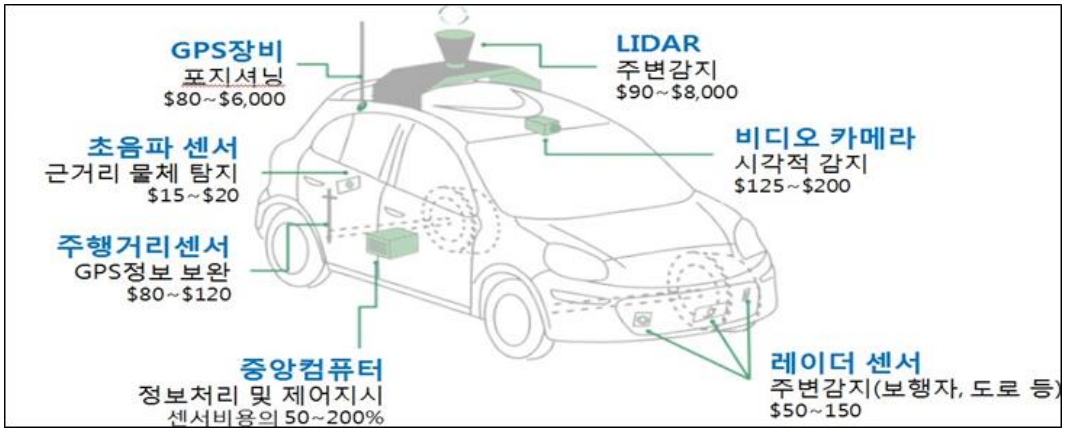
자율주행자동차 확산 전망

- 레벨4의 완전 자율주행자동차의 상용화는 2020년 전후로 전망해 기술적 완성은 낙관적인 상황이다. 자율주행차의 확산을 전망하기에 앞서 기존 차량에서 자동변속기, 에어백, 하이브리드 시스템 등 자동차 신기술이 개발되어 확산되기까지의 과정을 살펴보면 자율자동차의 확산을 이해하는데 도움이 될 것 같다.
- 즉 자동차 관련 새로운 기술이 완성되어 관련 법규를 제정하고 시장으로 확산도기까지 약15년 ~ 30년 가량 소요되고 있다. 예를 들어 자동변속기는 1930년 발명 이후 1980년까지 안전성 검증에 시간이 소요되어 현재는 중저가 차량에서부터 고급차 시장까지 고르게 분포된 것이다. 에어백의 경우도 1973년 시장에 소개된 이후 대중차량에 적용되기까지 약 15년이 소요되었고 1998년이 되어서야 미국에서는 의무장착 법규가 마련된 것이다. 아래의 표에는 자동차의 신기술이 개발되어 확산되는 과정을 정리한 것이다.

기술	확산주기	평균추가비용	시장채택률
에어백	25년 (1973~1998)	U$수백	100% (의무장착)
자동변속기	50년(1940~1990)	U$1,500	미국 90%, 기타 50%
내비게이션	30+년(1985~2015+)	U$500(빠르게 하락 중)	불확실, 약 80%
GPS 서비스	15년	연간 U$150	2~5%
하이브리드기술	25+년(1990~2015+)	U$5,000	불확실, 약 4%

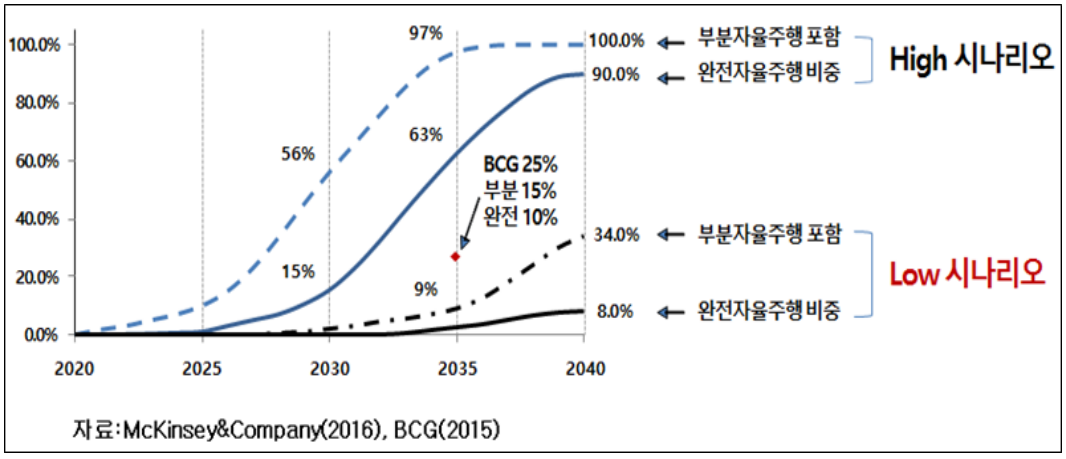
자료: Victoria Transport Policy Institute(2015)

