VOLUNTARY SAFETY SELF-ASSESSMENT **(VSSA)**

Autonomous Vehicle
Safety Ecosystem

2021

Motional

Table of Contents

Acronyms

ASIL	Automotive Safety Integrity Level
AV	Autonomous Vehicle
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
GPS	Global Positioning System
HARA	Hazard Analysis and Risk Assessment
HIL	Hardware-In-the-Loop
IMU	Inertial Measurement Unit
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LIDAR	LIght Detection and Ranging
NCAP	(European) New Car Assessment Programme
NHTSA	National Highway Traffic Safety Administration
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
TR 68	Singapore's Technical Reference 68 for autonomous vehicles
SAFAD	SAfety First for Automated Driving
SAE	Society of Automotive Engineers International
SDL	Security Development Lifecycle
SIL	Software-In-the-Loop
SOTIF	Safety Of The Intended Functionality
SPICE	Software Process Improvement and Capability dEtermination
STPA	Systems Theoretic Process Analysis
VSSA	Voluntary Safety Self-Assessment

A letter from our CEO, **Karl Iagnemma**

Self-driving technology promises to deliver vast benefits to humanity: increased mobility, more free time, and—most importantly—safer roads and fewer accidents. But the only way to fulfill this promise tomorrow is to invest in the safety of the technology today.

At Motional, we're making self-driving cars a safe, reliable, and accessible reality. We're developing this technology for all people—for families, for commuters, for elderly passengers who need better access to mobility, and for urbanites who want to choose how they move through their cities. We prioritize the safety and security of passengers and the public at every step.

Our safety track record stands out. Our vehicle design, development and testing efforts ensure we're as safe as or safer than human drivers. Our focus on safety has real-world impact, and we're proud to report that we've driven over one million autonomous miles, in challenging city environments around the globe, while maintaining a record of zero at-fault incidents.

Our team is responsible for some of the industry's largest leaps forward, including the first fully-autonomous cross-country drive in the US, the launch of the world's first robotaxi pilot, and operation of the world's most-established public robotaxi fleet. That fleet has provided over 100,000 rides, with 98% of riders awarding their ride a five-star rating. But our public partnership is only one dimension of our fundamental commitment to safety.

We believe that industry collaboration is critical. We co-published "Safety First for Automated Driving," recently released as an official Technical Report of the International Organization for Standardization, as the most comprehensive report to date on how to build, test, and operate self-driving vehicles safely. Motional's Voluntary Safety Self-Assessment is another step in our team's continued emphasis on the safety, verification, and validation of self-driving vehicles.

We believe that safety transcends competition. That's why, in 2019, we launched nuScenes, a first and largest-of-its-kind dataset of challenging scenarios for driverless vehicles to navigate in order to safely engage with their ever-changing road environments. It's also why we made that data freely and publicly available to the research and academic communities, and why we significantly expanded that dataset in September 2020. We're proud of the safety-driven culture of data-sharing that nuScenes catalyzed, with more than ten similar datasets now available from other major industry players.

Our relentless focus on safety is why people trust us and governments partner with us. We'll keep working hard to maintain that trust.

We're Motional, and we're changing how the world moves.

Executive summary

Our approach to autonomous vehicle (AV) safety encompasses a full ecosystem of technologies and interactions with the world around us. In addition to the physical vehicle, this ecosystem includes AV technology, data infrastructure, the operating environment, operation centers, fleet management, AV passengers, and AV operators.

Today's government standards for vehicle safety do not address hazards specifically associated with more complex technologies, such as the driverless systems Motional is developing. As governments work alongside the industry to create new standards to fill this gap, the United States Department of Transportation encourages AV companies to provide a Voluntary Safety Self-Assessment (VSSA) to describe their safety programs to the public. This VSSA describes our comprehensive approach to AV safety in the following areas:

Our guiding safety framework

Built upon underlying safety principles, our safety framework articulates how we conduct AV ecosystem safety activities and evaluate all safety-related evidence. We design our systems using established industry standards for functional safety (from the ISO 26262 standard), and state-of-the-art practices for cybersecurity and safety of the intended functionality (from the ISO 21434 and 21448 standards under development, respectively).

