# Our Approach to Automated Driving System Safety

February 2019

## Introduction

At Apple, by relentlessly pushing the boundaries of innovation and design, we believe that it is possible to dramatically improve the safety and well-being of our customers. Our interdisciplinary approach and position at the intersection of technology and liberal arts influences not just our focus on creating great user experiences for our customers, but also our desire to leave the world better than we found it.

Apple uses artificial intelligence and machine learning to make our products and services smarter, more intuitive, and more personalized. We are investing heavily in the study of machine learning and automation, and we are excited about the potential of automated systems in many areas, including transportation. In particular, we believe that automated driving systems (ADS) have the promise to greatly enhance the human experience in three key areas: improving road safety, increasing mobility, and realizing broader societal benefits.

We apply Apple's values to the safe and secure research, design, and development of ADS. We believe it is vital that all organizations developing and deploying ADS follow rigorous safety principles in design and production.

Apple has a safety review process that involves interdisciplinary safety and engineering experts from across the company. Prior to use on public roads, a comprehensive cross-functional safety review is conducted to ensure the safe, legal operation of test vehicles, including rigorous verification testing through simulation and on closed-course proving grounds.

All of our employees and other personnel involved with our ADS development, including but not limited to safety drivers and operators, are encouraged to immediately raise any safety concerns. All concerns are reviewed, escalated as necessary, and can inform modifications to the ADS, test vehicles, operational policies, and driver training. All escalations have the ability to ground the vehicle fleet and initiate a comprehensive safety review. In addition, there are daily meetings with all drivers and operators to review operational constraints, software updates, and any new information about test routes.

### Security and Privacy

Security is a core value at Apple. Apple conducts threat assessments and takes steps to mitigate known and anticipated risks. This security approach is applied throughout the development of our ADS to ensure safe operation on the road, to prevent data theft and tampering, and to protect privacy and intellectual property.

Our data collection practices are guided by Apple's belief that privacy is a fundamental human right. We protect sensitive data and limit data collection to only what is needed for the development of our ADS. More information about Apple's privacy policy can be found at https://www.apple.com/privacy/.

## How Our System Works

Our autonomy system consists of three main components operating in a cooperative continuous loop that repeats multiple times per second. These components are responsible for sensing the environment, planning the vehicle response, and executing the planned action.

### Sense

The sensing component is able to determine where the vehicle is located in the world and can identify and track surrounding objects, such as other vehicles, pedestrians, and bicyclists. This is accomplished using a combination of sensors, including LiDAR, radar, and cameras, and provides high-resolution 360-degree 3D coverage around the vehicle.

### Plan

The planning component is responsible for determining how the vehicle will navigate safely through the world. It uses the ADS's detailed map and accurate positioning technology, together with information from the sensing component, to predict where the vehicle and every surrounding object will be many seconds into the future. This information is used to determine the next action for the ADS to take.

### Act

The action component converts the planning component's location and trajectory information into commands for the vehicle's steering, braking, and propulsion systems.

In addition to the commands generated by the action component, our ADS includes supporting hardware and software systems that monitor the state of safety-critical systems and is capable of immediately transferring control of the test vehicle to the safety driver when needed.

## Crash Safety

Our test vehicles are based on a vehicle that is certified to the Federal Motor Vehicle Safety Standards and has top crashworthiness ratings in consumer crash tests. Any modification we make to the test vehicles is assessed to ensure that they maintain the crash safety of the base vehicle, in order to protect vehicle occupants and the general public in the event of a crash.

External equipment is securely mounted and designed to minimize risk to pedestrians and occupants of other vehicles and is validated using simulation and physical testing. Any modification made inside the occupant compartment is analyzed to ensure no interference with airbags and seatbelts, and secure mounting locations that protect against injuries in the event of a crash.

## System Safety Analysis

The ADS design and integration into the test vehicle is analyzed using various industry safety analysis methods and best practices. The analyses begin during the development process to identify potential hazards so that the design can be easily changed to prevent or reduce the identified hazards.

The hazard analysis is focused on the planned use case of the test vehicles (including driving maneuvers, objects, and events expected to be encountered on the road) and the fact that a safety driver will always be present. Hazards can include malfunctions that could lead to unintended vehicle motion, human-machine interface (HMI) hazards, and environmental hazards.

The cause of any malfunction that could result in potential hazards is assessed at the vehicle, system, subsystem, and component level as appropriate. Design changes to address the cause of malfunctions are identified and evaluated for effectiveness before they are incorporated into the design. Changes include techniques such as design improvements to eliminate a malfunction, diagnostics to detect a potential malfunction, and limits to steering and acceleration actions. The ADS HMI is designed and tested to ensure that it is effective in warning the safety driver and operator when vehicle control should be taken back to mitigate a hazard.

Any malfunctions and scenarios that require the safety driver to take control of the vehicle to address a hazard are further studied to confirm that the safety driver could regain manual control of the vehicle safely. This includes simulations and vehicle testing with induced faults at proving grounds.

## System Verification

System verification is a critical part of our hardware and software development and release process. Verification that functional requirements are met begins at the component level with hardware and software modules. Further verification is completed as functionality increases and expands with other components and software at the subsystem, system, and ultimately the fully integrated vehicle level through a series of tests and simulation.

The verification testing process begins as soon as a new ADS capability is identified. Verification tests are designed to exercise the hardware and software in environments that mimic the operating environment and inputs that would be expected at each level of integration. In parallel to this test development, an independent verification team creates a rigorous test plan for execution in simulation, test benches, and testing at closed-course proving grounds.

