

# 2022 전략트렌드

## 자율주행차

2022 Insight Into Technology and Standard



산업통상자원부  
국가기술표준원

KSA 한국표준협회





## ●● Contents

---

1. V2X 보안 국제 표준화 동향 및 이슈 ..... 1  
■ 한국교통안전공단 자동차안전연구원 **엄성욱** 선임연구원
2. 자율주행 자동차 보안 기술 및 국제표준화 동향 ..... 11  
■ TTA 표준화본부 **강석규** 팀장
3. 자율주행을 위한 정밀도로지도 구축·갱신 및 LDM 기술 현황 ..... 21  
■ 웨이즈원(주) **김동수** 상무
4. NR-V2X 사이드링크 기반 유니캐스트 및 그룹캐스트 통신 ..... 38  
■ KT 융합기술원 인프라DX연구소 **김남규** 전임연구원 · **이석원** 선임연구원
5. 자율주행차 상용화 이슈와 제안 ..... 49  
■ 한국자동차연구원 **이원석** 책임연구원





# V2X 보안 국제 표준화 동향 및 이슈



한국교통안전공단 자동차안전연구원 **엄성욱** 선임연구원

## 1. 서론

V2X 통신을 활용하여 차량과 주변 차량(V2V), 차량과 도로 인프라(V2I), 차량과 보행자(V2P) 간의 연결을 통해 Connected Vehicle을 구성하여, 도로 교통의 안전, 효율성을 높이고자 하는 노력들이 C-ITS(Cooperative Intelligent Transportation System) 분야에서 이루어져 왔으며, 4차 산업혁명의 핵심 분야인 자율주행 분야에서는 V2X 통신을 통해 수집된 정보를 활용하여 자율주행 성능을 높이고, 차량간 의사 전달을 하는 자율협력주행으로 발전하고 있다.

자동차의 연결성 확대는 자동차에 대한 해킹 등의 사이버공격의 리스크를 발생시키며, 이로 인해 운전자와 보행자의 생명과 안전을 위협할 수 있을 것으로 우려된다. 이러한 위협을 방지하기 위한 V2X 보안 기술이 북미, 유럽, 중국 등 각 지역별로 표준화되고, 개발되어 적용되고 있다.

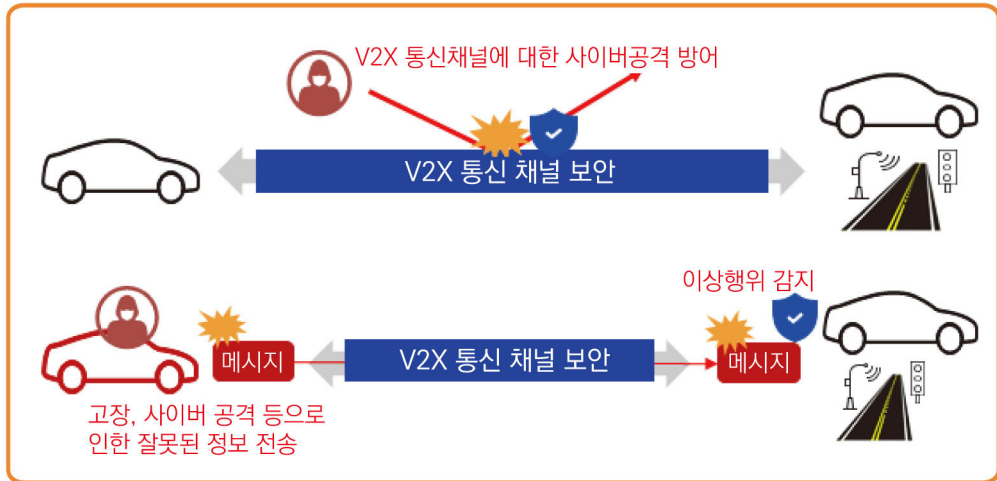
V2X 보안의 핵심 기술로는 V2X 통신보안, V2X 보안인증(SCMS, Secret Credential Management System), V2X 이상행위 관리가 제시되고 있으며, 이에 대해 표준화 및 기술 개발이 활발하게 진행 중이며, 상용화를 위한 다양한 실증사업이 진행 중에 있다.

V2X 통신보안에 대한 대표 표준은 IEEE 1609.2(2016)로 PKI(Public Key Infrastructure)기반 보안규격을 정의하고 있다. V2V, V2I간의 통신보안을 위해 메시지에 대한 전자서명 기법, 암호화 기법, 키 쌍 생성 기법, 해시 알고리즘 등의 보안 기술 규격이 정의되어 있다. 본 규격은 본래 WAVE 통신표준인 IEEE 1609 시리즈의 보안 규격 파트로 개발되었지만, 셀룰러 V2X 역시 별도의 보안표준을 정의하지 않고 보안 기술은 IEEE 1609.2를 그대로 사용하도록 하였다.

V2X 보안인증(SCMS)는 V2X 보안통신에 활용되는 V2X 전자인증서의 생성·발급·유효성 검증 등을 수행하는 전자인증서 관리 시스템과 인증서를 활용한 V2X 보안프로토콜 등을 정의한다. 2016년 미국연방교통부(US DOT)와 CAMP(Crash Avoidance Metrics

Partnership)가 설계한 SCMS를 시작으로 규격이 정의 되었으며 최근 IEEE 1609.2.1로 개선된 표준이 공개되었다.

V2X 이상행위 관리기술은 차량의 고장이나 해커의 사이버공격으로 인해 잘못된 정보(V2X 이상정보)를 V2X 환경에 공유하는 차량을 감지하고, 이에 해당 인증서를 폐지하여 신뢰성 있는 C-ITS 환경을 확보하게 해준다. V2X 이상행위 탐지기준, 이상행위 보고규격 등 관련 규격들이 미국, 유럽 등에서 활발히 표준화 진행 중이다.



V2X 통신보안은 V2X 통신 채널에 대한 보안으로 제3자에 의한 사이버공격으로부터 V2X 통신을 보호해주며, V2X SCMS는 V2X 통신 보안에서 사용하는 차량용(인프라용) 전자인증서를 발급·관리·폐지하는 보안인증체계이다. V2X 이상행위 관리기술은 V2X 보안통신 채널을 통해 전달된 메시지가 비정상적인지 탐지·판단 해준다.

본 문서에서는 표준화가 진행 중인 V2X SCMS와 V2X 이상행위 관리 기술에 대한 북미, 유럽, 중국의 표준화 동향을 알아보려고 한다.

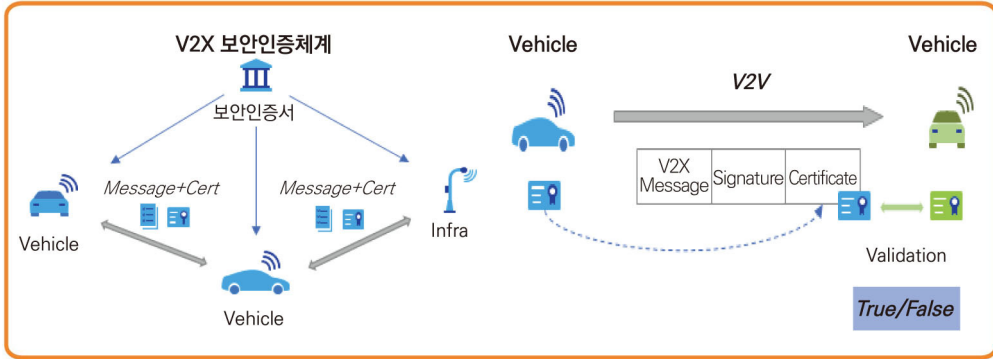
## 2. 본론

### 가. V2X SCMS

#### 1) V2X 보안인증 시스템 개요

신뢰할 수 있는 인증기관이 검증된 차량·인프라 등의 V2X 기기에게 PKI 기반 V2X

전자인증서를 제공하고, 각 검증된 V2X 기기 사이 통신은 메시지와 제공 받은 V2X 전자인증서를 이용하여 상호 통신하며, 각 V2X 기기는 수신받은 메시지에 포함된 인증서의 신뢰 여부에 따라 메시지를 신뢰할 수 있도록 만들어진 체계이다. 북미, 유럽, 중국은 각 지역별로 V2X SCMS를 개발·실증 중에 있다.



## 2) V2X 보안인증 시스템 국제 표준 비교

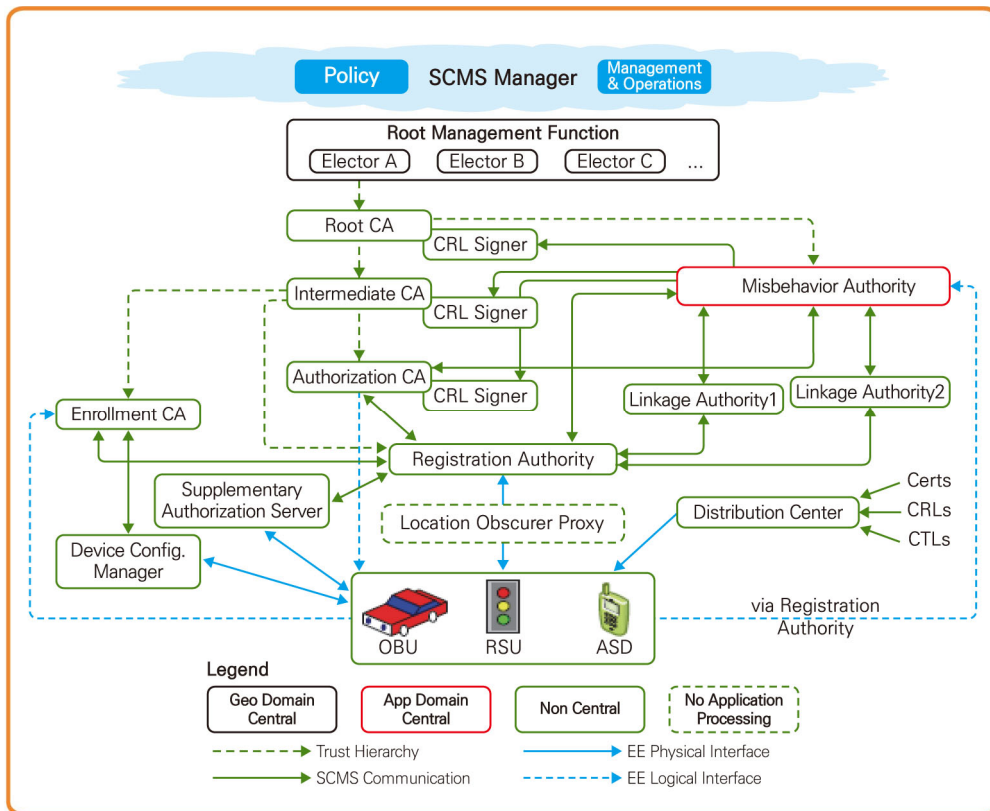
구분	북미		유럽	중국
	CAMP SCMS(2016)	IEEE 1609.2.1.(2021)	CCMS	SCMS
암호화 알고리즘	<ul style="list-style-type: none"> <li>대칭 키 암호 (AES-CCM)</li> <li>해시(SHA-356, SHA-384)</li> <li>전자서명(ECDSA)</li> <li>공개키 암호화 (ECIES)</li> <li>타원곡선 (NIST-P256, Brainpool256)</li> </ul>	<ul style="list-style-type: none"> <li>대칭 키 암호 (AES-CCM)</li> <li>해시(SHA-356, SHA-384)</li> <li>전자서명(ECDSA)</li> <li>공개키 암호화 (ECIES)</li> <li>타원곡선 (NIST-P256, Brainpool256)</li> </ul>	<ul style="list-style-type: none"> <li>대칭 키 암호 (AES-CCM)</li> <li>해시(SHA-356, SHA-384)</li> <li>전자서명 (ECDSA)</li> <li>공개키 암호화 (ECIES)</li> <li>타원곡선 (NIST-P256, Brainpool256)</li> </ul>	<ul style="list-style-type: none"> <li>대칭 키 암호 (SM4)</li> <li>해시 (SM3)</li> <li>전자서명 (SM2)</li> <li>공개키 암호화 (SM2)</li> <li>타원곡선 (SM2)</li> </ul>
Root CA 신뢰 근거	• Elector의 Root CA 서명(Ballot)	• Elector의 유효한 CTL 서명	• TLM의 ECTL 서명	• TRCLA의 TRCL 발급
인증서 종류	<ul style="list-style-type: none"> <li>등록인증서</li> <li>보안인증서 (익명/실명/응용)</li> </ul>	<ul style="list-style-type: none"> <li>등록인증서</li> <li>보안인증서</li> </ul>	<ul style="list-style-type: none"> <li>등록인증서</li> <li>보안티켓(인증서)</li> </ul>	<ul style="list-style-type: none"> <li>(등록인증서, AT)</li> <li>보안인증서</li> </ul>
단말인증서 형태	• Implicit	• Implicit	<ul style="list-style-type: none"> <li>Explicit</li> <li>Implicit</li> </ul>	• Explicit
인증서 발급 정책	• 3년 일괄 발급, 1주 20장	• 3년 일괄 발급, 1주 20장	• 필요 시 요청/발급, 1주 20장	• 미정, 1주 20장 (호환성 테스트 시)
인증서 사용 제어	• CRL에 의한 인증서 폐지	• CRL & ACPC	• 등록인증서 Blacklist 등록	• CRL

구분	북미		유럽	중국
	CAMP SCMS(2016)	IEEE 1609.2.1.(2021)	CCMS	SCMS
단말인증서 교체	<ul style="list-style-type: none"> <li>+1시간 유효기간</li> </ul>	<ul style="list-style-type: none"> <li>Offset, Alternative Offset</li> </ul>	<ul style="list-style-type: none"> <li>+1시간 유효기간</li> </ul>	<ul style="list-style-type: none"> <li>+1시간 유효기간</li> </ul>
최신 현황	<ul style="list-style-type: none"> <li>IEEE1609.2.1. (2020)로 업데이트</li> </ul>	<ul style="list-style-type: none"> <li>각종 오류 수정 한 Revision 예정 (2022)</li> <li>ACPC, SAS, Canonical ID에 대한 명확한 구현 방안 미비 (RevisionDraft에도 누락)</li> </ul>	<ul style="list-style-type: none"> <li>Butterfly Key Expansion 도입</li> <li>BKE 도입 이후에도 인증서 발급 정책은 1주 단위 신청</li> </ul>	<ul style="list-style-type: none"> <li>(중국 각지) 대규모 단말 호환성 테스트 수행</li> </ul>

### 3) V2X SCMS 국제 표준화 동향

- (북미) 2021 하반기 북미 상호호환성 테스트(OmniAir Plugfest)에서 IEEE 1609.2.1 테스트 예정이었으나 연기 되는 등 일정이 지연 중이다. IEEE 1609.2.1. Draft는 2022년 Revision될 계획이다.
- (유럽) 북미 SCMS 개념 일부 도입(BKE 등) 하였으며, 현재 ETSI를 중심으로 표준화가 진행 중이다. 2022 상반기 사이에 대규모 상호호환성 테스트(ETSI Plugtests) 진행 예정이다.
- (중국) C-V2X 기반으로 표준화가 진행 중이고, 각 지역별로 대규모 실증을 진행 중이며, 대규모 상호호환성 테스트(new4layer, 씬스파)에 국내 OEM 및 Global Vendor들이 참여하고 있다(40여개 자동차 업체, 40여개 단말 업체, 10여개 칩 모듈 업체).

#### 4) IEEE 1609.2.1.표준 특징



IEEE 1609.2.1의 정식 명칭은 ‘IEEE Standard for Wireless Access in Vehicular Environments(WAVE) - Certificate Management Interfaces for End Entities’로, 자동차용 전자 인증서를 만들고 관리하는 PKI 인프라에 관해 새롭게 정의한 표준이다. 기존 CAMP SCMS(1.2.2)와 비교하여, 시스템의 가용량 및 효율 향상, 인증기관의 부하 분산을 위해 PKI 기관 구성에 변화가 있으며, 인증관리체계의 신뢰성 및 효율 향상을 위한 신규 기술을 도입하였다. 2020년 12월에 최초 발행되었으며, 2021년 11월 draft 4까지 작성되었다. IEEE 1609.2.1 표준이 확정될 시, 기존 CAMP SCMS(CAMP 1.2.2)와 다르게 채택된 새로운 적용 방식으로 인해, V2X SCMS 운영체제 및 단말 환경에 영향이 있을 것으로 예상되며 기존 CAMP SCMS 관련 규격과 비교하여 나타난 특징은 다음과 같다.

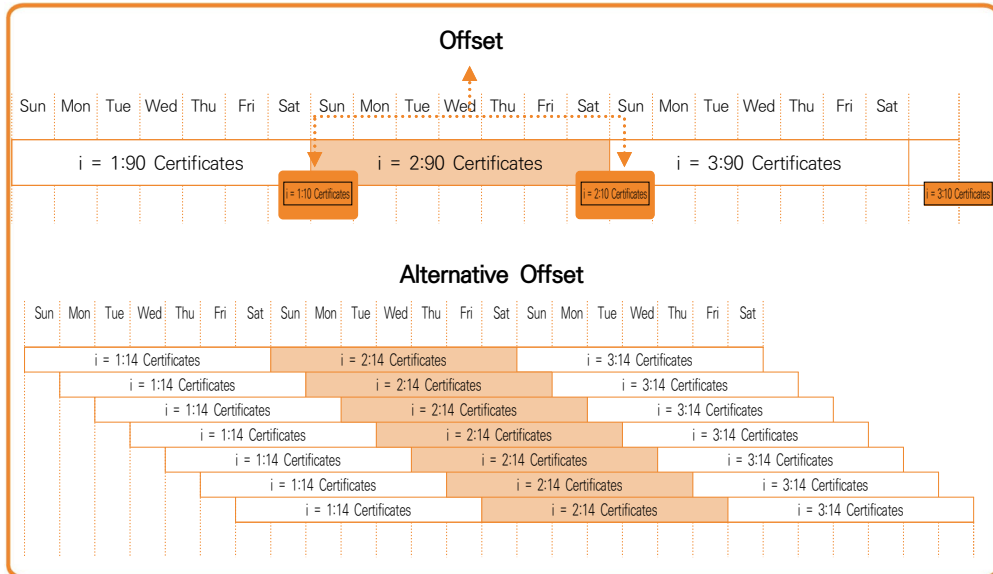
- (CTL 채택) 유럽의 CCMS(C-ITS Security Credential Management System) 체계에서 사용하고 있는 인증서신뢰목록(CTL, Certificate Trust List) 방식을 채택하였다.

- (복수의 CRL Signer 체계) 기존 CAMP SCMS에서는 CRL Generator가 MA, PG 인증서를 제외한 모든 인증서를 폐지하는 기능을 담당하였다면 IEEE 1609.2.1에서는 Root CA, ICA, ACA 등 자신이 발급한 인증서를 각자 자신에 속한 복수의 CRL Signer가 담당하게 되었다. 이 결과 기관의 분리, 차량 증가 등에 따라 CRL Generator에 인증서 폐지를 번번이 요청함으로써 발생할 수 있는 시스템의 비효율성을 개선하였다.
- (PG, CS(Certificate Service) 컴포넌트 제외) CAMP SCMS에서 존재하였던 PG, CS 컴포넌트가 IEEE 1609.2.1 아키텍처에서는 제외되었다.
- (SAS 기능) SAS는 단말이 정상적인 등록인증서를 보유함과 관계없이 비즈니스 프로세스상 추가적인 인증 및 접근통제(access control)가 필요하다고 판단될 시 사용할 수 있는 별도의 보안인증체계로, 단말은 RA에 접근하기 전에 SAS로부터 OAuth2.0에 기반을 둔 인증 서버로부터 별도의 인증 절차를 통해 접근토큰(AT, Access Token)을 획득하고, 해당 토큰의 검증이 완료된 후에야 비로소 RA로의 접근이 허용된다.
- (Distribution Center의 역할) DC는 단말이 아무런 보안 절차 없이도 제공 받을 수 있는 인증서 체인, CTL, CRL을 배포하는 컴포넌트로, RA의 경량화 및 단말 등의 접근성 개선에 기여한다.
- (TLS 외 다양한 보안 프로토콜) 각 layer, 용도별로 다양한 보안 프로토콜(TLS 1.2, TLS 1.3, ISO 21177 등)을 사용할 수 있도록 정의되어 확장성을 도모할 수 있도록 개선되었다.layer 및 용도별 사용 가능한 보안 프로토콜은 아래 표와 같다.