To validate the safety of our AVs, we complement traditional functional safety testing, such as direct component and system testing against requirements, with scenario-based testing and statistical safety testing. Scenario-based testing confirms that our technology safely handles pre-conceived scenarios in simulation and on a closed course. To ensure safe performance in unconceived scenarios, we also conduct extensive, driver-supervised, statistical safety testing on public roads. This method demonstrates that the AV system is, on average, as safe as or safer than human drivers.

Our technology, operations, and processes

This VSSA describes the AV technology and vehicles we use to achieve our safety objectives, the AV operations and processes in place to ensure the safe operation of our self-driving taxis, the cybersecurity measures and data management infrastructure we institute to protect the integrity of our data and public privacy, as well as our efforts to ensure the transparency of our technology and our work to collaborate on safety.

Our commitment to safety and collaboration

With this VSSA, we commit to fulfilling the promise of self-driving technology to simultaneously save lives and increase mobility. We also commit to working closely with lawmakers and regulators to establish best practices for safety, and we continue to contribute to the creation of standards, whitepapers, and technical publications related to AV safety.

About Motional

Headquartered in Boston, Motional has operations in the US and Asia. Motional is a joint venture between Hyundai Motor Group, one of the world's largest vehicle manufacturers, and Aptiv, a global technology leader in advanced safety, electrification, and vehicle connectivity.

Introduction

Introduction

Motional is committed to improving the safety of our roads — and we believe that driverless technology and autonomous vehicles (AVs) will deliver safer roads.

Road safety has improved dramatically in the last century. However, road transportation continues to claim lives at an unacceptable rate: every year, over 1.3 million fatalities occur worldwide [1]. The National Highway Traffic Safety Administration (NHTSA) estimates that human error is the critical reason for 94% of motor vehicle collisions [2].

Motional is committed to improving the safety of our roads, and we believe that driverless technology and autonomous vehicles (AVs)[1] will deliver safer roads. AVs process precise information to make safe driving decisions, and do not suffer from the same risks as distracted drivers or drivers under the influence. Beyond safety, other benefits of AVs include more efficient road and land use [3], more affordable and accessible mobility, and better use of commuting time.

At Motional, we are building SAE Autonomy Level 4 full-stack AV systems[2]. We develop a full ecosystem of technologies to deploy a fleet of self-driving taxis through on-demand mobility networks. This ecosystem includes the AV technology, data infrastructure, operating environment, command center and fleet management, and our passengers and AV operators.

AVs provide enormous potential benefits but also bring unprecedented challenges, including designing safe AVs, and providing the evidence that AVs are safe to operate on public roads.

For traditional automotive technologies (i.e., up to SAE Autonomy Level 2), the human driver is responsible for safe driving. The vehicle manufacturer is primarily responsible for ensuring that the motor vehicle meets applicable safety standards and is free from defects that may pose an unreasonable risk to motor vehicle safety. For more advanced autonomous driving systems (i.e., SAE Autonomy Levels 3–5), the responsibility for safe driving shifts from the human driver to the AV system.

The current set of government automotive standards does not address hazards specifically associated with more complex technologies providing these new, higher SAE Autonomy Levels. Current industry guidelines recommend creating new standards for future AV technologies, and governments are working alongside the industry towards that goal [4] [5]. In the absence of a comprehensive regulatory framework for AV technologies, the United States Department of Transportation has encouraged AV companies to provide a Voluntary Safety Self-Assessment (VSSA) to describe their safety programs to the public [6] [7].

Partly in response to this request, Motional and 10 other automotive technology companies participated in a joint effort to develop an approach for the safe design and testing of AVs, published in a whitepaper entitled "Safety First for Automated Driving" (SAFAD) [5]. The SAFAD collaboration highlights our core belief that we need to achieve safety and trust in our technology together as an industry. We fundamentally believe that road safety is something we need to achieve collectively, not individually, with industry competitors, infrastructure providers, regulators, and the public.

