Automated Driving Systems (ADS) Safety: A Holistic Approach

Ensuring the safe deployment of ADS-equipped vehicles is perhaps the greatest challenge faced by industry and regulators alike

UL Solutions

Safety. Science. Transformation.

Introduction

For more than 100 years, automobiles have played a crucial role in enabling and expanding personal access to jobs, shopping, recreation, schools and our quality of life. It's hard to overestimate the role of automobiles in shaping our cities and modern society.

And up until recently, these vehicles have been completely dependent upon human drivers for sensing road conditions and traffic controls and deciding vehicle direction and speed. Now, increasingly capable electronic sensors and sophisticated algorithms are assisting drivers in controlling the vehicle and are even allowing for fully automated driving under certain driving conditions. Indeed, automated driving systems (ADS) offer the potential for more convenient, safer and efficient transportation for the future of mobility.

Most automakers, as well as many tech companies and startup ventures, are heavily investing in the development of autonomous vehicles and enabling systems and technologies. Many governments at both the national and local levels are actively supporting these efforts as well. Ensuring the safe deployment of ADS-equipped vehicles is perhaps the greatest challenge faced by the automotive industry and regulators alike. Intuitively it may seem that safety is all but assured by ADS, which are not subject to distraction, fatigue, and other human frailties , but the reality is far more complex. This white paper considers a holistic approach to safety and introduces a graphic as a summary of important ADS safety elements.

A brief history of product safety

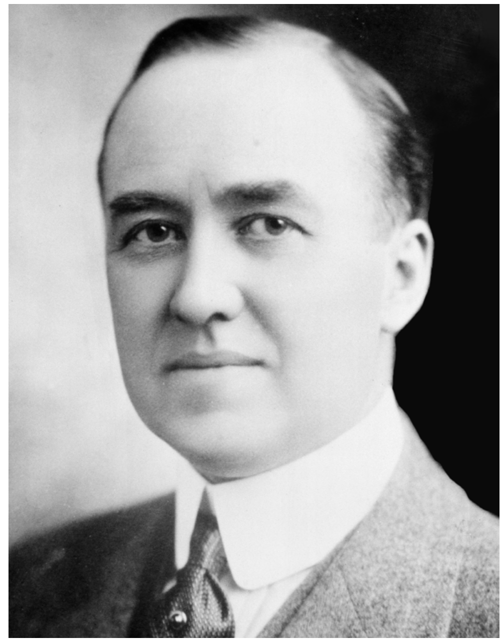
When discussing a topic as new and complex as ADS safety, it may be helpful first to review previously established general principles in product safety for guidance. Historically, the concept that the maker of a product bears some responsibility for its safety is at least several thousand years old. Consider, for example, the Code of Hammurabi from ancient Babylon, where Code 229 instructs that if one builds a house for someone but does not construct it properly so that it collapses and kills the owner, then that builder shall be put to death.[1] This is a very early example of government asserting its authority over rule making, assignment of responsibility, and enforcement related to product safety.

Since the Industrial Revolution, and especially in recent times, there has been a dramatic proliferation in products and consumer items, which have brought many modern conveniences, but also safety considerations which must be carefully managed. Some of the earliest consumer products for sale in the U.S. were food items and drugs. By the late 1800s, several grassroots movements and journalistic exposes publicized the need for better standards and oversight to ensure safe foods and medicine. These movements culminated in Upton Sinclair's writing about the horrific conditions of the meat processing industry in "The Jungle," which led to the United States enacting its first comprehensive food and drug law – the Pure Food and Drug Act of 1906.[2] It would be another 60 years before rapidly rising automobile fatalities prompted the United States to enact the National Traffic and Motor Vehicle Safety Act of 1966, leading to the adoption of Federal Motor Vehicle Safety Standards.[3]

