ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 21-03-24
154
j.inst.Korean.electr.electron.eng.Vol.25,No.3,565~570,September 2021
https://doi.org/10.7471/ikeee.2021.25.3.565

자율주행자동차를 위한 안전성 평가 표준: UL 4600

Evaluation Standard for Safety of Autonomous Cars: UL 4600

이 성 수*, 임 상 혁*★

Seongsoo Lee* and Sahng-Hyeog Ihm*★

Abstract

This paper describes UL 4600, a new international safety standard to ensure safety of autonomous cars. Conventional vehicular safety standards such as ISO 26262 and ISO/PAS 21448 suffer from large limitations to be applied to autonomous cars, but UL 4600 exploits new approaches to be applied to autonomous cars. Conventional standards define various technological aspects to ensure safety and require manufacturers to certify these aspects. On the contrary, UL 4600 requires manufacturer to explain and prove why autonomous cars are safe. In UL 4600, (1) under specific environments where the system is designed to operate with, (2) claims should be defined to guarantee given safety, and (3) arguments should be suggested to satisfy given goals, and (3) evidences should be presented to prove given arguments. UL 4600 is technology-neutral since it does not require specific designs nor technologies. So UL 4600 only requires manufacturers to prove given safety goals regardless of methods and technologies. Also UL 4600 admits various cases of autonomous car field operations into the standard via feedback loop. So UL 4600 effectively maneuvers various dangers unknown at the time of standard establishment.

요 약

본 논문에서는 자율주행자동차의 안전성을 보장하기 위해 새로 개발된 국제 표준인 UL 4600에 대해 다룬다. 자동차 안전성 분야의 기존 표준인 ISO 26262와 ISO/PAS 21448 등은 자율주행자동차에 적용되기에 상당한 제한이 있는데 UL 4600은 새로운 접근 방식을 통해 자율주행자동차에 적용이 가능하다. 기존 표준은 안전을 보장하기 위한 다양한 기술적 확인 조건을 구체적으로 표준에 적시하고 제조사가 이를 지켰는지를 인증하도록 하는데 비해 UL 4600은 자율주행자동차가 왜 안전한지를 제조사가 설명하고 증명하도록 한다. 즉, UL 4600은 (1) 시스템이 설계될 때 가정된 특정 운행 환경에서 (2) 안전성을 보장하기 위한 주장을 설정하고 (3) 이 주장을 만족하는데 필요한 논증을 제시하며 (4) 이 논증을 실제적으로 증명할 수 있는 증거를 제시하도록 한다. UL 4600은 특정 설계나 특정 기술을 요구하지 않으므로 기술 중립적이며 제조사에게 수단 방법과 관계 없이 안전 목표를 증명할 것만 요구한다. 또한 UL 4600은 자율주행자동차를 운용하면서 발생한 다양한 사례를 피드백 루프를 통해 표준 내에 수용하며, 이를 통해서 표준 제정 단계에서는 알 수 없는 다양한 위험에 효과적으로 대응할 수 있다.

Key words : UL 4600, ISO 26262, ISO/PAS 21448, Autonomous Driving, Safety Standard

* Soongsil University (Professor, Professor)
★ Corresponding author
E-mail : truthfinder@ssu.ac.kr, Tel : +82-2-820-0483

※ Acknowledgment
This work was supported by the Soongsil University Research Fund of 2018. This work was also supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE). (P0017011, HRD Program for Industrial Innovation)
Manuscript received Sep. 18, 2021; revised Sep. 24, 2021; accepted Sep. 27, 2021.

I. 서론

자동차가 설계된 대로 동작하고 어떤 부분에 고장이 발생하더라도 다양한 예비책을 통해 안전성을 보증하는 것은 자동차 회사에서 매우 중요한 의무의 하나이다. 자동차의 안전성은 단순히 소비자가 안심할 수 있다는 점을 떠나 다양한 법적 배상 책임과 연관되어 있으며 이를 충족시키지 못할 경우에는 자동차를 판매할 수 없게 될 수도 있기 때문이다[1][2].

