STANDARDS ACADEMY
By UL Research Institutes
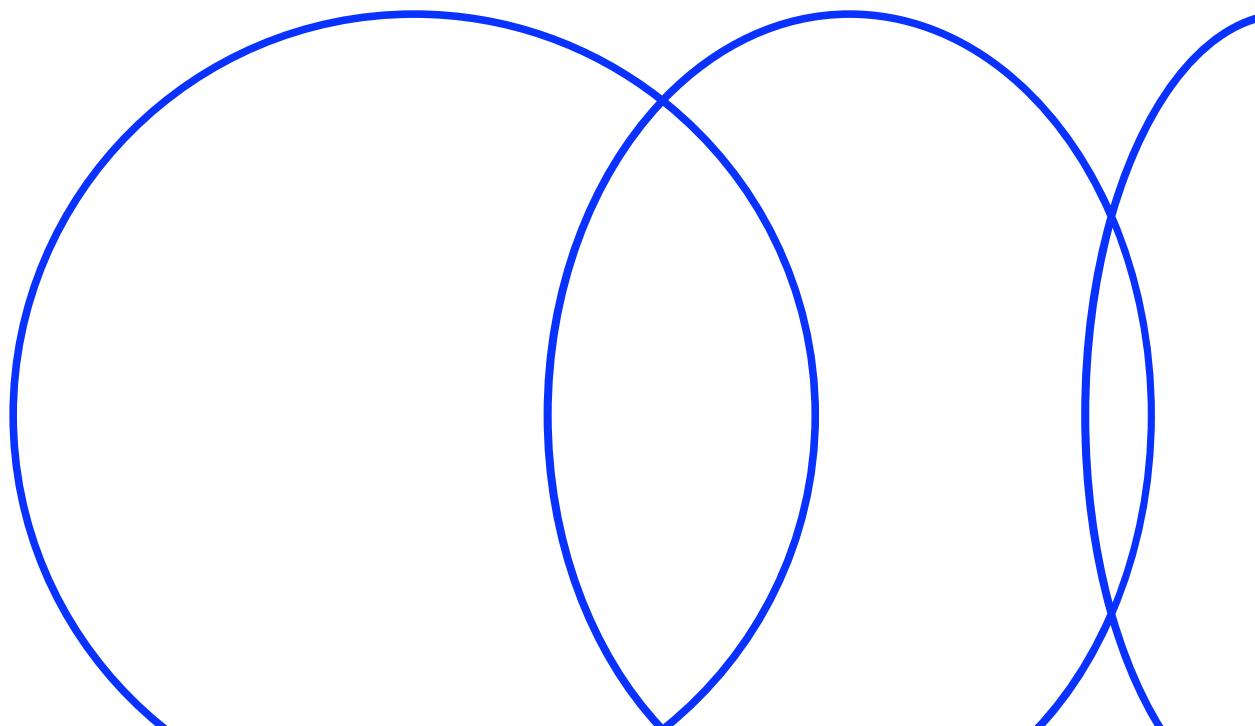
STANDARDSACADEMY.ORG

Making Autonomous Vehicles Safer

UL 4600

Brought to you by

UL Research Institutes

UL Standards & Engagement

Learn about the first comprehensive safety standard for autonomous vehicles.

Table of Contents

Abstract

Autonomous vehicles (AVs) are no longer an idea of the future. Replacing some — or all — of the need for a human driver, AVs are already being used in personal, commercial, and military applications. However, their safety is far from automatic. Vehicle producers make thousands of decisions when designing AVs. As participants in UL Standards & Engagement's standards development process, experts in safety and transport developed and published UL 4600, the Standard for Safety for Evaluation of Autonomous Products, to support the design of these vehicles and ensure safety on the road. This case study describes how the ULSE's TC 4600, the Technical Committee for Evaluation of Autonomous Products, convened around the need for an AV safety standard and how its safety case solution provides comprehensive guidance to AV producers for safer innovations in vehicle autonomy.

Learning Objectives

- Understand that a safety case allows manufacturers to share their product's safety and viability considerations through claims supported by evidence.

- Learn how UL 4600, the Standard for Safety for Evaluation of Autonomous Products, diverges from traditional safety standards by utilizing a comprehensive "safety case" method for autonomous vehicles.

Real world context

Autonomous vehicles promise safer and more efficient driverless transportation, something that was once a science fiction fantasy.