- 그럼 자율주행자동차의 확산 전망은 어떨까? 기존 자동차에 자율주행 기능을 구현하기 위한 핵심장비로는 여러 대의 카메라, 센서, 그리고 고가의 라이다가 핵심이다. 이러한 장비를 추가하는데 드는 비용은 현재 10만 달러 수준이다(그림 참조). 구글의 자율주행 시스템의 경우에도 구축비용은 기존 차량에 5만 달러 이상이 추가되어야 한다. 이러한 자율주행차의 보급이 확산되려면 추가 장비 비용이 1만 달러로 낮춰져야 가능하다고 전망을 하고 있다. 즉, 보급 확산이 가능한 시점을 앞으로 10년으로 전망하기도 한다.



[자율주행차 주요 장비별 비용 예시]

- 아울러 자율주행자동차가 확산되기 위해서는 소비자의 인식전환, 기술의 경제성, 안전성 입증과 관련 법규 제정이 필요하기 때문에 조사기관에 따라 '빠른 확산(High)'과 '더딘 확산(Low)' 시나리오로 접근하고 있다.



- 한편 자율주행자동차의 확산 전망을 기업 대 기업(B2B) 시장에서 먼저 열린 것으로 전망한다. 초기 상용화 될 자율주행차의 경우에는 비싼 가격대로 자율주행차가 형성되어 일반 고객은 소극적 구입 의지를 보이기 때문에 B2B시장에서 먼저 시작하여 규모의 경제가 형성되면서 낮은 판매가가 가능한 시점에서 소비자를 대상으로 시장이 열릴 것으로 본다.

자율주행차에 의한 긍정적 변화

- **안전성 향상**

  자동차 사망 사고의 대부분이 판단실수 등 운전자의 부주의에 기인하는 것으로 분석되고 있다. 미국에서만 연 3만3,000여 명, 중국에서는 연 26만 명, 한국에서는 4,621명(2015년)이 자동차 사고로 사망하고 있다. 미 교통안전국(NHTSA)의 분석에 따르면 미국에서 발생한 교통사고는 94%가 운전자에 기인하였고, 차량의 기계적 결함은 2%이하로 나타났다.

- **안전성 향상**

  따라서 모건 스탠리는 자율주행시스템이 사람의 실수 가능성을 막아주어 연간 3만 여명 생명을 구하고 4,880억 달러의 자동차 사고처리 비용을 절감할 것으로 추산하고 있다.

  구글 자율주행자동차의 경우에는 지난 6년 동안 17건의 경미한 사고를 기록했는데 발생 사고 대부분 사람이 개입한 시점에서 발생하였거나 상대방의 실수에 의한 사고로 자율주행 인공지능시스템으로 다양한 상황에 노출될수록 더욱 완전해져 자동차 사고는 더욱 줄어들 것으로 예상하고 있다.

- **편의성 향상**

  자율주행차에서는 차량이동 중에도 다른 생산적인 일을 할 수 있는 자유가 주어진다. 하루 평균 1~2시간 소요되는 출퇴근 시간동안 차 안에서 업무를 보거나 휴식을 취할 수 있어 생산성이 향상되는 효과가 있다. 또한 시각장애인 등 장애인, 운전면허를 보유하지 않은 잠재수요자까지 혜택을 돌아가고 소외계층인 장애인, 미성년자 등도 차량 이용에 대한 불편을 해소할 수 있을 것으로 전망한다.

[시각장애인의 자율주행차 탑승]

[자율주행 중 생산성 업무 가능]

- **교통정체 해소 및 완화**

  교통정체에 따른 경제적 손실은 국내는 2012년 기준 약 30조 3,000억 원의 혼잡비용이 발생(교통연구원)하였고 미국은 연간 500억 달러(약 56조원)로 추산하고 있다. 교통정체의 원인으로는 병목구간이나 합류점, 교통법규 미준수 등이 손꼽히는데 자율주행차량의 경우에는 경로 및 목적지 정보 공유 등의 효율적 교통분산으로 교통정체를 해소하거나 완화할 것으로 예상한다.