UL(Underwriters Laboratories)은 1903년에 설립된 미국의 표준 제정 기관으로 1,700개 이상의 표준을 제정하여 세계 제조 산업에 막대한 영향력을 행사하고 있다. UL에서는 2020년에 자율주행자동차를 위한 UL 4600[3]을 제정하였는데, 이 표준에서는 지금까지 제정된 자동차 안전성 분야의 국제 표준을 자율주행자동차에 적용하기 위해 새로운 접근 방식을 채택하였다. 본 논문에서는 UL 4600에 대해 자동차 안전성 분야의 기존 표준과 어떻게 다르고 안전성을 증명하기 위해 어떤 방식으로 접근하는지를 자세히 살펴본다.

II. UL 4600의 필요성

대부분의 나라에서는 제조물 책임법을 통해 제조물의 결함으로 생긴 손해를 제조사에게 엄격하게 묻고 있으며 제조물에 결함이 없음을 입증하는 책임도 기본적으로 제조사가 져야 한다. 그러나 결함의 상당 부분은 철저한 분석을 통해서도 예측하거나 발견할 수 없기 때문에 제조사가 제조물에 결함이 없음을 입증하기는 쉽지 않다. 따라서 제조사가 과실이 없음에도 책임을 지는 무과실 책임이 발생할 수도 있다. 이렇게 되면 제조사가 실질적으로 제조물에 대한 무한 책임을 지게 될 수 있어서 개발 활동이 크게 위축될 수 있으므로 대부분의 나라에서는 '개발위험의 항변'을 인정하고 있다. 이는 '제조사가 해당 제조물을 개발할 당시의 과학·기술 수준으로는 결함의 존재를 발견할 수 없었다'는 점을 증명하면 결함이 없다고 간주한다는 의미이며 한국에서도 제조물 책임법 제4조 1항 2호에서 이를 인정하고 있다.

그러나 '개발위험의 항변'을 증명하기는 여전히 쉽지 않기 때문에 안전성에 관한 다양한 표준을 엄격히 지키면 증명했다고 보는 견해가 다수이며 우리나라에서도 유력하다[1]. 자동차의 경우 안전성 분야의 대표적인 표준으로 ISO 26262[4], ISO/PAS 21448[5] 등이 제정되어 있는데 문제는 이들 국제 표준이 자율주행에 적용하기가 쉽지 않다는 점이다. 자율주행자동차의 운행은 일반적으로 센싱, 판단, 동작의 3단계를 거치는데 ISO 26262, ISO/PAS 21448은 센싱 단계와 동작 단계에는 적용되지만 판단 단계에는 적용이 어렵기 때문이다[1][2].

이외에도 자율주행자동차에서 안전성 분야의 표준을 개발하는 경우에는 다양한 문제점이 존재한다. 기존 자동차는 대부분 원리나 기술적인 면에서 어느 정도 정형화되어 있어서 여기에서 발생하는 위험성에 대해 기술적으로 증명하면 되지만 인공지능에 기반한 자율주행자동차에는 매우 다양한 기술이 여러 가지 방법으로 결합되어 사용되기 때문에 차종마다 고유한 기술적 특성을 가진다고 볼 수 있다. 따라서 기존 안전성 표준이 자율주행자동차에 적용되기 위해서는 매우 많은 종류의 기술적 증명을 표준 내부에 규정해야 하는데 이는 표준으로서는 비현실적에 가깝다.

또한 기존 자동차와 달리 자율주행자동차는 매우 빠른 속도로 기술 개발이 이루어지고 있으며 이에 따라 표준 제정 당시에는 예측할 수 없었던 중대한 위험이 나중에 드러나는 경우도 많다. 이렇게 되면 기존 안전성 표준은 새로이 드러난 위험에 대응하기 위한 기술적 증명을 일일이 개정 수록해야 하는데 이 또한 비현실적에 가깝다.

