국토교통부

TS 한국교통안전공단 자동차안전연구원

레벨4 자율주행자동차 제작·안전 가이드라인

2020.12.15(화)

목 차

1 추진 배경

○ 2019년 12월 31일 국토교통부는 세계 최초로 레벨3 부분자율주행자동차 안전 기준을 마련하였고, 2020년 4월 7일 자동차손해배상보장법을 개정 공포하여 자율주행자동차 관련 사고책임과 원인 규명을 위한 사고조사위원회를 도입함으로써 자율주행자동차 상용화를 위한 제도적 기반을 확보하였다.

○ 또한, 정부는 2019년 10월 15일 「미래차 비전 선포식」을 통해 2024년까지 레벨4 완전자율주행을 위한 제도적 기반을 구축한 후, 2027년 상용화 목표를 제시하였다.

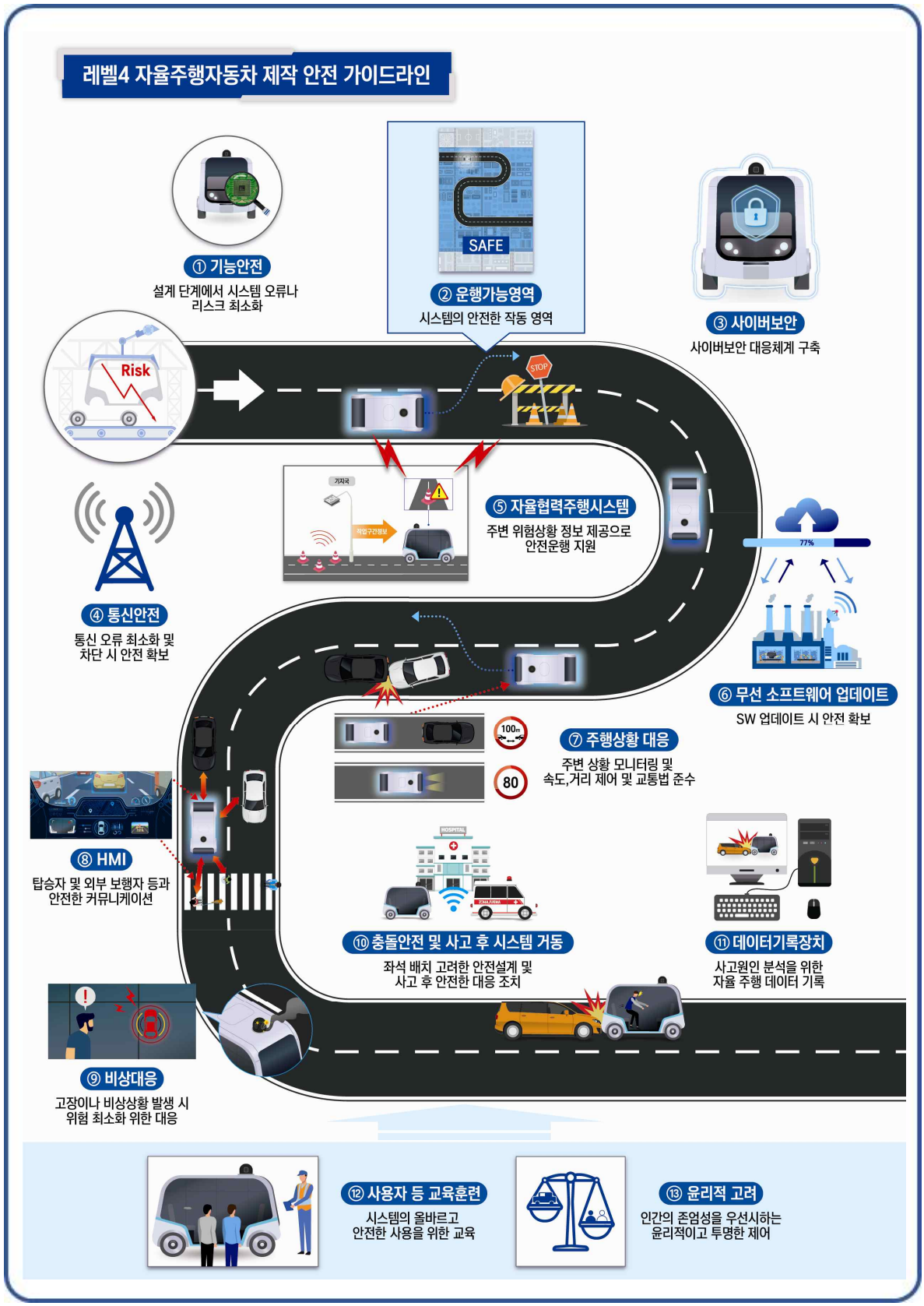
○ 한편, 2016년 자율주행자동차의 실도로 시험운행을 위한 임시운행허가제도가 도입된 이후 현재까지 국내·외 자동차제작사, IT 및 전자회사, 스타트업, 대학 및 국책연구소 등 다양한 기관에서 120여대의 자율주행자동차가 운행허가를 받아서 운행 중이며, 소형차에서 대형 승합 및 무인셔틀에 이르기까지 다양한 형식과 레벨의 자율주행기술이 상용화를 준비 중이다.

○ 본 가이드라인은 레벨4 이상 완전자율주행자동차의 상용화를 위한 제도적 기반이 완비되기 이전에, 중요한 안전 관련 항목들과 각 항목별로 자율주행시스템을 설계·제작하기 하기 위한 지침을 정함으로써, 제작자나 운영자 또는 사용자(소비자) 등이 자발적으로 확인·준수하도록 하여 사고 없는 안전한 자율주행 기술개발 환경을 구현하고자 한다.

2 적용 범위

○ 본 가이드라인의 적용대상은 사람이 직접 운전에 관여하지 않는 레벨4 이상 완전자율주행시스템이 장착된 자동차를 설계·제작 및 운행하려는 자와 그 사용자(소비자) 등을 대상으로 한다.

○ 본 가이드라인은 자율주행시스템 자체의 안전성을 확보하기 위한 ‘시스템 안전’, 주행 시 안전한 상호작용 및 상황대응을 위한 ‘주행 안전’ 및 사회적 수용성을 높이기 위한 ‘안전교육 및 윤리적 고려’의 3개 분야에 대해 총 13개 안전항목으로 구성한다.


레벨4 자율주행자동차 제작 안전 가이드라인
① 기능안전
설계 단계에서 시스템 오류나 리스크 최소화
SAFE
② 운행가능영역
시스템의 안전한 작동 영역
③ 사이버보안
사이버보안 대응체계 구축
Risk
STOP
④ 통신안전
통신 오류 최소화 및 차단 시 안전 확보
⑤ 자율협력주행시스템
주변 위험상황 정보 제공으로 안전운행 지원
77%
⑥ 무선 소프트웨어 업데이트
SW 업데이트 시 안전 확보
100m
80
⑦ 주행상황 대응
주변 상황 모니터링 및 속도,거리 제어 및 교통법 준수
⑧ HMI
탑승자 및 외부 보행자 등과 안전한 커뮤니케이션
HOSPITAL
⑩ 충돌안전 및 사고 후 시스템 거동
좌석 배치 고려한 안전설계 및 사고 후 안전한 대응 조치
⑪ 데이터기록장치
사고원인 분석을 위한 자율 주행 데이터 기록
⑨ 비상대응
고장이나 비상상황 발생 시 위험 최소화 위한 대응
⑫ 사용자 등 교육훈련
시스템의 올바르고 안전한 사용을 위한 교육
⑬ 윤리적 고려
인간의 존엄성을 우선시하는 윤리적이고 투명한 제어

3 용어 정의

○ ‘자율주행자동차’란 「자동차관리법」 제2조제1호의3에 따른 운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차를 말한다.

○ ‘자율주행시스템’이란 운전자 또는 승객의 조작 없이 주변상황과 도로 정보 등을 스스로 인지하고 판단하여 자동차를 운행할 수 있게 하는 자동화 장비, 소프트웨어 및 이와 관련한 일체의 장치를 말한다.

○ ‘기능안전’이란 전기 및 전자 시스템의 오류로 인한 위험발생을 방지하고 나아가 성능의 한계 및 운행환경 등에 기인한 의도치 않은 위험으로부터 안전을 확보하기 위해 설계, 제작 및 검증(사용단계에서의 모니터링에 의한 검증 포함) 등 각 단계에서 수행해야 하는 활동을 총칭한다.

○ ‘운행가능영역’이란 자율주행시스템의 기능이 정상적이고 안전하게 수행 될 수 있는 작동영역(도로, 기상, 교통 등)을 말한다.

○ ‘위험최소화운행’이란 고장 또는 운행가능영역 이탈 등에 의해 자율주행시스템의 작동 및 제어 관련 기능이 정상적으로 수행되지 않거나, 정해진 목적지까지 운행이 불가능하게 된 경우 시스템이 스스로 알아서 운행에 따른 위험을 최소화하기 위해 수행하는 기능(감속이나 갓길 정차 등)을 말한다.

○ ‘HMI(휴먼-머신 인터페이스)’란 자율주행시스템과 인간 사이의 상호 작용을 말하며, 시스템이 의도하는 기능 및 성능과 주행상황에 대한 정보를 정확하게 인간에게 전달하는 것을 말한다.

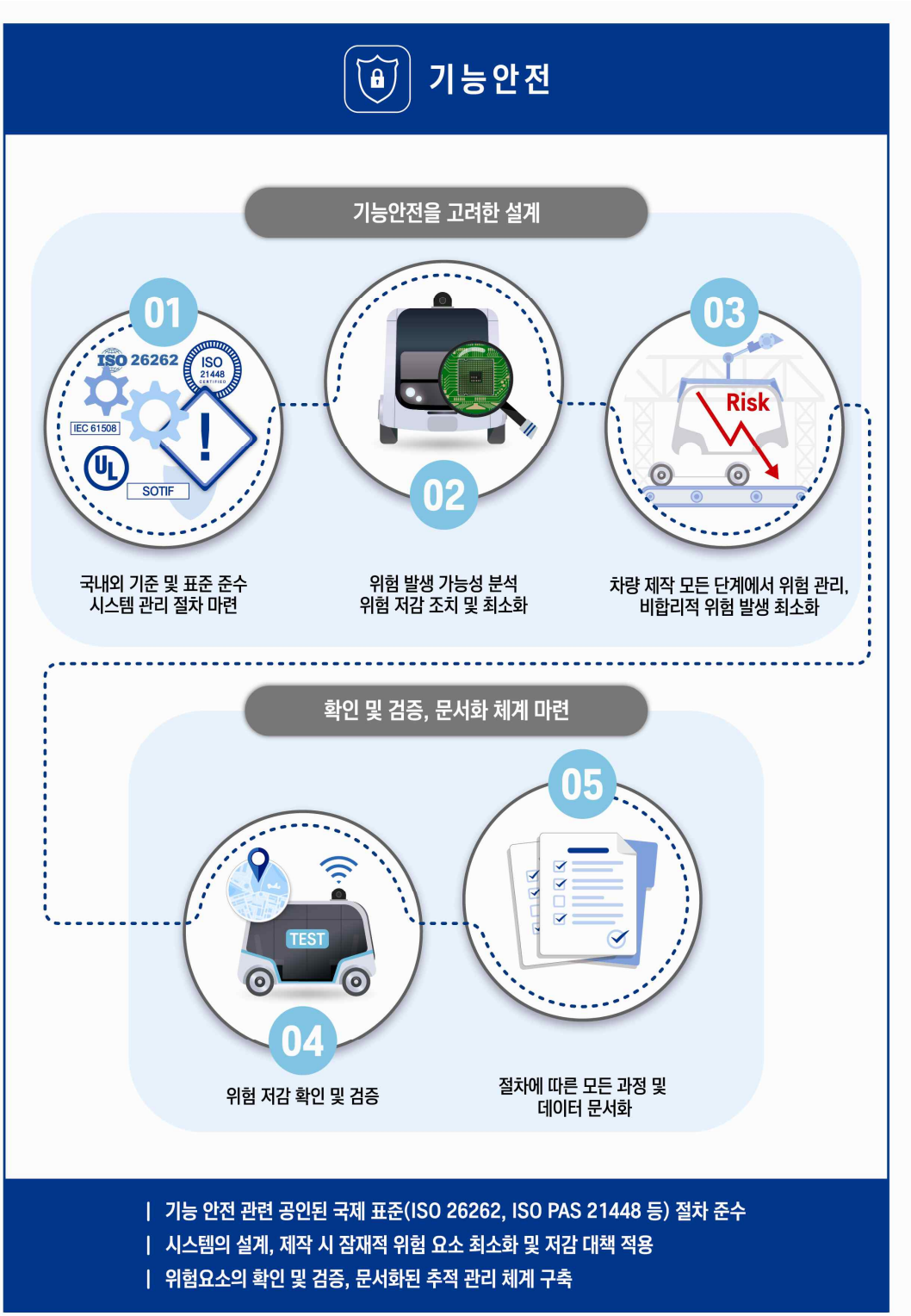
○ ‘협력주행 통신장치’란 무선통신 기술(WAVE, C-V2X 또는 5G)을 사용하여 자동차와 자동차 간(V2V) 및 자동차와 노변기지국 간(V2I)에 다양한 안전메시지를 송·수신할 수 있는 장치를 말한다.