But there are risks

But even autonomous vehicles have been involved in traffic accidents, injuring people inside and outside of the vehicles, and damaging property.

For example

When anything happens outside of the vehicle's expectations, the risks for harm can increase.

> Makers of autonomous vehicles must try to anticipate unexpected conditions, but how could an autonomous vehicle possibly be prepared for everything?

Background

Kaylien Miller, a woman in rural Grand Rapids, Minnesota, has an autoimmune disorder called lymphedema which makes her legs sting when she walks. Without a driver's license of her own, Miller independently gets around town and to her job in autonomous vehicles (AVs). She finds the vehicles to be "reactive" and said that reactivity once helped the car she was in avoid an accident by braking sharply (Kutterer, 2024). But an AV's reactions also caused a woman in San Francisco to be pinned and dragged approximately 20 feet as the vehicle followed post-accident protocol to clear the roadway following its own collision with the woman (Wong, 2023). In this case, the safety maneuver made the situation worse.

These examples show the benefits of AVs, as well as the risks. The vehicles themselves offer novel solutions to transportation issues worldwide, from simple things like food delivery to critical tasks including transporting sick individuals to hospitals and clearing areas where landmines have been buried. AVs can increase mobility for elderly or disabled persons like Miller, improve traffic efficiency and safety, and even reduce emissions if clean propulsion is used (Golbabaei et.al., 2020; Greenblatt & Saxena, 2015). However, the complexities of driving mean that driverless safety is not clear-cut. While some technologies are made of one system or function, AV technologies involve numerous interdependent systems within a vehicle,

including traditional vehicle systems (power, emissions, steering, climate control) and new autonomous systems for navigation and sensing, which rely on computer programming and predictive modeling.

AVs create and update a map of their surroundings as they drive, integrating input from sensors with static (e.g., maps) and dynamic (e.g., real-time road hazard or weather updates) navigation information. Recognition systems note traffic, obstacles, signs, stop lights, and humans. A human or vehicle must trigger instant decisions to avoid safety incidents such as near hits, vehicle crashes, or vehicle mechanical failures. And as we've noted above, what is safe in one instance may be dangerous in another.

Several safety standards support safe motor vehicle operation, including the International Organization for Standardization standards ISO 26262, Road Vehicles — Functional Safety, for traditional, nonautonomous vehicles and ISO/PAS 21448, Road Vehicles — Safety of the Intended Functionality, for semiautonomous vehicles. Semiautonomous vehicles, which hand off responsibility between a driver and the autopilot, still rely on driver oversight to ensure the vehicles' safe operation (Othman, 2022). In 2017, fully autonomous taxis debuted in San Francisco, introducing a host of new, nonhuman-mitigated safety threats into city driving. For the first time, human oversight of vehicular safety was completely removed from vehicle operation, which meant that the machine had to be entirely responsible for the safety of the vehicle, its passengers, and its surroundings. No safety standards existed to regulate completely autonomous vehicles for human and goods transportation. What would this mean for public safety?

> Explore the AV incident database to learn more about autonomous vehicle incidents and the rise in incidents since 2017.

Problem

Since 2017, there have been 712 autonomous vehicle accidents in the U.S., and 15% of these incidents injured someone inside or outside of the vehicle (Transport Research Centre, n.d.). The safety community, including the National Highway Traffic Safety Administration and various standards development organizations, took notice (Koopman, 2022). The problem emerged that typical standards-setting processes would not work for a system as complex as an AV. Philip Koopman, an associate professor at Carnegie Mellon University, initiated a conversation with UL Standards & Engagement's TC 4600, the Technical Committee for Evaluation of Autonomous Products, to explain the problem and offer a novel solution.

Typical safety standards, like those developed up to this point by ULSE, state clear guidelines for how safely the product should work under a given set of circumstances and what tolerance there is within its safe operation. These safety assurance efforts are either prescriptive, requiring specific designs to meet specific codes or requiring the inclusion of fail-safe design and protection systems, or process-oriented, requiring specific construction or maintenance actions to ensure safe products and safe use (Leveson, 2011).

Picture a car airbag, for example. Expert committees determine acceptable safety thresholds for airbag deployment and design tests to determine whether a particular airbag can be certified as "safe" based on test performance. With these standards and tests in mind, designers construct airbags that should function safely and meet the standard's testing thresholds when used in predictable conditions. If an error is detected later, such as an airbag that gets too hot and burns passengers when it deploys in a crash, then a recall will pull back the product or component to ensure public safety.