  예를 들어 차량간격을 촘촘히 유지하며 주행하는 군집운행(Platooning) 기술의 경우 현재는 1.6km 길이의 도로에 200대의 차량이 약 60km/h로 주행한다면, 군집운행을 한다면 같은 도로에서 320대의 차량이 100km/h로 주행이 가능하여 고속도로 인프라 활용도를 증가시킬 수 있다.

  또한 도심의 주차난을 해결해 줄 것으로 기대한다. 즉, 자율주행택시를 이용하거나 자택 주차장으로 차를 돌려보내는 테슬라의 소환(summon) 기술을 이용하게 되면 도심의 주차난을 해소할 것으로 보고 있다.

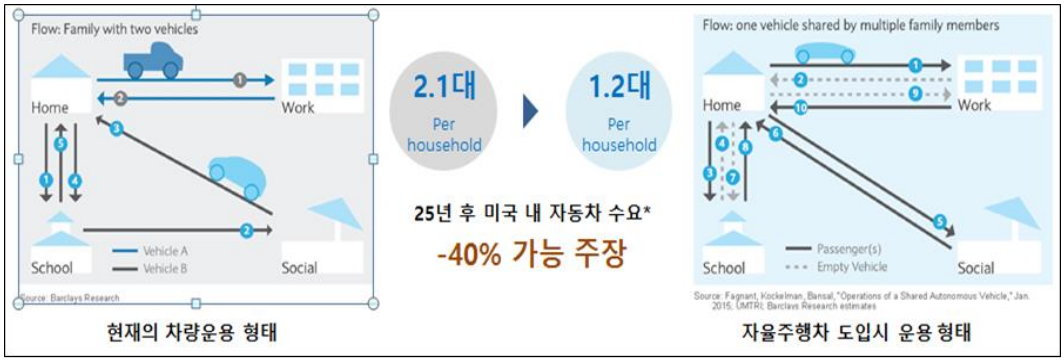
잠깐!

군집운행 기술: 여러 대의 차량이 좁은 간격을 유지하며 열차가 움직이는 듯 하나의 몸체처 럼 주행하는 기술

소환(summon) 기술: 자동주차, 출차 기능

친환경성 향상

친환경성의 향상은 공유경제 효과에 기인한다. 미국교통연구원(TRB)에 따르면 공유차량이 한대 증가하면 약 15대의 신차구매 억제효과가 있어 자동차 소유가 감소할 것으로 전망하고 있다. 즉, 자율주행차와 공유차 기업인 우버가 만나면 현재 택시보다 저렴한 비용으로 차량소유 동기가 약화되고 효율적 운행으로 연료사용과 온실가스배출이 줄어들 것으로 보고 있다. 미국 1가구당 평균 2.1대를 운용하던 자동차 대수가 이론적으로 1.2대로 줄여 운용할 수 있다는 연구도 발표되고 있다. 아래 그림은 자율주행차에 의한 가구당 소유대수 축소 효과를 도시한 것이다.



자료: Fagnant, Kockelman, Bansal, ,Operations of a Shared Autonomous Vehicle', UMTRI(2015)

자율주행차의 극복 과제

기술적 한계

구글의 자율주행차 등 현재 기술의 한계에 대해서는 인정하고 있고 수년 내 해결하는 것을 목표하고 있다. 즉, 폭설, 폭우 등 악천후 환경 주행에는 어려움이 있고 사람의 수신호 인지, 사물의 유형구분(예. 돌과 종이박스) 등은 아직 극복해야 할 대상인 것이다.

자율주행차 안전사고 극복 노력

자율주행차의 시범운행에서 안전사고가 발생하면서 자율주행차의 안전에 대한 불신이 적지 않다. Google(Waymo), Tesla, Uber 등이 기업에서 자율주행차의 시험 주행거리가 증가하면 서 인명사고도 발생하고 있는 것이다. 예를 들어 Tesla의 자율주행 모드에서 발생한 2016년 5월의 첫 사망사고는 차량이 전방의 백색 트레일러를 인식하지 못하면서 발생한 충돌사 고로 인한 것이다. 아래의 표는 자율주행차 시험운행 중 발생한 사고 현황이다.