○ ‘자율협력주행시스템’이란 도로상의 신호기, 안전표지 및 교통시설 등을 활용하여 자율주행기능을 지원 · 보완함으로써 효율성과 안전성을 향상시키기 위한 장치를 말한다.

4 시스템 안전

① 기능안전

자율주행시스템 자체의 오류나 오작동 등에 의한 위험을 줄이기 위해 국제표준에서 정하는 절차와 방법을 준용하여 안전하게 제작한다.



○ 자율주행시스템의 설계상 잠재적인 위험요인을 최소화하고 의도치 않은 위험 발생을 줄이기 위해 공인된 국내외의 기준·표준(ISO 26262, ISO PAS 21448 등)에서 규정하는 절차를 따른다.

- 자율주행시스템은 센서, 컨트롤러, 액추에이터 등 다양한 장치들과 단위요소(부품, 소자 및 소프트웨어 등)들로 구성되어 있음
- 이들 각 단위요소들을 조합하여 시스템을 제작하고 운영하기 위해서는 다양한 사용조건에서 잠재적인 오류와 의도치 않은 기능 이상이 발생 하지 않도록 사전 검토 및 안전성 검증을 수행하며, 이를 위해서는 국제표준*,**에서 정하는 절차가 준용될 수 있음

* ISO 26262(Functional safety) : 자동차에 탑재되는 전기 및 전자시스템의 오류로 인한 위험 및 사고발생을 방지하기 위한 국제 표준으로, 안전을 확보하기 위한 절차(process)에 따른 활동과 유무형의 증거물(문서화 과정 등)을 정의함

** ISO PAS 21448(Safety Of The Intended Functionality) : ISO 26262 표준 등에서 의도하는 대로 설계 및 제작이 되어 HW 또는 SW 오작동이 없다 하더라도, 성능상의 한계나 사용자 요인 또는 주변의 운행 환경 등에 따라 의도지 않은 동작 오류가 발생할 수 있으며 이를 줄이기 위한 활동 및 절차를 규정함(충분한 자율주행기술력이 축적되지 않은 상태에서 운행 시 발생할 수 있는 보다 다양한 위험요인을 최소화하기 위함)

○ 자율주행시스템의 각 요소 및 작동단계에 따른 잠재적인 위험요인 또는 고장 유형과 이에 따른 위험 발생 가능성을 분석하고 위험을 최소화하기 위한 대응조치를 수립한다.

- 위험 요인 : 전기회로 단선, 센서 수신 장애, 소프트웨어 오류 등
- 고장 유형 : 서브시스템(조향, 제동 등) 작동 이상, 주행위치 확인 오류 등
- 위험 발생 : 차선이탈로 인한 타차량 충돌, 전방 보행자 인지 불가로 인한 사고 위험, 교통법규 위반 등
- 대응조치 : 시스템 고장에 대비한 이중 설계, 서브시스템 고장 발생 시 셧다운(가속 제어 불가능시 가속기능 셧다운 및 감속), 무인시스템의 경우 제어센터의 긴급 제어 가동 등

ㅇ 자율주행시스템의 각 기능에 비합리적인 위험이 발생하지 않도록 한다.

- 비합리적인 위험 : 주행차로 전방의 보행자를 인지하지 못하여 발생한 사고, 교차로가 아닌 지역에서 좌우회전 등

ㅇ 위의 과정은 모든 운행가능영역을 포함하여 검토되어야 하며, 자율주행시스템의 정상적인 작동여부를 확인 및 검증한다.

- 자율주행시스템의 모든 운행가능영역을 대상으로 국제표준(ISO 26262 등) 절차에 따라 시스템 안전성의 확인 및 검증 과정 수행

ㅇ 위의 절차에 따른 모든 과정과 데이터는 추적이 가능한 형태로 문서화한다.

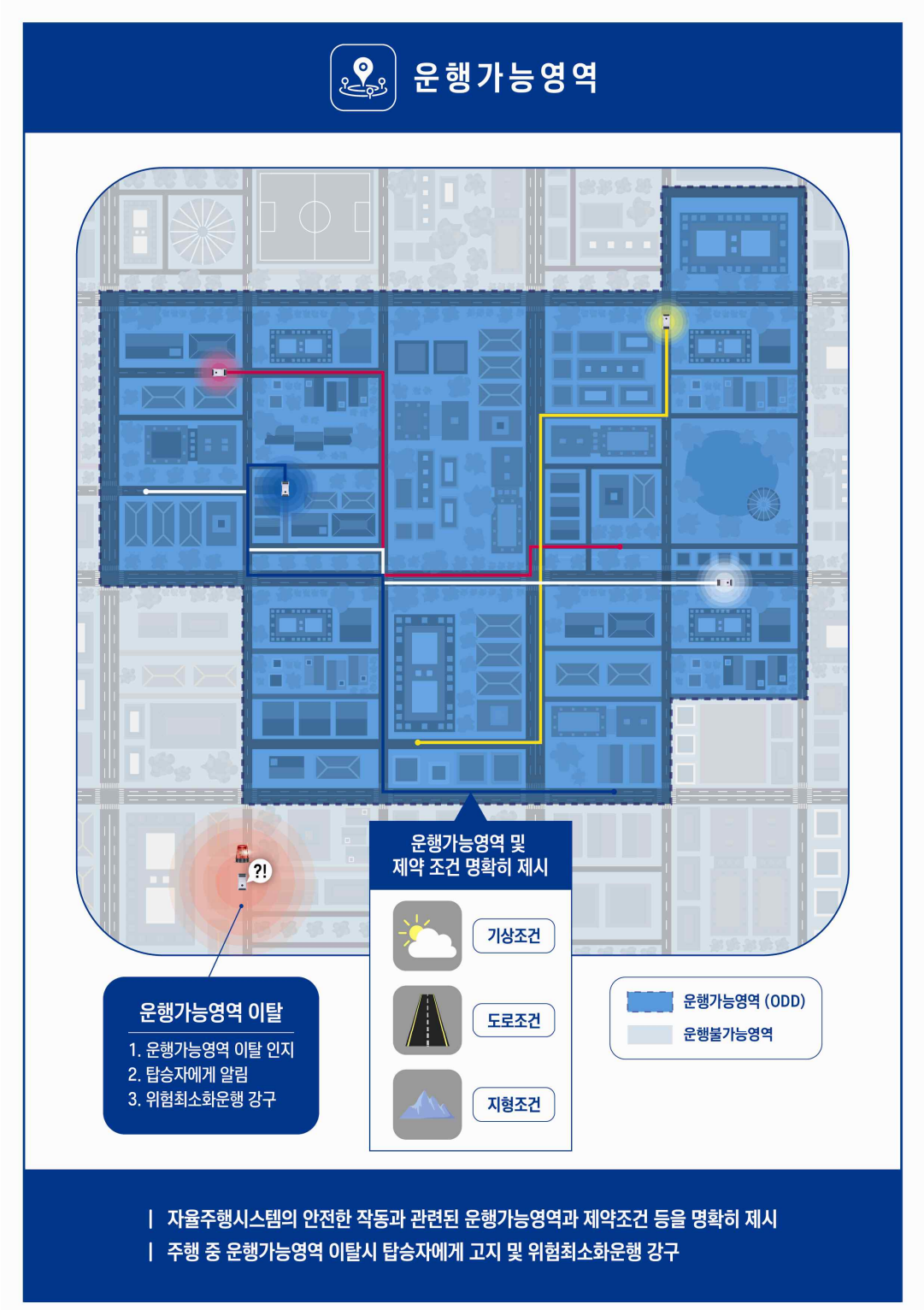
- 시스템 안전 확보를 위한 위험분석 방법 및 과정, 위험에 대한 대응조치, 검증 과정 등을 문서화하여, 향후 문제 발생 시 추적을 통해 원인 분석 및 유사 문제 재발 방지

ㅇ 자율주행시스템 이외의 운행과 관련된 책임을 공유할 수 있는 다른 객체(운전자 또는 무인운전인 경우 운영관리센터)에 의한 대응방안이 포함되는 경우 대응방식과 절차를 구체적이고 명확하게 제시한다.

- 시스템 안전 확보를 위한 대응전략에 운전자나 운영관리센터 등이 포함되는 경우(시스템 고장 시 운전자나 운영관리센터가 백업을 해야 하는 경우 등) 이를 명확히 확인할 수 있어야 함

② 운행가능영역

자율주행시스템의 안전한 작동과 관련된 운행가능영역을 명확히 제시한다.



ㅇ 운행가능영역에는 도로유형, 지리적 범위, 기상환경, 속도범위 및 기타 제약조건들을 포함한다.

- 자율주행시스템이 정상적이고 안전하게 작동될 수 있는 영역(도로, 기상, 교통 등)을 명확하게 제시하여 운전자나 운영자 등이 쉽게 확인할 수 있어야 함

- 운행가능영역을 명확히 제시함과 동시에, 운행가능영역을 벗어나는 경우 시스템의 상태정보 제시

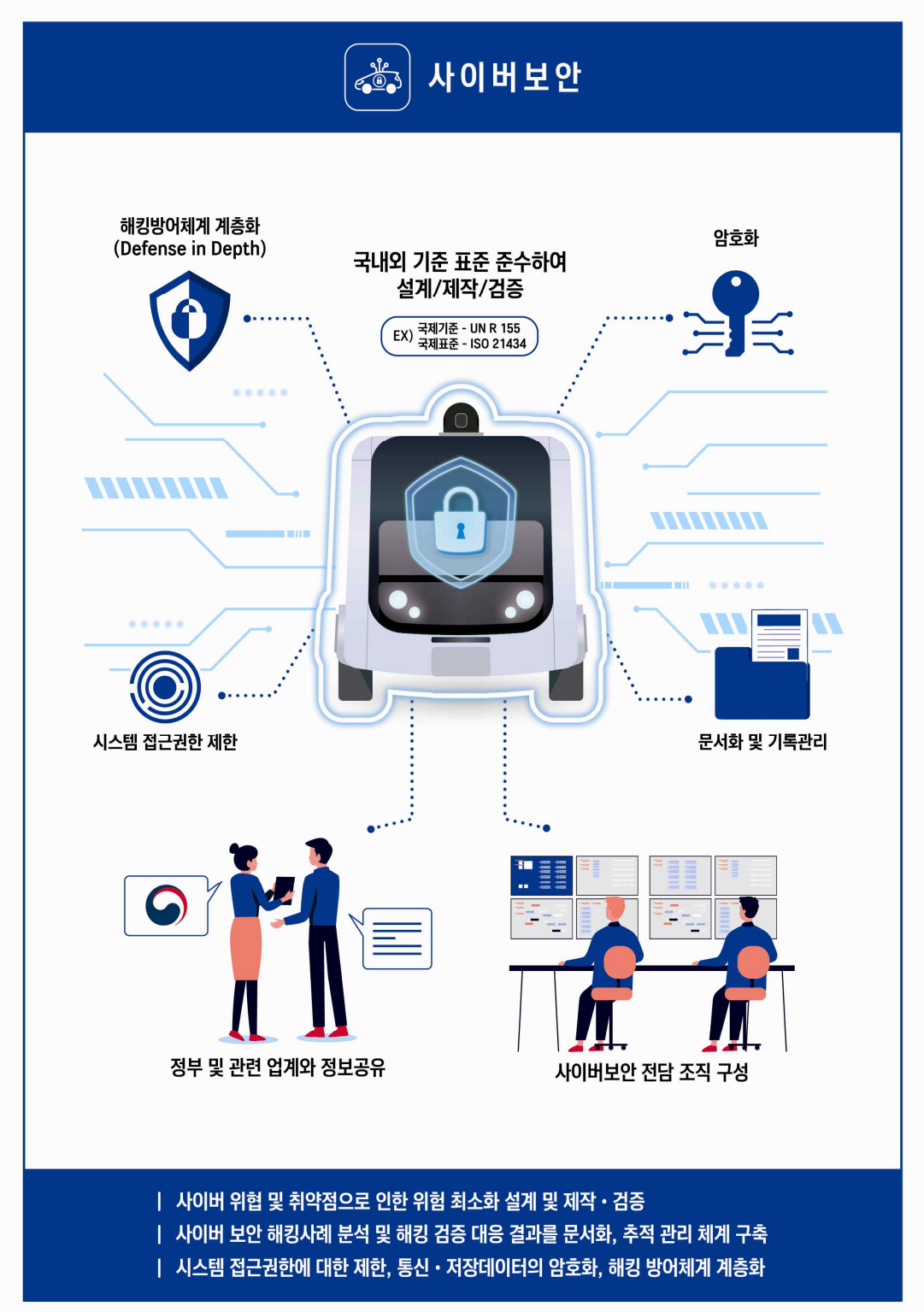
ㅇ 자율주행시스템은 주행 중 운행가능영역을 벗어나게 되는 경우 이를 인지할 수 있어야 하며, 필요한 경우 탑승객 등을 위한 알림과 함께 자발적인 안전조치(위험최소화운행 등)를 강구한다.