1. In this report, the term AV (also known as self-driving car, self-driving vehicle, driverless car, driverless vehicle, autonomous driving system, highly automated vehicle, highly automated driving system) refers to a driving system consisting of software, hardware, and a vehicle platform that can autonomously perform the driving task without the help of a human driver.

2. Society of Automotive Engineers International (SAE) Autonomy Levels refer to SAEs scale of driving automation. SAE Autonomy Level 2 refers to automated systems in which the driver retains the primary responsibility for the driving task. Level 3 systems may initiate a human intervention upon reaching its functional limit. Level 4 systems perform the driving task in a restricted environment without relying on a human in the vehicle. Level 5 would remove geophysical restrictions [46].

Introduction

The AV ecosystem

This VSSA describes how we apply the SAFAD approach, existing standards and guidance, and novel safety concepts to deliver safe AVs. It covers both our ongoing safety driver–supervised AV testing operations and our approach to the system design and safety validation of a fully self-driving taxi service. Figure 1 defines the stages of development as part of our product roadmap.

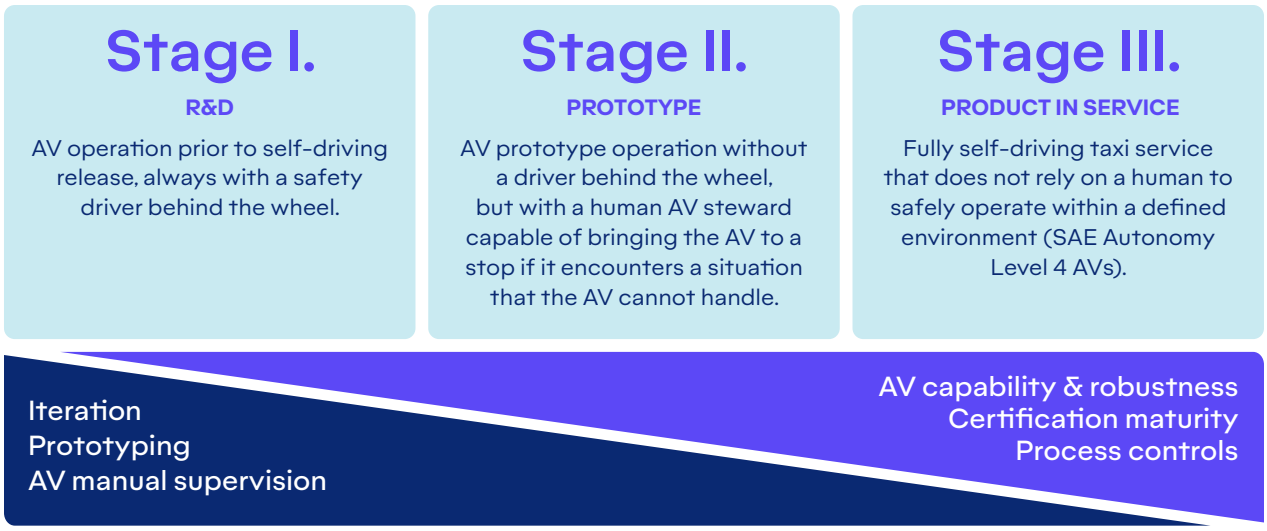
Our approach to designing a safe and robust AV fleet leverages the entire AV ecosystem (see Figure 2). System Safety (chapter 1) applies to the full ecosystem and focuses on:

- Proactively designing a safe system;
- Confirmation through validation testing that the system meets the design's safety requirements; and
- Structured review of documentation and evidence to evaluate and confirm Safety Readiness.

AV technology is at the core of the ecosystem (chapter 2). This technology detects and responds to the outside world through advanced perception, localization, planning, and control systems. Our AV technology includes fallback mechanisms that intervene when individual components fail or encounter rare situations. Our current approach to development involves modifying vehicle hardware to allow the AV technology to operate with an existing passenger vehicle platform. We design these modifications to comply with the same safety performance requirements as existing motor vehicles, including crashworthiness, and safe integration of the vehicle platforms and AV technologies.