Layer	용도	사용 가능 프로토콜
Application PDU	eeAuth (단말 인증)	none, canonical, authorization, enrollment, X.509 enrollment
Web API	eeAuth (단말 인증)	none, OAuth2.0
Secure Session	eeAuth (단말 인증)	none, physical, ISO 21177-authorization, ISO-21177-enrollment, TLS-X.509
	scmsAuth (기관 인증)	physical, TLS 1.2, TLS 1.3, ISO 21177

- (ACPC, Activation Codes for Pseudonym Certificates) 도입) 폐지된 차량 대수의 증가에 따른 CRL 용량 증가 및 그에 의한 네트워크 부하 및 인증서 검증기간의 증가 문제에 대한 대안으로, IEEE 1609.2.1에서는 ACPC를 이용한 효율적인 인증서 폐지 방식이 제안되었다.

- (신규 보안인증서 교체 방안) 보안인증서 교체 시기에 발생할 수 있는 이상행위 차량의 이상행위 공격 등의 보안 허점을 방지하기 위해, 기존의 Overlap 방식의 익명인증서 교체 방안에 추가로 Offset, Alternative Offset 두 가지 신규 방안이 제안되었다.



- (CSR, Certificate Signing Request 내 권한 설정 도입) 기존 CAMP SCMS에서는 등록인증서의 권한을 그대로 승계할 수밖에 없는 한계점이 있었으나, IEEE 1609.2.1에서는 권한을 부여할 수 있도록 정의되어 등록인증서 한 장당 여러 종류의 보안인증서 발급 및 사용이 가능해졌다.
- (Butterfly Key Expansion 기법 추가) 기존의 Original BKE 기법 외에도 Unified, Compact Unified BKE 기법이 추가되어, 이에 각각 단말과 ACA의 성능 향상이 있을 것으로 예상된다.
- (Canonical ID 추가) 기존 CAMP SCMS의 DCM을 통해 ECA에 등록인증서 요청을 수행하는 방식의 간접적인 등록인증서 발급 방식에 추가로 Canonical ID를 이용한 직접적인 등록인증서 발급 방식을 언급하였다. 이를 통해 향후 등록인증서 발급 과정의 간소화가 가능할 것으로 예상된다.
- (SCMS REST API 버전업) 상기 신규 항목(각 layer 및 용도별 보안 프로토콜의 추가, Canonical ID의 도입 등)에서 필요로 하는 REST API를 추가하여 v2에서 v3로 버전업 예정이다.

IEEE 1609.2.1에는 유럽의 Canonical ID를 이용한 등록인증서 발급 형식을 도입하였고, 반대로 유럽의 CCMS 아키텍처 표준(ETSI TS 103 940, 해당 표준은 본 문서 미포함)은

IEEE 1609.2.1의 BKE를 도입한 것을 토대로, 미국/유럽이 각국의 보안인증체계 간의 상호 호환을 고려하는 방향으로 확장하고 있음을 알 수 있다.

## 나. V2X 이상행위 관리기술

V2X 통신 기반의 자율협력주행에서 V2X 메시지의 신뢰성은 필수불가결하다. 만약, 차량 센서의 고장이나 사이버 공격으로 인해 OBU에서 송신하는 V2X 메시지에 잘못된 정보가 있다면 메시지를 수신한 차량의 자율협력주행에 문제가 발생할 수 있다.

이에 대응하고자 북미의 SCMS Manager, 유럽의 ETSI 등 표준화 단체 및 기구에서는 V2X 통신에서 발생할 수 있는 이상행위(misbehavior)를 정의하고, 이상행위 관리 기관(Misbehavior Authority, 이하, "MA"라 함.)로 이상행위를 보고하기 위한 서비스와 메시지 프로토콜을 표준화하고 있다. 아래 표는 국제 표준화 기관별 V2X 이상행위 관리기술 관련 표준화 현황이다.

기관/단체명	산출물명	상태	버전	발행연월
SCMS Manager	MISBEHAVIOR REPORT AND APPLICATION SPECIFICATION	public	v1.0	2019-02
		draft	v1.12	2021-09
	Misbehavior Report ASN.1 규격	public	v1.1	2019-04
		draft	v1.2	2021-05
5GAA	Misbehavior Detection White Paper	draft	v0.6	2021-07
ETSI	ETSI TS 103 759 (ITS; Security; Misbehaviour Reporting service)	draft	v0.0.6	2021-12
	Misbehaviour Report ASN.1 규격	draft	-	2021-12

SCMS Manager(북미)의 Misbehavior Reporting WG(이하, "MBR WG"라 함.)은 OBU가 주기적으로 송신하는 SAE 표준의 BSM(Basic Safety Message)의 위치, 속도 및 가속도 정보를 이용하여 탐지할 수 있는 이상행위 항목을 식별하고, 탐지된 이상행위를 SCMS의 MA에 보고하기 위한 이상행위 보고(Misbehavior Report, 이하, "MBR"이라 함.) 규격을 정의한다. 2019년 2월, 규격 v1.0을 배포하였고, 현재는 전체적인 설명 보완, 탐지 기준값 수정, MBR 규격 수정 등을 포함한 차기 버전을 2022년 2월 배포 목표로 작업 중이다.



아래 표는 북미에서 현재 정의하고 있는 이상행위 항목 및 기준이다

No.	구분	이상행위(MB)	설명
1	위치	수신 불가 거리에서 송신한 BSM (Location Beyond Acceptable Range)	수신한 BSM의 위치 정보가 BSM 수신 가능 거리(2000 m)보다 먼 거리에서 송신했음. 단, 속도나 가속 정보 등 다른 정보는 유효함.
2	위치	고정 위치 (Constant Position)	차량의 속도가 0이 아니고, 차량 오류 경고 신호를 송신하지 않는데 연속된 BSM의 위치 정보가 동일함.
3	위치	위치 불일치 (Location Mismatch)	수신한 BSM의 위치 정보가 부정확함(GPS 오차 범위를 넘음.) 단, 속도나 가속 정보 등 다른 정보는 유효함.
4	위치	임의 위치 (Random Position)	동일한 차량이 연속적으로 송신한 BSM 간의 위치 정보가 불규칙함.
5	위치	가속 정보와 일관되지 않는 위치 (Position Acceleration)	2개의 연속된 BSM 간의 거리가 차량의 가속 정보와 일관되지 않음.
6	동작	유효하지 않은 최대 속도 (Invalid Max Speed)	BSM의 최대 순간 속도가 실제 도로에서 운행되며 가장 빠른 차량의 최대 속도보다 더 큰 값.
7	동작	유효하지 않은 속도 (Invalid Speed)	BSM을 송신한 OBU의 순간 속도가 가능 속도 범위를 벗어남.
8	동작	유효하지 않은 최대 가속 (Invalid Max Acceleration)	순간적인 BSM의 최대 가능 가속 정보가 실제 도로에서 운행되는 차량의 가속도 최고 기록보다 큰 값.
9	동작	제동 중 가속 (Brake Acceleration)	제동 중인데 가속도가 0 이상임. (Phase 2에서 다루도록 연기함.)

ETSI(유럽)에서는 TS 103 759 WG에서 이상행위 보고 서비스에 대한 유럽 표준을 정의하고 있다. SCMS Manager에서 V2X 메시지 기반의 이상행위 항목만을 우선 정의하는 것과 달리, ETSI는 V2X 메시지 외에도 차량 센서 정보 및 주변 지역 환경 정보를 이용하여 탐지할 수 있는 이상행위 항목을 모두 고려하여, Class 1~5까지의 탐지 분류를 정의하고 있다.

탐지 분류	탐지 범위
Class 1	단일 메시지에 불가능한 값 탐지
Class 2	동일 장치의 연속된 동일한 타입(CAM 혹은 DENM)의 메시지 간의 불일치 * CAM: Cooperative Awareness Message * DENM: Decentralized Environmental Notification Message
Class 3	지역 환경 정보와 불일치
Class 4	인지된 물리적 속성들(차량 센서나 V2X 물리 계층 정보)와의 불일치
Class 5	동일 단말의 연속된 다른 타입(CAM 혹은 DENM)의 메시지 간의 불일치 혹은 다른 단말의 메시지(메시지 타입 무관)와의 불일치

SCMS Manager의 MBR WG과 ETSI TS 103 759 WG은 2021년 중순부터 상호 협력하여, 북미의 BSM 기반 이상행위와 유럽의 CAM, DENM 기반 이상행위를 모두 아우르는 통합 MBR 규격을 정의하고 있다.

### ● 3. 결론

국내에서는 국토교통부 주도로 2019년부터 북미 표준(CAMP SCMS) 기반 V2X 보안 인증 실증시스템을 운영하고 있으며, ‘자율주행자동차 상용화 촉진 및 지원에 관한 법률’ 개정(‘21.7)을 통해 V2X 보안인증체계(자율협력주행 인증관리체계)의 구축 및 운영을 위한 법적 근거도 마련된 상태이다. 또한 2023년을 목표로 자율주행차 표준화 포럼 산하 보안인증 작업반에서 ‘V2X 보안인증체계 국가표준’을 개발 중에 있으며, V2X 이상행위 항목 및 보고규격에 대한 ITS-K 단체 표준을 개발 중이다.

아직 완성차 등록인증서 발급·관리 방법, V2X 이상행위 관리기술 및 IEEE 1609.2.1에서 도입된 신기술에 대한 대규모 실증 등 부족한 점도 존재하지만, 민·관·산·학이 힘을 모은다면 자율협력주행 상용화의 선결과제인 V2X 보안에 대한 국가 체계 마련은 그리 멀지 않은 미래라고 기대해 본다.

## 자율주행 자동차 보안 기술 및 국제표준화 동향

TTA 표준화본부 강석규 팀장



최근 디지털 기술 혁신을 기반으로 하는 4차 산업혁명 시대를 맞이하여 기존 ICT기술의 지능화, 복잡화 등을 통해 전통적인 자동차 산업의 패러다임도 함께 변화하고 있다. 지금까지의 전통적인 자동차 구조하에서 교통사고 등으로 인한 인명손실과 사회적 비용 지불 등의 문제를 해결하기 위해 글로벌 자동차 업체는 ICT를 기반으로 하는 자율주행 자동차의 개발 및 상용화에 박차를 가하고 있다.

자율주행 자동차는 자동차가 스스로 주행환경을 인식하고, 경로를 스스로 판단해 주행하며, 동시에 고신뢰·고성능의 기능을 탑재한 센서 정보를 네트워크를 통해 교통 인프라와 연결함으로써 자차의 위치와 주변환경, 주행경로를 실시간 탐지하고 계획하며, 자동차 스스로 충돌 위험을 회피하고, 교통법규에 따라 안전하게 운행이 가능한 자동차를 의미한다.

자율주행 자동차는 차량을 제어하는 주체가 운전자인지 자동차인지에 따라 자율주행 레벨의 수준이 결정된다. 이같은 레벨의 정의는 미국자동차공학회(SAE)에서 처음 제안되었으며, 현재까지 국제적인 기준으로 통용되고 있다. 자율주행 레벨 0은 운전자가 100% 개입하여 자동차 운전이 이뤄지는 단계이며, 레벨1부터 레벨2까지는 운전자가 일부분 차량간 거리, 속도, 조향 등을 변경하는 주체로써 기능한다. 레벨 2까지는 자율주행이 운전자의 역할을 보조하는 기술 수단으로 인식된다. 레벨 3부터는 시스템이 주요 운전 주체로써 기능을 수행하며, 긴급 상황에 대해서만 운전자가 개입하는 수준으로 본격적인 자율주행 단계에 해당된다.

표 1. 단계적 자율주행 레벨 구분

레벨구분	레벨0	레벨1	레벨2	레벨3	레벨4	레벨5
명칭	無 자율주행	운전자 지원	부분 자동화	조건부 자동화	고도 자동화	완전 자동화
항목	없음	조향 또는 속도	조향 및 속도	조향 및 속도	조향 및 속도	조향 및 속도
운전자 관여	항상 관여	항상 관여	항상 관여	시스템 요청시	관여 불필요	관여 불필요
자율주행 구간	없음	특정 구간	특정 구간	특정 구간	특정구간	전 구간
시장현황	대부분 완성차 양산	대부분 완성차 양산	7~8개 완성차 양산	1~2개 완성차 양산	3~4개 벤처 생산	없음

출처: 미국자동차공학회(SAE), 국토부

우리나라는 과기부/산업부/국토부/경찰청 등 다부처 협력으로 2027년까지 레벨4 이상의 자율주행 핵심기술 개발 사업을 추진 중이며, 5개 분야 84개 세부과제를 통해 자동차 ICT 융합신기술 개발 및 생태계 마련, 자율주행 신뢰성 확보를 통한 국민 수용성 향상 등을 기대하고 있다.

자율주행자동차는 사용자의 편의성 및 안전성 향상 요구 증대와 고령화, 도시화, 공유화 등으로 인하여 점차 수요가 늘어나고 있는 상황이다. 레벨3 이상의 자율주행 시장은 2030년까지 전체 자동차 시장의 62%를 차지하게 될 것으로 예상되며, 전세계적으로 2021년 현재 대부분 글로벌 제조업체들은 레벨2 이상의 기술력을 확보했으며 3 단계 상용화를 위해 경쟁 중인 것으로 파악된다.

이와 같이 자율주행 자동차의 상용화와 시장 점유를 위해서는 자율주행 자동차 운행 중 발생할 수 있는 보안 위협으로부터 운전자 및 보행자를 보호할 수 있는 기술은 자율주행차 대중화에 필수 핵심기술이라고 볼 수 있다.

자율주행차 상용화 시대를 앞두고 자율주행차에 대한 해킹 위협에 대응하기 위한 사이버 보안 등의 중요성이 대두됨에 따라, 국토교통부는 지난 2020년 12월 자율주행차의 보안윤리안전에 대한 기본 방향을 제시하는 자동차 사이버보안 가이드라인을 발표했다. 이번 가이드라인은 자동차 제작사 등이 보안기준의 시행에 대비하여 사이버보안체계를 준비할 수 있도록 권고안, 보안정책 방향 등을 담고 있다. 이와 함께, 차량 자체에 대한 사이버보안 관리에 대해 차량에 대한 보안위협 식별, 평가, 보안조치, 충분한 사전시험 등의 수행을 해야한다고 명시되어있다. 즉 사이버공격의 탐지 및 예방 조치, 위협모니터링 지원조치, 사어버공격 분석을 위한 데이터 포렌식 지원조치 등이 포함된다. 앞으로 국토교통부는 22년 7월 국내 기준 시행을 목표로 자동차 관리법 및 하위법령을 개정할 계획이며, 앞으로는 보안기준에 따라 차량을 시험/평가하고 사이버 위협등을 모니터링 할 수 있는 자동차 보안센터를 구축할 계획이다.

일례로, 2014년 지프 체로키 차량의 유커넥트 시스템을 대상으로 진행된 해킹 시연을 통해 수 km 거리가 떨어진 원격지에서 약 100km/h의 속도로 주행하던 차량의 엔진을 정지시키거나, 핸들을 임의 조작함으로써 보안 취약성을 증명한 바 있으며, 이후 차량 제조사는 약 140만대를 리콜함으로써, 제품 이미지 하락과 막대한 비용을 부담한 바 있다. 미쓰비시사의 아웃랜더 차량은 스마트폰 앱을 통해 자동차의 상태를 확인하고, 문잠금 해제나 차량 공조장치 조작 등의 기능을 제공하였는데, 2016년에 앱과 차량간 연결 네트워크를 해킹하여 차량 기능을 원격에서 임의로 조작한 경우도 있었다. 테슬라의 경우도 원격으로 운전자의 의지와 상관없이 급제동을 일으키거나, 아무도 타지않은 차량의 창문이나 문 잠금을 해제되는 등 보안 취약성이 확인된 바 있다. 이렇듯 자율주행차를 대상으로 한 해킹 사례는 시연이나 실험 목적으로 이뤄진 것이긴 하나, 분명한 것은 여전히 우리 주변에 운행되는 일부 자율주행자동차의 보안성에 상당히 취약한 부분이 있다는 것이다. 물론 자율주행 자동차 보안을 위한 다양한 보안기술과 솔루션이 개발되고 있긴 하나, 점점 지능화·고도화되는 차량 사이버 보안 공격에 대한 대응책이 필요하고, 자율자동차 보안 기술에 대한 전반적인 표준화 논의가 중요한 시점이다.

지난 2020년 한국인터넷진흥원(KISA)는 자율주행차 서비스 유형별로 데이터 흐름을 분석하고, 이 과정에서 발생될 수 있는 유형별 보안위협을 정의한 자율주행차 보안모델을 발표한 바 있다. 자율주행차 서비스 보안 위협이 발생할 수 있는 영역을 백엔드 인프라, 통신, 차량 등 크게 세 부분으로 분류하여, 각 영역별로 발생가능한 보안 위협은 아래 표와 같이 정리하였다.

표 2. 자율주행 자동차 서비스 구간별 보안 위협

영역	구간	보안위협
차량	-	ECU 펌웨어 해킹 및 위변조 IVI 해킹, 차량불법 조작 서비스 거부(DoS)
통신네트워크	차량 간 (V2V)	도청, 메시지 위변조, 악의적 제어 메시지 전송, 정보무단획득 등
	차량-인프라(V2I)	
	인프라 간(I2I)	
백엔드 인프라	-	정보유출, 권한상승, 서비스거부(DoS) 등

출처: 한국인터넷진흥원 '자율주행차 보안모델(2020)' 자율주행차 서비스 구간별 보안위협 일부 재구성

자율주행차 서비스 확산을 방해하는 보안위협 요소는 자율주행 기술발전과 새로운 서비스 등장으로 변화될 수 있으며, 변화에 맞춰 대응 가능한 보안기술 역시 활발하게 연구되고 있다. 앞서, 정리한 자율주행차 서비스 영역별 보안 위협에 대응하기 위한

기술을 정리하면 아래 표와 같다.

표 3. 자율주행 자동차 보안위협별 보안기술

영역	보안위협	보안기술
차량	펌웨어 위변조	보안부팅, secure debug, Secure diagnosis, Secure flash 등
	IVI 해킹	IDS, SecOS 등
	서비스 거부(DoS)	IDS
	차량 불법조작	Secure access, Secure diagnosis
통신네트워크	차량간 (V2V)	IPSec, 5G/WAVE 통신 보안기술
	차량-인프라(V2I)	
	인프라 간(I2I)	
백엔드 인프라	정보유출	방화벽, DB암호화, 접근통제 등
	권한 상승	접근제어
	서비스 거부(DoS)	방화벽

출처: 한국인터넷진흥원 '자율주행차 보안모델(2020)' 보안위협별 대응 보안기술 일부 재구성

언급된 위협 별 대응 보안 기술은 전체 영역에 대한 보안성 제공이 적절하게 이뤄져야지만 효과적인 자율주행차 서비스 보안 위협이 통제될 수 있다.