- 위험최소화운행 : 발생 가능한 사고에 의한 위험을 최소화하도록 주행차로 내에서 감속 및 정차하거나 갓길 등으로 이동하는 조치에 해당하며, 위험최소화운행을 하는 동안에는 알람 등에 의해 탑승객이라 주변 차량에 시스템의 거동상태에 대한 정보를 제공

ㅇ 운행가능영역이 변경되는 경우 변경된 운행가능영역에 대한 기능안전절차를 수행한다.

③ 사이버보안

사이버 위협 및 취약점으로 인한 위험을 최소화하도록 공인된 국내외의 기준·표준에서 정하는 체계적인 방식에 의해 자율주행시스템을 설계·제작하고 검증한다.



○ 사이버보안 관련 기준은 UN Regulation No.155(Cyber Security)과 국제 표준으로는 ISO/SAE 21434(Road vehicles – Cyber security engineering)가 참조 될 수 있다.

○ 사이버보안 위험 관리를 위해서는 시스템 접근권한에 대한 제한, 통신·저장 데이터의 암호화, 해킹 방어체계 계층화, 메시지에 대한 보안 인증 등을 적용한다.

- 시스템 데이터/코드를 보호하기 위한 접근 제어
- 내부자 공격 위험 최소화를 위한 보안 제어
- 무단 접근 방지 및 탐지 조치
- 수신하는 메시지의 신뢰성 및 무결성 검증
- 차량과 송수신하는 기밀 데이터 보호 조치
- 사이버 공격 탐지 및 복구 조치
- 내장된 바이러스/악성 코드로부터 시스템을 보호하기 위한 조치
- 악의적인 내부 메시지 탐지 조치
- 안전한 소프트웨어 업데이트 절차 사용
- 소프트웨어 보안 평가, 인증 및 무결성 보호 등

○ 사이버보안과 관련된 시스템의 설계, 업데이트, 해킹사례 분석 및 해킹 대응 검증 결과 등에 대해 문서화 하고, 변경 이력이 추적될 수 있도록 문서버전을 관리한다.

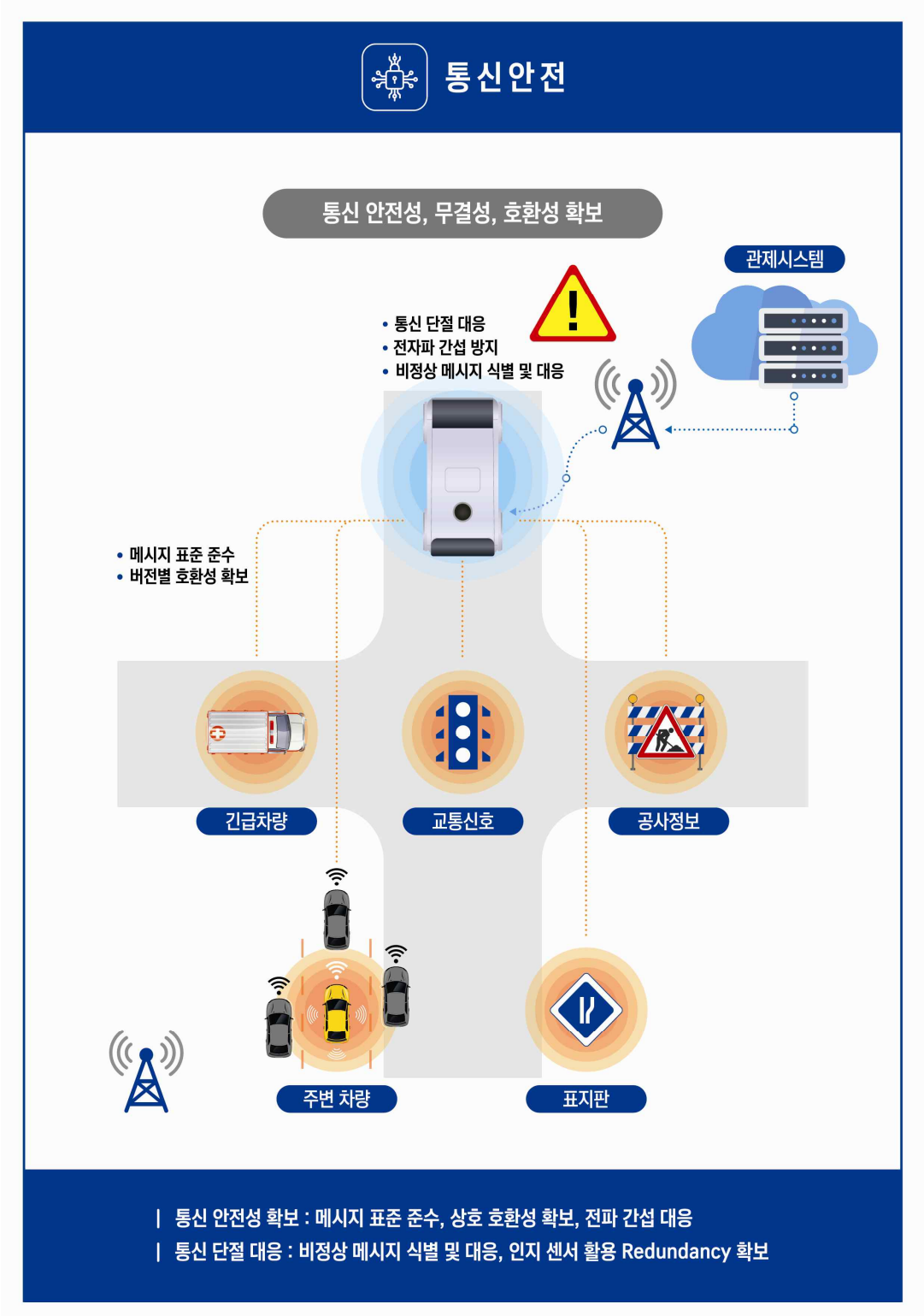
- 사고 대응 프로세스의 모든 과정을 문서화하고, 사고의 우선순위, 역할과 책임을 명확하게 명시함

○ 자율주행자동차 제작자는 사이버보안을 담당하는 상설부서를 상위부서로 구성 하여 조직적으로 사이버보안을 책임질 수 있도록 부서의 권한, 역할을 명시하며, 해킹 시도 및 사례 등에 대해서는 정부 및 관련 업계와 공유한다.

- 제작자는 보안 절차를 정의하고 준수되도록 보장하여야 함
- 부품업체 등의 공급업체와 서비스 제공업체 등을 포함한 모든 조직은 시스템의 보안을 강화하기 위해 협력해야 함

④ 통신안전

자율주행자동차에 설치하는 협력주행 통신장치와 송·수신 메시지는 공인된 국내·외 표준을 따르며, 통신 장애나 정보 오류 등에 의해 시스템의 안전성능에 영향을 받지 않도록 한다.



○ 협력주행 통신장치의 메시지 표준은 SAE 2735, SAE 2945, IEEE 802.11p, IEEE 1609 시리즈, 3GPP Release 14~16 등이 적용된다.

- 협력주행 통신장치는 V2X 메시지 표준 및 기술표준을 준수해야함
  - 메시지 표준 : SAE J2735
  - 통신 계층 별 표준 : IEEE 1609 시리즈
  - WAVE 관련 표준 : IEEE 802.11p, SAE J2945 시리즈
  - C-V2X 관련 표준 : 3GPP Release 14~16 (LTE 및 5G-V2X)

○ 협력주행 통신장치에 적용된 무선통신 기술은 이전 버전과의 호환성을 지원한다.

- 같은 종류의 무선통신 기술일 경우 신기술과 이전 기술은 상호 인지할 수 있어야 하며 동일한 우선순위로 무선채널 접속 기회를 가지고 서로 공존해야 함

○ 자율주행자동차 내·외부에서 사용하는 타 통신시스템 및 전장품과의 간섭으로 인해 협력주행 통신장치의 통신이 방해 받지 않도록 한다.

- 협력주행 통신장치는 차량에 장착된 전장품에 의해 발생되는 전자파 노이즈에 의해 장치 동작 및 통신 기능에 방해 받지 않아야함

○ 자율주행자동차는 협력주행 통신장치가 정상동작 하지 않는 경우를 포함하여 비정상적인 메시지에 대한 식별 및 대응방안을 수립한다. 이 경우, 통신 메시지의 신뢰성이 보장되지 않는다면 자율주행시스템의 주행환경 인지센서(카메라, 레이더, 라이다, 초음파 등)에 의해 주행상황을 자체적으로 인지·판단하여 주행하도록 할 수 있다.

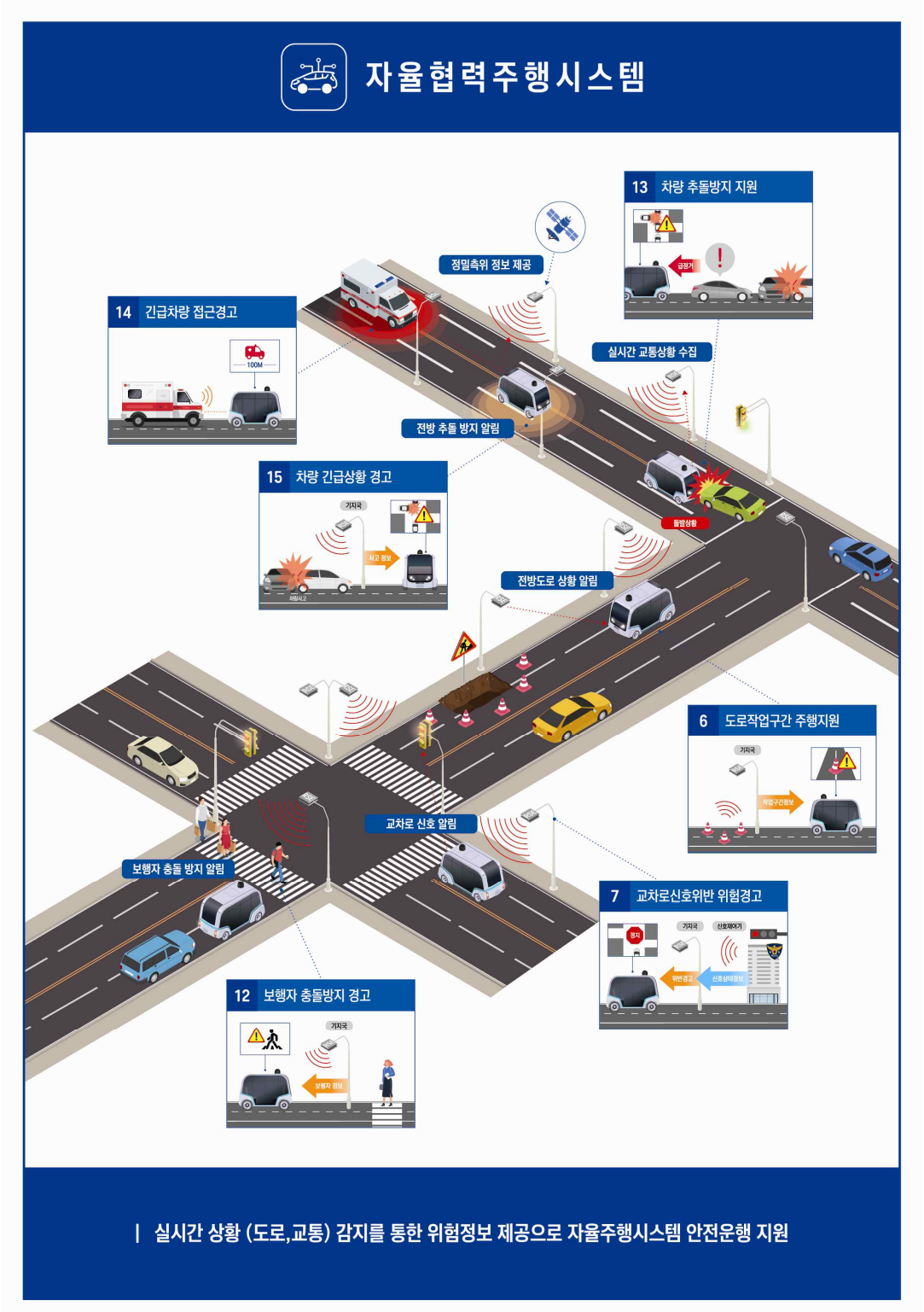
- 협력주행 통신장치에 의해 수신된 메시지를 자율주행시스템 제어에 활용할 경우 메시지 유효성에 대해 검사할 수 있어야 하며 수신된 메시지가 신뢰할 수 없고 자율주행시스템 안전에 위협이 된다고 판단되면 관련 메시지를 제어에 사용하지 않아야 함

○ 인포테인먼트(IVI, In-Vehicle Infotainment)를 목적으로 하는 정보 전달은 안전과 관련하여 시스템 및 탑승객의 판단에 영향을 미치지 않아야 한다.(사이버보안 및 HMI 등 연계)

- 탑승객 편의 정보(휴게소, 주유소, 쉼터 등) 및 다양한 엔터테인먼트 기기들과 연동되어 전달되는 정보의 오류(변경 사항 미갱신 등)에 의해 시스템 안전이 영향 받지 않아야 함

⑤ 자율협력주행시스템

자율협력주행시스템은 C-ITS(Cooperative-Intelligent Transport Systems)와 연계하여, 도로 및 교통상황을 모니터링하고 안전과 관련된 정보를 제공함으로써 자율주행시스템의 인지한계 등을 극복하는데 도움을 주기 위하여 사용된다.



