# A principled approach to safety

# Table of Contents


1.0
Letter to the Reader p.3

2.0
Executive Summary p.5

3.0
Uber ATG Safety Approach Overview p.7

4.0
New Enhancements to our Safety Approach p.11

5.0
Development According to Uber ATG's Safety Approach p.17

5.1
Proficient p.18

5.2
Fail-Safe p.50

5.3
Continuously Improving p.55

5.4
Resilient p.64

5.5
Trustworthy p.77

# 1.0 → Letter to the Reader

**Dear Reader,**

The inaugural release of our Safety Report in 2018 was a key milestone for Uber Advanced Technologies Group (ATG), and representative of transparency and openness to our stakeholders — future riders, policymakers, regulators, other self-driving technology developers, and those with whom we share the road — and an opportunity to represent the progress and future vision of self-driving safety at Uber ATG. We also noted in the 2018 Safety Report that we would update these various stakeholders about key developments in our program's approach to safety.

In this 2020 Safety Report, we therefore continue our commitment to transparent communication on self-driving safety by providing an update on the current state of our technology, our way of work, our organization, and the road we envision ahead. Since the release of our 2018 Safety Report, we have:

- **Built on our principled approach to safety.** → This second edition of our Safety Report incorporates a number of important enhancements. We are particularly proud of the work that we have undertaken to make our approach to technology development transparent — open-sourcing our Safety Case Framework, establishing and launching our Self-Driving Safety and Responsibility Advisory Board, publishing our first Public Safety Officials and First Responders' Guide, and beginning to implement a Safety Management System (which we call our Organizational Approach to Safety Management in this document).
- **Continued to take a measured, phased approach to testing on public roads.** → We are now testing our self-driving system on public roads and engaged in efforts to expand our operational footprint. Each step of the way, we worked closely with city, state, and federal officials, sought to engage communities on these steps, and messaged clearly and openly about our testing activities.
- **Encouraged and contributed to industry efforts to enhance safety approaches and define safety standards for self-driving systems.** → We released and open-sourced the first edition of our Safety Case Framework in the hope that other developers might provide feedback, identify opportunities for improvement, and/or use parts of the Safety Case Framework to inform their own safety approaches. We joined and contributed to a number of industry groups working to develop standards for self-driving vehicle safety, including UL 4600, the Automated Vehicles Safety Consortium convened by SAE International, and others.

While this VSSA update reflects important progress, many aspects of our approach to this technology remain consistent with what we described in our 2018 Safety Report. All of the following remain key animating principles for our efforts:

- The transition toward this technology will take time. We continue to appreciate that the technology roadmap should necessarily take its time to incorporate the right product and safety requirements.
- We can all benefit from this technology sooner by envisioning an eventual deployment through shared, professionally-managed fleets. And, in particular, we envision that the deployment of self-driving technology should proceed incrementally and side-by-side with conventional vehicles, and we look forward to leveraging the depth and breadth of the Uber network in service of these goals. We continue to bring these perspectives to both our business strategy development and public engagement.
- This transition is not achievable without testing on public roads, and that testing on public roads can only be done with visibility of our safety protections and plans and confidence in our ability to deliver on them.
- Open, regular communication with the public and with other stakeholders is absolutely essential — not only to earn trust, but to ensure that the technology and the platform we are building will serve the public's needs and high expectations.

These premises are central to how we operate today, and we continue to strive to live by them and up to them. This report furthers our commitment to continuously improve, with detailed attention to the extraordinary safety potential of this still nascent technology, and our commitment to share our progress and our learnings as we go. The team at Uber ATG understands our responsibility and are working every day to make this safer future a reality.

Sincerely,
Eric Meyhofer

# 2.0 → Executive Summary

As our own self-driving technology makes great strides toward deployment and commercialization, Uber Advanced Technologies Group (Uber ATG) continues to evolve and strengthen our approach to safety. As demonstrated by our first Safety Report (which is similar to NHTSA's Voluntary Safety Self-Assessment (VSSA)), **A Principled Approach to Safety**, and this 2020 report, we are committed to continuing a public safety dialogue through transparency and open communication. This Safety Report discusses Uber ATG's current approach to the safe development and operation of self-driving vehicle technology and the opportunities we see for possible improvement in the future.

This report is intended to speak to a number of audiences, including: future users of self-driving technology interested in how our developmental technology works today; those interested in how Uber ATG is working to promote safety in its development; policymakers, including legislators, regulators, and local officials, who may be interested in understanding our organization or the current state of the technology; and other developers who may be interested in identifying opportunities to collaborate.

In **Section 3: Uber ATG Safety Approach Overview,** we discuss Uber ATG's five Safety Principles as the foundation for our approach to self-driving safety — spanning the vehicle level through enterprise level. We discuss how the Safety Principles address regulatory guidance for self-driving technology developers and how they inform the way we work.

**Section 4: New Enhancements to our Safety Approach** highlights significant improvements to Uber ATG's safety approach. It introduces the Uber ATG Safety Case Framework as our standardized, open-source framework for achieving acceptable levels of safety for self-driving operations on public roads. The Safety Case Framework incorporates the diverse considerations for safe self-driving technology within a single framework that is broad enough to serve the self-driving enterprise and deep enough to take a self-driving vehicle through its system lifecycle. It also clarifies the importance of tailoring the Safety Case Framework to create individual safety cases that address specific needs to help ensure acceptable safety of each specific system and its uses. Finally, this section discusses Uber ATG's Organizational Approach to Safety Management and our implementation of a Safety Management System (SMS).

**Section 5: Development According to Uber ATG's Safety Approach** takes a deeper focus on each of the five Safety Principles: Proficient; Fail-Safe; Continuously Improving; Resilient; and Trustworthy. An in-depth discussion of each Safety Principle decomposes considerations supporting each top-level safety goal. This includes the policies, processes, and philosophies that define the way Uber ATG currently performs its work and builds confidence in the safety of its systems and operations. Details of our current technology, along with areas for possible future improvements, are provided throughout the section.

3.0

# Uber ATG Safety Approach Overview

This report begins with a brief introduction of Uber ATG's approach to safety as governed by our Safety Principles and creates context for two essential components thereof: our Safety Case Framework for self-driving and our Organizational Approach to Safety Management.

01

# Uber ATG Self-Driving Safety Principles

This section provides a top-level view of Uber ATG's Self-Driving Safety Principles, with latter sections detailing how our work embodies them. These top-level principles, unaltered since their introduction in our first safety report, represent our view on the set of necessary high-level criteria governing our safety-conscious development and deployment of self-driving technology. Fulfilling these principles requires both rigorous system development and organizational processes. We believe that for a self-driving vehicle to be acceptably safe to operate, it must be shown to be: **Proficient, Fail-Safe, Continuously Improving, Resilient, and Trustworthy**.

- **Proficient** → In the absence of system faults, how do we demonstrate that our system is acceptably safe during nominal operations?
- **Fail-Safe** → How do we ensure that the system is acceptably safe in the presence of faults and failures? How will the system mitigate harm in the event of a fault or failure?
- **Continuously Improving** → How do our developmental and operational processes identify, evaluate, and resolve anomalies that can potentially affect the safety of the self-driving vehicle? How can we actively cultivate a strong culture of safety, where the organization is engaged and empowered and holds all employees at all levels accountable for their active participation?
- **Resilient** → How do we ensure the self-driving vehicle is acceptably safe in case of reasonably foreseeable misuse or unavoidable events?
- **Trustworthy** → How do we earn and keep the trust of our riders, regulators, legislators, public safety officials, other road users, and advocacy organizations and provide them evidence of the safety measures of our self-driving enterprise?

# NHTSA Safety Elements / ATG Safety Principles Crosswalk

| ✓ = Primary Coverage<br>✓ = Supporting Coverage | Principle 01<br>**Proficient** | Principle 02<br>**Fail-Safe** | Principle 03<br>**Continuously Improving** | Principle 04<br>**Resilient** | Principle 05<br>**Trustworthy** | Is given NHTSA VSSA safety element addressed? |
|---|---|---|---|---|---|---|
| System Safety | ✓ | | ✓ | | | ✓ |
| Operational Design Domain | ✓ | ✓ | | | | ✓ |
| Object & Event Detection & Response | ✓ | | ✓ | | | ✓ |
| Fallback (Min Risk Condition) | | ✓ | | | | ✓ |
| Validation Methods | ✓ | | | | | ✓ |
| Human Machine Interface | ✓ | ✓ | ✓ | | | ✓ |
| Vehicle Cybersecurity | | | | ✓ | | ✓ |
| Crash-worthiness | | | | ✓ | | ✓ |
| Post-Crash ADS Behavior | | | ✓ | ✓ | | ✓ |
| Data Recording | | | | ✓ | | ✓ |
| Consumer Education & Training | | | ✓ | | ✓ | ✓ |
| Federal, State, & Local Laws | ✓ | | | | ✓ | ✓ |

These self-driving Safety Principles ground our holistic approach to safety during development efforts and ensure that safety is ingrained throughout the process, from initial concept through vehicle decommissioning. Guidance from the U.S. DOT and its National Highway Traffic Safety Administration (NHTSA) identifies 12 safety elements, or core areas of consideration with respect to safety and self-driving.[01, 02, 03] Related guidance from Transport Canada (TC) recognizes 13 expected outcomes as they relate to automated driving system (ADS) capabilities, design, and validation, user-centered safety, and cybersecurity and data management.[04] Our Safety Principles encompass all of these safety elements; each element is represented within at least one, if not each, principle.

These principles help focus our development and operational efforts, with the approach to fulfilling each principle evolving over time. So we will always endeavor to develop a system that meets our goals for Proficiency, Trustworthiness, and so on — even as the specific approach to each principle may change to reflect the particular developmental stage and use case involved.

We also expect that formal and informal best practices and standards will continue to emerge over time, and that these will necessarily flow into our approach to developing safe self-driving technology. Such standards governing self-driving vehicle safety will be incorporated and represented in our safety case. We are actively working with stakeholders throughout industry, government, and the broader community to contribute to the development of those standards and best practices.

These Safety Principles drive and guide development of safe self-driving technology, which we assess in Section 05. From these Safety Principles, we built the ATG Safety Case Framework and the ATG Organizational Approach to Safety Management.

The Safety Case Framework architects a structured argument through which one may, in our view, demonstrate and assess various safety aspects of the self-driving enterprise, including the development and deployment of self-driving vehicles. The Safety Case Framework incorporates the same five Safety Principles introduced above, and expands upon them to include significantly greater detail on safety areas we believe are appropriate for self-driving.

A critical part of Uber ATG's approach to safety is the inclusion of ATG's Organizational Approach to Safety Management in our Safety Case Framework. This approach is a formal and systematic framework for managing safety and facilitating organizational risk-based decision making, while providing the proper structure, safety authority and responsibilities at appropriate levels throughout the organization. It also includes an active Safety Assurance and Oversight program to continually monitor the effectiveness and change within safety controls and identify areas for process improvement in critical development, testing, and operational areas of the organization.

01. NHTSA, 2017, 'Automated Driving Systems 2.0: A Vision for Safety.'
02. USDOT, 2018, 'Preparing for the Future of Transportation: Automated Vehicles 3.0.'
03. USDOT, 2020, 'Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0'
04. Transport Canada, 2019, 'Safety report for Automated Driving Systems in Canada.'

4.0

# New Enhancements to our Safety Approach

# 01 ATG Safety Case Framework

At Uber ATG, our five Safety Principles — **Proficient, Fail-Safe, Continuously Improving, Resilient, and Trustworthy** — guide the way we do our work. In 2019, we published the codification of these principles and our safety approach in Uber ATG's Safety Case Framework — our framework for the responsible development and deployment of self-driving vehicles within a self-driving enterprise. This milestone represented the culmination of an extensive internal effort to develop a standardized approach to safety case development for self-driving technology.

The safety case is a mechanism found in other industries for communicating complex safety concepts. The concept of a Safety Case was first introduced in the early 90's following the Piper Alpha tragedy in the Oil and Gas industry.[05] Over the years since, Safety Case approaches have been used in applications for military, aerospace, rail, food & drug, and nuclear industries.

The scope of our Safety Case Framework applies to both the development and full-scale operations of our self-driving vehicles. We believe this framework could be tailored to any organization's self-driving vehicle programs — especially when operated as part of a transportation service. This means that we, or any self-driving enterprise developer, would populate the Safety Case Framework with different evidence depending on the specifics of the system and the intended uses (i.e., potentially different evidence for a system utilizing safety drivers versus not; a system involving passengers versus one without; etc.). The Uber ATG Safety Case Framework incorporates guidance from government organizations, best practices from safety-critical industries, voluntary industry standards and consortia, and academic research with the learnings of our own work. Uber ATG also engaged with multiple independent external subject matter experts during the development of the Safety Case Framework. These experts peer reviewed the concept and argument structure, and their input informed the July 2019 published version of the Safety Case Framework.

05. Cullen, 1990, 'The Public Inquiry into the Piper Alpha Disaster.'

We released our Safety Case Framework to the public domain under Creative Commons Zero for the purpose of aiding the broader industry's need for examples of self-driving vehicle safety case development. Through openness and transparency, the best ideas will emerge and contribute to efforts by the public and government agencies to appreciate issues implicated by self-driving enterprises. A Safety Case Framework is evolutionary. Refinements of the Safety Case Framework will be made over time in response to advancements in the state of the art. As such, our future safety reports will also exhibit this evolution in our technology, development, operations, and policies — which, among other elements, speaks to NHTSA's focus on Consumer Education and Training and our approach to incorporating State and Local laws.

Following on the evolutionary concept, Uber ATG applied learnings from its development, industry, and experiences — including our participation in the Underwriters Laboratory industry effort to create a standard for a safety argument (UL4600) — to create an updated version of our Safety Case Framework. As with version one, this version of the Safety Case Framework included evaluation by a different independent third-party expert of the evidence and arguments to identify opportunities to revise and update specific facets of the Safety Case Framework, including a detailed review of Uber ATG's Safety Case Framework against UL4600 with the goal of producing a new, refined version of our framework. Our Safety Case Framework continues to include content and claims that exceed the current industry standard, for example, where we address the role of the Mission Specialist. An updated Safety Case Framework was published in July 2020.[06]

Due to the complexity of a self-driving vehicle and the myriad of interactions and dependencies within the system and the operating environment, adequately explaining the basis for a conclusion on safety is complex. At the same time, clarity in communicating a safety argument is essential to safety itself, in no small part because of the important role that public understanding plays in community safety. A successful safety case communicates to stakeholders that the risk of harm from a system has been reduced to an acceptable level.[07]

While Uber ATG's Safety Case Framework was written to address fully driverless operations, Uber ATG intends to tailor the framework to achieve interim milestones and projects that lie ahead on the path to self-driving vehicles. By aligning workflows to satisfy the safety case at every stage of development, Uber ATG is well positioned to utilize available resources and gauge progress towards safe self-driving transportation.

06. Uber Advanced Technologies Group, 2020, 'Safety Case Framework.'

07. Kelly, 2004, 'A Systematic Approach to Safety Case Management.'

02

# Creating a Safety Case

The Safety Case Framework provides a generalized approach presenting a structured argument addressing safety issues implicated by self-driving technology across various potential developmental stages and use cases. Any individual developmental stage and/or use case would (under this approach) necessitate a tailored safety case derived from these top-level Safety Case Framework principles and specifically applied to a vehicle system, its Operational Design Domain (ODD), and its intended functional use.

In order to tailor the Safety Case Framework to a safety case for a specific program, we draw on Uber ATG's experience and the expertise of its internal subject matter experts in maturing its own self-driving vehicles, as well as the experience of external safety engineering experts across the autonomous vehicle industry, and our shared experience developing industry voluntary standards and best practices. We include all goals, arguments, and required evidence for all applicable portions of the Safety Case Framework to support the proposition that a self-driving car is acceptably safe for use in the real world. We then work collaboratively with the respective functional departments of the company to identify and capture the required evidence to substantiate each claim.

Since a fully developed safety case would require several thousand pieces of evidence, Uber ATG continues to invest in tooling to support the curation and tracking of safety case evidence. With robust tooling and safety culture, Uber ATG will be able to track and achieve multiple safety cases for multiple internal projects and milestones in tandem.

03

# An Organizational Approach to Safety Management

Uber ATG is committed to a formal and systematic business-like approach to managing safety. A robust Organizational Approach to Safety Management, generally based on the ICAO Safety Management principles and generally referred to as Safety Management System (SMS),[08] works to build and reinforce a culture of safety, which in turn helps to continuously improve an organization's safety performance by proactively managing safety risk while providing safety assurance oversight of its many programs and processes. This approach requires planning, organization, communication strategies, key metrics, and direction of the entire organization.

By focusing on four key components — a detailed Safety Risk Management structure, a robust Safety Assurance program, disciplined documentation of its Safety Policy, and Safety Promotions and Education — ATG's organizational safety management approach influences our engineering decisions and promotes a positive Safety Culture supported by an organization's leadership, core values, and employee engagement. Each component plays an important role in cultivating a strong and effective organization-wide safety program and is necessary to enable a high functioning organization.