While governments have historically played a major role in setting safety requirements and consequences for falling short of these, regulations alone are rarely sufficient to ensure the safety of a product – especially as the complexity of the product increases. At the end of the 1800s when the use of electricity was new, few regulations existed to govern its safe use. Fire insurance underwriters were keen to understand the risks associated with the electrical installations of their customers and often hired expert inspectors to advise them on major projects. One such inspector foresaw how testing could be applied to better understand the fire safety aspects of electrical equipment.[4]

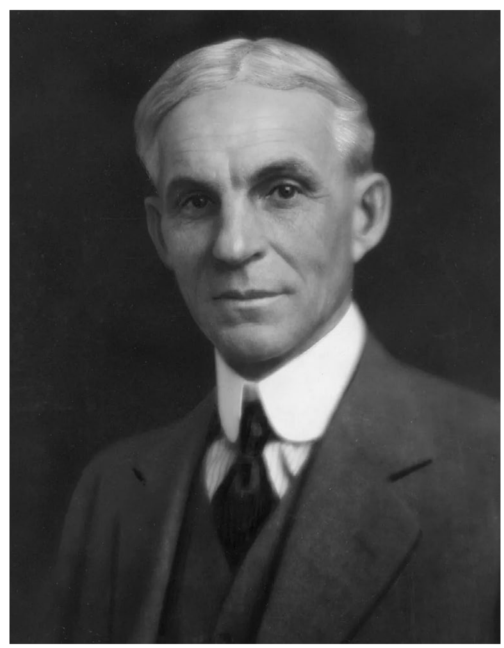
The Code of Hammurabi,
The Louvre Museum, June 16, 2016.

Underwriters Electrical Bureau was founded in 1894 by William Henry Merrill, Jr., and became Underwriters Laboratories in 1901.[5] Now UL Solutions, the company is one of the world's oldest safety science companies. Merrill, a graduate of the Massachusetts Institute of Technology, recognized the need to test new electrical inventions and building materials for safety before they entered production. Merrill espoused a fundamental and enduring product safety principle, "know by test," which is as true today as it was then. Reflecting on the importance of his safety testing mission, Merrill stated, "We are doing something for manufacturers and buyers and property owners everywhere – we are doing something for humanity." [6]



William Henry Merrill, Jr, founder of Underwriters Electrical Bureau

While regulations and product testing and certification contribute much to the safety profile of manufactured products, limitations still exist to solely relying on these approaches. For example, it may be practical to test only a limited sampling of a manufactured product rather than every unit produced, and so methods of ensuring that future production does not vary adversely from the tested sample are necessary. Further, it may not be practical or possible to completely test all aspects of a highly complex system, or even to anticipate every test which may be necessary to ensure safety. Fortunately, the science of standardization of design and manufacturing best practices and the implementation of process control methods were also rapidly advancing. While the initial motivation for these advances may have been to improve quality and reduce costs, standardization and process methods also proved useful for improving the safety posture of products. Henry Ford, the founder of Ford Motor Company, and an earlier pioneer of automotive mass production, understood the essential role that standardization played in his company's success, saying, "If you think of standardization as the best that you know today, but which is to be improved tomorrow, you get somewhere."[7]



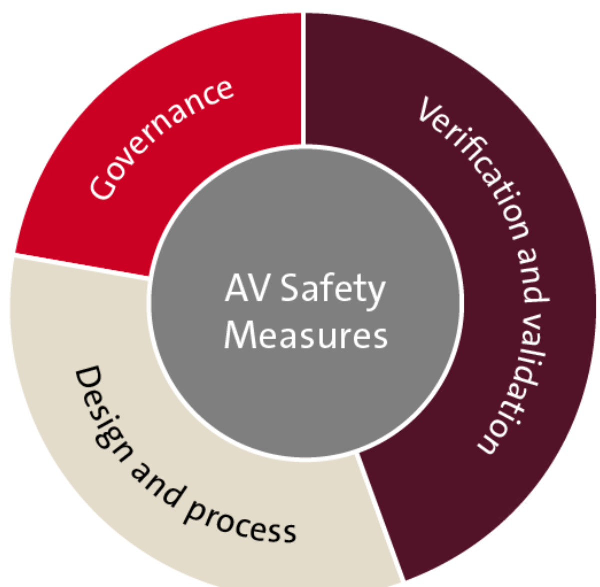
Henry Ford, the founder of Ford Motor Company, (Image courtesy of Encyclopædia Britannica)

