tu simple

Dec 9th, 2021

TuSimple's Safety Framework for The First Semi-Truck Driver-Out Pilot Program

At TuSimple, our mission is to deliver the safest, most-reliable, fuel-efficient, and low-cost autonomous freight capacity to market at scale. A major milestone towards achieving our mission is safely proving technical maturity and capability by demonstrating safe, fully autonomous, driver-out operations. TuSimple's Driver-Out Pilot is a safety and engineering development program designed to showcase driver-out operations for class 8 trucks on open roads. When completed, we believe this fully autonomous, Driver-Out Pilot will be an industry-first accomplishment. Achieving this milestone requires defining a world-class safety framework.

Unlike the traditional automotive industry, which has long-established standards to prove safety and road-worthiness of human-driven vehicles, the autonomous vehicle (AV) industry is at its beginning stages of development. This gives us the opportunity to be an integral and active part of creating wholly-sufficient standards. We believe it is our responsibility to develop and employ standards-based methodologies to guide AV-specific standardization and to communicate our overall safety solution.

Given the above context and the unprecedented complexity of autonomous driving technology, we choose to build on the current automotive industry regulations for safety by incorporating multiple substantive safety methodologies when designing our safety framework. This enables us to go beyond basic compliance with standards and quantitatively establish that we believe we have produced the safest autonomous trucks on the road.

At TuSimple, our approach to safety is holistic, spanning our organization, processes, technology and operations. This approach is designed to not only ensure reliability and safety, but also enable us to show the maturity of our technology and operations through our Driver-Out Pilot. This pilot is significant because it reinforces what we believe is our unique position at the forefront of autonomous driving technology and our track record of setting industry standards, similar to our introduction of the TuSimple Autonomous Freight Network (AFN) last year. To date, no one has taken a human driver entirely out of the cab of a semi-truck to deliver freight on open public roads. With the maturity of our technology and our robust safety framework, we intend to change that.

> "This enables us to go beyond basic compliance with standards and quantitatively establish that we believe we have produced the safest autonomous trucks on the road."

Our Driver-Out Pilot is a significant step forward on our road to full commercialization. We believe that this is an industry-first undertaking and that we are on a path to be the first to launch autonomous freight operations at scale to provide safe, low cost and reliable freight capacity.

TuSimple's Safety Framework for The First Semi-Truck Driver-Out Pilot Program

tu simple

> A critical capability of our product development process must be robust requirements discovery at speed.

TuSimple's Safety Culture & Governance

Safety starts with building a culture of safety that is reinforced throughout the entire organization. At TuSimple, our Organizational Structure & Safety Governance framework is responsible for our safety culture. Collectively they reinforce our clear accountability in development, operations and our safety policies, as well as our ability to transparently communicate safety processes and milestones, maintain the safety organization and continuously monitor and measure the safety performance metrics across the organization. Safety is embedded in our hiring and training on a day-to-day basis. Employees actively identify and address safety concerns, including via a confidential safety hotline. Additionally, our Safety Policy Steering Committee, which comprises a cross section of senior leadership, takes responsibility for safety oversight across the organization, including, in particular, the Driver-Out Pilot.

TuSimple's Safety Processes and Best Practices

At TuSimple, our safety framework covers aspects of both traditional safety case framework structure as well as augmentative elements, spanning across our internal processes and best practices, which help to ensure the successful implementation of our safety framework.

TuSimple's Use of the V Model & Agile: At TuSimple, we understand the need to balance the creation of innovative, industry-leading technologies with the need for safety of our products, employees and the broader community of road users. Vehicular autonomy entails (1) creating novel robotics technologies, (2) maturing those technologies to a readiness level suitable for safety-critical operations, and (3) integrating those technologies together to produce L4 autonomous trucks. Therefore, a critical capability of our product development process must be robust requirements discovery at speed. Consequently, we implement a hybrid of the V Model traditionally used in safety-critical industries and the Agile design maturation model more common in technology companies. Together these provide a multifaceted view of the safety needs of the product along with the accelerated mechanism needed to implement and validate them.