The self-driving vehicle industry lends itself to benefitting from this organizational approach to safety in a number of ways. The nascent, rapidly evolving technology and varying Operational Design Domains (ODDs) characterized by differences in density and behavior between cities (among other factors) add particular complexity to the development and operation of self-driving technology. The measured and structured approach of a Safety Risk Management framework coupled with the clear accountability and responsibility for safety through a strong Safety Policy provides a clear platform and methodologies to make informed and risk-based organizational decisions. Similarly, lacking historical safety performance data like longer-lived industries, and in light of emergent industry standards, the self-driving enterprise can greatly benefit from building a robust and comprehensive Safety Assurance program to ensure proper safety oversight through regular and ongoing monitoring and evaluation of safety performance.

08. International Civil Aviation Organization, 2009, 'Safety Management Manual (SMM).'

Over the past 2 years, Uber ATG has architected and enhanced many components within the Organizational Safety Management structure, beginning with a foundation of a clearly defined and documented Safety Policy to include specific accountability and commitment to safety throughout the organization. Uber ATG has stood up a Safety Review Board chaired by the CEO — who has been designated as the Accountable Executive for safety, which is the highest level of safety risk decision making and safety risk socialization in the organization. Uber ATG has defined an Open and Just Culture with various voluntary and confidential tools for reporting safety concerns and issues without fear of reprisal. Borrowing from aviation as well as James Reason's safety risk methodology, Uber ATG has defined a Safety Risk Management process that captures organizational change, analyzes the risk associated with that change, and presents the risk to organizational leadership to determine if it is within the organization's safety risk appetite.[09, 10] Further, using Uber ATG's Safety Case Framework, we have developed a safety assurance and oversight program that will be effective at identifying reactive and as well as proactive safety risk and the effectiveness of existing safety risk controls. Finally, Uber ATG has built a robust Safety Promotions and Education program that is continually communicating to and educating the organization.

We believe that tailoring and systematically applying these four key components of Uber ATG's organizational safety approach are critical for the acceptably safe and responsible development and eventual full-scale operation of self-driving vehicles, and we have worked diligently to stand up the components in our organization in the time since we released our first safety report.

09. J. Reason, 1997, 'Managing the Risks of Organizational Accidents.'
10. J. Reason et. al., European Organisation for the Safety of Air Navigation, 2006, 'Revisiting the Swiss Cheese Model of Accidents.'

5.0

# Development According to Uber ATG's Safety Approach

This section explores Uber ATG's Self-Driving Safety Principles as applied to development and deployment of our technology. We have designed the discussion of these principles to align with the detail of the Safety Case Framework discussed throughout this report.

# 5.1 → Principle 01 Proficient

The Self-Driving Vehicle is acceptably safe during nominal operation.

# 01 Supporting Concepts

→ **Nominal operation** is performance in the absence of system faults, i.e., when the vehicle's systems are working as intended and operations are managed appropriately. Nominal operation includes all typical and atypical driving scenarios the self-driving vehicle might encounter in the defined ODD. We address what happens in the case of a detected fault in the discussion of **Principle 2: Fail-Safe**.

→ We anticipate that demonstrating an acceptable level of safety during nominal operation will require quantifying safe driving with tractable, credible methods and metrics. At Uber ATG, we reference standards, including laws, regulations, and industry best practices, to establish the requirements by which we engineer our systems. Those requirements decompose relevant standards and best practices to specific system-, subsystem-, and component-level engineering requirements, which can then be traced back to an origin in a standard. We evaluate how our system performs over an aggregation of tests comprising both common and rare scenarios representative of the system's intended use, including measures such as traffic rule infractions and vehicle dynamics attributes.[11] For example, we evaluate our system's ability to command vehicle braking sufficient to maintain a safe following distance from another vehicle that abruptly enters its path of travel, and we endeavor to quantify and achieve a "safety envelope" to dynamically assess the maintenance of a safe distance for other roadway actors. Further, we must track performance over time to ensure we are continuously improving (Principle 3). In crafting our approach to this principle, we additionally look to industry best practices in systems engineering methods,[12] coding and tool qualification standards,[13] configuration management approaches,[14, 15] and safety culture models.[16] We also employ a variety of methods including component reliability & performance testing, simulation, hardware-in-the-loop testing, track testing, and on-road testing to gauge overall system performance.

11. RAND Corporation, 2018, 'Measuring Automated Vehicle Safety: Forging a Framework.'
12. Voirin, 2017, 'Model-based System and Architecture Engineering with the Arcadia Method.'
13. RTCA, 2011, 'DO-330 Software Tool Qualification Considerations.'
14. SAE International, 2011, 'EIA 649B Configuration Management Standard.'
15. Institute of Electrical and Electronics Engineers (IEEE), 2012, 'IEEE 828 Standard for Configuration Management in Systems and Software Engineering.'
16. National Aeronautics and Space Administration (NASA), 2015, 'NASA-HDBK-8709.24 NASA Safety Culture Handbook.'

02

# Federal, State, and Local Laws

## Federal Motor Vehicle Safety Act and Federal Motor Vehicle Safety Standards

Uber ATG's current testing and development efforts utilize vehicles that Uber ATG purchases from an Original Equipment Manufacturer (such as Volvo) and then subsequently modifies. Prior to Uber ATG's receipt of these vehicles, the manufacturer has certified its base vehicles as meeting all applicable Federal Motor Vehicle Safety Standards (FMVSS). Additionally, we assess the effect of modifications by Uber ATG to ensure continued compliance with the Motor Vehicle Safety Act.

We recognize that the U.S. Department of Transportation continues to consider the potential value of new regulations specifically focused on self-driving vehicles. This includes, but is not limited to, new FMVSS and/or changes to existing FMVSS that may be promulgated to address unique features of self-driving vehicle design and capability, or to allow for test features specific to self-driving vehicles (such as NHTSA's Notice of Proposed Rulemaking to modernize occupant protection safety standards for vehicles without manual controls).[17] We welcome such further possible developments and plan to engage collaboratively with the U.S. DOT and NHTSA as it seeks to prioritize, develop, and implement these standards.

Uber ATG is one of nine companies and eight States that have signed on as the first participants in a new initiative led by the U.S. DOT to improve the safety and testing transparency of automated driving systems called the Automated Vehicle Transparency and Engagement for Safe Testing (AV TEST) Initiative. This voluntary initiative will include a series of public events across the country as well as an online, public-facing platform aimed at improving transparency and safety in the development and testing of automated driving systems and sharing information with the public.[18]

17. NHTSA, 2020, NHTSA-2020-0014-0001 'Notice of Proposed Rulemaking: Occupant Protection for Automated Driving Systems.'

18. NHTSA, 'U.S. Transportation Secretary Elaine L. Chao Announces First Participants in New Automated Vehicle Initiative to Improve Safety, Testing, and Public Engagement.'

## State and Local Laws

Rules of the road are frequently set by state, tribal, and local governments (depending on the jurisdiction). Safe deployment of self-driving vehicles requires attention to these rules to enable successful integration of self-driving vehicles with the broader set of actors in the transportation environment.

When developing autonomy capabilities, we assess the relevant traffic laws and norms for a given ODD to ensure that those rules are integrated into the self-driving system. As with other limitations on the behavior of the self-driving system, we enact formal limits within the self-driving system software to reflect these rules. For example, we build certain state and local road rules into our high-definition maps and program the ADS to follow these and other applicable rules.

03

# Developing a Nominally Safe System

A robust systems engineering approach to ODD selection and characterization along with Object and Event Detection and Response (OEDR) serves as a crucial foundation to realizing our first Safety Principle. By limiting our self-driving vehicles to a specific ODD, we can more effectively manage safety risk. Not unlike the systems engineering processes of developing an operational concept and system requirements, defining a target ODD facilitates the generation of relevant requirements and development processes for our self-driving vehicles. We restrict operations to the intended ODD to maintain efficacy of our system safety features during use. It is through the combination of these approaches, evaluated by our rigorous verification and validation methods, that we can progress towards acceptably safe operation in a given ODD.

## Operational Design Domain

Before beginning any self-driving testing on public roads, we establish the ODD. The ODD describes the specific conditions under which the self-driving system is intended to function, including where and when the system is designed to operate. This parameterization is not only designed to address the performance of the base vehicle platform, but also system level capabilities, environmental scenarios, and appropriate self-driving system responses. We employ a three-pronged process to address the ODD: identify, characterize, and constrain.

## Identifying the ODD

We begin by identifying specific geographies where we would like to ultimately deploy self-driving vehicles on the Uber network by taking into consideration a number of factors, including the regulatory environment and areas where we can extend our network's reach to better serve riders. Using data from sources such as Uber's existing lines of business, Uber ATG's internal domain characterization process, and information layers of our high-definition maps, we derive features characterizing the geography of interest. These features define the intended production ODD and inform the set of autonomy capabilities required for autonomous operation.

This intended production ODD is converted into a technology roadmap, which describes the incremental expansion of our ODD to reflect new capabilities and the maturation of existing capabilities.

## Characterizing the ODD

The ODD characterization process includes:

- **Leveraging externally-sourced data —** such as already-extant maps and city data from Uber's core rideshare business.
- **Driving the area manually —** to collect detailed data and logs on the scenarios and actors that exist within the ODD.
- **Adding data tags —** to camera and LIDAR data collected from manually-driven logs, highlighting potentially relevant attributes of actors in and around the road as well as attributes of road design (e.g., road geometry or curvature, traffic control measures).
- **Synthesizing the tagged data —** to identify and break down information on all observed scenarios and subsequent system behavior requirements for each scenario.
- **Creating representative simulation and track tests —** to evaluate current and future software releases and perform tests at the subsystem and integrated system level.

This process enables us to:

- Confirm requirements for self-driving system capabilities;
- Identify sufficient test coverage both through simulation and track testing to assess performance of the self-driving system before testing on public roads;
- Analyze and assess particular safety risks that may be associated with the specific ODD;
- Provide clear operational guidelines and performance requirements to support on-road operations, e.g., policies governing system takeovers and handling scenarios not captured in the pre-approved and established ODD.

Once we have characterized an ODD, the self-driving system must pass the identified set of offline tests and track tests before operating on public roads. The process of offline and track testing serves to validate and update any relevant Safety Risk reports throughout the entire process, ensuring safety risk is understood by the organization.

## Constraining the ODD

The ODD can be constrained by multiple methods. One method, specific to the geographical aspect of the ODD, is to prevent our self-driving system from operating outside of the intended ODD, which involves various software constraints that restrict vehicle routing outside approved areas or road networks. So, for example, our self-driving system is prevented from driving in geographical areas outside of the ODD via geofencing techniques that impose a system prohibition on driving across the geofence. These constraints can also restrict routing of the self-driving vehicle at the lane level based on a set of configurable ODD elements, e.g., road speed, road type, and traffic control devices. Additionally, a software feature of the self-driving system prevents Mission Specialists from engaging self-driving capability if outside the approved ODD geography.

Another constraint method is operational. Our Mission Specialists help to enforce ODD constraints by monitoring road conditions while operating in the field. Mission Specialists are trained on the governing ODD, and are prepared to take manual control of the vehicle when presented with a scenario or conditions not included in the relevant ODD. When one of our vehicles encounters a situation that the Mission Specialists know is not in scope for a current self-driving vehicle during self-driving operations (e.g., a failed traffic control device), the left-seat Mission Specialist, or Pilot, is trained to take manual control of the vehicle and the right-seat Mission Specialist, the Co-Pilot, is trained to report the condition by entering a time and geo-stamped comment which is then recorded to the self-driving vehicle's logging system. This information then initiates a process by which a live operational constraint or crew notification may be created and distributed to the fleet with an appropriate solution, such as precluding certain future encounters with the location.

Additional operational constraints address other environmental factors. Our present test operations mitigate risks posed by natural factors during road operations by constraining driving to particular weather and road conditions. During development, local weather and events are assessed prior to deploying vehicles for on-road testing. If prevailing conditions are not in the vehicle ODD, Mission Specialists are notified to disengage self-driving operation and/or cease further operations until conditions change. The combination of the various ODD constraints in any given ODD serve as important controls for safety risk that may be not acceptable to the organization at any given stage of development, testing, or operation.

# Object and Event Detection and Response

Once the ODD is defined, we define and assess the appropriate system behaviors for detecting and responding to actors and scenarios in a given ODD. OEDR refers to the detection of any object or event that is relevant to the driving task, as well as the implementation of the appropriate response to such circumstances.[19] In order to achieve acceptably safe operation, the self-driving system must be capable of detecting and responding to a variety of static and dynamic objects in the road environment. The following sections expound on how the self-driving system delivers on this response.

## Behavioral Competencies

When determining the autonomy capabilities that constitute nominal operation, there are a number of inputs that inform performance of a self-driving system that can complete trips with acceptable levels of safety and reliability without a human operator controlling the vehicle. In order for the self-driving vehicle to complete these trips and share the road with other actors, we must implement a vehicle behavior that is effective in its environment. As that environment becomes more complex, so too does the set of behavioral competencies necessary to demonstrate. We continue developing system autonomy capabilities to operate effectively with an acceptable level of safety, and we leverage multiple reference data sources, including NHTSA's recent report, "A Framework for Automated Driving System Testable Cases and Scenarios."[20] Critical behaviors for an ODD or OEDR are considered throughout development.

19. NHTSA, 2017, 'Automated Driving Systems 2.0: A Vision for Safety.'
20. Thorn, Kimmel, & Chaka, NHTSA, 2018, Report No. DOT HS 812 623 'A framework for automated driving system testable cases and scenarios.'

## Current Generation Self-Driving System Hardware

Successful OEDR at the system level is supported by essential self-driving system hardware subsystems, such as the main system computer and a diverse sensor suite. Key self-driving hardware aspects of Uber ATG's technology include the following:

- **Light Detection and Ranging (LIDAR)** → LIDAR is a remote sensing method that uses light in the form of a pulsed laser to measure distances to actors and objects. Each current Uber ATG self-driving vehicle is equipped with one top-mounted LIDAR unit. Uber ATG's self-driving system utilizes a LIDAR unit with a range of over 100 meters (m).
- **Cameras** → Each current Uber ATG self-driving vehicle is equipped with cameras that provide high resolution, near-, medium-, and long-range imagery. There are cameras mounted in the sensor pod on top of the vehicle and around the vehicle with the goal of providing 360˚ sensing coverage. The camera hardware and accompanying firmware are custom to the Uber ATG self-driving system. Some of these cameras have a wide field of view and some have a narrow field of view. Another system of cameras provides imagery to support near-range sensing of people and objects within 5m from vehicle, in particular to assist during pick up and drop off, lane changing, and parking. The cameras housed in the on-roof sensor pod are equipped with a special cleaning system to remove or prevent accumulation of debris or precipitation.
- **Radar** → Each current Uber ATG self-driving vehicle is equipped with radars that provide object detection, ranging, and relative velocity of objects. Forward-facing radars are mounted below the headlamps, side-facing radars are mounted in the front and rear corners of the vehicle, and rear-facing radars are mounted near the ends of the bumper beam.
- **Global Positioning System (GPS)** → The onboard GPS receives GPS satellite signals to calculate coarse SDV position. While the GPS is not specifically used by the self-driving software for high-precision localization, it provides useful vehicle position information in support of localization, vehicle routing, and map data collect missions.

- **Self-Driving Computer →** The self-driving computer is the main system computer running Perception, Prediction, Motion Planning, and other software. The computer hardware and firmware are custom to Uber ATG's self-driving system. The computer is liquid-cooled for high-performance heat rejection.
- **Telematics →** Custom telematics hardware and software provide cellular data communication and can support carrier network redundancy, secure mobile data traffic, and authenticated cloud communication.
- **Vehicle Interface Module (VIM) →** The VIM is a gateway to allow the self-driving computer to communicate with the various vehicle control systems. It incorporates principles from International Organization for Standardization (ISO) 26262 Automotive Safety Integrity Level D (ASIL-D)[21] and provides closed-loop motion control, undertaking both trajectory management and trajectory tracking. The VIM is designed with a fail-operational architecture to provide high availability in the presence of faults. Its onboard inertial measurement units (IMUs) help enable the VIM to safely navigate the vehicle to a stop in the event of certain autonomy system faults.

## Current Generation Self-Driving System Software

The self-driving system must be capable of detecting and responding to a variety of static and dynamic actors and objects in the road environment. Sensing hardware, including LIDAR, cameras, and radars, generate input data for the vehicle's self-driving software system. Our self-driving software uses high-definition maps together with sensor input data to observe and categorize actors and objects in the environment, predict the actions of the actors and objects it detects, and then plan a path for the vehicle premised on safe driving principles and the rules of the road.