And W. Edwards Deming, the founder of Total Quality Management, believed that robust design and process controls could minimize reliance on product inspections and testing during the manufacturing process. Today, many standards making bodies around the world actively contribute to the advancement of product safety by publishing safety standards for new products, while updating existing standards with new innovations and knowledge.

A holistic approach to safety

Today, the automotive industry is experiencing a period of rapid transformation and incredible innovation. Advances in electronics, especially in processing power and sensors, along with sophisticated control algorithms and artificial intelligence promise to make fully autonomous vehicles (AV) a reality. While the potential benefits of this technology are many, new safety challenges continue to emerge. Ensuring the safe and secure operation of increasingly intelligent and complex vehicle systems imposes serious responsibilities. Are the safety methods and best practices of the past still applicable to autonomous vehicles? Many new tools and safety standards are being developed to address autonomous safety — what role do they play? As we look at these questions, it is not our intention to critique or evaluate in detail specific safety approaches and tools, but rather to provide an overall context to better understand the role each plays in the larger, more holistic view of autonomous safety.

In our view, many aspects and contributing elements impact the safety profile of a product. And focusing only on some of these areas may lead to safety deficiencies in other areas. In general, the more complex the product, the more complex the assurance of its safety. And the greater the potential severity of an adverse safety incident, the greater the importance of a comprehensive and robust safety framework. Informed by the historical record of safety best practices, we have divided safety measures into three primary categories in the figure on the right: Governance, Design and Process, and Verification and Validation. From a high level, these categories represent sound safety principles which are applicable to a broad range of products. Specific methods and tools utilized within these categories may differ based on the characteristics and safety risks of a particular product type. In the following sections, we will look at some important elements related to the safe development and deployment of autonomous vehicles.



Governance measures

As mentioned, governments play an important role in ensuring public safety by setting and enforcing rules which regulate safety aspects of products. More generally, we may refer to these aspects as governance measures, which also may include a system of third-party or even self-oversight. Key aspects for effective governance include objectivity and avoidance of conflicts of interest.

Governance measures may be further categorized by those measures which are strictly the domain of governmental authorities, such as legal regulations and enforcement actions, and those measures which may be reasonably accomplished by other parties which maintain a sufficient level of objectivity to avoid conflicts of interest.

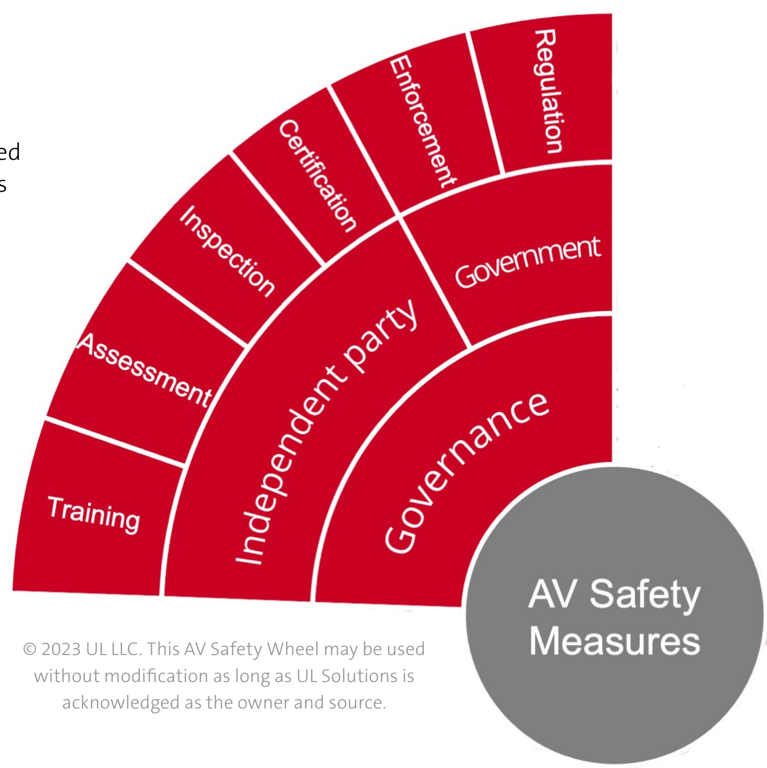
In the figure below, we have categorized typical governance measures into three levels – with the inner level being the most general and the outer level being examples of typical specific measures.