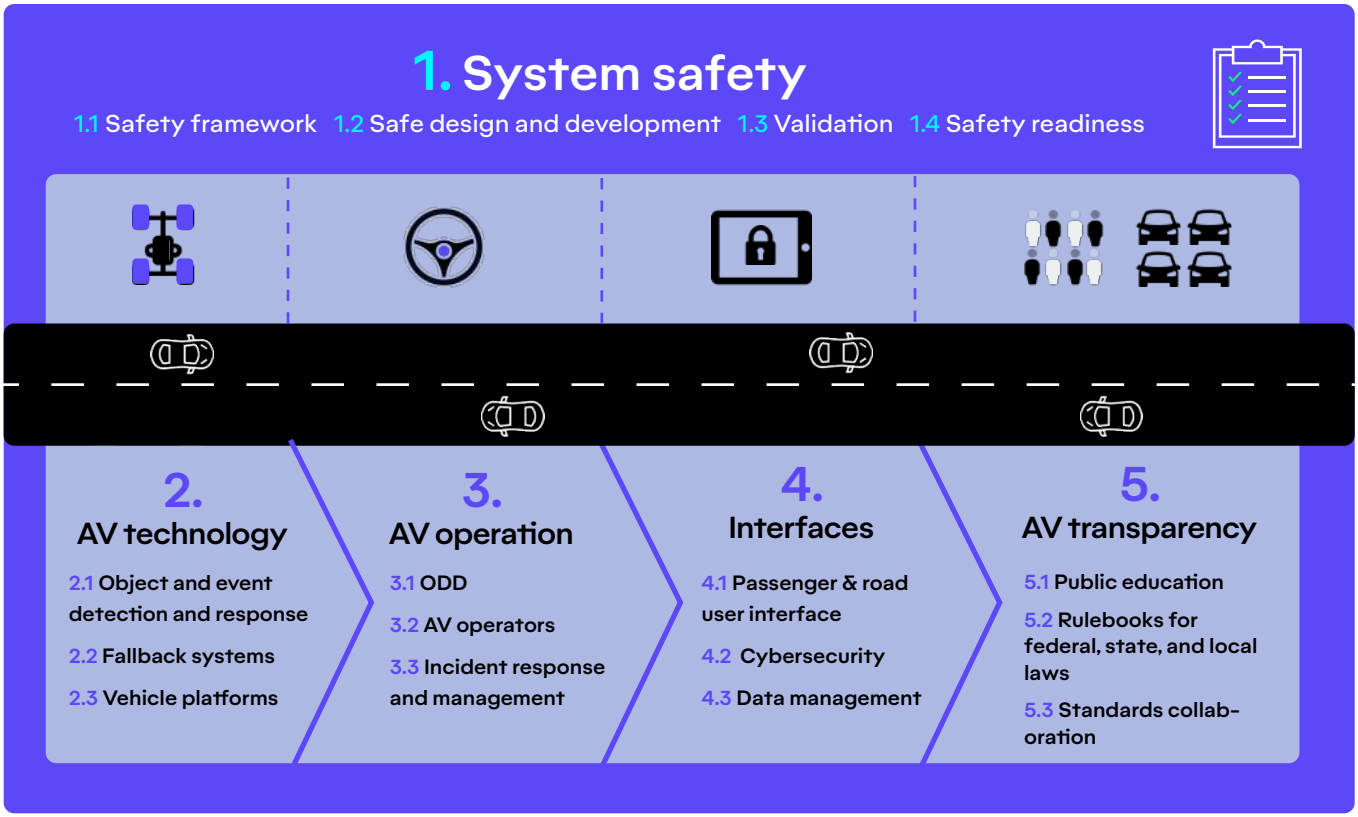
Safe operation of SAE Autonomy Level 4 AVs (chapter 3) starts with a defined operational design domain (ODD). The ODD comprises physical road infrastructure and environmental conditions. AV operators such as safety drivers and AV stewards ensure the safety of AV testing operations on public roads. Operating fleets of AVs also necessitates carefully conceived processes for responding to incidents and interacting with first responders.