이에 따라 자율주행자동차의 판단 단계에도 적용이 가능하며, 안전성을 보장하기 위한 수많은 기술적 증명을 표준 내부에 수록할 필요가 없고, 제정 당시 알려지지 않았지만 나중에 드러난 중대한 위험을 피드백 형식으로 대응할 수 있는 새로운 표준이 필요하게 되었는데 여기에 부합하도록 새롭게 제정된 안전성 표준이 UL 4600이다.

III. UL 4600의 특징

ISO 26262, ISO/PAS 21448과 같은 기존 안전 표준은 주로 SAE J3016[6]에서 정의한 자율주행의 3단계 이하에 적용되어 운전자가 있다는 전제 하에 개발된 데 반하여 UL 4600은 SAE J3016의 4단계 이상, 즉 운전자가 필요 없는 완전 자율주행 (fully

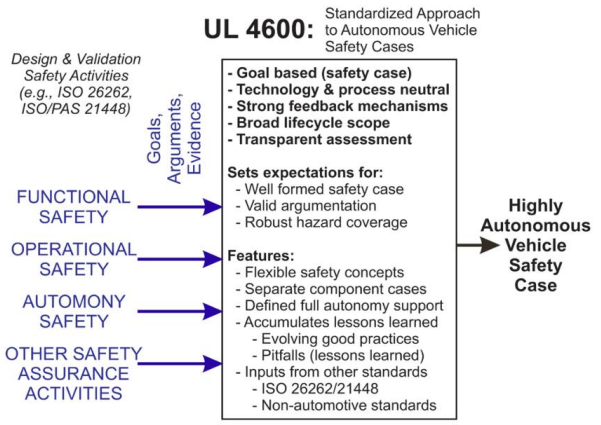

Fig. 1. Overview of UL 4600 [7].
그림 1. UL 4600의 개요 [7]

autonomous driving)에 적용된다. 이 단계의 자율주행은 복잡하고 비결정적이며 예측하기 어려운 특성을 가지며 신기술이 빠르게 업데이트되기 때문에 UL 4600에서는 자율주행자동차의 안전성을 증명하기 위해서 그림 1과 같이 기존 안전 표준과는 다른 방법을 적용한다[7]-[10].

UL 4600은 특정 설계, 특정 방법, 특정 기술을 요구하지 않으므로 기술 중립적이고 개발 프로세스와 무관하며, 제조사에게 수단 방법과 관계없이 제시된 안전 목표를 엄밀하게 증명할 것만 요구한다. UL 4600에서는 기술적 사항을 규정하는 것이 아니라 안전 목표를 증명하기 위해 필요한 방법과 절차를 규정할 뿐이다. 이 방법과 절차 중에서 상당수는 UL 4600에 규정되어 있으며 이외에도 제조사가 다양한 방법과 절차를 스스로 선택하고 입증하도록 하고 있다.

UL 4600은 자율주행자동차의 안전성을 보장하기 위해 기술적 증명이 아닌 논리적 증명을 채택한다. 기존 표준은 안전을 보장하기 위한 다양한 설계 방법, 기술 조건, 검증 방법, 목표 수치 등을 표준에 수록하고 자동차의 설계, 제조 과정에서 이를 지켰는지를 인증하도록 하지만 UL 4600은 자율주행자동차가 왜 안전한지를 제조사가 논리적으로 설명하고 이를 증명하도록 한다. UL 4600의 안전 증명 과정은 IV장에서 설명한다.