2016년	2월, Google – 차선 변경 중 버스와 접촉사고 발생
	5월, Tesla – 교차로에서 전방의 백색 트레일러를 인식하지 못하여 충돌
	9월, Tesla – 공사구간에서 유도차선 인식 실패로 사고 발생
	Google – 교차로 진입 중 정지신호를 무시한 상대차량에 의해 사고 발생
	10월, NuTonomy – 차선변경 중 트럭과 충돌
	12월, Uber – 자율주행 중 도로 옆 바리케이드를 들이받는 사고
2017년	3월, Uber – 자율주행 중 옆 차선 차량과 접촉 후 전복

- **사고에 대한 책임과 기계 윤리**

  2016. 5월 미국 플로리다 테슬라 자동차 사고가 발생하였다. 오토파일럿(자율주행) 중 대형 트레일러를 인식하지 못하고 발생한 충돌사고는 첫 사망사고로 많은 논란이 점화되었다. 그 사건으로 독일에서는 자율주행차량을 대상으로 블랙박스의 설치를 의무화하였고, 중국에서는 실 도로 상에서 주행테스트를 금지하는 등의 조치가 이어졌다. 자율주행차의 추가적 사고에 대한 우려로 주요국에서는 법규 마련에 많은 고심을 하고 있다.

  또한 사고위험의 순간 핸들의 방향에 대한 선택권 논란이 발생하였다. 의사결정을 '인공지능이 해야 한다'와 '사람이 해야 한다'가 맞서고 있는 가운데 대중은 여전히 사람이 결정해야 한다는 의견이다. 그것은 10명의 보행자와 1명의 탑승자 가운데 누군가 희생되어야 하는 사고 상황에서 탑승자를 희생하도록 기계윤리가 프로그래밍된 차에 대한 소비자의 선택은 무엇일까?

- **트럭, 택시 운전사 일자리 감소**

  차량 공유서비스인 우버 택시가 등장하면서 택시업계 등에서 반발이 거세다. 무인차량이 상용화되면 트럭이나 택시 등 관련 일자리가 급감할 것이라는 우려이다. 하지만 미국의 로컬모터스는 3D 프린팅된 자동차 생산으로 유명한 기업인데 워싱턴 DC에 '올리'라는 무인주행버스를 시범운행 중으로 대중교통 무인화를 선도하고 있으며 우버는 자율주행차와 차량공유를 결합한 개념을 실현하고자 지속적인 노력을 하는 등 기존의 대중교통수단을 위협할 전망이다.

[IBM Watson 인공지능 시스템을 이용한 로컬 모니터 'Olli' 무인버스]

- **역효과와 역차별**

  자율주행차의 상용화로 자동차가 대수가 증가하고 그로인해 교통 혼잡도도 높아지는 역효과를 우려하는 의견도 있다. 자율주행차의 편의성과 경제성 혜택이 노년층, 장애인, 미성년자로 확대되면서 기존 대중교통에 대한 이용 수요를 크게 흡수하여 교통량이 증가할 것이라는 주장이다.

  초기 자율주행차와 일반차량이 혼합주행하는 상황이 전개되면서 복잡성이 증가할 것이라는 분석도 있으며 기계에 대한 과신으로 탑승자가 위험상황에 대해 무감각해지는 리스크 오프셋 현상도 발생할 것으로 전망한다. 한편 자율주행시스템을 선택하지 않은 경우 집단주행(플래툰) 자율주행차량들 틈 사이에서 운전해야 하는 운전자에 대한 역차별이 발생한다는 비판도 있다.

- **사생활 침해와 보안 취약성**

  자율주행차의 대표적 적용분야인 카셰어링의 경우는 탑승자의 동선이나 개인정보 등이 노출되기 쉬운 환경이다. 개인적 공간으로 익숙한 자동차가 공용화되면서 실내 카메라 촬영, 동선기록 등으로 인해 사생활 노출로 반감이 존재할수 있다.

  또한 시스템 오류나 해킹에 대한 취약성도 우려된다. 자율자동차도 일종의 인터넷 기기로 간주할 수 있기 때문에 통신장애나 시스템 오류에 취약할 수밖에 없다. 즉 자율주행기술은 교통체계, 전자지도, 차량간 통신이 동반되어야 안전한 시스템이다. 2016. 7월 미국 국가안보국(NSA)출신의 해커가 PC를 이용해 원격으로 일반 차량의 와이퍼와 핸들을 조작하는 시연이 벌어지면서 실제 차량의 리콜사태로 연결되기도 하였다.