○ 자율협력주행시스템은 자율주행자동차의 안전한 운행과 관련된 도로상황, 교통상황 및 기상상황 등을 검지하고, 주변의 도로를 통행하는 객체(자동차, 보행자 등)에 대한 정보를 수집한다.

- 도로상황 및 교통상황 수집 : 레이더센서, 추적카메라 등
- 도로기상정보 수집 : 강우계, 풍향풍속계, 적설계, 안개센서 등
- 보행자검지기 등을 활용하여 각종 정보를 실시간으로 수집

○ 자율협력주행시스템은 수집된 위험정보와 교통안전 관련 메시지를 노변 기지국의 통신영역 내에서 주변 자율주행자동차와 송·수신하여 제공한다.

- 일반도로, 터널, 도심구간 등 모든 도로상에서 안전정보를 원활히 주고받도록 지원

○ 자율협력주행시스템은 노변기지국의 통신영역 내에서 주변 자율주행자동차의 안전한 주행을 돕기 위해 측위 보정과 관련된 정보를 제공한다.

- 노변기지국은 자율협력주행시스템이 제공하는 GPS보정 정보를 주변 자율주행자동차에게 주기적으로 제공

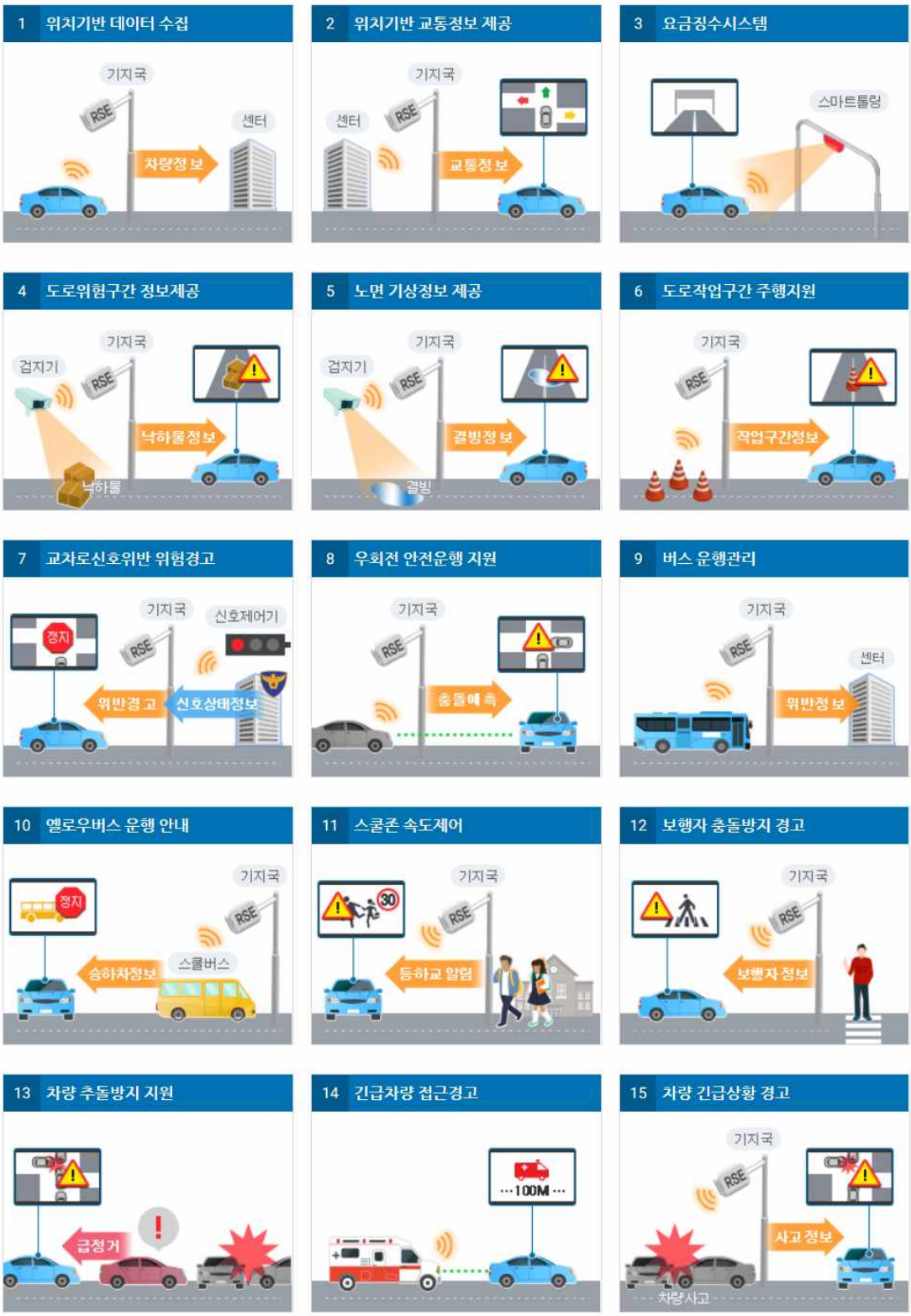
○ 자율협력주행시스템의 적절한 유지·관리 및 성능개선을 통하여 위험정보, 교통안전 관련 메시지 및 측위 정보 등이 신뢰도 있고 안정적으로 제공되도록 한다.

- 자율협력주행시스템이 제공하는 모든 정보는 높은 신뢰성과 안정성이 보장될 수 있도록 지속적인 성능개선 및 관리가 필요

○ 자율협력주행시스템은 안전서비스 항목(현재 15개)을 지속적으로 개발 및 표준화하여 자율주행시스템의 안전운행을 지원한다.

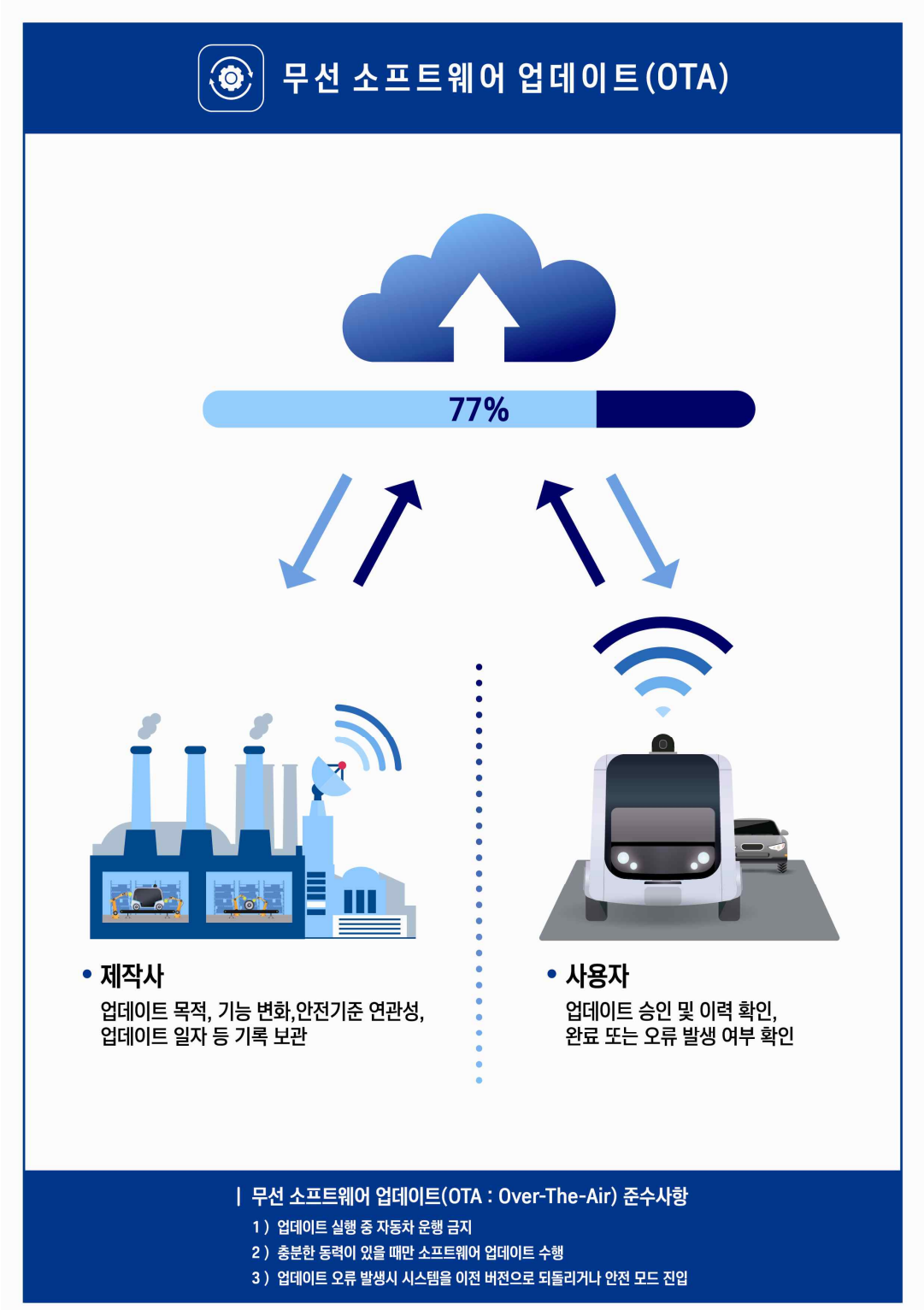
- 다양한 돌발상황 및 위험상황에서 자율주행자동차의 안전성을 높일 수 있는 안전서비스를 추가 개발하여 안전운행을 지원해야 함
  (예, 좌회전 지원 또는 비보호 좌회전 위험 경고 등)

• 안전서비스 15개 항목(C-ITS)



⑥ 무선 소프트웨어 업데이트

제작자는 무선 소프트웨어 업데이트 시 안전기준과 관련된 성능을 사전에 충분히 확인하고, 안전한 업데이트를 보장하기 위한 절차를 확보한다.



○ 제작사는 소프트웨어 업데이트의 목적, 기능상 변화, 안전기준 연관성, 업데이트 시행 방법 및 조건 등을 기록하여 보관한다.

- 소프트웨어 업데이트 안전 확보를 위한 버전관리 및 업데이트 내용 등을 문서화하여 문제 발생 시 추적을 통해 원인 분석 및 유사 문제 재발 방지
- 안전기준과 연관된 중요사항의 업데이트 시에는 업데이트 전후 과정과 성능상의 변화를 명확하게 기록

○ 소프트웨어 업데이트는 사이버보안 가이드라인에 따라 안전하게 실행되도록 한다.

○ 제작자는 소프트웨어 업데이트의 결과로 인한 기능상 변화가 자동차관리법 제29조에 따른 자동차안전기준과 연관성이 있는 경우, 자동차관리법 제30조에 규정된 성능시험대행자와 협의 후 진행되도록 절차를 갖춘다.

- 무분별한 소프트웨어 업데이트를 지양

○ 자동차의 안전에 영향을 줄 수 있는 소프트웨어 업데이트의 경우에는 정차 등 안전이 확보된 상황에서만 실행되도록 한다.