현재 자율주행 자동차 보안기술 표준화는 차량통신보안, 차량센서 데이터 보안 및 사이버 보안 위협 식별 및 관리 등 다양한 보안기술 분야에 대해 진행되고 있다. 예상치 못한 보안 위협 또는 문제 발생은 자율주행차의 상용화를 지연시키는 위험요소일 뿐만 아니라 차량 운전자에게 심각한 피해를 입힐 수 있다는 측면에서 보안기술의 중요성이 증가하고 그만큼 자율주행차 통신 및 서비스 생태계에서의 보안기술 표준화는 매우 중요하다고 볼 수 있다.

자율주행차 보안 표준화를 다루는 여러 국제공식 및 사실표준화기구를 살펴보면, ISO TC22는 자율주행차 부품과 시험관련 표준을 중심으로 표준화작업을 진행 중이다. 기능안전 표준인 ISO 26262를 기반으로 자율차에 적용되는 SOTIF 표준을 다루고 있으며, 정보보안 뿐만 아니라 클라우드 연계 기능인 Extended Vehicle 표준화도 추진 중이다.

자율주행차 네트워크 보안과 관련해서는 주로 ISO TC22/SC32에서 표준화 활동이 진행되고 있다. SC32 산하에는 14개의 WG이 운영되고 있으며 그 중 WG8(Fuctional Safety)과 WG11(Cyber Security)에서 중점적으로 표준화가 논의 중이다.

표 4. ISO/TC 22/SC 32 구성

그룹	그룹명
WG 1	Ignition Equipment
WG 2	Environmental conditions
WG 3	Electromagnetic compatibility
WG 4	Automotive electrical cables
WG 5	Fuses and circuit breakers
WG 6	On-board electrical connections
WG 7	Functional characteristics of starting devices and electrical generators
WG 8	Functional safety
WG 9	Electrical connections between towing and towed vehicles
WG 10	Optical components - Test methods and requirements
WG 11	Cybersecurity
WG 12	Software update
WG 13	Safety for driving automation systems
WG 14	Safety and Artificial Intelligence

지금까지 ISO TC22에서 제정된 자율주행차 성능시험과 안전, 사이버 보안 분야의 표준제정 현황은 다음 아래 표에 정리하였다.

표 5. ISO/TC 22 표준화 현황

표준번호	표준명	주요 내용
ISO/TR 4804	Safety and Cybersecurity for automated driving systems - Design, Verification and validation	<ul style="list-style-type: none"> <li>SAE 3061:2018에 따라 자율주행 레벨 3/4 기능이 있는 차량에 중점을 둔 자동 운전 시스템의 검증, 설계 시 안전 및 사이버 보안 사항에 대한 표준</li> </ul>
ISO 26262-4	Functional Safety-Part 4: Product development at the system level	<ul style="list-style-type: none"> <li>시스템 수준의 자동차 어플리케이션 개발을 위한 요구사항                             <ul style="list-style-type: none"> <li>시스템 수준에서의 제품 개발을 시작하기 위한 일반 기술적 안전 요구사항</li> <li>기술적 안전에 대한 개념</li> <li>시스템 아키텍처 설계</li> <li>항목 통합 및 테스트</li> <li>안전 검증</li> </ul> </li> </ul>
ISO 26262-6	Functional Safety-Part 6: Product development at the software level	<ul style="list-style-type: none"> <li>소프트웨어 수준의 자동차 어플리케이션 개발을 위한 요구사항                             <ul style="list-style-type: none"> <li>소프트웨어 수준에서의 안전 요구사항</li> <li>소프트웨어 아키텍처 설계</li> <li>소프트웨어 유닛 설계 및 구현</li> <li>소프트웨어 유닛 검증</li> <li>소프트웨어 통합 및 검증</li> <li>임베디드 소프트웨어 테스트</li> </ul> </li> </ul>

표준번호	표준명	주요 내용
ISO/SAE 21434	Cybersecurity engineering	<ul style="list-style-type: none"> <li>자동차의 전기/전자(E/E) 시스템의 개념, 제품 개발, 생산, 운영, 유지 관리 및 폐기와 관련된 사이버 보안 위험 관리에 대한 엔지니어링 요구사항</li> <li>사이버 보안 프로세스에 대한 요구사항</li> <li>사이버 보안 위험 전달 관리를 위한 공통 용어 및 프레임워크 정의</li> </ul>
ISO/TR 15497 :2000	Development guidelines for vehicle based software	차량 기반 소프트웨어 개발을 위한 안전 관련 지침 제공 (구체적인 Scope는 비공개)

ISO TC 204는 지능형 교통체계(ITS) 분야에 대한 표준화를 다루고 있으며, ACC, LKAS 등 ADAS 표준과 레벨 2 자율주행, 자율주차, 자동차선변경, 자율주행차 용어 표준이 진행되고 있다. 최근 긴급대응기능(MRM), 발렛주차, 레벨3자율주행, 군집주행 표준이 시작되었으며, 자율주행차 보안과 관련해서는 V2X의 원활한 데이터 정보 교환을 위한 표준을 개발하고 있다. 특히, 네트워크의 안전성과 관련해서는 현재까지 6건의 국제표준을 제정하였고, 자율주차기능에 있어서 보안기능 통합에 대한 기술문서 (Automated velet parking systems(AVPS)-Part 2:Security integration, ISO/AWI TS 23374-2)를 개발 중이다. 앞서 언급한 ISO TC 204의 표준화 현황을 표로 정리하면 아래와 같다.

표 6. ISO/TC 204 표준화 현황

표준번호	표준명	주요내용
ISO/TR 11766:2010	Communications access for land mobiles(CALM)-Security considerations for lawful interception	<ul style="list-style-type: none"> <li>CALM 환경과 CALM/ITS가 일반적으로 제공하는 IPv6 도메인 제공 서비스 고려한 ITS 환경과 ITS 배포에 대한 차단 조항에 대한 검토 요구사항</li> </ul>
ISO/TS 15638-4:2020	Framework for cooperative telematics applications for regulated commercial freight(TARV)-Part 4:System security requirements	<ul style="list-style-type: none"> <li>하드웨어 및 소프트웨어 양측면에 대한 보안 요구사항</li> <li>규제 대상 상용차의 텔레매틱스 어플리케이션에 대한 요구사항               <ul style="list-style-type: none"> <li>- 위험, 취약성 및 위험 분석</li> <li>- 보안 서비스 및 아키텍처</li> <li>- 신원관리</li> <li>- 보안 아키텍처 및 관리</li> <li>- 신원 신뢰 및 개인 정보 관리</li> <li>- 보안 접근 통제</li> <li>- 보안 기밀 유지 서비스</li> </ul> </li> </ul>
ISO/TS 21177:2019	ITS station security services for secure session establishment and authentication between trusted devices	<ul style="list-style-type: none"> <li>데이터 전송 객체 간 교환되는 정보의 무결성과 서비스 신뢰성 보장에 필요한 ITS 스테이션 보안 서비스에 대한 요구사항</li> <li>객체 간 정보 교환에 필요한 인증 및 보안 설정 요구사항</li> </ul>
ISO/TS 21185:2019	Communication profiles for secure connections between trusted devices	<ul style="list-style-type: none"> <li>표준화된 통신 프로토콜 기반의 ITS-SCP 정의 및 ITS-SCP 지정</li> </ul>



표준번호	표준명	주요내용
ISO/TR 21186-3:2021	C-ITS-Guidelines on the usage of standards-Part 3:Security	ISO/TR 21177에 기반하여 ITS 내 어플리케이션 보안, 접근 제어, 장치 보안 및 PKI 보안에 대한 요구사항
ISO 24102-4:2018	ITS station management-part 4:Station-internal management	ITS 스테이션 내부 관리 통신에 대한 요구사항

ITU-T SG17 표준화 그룹은 통신분야의 표준화를 다루는 국제기구인 ITU-T 산하의 사이버 보안 기술에 대한 전문 표준화 그룹이다. 산하에 12개 그룹이 있는데 그중 Q.13에서는 전반적인 차량통신 보안 분야의 표준을 개발하고 있으며, 자율주행차의 차량 내/외부망 보안, ITS 네트워크 응용 보안 표준화가 진행 중이다. ITS 보안 표준화는 V2X통신 보안, 차내망 보안, 교통인프라 시스템 보안, 차량 접속 디바이스 보안 등이 있다.

표 7. ITU-T SG 17 Q13에서의 표준 개발 현황

표준번호	표준명	중점 내용
X.1371	Security threats in connected vehicles	<ul style="list-style-type: none"> <li>• 커넥티드 카 및 ITS에 연결된 보안 위험에 대한 표준</li> <li>• UNECE WP.29의 차량 사이버 권고안의 위험과 연계된 보안 위험 정의</li> <li>• 차량 생태계에서의 사이버 보안 위험 정의</li> </ul>
X.1372	Security guidelines for V2X communication systems	<ul style="list-style-type: none"> <li>• V2X 통신 시스템에 발생 가능한 보안 가이드라인</li> </ul>
X.1373	Secure software update capability for intelligence transportation system communication devices	<ul style="list-style-type: none"> <li>• ITS 통신 장치에 대한 보안 소프트웨어 업데이트 절차 정의</li> </ul>
X.1374	Security requirements for external interfaces and devices with vehicle access capability	<ul style="list-style-type: none"> <li>• 차량 외부 접속 디바이스에 대한 보안 요구사항(차량&amp;외부 장치)</li> </ul>
X.1375	Methodologies for intrusion detection system on in-vehicle networks	<ul style="list-style-type: none"> <li>• 차량 내 네트워크(IVN)에 대한 침입 탐지 시스템(IDS)에 대한 요구사항</li> </ul>
X.1376	Security-related misbehaviour detection mechanism based on big data analysis for connected vehicles	<ul style="list-style-type: none"> <li>• 보안 관련 오작동 감지 메커니즘에 대한 정의</li> <li>- 데이터 수집, 탐지</li> </ul>
X.itssec-5	Security guidelines for vehicular edge computing(VEC)	<ul style="list-style-type: none"> <li>• VEC는 최종 사용자에게 더 빠른 서비스 응답 시간을 제공해야 함에 따라 많은 보안 문제에 취약성이 존재함에 따라 VEC 내에서 식별된 위험 및 취약성에 대한 분석을 기반으로 VEC에 대한 보안 지침 및 관련 보안 요구사항</li> </ul>

표준번호	표준명	중점 내용
X.srkd	Security requirements for categorized data in V2X communication	<ul style="list-style-type: none"> <li>V2X 통신에 사용되는 데이터를 객체 속성 데이터, 차량 상태 데이터, 환경 데이터, 어플리케이션 서비스 데이터, 행동 데이터, 기밀성 데이터 등의 여러 유형의 데이터 정의</li> <li>분류된 데이터 유형에 대해 보안 수준을 할당 후, 할당된 데이터를 기반으로 V2X 통신에서 분류된 데이터에 대한 보안 요구 사항 제공</li> <li>개인 정보 보호와 관련된 문제는 본 표준에서 다루지는 않음</li> </ul>
X.fstiscv	Framework of security threat information sharing for connected vehicles	<ul style="list-style-type: none"> <li>커넥티드 차량의 보안 위협 정보 공유 개요 설명, 위협 정보 공유 커넥티드 차량의 보안 위협 정보 공유 시스템에 대한 요구사항</li> <li>권장 사항은 주요 처리 절차와 함께 연결된 차량의 보안 정보 공유를 위한 프레임워크 정의</li> <li>위협 정보 공유 강화를 통해 사이버 보안 공격의 잠재적 영향 완화·보안 강화를 목적으로 함</li> </ul>
X.eivnsec	Security guidelines for the Ethernet-based in-vehicle networks	<ul style="list-style-type: none"> <li>이더넷 기반 차내망 보안 위협 및 요구사항 정의</li> <li>이더넷 기반 차내망 유즈케이스 정의</li> </ul>
X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment	<ul style="list-style-type: none"> <li>클라우드 기반 차량 사고기록장치 보안 위협 및 요구사항 정의</li> <li>클라우드 기반 차량의 사고기록장치의 유즈케이스 정의</li> </ul>
X.ipscv	Methodologies for intrusion prevention systems for connected vehicles	<ul style="list-style-type: none"> <li>차량용 IPS 구현 방법론 정의</li> </ul>
X.rsu-sec	Security requirements for road-side units in intelligent transportation systems	<ul style="list-style-type: none"> <li>ITS에서 RSU에 대한 보안 요구사항</li> <li>보안 위협 분석 기반의 RSU에 대한 보안 요구 사항 제공</li> </ul>
X.evtol-sec	Security guidelines for electric vertical take-off and landing (eVTOL) vehicle in an urban air mobility environment	<ul style="list-style-type: none"> <li>도시 항공 모빌리티 서비스와 관련된 산업에 보안 지침을 제공하기 위한 eVTOL 시스템, 보안 위협 분석 및 eVTOL에 대한 보안 요구 사항에 대한</li> <li>개요를 제공</li> </ul>

V2X 보안 분야에서는 전반적인 보안 가이드라인이 X.1372에서, 데이터 속성에 따른 보안 등급 분류는 X.srkd에서 다루고 있다. 차량 진단 포트 및 블루투스를 통해 차량에 접속하는 디바이스 보안은 X.1374에서 다루고 있으며, 보안관리서버, 교통관제 서버 등의 인프라 및 클라우드에 연관된 보안 표준화는 X.1376, X.fstiscv 및 X.itssec-5에서 다루고 있다. 특히 C-V2X 환경에서의 도로기지국의 보안요구사항은 X.rsu-sec에 담길 예정이며, 차량 내부망 보안측면에서 일반적인 차량용 침입탐지시스템 방법론이 X.1375에 담겨있다. 차내망에서 발생한 이상징후 탐지를 이용하여 침입탐지시스템을 구현하기 위한 표준이 지난 2019년 9월 신규아이템으로 채택되어

X.ipscv로 개발 중이다. 차량용 이더넷 분야 및 사고기록장치의 표준화를 위해 두 개의 워크 아이템(X.eivnsec, X.edrsec)이 진행되고 있다.

이밖에 글로벌 사실표준화 기구에서의 자율주행차 보안 표준화 동향을 살펴보면, 먼저 IETF는 인터넷 아키텍처와 프로토콜 관련 표준화를 연구하는 기구로서 보안분야는 주로 Security Area(SEC), Transport Area(TSV) 그룹에서 다뤄지고 있다. 이들 그룹에서 자율주행차 네트워크 관련된 표준으로 RFC 7203, An Incident Object Description Exchange Format(IODEF) Extension for Structured Cybersecurity Information, RFC 5062 Security Attacks Found Against the Stream Control Transmission Protocol and Current Countermeasure 표준이 있다.

미국자동차공학회(SAE) 역시 자율주행차에 대한 표준화를 진행하고 있는데, Motor vehicle council 산하의 Data Link Connector Security Committee, Vehicle Cybersecurity Systems Engineering Committee, V2X Security Technical Committee 등에서 아래 표에 정리된 것과 같이 표준을 제정하였다.

표 8. 표준화 현황

표준번호	표준명	중점 내용
SAE J2945/5	Service Specific Permission ans Security Guidelines for Connected Vehicle Applications	<ul style="list-style-type: none"> <li>어플리케이션 지정자가 어떤 영역과 활동이 SSP 제약을 받아야 하는지 결정하고, 해당 어플리케이션의 SSP에 대한 구문과 의미를 지정하는데 사용 가능한 보안 시스템 엔지니어링 프로세스 요구사항 제공</li> </ul>
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	<ul style="list-style-type: none"> <li>Cyber-Physical 차량 시스템의 사이버 보안에 대한 지침과 적용 방안을 제시</li> <li>정의, 개념, 생산, 운영, 서비스 및 폐기까지 사이버 보안을 Cyber-Physical 차량 시스템에 통합하기 위한 라이프 사이클 프로세스 프레임워크 정의</li> <li>차량 시스템의 사이버 보안에 대한 기본 지침 제공</li> </ul>
ISO/SAE 21434	Road Vehicle - Cybersecurity Engineering	<ul style="list-style-type: none"> <li>자동차의 전기/전자(E/E) 시스템의 개념, 제품 개발, 생산, 운영, 유지 관리 및 폐기와 관련된 사이버 보안 위험 관리에 대한 엔지니어링 요구사항</li> <li>사이버 보안 프로세스에 대한 요구사항</li> <li>사이버 보안 위험 전달 관리를 위한 공통 용어 및 프레임워크 정의</li> </ul>

현재 SAE산하 Orad(On-Road Automated Driving) Committee에서는 위 언급된 표준 이외에도 자율주행 자동차 S/W와 H/W에 대한 보안성 테스트 방법론(J3061-2), 자율주행 시스템 테스트에 필요한 사이버/물리적 보안 요구사항(J3247), OBD(on-Board Diagnostics) 보안(J3273) 등의 새로운 표준을 개발 중이다.

이 외에도, 표준화기구는 아니지만 유럽경제위원회(UNECE)산하 WP29(자동차 분과 실

**무위원회**는 2020년 6월 자동차 사이버 보안과 차량형식 승인에 대한 기준(**UNR 155**)을 채택했다. 이는 자동차 산업에 있어 구속력을 갖는 최초 규정으로써, 차량 사이버보안 및 소프트웨어 업데이트에 대한 보안 요구사항을 명시한다. 이 기준은 유럽 54개 회원국 외에도 유럽과 상호인증협정을 맺고 있는 우리나라에도 적용된다. 2022년 7월 이후 유럽에서 형식 등록되는 신차는 해당 제품의 개발단계에서부터 사이버보안이 고려되었는지를 증명해야 하는 의무가 발생하고, 추가적으로 차량 제조사는 사이버보안 관리 능력에 대한 인증을 반드시 받아야 한다. 이를 위해서는 차량제조사는 생산 전주기에 사이버 보안을 관리·개선할 수 있는 사이버보안관리시스템(**CSMS**)를 구축해야 한다. CSMS는 차량 사이버보안을 위협하는 각종 위협 요소를 정의하고, 공격으로부터 안전하게 차량을 보호할 수 있도록 하는 거버넌스 체계 구축을 포함한다. 이를 준수하기 위해서는 차량의 개발, 생산, 운행, 폐기 등 전체 라이프사이클에 대한 보안 프로세스를 정리하고 적용해야 하는 것이다.

앞서 기술한 바와 같이 자율주행 자동차는 기존 차량과 비교하여 외부 네트워크를 통해 V2V, V2I 등의 V2X 통신을 수행하며, 이러한 차량통신기술은 자율주행 자동차의 필수 요소 기술로 상용화가 진행 중이다. 내부적으로는 자율주행 차량에서 데이터 수집을 위한 센서의 증가로 차량 내부 데이터 처리를 위한 차량 이더넷 활용의 범위는 계속 확대되지만, 이더넷 환경의 보안 취약점은 아직까지 존재하고 있다. 이에 자율주행 자동차 보안 기술 및 클라우드와의 연계를 통한 차량 사이버 보안성 강화의 중요성은 부각되고 있다. 예상하지 못한 보안 위협 또는 문제의 발생은 자율주행 자동차의 완전한 상용화를 지연시키는 위협 요소이기 때문에 앞으로 자율주행 자동차 통신 환경과 지능형교통시스템(**ITS**)의 생태계에서의 사이버보안 방지를 위한 연구 개발 및 다양한 국제표준화 활동의 노력은 끊임없이 계속되어야 할 것이다.

# 자율주행을 위한 정밀도로지도 구축·갱신 및 LDM(Local Dynamic Map) 기술 현황

웨이즈원(주) 김동수 상무



## 1. 서론

### 가. 정부 정책 추진현황\*

#### 1) 자율차 상용화

정부는 2027년까지 운전자의 개입이 없는 ‘자율차 상용화’를 추진하기 위해 40개의 규제를 개선하기로 했다. 미래 시나리오를 바탕으로 2030년까지 단기와 중기, 장기로 나눠 규제혁신 과제 40개를 마련했다. 단기적으로 정비 업체를 방문하지 않고도 전자·제어장치 등을 업데이트할 수 있도록 자동차관리법 시행규칙을 개정하고, 중장기적으로는 레벨4 자율차 운영을 위한 보험·교통 법규 위반 등에 대한 기준을 마련하기로 했다. 현재 운전자 개입이 없는 레벨4 자율차 사고에 대해 제조사 등 책임 원칙을 명확히 할 계획이며, 이와 함께 레벨3 상용차와 레벨4 자율차 안전기준도 확립하기로 했다. 향후 2025년에는 레벨4 저속 셔틀, 2027년에는 레벨4 자율차가 상용화될 것으로 예상했다.