FIGURE 1: STAGES OF AV DEVELOPMENT WE USE THROUGHOUT THIS VSSA



Introduction

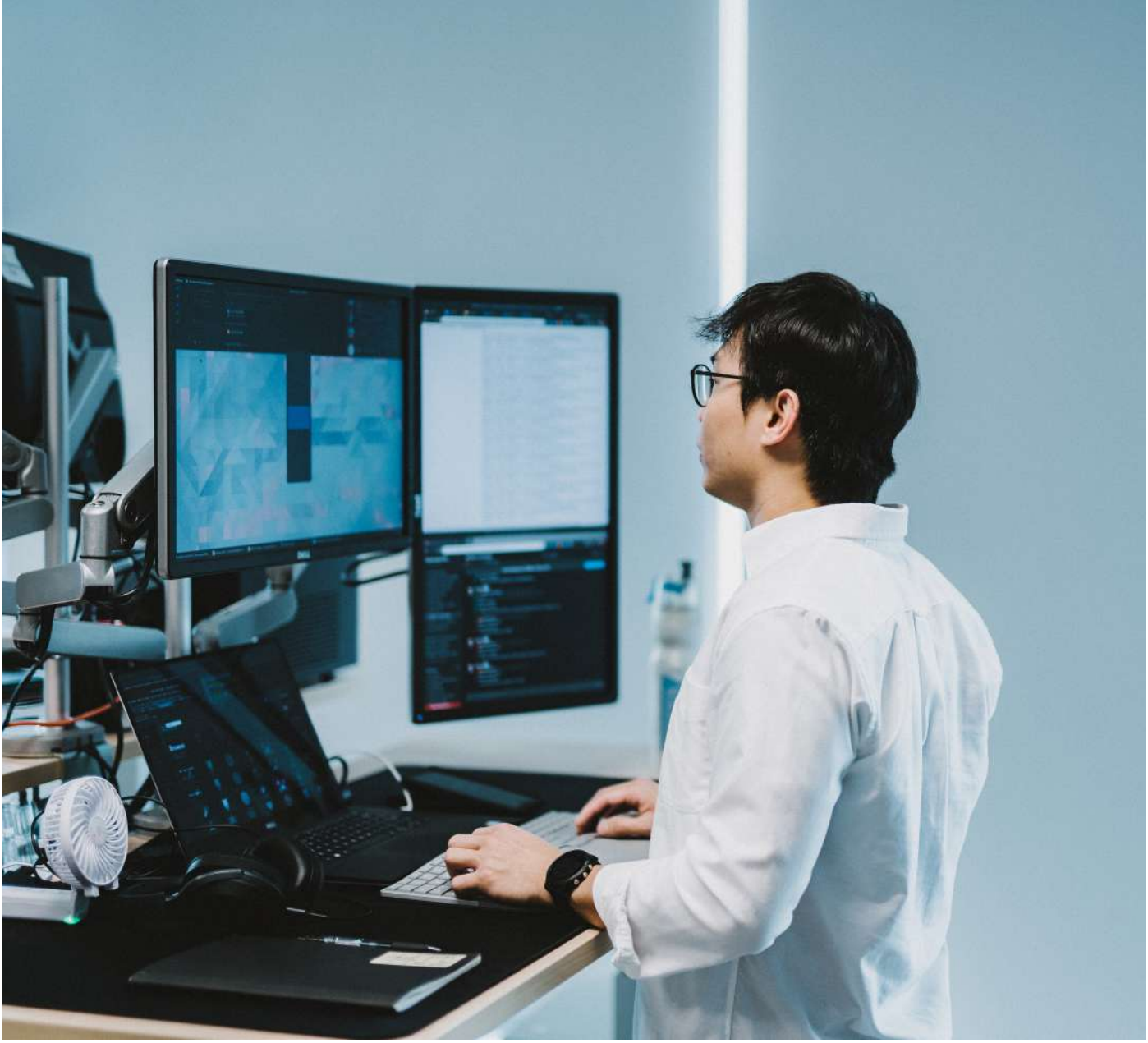
FIGURE 2: THE AV ECOSYSTEM. NUMBERS CORRESPOND TO THE CHAPTER AND SECTION NUMBERS OF THIS VSSA



The AV ecosystem cont.