How could a safety standard — a collection of performance expectations and tests for compliance in predetermined situations — be written to encapsulate a vehicle's possible safe or unsafe behavior in widely variable conditions? AVs must operate safely in variable weather, geography, and surroundings, navigating varied speed limits, street markings, and signage while carrying infinitely variable passenger and cargo loads. What happens if an error occurs in a system that is so complex it becomes hard to tell which system was at fault or which component to recall?

How safe is safe enough for you? Would you be willing to ride in a fully autonomous vehicle as a driver who could take the wheel or as a passive passenger? In 2016, 61.5% of U.S. drivers said they were unwilling to ride in an autonomous vehicle (Menon et al., 2016). Do you agree or disagree with them? What would help you feel safe riding in an AV?

Approach

To meet the complex needs of autonomous vehicles, UL Standards & Engagement published its first-ever safety case-based standard, UL 4600, the Standard for Safety for Evaluation of Autonomous Products. UL 4600 requires manufacturers to write safety cases consisting of safety-related claims supported by arguments and evidence. The safety case method contrasts with the traditional safety standard, which mandates that products meet prescribed construction or performance metrics.

The safety case method shifts responsibility for risk management to manufacturers and emphasizes meeting safety goals and documenting how they are met (Leveson, 2011). Safety

cases require authors to fully describe how a product is designed as a safe system, using evidence to justify their argument that the product is "safe enough." UL 4600 does not set the bar for what is "safe enough," instead relying on the manufacturers to set and explain their own thresholds for safety. Koopam, the safety expert who brought the suggestion of using a safety case standard for the complex AV problem to ULSE, said, "We're not standardizing the product, we're standardizing the safety case." (Berman, 2020).

In a safety case, manufacturers construct logical trees of reasoning, branching from safety claims and subclaims (e.g., premises or goals) to linked logical arguments about how each claim could be valid if specific evidence could be collected (Figure 1). Finally, the tree terminates in the corresponding data to support the claim. Data should be collected from the product's safety performance indicators to support the claim. Hence, SPIs are metrics used to justify a claim (Koopman, 2022).
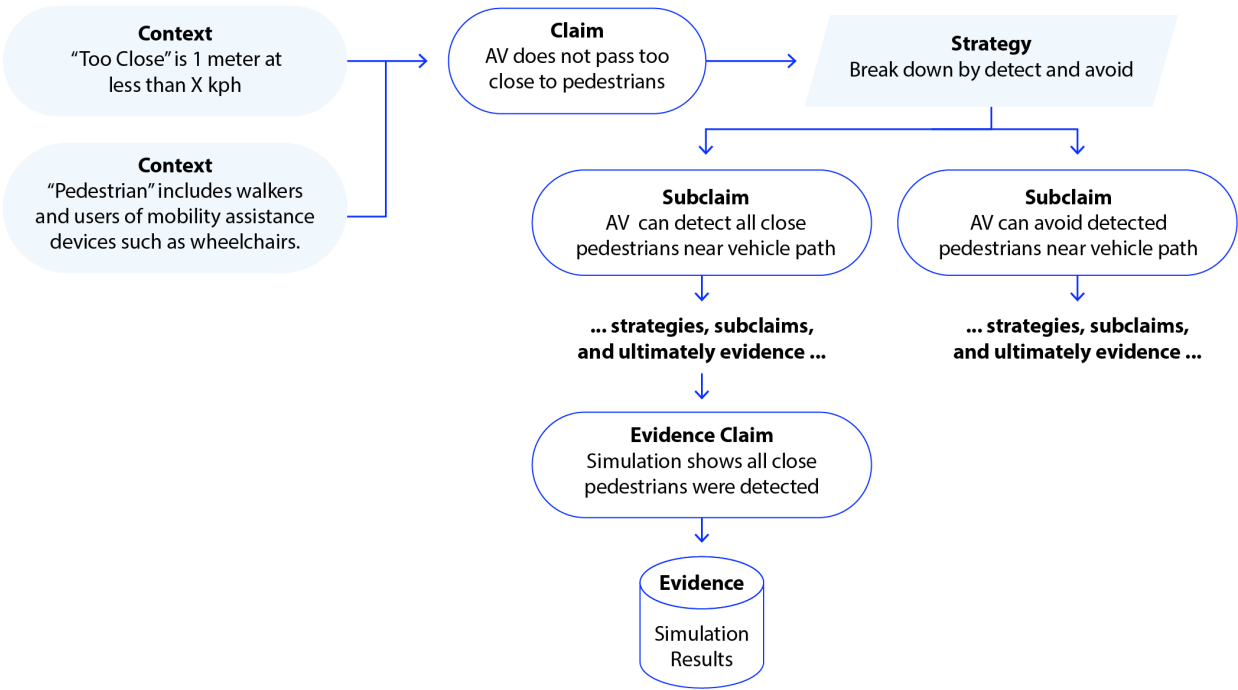
Figure 1. Example Safety Case Logic Tree (Source: Koopman, 2022, p. 25).