UL 4600에서 안전 증명의 목표와 과정을 제조사에게 제시하고 설명하도록 한다고 해서 기존 안전 표준보다 결코 느슨하다고는 할 수 없다. UL 4600은 제조사가 안전성을 증명하기 위해 설명하는 과정에서 놓칠 수 있지만 실제로 빠뜨리면 안 되는 수많은 방법과 절차를 다양하게 규정하고 있으며 기본적으로 제조사가 현재 사용할 수 있는 가장 강력한 방법과 절차를 최대한 많이 결합하고 사용하여 안전성을 증명할 것을 요구하고 있다. 또한 제조사의 설명대로 안전성이 증명되었는지는 독립적인 심사자가 UL 4600을 체크리스트로 사용해서 관련된 보고서를 검토하여 설명 및 증명 과정에서 빠진 것이 없는지를 샅샅이 찾아내도록 한다.

UL 4600은 안전 목표가 증명되어도 자율주행자동차가 운행하는 사용 전 주기(life cycle) 동안 계속 현장에서의 피드백을 통해 예상하지 못한 위험요인이 나타났을 때 이를 즉각 해결하고 이를 반영할 것을 요구한다. 나아가서 UL 4600은 이렇게 나중에야 드러나는 수많은 문제들을 표준 자체에 주기적으로 업데이트하도록 관리되고 있어 시간이 지날수록 더욱 안전성을 높일 수 있다.

UL 4600의 업데이트 과정은 몇 가지 큰 의미를 가진다. 먼저, 복잡하고 비결정적이며 예측하기 어려운 인공지능에 기반한 자율주행자동차가 필연적으로 내포하는 '예측하지 못한 위험'을 최대한 빠르게 해결함으로써 자율주행자동차의 빠른 상용 보급과 최대한의 안전성 보장을 함께 추구할 수 있다. 또한 지속적인 업데이트를 통해 안전성과 관련하여 다양한 제조사가 보고하는 여러 가지 이슈와 정보를 집대성하고 산업계 전반에 걸쳐 이를 공유하는 허브 역할을 수행할 수 있다.

UL 4600은 ISO 26262, ISO 21448과 같은 기존 안전 표준과 상충되지 않도록 세심하게 고려하여 개발되었다. 또한 기존 안전 표준을 UL 4600의 일부 요소로 사용하여 안전성을 증명할 수 있다.

UL 4600은 지속적으로 업데이트되지만 그 초기 버전에서부터 실제 자율주행자동차에 적용할 수 있도록 다양한 요소를 다음의 예와 같이 구체적으로 규정하고 있다[7].

- 실세계에서 일어나는 주요 안전 이슈에 대한 설명(예: 시각 장애인, 관리 해태, 컴포넌트 고장 등)
- 안전 논증의 내부 일관성 보장(예: 논증을 통해 모든 위험을 대상으로 그 위험이 적절히 완화됐다는 충분한 증거를 확인)
- 예측하기 힘들어 간과하기 쉬운 비정상적인 조건에 안전하게 대응(예: 터널 화재, 사막의 비 등)