Our vehicles transmit and receive information through various interfaces (chapter 4). AVs interact directly with AV operators, passengers, and other road users through human-machine interfaces. AVs also connect with other software systems via data interfaces. Data interfaces necessitate protection from malicious actors through appropriate cybersecurity measures and safe remote access. AV fleets also generate large amounts of data that can foster continued learning and improvement of the safety of AV technologies. We recognize the need for responsible use of this data, and we manage data with rigorous processes and tools.

Public adoption and safe interactions with AV technology will depend on understanding of and trust in the technology (chapter 5). We support various campaigns aiming for a broad understanding of our AV products through public education, collaboration, and research [8]. We developed a framework called Rulebooks to capture differences in laws that govern rules of the road and acceptable driving behavior at the federal, state, and local level, and to enable compliance with these laws when operating in different locations [9]. We commit to working closely with lawmakers and regulators to establish best practices for safety, as well as to continue to contribute to the creation of standards, whitepapers, and technical publications related to AV safety [5] [10]. ■



1. System safety

1. System safety

System safety is at the core of our work and refers to safe design and thorough validation and testing, culminating in a formal Safety Readiness assessment.

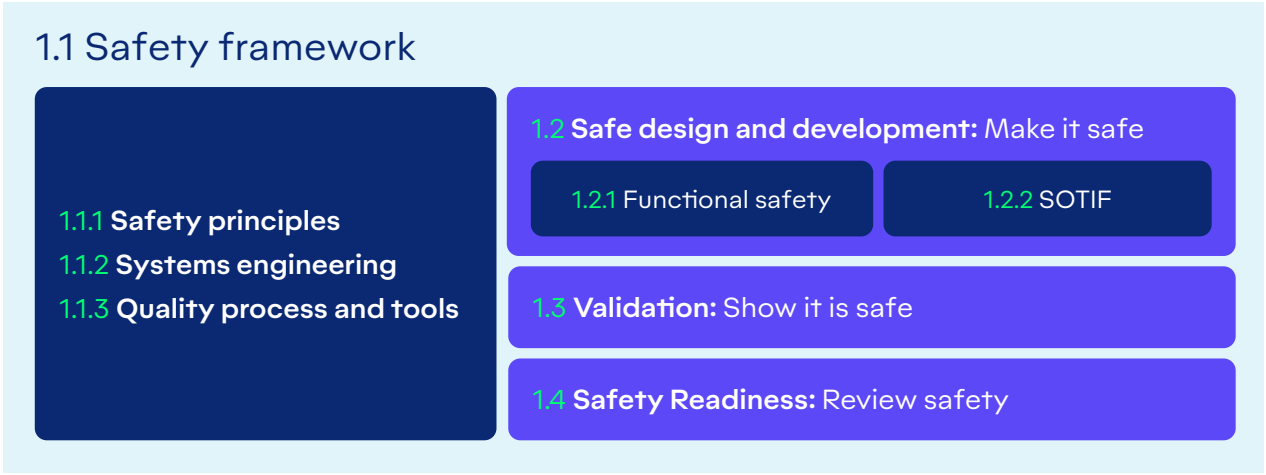
Our safety framework ties together all the safety activities we implement to deliver a safe AV ecosystem (see Figure 3). This framework builds on our underlying safety principles and addresses the requirements of functional safety, safety of the intended functionality (SOTIF)[3], and other safety elements.