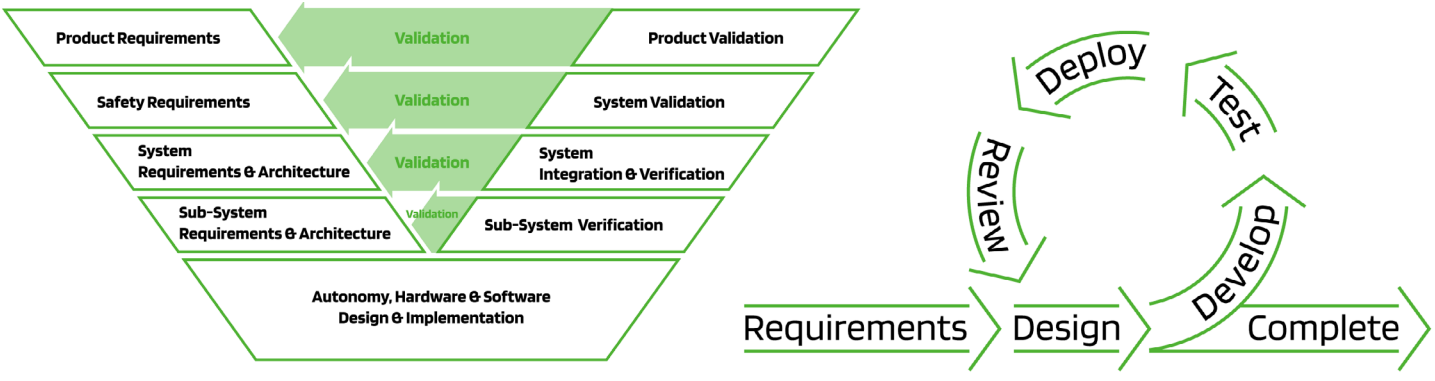
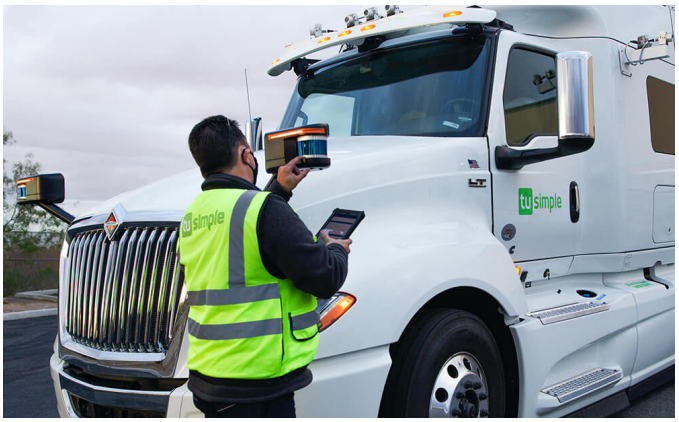


Figure 1: TuSimple leverages both the V Model and Agile for product development

TuSimple's Safety Framework for The First Semi-Truck Driver-Out Pilot Program

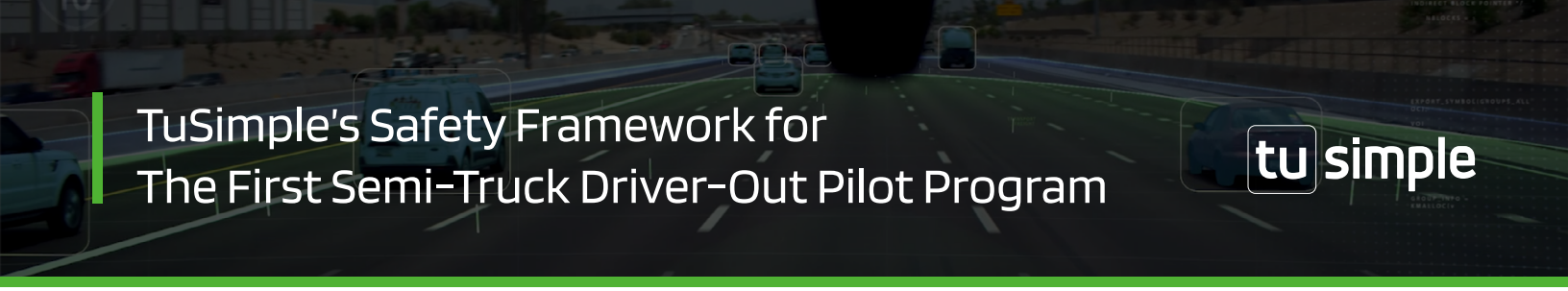
TuSimple's Truck Behavioral Safety Principles:
We define explicit behavioral safety principles that form a boundary around what our autonomous driving system shall never do while operating. Although we work to ensure the highest level of safety with our autonomous trucks, the fact of the matter is that human drivers make mistakes, creating situations where a collision with another human driver or an autonomous truck cannot be completely avoided. For that reason, we develop our system to attempt to do everything it can to reduce the level of potential injury and probability of fatality in potential accidents where human drivers are at fault.