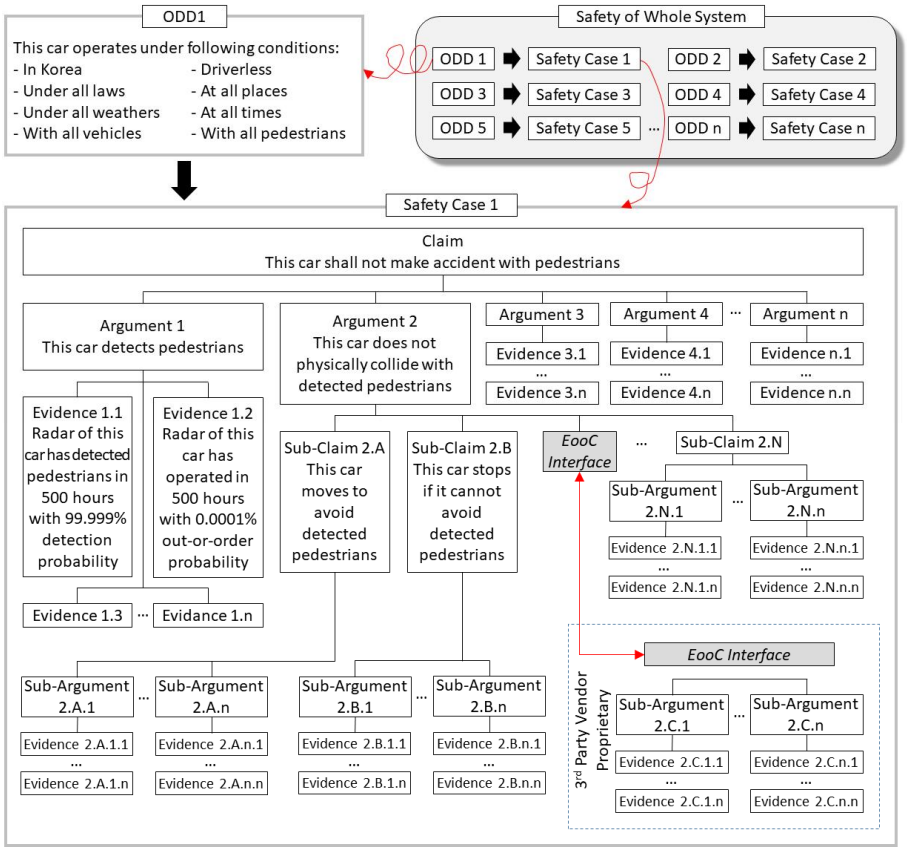

Fig. 2. Examples of ODD, safety case, claim, argument, and evidence in UL 4600.
그림 2. UL 4600에서 운행 설계 범위, 안전 사례, 주장, 논증, 증거의 예

- 전체 차량 수명주기 및 공급 체인을 고려(예: 세차를 통해 카메라가 깨끗해질 것이라고 주장하는 경우, 엔진 오일이 시간에 따라 없어지는 경우 등)

Ⅳ. UL 4600의 안전성 증명 방법

ISO 26262, ISO/PAS 21448와 같은 기존 표준에서는 A, B, C...와 같은 여러 기술적 조건이 표준 내에 정해져 있어서 자동차 제조사는 이를 문서, 시험, 측정 등을 통해 확인한 다음 모두 만족하는 것이 증명되면 해당 자동차가 안전하다고 인증한다. 그러나 UL 4600에서는 아래 (1)~(4)와 같이 상당히 다른 방식을 사용한다[7]-[10].

(1) 이 차는 A라는 환경, 즉 '운행 설계 범위(ODD: operational design domain)' 내에서 운행한다고 설정한다.
(2) A라는 환경에서 이 차가 안전하게 운행하기 위해서는 B1, B2, B3...라는 특성을 만족해야 한다고 '주장 (claim)'한다.
(3) 이 차는 C1, C2, C3과 같은 조건이 충족되면 위 (2)의 특성을 만족한다고 '논증(argument)'한다.
(4) 분석, 시뮬레이션, 측정, 테스트 등을 통해 이 차가 위 (3)의 조건을 만족한다는 D1, D2, D3...라는 '증거 (evidence)'를 제시한다.

UL 4600에서는 그림 2와 같이 (2)~(4)의 '주장', '논증', '증거'를 묶어서 '안전 사례(safety case)'라고 하며 해당 '안전 사례'를 논리적, 실증적으로 증명한다. 자율주행자동차가 겪을 수 있는 모든 경우에 대해 이러한 '안전 사례'를 증명한다면 이 차는 안전성이 보장된다고 할 수 있다.