\* [출처] 대한민국 정책브리핑(www.korea.kr)

이에 맞추어 과학기술정보통신부는 자율주행산업 경쟁력 강화를 위해 22년 자율주행 기술 개발에 283억 원을 추가하고, 2027년까지 총 2,000억 원 규모로 확대 지원하기로 했다. 레벨4 이상의 자율주행 상용화를 목표로 국토교통부와 함께 자율주행 지원 표준화를 위해 공동 실증 및 시범사업을 함께 추진할 예정이다.

## 2) 2022년 디지털 뉴딜

‘디지털 뉴딜’은 코로나19 경제위기를 극복하고 경제·사회 전반의 디지털 대전환을 위해 추진 중인 ‘국가 혁신프로젝트’이다. 정부는 추진 1주년을 맞아 재정투자 규모를 49조 원으로 확대한 디지털 뉴딜 2.0을 발표했고, 자율주행 등 신산업 기반 구축을 위한 사회간접자본(SOC) 핵심 인프라를 디지털화 및 스마트화를 목표로 연관산업 경쟁력을 향상하고자 2025년까지 9.7조 원을 투자한다. 4대 분야 핵심 인프라 중 ‘디지털 트윈’은 주요 지역 3D 지도 작성 및 지하 시설물 지도를 77개 군, 정밀도로지도는 일 반국도까지 구축 완료하며, 다양한 트윈 간 연계를 위한 연합핵심기술을 개발하고 제조와 산단 등에 트윈을 적용·실증하고자 한다.

그에 따라 국토교통부는 정밀도로 구축 및 갱신을 위한 행정규칙 개정하였다. 향후 도로를 신설하거나 확장·개량할 때는 자율주행 자동차 운행을 위한 정밀도로가 지도에 반영된다. 정밀도로지도는 국토지리정보원이 제작하는데 직접 도로 공사정보를 수집해야 하므로 최신 정보를 반영하는 어려움이 있었지만, 현재는 도로관리청에서 기존에 정밀도로지도가 구축 완료된 구간에 변경사항이 발생하거나 정밀도로지도가 구축 완료된 구간에 접하여 도로를 신설하는 경우 이를 통보하도록 변경되어 효과적으로 반영할 수 있게 되었다.





## 나. 정밀도로지도 기술 및 동향

### 1) 정밀도로지도 구축 자동화 기술

#### - Map Auto-Creation 시스템 개발 프로젝트\*

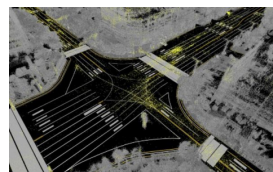
현대오트오에버(Hyundai AutoEver)는 정밀도로지도 구축 자동화 기술을 개발하고 있다. 수작업으로 정밀도로지도를 하루 4km로 3개월 동안 16,000km 구축할 때, 67명의 작업자가 필요하지만, 100% 자동화가 된다면 하루 작업량은 100km당 3명의 인력으로 가능하게 된다. 위치정확도 20cm의 품질을 확보하며 학습데이터 제작을 하였고, 현재 자동화 수준은 90%(자동차 전용도로 기준) 계속되는 기술 개발로 더 많은 인력과 비용을 줄일 수 있을 것으로 예상된다. 기술적 한계로는 노면 상태, MMS 조사 범위, 차량의 노이즈 등 환경적인 오차에 대한 수작업이 있지만, 자동 편집 기능 강화를 통한 정밀도로지도 구축 및 업데이트 기간을 단축하며 Crowd 기반 실시간 업데이트를 목표로 하고 있다.

### 2) 국·내외 기업 동향

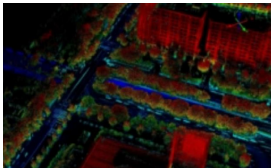
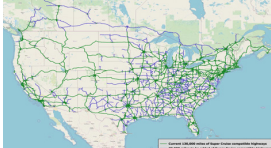
정밀도로지도의 중요성이 높아지고 있음에 따라 자율주행차 선진국들도 정밀도로지도의 효율적 구축 및 확대를 위해 치열한 경쟁을 벌이고 있다. 독일에서는 BMW, 아우디, 다임러(Daimler) 컨소시엄이 노키아로부터 지도정보서비스 부문인 히어(HERE)를 인수하여 미국·유럽에 대한 정밀도로지도를 공동 구축하였고, 일본은 다수의 민간기업과 공공이 함께 투자하여 DMP(Dynamic Map Platform)의 설립으로 일본 고속도로에 대한 정밀도로지도 구축하였다. 잇따라 주요 기업들이 정밀도로지도 제작은 물론이고 활용성 확대를 위한 개발 등 다양한 방법으로 확장하고 있고, 기업들의 동향은 다음과 같다.

표 1. 정밀도로지도 국·내외 기업 동향

국내 기업	
Hyundai AutoEver	<ul style="list-style-type: none"> <li>• 전국 자동차 전용도로 정밀도로지도(HD map) 16,000km 구축(오차범위 20cm 이내)</li> <li>• 글로벌 지도 업체 '히어(here)'와 HD map MOU 체결</li> </ul>



\* HMG Developer Conference 발표자료

NAVER LABS	<ul style="list-style-type: none"> <li>• 도시 시뮬레이션 및 자율주행을 위한 HD map 제작</li> <li>• 딥러닝을 이용한 도로 HD map의 변화탐지 기술 적용</li> <li>• 日 softbank와 협업하여 HD map 제작 프로젝트 진행</li> </ul>	
KAKAO Mobility	<ul style="list-style-type: none"> <li>• MMS 내 영상에서 나오는 신호등, 간판 등의 정보를 라이다의 좌표값과 매칭, 실시간으로 클라우드에 전달, HD map이 자동으로 업데이트되는 방식을 개발</li> <li>• 디지털 트윈 구축을 위해 HD map 제작 확대, 모바일 맵핑 시스템(MMS) 및 클라우드 데이터 결합 개발</li> </ul>	
<b>국외 기업</b>		
HERE	<ul style="list-style-type: none"> <li>• 전 세계 자율주행차의 글로벌 표준을 위해 협력 및 고화질 지도 제공</li> <li>• 실시간 교통 상황 알림</li> </ul>	
DEEPMAP	<ul style="list-style-type: none"> <li>• 도로의 변화를 실시간으로 반영하는 HD map</li> <li>• LiDAR와 카메라 이미지를 결합하여 실시간 3차원 도로데이터 생성</li> </ul>	
TOMTOM	<ul style="list-style-type: none"> <li>• Close Loop 시스템을 통한 세계 최대 고정밀지도 플랫폼 서비스 진행</li> <li>• ADAS, HD map 콘텐츠 및 실시간 교통정보 제공</li> </ul>	
Google Waymo	<ul style="list-style-type: none"> <li>• 전세계 단위의 지도 데이터 대량 확보 및 누적 거리 300만 마일(약 480만km) 자율주행차 테스트 진행</li> <li>• 구간별 HD급 데이터 베이스 구축 및 미국 전역 25개 도시 이상으로 확대하는 프로젝트 진행</li> </ul>	
USHR	<ul style="list-style-type: none"> <li>• GM, 북미 95% 이상의 주행상황 대처 가능한 울트라 크루즈 발표</li> <li>• 정밀도로지도 200만 개의 도로 적용, 이후 미국, 캐나다 내 최대 340만 마일(574만 km) 확정 예정</li> </ul>	

[출처] HMG Developer Conference 발표자료 및 기업 홍보자료

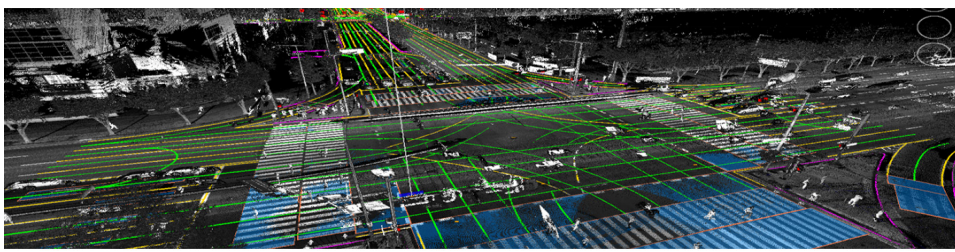


## ● 2. 본론

### 가. 정밀도로지도

#### 1) 정밀도로지도 정의

정밀도로지도란 자율주행차량 및 도로·교통 관리 지원을 위해 도로의 차선 단위까지 정밀하게 구축하는 도로지도이다. 4차 산업혁명의 핵심기술 중 하나인 자율주행 기술은 차량뿐만 아니라 청소, 배달 등 다양한 분야로 적용되고 있다. 이러한 자율주행 모빌리티 운영에는 서비스 지역에서의 차량 위치 파악 및 주행경로 추정에 필요한 고정밀 도로 정보가 매우 중요한데 정밀도로지도는 센서가 인지하지 못하는 원거리의 상황이나 서버에서 전송하는 주변 정보 및 주행에 참고할 수 있는 주행환경정보를 포함하고 있어 자율주행시스템의 의사결정에 중요한 역할을 한다.



정밀도로지도

정밀도로지도는 규제선(차선, 경계선 등), 도로 시설(터널, 교량 등), 표지시설(교통안전표지, 노면표지, 신호기)등을 3차원으로 표현한 정밀도 25cm 이내의 전자지도로 차로 수준의 상세한 도로 노면/시설물의 위치를 모델링한 지도 데이터이다. 3차원 점(point), 선(curve), 면(polygon)의 Geometry Type과 Attribute/Relation을 가진 GIS 데이터로 구성되어 있고, 정밀도로지도의 제공 데이터의 종류는 벡터(정밀도로지도), 점군데이터, 영상정보, GNSS 수신정보, 기준점 정보를 제공하고 있다.

표 2. 정밀도로지도 데이터

<p>자율주행과 정밀도로지도의 관계</p>	<p>점군 데이터(점, 기반자료)</p>	<p>벡터 데이터(점 · 선 · 면 + 속성)</p>

○ 기존지도와의 차이점

정밀도로지도는 기존 지도가 항공측량 방식에 의해 구축되는 것과 달리 차량 탑재 레이저 스캐너(LiDAR), GNSS, IMU 등의 데이터를 이용하여 제작되며, 정확도 수준에서 1/5,000 지도의 3.5m, 1/1,000 지도의 0.7m와 달리 0.25m의 정확도로 매우 정확하게 구축한다. 자율주행차에서의 자차위치 결정, 경로의 설정 및 변경, 도로교통 규제 인지를 위한 기본 인프라로서 정밀도로지도의 활용은 앞으로 매우 확대될 것으로 예상된다.

표 3. 수치지형도 및 정밀도로지도 비교

구분	수치지형도	정밀도로지도
지도		
방법	항공사진 측량 / 2차원 전자지도	MMS 측량 / 3차원 전자지도
정확도	(1/5,000) 평면: ±3.5m / 수직: ±1.67 (1/1,000) 평면: ±0.7m / 수직: ±0.33	평면: ±0.25m / 수직: ±0.25
자율주행차 지원 정보	<ul style="list-style-type: none"> <li>• 차선 : ×</li> <li>• 도로중심선: ×</li> <li>• 규제선: ×</li> <li>• 도로경계: ○</li> <li>• 도로중심선: △</li> <li>• 교통표지: △ (도심지, 위치정보)</li> <li>• 노면표지: ×</li> </ul>	<ul style="list-style-type: none"> <li>• 차선 : ○</li> <li>• 도로중심선: ○</li> <li>• 규제선: ○</li> <li>• 도로경계: ○</li> <li>• 도로중심선: △</li> <li>• 교통표지: ○ (위치+속성정보)</li> <li>• 노면표지: ○ (위치+속성정보)</li> </ul>
활용	국토 및 도시관리, 건설, 토목, 행정, 인터넷 지도, 내비게이션 지도 등	자율주행차 연구, 개발 및 상용화, 도로 관리, 정밀 내비게이션 지도 등

[출처] 국토지리정보원

○ 정밀도로지도 구축의 중요성

자율주행차는 차량에 장착된 센서(sensor)정보와 센티미터(cm) 단위의 정밀도로 제작된 3차원 도로지도 정보를 결합하여 주행하는 차량의 위치를 차선 단위로 정확히 파악한다. 정밀도로지도는 센서가 인지하지 못하는 원거리의 상황이나 서버에서 전송하는 주변정보 및 주행에 참고할 수 있는 주행환경정보를 포함하고 있어 자율주행시스템의 의사결정에 중요한 역할을 한다.



자율주행차 센서 인식 범위 및 정밀도로지도

[출처] HMG journal

## 2) 정밀도로지도 제작

정밀도로지도의 제작 과정은 MMS(Mobile Mapping System)을 활용한 현장 조사와 점군 데이터 생성, 도화, 편집 등의 실내 작업으로 구성된다. 세부 프로세스는 다음과 같다.

### ○ MMS 표준자료제작

- GNSS/INS/IMU 자료처리
- 점군데이터 및 영상데이터의 정합
- 데이터 보정 및 정합 결과에 대한 보완 및 수정

### ○ 객체추출 및 묘사

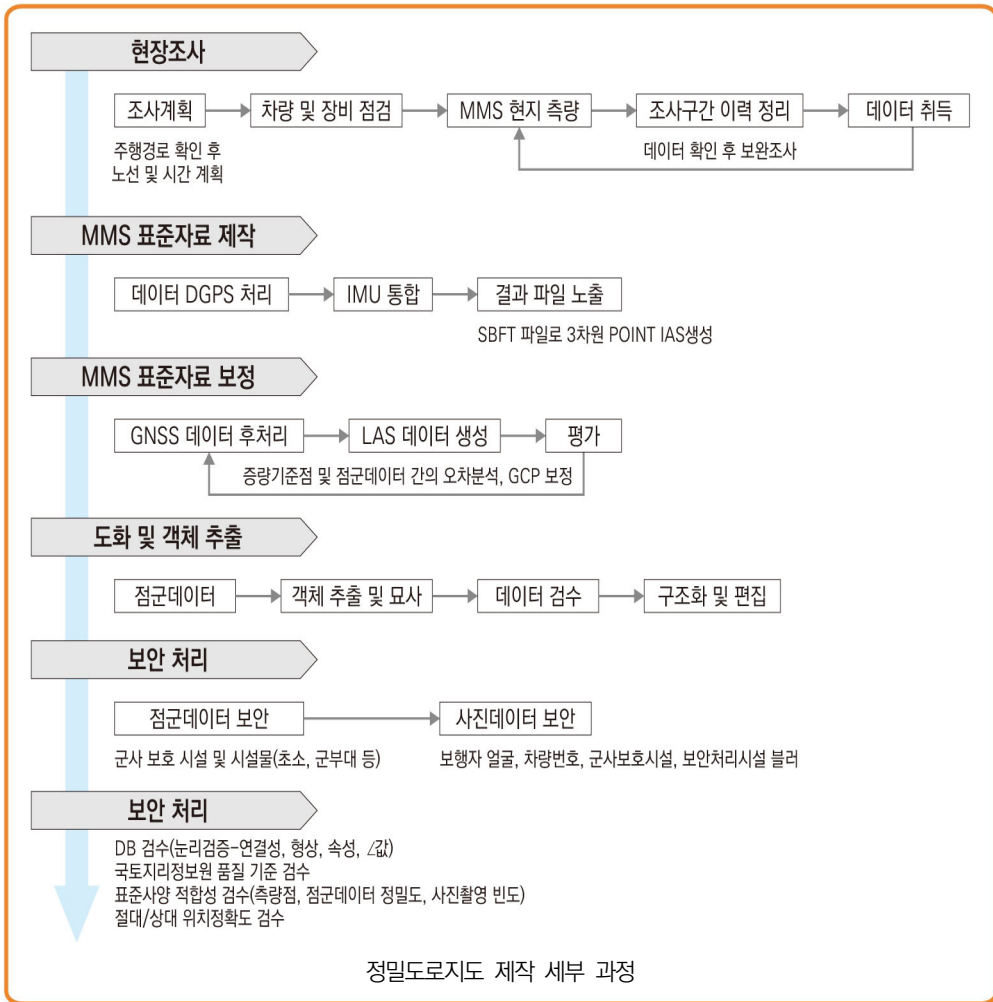
- 차선, 시설물 등의 객체추출 및 묘사
- IC/JC, 톨게이트, 터널 등의 시설물 혼재 지역의 추가 객체 추출 및 묘사
- 기 구축/신규구축 데이터의 연결성 묘사

### ○ 데이터 보안처리

- 개인정보 및 국가보안시설 등의 비공개 정보에 대한 점군데이터 삭제 및 사진데이터 블러(Blur)처리

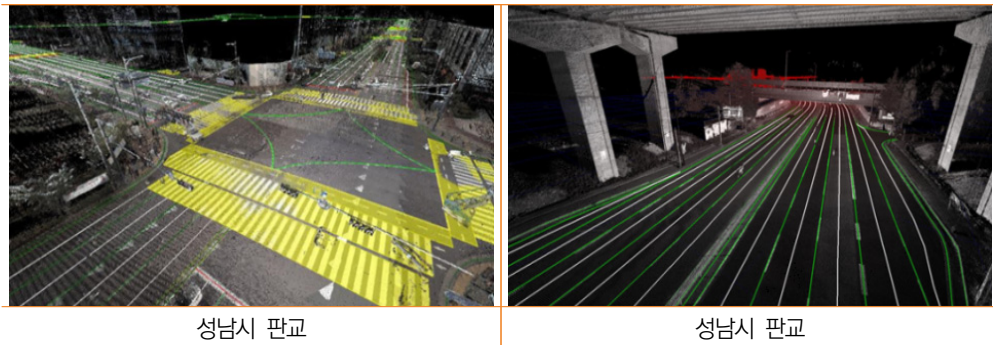
### ○ 구조화 편집

- 점, 선, 면 데이터의 공간 편집
- 편집된 공간데이터의 대한 속성 입력
- 노드/링크 데이터의 연결성 확보

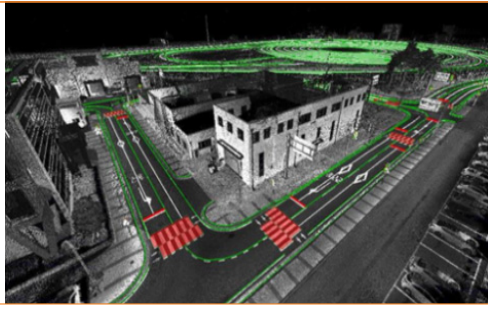


[출처] 웨이즈원(www.ways1.com)

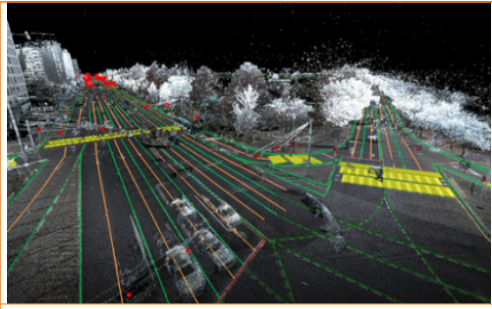
표 4. 정밀도로지도 구축 예시



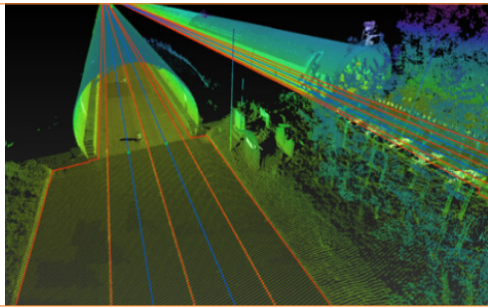




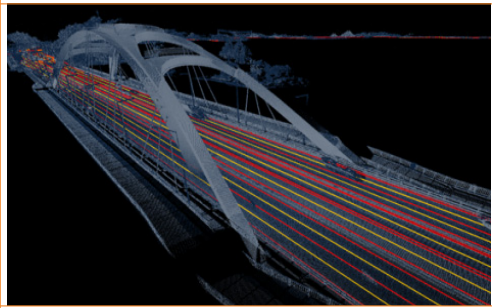
대구광역시



여의도



영동고속국도



세종특별자치시

[출처] 국토지리정보원

### 3) 정밀도로지도 구축 현황 및 계획

우리나라는 민간에서 구축하는 정밀도로지도와 별개로 정부 차원에서 국토교통부 산하기관인 국토지리정보원에서 정밀도로지도를 구축하고 있다. 2015년부터 구축을 시작해서 전국 고속도로와 주요 도심을 포함 총연장 약 18,973km 구간을 구축하였다. 정부는 올해(2022년) 정밀도로지도 신규 및 갱신 물량을 총 약 3,248km를 계획하고 있으며, 향후 2030년까지 전국 모든 도로에 대한 정밀도로 구축을 목표로 한다. 정밀도로지도 구축이 완료된 구간은 민간기업·연구기관·학교 등에서 사용할 수 있도록 무료로 배포하고 있다.