## Mapping

**Understanding the Existing World →** In addition to data generated by the sensor suite described in the prior section, our self-driving software uses a set of our high-definition maps, which we develop to improve real-time understanding of the driving environment. By storing and accessing precise road information on a virtual map, the vehicle can anticipate proper behavior without requiring as much real-time scene understanding. Maps can improve safety by enabling the vehicle to anticipate the need to slow down or otherwise optimize its motion plan, e.g., before the Perception system (described in the next section) would otherwise observe an upcoming tight turn. Our maps include the following information layers, among other data:

- Geometry of the road and curbs
- Drivable surface boundaries and driveways
- Lane boundaries, including paint lines of various types
- Bike and bus lanes, parking regions, stop lines, crosswalks
- Traffic control signals, light sets, and lane and conflict associations
- Railroad crossings and trolley or railcar tracks
- Speed limits, constraint zones, restrictions, speed bumps
- Traffic control signage

21. ISO, 2018, 'ISO 26262 Functional Safety for Road Vehicles.'

## Perception

**Detecting the Environment, Actors, and Objects →** Our self-driving vehicles are equipped with a number of overlapping sensors around the vehicle. Each sensing modality has its own strengths; combining these modalities provides a more complete, more accurate view of the environment.

Our Perception software detects and tracks individual actors and objects in order to generate estimates of their position, orientation, and velocity and register other attributes that may inform their future motion. For example, turn signals and hazard lights may convey information about the intent of other vehicles; however, a car with its left turn signal on may not actually turn left. So, while the system perceives the turn signal, it continuously estimates position, orientation, velocity, and other variables in order to ensure it can respond appropriately to the vehicle's ultimate course of action. The system also forms a view of stationary objects that convey useful information that should govern its motion, e.g., reading the state of traffic lights.

The main detection and classification stages that operate on sensor data are machine learned modules that are trained and evaluated using extensive labeled datasets covering the ODD. These datasets are made more comprehensive and detailed over time through tooling, offline algorithms, and human efforts. The system is designed to handle elements of uncertainty, or cases in which an object or actor may not be definitively classified by the onboard software. In addition to reasoning about uncertainty, the system has a second stage to account for actors or objects in the world that have sensor data, but have not been explicitly detected as a known actor or class of object. For these cases, the system estimates the actor's state and velocity, while allowing for conservative SDV reactions in case the actor moves in an unexpected manner.

Additionally, inputs from our sensor suite and our high-definition maps allow our self-driving system to precisely determine its own location — down to within a few centimeters.

## Prediction

**Reasoning About What Actors And Objects Might Do →** Our Perception software creates a representation of the SDV's active surroundings and our Prediction software uses this representation to predict what the actors or objects in the environment may do next. Some objects are fixed structures, such as buildings, ground, and vegetation, and we do not expect these objects to move. Actors, such as vehicles, pedestrians, and bicyclists, are expected to move. Our software considers how and where all actors and objects may move over the next several seconds.

Our prediction software applies different models of behavior for different actor and object classes: If an actor is perceived as a moving vehicle, it requires different possible predictions (of e.g., speed, direction) than if it were perceived as parked. At the same time, the system accounts for the prospect that an actor's current velocity may not definitively indicate next steps: A vehicle driving straight may elect to turn, or a parked vehicle may elect to begin moving forward.

The Prediction software considers and presents multiple anticipated motion paths for objects — i.e. possibilities of what the tracked "object" might do next — to the Motion Planning software, including intents that the system predicts may put the actors or objects in the self-driving vehicle's path, even when the self-driving vehicle has the right-of-way. The Prediction system seeks to determine the probabilities of multiple future paths for each actor in the scene. The Motion Planning system then uses these probabilities to effect an appropriate amount of caution in response to less predictable actors or objects. The system performs these predictions many times a second so as actors change direction or intent the system continually reassesses their likely next move.

**Improved Perception and Prediction Architecture →** Uber ATG is transitioning to an improved software architecture that effectively creates a joint Perception-Prediction subsystem. We anticipate that this change can further improve the self-driving system's performance when identifying and predicting motion of actors and objects in its surroundings.

## Routing, Navigation, and Motion Planning

**Planning What To Do →** Our Routing and Navigation software plans a route for the self-driving vehicle, taking the vehicle from its current position to its desired destination according to the rules of the road encoded in the map, any active constraints on the available road network, and provisions for safe driving.

Our Motion Planning software then combines information from the generated route, as well as perceived actors and objects and their anticipated movement from Perception and Prediction, as inputs and creates a specific motion plan for the vehicle for the next portion of travel.

Motion Planning provides for defined spatial buffers to be maintained at all times between the vehicle and other actors and objects in the environment; the size of these buffers varies as a function of speed to provide more space when the SDV is moving faster, as well as the type of actor involved. To preserve an appropriate buffer between the vehicle and any actors in the environment, the system may take a variety of actions, such as shifting laterally within a lane, opting to change lanes, braking to restore a safe following distance, or coming to a controlled stop and waiting until the situation clears or the self-driving vehicle is assisted.

Occlusions, or obstructed views, present challenges for both self-driving and human-driven vehicles. Our self-driving system reasons about occlusions and seeks to maintain the ability to avoid actors coming out of an occlusion at any reasonable speed.

## Vehicle Control

**Executing The Vehicle Plan →** Vehicle Control executes the trajectory supplied by Motion Planning by controlling actuation of the vehicle (including steering, braking, turn signals, throttle, and gear) through communication interfaces with the vehicle's steering, brakes, propulsion, and immobilization systems. Vehicle control is also relied upon to counteract sudden disturbances like crosswinds and potholes to keep the vehicle on the intended path.

Further, Vehicle Control is responsible for analyzing the dynamic limits and present condition of the vehicle, including any faults or error conditions that may affect Vehicle Control, and communicating this information back to the self-driving system. Fault handling and fail-safe design are discussed in greater detail in **Principle 2: Fail-Safe**.

We develop our Vehicle Control software in partnership with the manufacturer of the base vehicle, thereby promoting operation within the capability of the base vehicle platform.

## Traceability

**Graph Representation of Self-Driving Software →** The self-driving software running onboard our self-driving vehicles has transitioned to a new architecture suitable for representation as a directed graph. Through the deployment of a new software library, computation is represented by nodes, or discrete units of execution performed at runtime. The inputs and outputs of each node are represented by ports, allowing express representation of interactions between nodes as edges in a graph topology. Modeling the self-driving software this way enables direct traceability of inputs to outputs and resulting dependencies. This helps to achieve “determinism,” which is the ability to repeat conditions precisely for testing and debugging.



## Mission Specialists

Mission Specialists play a key role in the development of self-driving vehicles and are essential to collaboration between software, hardware, and test teams. During the developmental phase, Mission Specialists help promote safe driving, including in situations outside the system's ODD (as discussed above). The ability of our Mission Specialists to help preserve control of the vehicle during testing is achieved through self-driving system design, training, and operational procedures and policies.

At present, we operate our self-driving vehicles with two trained safety operators (e.g., Uber ATG-certified Mission Specialists or Training Specialists) in the vehicle when we are on public roads. The Pilot, or operator behind the steering wheel, is solely focused on helping preserve safe operation of the vehicle, while the Co-Pilot, the second operator in the right front seat, is tasked with monitoring, communicating with the Pilot and annotating the behavior of the self-driving system via a laptop.

Our Mission Specialists are key to understanding and evaluating the performance of our self-driving system. They bring the evolution of feature development full circle by providing significant insights from closed course and road testing. Proper training, continuous education, and open lines of communication with our engineering teams help ensure our Mission Specialists are able to do their jobs safely, effectively, and efficiently.


## Hiring and Screening

Because the operational responsibilities of our Mission Specialists differ from those of conventional drivers, candidates undergo a multi-step interview process which assesses technical, communication, and reasoning skills in addition to physical vehicle control.

1. **Application Review and Phone Screen** → The Mission Specialist hiring process begins with review by our recruiting team. Recruiters screen using a variety of questions intended to assess technical competency and testing experience, safety awareness and training, and driving history. Once the recruiting team completes the screening report, hiring managers determine if the candidate meets minimum requirements to move to the next stage.
2. **Homework** → Candidates are asked to complete an assignment that involves identifying how a self-driving vehicle might be affected, for example, by weather. The candidate is asked to prepare himself or herself to present to a group of engineers. This homework assignment is used to identify the candidate's ability to identify the capabilities and limitations of a system and apply these in a manner supporting safe and successful vehicle operations over a set of operating conditions. Strong candidates appreciate the potential strengths and weaknesses of the self-driving vehicle's sensors and controls and focus on safety.
3. **Onsite Interview** → Candidates are invited to interview with hiring managers, analysts and engineers, and relevant subject matter experts who assess their understanding of the position and qualifications. Managers assess the candidate's competency for safety procedures and their ability to work through difficult situational scenarios. This interview consists of an in-vehicle driving skills evaluation. Candidates are assessed on their ability to safely and responsibly operate a vehicle during manual driving, perform their duties in the presence of distraction, and effectively provide information about the driving environment and technology.
4. **Debrief and Hiring Decision** → Hiring managers and interviewers work with recruiting teams to determine if the candidate exceeds requirements set for the position. All candidates are also subject to certain screenings including a motor vehicle record check, drug screening, and a check for fitness for duty.

Prior to operating a self-driving vehicle, Mission Specialists undergo extensive training on our self-driving vehicles — including the software, hardware, and operating skills. We believe this to be a critical aspect of promoting the safety of our developmental self-driving system. Mission Specialist training is further detailed in the following sections.

## Policies

Recognizing key distinctions between conventional driving activity and operating a developmental self-driving vehicle, we have implemented a number of technologies and policies for Mission Specialists to assist with the safety of self-driving vehicle operations.

**Hours of Service →** We implemented an Hours of Service policy informed by U.S. Federal Motor Carrier Safety Administration (FMCSA) Hours of Service Regulations[22] and public fatigue management research.[23] We believe this research is currently the most relevant public information to self-driving vehicle operation in light of the complexity of self-driving systems and the attention required to maintain vigilance and control of the vehicle during testing (a set of skills that differ significantly from maintaining attention and control over a conventional vehicle).

Our policy requires that:

- There is confirmation that Mission Specialists have attained sufficient sleep.
- Managers are trained using U.S. DOT's Drug and Alcohol Supervisor Guidance[24] to look for signs of tired or impaired Mission Specialists.
- Managers must approve any over-time hours for in-vehicle work beyond an eight-hour workday.
- Mission Specialists must take an off-duty 30 minute break before the end of their fifth consecutive hour on-duty and are also required to take two 10 minute off-duty breaks during every 5 hours of operation. This means that in a 10 hour shift, there are two 10 minute breaks around the 2.5 hour and 7.5 hour marks and one break of 30 minutes around the 5 hour mark.
- Mission Specialists work fewer than 50 hours in a rolling seven-day period.
- Mission Specialists are limited to no more than four hours behind the wheel in self-driving in a given workday and no more than two continuous hours behind the wheel without taking a break or switching positions.
- Missions Specialists are asked to alert their manager in the event they do not feel fit for planned duties.

22. FMCSA, 2017, 'Summary of Hours of Service Regulations.'
23. North American Fatigue Management Program, ND, 'North American Fatigue Management Program: A Comprehensive Approach for Managing Commercial Driver Fatigue.'
24. U.S. DOT, 2015, 'Drug and Alcohol Supervisor Training Guidance.'

**Cell Phone Use →** Mission Specialists are strictly prohibited from interacting with their mobile devices while the vehicle is in motion or stopped in traffic. Our policy calls for a violation of this prohibition to result in discipline up to and including termination.

**Monitoring →** All of our self-driving vehicles are equipped with a third-party driver monitoring system that is operational during testing. If the system detects distracted driving, an audible alert sounds in the cabin and a notification is simultaneously sent to our remote monitoring team for review and escalation. We have also introduced an audible alert whenever the speed limit is exceeded when the vehicle is operating in manual mode.

This third-party monitoring system records acceleration, braking, cornering, and tailgating events and sends this data to a specially-trained team for review. This information makes it possible to provide evidence-based feedback to Mission Specialists and moreover facilitates coaching for continuous improvement. The monitoring system also routinely shows examples where a mission specialist has performed exceptionally when encountering a difficult situation on the road. In these instances the team can collectively learn from this experience.

## Manual Driving Training

Mission Specialists are required to complete a comprehensive training program to prepare them to safely operate a self-driving vehicle and protect its surroundings and occupants from harm.

Every Mission Specialist must be capable of safely operating our vehicles, which are equipped with non-standard technology features and physical equipment specific to self-driving operations, whether during manual or self-driving operations. For this reason, we open our training program with safe manual driving habits, first on a closed course, followed by public road training.

**Driving Training →**

- **Driving dynamics and awareness —** via in-classroom instruction and driving drills on the test track.
- **Emergency maneuver exercises, —** including collision avoidance, anti-lock braking, and slalom driving (zig zag in between cones) at speeds, as relevant to our ODD.
- **Parking and reversing exercises —** to assess spatial awareness, vehicle size limitations, vehicle placement relative to other actors, and the proper use of mirrors and reverse cameras.
- **Navigating occluded views —** during manual driving.
- **Defensive driving**[25] **—** online course to educate Mission Specialists on driving habits and new defensive driving techniques for operating self-driving vehicles.
- **Policy Overview —** to brief all new, updated, and applicable policies within operations that impact a variety of operational domains and the employees involved.
- **Fatigue Management —** to raise awareness of what fatigued driving is, the possible consequences internal and external to Uber ATG Policy, and steps to manage fatigue and avoid operating while fatigued. Content was developed upon consultation with resources from the U.S. National Transportation Safety Board (NTSB) and the FMCSA.
- **Incident Response —** to ensure Mission Specialists can handle all levels of incidents effectively while remaining confident and calm.
- **Distracted Driving —** to educate Mission Specialists on how to avoid becoming distracted in connection with policies restricting phone use and how to identify other motorists who might be distracted.

25. NSC, 2017, 'Defensive Driving Online Course - 4 Hours.'

ODD and Vehicle Platform Training →

- **Overview of ODD —** to educate Mission Specialists on its scope and required capabilities.
- **Overview of traffic laws —** relevant to the ODD.
- **Incident response simulation —** to practice confident handling of incidents.
- **Platform failures exposure —** and report.
- **Base Vehicle Advanced Driver Assistance System —** explanation.

## Technical Education

To safely operate a self-driving vehicle, a Mission Specialist must understand the essentials of the self-driving system. Mission Specialists undergo extensive hardware and software training on:

- **Hardware on the Vehicle —** The program reviews sensor functions and limitations, as well as vehicle control hardware. Mission Specialist trainers also demonstrate sensor range, vehicle positioning, fields of view for all sensor modalities (LIDAR, Radar, Cameras, and Ultrasonics).
- **The Self-Driving Software —** The training program uses the self-driving system architecture to explain how the vehicle processes information. This includes a thorough review of maps, sensors, Localization, Perception, Prediction, Routing and Navigation, Motion Planning, and Vehicle Control.

Our training program includes modules on vehicle capabilities, limitations of the hardware and software, and how the self-driving vehicle reasons about and interacts with its environment. Training modules include:

- **Software limitations module —** describes the system's capabilities in the ODD.
- **Occluded views module —** explains how self-driving vehicles identify and handle occlusion. The content in this section covers the vehicle's self-driving capabilities in managing occlusion and proper procedures for piloting a self-driving vehicle through an occluded intersection or scenario. Exercises are both in-classroom and in-vehicle.
- **Pedestrians and cyclists interactions module —** demonstrates how the self-driving vehicle responds to pedestrians and cyclists. Exercises are both in-classroom and in-vehicle.

Developing a Nominally Safe System
→ Mission Specialists
→ Piloting
→ Co-Piloting
→ Continuous Education
→ Communication



## Piloting

Before operating a vehicle in self-driving, a Mission Specialist must complete piloting training. As with the manual driver training, we first introduce these fundamentals in the classroom and on a closed-course track prior to public roads.

### Piloting Fundamentals

- **Engaging and disengaging techniques —** cover procedures on how to safely engage and disengage self-driving, first in a stationary vehicle then in a moving vehicle. This course also covers the vehicle controls and nominal self-driving operations as well as the visual and audio cues that are presented upon system state transition.
- **Safety and personalization —** covers adjusting mirrors and seat position to properly and comfortably pilot the vehicle.
- **Touch grip —** training covers proper hand position on the steering wheel. This hand position allows the Mission Specialist to disengage self-driving using the steering wheel when appropriate.
- **Pedal shadowing —** covers disengagement from self-driving by depressing the accelerator or brake pedals. Mission Specialists are trained to hover a foot over the proper pedal to help ensure a smooth and safe takeover if the vehicle is in motion.
- **Operator Tablet interactions —** cover the policies for interacting with the integrated tablet display.