For example, let's consider the specific U.S. regulation applied to air bag protection for passenger cars. The U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) administers Federal Motor Vehicle Standard (FMVSS) 208 that contains requirements for occupant crash protection including air bags. The history of air bag regulation under FMVSS 208 is decades long and rather complicated. However, key milestones include a 1984 amendment to FMVSS 208 that required automatic occupant protection for which air bags were one option, a 1993 amendment specifically mandated the use of frontal airbags, and a 2000 amendment required advanced frontal airbags designed to reduce the risk of air-bag-induced injuries of smaller occupants such as young children.[8]

The power and benefits of effective safety regulation are clearly evidenced in NHTSA's claim that frontal air bags saved 50,457 lives from 1987 to 2017.[9] Automotive manufacturers benefit as well from appropriate safety regulation that requires all competitors meet a common target.

However, regulatory measures are often limited. For example, they may be reactive rather than proactive, may take considerable time to implement, may not foresee unintended adverse effects and may not address the potential for design and manufacturing flaws that negatively impact safety.

NHTSA's recent safety recalls of certain air bags highlight some of the potential challenges and limitations of safety regulation. Due to the enormous complexity of autonomous vehicle systems, we should anticipate both a great need for and great challenges in developing appropriate and effective safety regulations.



Design and process measures

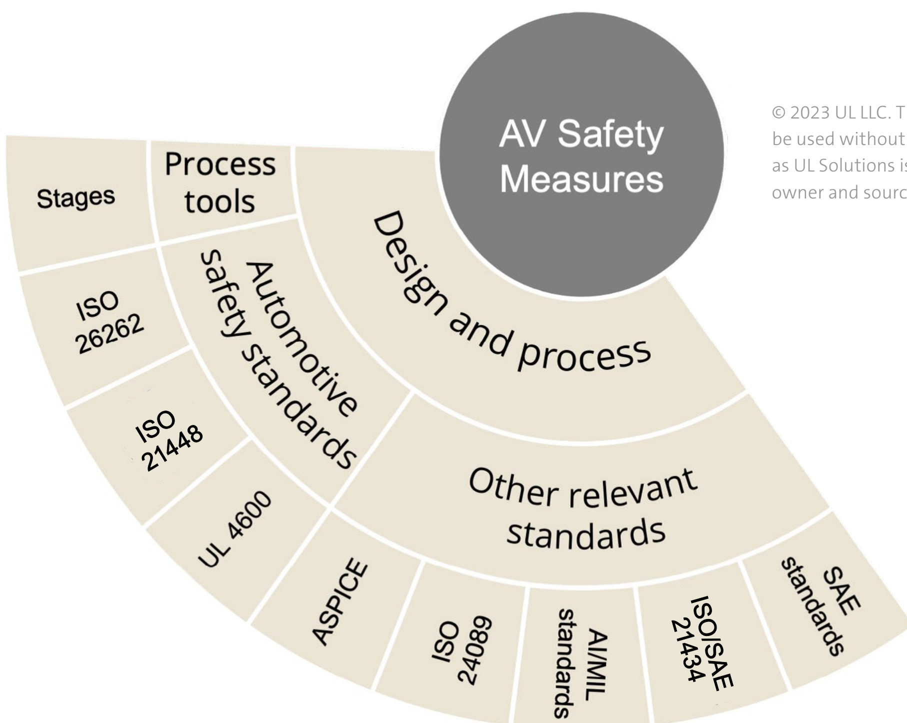
To help ensure that a product will meet or exceed safety requirements, companies adopt suitable methodologies into their processes which guide the safe development, manufacturing and support of their products.