#### 4) 정밀도로지도의 갱신\*

도로의 정보는 시간, 사건·사고 발생 등에 따라 변화하기 때문에 이를 수집하고 갱신하여야 의미 있는 정보체계의 유지가 가능하며, 자율주행에 있어 이러한 도로 변화 정보는 실시간적인 정보(교통량, 사고정보 등)와 더불어 중요한 요소가 된다.

도로변화의 요인은 크게 국가계획에 따른 도로변화, 재난·재해 발생에 따른 도로변화 등으로 구분되며 그 항목은 도로 차선의 신설과 확장 또는 도로시설물의 신규 생성 및 노후화로 인한 교체, 재난과 자연재해에 의해 도로의 파손과 시설물의 훼손으로 인한 변화가 대표적인 예이다.

#### ○ 국토교통부 정밀도로지도 갱신 현황\*\*

국토교통부는 「자율주행차 상용화 지원 방안(15.5월, 규제개혁장관회의)」에 따라 '15년부터 정밀도로지도 구축을 시작하였으며, '스마트 도로 인프라 구축'의 일환으로 C-ITS

\* 설재혁 외 “우리나라 정밀도로지도의 갱신체계에 관한 연구”, (한국지리정보학회지, 2019)

\*\* 국토교통부 정밀도로지도 갱신 세부 지침

등과 연계하여 정밀도로지도 제작 중이다. 또한 「한국판 뉴딜 종합계획(20.7, 부처합동)」 및 「미래자동차 산업 발전전략(19.10, 부처합동)」에 따라 '25년까지 일반국도 및 지방도 C-ITS 설치구간 등에 대한 정밀도로지도 구축 완료를 목표로 사업 추진 중이다. 정밀도로지도는 자율협력주행, C-ITS의 기본지도이자, 자율주행 자동차의 안정적인 주행을 위한 핵심 인프라로 국민 안전 및 교통사고 예방 등을 위해 신속한 갱신체계 유지 필요가 필요하다.

## ○ 정밀도로지도 갱신 기술

### ① 국내 연구자료

정밀도로지도 갱신기술 평가를 위한 기준 도출 연구\*에서는 갱신된 정밀도로지도의 품질을 확보할 수 있도록 관련 기술의 기준 및 평가 방법을 제시하였다. 정밀도로지도는 자율주행 안전을 위해 지도의 무결성 및 정확성이 요구되며, 이를 위해 국토지리정보원(2018)에서는 검사 방법을 만들어 확인하고 있다. 갱신된 정밀도로지도 품질을 확보할 수 있도록 관련 기술의 기준 및 평가 방법이 필요하므로 자율주행을 위한 도로변화 신속 탐지 및 갱신기술을 분석하고, 통합 품질 검증을 위한 평가 기준과 항목을 선정하였다. 위치정확도와 판독정확도의 평가항목과 평가 기준을 바탕으로 실시간 변화 탐지 및 정밀지도의 갱신기술에 대한 평가 방법을 제시하였다.

### ② 민간기업 기술 현황

현대오토에버(Hyundai AutoEver)는 고정밀지도 구축을 위해 차선 및 구조물 등을 정확하게 인식하고, 변경 여부를 실시간으로 감지하는 '레드박스(RedBox)'를 개발하였다. 레드박스(RedBox)는 차량 주행 시 다양한 센서로 도로 차선, 시설물, 구조물 등을 모니터링하고 실시간 수집해 서버로 전송한다. 지도자동제작(MAC) 기술을 활용해 수집정보를 HD맵으로 가공한 뒤 딥러닝, 컴퓨터 비전, 위치 측정 및 동시 지도화(SLAM) 기술을 활용해 도로 위 객체를 추출한다. 카메라 기반 솔루션이라는 점에서 기존 HD맵을 구축·갱신 장비인 모바일 맵핑 시스템(MMS)보다 저렴한 것이 장점이다.

\* 박유경 외 “자율주행 지원을 위한 정밀도로지도 갱신기술 평가를 위한 기준 도출 연구”, (한국지리정보학회지, 2019)



- 센서와 카메라 등을 통해 차선, 도로 시설물을 정확하게 인식
- 도로의 각종 변경 정보를 탐지하여 무선 통신을 통해 변경 데이터 전송
- 지도 조사 전문 장비 MMS와 일반 차량 레드박스를 통해 도로 변화 정보 수집

현대오토에버(Hyundai AutoEver) - 레드박스(RedBox)

SKT는 HD맵 업데이트 기술을 적용한 '로드러너'를 개발하였다. 차량 운행 중 차선, 신호등, 교통 상황 등의 교통정보를 감지해 HD맵을 실시간으로 업데이트하는 기술로 자율주행차의 '두뇌'와 다름없는 HD맵에 최신 정보를 즉각 반영하는 중요한 역할을 담당한다. 서울시는 총 1,700대(시내버스 1,600대, 택시 100대)에 로드러너를 적용, C-ITS(차세대 지능형 교통 시스템) 사업에 활용하였다.



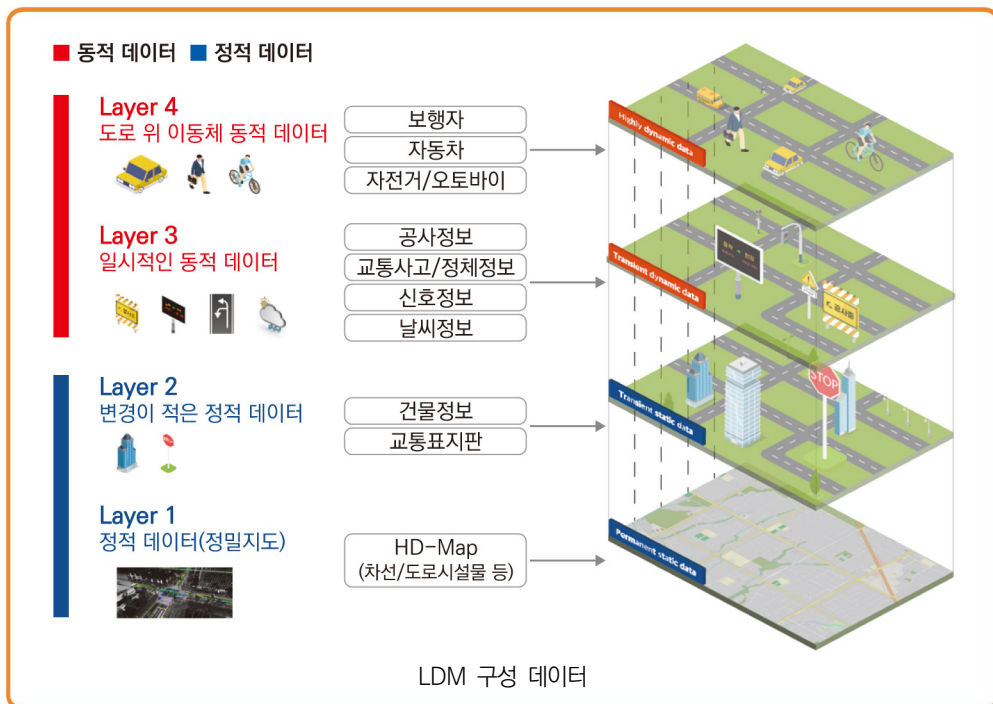
SKT 로드러너(Road Learner) 예시



## 나. LDM(Local Dynamic Map)

### 1) LDM(Local Dynamic Map) 정의

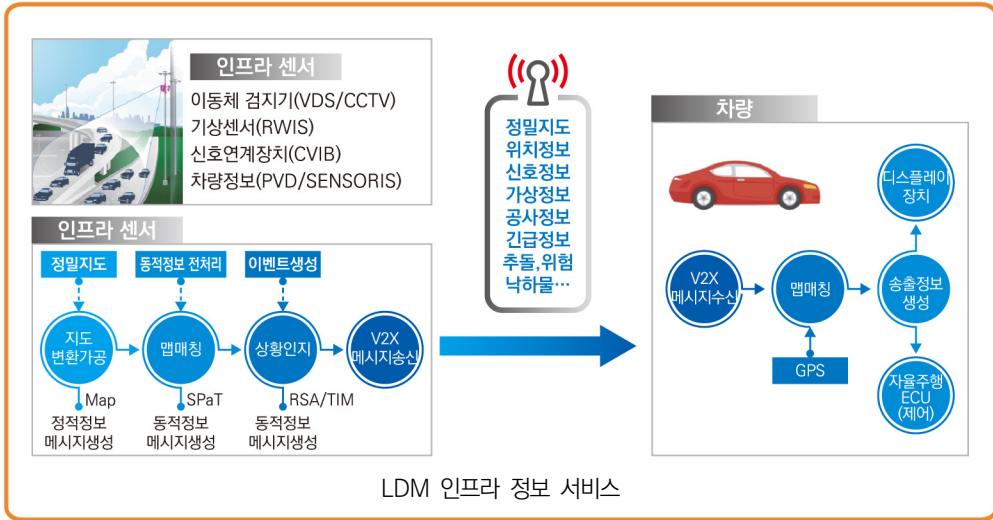
LDM(Local Dynamic Map)은 정적정보인 정밀도로지도 위에 차량 이동 및 센서 정보, 날씨, 공사 정보 등 동적정보를 실시간으로 수집하고 가공하여 저장, 관리 및 제공하는 시스템이다. 레벨4 수준의 자율협력주행 실현을 위한 정밀도로지도와 도로상 동적정보의 입출력 및 저장에 대한 ITS 분야 국제표준규격으로 노변 검지기/센서로부터 동적정보를 수집 후 정밀지도를 활용하여 서비스용 메시지를 생성 및 송출한다. LDM은 노변 인프라(정보 인코딩·제공), 차량(정보수신·디코딩), 센터(관제·모니터링)에서 데이터를 받아 동적 데이터 및 정적 데이터가 각각의 레이어에서 처리된다.



[출처] 웨이즈원(www.ways1.com)

### 2) LDM 인프라 정보 서비스 제공

정밀도로지도와 인프라 센서 데이터 및 이를 융합한 정보로 I2V 서비스를 위한 동적정보 생성하며 표준 메시지셋(J2735)으로 인코딩하여 V2X 서비스를 제공한다.



### 3) C-ITS와 LDM 자율협력주행 시스템의 차이

C-ITS와 LDM 자율협력주행 시스템의 가장 큰 차이는 인프라 정보가 운전자 개입을 거치지 않고, 자율주행차량에 직접적으로 송출되는 것이다. LDM으로 송출되는 인프라 정보는 정밀지도를 사용하여 정확한 위치정보 생성을 실시간으로 수행하며, 인프라 수집정보와 정밀도로지도의 융합 정보가 가공된 상태로 전달된다.

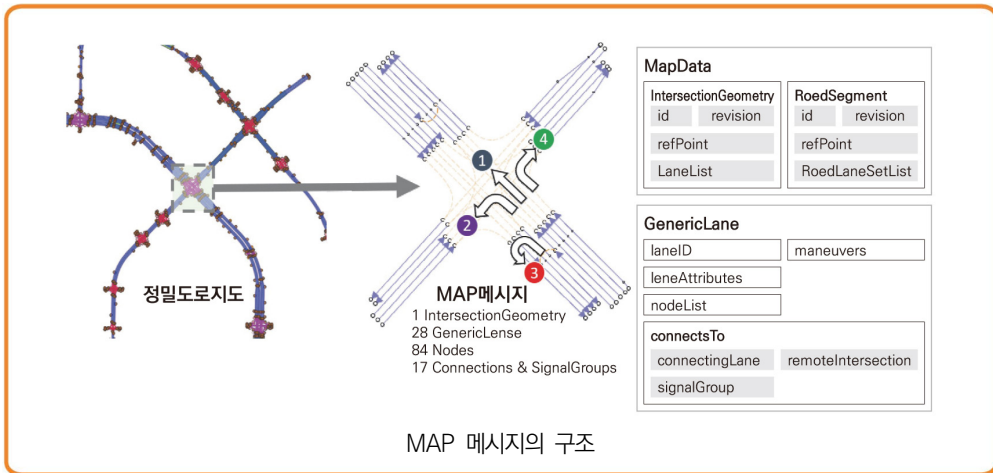
표 5. C-ITS 및 LDM 자율협력주행 도로 인프라 시스템 비교

구분	C-ITS 도로 인프라 시스템	LDM 자율협력주행 도로 인프라 시스템
서비스 목적	운전자에게 정보(텍스트/그림) 제공	자율주행 제어기에 수치화된 정보 제공
동적정보 수집방법	인프라 센서, 교통정보센터, 차량	인프라 센서, 교통정보센터, 차량
서비스 제공방법	SAE J2735 메시지셋	SAE J2735 메시지셋
위치정보 생성방법	개발 단계에서 구축된 고정된 정보 사용	정밀도로지도를 이용하여 실시간 생성 및 높은 정확도
서비스 가능 수준	수집정보의 단순 전달	수집정보+지도 융합/가공된 정보 전달
도로 변경 시 대응	소프트웨어 유지보수 개발 필요	정밀도로지도 갱신/배포로 대응 가능
서비스 흐름도		

#### 4) LDM의 서비스 기능\*

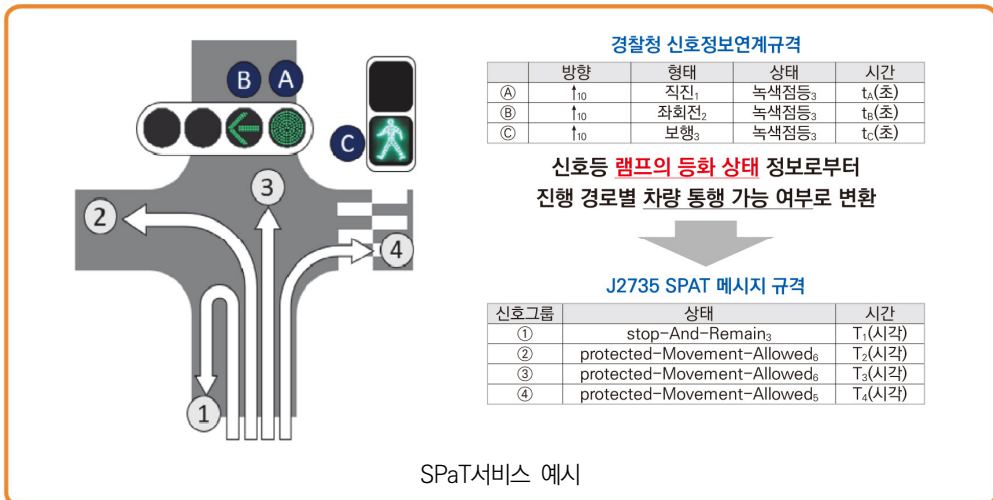
##### ○ 지도정보 서비스(MAP 메시지 생성)

교차로/도로구간 자동 추출 및 J2735 Map Data 메시지를 자동 생성하여 차로 형상, 차로 속성, 회전 정보, 연결 관계 등을 변환 옵션에 따라 선택적 생성이 가능하다. 또한 지도 갱신 시 실시간 자동 변환 수행으로 유지보수가 쉽고, 정확한 위치를 특정할 수 있다.



##### ○ 교통신호정보 서비스(SPaT 메시지 생성)

교차로 통행 규칙과 신호 상태 융합하여 통행정보를 생성한다.



\* [출처] 웨이즈원(www.ways1.com)

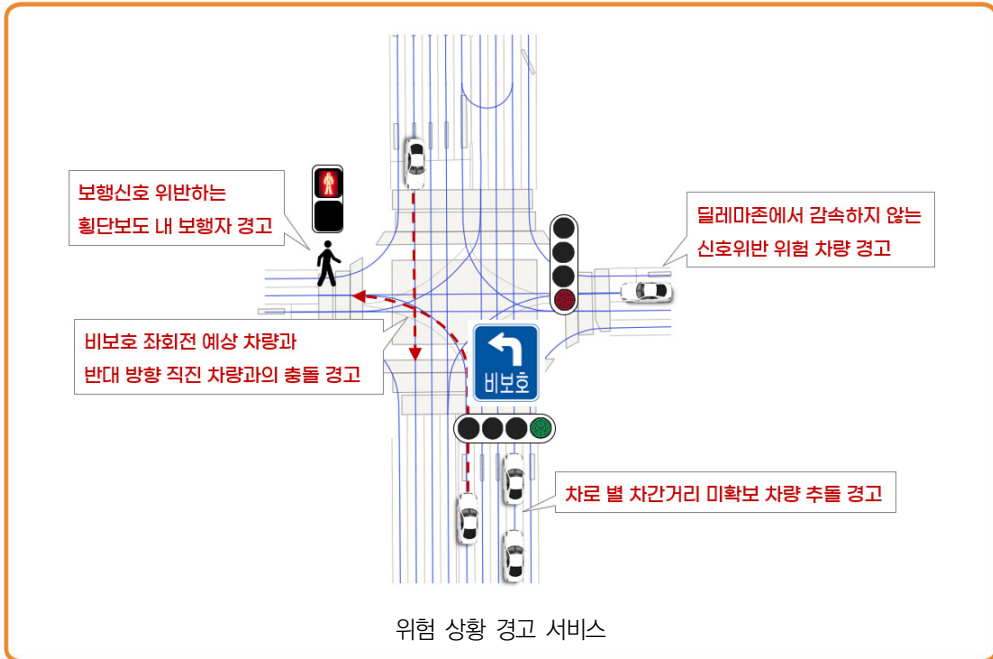
○ 운행정보 서비스(TIM 메시지 생성)

좌표, 이정, 유효차로, 길이 등으로 수집된 도로 위 상황 정보를 정밀지도를 이용하여 공간 범위를 표현할 수 있다.



○ 위험 상황 판단 및 예측 알고리즘

정밀도로지도를 기반으로 신호정보와 이동체 정보를 융합하고, 교차로의 사고 위험도를 판단/예측하여 경고 서비스를 제공한다.