### Fault Injection Training

During Fault Injection Training (FIT), faults are intentionally triggered in the system while on a closed course so trainees can safely gain exposure to the vehicle's behavior in a variety of fault situations. Fault Injection Training is discussed in greater detail under **Principle 2: Fail-Safe.**

## Co-Piloting

By operating with a capable safety operator, such as a certified Mission Specialist, in both the front left and right seats of the vehicle at all times, the Co-Pilot is always available to support safe operation of the self-driving vehicle through his or her use of Robot Studio (via a dedicated Co-Pilot workspace run on an in-vehicle laptop) and effective communication of complex technical issues.

## Continuous Education

During development, vehicle behaviors, capabilities, and system-level features are constantly evolving. In order to provide our Mission Specialists with the most up-to-date information on our system, we hold daily mission briefings and require completion of online learning modules and in-vehicle or in-classroom training. We train Mission Specialists on new capabilities and functionalities before operating in the presence of those capabilities or functionalities; examples of changes resulting in new training include enabling self-driving lane changes, increasing vehicle operating speeds, and expanding ODDs.

## Communication

Effective communication between the Pilot and Co-Pilot plays an important role in acceptably safe self-driving vehicle operations. Our training program covers guidelines for managing in-vehicle communication. Further, Mission Specialists are trained to share relevant information from the Co-Pilot workspace that can assist the Pilot.

## Fatigued / Distracted Driving Prevention

In light of the particular opportunities for distraction and fatigue while operating automated systems — issues that, with monitoring automated systems, are more acutely present than when driving conventional vehicles — our training programs focus on assisting Mission Specialists in recognizing and managing these situations.

- Our **Distracted Driving** module raises awareness of distracted driving, possible consequences, and steps to avoid this behavior. Mission Specialists read and discuss the National Safety Council's (NSC's) "Understanding the Distracted Brain"[26] and complete exercises to ground their learning.
- Our **Fatigued Driving Prevention** module references guidance from the U.S. National Transportation Safety Board[27] and U.S. Federal Motor Carrier Safety Administration.[28]

## Operational Safety

To ensure a high level of proficiency in day-to-day operations, Mission Specialists must be aware of and responsive to their operating environment, both inside and outside of the vehicle.

As described, we train Mission Specialists in the classroom on the ODD, including the limits of the self-driving system, how and when to resume manual control of the vehicle proactively or in the event of a system fault or failure. We scope our public road driving such that mission operating conditions are designed to stay within the system Operational Design Domain. For a geographic area of interest, we define permissible road networks, speed limits, and maneuvers based on current system capability and performance. We then layer parameters like time of day, weather, and road conditions to limit self-driving operations to an envelope domain within which the self-driving vehicle and Mission Specialists can perform safely.

Our Mission Specialists are trained on the envelope of permissible operating conditions, along with special actors, conditions, or events which the SDV may not be able to handle performantly and are therefore considered out of scope for self-driving. Conditions recognized as out of scope for self-driving instigate a Mission Specialist takeover wherein the self-driving system is preemptively disengaged and driving control is returned to the Pilot. This information is reinforced during in-vehicle training and FIT training modules and prepares the Co-Pilot to inform the Pilot of any upcoming events that may require a transition to manual mode.

Mission Specialists also receive a daily, pre-mission briefing on the current operational test plan, ODD, and software release status. As the ODD evolves, we brief or train Mission Specialists, depending on the scope of the change.

26. NSC, 2012, 'Understanding the distracted brain.'
27. NTSB, 2017, 'NTSB 2017-2018 Most Wanted List of Transportation Safety Improvements: Reduce Fatigue-Related Accidents.'
28. FMCSA, 2014, 'CMV Driving Tips - Driver Fatigue.'

## Operator Tablet and Display

Human drivers are constantly receiving new information from the driving environment, processing this information, and making informed decisions. All of our self-driving vehicles are equipped with a touchscreen tablet that communicates important information to our Mission Specialists, including turn-by-turn directions for the planned route and whether the system is currently under manual or self-driving control. We enforce security by having drivers, including Mission Specialists, securely log on to the tablet prior to operations.

Recognizing the particular challenges arising in supervising highly automated systems, we leverage NHTSA's Human Factors Guidance for Driver-Vehicle Interfaces[29] and Human Factors Design Guidance for Level 2 and Level 3 Automated Driving Concepts[30] to minimize potential distraction due to installed vehicle components, and we have established a complementary set of policies to protect against inappropriate use. During current operations, the touchscreen:

- Does not require any input from the Pilot while driving;
- Minimizes use of text, background information, and options for interaction;
- Uses audio and user interface transitions and map motion to clarify information presented;
- Employs a visual system focused on color, iconography, and visual layout to improve glanceability;
- Optimizes color for time of day.

29. NHTSA, 2016, 'Human Factors Design Guidance For Driver-Vehicle Interfaces.'
30. NHTSA, 2018 'Human Factors Design Guidance for Level 2 and Level 3 Automated Driving Concepts.'

# Transitioning Between Self-Driving and Manual Driving

Transitions to and from manual driving help facilitate safe testing and help to manage a number of types of risk. Under normal conditions, these transitions are only completed by Mission Specialists who have received the training necessary to understand how and when to do so safely; however, First Responders may disengage the self-driving system as explained in our Public Safety Officials and First Responders' Guide. Similarly, Mission Specialists must be able to easily transition out of self-driving and into manual driving whenever necessary to help ensure safe operation.

We have designed the self-driving system to have multiple means of shifting between manual driving and self-driving.

- **Shifting Into Self-Driving →** While the vehicle is in park at the start of a mission, Mission Specialists authenticate to Uber ATG infrastructure and verify a two-factor challenge. This authorization and authentication is intended to ensure appropriate access prior to enabling the self-driving system. Once authenticated, the Pilot begins manually maneuvering the vehicle, including maneuvering it into the approved ODD. When the vehicle is in the ODD, the Mission Specialist is informed of system readiness via visual indicators on the Operator Tablet that specify whether the system is ready to transition into self-driving control. In addition to displaying readiness for self-driving control, the Operator Tablet persistently indicates whether or not self-driving control is currently engaged.

  In our current self-driving vehicles, the Pilot, or Mission Specialist occupying the driver's seat, can shift into self-driving by pulling both steering wheel shift paddles simultaneously. Upon shifting into self-driving, audio and visual cues confirm the successful transition.

- **Shifting Out of Self-Driving →** At any time, the Pilot can shift out of self-driving using any of the following methods:
  - Depressing the accelerator pedal;
  - Depressing the brake pedal;
  - Depressing the steering wheel shift paddles;
  - Turning the steering wheel.

  While not intended as primary disengagement methods, a Pilot disconnecting his or her seatbelt or opening the driver's door will also disengage self-driving control. These disengagement methods help prevent a driver inadvertently leaving the vehicle while self-driving is active.

- **Knowing Which System State is Active →** In each discrete self-driving system state (manual, ready, self-driving), the current operational state is displayed to the Mission Specialists on the Operator Tablet using a persistent banner that changes color and text depending on the mode. The route lines utilized in the turn-by-turn instructions on the touchscreen tablet also match the color of the banner.

- **Knowing When the System State Changes →** As described above, when the system shifts into self-driving, audible and visual cues are presented to the Mission Specialists. Similarly, when the system returns control to the Pilot, audible and visual cues are presented.

  Uber ATG's designs ensure the Mission Specialist is always informed of the current operating state of the vehicle and any changes to operating state using multiple modes of Human Computer Interface which, in combination with our robust Mission Specialist training program, are essential for safe operation.

04

# Integration, Verification & Validation Methods

We have built and continue to build robust tools and processes at every step in our development cycle to track and respond to system issues. Both our software and hardware development processes thoroughly evaluate the self-driving system prior to any testing on public roads.

The quality management, verification, and validation activities addressed in this section are key components of Uber ATG's approach to system safety.[31] These efforts support traceability and change management throughout our development process and are complementary to the design, planning, and operational considerations discussed above.

31. NHTSA, 2017, 'Automated Driving Systems 2.0: A Vision for Safety.'

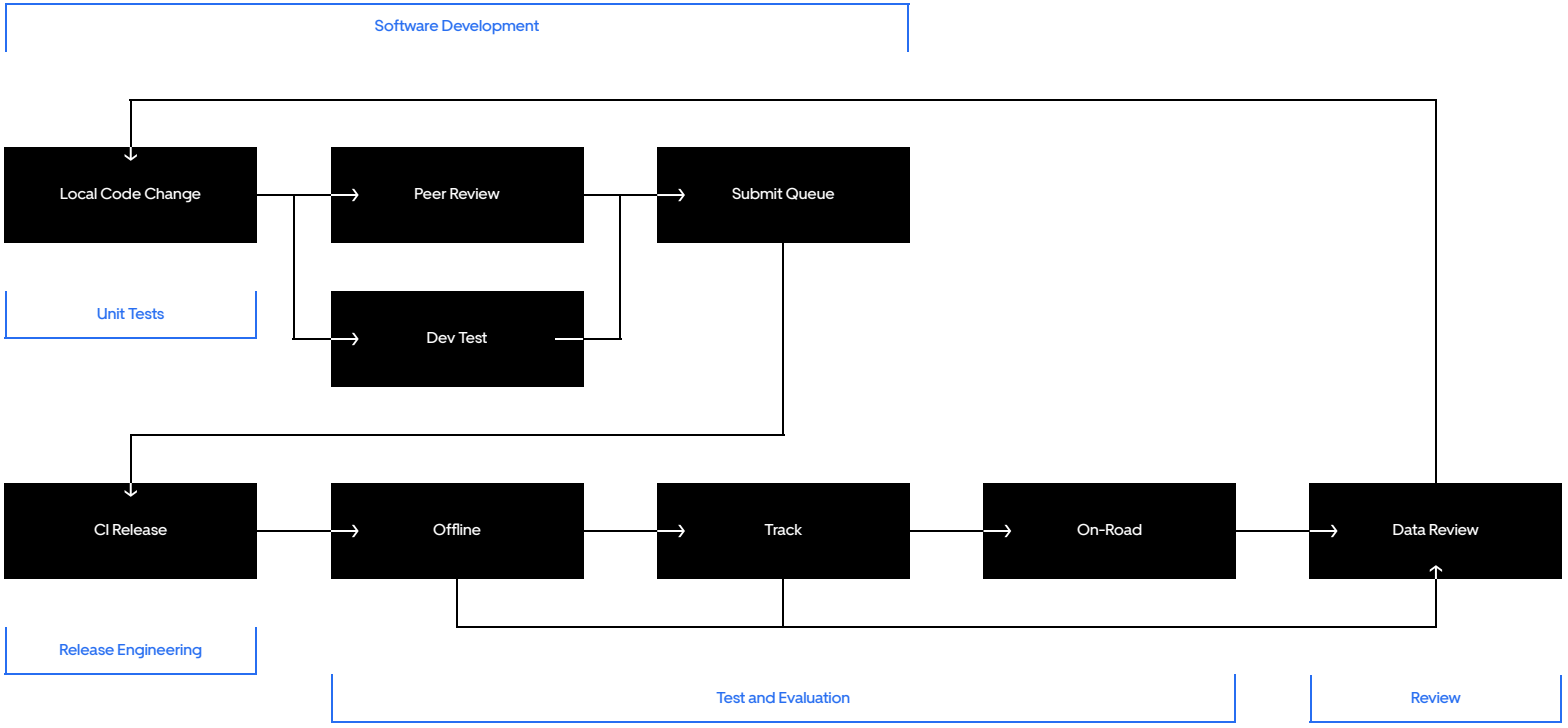
## Self-Driving Software Quality Processes

Uber employs a rigorous verification and validation process from an initial software change through real-world testing.

Deviations from expected operation during offline, test track, and on-road testing and data collection are recorded and shared with self-driving system development teams. In particular, comments from our Mission Specialists provide a firsthand account of the in-vehicle experience. Data created by noteworthy events, such as large deviations from one planned trajectory to the next, system diagnostics, or Mission Specialist interventions, are identified for our data review process.

We then track these events from discovery to resolution. For example, we may re-simulate software changes to evaluate their impact on these key events, to confirm issues are resolved as intended, and to confirm unexpected failures are not introduced. Many events are incorporated into datasets for machine-learning algorithms, while others are utilized as challenging test cases. Once issues are resolved, the resolution factors into every new software change with an eye to preventing the accidental re-introduction of previous behaviors.

# Software Development and Verification Process



## Offline Testing

We have developed a suite of offline testing tools that enable us to test code as soon as it is written, providing valuable insights into potential issues as early as possible in the development lifecycle.

Each software release is subjected to a battery of automated offline tests that provide a baseline level of confidence that the release should advance to the next release testing stages. If a release does not pass the offline release evaluation process, it does not move forward. A sample of offline release tests include:

- **Static Analysis →** Resources including linting tools, compiler-level analysis, and memory and threading sanitizers are entirely automated and applied to identify common errors and security problems early in software development. They are required prior to merging software changes to the code base and help inform other processes such as peer review.
- **Unit Tests →** Tests that are designed to test atomic (non-divisible) portions of code, and are run independently on software changes prior to landing on the code base.
- **Map Compatibility Test →** As our self-driving software requires a map in order to support autonomous operations, this test ensures both the latest map and self-driving software release being tested have no integration issues.
- **Onboard Integration Tests →** This set of tests confirms that the latest self-driving software release has been correctly deployed to the vehicle, that the software connects to the vehicle platform as desired, and that notifications are passed correctly between the software, self-driving system hardware, and base vehicle.
- **Virtual Simulation Regression Set Test →** Set of simulations representative of nominal on-road scenarios against which all software releases are tested for regression, i.e., when the simulated self-driving system behavior fails a scenario that it previously had passed.
- **Reaction Time Metrics Test →** Evaluates whether the reaction time of the self-driving system software meets our expected requirements.

We handle failures in relationship to where they arise in the software release process:

- **Failures in Testing Prior to Integration →** Failures found prior to integration into the master code repository are generally provided directly to the author of the code change for resolution as part of the peer review and development testing process.
- **Failures in Release Testing →** We treat failures found during release testing phases as very high priority. We conduct an initial triage of the failure to understand root cause and support a resolution.
- **Preserving Accuracy of the Testing Regime →** In addition to addressing anomalies in the system, we work to prevent and address anomalies in the testing regime itself. When the reliability of a test is deemed questionable, such as if the test may reflect false-positives, the test owner reviews the test for validity and/or revision.

Where possible, a parallel effort begins to create an offline test that seeks to detect this failure prior to entering the codebase in the future. This helps our battery of tests to become more comprehensive over time. Additionally, if an issue is identified as safety critical, we have the option to immediately and remotely stop operations entirely or within a specific ODD through real-time communications with the vehicle fleet.

**Hardware in the Loop (HIL) Testing**

HIL testing is concerned with ensuring performance of our software when running on representative hardware. By coupling our self-driving system software with our self-driving system hardware prior to it actually being placed on a vehicle, we are able to isolate and diagnose problems that may not be revealed through software testing alone. While HIL testing is not performed for every software change, it is a valuable tool for challenges such as timing analysis and subsystem compatibility assessment.

**Simulation**

Simulation plays a key role in self-driving software development: It enables testing of relatively rare, challenging scenarios without the physical risk associated with test track or on-road testing. It also allows testing more routine scenarios with controlled variations. Simulation tests have different permutations and combinations of traffic patterns, speeds, and trajectories for all the actors and objects in a scenario — including our self-driving vehicle.

Benefits of simulated driving test approaches include:

- **Safety →** Simulations allow us to safely test high-risk scenarios that would raise different risks if tested in the real world.
- **Repeatability →** Simulations can be rerun in the same exact way over time. This predictable deterministic setup allows us to evaluate progress of subsequent builds of self-driving software against the same scenarios with a degree of repeatability that is not possible by track testing.
- **Frequency of occurrence →** Many of the challenging scenarios we need to test occur infrequently in the real world. In simulation, we can increase the frequency of these scenarios in order to test our system's ability to handle lower-probability events.
- **Variance →** We can run numerous variations of the same test scenario.
- E**fficiency →** Testing our self-driving system in simulation requires fewer resources than real-world testing.

We are focused on the reliability of simulation results and on measuring and improving consistency between our real-world and simulated vehicles and between our test track and simulated scenarios.


**Test Scenario Development**

Fundamental to Uber ATG's strategy for the development of safe self-driving technology is alignment between design, test, and use. We employ a scenario and ODD development framework that characterizes design requirements, real-world events (such as those collected through driving logs), synthetic test scenarios, and operational policies using a unified schema.

A scenario includes the physical environment as well as actors or objects and their static or dynamic paths. Each scenario is defined by a number of criteria for success, including considerations such as speeds, distances, and descriptions of safe behavior. Our scenario documentation provides the basis for virtual scenario builds that can be run in simulation and on our test track. Scenario success criteria are aligned with applicable traffic laws.