These design and process measures include compliance with relevant standards for autonomous vehicles such as ISO 26262 "Road Vehicles – Functional Safety" which is concerned with mitigating risk due to system failures; ISO 21448 "Safety of the intended functionality" which is concerned with guaranteeing safety in the absence of a fault; and UL 4600 "Standard for Safety for the Evaluation of Autonomous Products," which is concerned with autonomous safety where there is no human in the control loop. General quality standards and methodologies, such as Automotive SPICE® (ASPICE), also play an important role in the safety profile of an autonomous vehicle. The included figure shows an example landscape encompassing applicable design and process measures.

Instead of trying to implement all applicable standards individually and independently, one best practice would be to define a set of processes that complies with all of them. For example, a properly defined system design process may cover the respective clauses of the safety and security standards, as well as the requirements of general quality standards.

With well-defined processes, every requirement in each of those standards can be mapped onto activities, roles, procedures, guidelines, checklists or work product templates. This allows efficient detection of compliance gaps across all standards and enables process adjustments without causing standard violations. Engineers and designers can follow one set of processes without having to worry about the individual standards. Process tools like Stages can help guide process definition, minimize manual overhead and accelerate adoption of new processes in practice.

Finally, as knowledge of emerging and highly complex autonomous vehicle systems continues to grow, we can expect new and revised design and process measures to capture improvements in the safety science.



Verification and validation measures

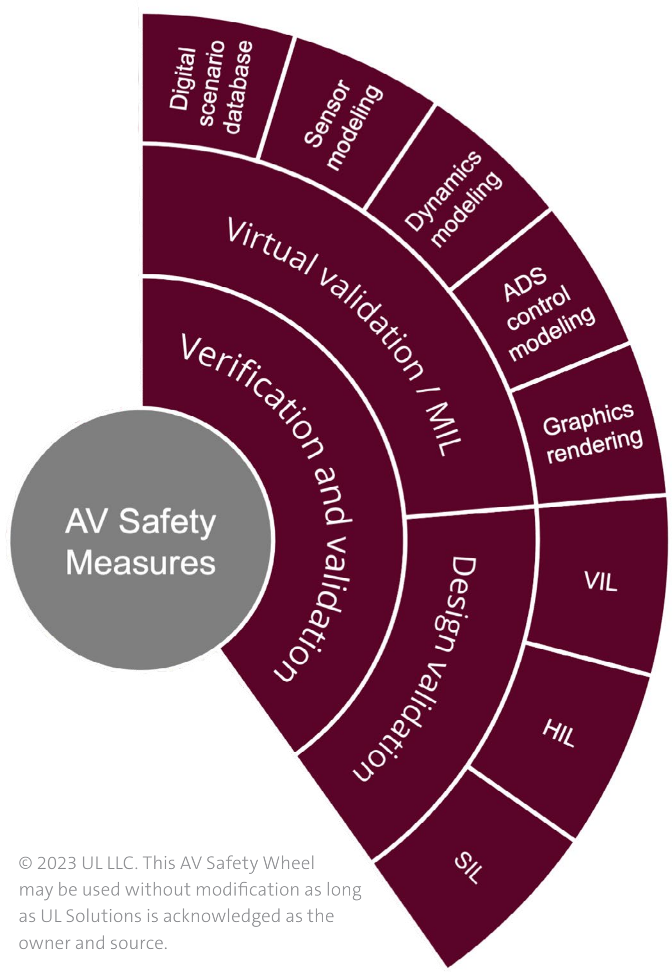
The third essential aspect of autonomous vehicle safety is verification and validation measures that seek to prove through testing that the safety performance of a vehicle meets requirements and expectations.