### 3. 결론

정밀도로지도는 레벨 3 이상의 자율주행차 상용화에 있어 핵심 요소가 될 것이며 국토부에서는 정밀도로지도 및 데이터 베이스 구축을 위한 사업이 계속되고 있다. 국토지리정보원 국토정보플랫폼(<https://map.ngii.go.kr>)을 통해 구축된 지도를 관련 기관 및 기업, 민간에 제공하고, 국가기본도(1:5,000)의 수시 수정, 일반국도 도로대장의 갱신 등에 활용하는 방안을 모색하여 자율주행 외의 다른 분야에도 활용 범위를 점진적으로 넓혀갈 계획을 세우고 있다. 과학기술정보통신부는 국토부와 함께 자율주행을 지원하는 차량 통신방식 단일 표준화를 위해 공동 실증·시험사업을 추진한다. LTE-V2X 기능에 대해 실증을 하고, 고속도로에서 두 통신방식(LTE-V2X/WAVE)을 병행하는 시험사업을 거쳐 2024년 이후 단일 표준화를 추진할 계획이다.\*



정밀도로지도는 도로의 교통 규제 시설정보 등 주행환경정보를 고정밀 3차원으로 제공하여, 센서가 인지하지 못하는 원거리 상황 예측, 자율주행차량의 현재위치를 보정 하기 위한 Localization, 기상 악천후 등으로 부정확한 센서 정보를 보완하는 등 좀 더 정확하고 안전한 자율주행 기술에 활용될 것으로 기대된다. 따라서 도로인프라와의 정보 공유로부터 가이던스 제공에 이르기까지 레벨4 이상의 자율주행 상용화를 위해서는 정밀도로지도를 기반으로 한 자율협력주행 도로인프라 구축이 조속히 이루어져야 할 것으로 보인다.

\* [출처] 대한민국 정책브리핑([www.korea.kr](http://www.korea.kr))

# NR-V2X 사이드링크 기반 유니캐스트 및 그룹캐스트 통신

KT 융합기술원 인프라DX연구소 김남규 전임연구원 · 이석원 선임연구원



## 1. 서론

차량과 사물간 통신을 일컫는 V2X (Vehicle-to-Everything)는 V2V (Vehicle-to-Vehicle), V2I(Vehicle-to-Infrastructure), V2N(Vehicle-to-Network), V2P(Vehicle-to- Pedestrian)를 모두 아우르는 용어이다. V2X 기술은 향후 자율주행 및 C-ITS(Cooperative Intelligent Transport Systems)를 위한 통신 인프라 구축에 필수적인 요소이다. 이동통신 표준화 단체인 3GPP(Third Generation Partnership Project)는 LTE(Long-Term Evolution), 5G 등 표준화된 이동통신 기술을 기반으로 V2X 통신을 제공할 수 있는 기술 표준화를 진행해 왔다.

Release 14에서 처음으로 LTE 규격을 기반으로 V2X 통신에 대한 표준화가 진행되었다[1]. LTE의 PC5 인터페이스에서 D2D(Device-to-Device) 통신을 위한 4개의 자원 할당 모드 중 모드 3과 모드 4에서 V2X 응용을 위한 자원 할당 방법이 고려되었다. NR(New Radio) V2X는 Release 15부터 표준화된 NR 이동통신 기술을 기반으로 Release 16에서 표준화 되었다. 이전 LTE-V2X는 PC5 인터페이스 기반의 사이드링크(Sidelink) 통신에서 브로드캐스트만 지원한 반면, NR-V2X는 군집주행 등의 서비스 시나리오에서 요구되는 신뢰성 있는 통신을 제공하기 위해서 유니캐스트 및 그룹캐스트 통신을 지원한다. 브로드캐스트는 주변에 있는 모든 단말에게 메시지를 전송하는 반면, 유니캐스트 및 그룹캐스트는 그림 1과 같이 지정된 하나의 수신 단말 또는 수신 단말 그룹에게만 메시지를 전송할 수 있다.

NR-V2X를 통한 V2X 시나리오 확장을 위해, Release 16에서 군집주행(Platooning), 첨단주행(Advanced Driving), 확장센서(Extended Sensors), 원격주행(Remote Driving)과 같은 구체적인 유스 케이스 및 요구사항이 새롭게 추가되었다[2]. 아래 표 2는 NR-V2X에서 새롭게 추가된 유스 케이스에 대한 성능 요구사항 중 단말간 최대 지연시간(Maximum end-to-end latency), 전송 신뢰도(Reliability), 전송 속도(Data Rate), 최소 요구 통신 거리(Minimum Required Communication Range)에 대해 나타낸 것이다[3]. LTE-V2X에





서 논의된 기본적인 도로 안전(Road Safety) 유스 케이스에 비해, NR-V2X에서는 더 짧은 지연시간과 더 높은 전송 신뢰도, 그리고 더 빠른 전송 속도가 요구된다. 군집주행, 확장센서 등 여러 유스케이스에서 전송 속도와 신뢰도를 높이기 위해 사이드링크 기반의 유니캐스트 및 그룹캐스트 통신을 지원하는 표준이 Release 16에서 추가되었다.

표 1. NR-V2X 유스 케이스별 성능 요구사항(SL: Sidelink, UL: Uplink, DL: Downlink)

시나리오	자동화 수준	최대 단말간 지연시간(ms)	전송 신뢰도(%)	전송 속도(Mbps)	최소 요구 통신 거리(m)
군집주행	낮은 수준	20~25	90	-	350
	높은 수준	10~20	99.99	50~65	80~180
	구분 없음	500	-	-	-
첨단주행	낮은 수준	25~100	90	-	700
	높은 수준	10~100	99.99	50~53	-
	구분 없음	3~10	99.99~99.999	SL: 10~50 UL: 0.25 DL: 50	500
확장센서	낮은 수준	50~100	90~99	10	100~1000
	높은 수준	3~50	95~99.999	10~700	50~1000
원격주행	구분 없음	5	99.999	UL: 25 DL: 1	-

본 고에서는 Release 16에서 표준화된 NR-V2X 사이드링크 기반의 유니캐스트 및 그룹캐스트 통신에 대해 살펴본다. 구체적으로, 2장에서는 Release 16에서 표준화된 NR-V2X 사이드링크 통신의 특징에 대해 정리하고, 3장에서는 NR-V2X 사이드링크 기반의 유니캐스트 및 그룹캐스트 통신 과정에 대해 살펴본다. 마지막으로 4장에서 현재 진행 중인 NR-V2X 표준화 현황 및 향후 전망에 대해 간략히 정리하면서 마무리한다.

## 2. 본론

### 가. NR-V2X 사이드링크 통신 특징

Release 14 및 15에서 표준화된 LTE-V2X는 전송 신뢰도 및 지연시간에 대한 요구사항을 만족하는 기본적인 도로 안전 유스 케이스를 지원하는 것에 초점을 맞추었다면, Release 16에서 표준화된 NR-V2X는 자율주행 및 차세대 교통 시스템과 연관된 V2X 심화 유스 케이스 및 요구사항을 정의하고 이를 지원하기 위한 기술에 초점을 맞추고 있다. 본 장에서는 Release 16에서 표준화된 NR-V2X 사이드링크 통신의 특징에 대해 살펴본다.

#### 1) Flexible Numerology

LTE-V2X 사이드링크는 15kHz 대역폭의 단일 부반송파 간격(Subcarrier Spacing, SCS)만 지원한 반면, NR-V2X 사이드링크는 NR Uu 인터페이스와 마찬가지로 다양한 주파수 대역 및 부반송파 간격을 지원한다. 가변 부반송파 간격 지원을 통해 V2X 시나리오 및 QoS 요구사항에 맞게 부반송파 간격을 선택할 수 있다. 예를 들어, 부반송파 간격을 15 kHz에서 60 kHz로 증가시키면 한 슬롯을 전송하는데 소요되는 시간이 1 ms에서 0.25 ms로 감소하므로 Low Latency에 특화된 서비스를 제공할 수 있다. 낮은 주파수 대역인 FR1(410 MHz ~ 7.125 GHz)에서는 15 kHz, 30 kHz, 60 kHz의 부반송파 간격을 지원하며, 높은 주파수 대역인 FR2(24.25 GHz ~ 52.6 GHz)에서는 60 kHz 및 120 kHz의 부반송파 간격을 지원한다.

표 2. NR-V2X 사이드링크에서 지원하는 SCS 종류

$\mu$	SCS ( $2^\mu \times 15$ kHz)	주파수 범위	Cyclic Prefix	슬롯 당 심볼 수	서브프레임 당 슬롯 수	슬롯 길이	최대 반송파 대역폭
0	15 kHz	FR1	일반	14	1	1 ms	50 MHz
1	30 kHz	FR1	일반	14	2	0.5 ms	100 MHz
2	60 kHz	FR1, FR2	일반	14	4	0.25 ms	100 MHz(FR1) 200 MHz(FR2)
			확장	12			
3	120 kHz	FR2	일반	14	8	0.125 ms	400 MHz

#### 2) 사이드링크 물리계층 채널 및 시그널

NR-V2X의 물리계층 채널은 PSCCH(Physical Sidelink Control Channel), PSSCH(Physical Sidelink Shared Channel), PSBCH(Physical Sidelink Broadcast Channel), PSFCH(Physical Sidelink Feedback Channel)로 구성된다[4]. PSCCH, PSSCH는 각각 제어 메시지와

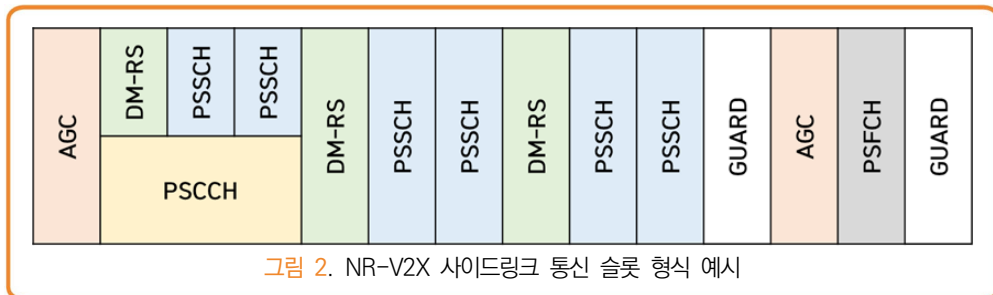


TB(Transport Block) 형태의 데이터를 전송하는데 사용된다. PSBCH는 S-PSS(Sidelink Primary Synchronization Signal) 및 S-SSS(Sidelink Secondary Synchronization Signal)와 함께 S-SSB(Sidelink Synchronization Signal Block)에 포함되어 동기화를 위한 정보를 전달한다. PSFCH는 NR-V2X에서 유니캐스트와 그룹캐스트를 지원하기 위해 새로 추가된 채널로, HARQ(Hybrid Automatic Repeat Request) 피드백을 전송하는데 사용된다.

NR-V2X에서 사이드링크 통신을 위한 제어 정보를 전달하는 SCI(Sidelink Control Information)는 1단계 SCI와 2단계 SCI로 나누어지는데, 1단계 SCI는 PSCCH를 통해서, 2단계 SCI는 PSSCH를 통해서 전달된다. 1단계 SCI는 우선순위, 주파수/시간 자원 할당, 자원 할당 주기, DM-RS(Demodulation Reference Signal) 패턴, 2단계 SCI 포맷, MCS(Modulation and Coding Scheme) 등에 대한 정보를 포함하며, 2단계 SCI는 HARQ 프로세스 ID, 새로운 데이터 표지자(New Data Indicator), 중복전송 버전, 발신자 ID, 수신자 ID, CSI 요청 등의 정보를 포함한다.

물리계층 시그널은 DM-RS, S-PSS, S-SSS, CSI-RS(Channel State Information Reference Signal), PT-RS(Phase Tracking Reference Signal)이 있다. DM-RS는 수신 UE(User Equipment)가 PSCCH, PSSCH, PSBCH를 복조하기 위한 Reference Signal로 사용된다. S-PSS와 S-SSS는 동기화를 위해 사용되며 PSBCH와 함께 S-SSB를 통해 전송된다. CSI-RS는 수신 UE의 채널 상태 정보를 측정하여 발신 UE에게 정보를 전달하는데 사용된다. PT-RS는 NR-V2X에서 밀리미터파 대역 통신을 지원하기 위해 새로 추가된 시그널로, FR2 대역 통신에서 도플러 효과로 인한 위상 오프셋을 추적할 수 있다.

그림 2는 NR-V2X 사이드링크 통신에서 데이터를 전송할 때 사용될 수 있는 슬롯 형식의 예시를 보여준다. 슬롯의 각 심볼은 PSSCH, PSCCH, PSFCH, DM-RS, AGC(Automatic Gain Control) 심볼, Guard 심볼을 포함할 수 있다. AGC 심볼은 수신 UE에서 수신 감도 조절에 사용되며, Guard 심볼은 송/수신 간 전환을 위해 사용된다. 그림 2에서 알수 있듯이, PSCCH는 연관된 PSSCH와 주파수 및 시간 영역에 대하여 다중화되어 전송된다.



### 3) 자원 할당

BWP(Bandwidth Part)는 다양한 주파수 대역 및 부반송파 간격을 지원하기 위해 NR에서 새롭게 도입되었는데, 주어진 부반송파 간격 및 Numerology에서 연속된 PRB(Physical Resource Block)의 집합으로 이루어진다. RRC 계층에서 BWP가 설정되면, 설정된 BWP 내에서 주파수 및 시간 영역에 대해 자원 풀(Resource Pool)이 정의되어, 해당 자원 풀 내에서 채널 및 시그널의 전송이 가능하다.

NR SL은 자원 할당을 위해 두 가지 모드를 지원하는데, 자원 할당을 결정하는 주체가 누구인지에 따라 모드가 달라진다.

- 모드 1: 기지국(gNodeB)이 커버리지 내에 있는 UE에 대해 자원을 할당한다. 모드 1은 또한 RRC 시그널링을 통해 자원이 할당되는 타입 1과, DCI(Downlink Control Information) 시그널링을 통해 자원이 할당되는 타입 2로 나뉜다.
- 모드 2: UE가 채널 센싱 과정을 통해 직접 자원을 할당한다. 센싱 과정은 미리 설정된 자원 풀 내에서 실행된다. 더 높은 우선순위의 트래픽을 가진 UE에 의해 사용되는 것이 아니라면, UE는 해당 자원을 전송 및 재전송을 위해 선택할 수 있다.

## 나. 유니캐스트 및 그룹캐스트 통신

### 1) 유니캐스트 및 그룹캐스트 통신 과정

앞서 언급하였듯이, LTE-V2X에서는 브로드캐스트 통신만 지원한 반면, NR-V2X에서는 다양한 유스 케이스 시나리오 및 요구사항을 만족시키기 위해 유니캐스트 및 그룹캐스트 통신이 추가되었다. 그룹캐스트 및 유니캐스트는 브로드캐스팅과는 달리 HARQ 피드백을 통해서 수신 UE가 정상적으로 수신하지 않은 경우 재전송을 통해 사이드링크 통신의 신뢰성을 향상시킬 수 있다. V2X 응용 서비스에 따라서 어떤 통신 모드(브로드캐스트, 그룹캐스트, 혹은 유니캐스트)를 사용하는지 달라진다. 예를 들어, 군집주행을 위해 그룹캐스트가 사용될 수 있으며, 이 경우, 하나의 군집이 그룹캐스트를 위한 그룹으로 설정되어 선두 차량이 전송하는 주행 관련 메시지를 군집 내 나머지 차량에게 주기적으로 전달하게 될 것이다.

V2X 메시지 송수신을 하려면, UE는 사전에 권한 부여 및 관련 정책 및 파라미터 정보가 구성되어야 한다[5]. 이 과정을 프로비저닝이라고 하며, 프로비저닝은 통신사업자에 의해 사전 구성되거나, V2X 응용 서버 또는 5G 코어 네트워크 구성 요소 중 하나인 PCF(Policy Control Function)에 의해 구성될 수 있다. 프로비저닝에서 구성되는 정보 중에는 각 V2X 응용 타입이 어떤 통신 모드를 사용하는지에 대한 매핑 정보가

포함된다. 따라서 이 구성 정보를 통해서 어떤 V2X 응용을 사용하는지에 따라서 통신 모드가 결정된다. UE에서 프로비저닝이 수행된 후, V2X 서비스에 따라 링크를 설정하여 V2X 메시지를 송수신한다.

NR-V2X를 통한 유니캐스트 링크 설정 및 통신 과정은 다음과 같다(그림 2).

- ① UE는 유니캐스트 링크 설정을 위하여, 시그널링 수신을 위한 2계층 ID를 결정한다.
- ② UE-1(링크 설정을 개시하는 UE)은 V2X 응용 계층으로부터 유니캐스트 통신에 필요한 V2X 서비스 타입, 응용 계층 ID, 응용 요구사항 등의 응용에 관련된 정보를 제공 받는다. 만약 기존에 사용하던 유니캐스트 링크를 재사용하는 경우, 별도의 링크 변경 과정을 진행한다.
- ③ UE-1은 유니캐스트 링크 설정을 위해 직접 통신 요청 메시지를 보낸다. 이 메시지에는 타겟 사용자 정보, V2X 서비스 정보, 보안 정보 등이 포함된다.
- ④ 만약 타겟 사용자 정보(특정 응용 계층 ID)가 제공되는 경우, 직접 통신 요청 메시지를 수신한 타겟 UE가 UE-1과 보안을 설정하여 응답한다. 만약 타겟 사용자 정보가 제공되지 않는 경우, 서비스 정보를 확인하여 관심이 있는 UE는 UE-1과 보안을 설정하여 응답한다.
- ⑤ 직접 통신 허가 메시지가 UE-1에게 전달된다. 이때 직접 통신 허가 메시지에는 발신 사용자 정보, QoS 정보, IP 주소 구성 정보, 링크 로컬 IPv6 주소 등이 포함된다.
- ⑥ V2X 서비스 데이터가 링크 식별자, PFI(PC5 QoS Flow Identifier) 등과 함께 유니캐스트 링크를 통해 전송된다.