Test scenarios are crafted using data gathered on public roads to represent the real world, and in the case of simulation, involve situations of increasing complexity with additional road users (vehicles, pedestrians, bicyclists, etc.), objects, and obstacles such as construction zones.

In addition to modeled behavior, our simulations include data gathered from public road testing, enabling us to replay events and assess how they would be impacted using new or updated software.

All proposed changes to our ADS software are first subjected to rigorous and comprehensive simulation testing that evaluates the software against predetermined criteria. After passing these simulation tests, the entire system then undergoes on-road testing at closed-course proving grounds. Software changes may be nominated for operation on public roads only after passing this array of extensive simulations and closed-course proving ground tests.

Software that passes to public road testing is incrementally deployed across the test vehicle fleet, with each stage monitored and analyzed. Additionally, changes deemed safety-critical undergo an extra phase of testing conducted by our most experienced drivers and operators.

## Operational Safety

We continuously evaluate the behavior of our ADS to ensure that it operates in a safe, responsible, and well-understood manner. The data we collect from safety evaluations, disengagements, simulations, and testing on proving grounds are used to demonstrate our system's capabilities and are a key component for informing our operational policies and training of safety drivers and operators. Any changes to the system that alter those policies go through a rigorous verification and review process that includes both our engineering and operations teams.

### Daily Checks

To ensure that vehicles are operating safely on public roads, we perform safety and functionality checks before and after each outing. These include manual vehicle inspections such as checking tire pressures and ensuring that sensors are clean, and automatic diagnostic tests to confirm that the correct ADS software is installed.

In addition, there are daily meetings with the safety drivers and operators to review operational constraints, software updates, and any new information about test routes.

### Safety Drivers and Operators

We currently require a safety driver and an operator to be in the front seats of the vehicle when it is in automated mode. The safety driver scans the roadway for potential conflicts between the vehicle and objects in the roadway, and takes control of the vehicle upon a disengagement or operational constraint, at the driver's discretion or at the direction of the operator.

The safety driver can assume control of the vehicle at any time by using any of the following: steering wheel, brakes, throttle, or gearshift lever, or by activating an emergency override button located on the center console. Safety drivers are currently required to keep both hands on the steering wheel when the ADS is activated, so that they can quickly respond to any event which might occur.

The operator's role is to monitor the system and inform the safety driver of the objects the system has detected and what the vehicle will do next. The operator also monitors the roadway during specific maneuvers and helps to ensure that the safety driver remains alert. Additionally, the operator can disengage the ADS at any time using a software interface.

Our safety drivers and operators work only one shift per day and are required to take frequent rest breaks while driving as needed to stay alert. Safety drivers are also free to request assignment to nondriving activities at any time. Drivers are allowed to use mobile devices only when the vehicle is parked at a safe location.

### Requirements and Training

We hire proficient and experienced safety drivers and operators who have a clear driving record with no serious accidents, DUI convictions, or any license suspensions or revocations within the last 10 years. They also must pass a drug screening and a background check before the training program starts. Each of our safety drivers and operators completes a training program that includes:

- Defensive driving on closed-course proving grounds, where a range of vehicle handling and emergency maneuvers are taught.
- Vehicle-specific training consisting of classroom instruction, simulation, and testing on closed-course proving grounds. Instruction includes emergency

braking and emergency maneuvers performed in a vehicle that accurately represents the driving dynamics of our test vehicles.

- Operational training for the ADS, including correct hand and foot placement, disengagement methods, and the use of the vehicle's human-machine interface.
- Supervised public road driving, followed by a video review and evaluation of the drive to identify areas for improvement. Supervised drives are conducted until the safety drivers demonstrate that they meet all of the required performance criteria.

Safety drivers and operators receive ongoing feedback on their performance and safety-critical responsibilities. Additionally, safety drivers are anonymously surveyed to assess mental and physical workload involved in operating the ADS, and to identify any concerns that they may have.

### Human-Machine Interface (HMI)

To ensure that drivers and operators can quickly identify a system malfunction and take control of the vehicle, the following measures are in place:

- A persistent visual display of the system's mode (for example, "ADS active") is visible to both the safety driver and the operator.
- A visual and audible signal indicates when the system needs to return control to the safety driver. Understanding this communication is a significant part of safety driver and operator training, and the signaling equipment is verified to ensure proper operation and fault tolerance.
- There are multiple, redundant, and fault-tolerant mechanisms for taking control of the vehicle.
- The steering, braking, and acceleration commands issued by the ADS have set limits to ensure that its actions can be anticipated and interrupted by the safety driver. For example, lane changes are performed in such a way that the safety driver can take control of the vehicle before it leaves its current lane.

### Incident Response

In the event of an incident, testing is paused until data logged by the ADS is reviewed and an internal investigation is completed. Testing is resumed if it is determined that the ADS or safety driver acted appropriately during the incident.

If the investigation determines that the ADS or safety driver behavior contributed to the incident, testing is resumed once all corrective actions are verified and implemented. This may include updates to the ADS, driver training, or operational policy changes.

## Ongoing Engagement

At Apple we appreciate the importance of proactive and candid engagement with federal, state, and local government agencies that play a critical role in advancing the development and deployment of ADS. We recognize the value and need to be transparent with government officials about our ADS testing on public roads, and we vigilantly adhere to relevant regulations and requirements.

We also stand ready to be a resource on current and future technological, regulatory, and public policy matters. To this end, we have established constructive working relationships and look forward to continued partnership with federal, state, and local government agencies and stakeholder groups.