In this way, the actual data of operation, which could be gathered from computer-monitored indicators, road test performance, or physical measurements such as temperatures, are used to demonstrate the item's safety in its safety case. Safety cases do not include ethical and societally acceptable factors such as assigning liability or blame following a safety incident. However, case authors do need to justify their chosen threshold values for safety with technical and nontechnical explanations. Logical arguments are required, and spurious or

nondeductive arguments are discouraged. Every claim must be falsifiable to be convincingly supported by evidence.

In addition to general operation, the safety case should justify safe functioning during real and imagined risks and describe how the system would mitigate any hazards. For example, sensors are ubiquitous on AVs to support real-time navigation and driving. To fully describe how an AV's sensors would operate safely, UL 4600 specifically mandates that authors create a fault model to address how their AV will handle a slew of adverse sensor reactions such as sensor faults triggered by environmental conditions (rain, water splash, mud, ice, dirt, low and high temperatures, and low and high humidity), man-made issues (sensor defacement, alignment compromise, gouged optics, blunt force impact), regular use (vibration and mechanical wear), and other "unknown unknowns" that could arise during operation. Safety cases even require the authors to list why they did not consider or mitigate a particular fault, ensuring that the safety case is comprehensive of a maximum number of in-scope threats or deliberately articulating which threats are out of scope.

Safety case methodology rests on the "claims, argument, evidence" approach. Compare this method to another form of reasoning you use when justifying how you approach design decisions in your field (e.g., mathematical proofs or claims, evidence, and reasoning in scientific argumentation). Compare your method to the safety case method. Which part of the claims, argument, or evidence do you rely on most to make your point?

Solution

UL 4600, the Standard for Safety for Evaluation of Autonomous Products, focuses on the quality of the safety argument and the considerations included in it. UL 4600 requires manufacturers to address an extensive variety of scenarios related to safety, asking the manufacturer, "did you think of that?" through a series of prompts. To make a strong argument, manufacturers should use the claim, argument, and evidence method to specifically address hundreds of potential AV-related faults provided in the standard, including those related to interactions with people inside and outside of the vehicle (e.g., passengers, bicyclists, pedestrians, construction crews, and toll booth workers); autonomy functions and support; software and systems engineering processes; dependability; data and networking; verification, validation and testing; integrated tools including commercial off-the-shelf components; life cycle concerns; and maintenance concerns. The lists of prompts in UL 4600 are extensive to clearly describe everything that might be included in an AV, from hardware to software, and sensors to battery management.

A safety case that addresses hundreds of pages of prompts with detailed evidence and arguments will be lengthy. To support authors in being comprehensive while prioritizing what to include, UL 4600 organizes prompts into five categories: requirement statements, overarching categories that must be fully addressed in the safety case; mandatory prompts, which will also be fully addressed; required prompts that can be avoided if shown to be intrinsically incompatible with the item; highly recommended prompt elements that could be plausibly excluded with rationale; and recommended prompt elements, which may be excluded without a rationale. This guidance indicates that if a prompt or fault is outside the operational design domain, it can be considered an element out of context, and the authors must indicate why they are not addressing it.

To encourage comprehensive safety considerations, UL 4600 includes examples for many of the prompts taken from real-life incidents and the authors' reasonable extrapolation of possible safety incidents. These examples are intended to help extend authors' thinking by articulating potentially relevant instances for AV use. For instance, prompts might remind authors that human passengers may need to use medical equipment in and outside of the vehicle and may require special considerations. Or, noting that vehicles may not always be used on well-regulated city streets, in fact, they could pass outside of the operational design domain in war zones, flooded areas, fire zones, police activity zones, or extreme weather areas.