02. 자율주행차와 사이버 보안

- 최근의 자동차는 컴퓨터 네트워크화 돼가고 있다. 커넥티드 카에서 발전한 자율주행차는 여러 차원에서 다양한 방향으로 통신이 가능하다. 온보드 통신은 자동차 내 계기반, 엔진 제어 유닛, 스티어링이나 제동에 관련된 장치들을 비롯해 다양한 제어장치 간의 정보교환을 가능하게 한다. 외부와의 통신을 사용해 운전자에게 교통체증에 관한 정보나 사고를 예방할 수 있는 정보를 알려줄 수 있다. 클라우드로 접속할 수 있음으로써 현장 소프트웨어 업데이트, 원격진단, 응급호출(eCall), 지불 시스템, 인터넷 서비스, 인포테인먼트, 교통정보, 앱 등과 같은 새로운 서비스들이 가능하다.즉 자율주행차는 다양한 서비스를 안전하게 제공하기 위하여 다수의 인터페이스와 게이트웨이가 포함되고 그에 따라 자동차 내에서 외부 세상과 접촉하는 이들 지점을 보호하는 포괄적인 보안 아키텍처가 필요하게 된다.

침입 경로

- 자동차는 크게 자동차를 직접 움직이는 구동부, 이를 제어하는 전자제어장치(ECU: Electronic Control Unit), 외부와 연결할 수 있는 인포테인먼트(Infotainment) 시스템으로 구분된다. 자동차에서 작은 컴퓨터라고 불리는 전자제어장치는 외부와 연결되지 않고 차량 내부 네트워크에서 운전자의 명령을 수행하는 전장 부품으로 운전자가 방향전환을 위해 핸들을 돌리면 해당 ECU 정보가 차체에 전달되고 바퀴에 명령을 내려 부드럽게 돌아가게끔 하는 운전자 명령을 수행한다.

- 이와 같은 ECU간 정보의 전송 및 교환은 CAN(Controller Area Network) 컨트롤러를 통해 이루어지며 차량에서 전기적으로 제어되는 다양한 부품으로 컴퓨터의 고속도로 역할을 한다. 따라서 CAN에 진입할 수 있기만 한다면 각 시스템을 제어하는 전자 메시지를 찾아낸 뒤, 변조된 메시지를 전송해서 브레이크, 변속기 등 핵심 부품을 원격으로 제어하는 것이 가능해진다. 이로 인해, CAN에 진입해 ECU 영역을 장악한 공격자는 자동차를 급발진 시키거나 브레이크 페달을 무력화 시키는 조작을 할 수 있다.
- 그렇다면 차량 내부의 네트워크에는 어떻게 진입할 수 있을까? 커넥티드 카와 외부는 V2X(Vehicle to Everything) 네트워크로 구성되며, V2X 네트워크에는 V2V, V2I, V2N으로 나눠진다.
- 차량과 차량 사이를 연결하는 차량 간 무선통신 V2V(Vehicle to Vehicle) 기술은 자동차의 통신제어장치를 통해 근처 차량의 위치파악, 속도 정보 등을 공유한다. 이러한 자동차와 자동차 사이의 통신은 교통사고를 예방하고 안전한 주행을 할 수 있게 하는 시스템으로 각광받고 있다.
- 차량과 도로 인프라 간 통신 V2I(Vehicle to Infrastructure) 기술은 도로 곳곳에 차량 내에 설치된 통신 단말기와 상호 정보를 교환할 수 있는 노변 장치와 일종의 기지국을 설치하여 차량으로부터 주행 정보들을 수집하고, 이를 중앙 서버에서 분석하여 교통상황 및 대처 방법, 빠른 길 안내 등 각종 서비스를 제공받는 기술이다.
- 뿐만 아니라, 운전자에게 멀티미디어 콘텐츠 등 부가가치 서비스 또한 제공한다. 차량과 모바일 기기 간 통신 기술 V2N(Vehicle to Nomadic device)은 차량 내의 네비게이션 시스템 같은 기기들과 스마트폰, 스마트패드 등 모바일 기기를 연결한 기술이다. 차량의 상태 파악이나 원거리 차량 관리의 기능을 제공하고 있으며 향후 모바일 OS를 통해서 더욱 편리한 서비스 발전이 예상된다.
- 이와 같은 차량과 모바일기기를 연결하는 인포테인먼트 시스템을 통해서 공격자는 차량의 내부 시스템에 접근할 수 있다. 블루투스를 통해 다운 받은 파일들이 충분히 검증되지 않았을 경우 자동차 내부 시스템에 영향을 줄 수 있는 악성코드가 설치 될 수 있으며, 차량 내 AVN(Audio, Video, Navigation) 시스템도 공격의 예외는 아니다. CD 등을 통한 펌웨어 취약점 공격과 GPS나 위성 라디오 채널을 통한 해킹에도 쉽게 노출 될 수 있다.