Our testing battery includes virtual models of scenarios that:

- **Require basic driving skills →** We identify and define basic driving capabilities necessary to operate in a given ODD during the ODD characterization phase.
- **Are known to be associated with crashes between conventional vehicles →** We developed a set of scenarios that are more frequently associated with crashes, based on a report, among other things, of data and frameworks from NHTSA,[32] PROSPECT Project[33] and The European New Car report Programme (Euro NCAP).[34]
- **Are more challenging for self-driving vehicles →** We add additional scenarios as they are identified through on-road operations or observed during offline testing.
- **Are ultimately intended to be representative of much of what our vehicles could encounter in the real world →** The world can create an infinite number of unique cases. As we encounter new scenarios that are not covered, we intend to add or substitute scenarios to continuously improve the set.

32. NHTSA, 2007, 'Pre-Crash Scenario Typology for Crash Avoidance Research.'
33. PROSPECT Project, ND, 'PROSPECT Project.'
34. Euro NCAP, 2018, 'Vulnerable Road User Protection.'


## Track Verification Testing

Software releases that pass offline testing advance to Track Verification Testing (TVT). We test and verify each software release on our closed course test track by subjecting the software to challenging scenarios, such as occlusion scenarios.

- **Track Test Development →** We develop the test suite for TVT through an iterative process that begins with identifying our target ODD, understanding the capabilities required in that ODD, and developing tests to measure performance of the system. TVT comprises both on-vehicle tests, which exercise the self-driving vehicle's behavior, and offboard functionality tests, e.g., operability on the Uber network, all within the controlled environment of the test track. Also performed at the track, fault-injection exercises simulate the effects of a malfunction or error in system hardware and software, such as loss of expected functionality at the system level.
- **Analysis →** TVT is conducted as often as several times per week to evaluate self-driving system performance. Evaluation criteria are established in capability-based product requirement documents, test plan and procedure documents, and design specifications.

  If the system fails a test, the basis for that determination is documented and tracked using a standardized system.
- **Release Reporting →** For each software release tested through TVT, we generate a report to show performance of the self-driving system, including pass/fail percentage across all tests and breakdowns of problems encountered. Only after having demonstrated proficiency against a representative set of offline and track tests is a self-driving software release deemed ready for on-road operation.

## On-Road Validation Testing

We believe that the potential of self-driving vehicles will only be realized if we are able to learn from real-world situations, while gaining and preserving public trust. On-road driving allows us to observe the performance of our system when faced with the diverse set of inputs that occur outside of closed environments. This controlled exposure under the supervision of our Mission Specialists enables us to both improve our technology in response to observed events as well as to prudently validate our virtual world and test track scenarios for greater test coverage on future releases.

As with all other methods of testing, On-Road Validation Testing is carefully monitored and any issues encountered are reported by the Mission Specialists. These issues are then analyzed for root cause, correction, and improvement of the offline and track tests are proposed to prevent recurrence of the issue where feasible and catch any recurrence as early as possible in the development cycle.

# Self-Driving Hardware Quality Processes

We also address potential hardware and software issues with the physical hardware components of the self-driving system hardware via quality processes.

## Design Quality

**Component Level Design Verification**

Hardware modules for our self-driving system undergo testing to confirm they are functioning properly, and to identify performance limits. Once we have confirmed appropriate function, individual components are validated via environmental qualification testing. This testing provides comprehensive coverage of thermal, vibrational, electromagnetic and other environmental factors beyond what is expected during normal operation. In addition, components undergo extensive reliability testing to ensure proper functionality throughout the intended product lifecycle. This testing exposes components to accelerated wear and tear, namely to simulate lifetime exposure and ensure no degradation of function or performance.

**Subsystem-Level Design Verification**

We test certain subsystems in order to confirm effective interactions between components. This stage of testing also leverages HIL and simulation testing across hardware and software interfaces in a controlled environment. We also perform fault injection testing at this level. Automation of tests makes it possible to conduct highly repeatable structured testing of hardware/software interfaces. This subsystem-level design verification is required before track and road testing.

**System-Level Design Verification**

Self-driving hardware and software components are integrated into the vehicle and tested to confirm performance of:

- **Mechanical interfaces —** including thermal and structural integration into the base vehicle.
- **Electrical interfaces —** including integration into the base vehicle power distribution system and onboard communication busses.
- **Control path interfaces —** including Application Programming Interfaces (APIs) to provide base vehicle platform motion (e.g., steering, braking and acceleration) as well as other key actuations (e.g., turn signals and gear changes).


## Manufacturing Quality

Uber ATG has implemented a comprehensive set of quality control processes. We follow an internal process informed by the principles of relevant industry standards[35] for both assemblies built in-house and sub-systems received from suppliers. Our process is described in the list below.

- **Supplier Selection** → Supplier selection is conducted relative to the part or component being sourced.

  As development of a build or module matures, we develop a quality control plan jointly with the supplier, which specifies the type and frequency of quality data recording. The quality control plan reflects the complexity of the product, maturity/stability of the process, and statistical significance of the sample size.

- **First Article Inspection Process** → At the start of manufacturing, the supplier produces a small first batch of parts, which is subjected to detailed inspection against specifications.

  The first articles are inspected to the design data package and approved/rejected by hardware design, manufacturing, and quality engineering teams. The first article inspection is required to authorize manufacturing of larger quantities and serves as a trial run for quality data recording.

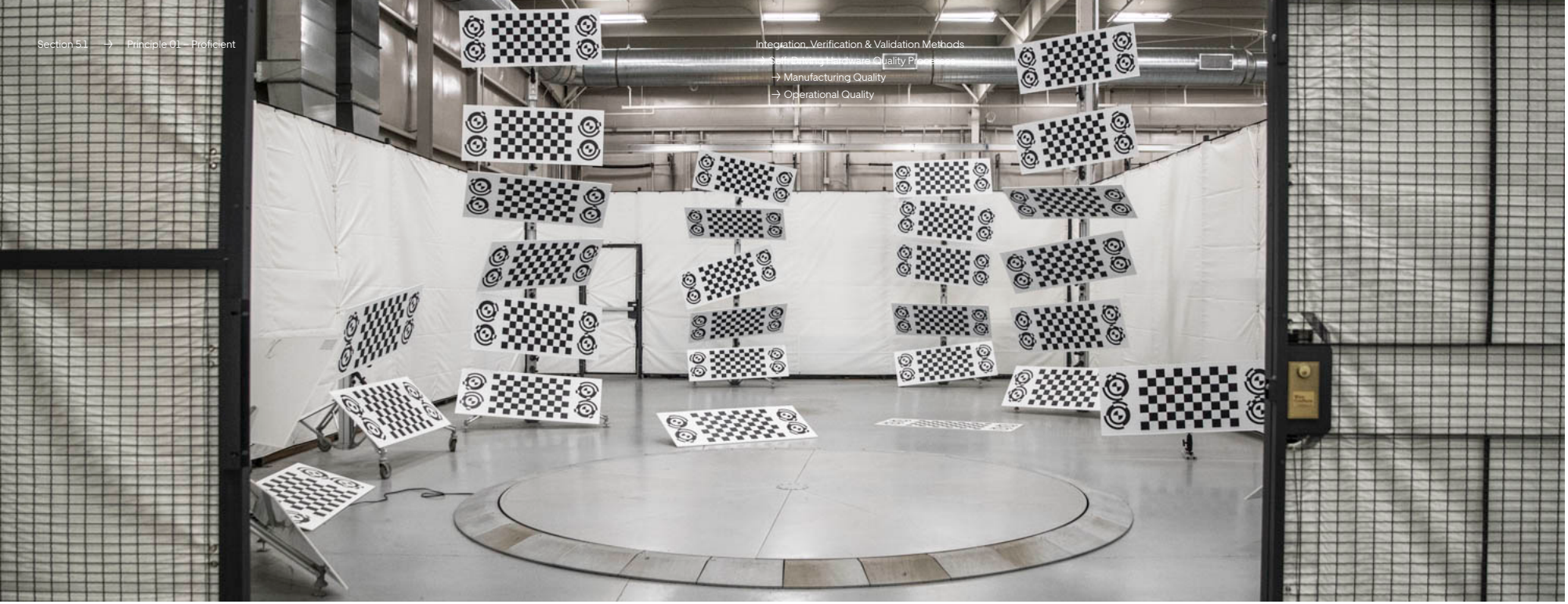
- **In-Process Inspection Plan** → The inspection plan is created before the assemblies are built based on the design data package. The plan informs the production technician team of pass/fail criteria for component assembly.

  We implement in-process quality checks at assembly stations; these must pass before moving the assembly or vehicle to the next production station.

- **Traceability** → All assemblies built in-house or from suppliers require traceability data recording of date/lot codes, component/module serial numbers, and revision tracking.

  For example, Uber ATG hardware assembly stations are set up with fastener tightening data recording. Fastener tightening data is collected through the use of smart tools. All torque tools and other applicable assembly tools are periodically calibrated, and we retain records for the life of the tool.

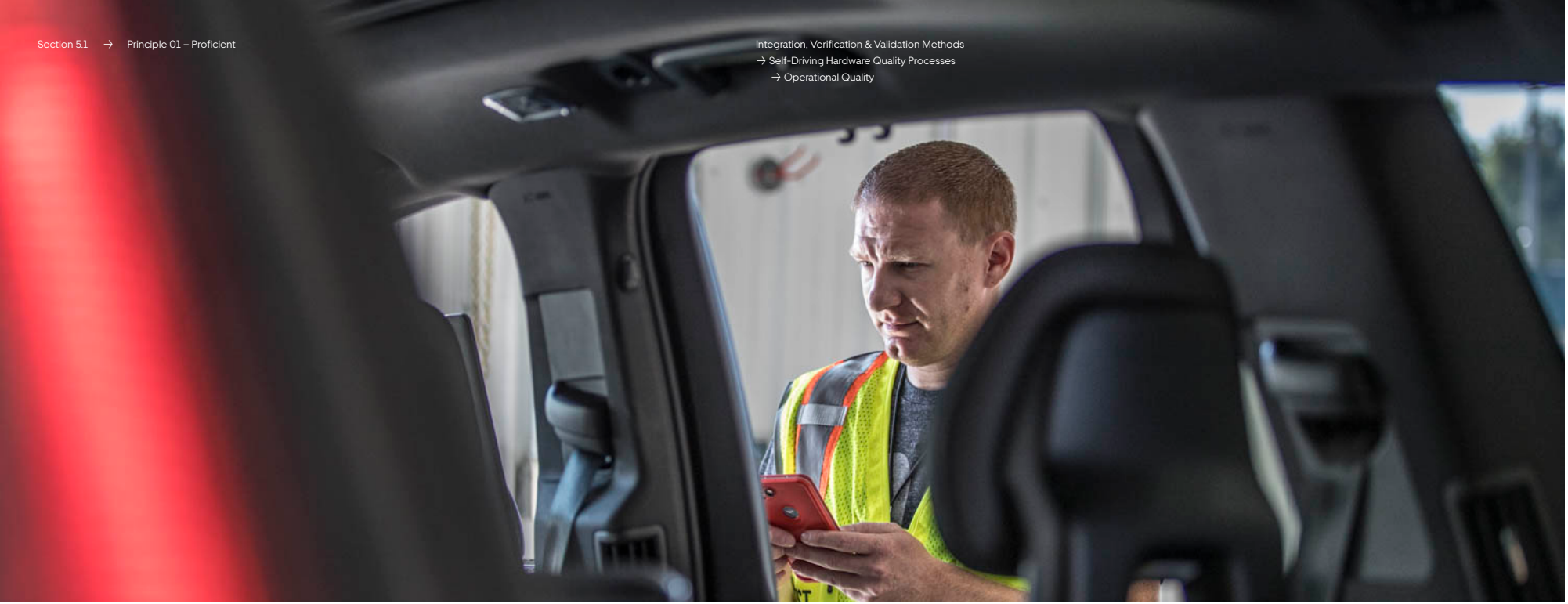
35. ISO, 2015, 'ISO 9001 Quality Management Systems.'







- **End-of-Manufacturing-Line Testing and Outgoing Quality Control →** The upfitted vehicle undergoes software updates and an extensive series of tests to ensure hardware performance when operating as a system. We develop the end-of-line testing plan in close coordination with design engineering. We undertake ongoing inspection, including redundant checks of critical fasteners, fit and finish checks, review of traceability data, and documentation to create the vehicle assembly quality data package. We then retain records for the service life of the as-built vehicle.
- **Calibration →** After passing outgoing quality control, the upfitted vehicle leaves the manufacturing facility and advances to calibration, road-released software loading, and closed course testing before on-road testing.



## Operational Quality

### Commissioning and Calibration

Commissioning and calibration is the final phase of the self-driving system hardware build validation process. The purpose of this phase is to ensure all sensors required for self-driving capabilities are fully functional, and to collect the data necessary to perform intrinsic and extrinsic calibration — or measurement of hardware parameters required to align and combine the data produced by multiple sensors. We expose the self-driving vehicle to specific targets and environments wherein data logs are collected for use in a quality assessment. Finally, we put the vehicle through a final driving test. Any issues identified throughout the process are tracked and resolved by trained technicians.

### Maintenance and Repair

Uber ATG-managed self-driving vehicle fleets undergo extensive maintenance and monitoring routines to help ensure they continue to perform as expected. Prior to performing a day's mission, Mission Specialists subject the self-driving system to health checks and inspections to ensure it is ready for operations. We track pre- and post-operational inspections digitally, and the results automatically generate issue tickets for tracking. This ensures every vehicle is properly inspected before it leaves our testing operations centers.

We track all platform software and hardware issues that emerge during commissioning and operations through to resolution. Once an issue is identified, our trained vehicle technicians are responsible for verifying, analyzing, isolating, repairing, and confirming operational viability across all of Uber ATG's self-driving vehicles.

# 5.2 → Principle 02
# Fail Safe

The Self-Driving Vehicle is acceptably safe in the presence of faults and failures.

# 01 Supporting Concepts

→ A **safety-relevant failure** is a malfunction that results in a reasonable probability of harm to a person or property. In addition to demonstrating that our system is safe when it is working correctly, we also have to demonstrate that it is acceptably safe when it encounters a fault. Other types of failures may result in non-safety related outcomes, e.g., a poor experience for a rider.

→ The **minimal risk condition** is a system state which "reduce[s] the risk of a crash when a given trip cannot or should not be completed… It may entail automatically bringing the vehicle to a stop within its current travel path, or it may entail a more extensive maneuver designed to remove the vehicle from an active lane of traffic and/or to automatically return the vehicle to a dispatching facility."[36] The appropriate maneuver depends on the particulars of the failure and the circumstances of the scenario.

→ We understand that in a complex system some safety relevant hazards cannot be completely eliminated. By proactively identifying hazards and understanding them, their risk can be mitigated and/or managed to a level considered minimal and acceptable.[37]

To fulfill this principle, we partition safety responsibilities to different parts of the system; we also institute fallback maneuvers during system-level failures. Any system in any product can experience failure. That is true here as well, where any part of the vehicle — base vehicle components, replacement hardware components, add-on electronics, or our software — has the potential to experience a failure during operation. We reduce the risk of harmful events initiated by loss of system functionality by minimizing common-cause failures through system architectural analysis, and we implement functional redundancies and implement component robustness where feasible. System diagnostics and implementation of a fault management system contribute an additional layer of detectability and prevention against system-level failures.

36. SAE International, 2018, 'Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016.'
37. Federal Aviation Administration, 2011, 'System Safety Analysis and report for Part 23 Airplanes.'

02

# Developing in the Presence of Faults and Failures

## Fault Tolerant System Design

No system is immune from abnormal conditions that interfere with its ability to function as intended. These conditions are faults; the related loss of functionality, if severe enough to create a risk of harm to person or property, is a safety-relevant failure.[38] Certain interruptions to self-driving system functionality, without appropriate mitigations, can pose a risk to the safety of those in and near the vehicle. A self-driving vehicle should therefore be designed, to the extent practicable, to function predictably, controllably, and safely in the presence of any faults and failures.

To mitigate potentially harmful effects of a safety-relevant failure, we have several options: We can make the precursory fault sufficiently improbable and/or implement a solution that transitions the system to a Minimal Risk Condition (MRC) in the presence of said fault or the resultant failure. We achieve this through use of robust and thoroughly-tested components, designing key redundancies (e.g., steering, braking) into the system, and implementing a subsystem that monitors the system for faults and takes action when they occur. Redundancies and fault detection software are tenets of fault tolerant system design.

## Preventing Faults

Our approach to fault prevention is informed by similar approaches in other industries, such as automotive and aerospace. For example, we leverage processes from an automotive industry functional safety standard,[39] to identify, assess, and mitigate faults and hazards for electrical and electronic components.

38. Consistent with failure (1.39) and fault (1.42) definitions in ISO, 2018, 'ISO 26262 Functional Safety for Road Vehicles.'