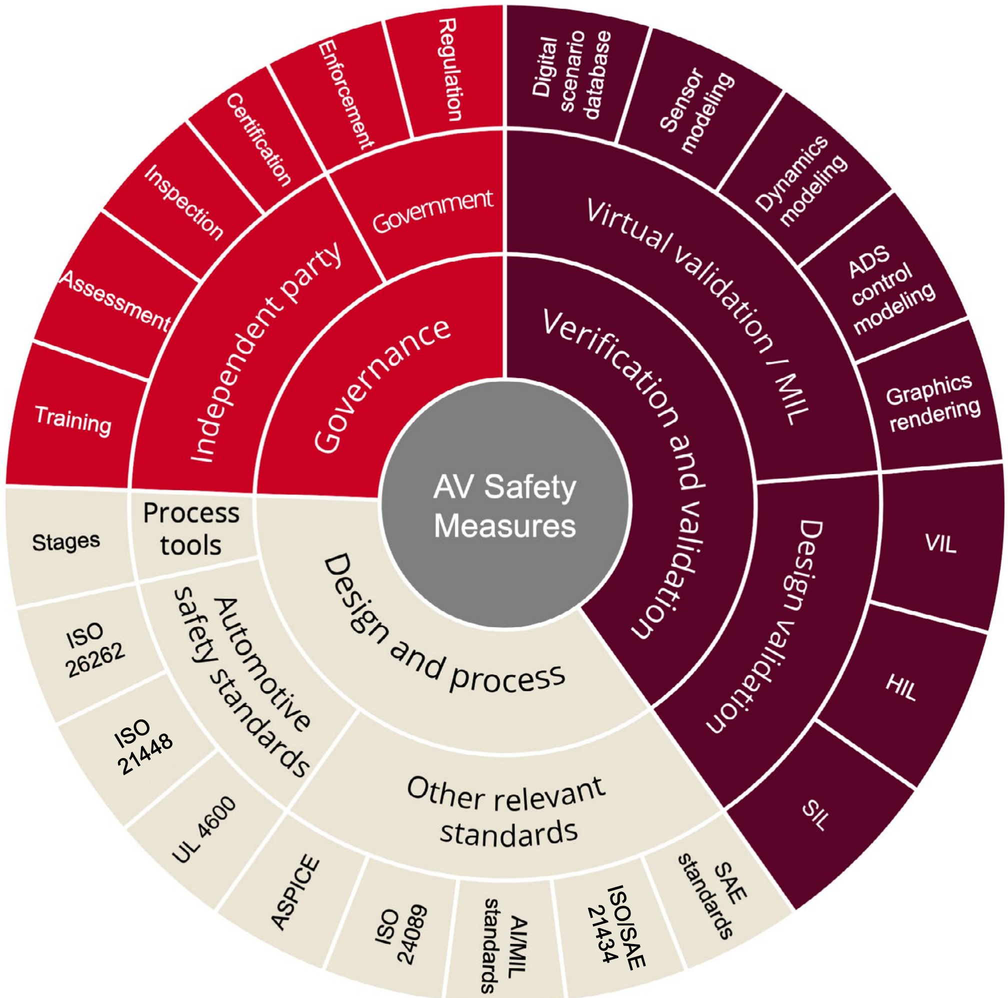
Whereas in the past a finite set of physical tests could be defined to provide a high level of confidence in the safety profile of a vehicle, this becomes increasingly impractical with autonomous vehicles due to the complexity and vast variety of situations in which these vehicles operate. Therefore, we expect a corresponding increase in the sophistication of verification and validation measures, including a significantly increased utilization of virtual modeling and validation techniques that test vast numbers of scenarios at a comparably low cost and a savings in time. Of course, this virtual modeling will not replace but will complement physical testing that is also evolving to meet the specific challenges of autonomous vehicles. The figure below provides a typical example of best practice measures utilized in the verification and validation testing of autonomous vehicles.