자율자동차의 보안 위협과 보안 기술

자율자동차 보안 위협

자율자동차에 대한 사이버 보안의 중요성은 갈수록 커가고 있다. 자동차 임베디드 시스템에 대한 해킹은 일반 PC와 달리 OS나 애플리케이션이 동작하지 않거나 데이터 삭제 정도의 피해가 아니라 최악의 경우 사망에 이르는 등 안전성에 커다란 위협이 된다. 특히 자율주행차의 특성상 연결성의 증대는 자동차의 보안 취약성과 쉬운 공격 지점의 증대로 이어지게 된다. 예를 들어 최근의 차에는 ECU가 차 당 70개 이상 들어가고 카 메이커들은 테슬라 모델S처럼 SOTA(Software Over-The Air), FOTA(Firmware Over-The-Air) 서비스, 텔레매틱스 원격 서비스, V2X 기능이 일반화되면서 알려지지 않은 취약점이 증가하게되고 그로인한 위협도 함께 늘어나게 된다.

- **자율자동차 보안 위협**

  자율자동차의 안전성에 영향을 미치는 보안위협은 일반적으로 사용자 조작 미숙으로 인한 보안위협과 해커에 의한 보안위협으로 구분할 수 있다.

  사용자 조작 미숙으로 인한 보안 위협은

  - 부적절한 세팅: 사용자의 인포테인먼트 기능 사용시 의도하지 않은 서비스 제공자에게 개인 식별 정보 등이 전송되거나 통신 내용이 유출
  - 바이러스 감염: 인포테인먼트 디바이스 장치의 바이러스에 감염된 콘텐츠가 차량 내 LAN에 유포되어 차량에 탑재된 다른 기기를 감염

- **해커에 의한 보안위협**

  인가되지 않은 사용: 정비공장 /유지보수 담당자를 해킹한 후 외부 공격자가 차량 전자기기에 접속하여 차량운행을 조작

  인가되지않은 설정: 장비의 패스워드/암호화 설정 등이 취소되어 차량 상태정보가 해커에게 자동으로 전송되거나 ECU나 차량내 장비가 오작동

  비 인가 정보 접근: 해커가 부적절한 세팅이나 취약점을 악용, 차량내 프로그램, 콘텐츠, 운행 기록 등을 확인

  스니핑(정보도청): 평문 전송되는 TPMS(타이어 압력 관리 시스템) 메시지 등은 타이어의 시리얼 번호 등을 포함하기 때문에 자동차와 특정 개인을 연결가능하여 운전자의 프라이버시를 침해할 수 있음

  서비스 거부공격: 자동차 텔레메틱스/원격 제어와 관련된 포트에 대량 패킷을 전송하여 자동차의 원격제어를 방해

  메시지변조: TPMS 메시지 등의 변조를 통하여 이상알림 게기판을 조작하여 자동차의 안정적인 운행을 방해하는 침해 발생

  로그삭제: 시스템의 로그를 삭제하거나 변경하여 침입 흔적 삭제하고 또는 로그가 기록되지 않도록 설정할 수 있음

  무단 릴레이: 스마트키 용 LF(Long Frequency) 주파수 대역에 해커가 침입하여 원격지에서 차량 문을 개폐 가능

- **자율자동차 보안 기술**

  자율자동차 보안에 대해 꼭 알아야 할 핵심기술과 그 판단기준을 간략히 학습하기로 한다. . 이는 단지 자동차업계 종사자에게만 필요한 정보가 아니다. 자율자동차 보안 기술은 누구나 알아야 할 기술이다. 자율자동차는 탑승자와 보행자를 가리지 않고 인간의 생명과 직결된 아주 위험한 물건이므로, 자율자동차 보안은 다른 어떤 분야 보안보다 훨씬 더 중요하다. 자율자동차 보안의 실패란, 사람의 목숨이 걸린 일이기 때문이다.