39. ISO, 2018, 'ISO 26262 Functional Safety for Road Vehicles.'

## Designing a Fault-Tolerant System

Self-driving vehicles must be able to tolerate faults. Fault tolerance in our application requires that the self-driving system is able to retain certain safety-relevant functionality even when faults occur. When faced with a safety-relevant fault, the system may return control to the Mission Specialist. Today, we primarily rely on Mission Specialists to resume control of the vehicle in the presence of a safety-relevant fault by providing robust training on system limitations, and alerting them to a transition out of self-driving via audio and visual cues. Mission Specialists are specifically trained on how to respond to system fault notifications as detailed in the following sections.

System-level fault protection involves implementing mitigatory mechanisms that transition the vehicle to a minimal risk condition in the case of a safety-relevant failure. The self-driving vehicle is designed to detect if a safety-relevant fault has occurred and initiate a fail-safe response. Engineers review all detectable faults and assign the appropriate fault action / minimal risk condition based on the following.

1. The functionality that the system retains in the presence of the fault.
2. The time it takes from the occurrence of the fault until a harmful event could occur as a result.

Vehicle control needs to provide highly-reliable operation, particularly in instances where the vehicle must be safely and immediately brought to a stop. Thus, we have chosen to develop vehicle control as a secondary computing system on embedded hardware that is distinct and independent from the self-driving computer. This distinct vehicle control computing system is called our Vehicle Interface Module.

This design provides fault tolerance through features such as redundancy, high integrity processors, and additional Inertial Measurement Units (IMU). This design provides continuous availability of safety critical functions like steering and braking. Through fail-operational design, we increase the likelihood that the desired trajectory can be executed safely and without interruption. Development of this subsystem took into account best practice and industry standards for functional safety, including ISO 26262,[40] ISO 16750,[41] MISRA C 2012,[42] and AUTOSAR 4.2.[43]

40. ISO, 2018, 'ISO 26262 Functional Safety for Road Vehicles.'
41. ISO, 2012, 'ISO 16750-2:2012.'
42. Motor Industry Software Reliability Association (MISRA), 2013, 'MISRA C:2012.'a
43. Automotive Open System Architecture (AUTOSAR), 2013, 'AUTOSAR Classic Platform Release 4.2.'

03

# Operating in the Presence of Faults and Failures

During developmental operations, the Mission Specialist is always alerted to failures necessitating the resumption of manual driving and also can at any time override even the system fault response by reverting the vehicle to manually-controlled driving.

## Fault Injection Training

During Fault Injection Training (FIT), trainers inject faults into the system so trainees can safely gain exposure to the vehicle's behavior in a variety of fault situations. This module takes place on a test track and has three parts:

- **Basic FIT —** exposes trainees to in-vehicle faults without the added complexity of environmental factors or outside actors and establishes a baseline reaction time for the trainee up to the maximum system capability, independent of context or environment. This module covers correct mechanics such as touch grip and pedal shadowing, vehicle controllers, and scenarios that can lead to faults or situations where these faults may become problematic.
- **Self-Driving FIT —** exposes trainees to the faults covered in the basic FIT module with the addition of environmental factors. For example, trainees will experience system faults in test-track intersections, before intersections, just after intersections, in turns, and on straightaways.
- **ODD Scenario FIT —** focuses on environmental fault initiators or actors and scenarios that are currently out of scope for the self-driving system and will therefore require that the Mission Specialist take over, e.g., complete lane blockages.

# 5.3 → Principle 03 Continuously Improving

Any anomaly that could affect the safety of the Self-Driving Vehicle is identified, evaluated, and resolved with appropriate corrective and preventative actions.

# 01 Supporting Concepts

→ An **anomaly** is an undesirable and unexpected behavior or result.[44] We are attentive to these kinds of events as warning signs of potential safety issues before they result in harm.

→ We implement processes and mechanisms to **consistently capture** and assess the risk of observed issues so that we can determine the potential impact of these issues on continued safe operation.

→ In response to an identified anomaly, we **determine and execute an appropriate corrective action**. This may include, e.g., implementing a hardware or software fix, changing operational procedures temporarily or revising them permanently, or determining that, while unexpected, the observation does not indicate an underlying safety risk.

To fulfill this principle, we draw on quality processes for software development and hardware component production. We have implemented and refined workflows for collecting and analyzing test results from both offline and track testing, as well as on-road driving. From concept design to public road testing, our vehicles and self-driving system components pass through manufacturing and commissioning tests. We run a series of standardized tests on each software release, and leverage standardized documentation and issue tracking tools to effectively capture learnings and see them through to a resolution. We also leverage Mission Specialists' feedback in addition to automated results. All these measures facilitate the identification, capture, and resolution of anomalies and deficiencies as early as possible, before a harmful event can occur.

44. Consistent with anomaly (1.2) definition in ISO, 2018, 'ISO 26262 Functional Safety for Road Vehicles.'

02

# Internal Safety Concern Reporting System

Within the framework of our Organizational Safety Management approach and our commitment to continuously improve the self-driving enterprise and how we work, we have an internal safety concern reporting system designed to collect valuable feedback, discover hazards or possible safety risks, analyze systematic issues, and institute solutions and improvements. We regularly encourage our employees to raise awareness of concerns or opportunities for improvement that have the potential to enhance the safety of our self-driving operations.

This approach aligns with the concept of just culture, a philosophy that encourages organizations to perform fair investigations, review processes, procedures, and training objectively and allow employees to openly communicate without fear of reprisal. Uber ATG's just culture policies empower managers to focus on holistic organizational factors instead of individual human errors.

The Safety Concern Reporting System provides a clear mechanism for reporting potential safety issues to the Safety Department by any employee, contractor, or vendor at Uber ATG regardless of level or tenure. Concerns can also be reported to a lead, manager, or supervisor on duty, encouraging open and transparent communication throughout the organization.

No punitive action will be taken against the reporter simply for the fact of reporting a safety concern. Each concern is taken seriously and assessed for potential safety risk, analyzed, reviewed, and resolved with appropriate corrective actions. Metrics on the usage of the safety concern reporting system, key findings and organizational trends are regularly presented to and reviewed by senior leadership and where appropriate, systemic fixes are instituted. Additionally we continually promote the reporting system to raise awareness around a proactive safety culture to the entire organization.

# 03 Safety Risk Identification and Resolution

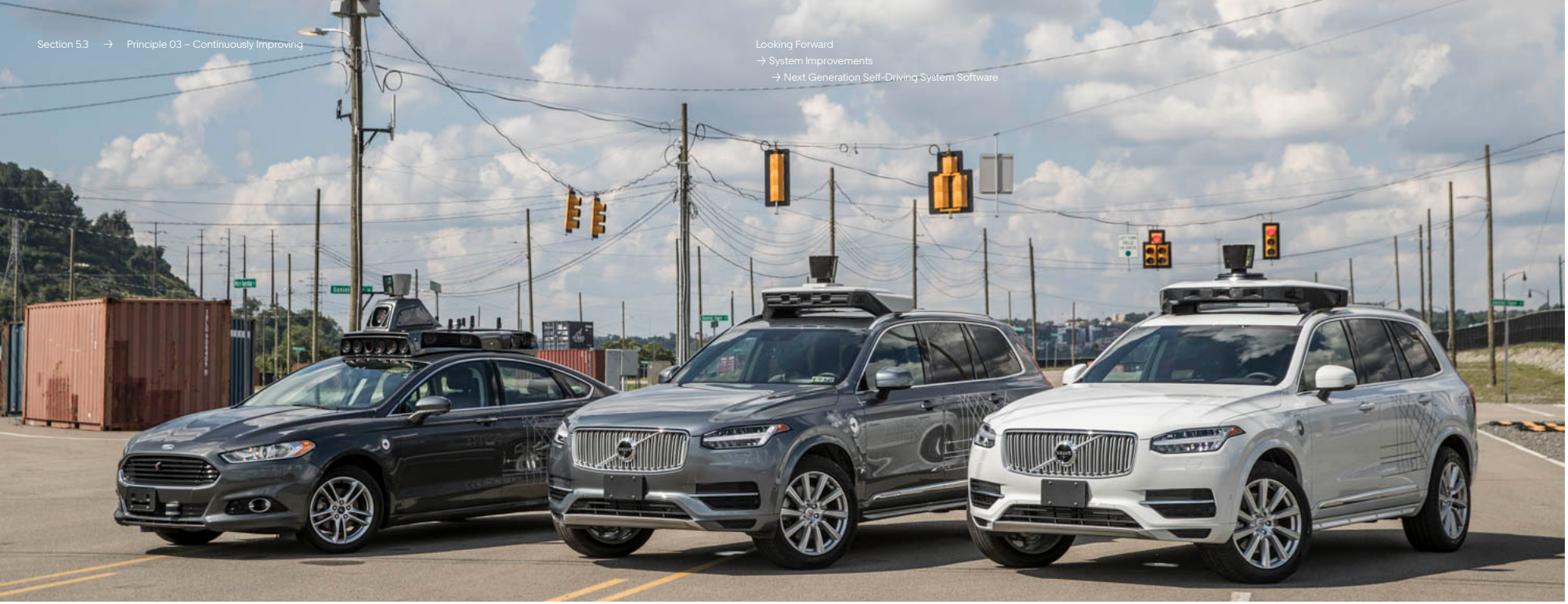
Uber ATG has institutionalized resources for the systematic identification and resolution of safety risks.

We work continuously to reduce risk whenever possible by identifying risks before they could result in harm to people or property. This is performed as part of our Safety Risk Management activities and is initiated on both a routine basis and in response to specific circumstances, and specifically prior to authorizing new (or changes to) operational configurations. We continually scan and monitor the organization's development, testing and operational activities in order to proactively identify risk analysis triggers throughout the organization. The end product is a Risk-Rating that is assigned to the appropriate leadership level to ensure timely decision-making as well as accountability, and as appropriate, create mitigations to reduce risk to As Low as Reasonably Practicable (ALARP).

Identifying causal factors of safety risks is only part of the solution; therefore, we also actively track safety risk control implementation and continuously monitor effectiveness. Changes in effectiveness of any safety risk control would trigger the Safety Risk Management process to begin again on that particular risk. Risks are reviewed by relevant stakeholders when initially identified and assessed, and kept in an active safety risk register to support socialization and review.

# 04 Looking Forward

While this report primarily focuses on where we are today, it is grounded in a greater context of where we anticipate heading. Our approaches, design features, and procedures discussed within are focused on our current capabilities and developmental process, accepting that we are always in pursuit of continuous improvement. This not only contextualizes our development processes and methodologies, but provides a clearer picture of the possible road ahead and path to scale. This “Looking Forward” section provides future-facing plans and potential evolutions.



# System Improvements

## Next Generation Self-Driving System Software

At Uber ATG, the software that enables our self-driving enterprise continues to evolve. We invest in improvements to all software segments of our self-driving enterprise, including onboard software (e.g., detector algorithms), offboard software (e.g., training data and labeling), and the software platform that enables the Uber transportation network to interface with self-driving vehicles belonging to Uber ATG and its business partners. The following are noteworthy features being developed with the goal of improving the performance and integrity of the software running on our self-driving system.

### Improved Maps and Embedded Data

In addition to the ongoing work done to generate and maintain the high-definition maps used by our self-driving system today, Uber ATG is developing its next generation maps software for improved performance on the road. This new maps software is designed to enable increasingly natural motion planning of our own vehicle by leveraging rich data on the mapped environment such as historical driving behavior and gives specific driving paths that are less dependent on road surface boundaries alone.

Looking Forward
→ System Improvements
→ Next Generation Self-Driving System Hardware
→ Mission Specialists
→ First Responder Guide



### Next Generation Self-Driving System Hardware

In addition to the elements described on the prior page, the next generation of our self-driving vehicles may include expanded sensing modalities as explained below. We expect these sensor improvements serve to increase our system's flexibility and its ability to detect and classify actors under an expanded range of conditions and in a greater number of scenarios.

- **Improved LIDAR Performance →** For our next-generation sensor suite, we are evaluating possible upgrades for top-mounted LIDAR hardware capable of higher-resolution sensing at increased range. This could improve sensing performance while driving at elevated speeds, operating in crowded or complex environments, and during advanced maneuvers.
- **Additional LIDAR Units →** We are also evaluating inclusion of additional LIDAR units intended to improve near-field sensor coverage over the single top-mounted LIDAR unit.

## Mission Specialists

As the performance of the self-driving system increases, the frequency of the need for intervention from a Mission Specialist would likely decrease — a dynamic that may raise its own challenges. We appreciate the importance of mitigating this risk and intend, going forward, to continue studying human factors, effective assistive measures, and overall support structures for safe, self-driving vehicle operations.

## First Responder Guide

Uber ATG is aware of the key role played by Public Safety Officials (including law enforcement, fire and rescue officials, emergency medical technicians, etc.) in the cities in which we operate. Self-driving technology has the potential to assist in the performance of these important duties; in the short term, we take seriously the imperative to seamlessly integrate our operations into cities so as not to disrupt Public Safety Official activities. With this in mind, Uber ATG has published an initial guide to assist Public Safety Officials with their interactions with Uber ATG self-driving vehicles,[45] should they encounter such vehicles in performing their duties. The current version of the guide is scoped to support Uber ATG's self-driving testing with Mission Specialists. Uber ATG is actively involved in the development of the forthcoming industry best practice from the Automated Vehicle Safety Consortium: "AVSC Best Practice for First Responder Interactions with Fleet-Managed ADS-DVs." We are committed to making subsequent versions of our guide available to address new or emerging guidance for emergency response protocols or interactions with new base vehicles platforms and/or driverless self-driving vehicles.

45. Uber ATG, 2019, 'Public Safety Officials and First Responders' Guide.'



## Rider Experience

Rider trust is key to the successful adoption of self-driving vehicles. At this stage in our development process, where members of the public are not riding in our self-driving vehicles, our primary rider experience goal is to build and maintain trust.

As we continue to develop our rider experience, we are focused on assessing the following types of functionality:

- **Transparency** → When a rider enters the vehicle, we are assessing different mechanisms (such as providing a touchscreen tablet in the backseat) to welcome them, and show the vehicle's route. During the ride, we envision enabling the rider to monitor trip progress.
- **Control** → When requesting a ride, we envision notifying a rider that they have been matched with a self-driving vehicle and give them the ability to opt out. We then envision allowing the rider to request a stop at any time using controls on the backseat touchscreen. When a stop is requested, we envision having the vehicle stop when and where it is acceptably safe and responsible to do so.
- **Comfort** → In addition to following the rules of the road, we envision our self-driving vehicles providing a comfortable rate of acceleration and avoiding unnecessary harsh braking.

# Remote Assistance

Current operations rely on Mission Specialists in the vehicle to navigate a variety of real-world scenarios that our self-driving vehicles cannot fully yet handle by themselves. In the future when our self-driving vehicles do not have Mission Specialists in the vehicle, riders may need advice on accessing the vehicle, they may require remote reminders about adhering to in-vehicle policies and local laws, or require assistance in the event of an emergency. Additionally, the self-driving vehicle itself may encounter scenarios that can safely be navigated if provided more information from a remote human assistant. We are developing a Remote Assistance system to facilitate some of these anticipated needs and to maintain appropriate levels of communication with riders.

## Select Considerations of the Remote Assistance System

- **Fail-Safe** → The self-driving vehicle is responsible for real-time safety; it needs to maintain safe and compliant operation in the absence of the Remote Assistance system. Specifically, the self-driving vehicle is responsible for incorporating human guidance from the remote operator while always preserving the ability to reject unsafe commands. The remote operator will additionally not be given tools to put the vehicle in a state where the autonomy system would be compromised or disabled (e.g., commanding open loop motion paths).
- **Dedicated Tools and trained Operators** → Each Remote Assistance session will require its own unique set of tools (and actions) to resolve. Not all tools / actions will be presented to the operator in all sessions, and the job of the Remote Assistance system is to determine the relevant tool / action given the scenario.
- **Finite Time Actions** → Actions have a certificate and are only valid for a set period of time, after which (due to comms latency for example) actions are no longer valid. Other use cases may imagine persistent actions (e.g., ground the fleet) but that is outside of the scope of the Remote Assistance system.

## Law Enforcement Interaction

We plan to include system features allowing a Remote Assistant to communicate with actors in the self-driving vehicle's surroundings, such as law enforcement, if needed.

# 5.4 → Principle 04 Resilient

The Self-Driving Vehicle is acceptably safe in case of reasonably foreseeable misuse and unavoidable events.

# 01 Supporting Concepts

→ We anticipate **reasonably foreseeable misuse** – scenarios in which our technology is used counter to its design or purpose – because self-driving vehicles, like any other technology, are subject to an innumerable set of theoretical misuse scenarios.[46]

→ **Mitigation** in the context of misuse involves preventing, protecting, and/or warning against potential harm; mitigatory strategies should be implemented in that order when practicable.[47]

→ Types of **misuse** considered under this principle include remote threats, malicious access to our self-driving computer, and intentional abuse of the self-driving vehicle.

→ There may be situations where a crash is **unavoidable**, or beyond our control, due to the actions of other road users. In this case, we work to minimize the likelihood and severity of harm.