As with the other safety measures, it is important for practitioners and others responsible for verification and validation to maintain objectivity and avoid conflicts of interest.

For example, let's consider the importance of the digital scenario database shown on the outer level of safety measures. This measure refers to the set of specific scenarios, conditions, test vectors, test descriptions, environmental factors and other aspects that are used to test in a virtual environment for proper vehicle operation in its intended operating design domain. Ideally, this set of virtual tests would accurately encompass every scenario that an autonomous vehicle might encounter in real-world operation. However, this may be neither practical nor possible to comprehensively achieve in every aspect, so great care must be taken in selecting an appropriate but finite set of tests.

The benefits of scenario testing in a virtual environment include the ability to repeatably and precisely execute a large number of tests at comparatively low cost with respect to performing the equivalent physical tests. However, the mathematical models and algorithms used in the virtual environment may have certain limitations as well as gaps in scenario coverage that may obscure a complete understanding of the actual safety profile of the system when operated in the real world. Physical testing and virtual testing are complementary when applied appropriately to the verification and validation of autonomous vehicles.





Summary

The AV Safety Wheel framework summarizes many of the best practices in product safety and provides a context for where specific AV safety measures fit in a holistic safety approach. While the example is not intended to be a comprehensive list of all relevant standards, tools, tests and regulations, it can certainly be expanded as necessary to capture the specific measures of organizations and programs. A key benefit of mapping safety measures in this manner is to help identify any potential gaps in the safety plan of highly complex autonomous vehicle developments.

The necessity for a holistic view and approach to autonomous vehicle safety cannot be overemphasized. Many excellent standards, tools and methods for autonomous safety already exist, many more are in various stages of development, and even more will doubtless be developed in the future. However, no matter how excellent a particular approach for a particular aspect of safety is, it will still be insufficient to the extent that it does not comprehend the full breadth of necessary safety measures.

To learn more, visit UL.com/mobility.

Endnotes

1. "The Code of Hammurabi," The Avalon Project : Code of Hammurabi (yale.edu). Retrieved October 29, 2022
2. "The Long Struggle for the Law," The Long Struggle for the Law | FDA. Retrieved October 31, 2022
3. "A Half Century of Highway Safety Innovations–1966 to 2016," https://www.bts.gov/archive/publications/passenger_travel_2016/tables/half. Retrieved October 31, 2022
4. "Engineering Progress," https://www.ul.com/sites/g/files/qbfpbp251/files/2019-05/EngineeringProgress.pdf. Retrieved October 30, 2022
5. "History," https://www.ul.com/about/history. Retrieved October 30, 2022
6. Merrill, W. H., Jr., "Underwriters' Laboratories, Inc.," *The Spectator* (May 1, 1913), 17-23.
7. Henry Ford, "Today and tomorrow" (1926).
8. "Timeline of Federal Motor Vehicle Safety Standards," https://www.nhtsa.gov/staticfiles/communications/pdf/Lives-Saved-Tech-Timeline.pdf. Retrieved October 30, 2022
9. "Air bags," Vehicle Air Bags and Injury Prevention | NHTSA. Retrieved October 30, 2022

Authors

John Currie
Business development director at UL Solutions

Dr. Erich Meier
Director product management at UL Solutions

Bill Taylor
Managing director - consulting, mobility and critical systems at UL Solutions

UL.com/Solutions

CS426315-01.23