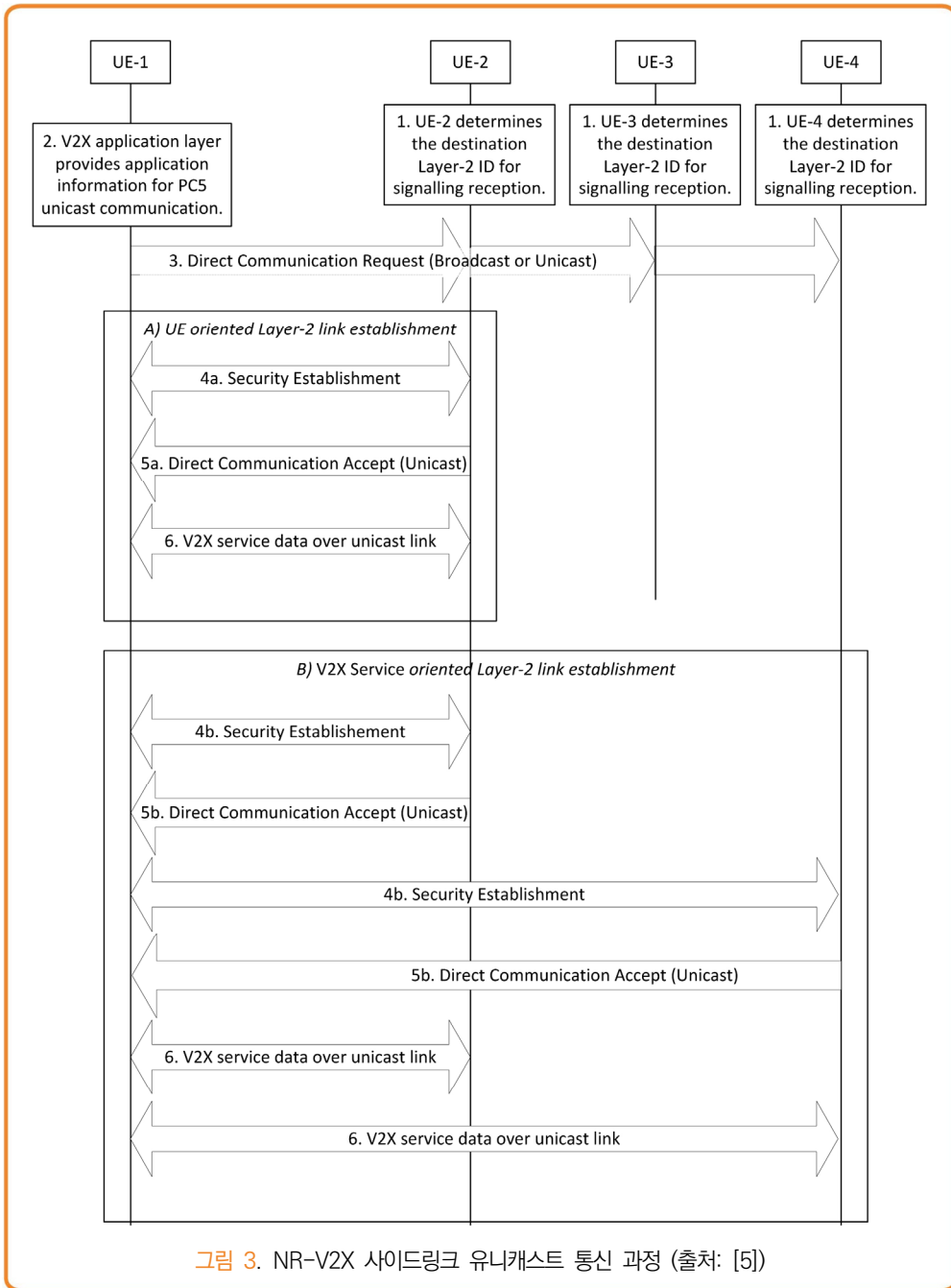
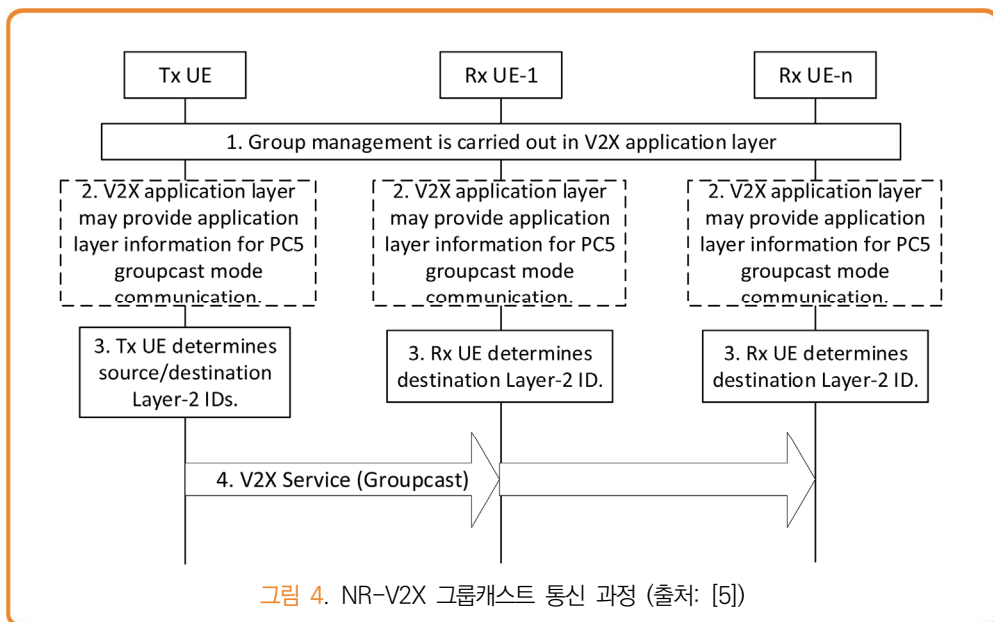


그림 3. NR-V2X 사이드링크 유니캐스트 통신 과정 (출처: [5])

NR-V2X 를 통한 그룹캐스트 링크 설정 및 통신 과정은 다음과 같다(그림 3).

- ① V2X 응용 계층에 의해 그룹의 관리가 수행된다.
- ② V2X 응용 계층에 의해 그룹 식별 정보, 응용 요구사항, 그룹의 크기, 그룹원 ID 등의 정보를 제공 받는다.
- ③ 그룹 내 발신/수신 UE는 다음과 같은 항목을 결정한다.
  - 발신자의 2계층 ID(발신 UE인 경우만), 수신자의 2계층 ID
  - PC5 QoS 파라미터
  - NR 발신 프로파일
- ④ 발신자/수신자의 2계층 ID를 기반으로 V2X 서비스 데이터를 전송한다.



## 2) HARQ 피드백

NR-V2X는 사이드링크 기반의 유니캐스트 및 그룹캐스트 통신을 지원하기 위해 HARQ 피드백을 도입하였다. HARQ는 FEC(Foward Error Correction), 에러 검출 코드 및 ARQ(Automatic Repeat Request)가 결합된 프로세스로, 이를 통해 데이터 전송의 신뢰성을 높일 수 있다. 수신 UE는 ACK(Acknowledgement) 혹은 NACK(Negative Acknowledgement)를 통해 정상적으로 TB를 수신하였는지 응답한다. 수신 UE에서 에러가 검출되었으나 FEC를 통해 에러 수정이 불가능한 경우에 HARQ 피드백을 통해 재전송을 요청할 수 있다. HARQ 피드백은 PSFCH로 전송된다.

유니캐스트 및 그룹캐스트 통신을 하는 발신 UE는 TB를 전송한 후 수신 UE로부터의 HARQ 피드백을 기다린다. 이때, ACK/NACK 피드백을 통해 가능한 응답은 총 3가지 중에 하나이다.

- ACK 수신: 수신 UE가 정상적으로 수신한 경우
- NACK 수신: 수신 UE가 수신하는 과정에서 에러가 발생한 경우
- 무응답: 수신을 위한 제어 메시지가 제대로 전달되지 않은 경우

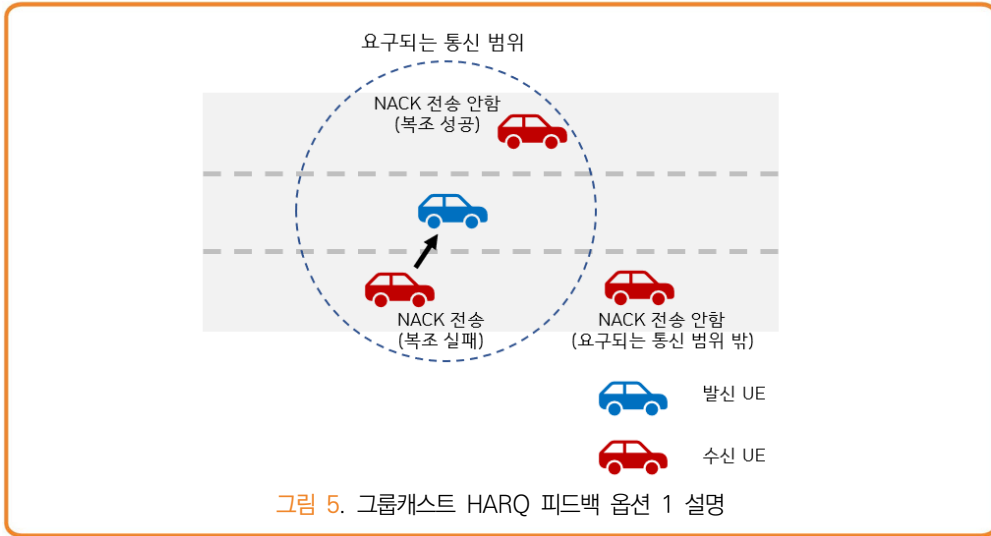
위의 경우 중 NACK를 수신하거나, 응답이 없는 경우 발신 UE는 TB를 재전송하며, 이때 전달 가능성을 높이기 위해 동일한 TB를 중복해서 재전송하는 것이 가능하다.

표 3. 통신 방식에 따른 HARQ 피드백 방식 설명

통신 방식	HARQ 피드백 방식	방식 설명	비고
유니캐스트	ACK/NACK 피드백	TB 복조 성공시 ACK, 실패시 NACK 피드백	
그룹캐스트	NACK-only 피드백 (옵션 1)	TB 복조 실패시 NACK-only 피드백	요구되는 통신 범위 내에 있는 수신 UE만 NACK-only 피드백 수행
	ACK/NACK 피드백 (옵션 2)	TB 복조 성공시 ACK, 실패시 NACK 피드백	그룹 내 모든 수신 UE가 피드백 수행

유니캐스트 통신에서는 ACK/NACK 피드백 방식만 사용한다. 수신 UE가 발신 UE가 보낸 TB를 성공적으로 복조하게 되면 ACK를 전송한다. 만약 수신 UE가 1단계 SCI는 복조에 성공하였으나, TB를 복조하는데 실패하게 되면 NACK를 전송한다.

그룹캐스트 통신은 두 가지 옵션이 존재한다. 옵션 1은 ACK는 사용하지 않으며, 복조하는데 실패한 경우에 NACK 피드백을 전송한다(그림 5). 또한 요구되는 통신 범위 내에 있는 수신 UE만 NACK 피드백을 전송하는데, 이를 위해 옵션 1을 사용하는 경우 발신 UE가 자신의 위치를 알고 있어야 한다. 옵션 2는 유니캐스트 통신에서와 마찬가지로 ACK/NACK 피드백 방식을 사용하며, 그룹 내 모든 수신 UE가 피드백을 전송한다. 옵션 1을 사용하는 경우 수신 UE는 NACK-only 피드백을 전송할 때 자원을 공유하는 반면, 옵션 2를 사용하는 경우 각 수신 UE는 ACK/NACK 피드백을 전송할 때 별도의 자원을 사용한다. 따라서 옵션 1은 옵션 2와 비교하여 자원을 효율적으로 사용할 수 있으나, 각 수신 UE 별 TB 복조 여부를 파악하는데 제한이 있다. 그룹캐스트 통신에서 발신 UE는 PSSCH를 통해 전송되는 2단계 SCI를 통해 옵션 1과 2 중 어떤 방식을 사용할 것인지 전달한다.



### 3. 결론

본 고에서는 NR-V2X와 LTE-V2X의 3GPP 표준 관점의 차이점과 NR-V2X 기반 유니캐스트, 그룹캐스트 통신의 방식 대해 알아보았다. 2022년 6월에 완료되는 것을 목표로 현재 진행 중인 Release 17 NR-V2X 표준에서는, 다양한 V2X 서비스에서 효율적인 통신을 지원하기 위해 NR 사이드링크 릴레이, 자원 스케줄링, 빔포밍, 전력 소모에 대한 개선이 이루어질 예정이다[6]. NR-V2X 기반 표준이 완성되고 향후 표준 기반의 인프라가 구축되면 자율주행, 협력주행, C-ITS 등 다양한 서비스 제공을 통한 사용자 경험 향상과, 현재보다 더 견고하고 안전한 교통 체계를 제공할 수 있을 것으로 기대한다.



## ● ● 참고문헌

- [1] M. Harounabadi, D. M. Soleymani, S. Bhadauria, M. Leyh and E. Roth-Mandutz, "V2X in 3GPP Standardization: NR Sidelink in Release-16 and Beyond," in IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 12-21, March 2021.
- [2] K. Ganesan, J. Lohr, P. B. Mallick, A. Kunz and R. Kuchibhotla, "NR Sidelink Design Overview for Advanced V2X Service," in IEEE Internet of Things Magazine, vol. 3, no. 1, pp. 26-30, March 2020.
- [3] Service requirements for enhanced V2X scenarios, document TS 22.186 V16.2.0, 3GPP, Jun. 2019.
- [4] M. H. C. Garcia et al., "A Tutorial on 5G NR-V2X Communications," in IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1972-2026, thirdquarter 2021.
- [5] Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services, document TS 23.287 V17.2.0, 3GPP, Dec. 2021.
- [6] Ganesan, Karthikeyan, Prateek Basu Mallick, and Joachim Löhr. "NR sidelink enhancement in 3GPP release 17," Journal of ICT Standardization, pp. 79-90, 2021.

# 자율주행차 상용화 이슈와 제안



한국자동차연구원 이원석 책임연구원

## 1. 서론

### 가. 글로벌 자율주행차 상용화 현황

2009년 미국 Google(현 Waymo)의 자율주행차로 인해 체계적인 제도적 논의와 함께 급격한 기술개발이 진행된 글로벌 자율주행 기술은, 마침내 2020년 Waymo One 완전 무인 유상여객 서비스(RoboTaxi)의 실현으로 이어져 마침내 자율주행이 특별한 이벤트가 아닌 일상에 일부가 되는 시대가 열렸다. Waymo One은 “안전요원 없이” 차량 단독으로 “일반인” 대상의 여객 운송 서비스를 제공하고 있으며, 이를 통해 “수익을 창출”한다는 점에서 기존의 자율주행 시연 및 시승 서비스와 명확한 차이를 보인다.

Ride with Waymo One  
- our autonomous  
ride-hailing service.

Phoenix, AZ San Francisco, CA

Now serving riders in Metro Phoenix

Waymo One™ is our ride-hailing service that's currently offering fully autonomous rides in the East Valley of Phoenix, Arizona. You can take a trip anytime you're in Metro Phoenix — just open the app and hail a car.

Download on the App Store GET IT ON Google Play

Waymo one 서비스 소개

출처: Waymo 웹사이트

이후 중국의 자율주행을 이끌고 있는 Baidu 역시 2020년 이후 창사, 창주, 북경, 광저우등 중국 각 대도시에서 공격적으로 여객 운송 서비스를 시작하여 최종적으로 100여개 도시로 확대를 목표하고 있어, 중국의 자율주행 상용화 실현이 얼마 남지 않은 모습을 보여주고 있다.



Baidu의 아폴로 로보택시

출처: 바이두 언론자료

자율주행차의 상용화는 여객 운송 서비스 뿐만 아니라 물류 운송에서도 진행되고 있으며, 현재 TuSimple이 UPS등과 협약을 통해 대형 트럭을 이용한 거점간 물류 운송 시범 서비스를 진행하여 사실상 상용화 단계에 진입하였다. 대형 트럭 서비스 외에도 Gatik은 월마트와 제휴하여 B2B 미들마일 물류 서비스를 진행하고 있으며, 유럽의 Easymile과 중국의 Startwell Westwell Lab은 각각 공항과 항만 내부의 폐쇄 공간의 무인 물류 서비스를 제공하고 있다.



Easymile의 Tracteasy 공항 자율 물류 시스템

출처: Easymile 홈페이지

이러한 자율주행차를 활용한 서비스 산업 진입과 달리, Tesla는 자율주행 기술의 소비자 판매를 목표로 하고 있다. 이를 위해 소비자 판매의 가장 큰 걸림돌인 원가 절감을 카메라 센서 집중과 정밀지도의 배제를 통해 실현하고 있으며 소비자가 납득 가능한 수준의 옵션가격을 실현하였다.

**360°**  
후방, 측방 및 전방 카메라가 최대의 가시성 제공

**250m**  
최대 250미터 범위에서의 강력한 시각적 처리

**12** 울트라소닉 센서  
주변 차량 감지를 통한 잠재적 충돌 방지 및 주차 보조

Tesla Model3 오토파일럿 소개

출처: Tesla 웹사이트

## 나. 국내 자율주행차 상용화 현황

국내에서도 자율주행 기술의 상용화를 통한 미래차 사회 대응을 위해 기술 개발과 함께 법제도 정비가 진행되고 있다. 레벨3이상 차량의 소비자 판매를 위한 제도적 장치가 준비되어 국내 완성차 업체의 소비자 판매가 22년 4분기에 예정되어 있다. 완성차 업체 외에 자율주행차를 연구개발하는 기업들의 수익 실현을 위해,

국회와 정부는 여객과 화물에 대해 자율주행 유상서비스를 허용하는 ‘자율주행 상용화 촉진 및 지원에 관한 법률’을 2019년 5월 제정해 2020년 5월부터 시행 중에 있으며, 이에 따라 각 자율주행 시범운행지구 내에서 유상운송 서비스가 가능해졌다.

이에 따라 서울, 세종, 대구, 제주에서는 여객 운수 서비스가, 광주에서는 특장차 서비스가 진행되고 있다. 국내 최초로 세종시에서 오토노머스에이투지가 카카오모빌리티 협업을 통해 15km 구간 5대 정류장에 대한 유상운송 서비스를 제공하기 시작하였으며, 서울에서는 21년 11월 42dot과 SWM에 영업면허를 수여하여 상용화 서비스를 진행하고 있다. 특히 SWM은 동일 차량으로 안양에서도 무료 운송서비스를 진행한다.

### 〈자율주행상용화촉진및지원에관한법률〉

제9조(여객의 유상운송에 관한 특례) ① 「여객자동차 운수사업법」 제81조에도 불구하고 사업용 자동차가 아닌 자율주행자동차를 활용하여 시범운행지구에서 유상으로 여객의 운송용으로 제공하거나 임대할 수 있다.

② 제1항에 따라 시범운행지구에서 자율주행자동차를 활용하여 유상운송을 하려는 자는 대통령령으로 정하는 바에 따라 국토교통부장관의 허가를 받아야 한다. 이 경우 국토교통부장관은 교통안전 확보 및 운송질서 유지 등에 필요한 조건을 붙일 수 있다.

③ 국토교통부장관 또는 시범운행지구를 관할하는 시·도지사는 「여객자동차 운수사업법」 제4조에도 불구하고 시범운행지구에서 자율주행자동차를 활용하여 노선의 운행을 하려는 자에 대하여 대통령령으로 정하는 바에 따라 한정운수면허를 발급할 수 있다.

④ 국토교통부장관 또는 시범운행지구를 관할하는 시·도지사는 제3항에 따른 한정운수면허를 발급하는 요건, 절차 및 그 밖에 필요한 사항을 정하여 미리 공고하여야 한다.

제10조(화물자동차 운송사업에 관한 특례) 시범운행지구에서 자율주행자동차를 활용하여 유상으로 화물을 운송하려는 자는 대통령령으로 정하는 바에 따라 국토교통부장관의 허가를 받아야 한다. 이 경우 「화물자동차 운수사업법」 제3조는 적용하지 아니한다.





오토노머스에이투지-카카오모빌리티의 세종시 서비스

출처: 오토노머스에이투지 웹사이트

이와 같이 국내도 글로벌 동향과 유사하게 택시-셔틀 서비스에 집중하고 있으며, 물류 분야에도 자율차 상용화가 준비되고 있다. 그러나 최근 해외에서는 이러한 흐름에 의문을 제기하는 상황이 발생하고 있다. 북미 자율주행을 선도하며 로보택시 상용화에 주력해온 존 크래프치크 Waymo CEO 퇴사(2021년 4월)와 덴 암만 Cruise CEO 퇴사(2021년 12월)로 로보택시의 상용화가 여전히 많은 난관을 안고 있는 것이 아닌지 의문을 던진다. 실제도 다수의 일반 차량과 보행자가 혼재한 도심 환경에서의 자율주행은 다양한 상용화 모델 중에서도 자율주행차의 인지-판단 기술 분야에서 가장 난이도가 높은 것으로 알려져 있으며, 현재 성공적으로 서비스를 진행하고 있는 기업이 매우 한정되어 있음을 통해 짐작할 수 있다. 다시 말하면, 현재의 자율차 상용화 모델은 국내의 다수 존재하는 자율주행 기업들 중에서 극히 일부 우수한 역량을 확보한 기업만이 성공하고, 대다수 기업들의 도태가 불가피할 것이라는 의미가 된다.