To achieve UL 4600 certification, a manufacturer should write its safety case and submit it to an independent, but not necessarily external, conformance assessor. UL 4600 works in tandem with other related safety standards and codes, which each have their own procedures for testing and certification. Like many safety standards, UL 4600 is a living document that will change over time in response to emerging technologies. It has been updated twice since it was first published in 2020, each time involving the same technical committee of experts to reach consensus and publication after public comments. Version three expands the scope of the standard to include heavy commercial autonomous trucks that operate on public roads.

Discussion Questions

Some autonomous vehicle proponents will argue that AV adoption will create an autonomous driving ecosystem to improve mobility options for the masses, including AV sharing, while reducing traffic jams and cutting greenhouse gas emissions. On the other hand, opponents argue that AV inclusion in transportation systems might increase road congestion, urban sprawl, and worsen socioeconomic divisions based on access.

◇ How do you think AVs should play into sustainable decision-making for transit systems? How might regulated AVs support a vision for sustainable transit?

◇ What role can local regulators play in helping keep AVs operating safely in their locality?

◇ Consider the implications for liability in AV safety. Who should be liable when an AV is involved in an accident? Debate whether liability rests with the owner of the vehicle, the manufacturer of the vehicle, or the manufacturer of a specific vehicle component or computer program.

How to Get Involved

UL Standards & Engagement is actively seeking all interested parties to participate in its standards development process and encourages diverse perspectives to join in by participating as a stakeholder. Stakeholders can submit, review, and comment on proposals for new standards or revisions to existing standards. While stakeholders do not vote, the TC considers their input during the standards voting process. Since standards affect everyone, all are welcome to participate as stakeholders. Register online through ULSE's Collaborative Standards Development System: csds.ul.com

Advance your career

Check out current internship and fellowship openings for opportunities to engage with standards professionals and to contribute to standards research and innovation.

Careers | UL Research Institutes: ul.org/about/careers

Careers | UL Standards & Engagement: ulse.org/careers

GEM Fellowships at ULRI-ULSE: ul.org/about/careers/gem-fellowships-at-ulri-ulse

References

Transport Research Centre. (n.d.). Autonomous Vehicle Crashes [Data set]. Czech Republic Ministry of Transport. <https://www.avcrashes.net/>

Berman, B. (2020, April 29). Underwriters Labs publishes first AV safety standard. SAE International. <https://www.sae.org/news/2020/04/underwriters-labs-publishes-first-av-safety-standard>

Golbabaei, F., Yigitcanlar, T., Paz, A., & Bunker, J. (2020). Individual predictors of autonomous vehicle public acceptance and intention to use: A systematic review of the literature. Journal of Open Innovation: Technology, Market, and Complexity, 6(4), 106. <https://doi.org/10.3390/joitmc6040106>

Greenblatt, J. B., & Saxena, S. (2015). Autonomous taxis could greatly reduce greenhouse-gas emissions of US light-duty vehicles. Nature Climate Change, 5(9), 860-863. <https://doi.org/10.1038/nclimate2685>

Koopman, P. (2022). The UL 4600 Guidebook: What to Include in an Autonomous Vehicle Safety Case. Carnegie Mellon University.

Kutterer, K. (2024, July 26). 10,000th rider spotlight: Grand Rapids, MN. May Mobility. <https://maymobility.com/posts/10-000th-rider-spotlight-grand-rapids-mn/>

Leveson, N. G. (2011). The use of safety cases in certification and regulation [White paper]. Massachusetts Institute of Technology, Engineering Division. <https://dspace.mit.edu/handle/1721.1/102833>

Menon, N., Pinjari, A., Zhang, Y., & Zou, L. (2016). Consumer perception and intended adoption of autonomous-vehicle technology: Findings from a university population survey (No. 16-5998).

Othman, K. (2022). Exploring the implications of autonomous vehicles: A comprehensive review. Innovative Infrastructure Solutions, 7(2), 165. <https://doi.org/10.1007/s41062-022-00763-6>

Wong, G. (2023, October 3). Woman critically hurt after being pinned under Cruise robotaxi in SF. San Francisco Examiner. <https://www.sfexaminer.com/news/transit/woman-hospitalized-after-being-pinned-under-cruise-car-in-sf/article_2a20709c-6224-11ee-8823-57142a0d0f9e.html>