- 소프트웨어 업데이트 과정에서 오작동이나 시스템 셧다운 등에 의한 위험을 미연에 방지하도록 안전한 환경에서 업데이트를 시행하며, 운전자 동의 없이 주행 중 소프트웨어 업데이트가 실행되지 않도록 설계

○ 무선 소프트웨어 업데이트의 경우 실행 전 운영자나 사용자가 업데이트 정보(목적, 예상시간, 리콜여부, 중요도 등)를 사전에 인지할 수 있도록 하며, 완료 후 성공 여부에 대한 확인이 가능하도록 한다.

○ 무선 소프트웨어 업데이트는 자동차 내에 충분한 전력이 있을 때에만 실행하며, 업데이트 과정에서 오류가 발생한 경우에는 자동으로 이전 버전으로 돌아가거나 안전모드가 실행되어 운영자나 사용자가 인지할 수 있도록 한다.

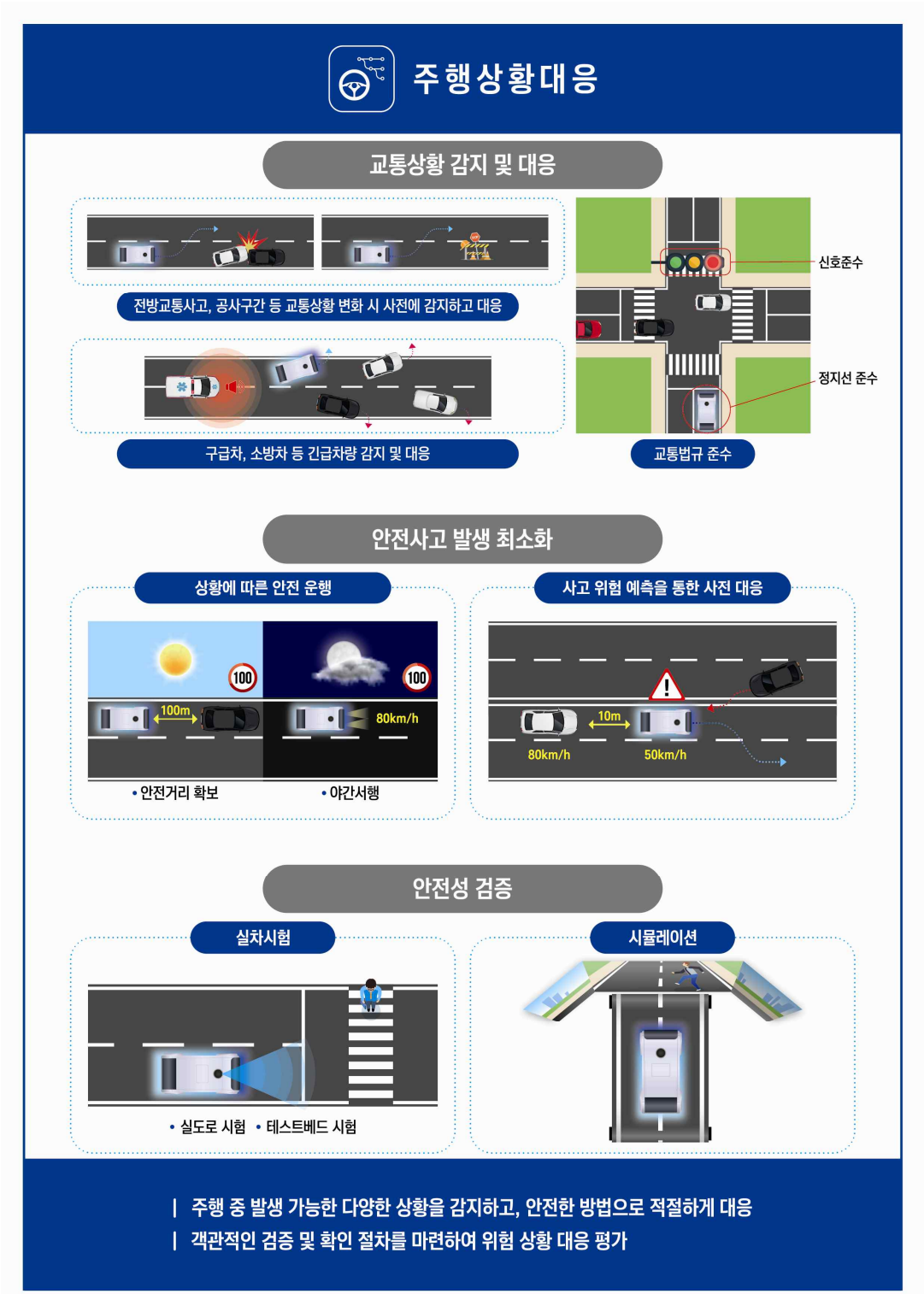
- 업데이트 중 전원이 꺼지면 위험할 수 있으며, 업데이트 오류 시 운전자의 조치가 불가능하므로 자동으로 이전 버전으로 돌아가거나 안전모드 실행 등을 수행하여 차량 운행이 가능하도록 해야 함

○ 자율주행자동차의 운영자나 사용자가 소프트웨어 버전을 알고자 할 때에는 용이하게 확인할 수 있도록 한다.

5 주행 안전

① 주행상황 대응

자율주행시스템은 운행가능영역 내 다양한 도로, 교통 및 환경 조건에서 주변의 통행 객체를 인지하여 제반 법규 위반이나 사고위험이 없도록 판단 및 제어를 수행하며, 이를 위해 객관적이고 충분한 확인 및 검증 절차를 수행하도록 한다.



○ 자율주행시스템에는 수동으로 작동(기능 'on') 및 해제(기능 'off')가 가능한 조작 장치를 갖춘 경우, 고장 등에 의해 시스템이 정상적인 성능을 발휘할 수 없거나 운행 가능영역 내에 있음을 명확하게 인지하지 못한 경우에는 작동이 제한되도록 한다.

○ 운행가능영역 내에서 주행 중 발생하는 다양한 상황(보행자, 자전거, 타차량 등 도로상 객체와 끼어들기, 합류·이탈, 차로변경상황, 좌·우회전 상황, 신호등, 도로표식 등)을 감지하고 안전한 방법으로 적절하게 대응한다.

○ 도로상의 안전 운행과 관련된 제반 법규(도로교통법 등)를 준수한다.

○ 주행 중 안전사고 가능성을 최소화하는 방향으로 운행되어야 하며, 예기치 못한 상황(사고 위험상황, 역주행, 후방 추돌 등)이 발생한 경우에도 사고에 의한 위험을 최소화하도록 대응한다.

- 정상적인 주행상태에서는 발생하기 어려운 상황이라 하더라도 사고사례가 있거나 교통환경에 따라 발생가능성이 있는 상황을 충분히 고려하여 주행안전성을 확보하고 사고 시 최소한의 대응이 가능하도록 설계

○ 주행 시 위험상황 대응과 관련된 객관적인 검증 및 확인 절차를 마련하여 자체적으로 또는 독립적인 제3자에 의해 시행한다. 이 경우 시뮬레이션, 테스트베드 환경 또는 유사 도로 환경 등을 대상으로 할 수 있다.

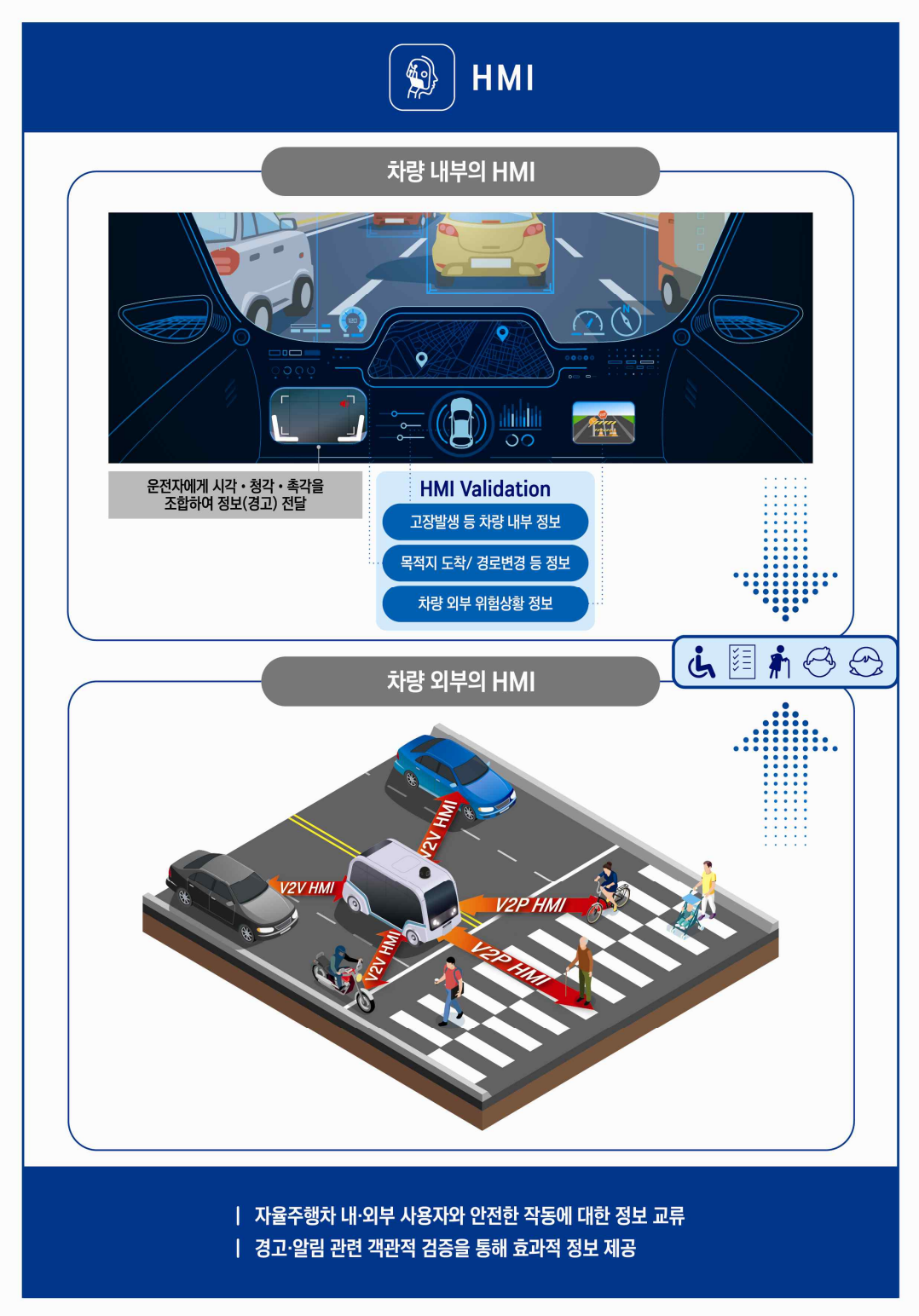
- 독립적인 제3자가 다양한 상황 시나리오에 대해 확인 및 검증함으로써 안전에 대한 주관적인 판단을 배제하도록 하며, 테스트베드 환경에서 안전성 검증이 불가능한 경우 시뮬레이션 등 다양한 방법 활용 가능
- 독립적인 제3자(자동차관리법 제30조에 규정된 성능시험대행자와 협의)는 제작자의 협력하여 객관적인 시각에서 안전성을 확인

○ 자율주행시스템은 자율협력주행시스템에 의해 위험정보와 교통안전 관련 메시지 등을 수신하는 경우 주행상황 대응을 위해 이를 선택적으로 활용할 수 있다.

- 자율협력주행시스템에 의해 제공되는 안전정보는 자율주행시스템이 환경인지센서(카메라, 라이다, 레이다, GPS 등)를 통해 직접 수집한 정보에 의한 안전상황 판단에 우선하지 않으며, 환경인지센서의 인지 범위를 넘어서는 안전정보인 경우 이를 선택적으로 시스템 제어에 반영

② HMI(휴먼-머신 인터페이스)

자율주행시스템은 운전자, 운영자(사용자), 탑승객 및 외부의 도로 이용자(다른 자동차, 보행자 등)에게 안전과 관련된 최소한의 정보를 적절한 수단에 의해 제공 한다.



○ 자율주행시스템은 운전자, 운영자(사용자), 탑승객 등에 기능의 작동·해제, 정상적인 작동 여부에 관한 정보, 안전(고장 포함)과 관련된 성능에 관한 정보와 함께 필요한 경우 적절한 수단에 의한 경고를 제공한다.

○ 안전 관련 정보나 경고의 경우 이와 무관한 다른 정보(인포테인먼트 등)에 우선하여 명확히 인지되도록 한다.