Our self-driving vehicles will not operate in a vacuum. They will encounter all types of road users, including other vehicles, pedestrians, bicyclists, scooters, and more. They will, in the future, pick up and transport real riders, and may serve as a potential target for people with illicit motives. Therefore, we must consider the ways in which our self-driving vehicles could be used or abused beyond what is intended for our product, so we can put in place reasonable protections. These unintended interactions may be infrequently experienced, and they may be intentional or unintentional, but we choose to address them proactively where possible.

46. This is consistent with the retiring of extremely unusual scenarios that is permitted in automotive hazard analysis per Clause 7 of ISO 26262-3:2011, which gives as an example the scenario of a vehicle involved in an incident which includes an aeroplane landing on a highway (see Annex B.3). See ISO, 2011, 'ISO 26262 Functional Safety for Road Vehicles.'

47. This is consistent with guidance of §174 of the European Commission's (EC's) Guide to Application of the Machinery Directive 2006/42/EC. See EC European Agency for Safety and Health at Work, 2010, 'Guide to application of the Machinery Directive 2006/42/EC.'

Misuse scenarios undergo a risk analysis to determine the likelihood of occurrence and severity of possible outcome(s). Reasonably foreseeable misuse focuses on human action, which cannot be fully characterized or controlled due to the complexity of human behavior. For this reason, we have tailored the risk schema from ISO 26262[48] and the U.S. Department of Defense (DOD) MIL-STD-882[49] to triage our initially discovered misuse scenarios. High-risk scenarios are scenarios very likely to occur and resulting in a high-severity outcome.

To fulfill this principle, we undertake a systematic process to:

- **Identify potential sources of potential misuse, from riders to other road users or would-be cyber intruders, and generate a register of possible misuse scenarios.** → We undertake various efforts to hypothesize possible misuse scenarios. Drawing on this research, we define actors and vehicle 'moments,' or points in time, during the vehicle's lifecycle, e.g., picking up or dropping off riders. We envision that the number of misuse scenarios may grow over time, so this analysis is continuous; however, by defining the actors and moments, we can take a systematic approach to defining the different permutations of interactions.
- **Assess the inherent risk, identify potential mitigations, and validate the effectiveness of our mitigations.** → Once a misuse scenario has gone through risk analysis, we design and implement an appropriate mitigation to minimize the likelihood of the misuse and severity of the possible outcome(s). In cases where risk cannot, as a practical matter, be eliminated completely based on reasonable mitigations, we aim to deter harmful human behavior, prevent a severe outcome, and/or put in place clear response policies. All mitigations go through a verification and validation process intended to continuously improve our identification and resolution of foreseeable misuse scenarios.

48. ISO, 2018, 'ISO 26262 Functional Safety for Road Vehicles.'
49. U.S. DOD, 2012, 'MIL-STD-882E System Safety.'

02

# Crashworthiness and Crash Avoidance

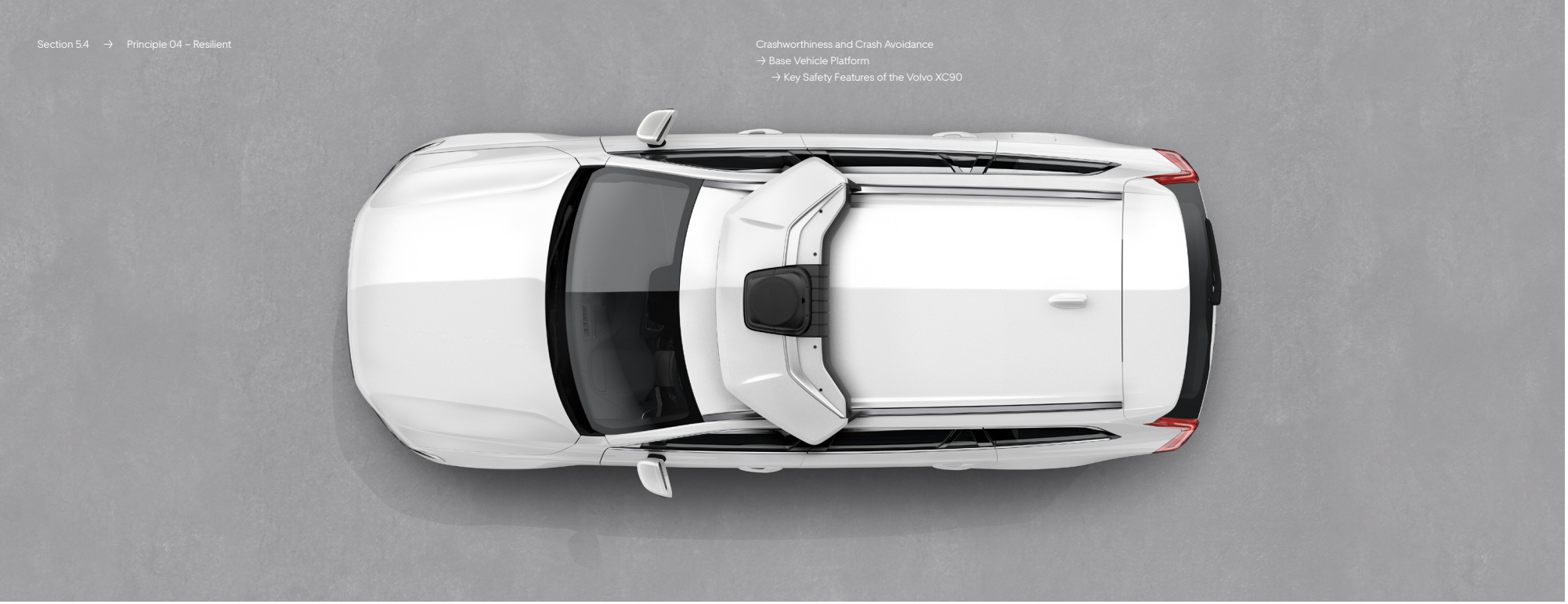
## Base Vehicle Platform

Crashworthiness of the base vehicle platform is an important selection criterion when choosing OEM partners and specific vehicle platforms. Crashworthiness of the base vehicle is defined by the vehicle structure, occupant restraint systems, and other factors. Uber ATG selects vehicle platforms with a strong track record of safety and high marks in passive safety testing by independent ratings agencies.

All the vehicles in Uber ATG's current fleet are recent model-year Volvo XC90 sport-utility vehicles, upfitted with sensors and our self-driving technology. The XC90 has been recognized as one of the safest vehicles in the world.[50, 51] In 2017 and 2019 the Volvo XC90 was an Insurance Institute for Highway Safety (IIHS) Top Safety Pick.[52]

Volvo supplies current generation vehicles to Uber ATG that serve as the base for our self-driving technology. To preserve the strong safety benefits of the Volvo XC90, we preserve vehicle crashworthiness features. Prior to Uber ATG's purchase, Volvo has certified these vehicles as meeting relevant Federal Motor Vehicle Safety Standards (FMVSS), including those covering crashworthiness. These FMVSS provide an important crashworthiness foundation for all vehicles.

50. Volvo Car Group, 2016, 'Volvo XC90 wins North American Truck of the Year – again.'
51. Automotive World, 2018, 'Volvo XC90 is a genuine life-saver.'
52. IIHS, ND, '2017 Volvo XC90.'



## Key Safety Features of the Volvo XC90[53]

These features are available on both our current and future generation vehicles.

- **City Safety Automatic Emergency Braking (FCW +AEB) System** → The City Safety system is a diverse sensing and compute software system which operates independently of Uber ATG's self-driving system. This driver assistance system provides support to the Missions Specialists by providing forward collision warnings (FCW) and potentially brake actuation depending on the Mission Specialist's response. The City Safety system includes a forward facing radar, camera, and Electronic Control Unit (ECU). The XC90's underlying AEB system is enabled and active while the Mission Specialist pilots the vehicle during both manual driving and supervised self-driving operations.
- **Anti-Lock Braking System (ABS)** → The ABS helps to improve vehicle control during braking by automatically modulating to help prevent lockup.
- **Electronic Stability Control (ESC)** → ESC consists of traction control, spin control, active yaw control, and engine drag control. It helps to reduce wheel spin, counteract skidding, and improve directional stability.
- **Seatbelts with Pre-tensioners and Load Limiters** → Pre-tensioners tighten safety belts in the event of a collision and load limiters minimize belt-inflicted injury.
- **Driver and Passenger Front and Side Curtain Airbags** → Airbags deploy in the event of collision to reduce the likelihood of injury of vehicle occupants.

53. Volvo Car Group, ND, 'Volvo XC90 Features.'

## Self-Driving System Hardware Integration

At Uber ATG, we add sensors, wiring, and computers to the base vehicle to enable the functionality of our self-driving system. We evaluate these modifications to minimize interference with the native Volvo safety equipment, and work closely with Volvo to avoid inconsistencies or incompatibilities. Modifications to the base vehicle are designed to preserve and/or enhance safety and structural integrity to minimize risk, including risk to passengers, in the event of a crash.

- **Sensor Wing →** The sensor wing is mounted to the roof using modified roof rails.
- **High Voltage Wiring →** Additional high voltage wiring is integrated into the base vehicle to power the self-driving computer and other devices. These cables are routed behind fixed interior panels to make them inaccessible to passengers, and wiring assemblies include high voltage interlock protection to minimize the risk of electric shock to passengers, first responders,[54] or others that may come into contact with the vehicle in event of a crash.
- **Low Voltage Wiring and Sensor Cleaning Tubing →** Low voltage wiring and other tubing has been added to the vehicle to connect the sensor wing to the self-driving computer and fluid and air compressors. Routing pathways through the vehicle have been selected in order to minimize risk of degrading crash-protection functions.
- **Self-Driving Computer →** The size of the current-generation self-driving computer has been greatly reduced (to roughly the profile of a medium-sized suitcase), and thermal management has become significantly more efficient. These improvements allow us to house the self-driving computer beneath a tamper-resistant, load-bearing floor in the trunk space of the vehicle.

## Post-Crash System Behavior

In the event of a collision, the Volvo XC90 base vehicle's post-impact safety features will continue to function as expected and may perform a variety of actions depending on the type and severity of the collision detected, including:

- **Passive Safety Features Activation →** Deploys front and side curtain airbags, activates seat belt tensioners, and automatically unlocks doors.
- **Safety Mode Activation →** Reduces vehicle functionality when any of the vehicle's vital functions may have been damaged in a collision. When activated, a warning may be shown on the dashboard with the message "Safety mode See Owner's manual."[55]
- **Post-Impact Braking →** Brings the vehicle to a controlled stop after the collision to avoid the vehicle entering the path of other vehicles.
- **Hazard Lights Illumination →** Warns other approaching drivers of the potential hazard.
- **High-Voltage Battery Disconnection →** Disconnects the high-voltage battery to minimize risk of electric shock to passengers and first responders. Should the collision result in the automatic disconnection of the high-voltage battery, the self-driving system will also lose power within 30 seconds.
- **Fuel Supply Disconnection →** Disconnects the fuel supply to the engine.

54. Uber ATG, 2019, 'Public Safety Officials and First Responders' Guide.'
55. Volvo Cars, 2018, 'Safety Mode.'

03

# Mission Specialists' Role in Incident Response

As part of their training, Mission Specialists undergo incident response training on how to appropriately respond after an incident and engage with emergency personnel. Where it is safe to do so, the Mission Specialist remains with the vehicle post-crash to provide reasonable assistance to involved parties, including law enforcement and first responders.

04

# First Responders Guidance

Working with public safety officials and first responders is an important part of how we connect with the communities in which we operate. Our Public Safety Officials and First Responders' Guide[56] provides information to trained public safety officials and first responders on how to safely interact with an Uber ATG developmental self-driving vehicle in the event of an emergency.

Mission Specialists undergo training that prepares them to respond to scenarios such as those involving emergency vehicles, manually-directed traffic, and routine traffic stops. They also undergo incident response training that prepares them to respond following an incident, including engagement with emergency personnel.

The guide is intended to complement the information found in this report, referencing post-crash safety features of the XC90 and methods for identifying system state. It also introduces information to be specifically mindful of in emergency response situations, e.g., locations of potentially harmful sources of stored energy such as fuel and high-voltage power, safe vehicle relocation and towing, considerations for incident data preservation. A web-based quick-reference version of the guide is also available, optimized for mobile download and use at the scene of an incident. Uber ATG is committed to engaging with public safety officials and first responders prior to beginning testing in a specific location, providing an opportunity to raise awareness of these materials and review our testing and development processes in greater detail.

While Uber ATG does not anticipate public safety officials or first responders needing to manually disengage, immobilize, or power down the system, familiarity with these protocols will enable first responders to understand the state of the automation system, should the Mission Specialist be unable to act or respond.

56. Uber ATG, 2019, 'Public Safety Officials and First Responders' Guide.'

# 05 Vehicle Cybersecurity

In addition to physical safety scenarios, we also consider and defend against common behaviors of actors seeking to access our systems as well as to alter and/or remove data. Although, during operations, much of the functioning of a self-driving vehicle relies on purely in-vehicle processes, self-driving vehicles (like most modern vehicles) interact across multiple information, network, and hardware domains, thereby giving rise to a number of possible threats from malicious actors.

Uber ATG's current fleet of self-driving vehicles is built on base vehicles designed for human drivers and therefore may contain component-limitations and communication-designs limiting active security measures. Because of these potential limitations, a robust cybersecurity program can further improve a vehicle's security features so as to promote the safe deployment of self-driving vehicles on public roadways. We have incorporated security mechanisms into the self-driving computer, sensor components, our software, and interactions with the base vehicle to reduce daily operating risks as well as in the event of attempted action by an unauthorized party. These security controls are integrated with individual components and incorporated within the platform design to defend against potential threats.

Our cybersecurity approach is informed by best practices described by NHTSA and relevant industry groups, including ISO,[57] SAE International,[58] and the Automotive Information Sharing and Analysis Center (Auto-ISAC).[59] Uber ATG adopts and designs controls with the expectation that high-risk domains (e.g., cellular-adjacent devices) may be occupied or manipulable by malicious actors.

Uber ATG has designed and is employing security-specific principles, controls, and technologies within the self-driving computer, vehicle platform, and network infrastructure as detailed below.

57. ISO 21434, 'ISO/SAE DIS 21434 [SAE] Road vehicles — Cybersecurity engineering'
58. SAE, 2012, 'Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061.'
59. Auto-ISAC, 2015, 'Best practices.'

## Key Hardware Security Controls

### Key Management

The Uber ATG self-driving vehicle utilizes cryptographic primitives to establish trust with remote entities and enable trusted execution. In order to securely manage these cryptographic primitives, we incorporated hardware security modules within various security domains on the vehicle platform.

### Functional Separation

The vehicle, sensors, and compute platform are designed to have distinct communication domains which separate a sensor, device, computer, or remote service operating within the larger system. Strongly-controlled security domains help, for example, to isolate certain components from motion-control devices. Some security domains on the vehicle are protected through physical means.

### Secure Networking Devices

Onboard, we have implemented redundant hardware and support for multiple network and cellular providers. Offboard, the vehicle's cellular modems and the Uber network terminus systems each have network-layer and hardware security devices and controls to help isolate these components from other on-vehicle and datacenter components. Vehicle messaging is controlled with cryptographic, logical, and policy-based approaches.

## Security Architecture

### Cryptographic Signatures

Autonomy pipelines and many of the motion control devices on Uber ATG's self-driving platform run on execution environments where code is executed only after we have authenticated the code's origin as a trusted source using cryptographic sources of identity. Consistent with cybersecurity best practice,[60, 61] these cryptographic signatures also provide a valuable integrity check by enabling code/firmware verification during updates and prior to execution.

### Mission Specialist and Data Access Control

Autonomous operations involving Mission Specialists on the track and on the road are strictly controlled through security workflows which require multi-factor authentication and functional authorization for specific missions. In certain elevated privilege circumstances, short-lived certificates will be issued after multi-factor user authentication has completed for the specific vehicle that needs to be accessed. This more privileged access generates logs which detail actions taken by the authenticated user or tool.

### Onboard Communication Security

The self-driving computer employs best practice[62] transport layer security when communicating over internal networks. This ensures that critical autonomous decisions are made over integrity- and intercept-protected channels.

### Remote Network Access Policies

A self-driving vehicle needs to be able to communicate with the data center through a secured network. These communications must be resilient to a broad spectrum of attacks relevant to any mobile network. The communication layers employ best practice secure protocols to protect the channel and transmitted data from interception and modification.

60. U.S. Department of Commerce National Institute of Standards and Technology (NIST), 2018, 'Platform Firmware Resiliency Guidelines.'
61. U.S. NIST, 2011, 'BIOS Protection Guidelines.'
62. U.S. NIST, 2019, 'Guidelines for the Selection, Configuration, and Use of Transport Layer Security Implementations.'