또한 물류 서비스와 택시-셔틀 서비스에 집중하고 있는 현재의 자율주행차 상용화가 계속 확대되는 경우, 최종적으로 기존 서비스 산업과의 충돌이 불가피하며, 기술을 확보하여 사업화를 진행하던 기업들도 이전 타다 사태나 우버 사태와 유사한 충격이 발생하여 기업의 존속을 위협할 수 있다.

본 기고에서는 국내 서비스 산업의 인력 현황을 검토하여 자율차의 상용화와 관련된 이슈를 도출하고, 자율주행 기술 개발에 대해 제안을 하려고 한다.

## ● 2. 본론

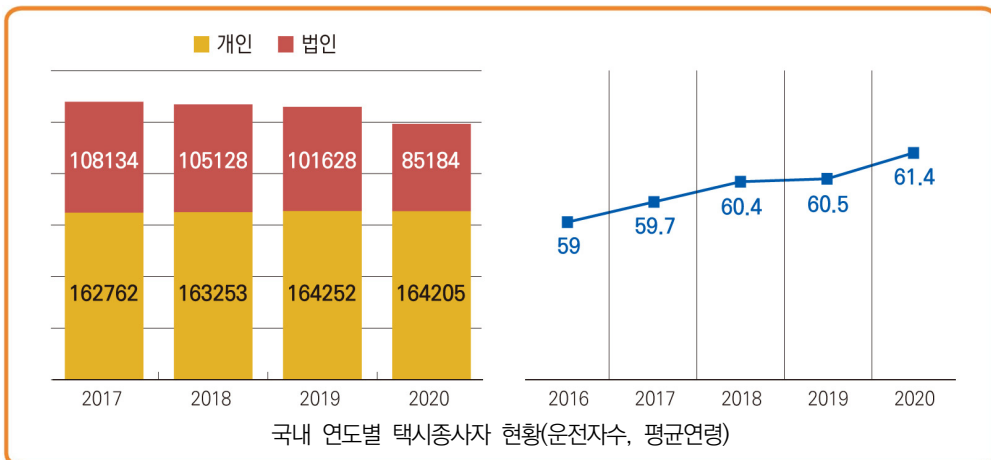
### 가. 자율주행 서비스 시장 특성

#### 1) 로보택시 서비스 시장

국내 자율주행은 승용차급 차량에 대한 자율주행 기술 개발에 집중되고 있다. 이 경우 가능한 수익 창출 방법은 (1)소비자 대상 자율주행 옵션의 판매, (2)자율주행차량을 활용하는 서비스 제공의 크게 두가지 방법이 있다.

국내의 경우 완성차 업체를 제외한 대부분의 기업은 전자를 선택하기 매우 어렵다. 낡은 조사이기도 하나 지난 2017년 국토연구원의 조사에서 국내 소비자가 원하는 LV4이상 자율주행 시스템의 옵션 가격은 평균 66만원으로 현실과 괴리가 매우 큰 수치였으며, 이후 2018년 대학생 대상 현대모비스의 조사에서도 평균 500만원 정도로 자율주행 기술개발 기업이 제품 판매를 실현하기에는 어려운 수준이다. 대부분의 자율주행 스타트업이나 IT 기업들의 경우에는 유상 여객운송을 통한 수익 창출이 불가피하며 이러한 관점에서 북미와 유사한 로보택시 서비스는 합리적인 선택으로 보인다.

이 경우 현행법의 테두리 내에서 자율주행 택시 서비스를 실현하는 가장 자연스러운 방법은 기존 모빌리티 서비스 기업에서 자율주행 차량을 인수하여 여객운송 서비스를 제공하는 것이다. 때마침 국내 택시 제도 개편과 코로나19 사태로 인해 서울의 경우 법인택시 운전기사가 2019년 30,527명에서 2021년 20,955명으로 31.4%가 급감한 상황이며, 법인택시 가동률도 2021년 평균 34.5% 수준에 머물게 되었다(서울시 도시교통실-택시정책과, '21.12).

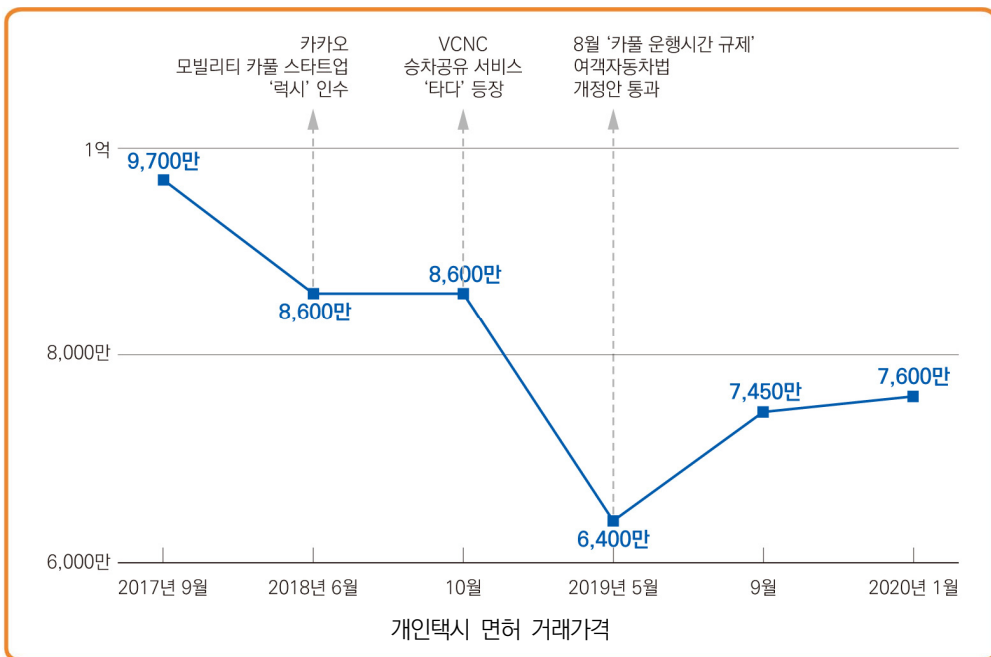


출처: 국토교통부 자료



이러한 현상은 전국적으로 유사하게 나타나고 있으며, 국토교통부 자료에 의하면, 2019년 10만 1628명이던 법인택시 운전자가 2020년 8만 5184명으로 급감한 상황이다. 따라서 법인택시 운전자를 보완하는 형태의 자율주행 차량 보급으로 현재 많이 언급되는 심야 시간대 택시 수요 대응, 기피 지역 배차 등의 문제도 수월하게 극복될 수 있을 것으로 보인다.

그러나 자율주행 택시의 확대는 불가피하게 개인택시 운전자의 경제적 손실을 야기할 수밖에 없다. 이로 인한 집단적인 반발은 과거 타다 사태를 통해 이미 증명되었으며 정부 역시 이를 인지하여 차량 감차를 시도 중에 있다. 문제는 최근 5년간 총 4049대의 면허가 반납되어 16만 4000여 개인택시 대비 단 2% 정도만 감소된 상태로 현실적인 효과가 없다는 부분이다. 더 큰 문제는 거래 가능한 개인택시 면허에 있다. 현재 서울 택시 운전자의 평균 연령은 61.4세로 개인 택시의 경우는 62.8세에 달하고 있다. 이들의 실질적인 퇴직금이자 노후 보장이 개인택시 면허의 거래가격이다. 22년 2월 현재 지역별로 8,000만원에서 2억원 사이에서 거래되고 있는 이들 면허를 통해 고령 운전자는 노후 자금을 마련할 수 있다. 만약 자율주행 택시가 현실이 되는 경우, 과거 플랫폼 기업의 시장 진입이나 카풀 사태와는 비교할 수 없는 면허 가격 폭락이 발생할 수 있으며 이는 대다수의 고령 운전자의 수익 및 노후 보장 장치가 동시에 증발하는 사태가 된다.



출처: 서울시 택시 업계

과거 국토부의 택시제도 개편안 때, 모빌리티 플랫폼 사업자들의 기여금을 통한 문제 해결 시도에서 본바와 같이, 이러한 경제적인 문제의 일부를 자율주행차를 납품하는 기업이나 서비스를 제공하는 기업이 추가적으로 부담할 우려가 있어 국내 로보택시 서비스가 과연 합리적인 시장이 될지는 고민의 여지를 준다.

## 2) 대형 화물 운송 서비스 시장

자율주행 화물 물류의 경우, 외국에서는 Hub-to-Hub의 대형 트럭을 사용한 대규모 물류 이동, Hub-to-Retail, Last mile delivery의 3단계로 분류하여 상용화가 진행되고 있으며, 이중 Hub-to-Hub에 많은 관심과 기술개발이 집중되고 있다. 북미에서는 2010년대 중반부터 트럭운전자 인력 부족이 예측되어 왔으며 이를 극복하기 위한 방안으로 자율주행 트럭 기술이 다각도로 연구되었다. 2024년 부족한 인력이 17만 명을 넘을 것으로 예상되어 이미 언급한 TuSimple을 비롯한 다양한 자율주행 기업들이 상용화 서비스를 서두르고 있으며 정부의 지원을 받고 있다.



야간 자율주행 중인 Gatik의 무인 물류 트럭

출처: Gatik사 Twitter (@Gatik\_AI)

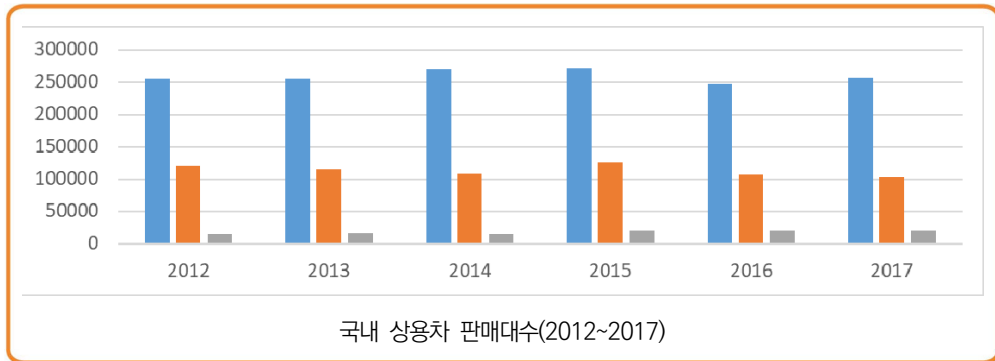


TuSimple의 자율주행 트럭과 야간 주행 영상

출처: TuSimple 웹사이트

유럽 역시 유사한 상황에 처해 있다. 브렉시트 및 코로나19 사태로 영국은 대규모 트럭 운전자 부족 사태를 겪었으며, 이로 인해 EU도 자체적으로 인력 부족 여부에 대한 조사를 진행하였다. 그 결과 EU도 물류 산업에 훈련된 인력이 부족하여 언제든 문제가 발생할 수 있음을 인식하였으며, 시장조사업체 트랜스포트 인텔리전스는 2021년 8월 유럽내 트럭 기사는 필요 인력보다 40만명이나 부족한 상황이라는 보고서를 제출하였다.

따라서 EU와 북미에서의 자율주행 트럭 기술의 개발은 인력이 부족하고 운전 부담이 큰 장거리 노선의 대형 화물트럭 중심으로 기술개발이 진행되고 있다.



출처: 한국자동차산업협회

이에 비해 국내 상용차 시장은, 신규 인력의 유입이 없다는 점에서는 글로벌 시장과 유사하나, 아직 기존 인력의 유출이 발생하지 않고 있으며, 여러 경제 이슈로 인해 잠재적인 노동 인력을 확보하고 있다는 점에서는 큰 차이를 보인다.

오히려 상대적으로 안정적인 직업으로 고려되어 운전인력의 평균연령이 2017년 평

균 54세 이후 년평균 0.5세씩 증가하는 고령화가 심화되고 있다. 이런 상황에서 외국과 유사한 형태의 무인 물류 방식 자율주행 트럭 도입은 기존 인력과의 마찰을 피할 수 없으며 이는 이미 논의한 택시와 유사한 사회적 충격과 혼란이 발생할 것임을 예상할 수 있다.

## 나. 상용화 분야 제안 및 필요 기술

자율주행 트럭 및 로보택시를 통한 자율주행차 상용화가 기존 산업과의 충돌을 최소화하면서도 본연의 역할을 다할 수 있게 하려면 자율주행차가 서비스하는 영역과 기존 서비스 영역을 분할하여 초기 시장을 형성한 후 단계적으로 시장을 혁신해 나가야한다.

이와 관련하여 지난 2021년 11월에 발표된 서울시의 자율주행 비전 2030은 좋은 가이드가 될 수 있다. 서울시는 자율주행을 통해 “남녀노소 구분 없이 모든 시민이 24시간 차별 없는 이동의 자유를 보장”할 것을 선언하고 있으며, 2023년에는 심야시간대 자율주행 버스 노선 신설, 2024년 순찰·청소 분야, 2025년 제설차 분야에 자율차를 도입할 계획을 제시하였다.

이는 자율주행 여객운송의 영역을 인간 운전자가 기피하는 시간대 및 노선에 집중하여 기존 인력과의 마찰을 최소화하고 일반 시민들의 이동권을 강화하여 자율주행이 일상에 빠르게 녹아들 기회를 제공한다. 상용차량의 자율주행 역시 일반 물류 영역이 아닌 제설차와 같이 비정기적이고 돌발적인 운행이 요구되는 영역에 집중한다. 이러한 영역의 경우 대규모 보급과 수익 창출에는 한계가 명확하나 안정적인 시장 진입과 함께 공공부분과 연계를 통한 안정적인 수익 확보가 가능하다는 장점을 갖는다.



출처: 한국 농어촌 공사 자료

이러한 사업 영역으로는 2014년부터 시범사업이 진행된 농촌형 교통모델 사업도 좋은 예시가 될 수 있다. 이는 대중교통이 취약한 지역의 고령·영세 주민들에게 대체 교통수단을 제공하여 실질적인 이동권을 보장하는 사업으로 수요응답 기반의 셔틀버스나 택시를 제공하는 교통복지 사업이다. 2020년 농림축산식품부 자료에 의하면 배정된 예산 중 51% 정도만 집행이 가능할 정도로 일반 여객운수 운전자의 호응을 확보하기 어려워 자율주행이 도입되더라도 별다른 마찰이 우려되지 않는 장점도 있다.

그러나 이러한 대체 분야의 자율주행차 상용화가 가능한지는 점검의 필요가 있다. 국내 대부분의 자율주행 기술은 대도시 도로와 같이 인프라 정비된 도로 상태를 전제로 안정적인 기상 조건을 고려하여 개발되었다. 따라서 일반 운전자가 기피하는 지역 조건, 기상 조건에서 정상적으로 동작할지에 대한 의문이 존재하며 특히 농촌형 교통 모델과 같이 외곽지역 도로 특성에 대응이 가능할지는 확인이 부족하다 할 수 있다.



농촌형 교통모델의 대상 지역 예시

기존 자율주행 기술과 가장 큰 차이가 예상되는 영역은 주행 제어 영역이라고 예상할 수 있다. 물론 기존의 도로 조건과 달리 불명확한 도로 경계 및 차선, 비정형 장애



물의 존재, 돌발적인 장애물 발생 등 인지 영역에서도 추가로 개발되거나 보완되어야 할 기술이 존재한다. 그러나 주행제어의 경우에는 기존과 여러 가지 상이한 전제 조건들로 인해 전체적인 수정이 필요하다.

기존의 주행 제어는 충분히 평탄하고 전체적으로 균일한 노면 마찰을 갖는 도로 상에서 조향 제어를 가정한다. 또한 교차로 등을 제외하면 충분히 작은 곡률을 전제로 주행 제어를 수행한다.

그러나 본 기고에서 제안하는 서비스 영역에서는, 악천후로 인한 노면 물 웅덩이 또는 빙결에 의한 편마찰, 노면 관리 상태 부족으로 인한 부분적인 파손으로 인해 균일한 노면 조건을 가정할 수 없으며, 대부분의 도로가 횡경사와 종경사가 결합된 복합적인 경사도를 보이고 급격한 곡선을 포함하는 등 일반적인 도로와는 상이한 주행 조건을 갖게 된다. 이러한 상황에서 탑승객의 승차감과 안전을 보장하기 위해 급격한 제어는 최대한 지양해야 하므로 주행 제어의 난이도는 더욱 높아지게 된다.

해외에서는 특별한 기상 조건이 고려되어야 하는 국가나 대형 화물차의 자율주행 기술 개발 과정에서 이에 대한 연구가 진행되었다. 핀란드 기술연구센터 VTT는 자체 제작 자율주행차로 눈길에서 40KPH 자율주행을 진행하여 눈덮인 노면에서 안정적인 인지-제어 기술을 증명하였다.



핀란드 기술연구센터의 Martti 자율주행차

앞서 소개한 TuSimple의 경우에는, 화물 적재에 의한 차량 조건 변동에도 차로 중앙 기준 5cm 이내 오차로 경로 유지하는 제어 기술을 증명하였으며 이를 해당 기업의

경쟁력으로 적극 홍보하고 있다.

글로벌 경쟁력 확보와 국내 자율주행차 상용화를 위해, ESC 등과 같은 사시 능동 제어 기술과는 별개로, 다양한 외란 상황에서 안정적인 주행 제어가 가능하도록 외란을 식별하고 이에 적응하여 주행 제어를 가변할 수 있는 지능형 제어 기술이 개발되어야 한다. 이를 위해 현재의 센서 및 인지 지능 중심의 자율주행 기술 개발을 다각화 하여 다양한 노면 및 환경 조건에서 차량의 주행 제어 성능을 향상할 수 있도록 차량 제어 기술 및 주행 제어 부품에 대한 연구개발도 확대될 필요가 있다.

### ● 3. 결론

자율주행차의 상용화는 피할 수 없는 흐름이며, 2030년 이전에 로보택시와 자율주행 셔틀버스가 대중 교통의 중심이 될 것은 분명해 보인다. 또한 화물운송 인력의 고령화로 인해 대형 물류도 상당 부분 자율주행 기술에 의존하게 될 것이다. 하지만 향후 5년간은 기존 인력과의 마찰이 불가피하므로, 자율주행차 상용화에서 핵심적인 서비스 시장이 아니라, 기존 운전자를 보완하는 영역에서 공존하며 미래차 사회 관련 정책을 정비하고 환경을 정돈할 시간을 확보하는 현명한 접근이 필요하다.

대다수의 국내 완성차 기업, IT 기업, 스타트업이 시도하고 있는 도심도로 자율주행이라는 획일적인 접근 보다는, 각 기업별로 명확한 시장을 선정하여 이에 맞춘 인지-판단-제어 기술의 개발과 함께 다양한 분야에서 자율주행 기업들이 수익을 창출하며 생존할 수 있도록 대비하는 지혜도 필요하다.

특히 현재의 센서와 인지 기술 중심의 자율주행 기술 개발을 판단 및 주행 제어 부분으로도 확장하여 기술개발을 다각화 할 필요가 있다. 또한 기술 개발과 병행하여, 센서분야와 유사하게 다양한 환경에서 주행제어 성능을 시험하고 인증하기 위한 기준 및 제도에 대한 검토가 요구된다. 이를 위해서는 다양한 기업들에서 공통적으로 참고하고 적용할 수 있는 표준의 제정이 필요하며, 기존 능동 사시제어 관련 표준과의 연계를 통해 빠르게 표준 기반의 마련이 가능할 것으로 생각한다.

기존 ADAS의 경우처럼 국내 대부분의 기업들이 도태되고 외국 기업들의 기술에 의존하는 상황이 발생하는 사태를 방지하기 위해서도, 국내의 현실을 충분히 고려한 합리적인 기술 개발과 제도 정비가 필요하며 이를 통해 국내 자율주행 서비스 시장의 보호와 토착 기업들의 성장이 실현될 수 있을 것이다.