- 정보의 우선순위 : 정보전달(인포테인먼트 포함) 및 경고에 대한 모든 시각, 청각, 촉각 전달은 상황의 긴급성에 따라 우선순위를 분류하고, 즉각적 대응이 필요한 상황에서는 다른 자극과 구별되는 형태로 제시해야 함

○ 주행 중인 자율주행시스템은 경음기나 등화 등의 수단을 사용하여 일반 자동차의 운전자에 준하는 수준으로 다른 도로이용 객체(다른 자동차나 보행자, 자전거통행자 등)에게 안전과 관련된 정보나 경고를 제공한다.

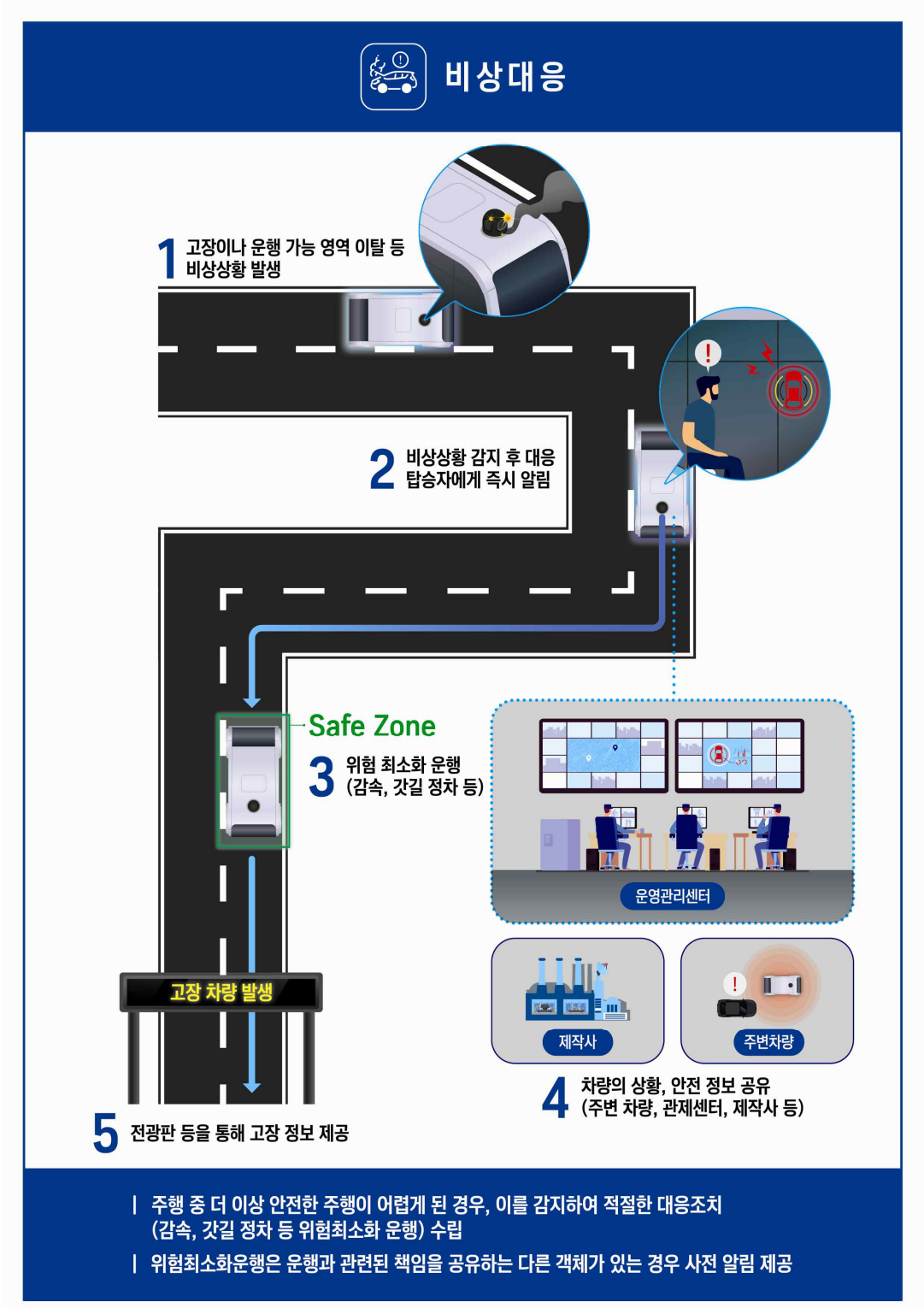
- eHMI(External Human Machine Interface) : 자율주행자동차 외부에 존재하는 도로를 공유하는 사용자(보행자, 자전거 탑승자, 다른 자동차 운전자 및 주변 자율주행자동차 등)와 시각, 청각 및 다양한 통신수단 등을 활용하여 정보를 주고받는 행위가 필요함

○ 자율주행시스템의 HMI 설계 안전성에 대해 객관적으로 검증 및 확인하는 절차를 마련한다.

- HMI 안전성 검증 : 인구통계학적 분포에 따른 다양한 성별 및 연령에 대한 다수의 반복 검증시험을 통해 인터랙션(Interaction) 방식에 문제가 없는지 검증

③ 비상 대응

자율주행시스템은 더 이상 안전한 주행을 담보할 수 없는 상황(고장이나 운행가능영역 이탈 등)이 발생하는 경우 이를 감지하고 적절한 대응조치(감속, 갓길 정차 등 위험최소화운행에 해당)를 취한다.



○ 자율주행시스템은 항상 주변 상황을 모니터링하며, 고장 및 비상상황이 발생하거나 발생할 가능성이 있는 경우 경고 및 비상대응(Fall-back)을 수행한다.

○ 고장 및 비상상황 대응이 개시되는 경우에는 내부 또는 외부 알림수단을 통해 상황판단 및 안전과 관련된 정보를 제공한다.

- 자율주행 시스템의 고장 발생 시 무선 통신 등의 방법을 통해 즉시 도로 관리자, 관제센터 등에 정보를 제공하여야함
- 후방 추돌 등 사고 예방을 위하여 주변 차량 및 관련자에게 무선 통신, 전광판 등을 활용하여 고장차량에 대한 정보를 공유 하여야 함

○ 비상대응을 위해 위험최소화운행이 수행되는 경우, 자율주행시스템 이외의 운행과 관련된 책임을 공유할 수 있는 다른 객체(운전자나 무인운전인 경우 운영관리센터)가 있는 경우 사전에 알림을 줄 수 있으며, 안전을 위한 목적상 필요한 경우 사전 알림 없이 자동으로 개시될 수 있다.

- 자율주행시스템이 스스로 비상대응(Fall-back)을 하도록 설계된 경우 또는 상황 발생 시에는 즉시 비상대응 수행
- 운전자가 있거나, 운영관리센터에서 비상대응을 할 수도 있고, 시간적 여유가 있는 경우에는 사전 경고를 통해 비상대응 요청
- 운전자나 운영관리센터에서 대응이 없는 경우는 즉시 비상대응 수행
- 고장 또는 운영가능영역 이탈로 자율주행 시스템에 의한 운전이 불가능할 경우 운전자에게 제어권 전환을 요청하거나 불가능 시 위험최소화운행으로 안전한 지역에 정지 하여야 함

○ 비상대응의 경우 대응 전·후 및 대응조치에 대한 데이터를 데이터기록장치에 기록한다.

○ 비상대응 상황이 종료된 경우에는, 운전자나 운영관리센터에 의해 시스템이 다시 작동될 수 있다.

④ 충돌안전 및 사고 후 시스템 거동

자율주행자동차는 다양한 좌석배치를 감안하여 사고충격을 최소화하도록 설계하며, 충돌사고 발생 시 안전한 사고처리 및 사후대응이 가능하도록 과정을 절차화 한다.

○ 자율주행자동차는 기존과 다른 좌석배치에 대비하여 충돌사고 발생 시 에너지를 효과적으로 흡수할 수 있는 구조로 한다.

○ 자율주행자동차의 좌석배치 상 특이점과 운행가능영역 내 다양한 충돌상황 시나리오를 감안하여 충돌 시 효과적으로 탑승객을 보호하기 위한 추가적인 방안을 고려한다.

- 자율주행자동차에 탑승하는 모든 연령과 다양한 위치의 좌석배치를 고려하여 탑승자를 보호할 수 있는 구조이여야 하며, 실차시험 및 해석 모델을 이용한 가상시험을 수행하여 안전성 확인

○ 주행 중 충돌사고 후 자율주행자동차를 안전한 상태로 유지하며 대응조치를 취할 수 있도록 하기 위한 방안을 마련한다. 이 경우, 사고 심각도에 따라 안전하게 동력이나 전력을 차단하고 주행차로 밖으로 이동할 수 있도록 하기 위한 조치를 포함한다.

- 사고 발생 시 사고 대응 절차에 따라 탑승자에게 즉시 알려야 하며, 운영관리센터, 119, 경찰 등에 신속히 사고정보를 제공하여 피해를 최소화 하여야 함

○ 자율주행시스템이 무선 통신에 의해 연결된 경우 운영관리센터 또는 응급센터 등에 사고발생 상황을 즉각 전달한다.

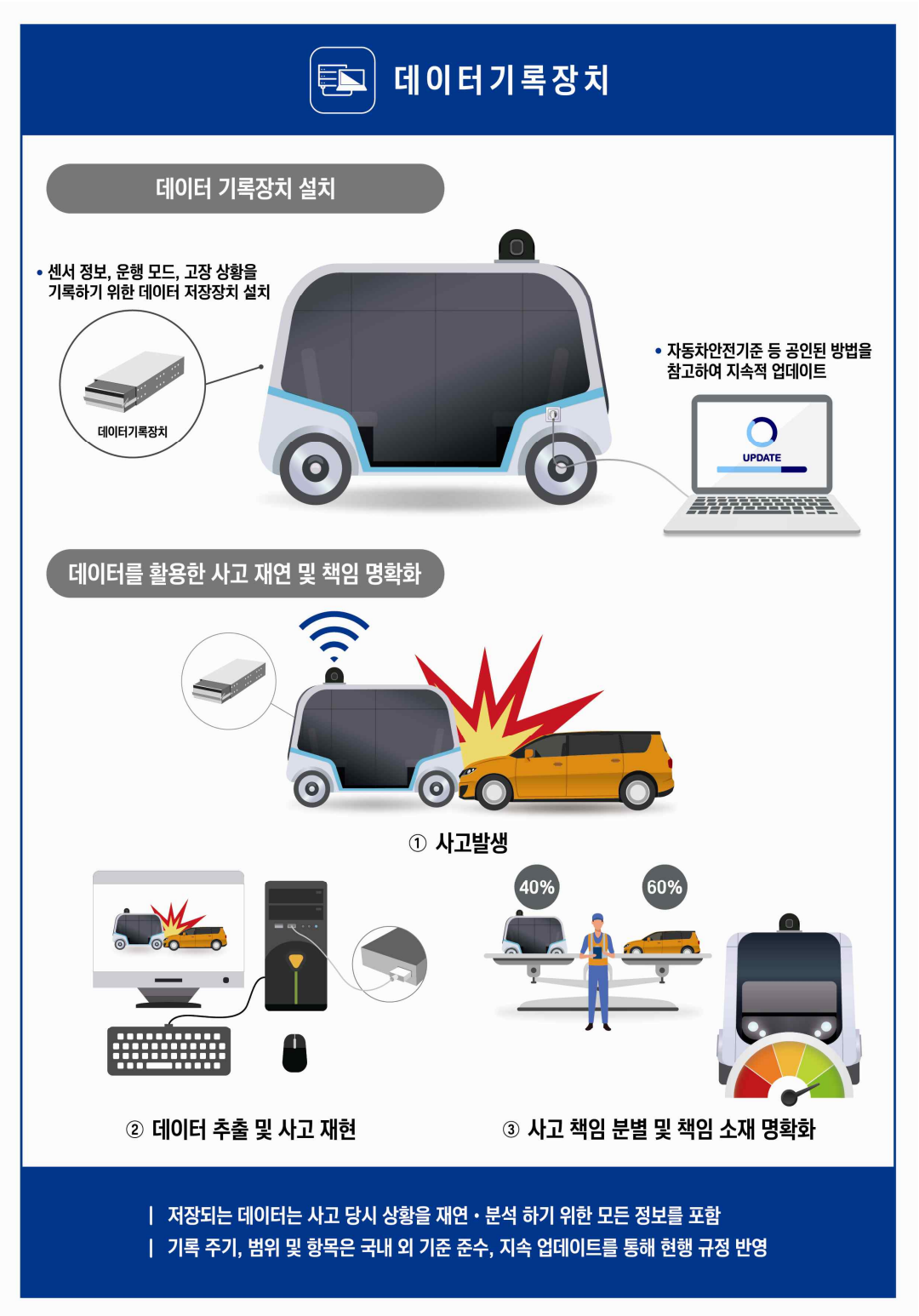
- 관제센터는 구급대원, 경찰, 견인차량 등에 자율주행자동차의 문 개폐방법, 좌석의 위치, 긴급 정지 방법 등 일반차량과 상이한 점을 즉시 알려 인명 구조에 차질이 없도록 하여야 함

○ 사고 후 자율주행시스템의 상태에 따라 자율주행기능을 재구동하거나 안전 조치를 취하기 위한 방법 및 수리 시 주의사항 등에 대한 내용을 문서화한 지침서(매뉴얼)를 마련한다.