## Secure Software Engineering

**Minimizing Attack Surface**

Our vehicle security development policies focus on attack surface reduction at every cross-domain interaction layer by requiring specific protocols and API definitions. Protocol-level controls inform the additional security constructs required within each domain and between domains. We employ various techniques to manage risk exposed by security domains that include inherently risky protocols.

**Adversarial Simulation**

The vehicle security team collaborates internally and with our partners to identify, document, and remediate weaknesses in hardware, software, protocols, APIs, and overall platform risks. These simulations and reviews are designed to evaluate the interactions of components at a platform level, identify any weaknesses associated with their incorporation, and evaluate platform security features and components. We document and evaluate risks to the vehicle platform and self-driving computer in order to recommend security improvements to individual components and improve platform-level security controls.

**→ Looking Forward**

Like others in the industry and in other industries seeking continuous improvement in managing cybersecurity threats, we continue to explore and invest in developing improvements for the security mechanisms, policies, and components described above. In collaboration with our partners, we are incorporating security improvements across the vehicle platform and are dedicated to pushing new security features into components to improve the security posture for future self-driving vehicles across the industry. This research is undertaken in connection with both hardware and software security.

Data Handling
→ Data Recording
→ Data Types
→ Data Logging and Storage



06

# Data Handling

## Data Recording

Our self-driving vehicles capture significant quantities of environmental and systems data during every second of operations. We use this high-resolution data in a number of ways, including system performance analysis, quality assurance, machine learning and testing, simulated environment creation and validation, software development, human operator training and report, map building, and validation.

## Data Types

Our self-driving vehicles record an array of data types, including telemetry, control signals, vehicle platform messages, system health (e.g., hard drive speeds, internal network performance, and computer temperatures), as well as sensor and camera data.

## Data Logging and Storage

This data is captured in real-time on the vehicle and then, after the conclusion of an operation, offloaded to our data centers for storage, cataloging, review, and labelling. We are developing onboard data storage with reliability and resilience in mind.

We verify each vehicle's data-logging capabilities and storage sufficiency before operation. Where appropriate and without risking existing stored data, the onboard storage volumes perform continuous self-reports, including monitoring read/write errors and disk fault detection.

In addition to data logged by the vehicle Event Data Recorder (EDR), all relevant logging modes in our system provide a baseline of data to assist in potential crash reconstruction.[63]

All vehicles are equipped with a backup battery to improve the system's ability to log data in the event of a crash. In the event of power failure, data is logged to solid state hard drives so as to facilitate data being written out of cache and onto non-volatile storage.

Uber ATG is reviewing the SAE J3197 Recommended Practice for Automated Driving System Data Logger.[64] This recommended practice identifies and defines data elements in order to assist in understanding the background and events leading up to a self-driving vehicle related crash.

63. Cf., NHTSA, 2017, 'Automated Driving Systems 2.0: A Vision for Safety.'

64. SAE, 2020, 'Surface Vehicle Recommended Practice: Automated Driving System Data Logger J3197.'

## Data Transmission

In addition to our regular onboard storage and the EDR, vehicles transmit a small amount of data Over-the-Air (OTA) to Uber ATG servers to provide real-time insights into how our vehicles are performing, where they are, and their current system state. This OTA communication is also used to provide the vehicle and its operators the information they need for their current mission. OTA transmissions are not required for safe operation of an Uber ATG self-driving vehicle, but these transmissions do assist in a variety of development and operational functions.

Data transmitted OTA may also be logged to onboard storage for later use. Our vehicles support multiple cellular providers in order to improve resilience and facilitate access to carrier networks as required for operations.

**→ Looking Forward**

For our current self-driving vehicles, vehicle power is shut off shortly after an impact. We are exploring the development of capabilities to offload emergency data using battery backup cellular devices to transmit certain telematics and other relevant data.

# 5.5 → Principle 05 Trustworthy

The Self-Driving Enterprise is trustworthy.

# 01 Supporting Concepts

- → Uber ATG's stakeholders must have confidence in the quality and safety of our products. Our stakeholders include riders, regulators, and legislators, along with all people with whom we share public roads and organizations that advocate on their behalf.
- → Taking steps to inform the public about our approach to safety and how we are working on self-driving vehicles is necessary and important for building trust. Uber ATG is actively consulting and partnering with stakeholders to understand their needs, and to continuously improve our approaches to best reflect this broader set of interests.
- → We believe that we cannot simply provide descriptions of the safety performance of our systems. We are committed to employing various methods to **provide evidence of safety performance**.

We recognize the importance of earning the trust and confidence of both the public and various levels of government in support of successful development and deployment of self-driving vehicles. We are committed to earning and maintaining that trust with our stakeholders — riders, government officials and policymakers, non-governmental advocacy and interest groups, industry, partners, employees, and the general public, which includes riders, drivers, and couriers on the Uber platform.

We believe that the most effective approach to building trust is to provide regular, consistent, accessible information on our development efforts, business plans, and the potential impacts of our operations on local communities where we operate. We want our stakeholders to have high-quality information on the technology in order to make informed decisions about the use and regulation of self-driving vehicles. The detail provided through this report represents one mechanism to supply such information. We also inform stakeholders through resources such as our open-sourced Safety Case Framework and Public Safety Officials and First Responders' Guide, both discussed above. With the introduction of Uber ATG's Safety Management System, we discuss how we design safety risk management into the way we work, follow through, and assure an effective outcome.

02

# Safety Promotion at Uber ATG

Uber ATG is committed to keeping all employees informed and engaged on matters of Safety. We value open, transparent, and regular communication with all levels of our staff with the end goal of increasing awareness around company safety policies, objectives, and processes.

On a routine basis, the organization provides promotional and educational material on safety, such as presentations from safety leadership (including during new-hire orientation and organization-wide town hall events), showcasing safety metrics or processes through bulletins or alerts, distribution of a monthly safety newsletter, and immersive employee events, campaigns, and workshops around safety concepts. A dedicated Learning and Development specialist was hired to develop an SMS training curriculum and education for all levels of the organization. The launch of SMS training efforts is currently underway.

Alongside these important aspects of internal communication, Uber ATG is committed to keeping our external stakeholders informed on our safety program and have released safety related information into the public domain including, but not limited to, Uber ATG's Safety Reports, its Safety Case Framework for Self-Driving, its Public Safety Officials and First Responders' Guide, various publications describing our safety programs, and participation in voluntary industry standards consortia.

03

# Self-Driving Safety and Responsibility Advisory Board

Uber ATG has established an external safety advisory board comprised of independent experts to provide objective reviews of and input onto aspects of our self-driving program. The Safety and Responsibility Advisory (SARA) Board is charged with reviewing, advising, and suggesting changes to Uber ATG's self-driving enterprise, including inputs on organizational goals and priorities. This panel of outside experts offer valuable independent advice as Uber ATG leads the safe development and deployment of self-driving technology on the Uber platform.

The SARA Board consists of recognized experts in a variety of relevant fields, drawing from aviation safety, insurance, emergency/trauma medicine, automotive safety, and academia. The SARA Board meets every quarter and its role is to identify and suggest improvements to the way Uber ATG develops self-driving technology and brings fully self-driving vehicles to market. Relevant SARA Board topics include:

- Internal policies, culture, operational procedures, and processes;
- Potential risks and corresponding follow-up actions;
- Ways to increase public understanding and trust in self-driving vehicles; and
- Uber ATG's approach to engaging in industry-wide conversation around relevant topics such as fully driverless operations and responsibility.

# 04 Independent Experts

We believe that engaging independent experts to review our safety approaches and performance is essential to our learning and development. These third-party reviews can also provide additional confidence to our customers, government officials, and others while self-driving technology is in development.

We have already undertaken a number of external reviews, including a 2018 review of Uber ATG's safety culture by a team of external experts, which included a former chairman of the National Transportation Safety Board. We intend to prioritize these kinds of reviews and look to share the results when appropriate.

We expect that, in certain instances, these independent reviews would consider particular elements of our safety approach, rather than assess our entire system for safe performance. This approach allows us to prioritize review efforts and engage experts with specific expertise and competence in particular areas. Additional information can be found in our **Uber ATG Safety Report Supplement: Internal and External Safety Reviews**.[65]

65. Uber ATG, 2018, 'Uber ATG Safety Report Supplement Internal and External Safety Reviews.'

# 05 Role of Industry Standards

Uber ATG has reviewed the best-practices and standards of other safety-critical industries and the existing automotive standards as well as U.S. DOT guidance in Preparing for the Future of Transportation: Automated Vehicles 3.0[66] and Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0[67] to identify those relevant to our system and operations. To ensure there are no gaps in coverage, we have external experts conducting a review and assessment of our findings. For those relevant best practices and standards, we are in the process of reviewing, interpreting and applying them across our organization. We do not intend to enumerate each and every one of those documents here; however, they can be summarized by the following categories:

- System Safety
- Operational Design Domain
- Object and Event Detection and Response
- Fallback (Minimal Risk Condition)
- Validation Methods
- Human-Machine Interface
- Vehicle Cybersecurity
- Crashworthiness
- Post-Crash ADS Behavior
- Data Recording
- Consumer Education and Training
- Testing
- Communications

As these technologies advance the self-driving industry is focused on collaborative technical efforts to rapidly develop and publish consensus best practices and standards to drive the safe development and deployment of the technology. Uber ATG is an active participant in multiple industry efforts to establish these best practices and standards. We have also engaged external support to assess the numerous standards development activities in a rapidly changing landscape and make recommendations regarding Uber ATG participation in these activities.

66. USDOT, 2018, 'Preparing for the Future of Transportation: Automated Vehicles 3.0'
67. USDOT, 2020, 'Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0'

06

# Safety Performance Metrics

We are developing a framework of subsystem and system level performance metrics to measure the safety of our self-driving vehicles in development, testing and deployment. We are collaborating with researchers, standards development organizations and industry partners to establish this set of safety performance metrics and clearly demonstrate their relationship to the overall safety of the self-driving vehicle in operations.

Throughout the industry, a number of system level metrics have been utilized by self-driving pilot program designers and self-driving developers as indicators of progress in development. In our view, overemphasis on some of these metrics may create unintended incentives and/or be applied and defined inconsistently across developers. Even those metrics that are applied consistently within the efforts of an individual developer and may provide some useful information on improvement over time, they may additionally be ill-suited for objective, cross-developer safety metrics in deployment.[68]

In continuing to develop meaningful and reliable metrics, we look to align each metric to at least one of our safety principles to ensure that they:

1. Minimize unintended incentives AND
2. Are representative of system-level performance

This alignment also allows for a clear picture of metrics applicability across all internal technical programs.

68. Fraade-Blanar, Blumenthal, Anderson, & Kalra, RAND Corporation, 2018, 'Measuring Automated Vehicle Safety: Forging a Framework.'

# 07 Privacy Considerations

Uber and Uber ATG are committed to being trusted stewards of our users' and employees' personal data. Uber's Privacy team — which consists of privacy professionals from Uber's legal, engineering, policy and communications departments — drive this commitment by ensuring that privacy and data security are considered throughout and built into Uber's product development process, that our privacy practices are clearly communicated in our Privacy Notice and elsewhere, and that individuals can exercise rights and choices with respect to their personal data.

Uber and Uber ATG also work hard to balance this commitment to privacy with the needs of law enforcement relating to criminal or other investigations. We have established a rigorous but efficient process for law enforcement to request relevant information. Such requests are closely reviewed by a dedicated team of employees trained to respond to such requests in a manner consistent with Uber's internal policies and applicable laws. For detailed information, please see our guidelines for law enforcement in the U.S. and outside of the U.S.

Regulators in the countries and cities where Uber operates often require certain data to perform oversight. We work with such regulators to provide any necessary data in a safe and secure manner that respects our users' privacy while enabling regulators to perform their duties. Such disclosures are described to users in our Privacy Notice, and our Transparency Report provides detailed information on our reporting requirements in the U.S. and Canada. We first launched this report in April 2016, and have updated it every year since then.

08

# Public Engagement

At Uber ATG, we believe in proactively and voluntarily sharing information about our technology and safety approach. We work to inform all levels of government, including law enforcement, about our development and both existing and intended operations in the public space. Our commitment to transparency and engagement with the public and with future customers drives us to publicly share information about our operations in current and planned cities through accessible channels such as our website, local meetings and events, and media posts.

## Consumer Education and Training

At Uber ATG, we proactively seek to educate consumers and stakeholders on safety features and interaction with self-driving vehicles through a number of channels, including blog posts and direct exposure to our self-driving vehicles. We intend to use these channels to explain the technology underlying our self-driving system and relay first-hand accounts of the rider experience. Additionally, we inform and engage with the communities where we operate by organizing community events, holding town hall sessions, providing notices of operation, and collecting feedback. Through proactive information-sharing and ongoing two-way dialogue that takes external views into account, we can both educate and learn from our stakeholders and others in the self-driving community.

## Voluntary Safety Self-Reporting

We believe that the voluntary safety report is an important platform for self-driving technology developers to communicate consistently and regularly regarding progress in development, remaining challenges, and plans for deployment.

This safety report is part of a series of regular updates, released at key points of transition and development of our self-driving system.

Where useful, Uber ATG makes available information beyond the scope of the safety report for the benefit of the industry and public, such as in the case of the information released for USDOT public docket NHTSA-2019-0036.[69]

69. NHTSA, 2019, NHTSA-2019-0036 'Removing Regulatory Barriers for Automatic Driving Systems.'

09

# Third-Party Safety Program

Uber ATG envisions a future in which the Uber network comprises a hybridized fleet of human Drivers, along with Uber's own self-driving vehicles and those developed and operated by third-parties, to provide diverse and reliable service to our customers. Uber ATG is preparing to bring self-driving technology to the world by making available rides with other developers' self-driving vehicles through the Uber network. As part of this effort, we are developing resources to enable potential third-party partners to share and verify their approach to safety so as to help responsibly onboard their self-driving vehicles to the Uber transportation network. The frameworks, policies, and procedures of our third-party safety program leverage the same Safety Principles represented in our Safety Case Framework to promote a safe self-driving enterprise during development and into the future.

# Disclaimer

This report, including but not limited to information contained in the sections labelled **Looking Forward**, contains management's current intentions and expectations for the future, all of which are forward-looking statements. The words "estimate," "plan," “may,” "intend," "expect," "believe," "anticipate," and similar expressions are intended to identify forward-looking statements. Actual results may differ materially from these forward-looking statements due to various factors. There can be no guarantees that forward-looking statements will be true. You should not place undue reliance on forward-looking statements, which speak only as of the date of this release.

# APPX → List of Acronyms

| | |
|---|---|
| Anti-lock Braking System | **ABS** |
| Application Programming Interface | **API** |
| Automated Driving System | **ADS** |
| Automatic Emergency Braking | **AEB** |
| Automotive Information Sharing And Analysis Center | **Auto-ISAC** |
| Automotive Open System Architecture | **AUTOSAR** |
| Electronic Stability Control | **ESC** |
| Electronic Control Unit | **ECU** |
| European Commission | **EC** |
| The European New Car report Programme | **Euro NCAP** |
| Event Data Recorder | **EDR** |
| Fault Injection Training | **FIT** |
| Federal Motor Vehicle Safety Standards | **FMVSS** |
| Forward Collision Warning | **FCW** |
| Global Positioning System | **GPS** |
| Hardware In the Loop | **HIL** |
| Inertial Measurement Units | **IMU** |
| Institute of Electrical and Electronics Engineers | **IEEE** |
| Insurance Institute for Highway Safety | **IIHS** |
| International Civil Aviation Organization | **ICAO** |
| International Organization for Standardization | **ISO** |
| Light Detection And Ranging | **LIDAR** |
| Motor Industry Software Reliability Association (MISRA) | **MISRA** |
| National Aeronautics and Space Administration (NASA) | **NASA** |
| National Safety Council (NSC) | **NSC** |
| Object and Event Detection and Response (OEDR) | **OEDR** |
| Operational Design Domain (ODD) | **ODD** |
| Original Equipment Manufacturer (OEM) | **OEM** |
| Over-the-Air (OTA) | **OTA** |
| Self-Driving Vehicle (SDV) | **SDV** |
| Safety Management System (SMS) | **SMS** |
| Track Verification Testing (TVT) | **TVT** |
| U.S. Department of Defense (DOD) | **DOD** |
| U.S. Department of Transportation (DOT) | **DOT** |
| U.S. Federal Motor Carrier Safety Administration (FMCSA) | **FMCSA** |
| U.S. National Highway Traffic Safety Administration (NHTSA) | **NHTSA** |
| U.S. National Institute of Standards and Technology (NIST) | **NIST** |
| U.S. National Transportation Safety Board (NTSB) | **NTSB** |
| Uber Advanced Technologies Group (Uber ATG) | **Uber ATG** |
| Vehicle Interface Module (VIM) | **VIM** |
| Voluntary Safety Self-Assessment (VSSA) | **VSSA** |

Uber Advanced Technologies Group

2020