UL 4600은 안전성을 증명하는 일부 과정을 '문맥 밖 요소(EooC : element out of context)'라는 이름으로 일종의 서브루틴처럼 사용할 수 있으며, 이를 위해 EooC을 연결하여 전체적으로 안전성을 증명할 수 있는 인터페이스를 그림 2와 같이 규정한다. 즉 하드웨어, 소프트웨어, 센서, 데이터 등 시스템

6.3 Hazards

6.3.1 **Potentially relevant hazards shall be identified.**

6.3.1.1 **MANDATORY:**

a) Hazard Log that lists identified hazards and mitigation status

1) Each hazard traces to a corresponding hazard mitigation approach

2) Mitigation status of each hazard is kept current and tracked to resolution to acceptable or accepted level of post-mitigation risk

b) Identify acceptable level of completeness of hazards listed

NOTE: This imposes an obligation upon the creator of the safety case to define a target level of completeness for hazard identification. The assessment criteria are: (1) the level of completeness has been defined; (2) in accordance with feedback requirements, any issue with that defined level being insufficiently rigorous is likely to be detected via the feedback mechanism.

c) Inclusion of hazards related to emergent properties and interactions of components

NOTE: Emergent properties and hazards due to component interactions are difficult to allocate to a single component level hazard, but can nonetheless present risk.

EXAMPLE: Missed timing deadline due to processor overload in a high-complexity operational environment.

6.3.1.2 **REQUIRED:**

a) Hazard log meets its defined level of completeness

b) Hazard log updated in response to newly identified hazards

c) Incorporation of hazards and risks identified in response to all clauses of this standard

d) Contribution of Commercial-Off-The-Shelf (COTS) items and other Non-Developmental Items (NDIs) to hazards

REFERENCE: See Section 13.4

6.3.1.3 **HIGHLY RECOMMENDED:**

a) Use of at least one of the following hazard identification techniques:

1) Failure Mode and Effects Analysis (FMEA)

2) Failure Mode, Effects and Criticality Analysis (FMECA)

3) Qualitative Fault Tree Analysis (Qualitative FTA)

4) ~ 16) omitted

16) Safety of the Intended Functionality (SOTIF)-style approaches

b) Use of at least one technique in each of the following categories

1) Bottom up analysis approaches

2) Top-down analysis approaches

3) Non-fault-based analysis approaches

c) **Pitfall:** Bottom-up approaches such as FMEA, FMECA, DFMEA are prone to missing hazards caused by component interactions, as well as correlated component faults, especially due to shared resources such as computational platforms (hardware, software, sensors, actuators)

NOTE: This Pitfall motivates combining bottom-up approaches with top-down approaches such as FTA and ETA.

d) **Pitfall:** Analysis approaches that involve hypothesizing a fault or failure are prone to missing hazards resulting from non-faulty component behaviors and interactions.

e) **Pitfall:** Methods that hypothesize a constrained component fault model are prone to missing fail-active hardware failure modes and unconstrained software failure modes.

6.3.1.4 **RECOMMENDED – N/A**

6.3.1.5 **CONFORMANCE:**

Conformance is checked by inspection of the hazard log and hazard analysis work products.

Fig. 3. Examples of normative elements in safety cases.
그림 3. 안전 사례에 포함되는 각 요소의 표기 예

을 구성하는 다양한 구성 요소를 제 3자가 제공하는 경우, 내부 설계 및 구현에 대한 정보를 제공하지 않고도 EooC 인터페이스를 통해 필요한 안전 관련 정보만을 전달할 수 있도록 한다.

UL 4600에서는 자율주행자동차를 위해서 다음과 같은 주요 항목을 규정하고 각각에 대해 '안전 사례'를 증명할 것을 요구한다.

- 6장: risk assessment
- 7장: interaction with humans and road users
- 8장: autonomy functions and support
- 9장: software and system engineering processes
- 10장: dependability
- 11장: data and networking
- 12장: verification validation, and test
- 13장: tool qualification, COTS, and legacy components
- 14장: lifecycle concerns

- 15장: maintenance
- 16장: metrics and safety performance indicators

UL 4600은 위의 주요 항목마다 '안전 사례'에 포함되어야 할 요소를 정의하고 하부 항목별로 나누어 이를 증명하도록 요구한다. 그림 3은 주요 항목인 risk assessment에 포함된 하부 항목인 hazard에 대해 '안전 사례'에 무슨 요소가 포함되고 증명되어야 하는지를 나타낸 예이다. 이 요소 들은 그 성격에 따라 numbered clause, mandatory, required, highly recommended, recommended, pitfall, conformance 등으로 표기하는데 그 의미는 다음과 같다.