- **어플리케이션 방화벽(AFW: Application Firewall)**

  자율자동차용 AFW는 자율자동차 통신 프로토콜에 최적화된 어플리케이션 방화벽이다. 차량 외부에서 유입되는 악성 통신뿐 아니라 차량 내부에서 발생하는 비정상적 통신 내용까지 모두 분석하고 대응한다.

- **어플리케이션 방화벽(AFW: Application Firewall)**

  통신 내용의 논리를 분석하여 기존 공격 외 변종 공격과 아직 정체가 밝혀지지 않은 새로운 공격까지 탐지하고 방어하는 지능형 엔진 탑재 여부가 AFW의 가장 중요한 판단기준이라 할 수 있다.

- **자동차-사물 통신(V2X)**

  V2X는 차량과 차량 소유자와 관련된 모든 민감한 정보를 총망라하는 통신이기 때문에, V2X 기술의 핵심은 사용자 인증과 데이터 암호화 시스템이다. 그리고 자동차는 산업의 특성상 한 나라 내수시장에서만 판매되지 않고 세계시장을 고려해 제작되어야 하기 때문에 국제표준규격 준수가 핵심이다.

- **암복호화 키 관리 시스템(KMS: Key Management System)**

  KMS는 인증서를 포함한 암복호화 키의 생성과 폐기 등 키의 생애주기별 관리 및 안전한 보관을 위한 시스템이다. 외부통신뿐 아니라 차량 내부 ECU(Electronic Control Unit) 통신을 위한 키 관리 및 안전한 저장, 접근제어 및 권한 관리를 통한 키 오남용 및 도용 방지 등의 기능을 맡아 자동차통신 체계 전체를 안전하게 유지한다.

- **공개키 인프라(PKI: Public Key Infrastructure)**

  PKI는 차량용 인증서를 생성하고 운영하고 관리하며, 교통관리 시스템은 PKI를 통해 각개 자동차의 존재를 공적으로 인식한다. PKI에는 운전자의 프라이버시를 보호하기 위한 익명화 기술을 포함하고 있다. 차량용 PKI는 국제표준인 IEEE1609.2에 따라 경량화된 시스템으로 성능이나 효율 문제는 없는지를 판단해야 한다.

- **지능형 교통시스템(ITS: Intelligent transportation system)**

  ITS는 주행 중인 차량이 교통 인프라와 통신하며 주변 교통상황을 파악하고 앞 차량 급정거나 도로 낙하물 등 위험 정보를 실시간으로 확인함으로써 교통사고를 예방하는 등, 위 PKI와 더불어 공적 개념의 인프라 기술이다. ITS는 국가 차원의 아주 거대한 시스템으로 자동차 관련 거의 모든 기술이 총동원되기 때문에 가장 중요한 것은 무조건 신뢰성이다. ITS 체계가 무너진다는 것은 자연재해 수준의 아주 심각한 문제다. ITS 기술의 핵심은 인증관련 서버 기술이고, 이러한 기술들이 앞서 이야기한 PKI 체계와 어우러져 전체 ITS의 중심을 이룬다.

- **자동차 물리보안**

  앞서 학습한 기술들은 모두 다 ICT 기술이다. 하지만 가장 큰 위험은, 자동차 자체다. 이런저런 수법들보다 자동차를 직접 조작해버리는 게 가장 간편한 해킹 방법이기 때문이다. 대부분의 차량에는 차량정보 수집장치인 'OBD(On-board Diagnostics)' 단자가 설치되어 있다. 문제는 OBD를 통해 쉽게 자동차 관련 정보를 수집할 수 있고 나아가 자동차가 오작동하도록 조작할 수도 있다는 점이다. OBD는 차량 내부에 있어서 차주 외에는 쉽게 접근할 수 없다고 가정하기 때문에 차문 개폐장치 외에는 따로 특별한 보안조치가 없다. 더 큰 문제는 이렇듯 OBD가 부실하게 관리되고 있음에도 불구하고 OBD에 연결되는 기기의 수가 점차 늘고 있다는 사실이다. 곧 실용화될 자율주행 관련 장치 또한 OBD에 연결될 것이다. 해커 입장에서 보자면 무선통신을 이용한 해킹보다 OBD를 직접 노리는 해킹이 훨씬 더 효율적이다.