- 제작사는 충돌 후 차량 수리, 정비 후 센서 위치 변경 등으로 인해 발생할 수 있는 시스템 오류를 방지하기 위하여 정비 매뉴얼, 센서 교정 절차 등 마련

⑤ 데이터기록장치

자율주행자동차에는 데이터기록장치 설치를 통해 안전한 운행과 관련된 정보를 기록하고, 사고 발생 시 사고원인을 파악할 수 있도록 한다.



○ 사고원인을 파악하고 책임소재를 명확히 하기 위해 시스템 제어정보와 사고 전후 상황을 기록하기 위한 데이터기록장치를 설치한다.

- 데이터기록장치는 자율주행시스템의 작동여부, 해제 원인, 제어권 전환요구, 비상운행의 시작과 종료, 위험최소화운행 시작, 고장상황 등을 기록
- 데이터기록장치는 각 상황별 발생 사유, 발생 날짜 및 시각을 초단위로 저장하고, 저장된 데이터는 최소 6개월 이상 또는 2,500건(자율주행 시작, 종료, 사용자 개입 및 주요 사건 이벤트 등의 저장 건수로 일 평균 12~15건씩 6개월 분량에 해당) 이상의 기록을 보존
- 저장된 데이터의 위변조 방지 대책을 마련

○ 기록되는 데이터의 종류 및 범위는 사고상황을 효과적으로 재현하고, 향후 사고상황을 통한 학습 및 성능개선에 활용될 수 있도록 설정한다.

- 자동차손해배상보장법 시행령에 따라 설립된 자율주행자동차 사고조사위원회를 통해 자율주행정보 기록을 수집 분석하고, 시스템간의 관련성을 파악하여 사고원인을 규명하며, 이해관계자와 사고 정보 공유

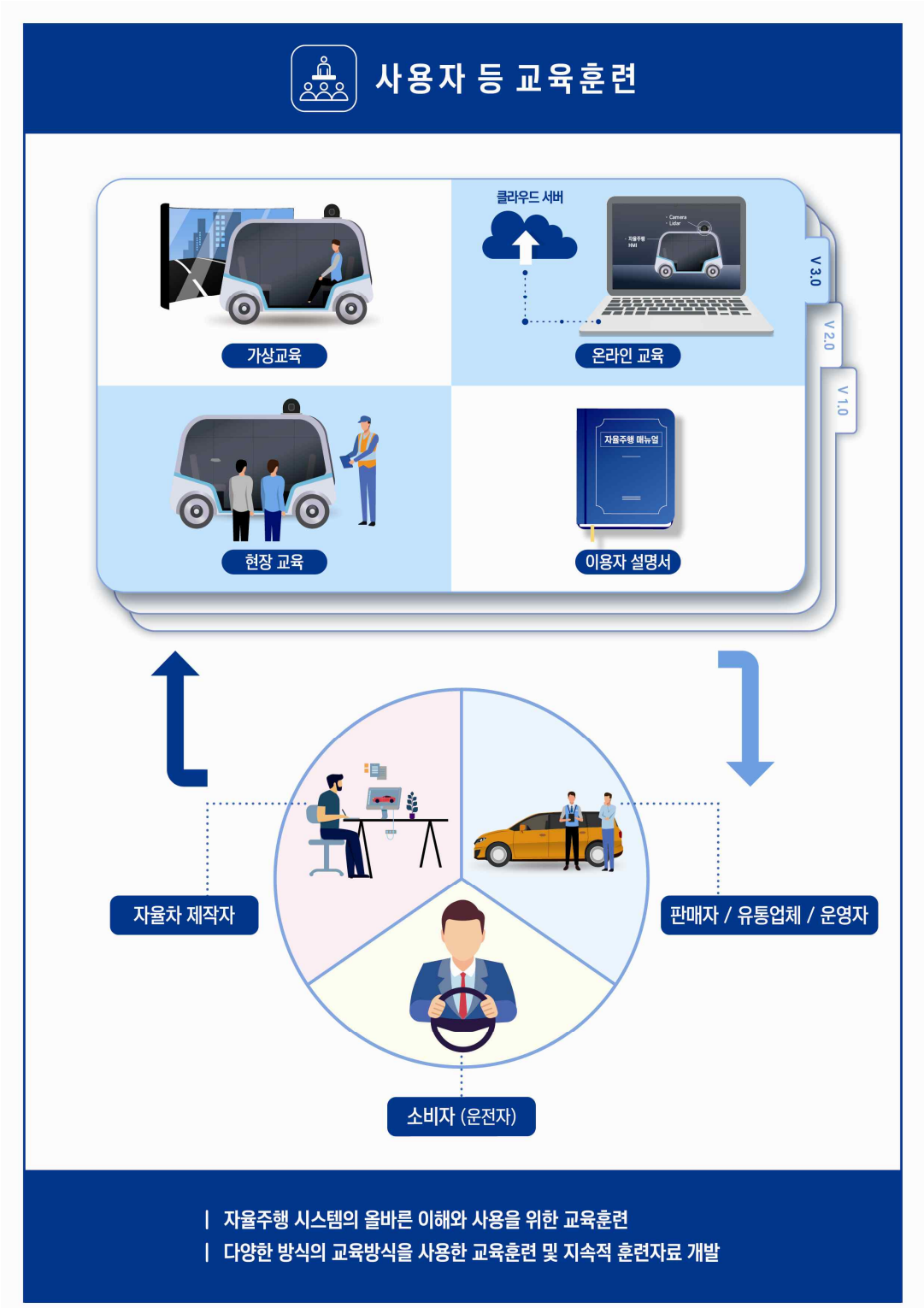
○ 데이터의 기록 주기, 범위 및 항목 등에 대한 기술적 사항은 공인된 국내·외의 기준·표준(자동차안전기준, UNECE/WP29 등)을 참조하여 정하고 지속적으로 업데이트한다.

- UNECE/WP29 관련 문서 : ECE/TRANS/WP.29/2020/81

⑥ 안전교육 및 윤리적 고려

① 사용자 등 교육훈련

제작자 또는 운영자는 자율주행자동차의 올바른 이해와 사용을 위한 교육 프로그램을 마련하여 운영한다.



○ 자율주행자동차의 제작자, 판매자, 유통업체, 운영자 또는 사용자(소비자) 등을 대상으로 자율주행시스템의 올바른 이해와 사용을 위한 교육훈련을 실시하며, 필요하다면 주기적인 교육훈련 프로그램을 개발한다.

- 자율주행자동차 관련자에 대해 자율주행시스템의 구성, 작동방법, 상황대처 요령 등에 대해 교육훈련 실시
- 교육 대상자는 지속적인 교육을 통해 정확한 작동 요령을 숙지

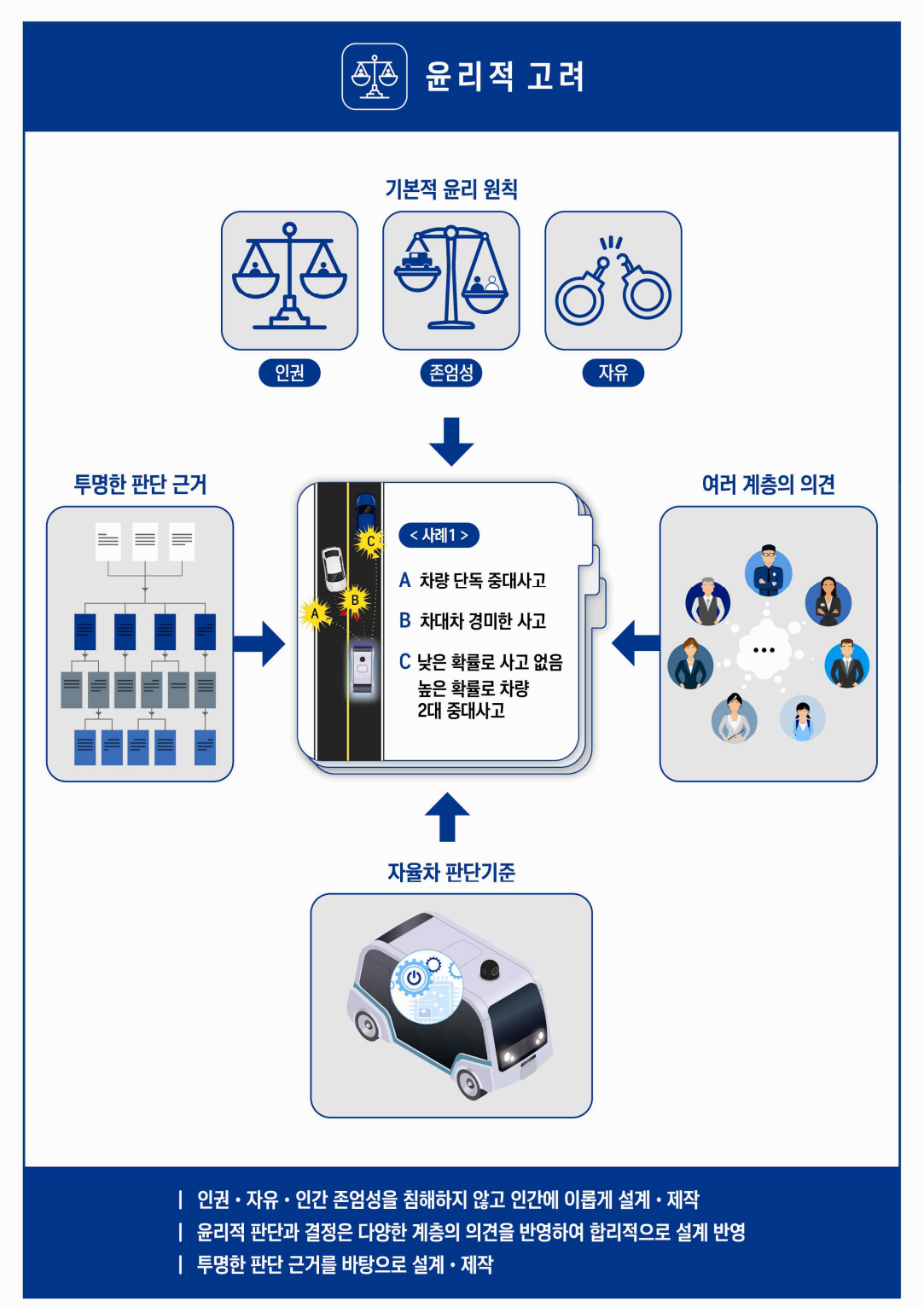
○ 교육자료에는 자율주행시스템의 목적, 기능, 운행조건, 운행가능영역, 작동 한계, 작동·해제 방법, 지시·표시기(알림 등)에 대한 설명, 고장·사고 대응절차, 위험최소화 운행, 잠재적 위험을 최소화하기 위한 정보 등을 포함한다. 또한, 교육과정은 실도로 주행, 가상현실 또는 시뮬레이터 환경 등을 활용하여 실제와 유사한 상황에서 충분히 이해될 수 있도록 한다.

- 가상시뮬레이터를 사용한 자율주행시스템 작동, 시스템 오류 시 대처 방법, 위험상황 시 요령 등에 대해 구체적이고 반복 체험할 수 있는 교육을 실시

○ 교육 프로그램은 참여자의 피드백 및 신기술 적용사항 등을 반영하여 주기적으로 효과를 확인하고 지속적으로 업데이트한다.

② 윤리적 고려

자율주행시스템은 항상 인간에 이롭게 작동하도록 제작하며, 윤리적 문제와 관련된 시스템의 판단이 필요한 경우 사전에 충분한 의견수렴 절차를 걸쳐 설계하며, 사후에 확인이 가능하도록 한다.



○ 자율주행시스템은 국제법적으로 인정된 인권·자유·인간존엄성 등을 침해하지 않고 인간에게 이롭도록 설계 및 제작한다.