- numbered clause(예: 6.3.1): 각 항목에 대한 정의이면서 동시에 규정된 내용을 반드시 문구 그대로 지켜야 하는 사항
- mandatory: 규정된 내용을 반드시 문구 그대로 지켜야 하는 사항
- required: 규정된 내용을 반드시 문구 그대로 지켜야 하는 사항. 단 해당 요소가 적용되는 대상의 특성상 문구 그대로 적용할 수 없는 경우에 한하여 그 이유를 설명하고 변경 가능함
- highly recommended: 규정된 내용을 가능하면 지켜야 하되 경우에 따라 생략할 수 있는 사항
- recommended: 규정된 내용을 지키면 더욱 좋지만 지키지 않아도 무방한 사항
- pitfall: 설명 및 증명에서 발생하기 쉬운 오류를 지적해놓은 사항
- conformance: 각 요소가 표준에 부합하는지 여부를 어떻게 판단할 것인지 설명해놓은 사항

Ⅴ. 결론

본 논문에서는 자율주행자동차의 안전성을 보장하기 위해 새로 개발된 국제 표준인 UL 4600에 대해 살펴보았으며 UL 4600의 가장 큰 특징인 안전성의 논리적 증명 방법에 대해 설명하였다. UL 4600은 극히 최근에 제정된 국제 표준이지만 개발 위험의 항변에 관한 증명 문제 등과 같은 논의에도 중요하게 작용할 수 있어서 자율주행자동차 산업에 미치는 영향이 매우 크기 때문에 더 많은 소개와 관심이 요구되고 있다. 본 논문을 통해 자율주행자동차 분야의 엔지니어들이 UL 4600에 대해 더 많이 이해하여 자율주행자동차 산업을 크게 발전시킬 수 있기를 기대한다.

References

[1] S. Ihm and S. Lee, "A Study on the Liability for Damages and the Burden of Proof Relating the Autonomous Car," *Yonsei Law Review,* vol.30, no.3, pp.309-332, 2020. DOI: 10.21717/ylr.30.3.10

[2] S. Lee, "ISO 26262 and ISO/PAS 21448 as Exemption Clauses of Product Liability," *j.inst. Korean.electr.electron.eng.*, vol.23, no.1, pp.346-349, 2019. DOI: 10.7471/ikeee.2019.23.1.346

[3] UL 4600, "Standard for Safety for the Evaluation of Autonomous Products," https://ul.org/UL4600

[4] ISO 26262-1:2018, "Road vehicles - Functional safety - Part 1: Vocabulary," https://www.iso.org/standard/68383.html

[5] ISO/PAS 21448:2019, "Road vehicles - Safety of the intended functionality," https://www.iso.org/standard/70939.html

[6] SAE J3016_201806, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," https://www.sae.org/standards/content/j3016_201806

[7] P. Koopman, "UL 4600 Overview: Standard for Evaluation of Autonomous Products," https://www.autoelectronics.co.kr/article/articleView.asp?idx=3552

[8] P. Koopman, "Key Ideas: UL 4600 Safety Standard for Autonomous Vehicles," https://www.youtube.com/watch?v=qDizhcn23RI

[9] D. Prince and P. Koopman, "UL 4600 General Stakeholder Overview," https://www.youtube.com/watch?v=yg1sfBeJTRI

[10] D. Prince and P. Koopman, "UL 4600 Technical Overview," https://www.youtube.com/watch?v=amsOg5Y6H14