> We have developed our own world-class safety engineering, design, and testing approach that leverages existing state-of-the-art, safety-related standards and guidelines.

TuSimple's Developed Safety Standards:
As a leading autonomous trucking technology company, we believe that a holistic safety framework should not fall short of leveraging the autonomous driving industry's use of automotive and technology standards, tools, methods and principles. At the same time, we are aware of the inadequacy of some of the standards and guidelines as well as the lack of federal and state policy covering the autonomous trucking application. For that reason, we have developed our own world-class safety engineering, design, and testing approach that leverages existing state-of-the-art, safety-related standards and guidelines.

Figure 2: TuSimple's Holistic Standards Approach to Autonomous Truck Safety



TuSimple's Safety Framework for The First Semi-Truck Driver-Out Pilot Program

TuSimple's Safety Case Framework

To support the safety for our Driver-Out Pilot, we have developed an extensive safety case framework which begins with two overarching safety principles:

[1] Is the Driver-Out Truck Safe to Operate Autonomously on the Designated Route?

Our System Safety function works to support the success of our first safety principle, that Driver-Out trucks are safe to operate autonomously on our Driver-Out route by helping each aspect of the system to be reliable, fail-safe, sufficient, and proven.

Reliable (Robust Design)	All hardware components (including sensors, computing, harnesses, and connectors) have been procured or built to relevant specifications with processes to stress-test them for the specific Driver-Out Operational Design Domain (ODD) application.
Fail-Safe (Functional Safety)	Hazard and risk analysis has been completed to identify safety-critical items for the Driver-Out pilot, including those in mechanical, electric, power, communications, and software subsystems. Fault trees have been developed with required mitigations with a process to verify through simulation, track, and road testing.
Sufficient (SOTIF)	Functional insufficiencies and misuse cases have been identified with a process for building mitigation using system theoretic process analysis.
Proven (Substantive Safety)	Our entire autonomous driving history has now been benchmarked to quantify our vehicle's safe performance throughout the entire Driver-Out ODD. In addition, our process of independent adversarial testing benchmarks performance against worst-case conditions that have not previously been encountered.

[2] Are the Driver-Out Operations Safe?

Our Operations Safety function works to support the success of our second safety principle, that Driver-Out operations are safe by helping each aspect of our operations to be prepared and proven.

Prepared (Training)	A process for hazard analyses has been established across all safety critical operations applicable to Driver-Out. Operational controls include surveys and chase vehicles, the Oversight system, police escort and driver training.
Proven (Stress Tested)	The Oversight system and remote monitoring have been successfully stress tested at the test track. Our testing also includes on-road dry runs of the entire Driver-Out pilot with the safety driver present in the vehicle cab.

Our safety culture and governance, use of best practices such as the V Model and Agile design model for product development, and the safety case framework for the Driver-Out Pilot, lay the framework for our safety philosophy and implementation. However, at TuSimple we see safety as a continuous journey rather than a single destination; safety is never truly complete. Thus, while our safety framework fully describes the safety approach we are taking with our Driver-Out Pilot, it represents just one significant step toward our eventual development of substantively safe autonomous freight operations at the global level. As we grow and scale our autonomous technology and operations, we plan to continue to communicate updates to our safety practices.

For more information, please access the full **TuSimple Driver-Out Pilot Safety Framework**.