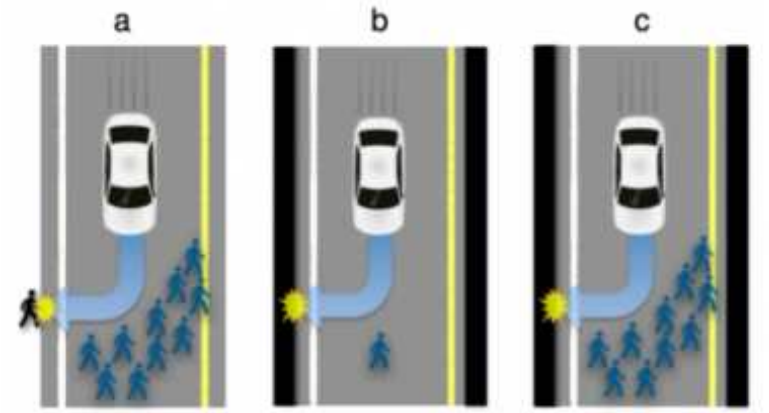
○ 자율주행시스템은 항상 인간의 판단과 통제에 따르도록 설계 및 제작한다.

- 자율주행시스템 운행 중 인간의 개입이 발생할 경우 즉시 이에 반응할 수 있도록 제작
- 자율주행 시스템의 해킹 및 조작으로 인해 범죄 및 테러에 활용되지 못하도록 예방수단을 마련

○ 정부, 이해관계자(운전자, 탑승객, 도로 이용자 등), 제작자 및 관련업체는 자율주행자동차의 윤리적 판단과 결정이 합리적이도록 환경 조성

○ 윤리적인 고려사항이 충돌하는 상황을 해결하기 위해 정부를 포함하여 다양한 도로운행자로부터 의견을 청취하여 설계에 반영한다.

- 트롤리 딜레마와 같은 윤리적 고려가 충돌되는 상황에 대해서는 관련 이해당사자의 의견을 수렴하여 반영



(MIT Technology Review : 'Why Self-Driving Cars Must be Programmed to Kill')

○ 자율주행시스템에 의해 특정 주행상황에 대한 판단이 내려진 경우 어떻게, 왜 판단이 내려졌는지를 추적하여 설명하고 해석할 수 있도록 투명한 방식으로 설계·제작한다.

- 자율주행자동차의 올바른 운행을 위해 정부 또는 법에 의해 위임받은 기관은 차량의 검사, 관리, 서비스제공, 이용 과정 등을 관리·감독할 수 있다.

7 결 론

○ 정부는 「미래차 산업발전전략」('19.10.15), 「미래차 확산 및 시장선점 전략」('20.10.30)에서 제시한 '27년 레벨4 자율차 세계최초 상용화라는 목표를 달성하기 위해 선제적으로 법·제도 정비, 인프라 구축, 서비스 활성화 등의 종합적인 정책을 추진 중에 있다.

○ 특히, 레벨4 자율차 출시에 필수적인 안전기준은 차량이 안전하게 출시되고 운행될 수 있도록 하는 제도적 기반으로 국토교통부는 레벨4 자율차 안전기준을 '24년까지 단계적으로 마련할 계획이다.

○ 국토교통부는 레벨4 자율차 안전기준을 본격적으로 마련하기 이전에, 제작자 등이 참고할 수 있도록 기본방향을 제시하여, 향후 기술개발 과정에서 제도적 불확실성에 의해 발생하는 애로사항을 최소화하고자 본 가이드라인을 마련하였다.

○ 본 가이드라인은 국내의 기술개발 환경을 감안하여 국제적 논의에 따른 안전 기준 및 안전성 평가·검증 방법이 마련되기 이전에 자율주행자동차가 확보하여야 할 3대 안전 원칙*에 따른 13개 항목을 제시하였으며, 제작자나 운영자 및 사용자 등이 스스로 검증 할 수 기반을 마련함으로써 안전한 자율주행 생태계 조성 및 상용화에 이바지 할 수 있을 것으로 기대한다.

* 운행가능영역 내에서 오류나 오작동 및 사이버위협을 최소화하기 위한 '시스템 안전', 다양한 통행 객체와 상호작용을 통해 사고 위험을 최소화하기 위한 '주행 안전', 올바르고 인간 우선적인 사용에 관한 '안전교육 및 윤리적 고려'

○ 본 가이드라인은 향후 자율주행 기술 발전, 상용화, 새로운 정책과 법 제·개정 등으로 인한 변동사항에 따라 업데이트 될 수 있으며, 자율주행자동차 제작자, 연구기관 및 사용자(소비자)와 긴밀한 소통을 통해 모든 이해당사자의 의견이 반영될 수 있도록 노력할 것이다.

부록 1 참고자료

· **자동차관리법** : 자동차의 등록, 안전기준, 자기인증, 제작결함 시정, 점검, 정비, 검사 및 자동차관리사업 등에 관한 사항을 정하여 자동차를 효율적으로 관리하고 자동차의 성능 및 안전을 확보함으로써 공공의 복리를 증진하기 위한 법령
(https://www.law.go.kr)

· **V2X(Vehicle-to-Everything)** : 차량이 유·무선 통신망을 이용하여 주변 차량 및 도로 인프라 등과 정보를 교환하거나 공유하는 기술을 의미하여 차량과 차량(V2V, Vehicle to Vehicle), 차량과 인프라(V2I, Vehicle to Infrastructure), 차량과 보행자(V2P, Vehicle to Pedestrian), 차량과 기기(V2N, Vehicle to Nomadic Device), 차량과 그리드(V2G, Vehicle to Grid) 등을 포함

· **WAVE(Wireless Access in Vehicular Environments)** : IEEE 802.11a 무선 랜 기술을 기반으로 차량 주행 환경에 적합하도록 물리 계층 및 매체접근제어(MAC, Medium Access Control) 계층을 개정한 무선 접속 표준(IEEE 802.11p)으로 V2X 시나리오에서 다양한 안전 메시지(충돌 경고, 도로 및 교통상황 정보, 신호 정보, 교차로 이동 보조 등)를 송수신하는데 주로 사용됨

· **C-V2X(Cellular V2X)** : 3GPP 무선 표준의 LTE와 5G 등의 셀룰러 기술에 기반을 둔 V2X 통신 기술로 통신 커버리지 확장을 위해 셀룰러 인프라 사용이 가능함
  - 3GPP Release 14(LTE-V2X) : LTE 기반의 안전 메시지 전달을 지원하는 기술 규격
  - 3GPP Release 15(LTE-eV2X) : 향상된 V2X 서비스 지원을 목적으로 한 LTE-V2X의 진화된 기술 규격
  - 3GPP Release 16(5G-V2X) : 5G 무선 기술을 기반으로 안전 서비스 및 다양한 엔터테인먼트 서비스 등을 지원하기 위한 기술 규격

· **IEEE 1609** : V2X 통신을 위해 매체접근제어(MAC) 계층 및 그 이상의 상위 계층에 대해 정의하고 있는 기술 표준
  - 1609.1 Resource Manager : WAVE 구조에서 제공되는 데이터 및 관리 서비스, 명령어 메시지 및 응답 메시지의 포맷 등 WAVE의 자원 관리 어플리케이션의 서비스 및 인터페이스에 대한 기술 규격
  - 1609.2 Security Services for Applications and Management Messages : 보안 통신을 위한 규격과 처리 절차에 대한 기술 규격
  - 1609.3 Networking Services : WAVE 데이터 교환을 위한 네트워크 및 전송 계층에 대한 기술 규격

- 1609.4 Multi-Channel Operation : 제어 및 서비스 채널로 구성되는 다중 채널 할당 및 전환을 지원하기 위한 기술 규격

· SAE J2735 Dedicated Short Range Communications(DSRC) Message Set Dictionary : 차량 환경 V2X 통신 애플리케이션에서 사용하기 위한 메시지 세트, 데이터 프레임 및 데이터 요소 등 메시지 구조에 대해 정의한 표준

· SAE J2945/1 On-Board System Requirements for V2V Safety Communications : 기본안전메시지를 기반으로 한 차량과 차량간(V2V) 안전 통신을 위한 온보드 시스템의 기능 및 성능 요구사항을 정의한 표준

· **C-ITS 홍보관** : https://www.c-its.kr/introduction/introduction.do

· **C-ITS 15개 안전 서비스** : https://www.c-its.kr/introduction/service.do

· ISO 26262 Road Vehicles - Functional Safety : 자동차에 탑재되는 E/E Electrical and/or Electronic) 시스템의 오류로 인한 사고방지를 위해 ISO에서 제정한 자동차 기능 안전 국제 표준

· ISO PAS 21448:2019 Road Vehicles - Safety Of The Intended Functionality : ISO 26262 표준에서 의도하는 대로 설계 및 제작이 되더라도, 기능상 한계나 사용자 오용 또는 운행 환경 등에 따라 비합리적인 위험이 발생하지 않도록 하기 위해 ISO에서 제정한 국제 표준

· ISO/SAE DIS 21434 Road vehicles - Cyber security engineering : 자동차 전 생애주기(Life-cycle)에 걸쳐 자동차 사이버보안을 관리하기 위하여 ISO와 SAE에서 제정한 국제 표준

· UN Regulation No.155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system : UN에서 제정한 사이버보안 및 사이버보안 관리시스템 관련 자동차 승인에 관하여 통일 규정 (http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf)

· Cybersecurity Best Practices for Modern Vehicles : 미국 NHTSA에서 발행한 첨단 자동차를 위한 사이버보안 모범 사례 (https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf)

· **무선 소프트웨어 업데이트(OTA : Over The Air)**는 WiFi 등을 사용하여 무선으로 소프트웨어를 업데이트 하는 기술로, 서비스센터에 직접 방문하지 않고도 차량의 소프트웨어를 최상의 상태로 유지 가능

· **데이터기록장치 관련 국내기준**(자동차 및 자동차부품의 성능과 기준에 관한 규칙) : https://www.law.go.kr

· **데이터기록장치 관련 국제기준** : https://undocs.org/ECE/TRANS/WP.29/2020/81

· **트롤리 딜레마** : 윤리학의 사고실험으로, 두개 혹은 그 이상의 상황이 서로 양립할 수 없는 경우에 선택을 요구하는 것을 의미한다. 다른 방법을 쓸 여유는 없고, 법적 책임은 지지 않는 것으로 설정된다. 오직 도덕적인 견해만을 문제로 하고 있으며, 응답자는 질문에 대해 (도덕적 관점에서) "허용된다"와 "허용되지 않는다"로 응답하게 되어 있다. (Philippa Foot, The Problem of Abortion and the Doctrine of the Double Effect in Virtues and Vices, Oxford: Basil Blackwell, 1978)

· **트롤리 딜레마 MIT Technology Review 이미지** : https://www.technologyreview.com/2015/10/22/165469/why-self-driving-cars-must-be- programmed-to-kill/

부록 2 집필진 및 기관 소개

· 국토교통부 첨단자동차과 : 조태영, 이정규, 최철민, 이은정, 이창기

국토교통부 첨단자동차과는 우리나라 자율주행자동차 관련 국내 정책, 법제도 및 인프라 구축을 책임지고 있으며, 안전하고 편리한 자율주행 시대를 앞당기고 미래자동차를 선도하기 위해 자율주행자동차 상용화 사업 및 관련 국가 R&D 사업을 총괄하고 있음

· 자율주행차 융복합 미래포럼(제도분과) : 윤영한(한국기술교육대학교), 권영실(법무법인 혜율), 류동근(우버코리아), 이항구(한국산업연구원), 윤석현(현대자동차), 윤용철(LG전자), 용기중(경일대학교), 이경수(서울대학교), 강경표(한국교통연구원)

자율주행차 융복합 미래포럼은 자율주행자동차 산업 육성 및 교통물류 혁신을 위해 사회 각 분야의 전문가 의견을 수렴하여 효과적인 정책수립 및 개선안 제시를 위해 2016년 6월 발족되었으며, 7개 정부부처 및 자동차, 인프라, 산업 및 사회 분야 産·學·硏 60여개 기관에서 약100명의 전문가가 참여하고 있음

· 한국교통안전공단 자동차안전연구원 : 조성우, 조광상, 최인성, 권석태, 김영선, 김종화, 문병준, 이은영, 조병찬

자동차안전연구원은 한국교통안전공단의 부설 연구기관 1987년 설립되었으며, '안전하며 편리하고 쾌적한 교통환경을 조성하여 모든 국민이 행복한 세상을 만든다'는 공단 미션 아래 제작결함조사, 자동차안전기준국제조화, 자동차안전도 평가, 미래자동차연구 등 우리나라 자동차 안전을 책임지고 있으며, 자율주행 자동차 상용화 위한 정부의 정책 및 법제도를 지원하고 있음

레벨4 자율주행자동차
제작 · 안전 가이드라인

국토교통부
TS 한국교통안전공단 자동차안전연구원