The safety framework applies appropriate supervision and methods for each stage of development. During the research and development stage of AV operation prior to self-driving release (Stage I), we make frequent incremental changes to improve the system using agile development methods, rapid prototyping, and quick turnaround in software releases. We operate systems with both a safety driver and a safety engineer (see section 3.2.1). During AV prototype operation and testing (Stage II), we use an AV steward and the development process shifts towards product-oriented design with prototype testing, validation, and certification of certain elements. When the AV technology matures to a fully self-driving taxi service (Stage III), we follow a fully product-oriented design process and seek comprehensive certification.

3. Functional safety refers to the absence of unreasonable risk due to hazards caused by malfunctioning behavior of [electrical and/or electronic] systems" [13]. SOTIF refers to the "absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons" [4].

1. System safety

FIGURE 3: MOTIONAL'S SYSTEM SAFETY FRAMEWORK FOR DELIVERING A SAFE AV ECOSYSTEM



As noted earlier, current automotive standards do not fully address the unique complexity of a fully driverless system. In response to this gap, several industry and research consortia are collaborating on best practices for safe AV deployment and working towards new and updated standards. We are a leading contributor to one such collaborative effort, which resulted in the common framework published in SAFAD [5], and are participating in several others[4].

This chapter describes our safety and validation practices and how they support an evaluation of Safety Readiness.

4. Participation includes International Organization for Standardization (ISO) committees (i.e., ISO 26262 [13], ISO/PAS 21448 [4], and the ISO technical committee for SAFAD), International Electrotechnical Commission (IEC) groups (i.e., IEC SC 65a, IEC 61508, IEC 61511), SAE committees (i.e., Automated Vehicle Safety Consortium, SAE On-Road Automated Driving committee for Systems Theoretic Process Analysis, and the G-48 committee for System Safety), the Consumer Technology Association's Technology Council Self-Driving Vehicles Advisory Group technical committee for Automated Vehicle standards [61], the World Economic Forum's Safety Pool initiative [60], Singapore's TR 68 [10], and the Institute of Electrical and Electronics Engineers (i.e., P2846 [42] and P2851 [48]).

1. System safety

In addition to following state-of-the-art methods for functional safety, we conduct both scenario-based testing and statistical safety testing to achieve a high level of system safety.

1.1. Safety framework

Guided by SAFAD's safety principles, we implement a safety framework built on systems engineering skills and quality processes and tools to ensure that we design and validate a safe AV system.

1.1.1. Safety principles

SAFAD complements existing safety standards by providing structure and guidance for AV safety. SAFAD's approach for design and development starts with 12 safety principles and outlines the capabilities, elements, and architecture needed for an AV system to satisfy the safety principles.

The 12 safety principles provide guidance on all parts of AV development, from safe design to operations to data recording. For example, one safety principle is that an AV can manage typical situations within its ODD and revert to a safe state as soon as it reaches the limits of its ODD. This guidance informs the AV capabilities needed. In this example, the AV needs to be able to detect that it is approaching the ODD limits and complete a safe stopping maneuver if it exceeds those limits. Various elements implement the capabilities that satisfy the safety principles, such as sensors, maps, and algorithms that tell the AV how close it is to an ODD limit. The architecture of the AV system connects these elements together in a way that supports the capabilities and manages component failures.

1.1.2. Systems engineering

Systems engineering skills and practices support safe design. We employ methods that cover functional safety, SOTIF, and the safety principles in our systems engineering efforts. This includes the use of analytical tools such as fault tree analysis (FTA), failure mode and effects analysis (FMEA), hazard analysis and risk assessment (HARA), and systems theoretic process analysis (STPA). These tools and methods cover both top-down and bottom-up approaches to prevent, detect, and mitigate failures that can lead to safety hazards in complex systems. We closely integrate our development processes for systems, software, and hardware with our safety and quality engineering processes.

1.1.3. Quality processes and tools

We have implemented an AV-specific product development process that integrates our functional safety and SOTIF processes. This product development process coordinates our systems engineering, safety, quality, and reliability objectives. We use a mature requirements management system that serves as the backbone of our design and development efforts and helps trace our FMEA and FTA analyses to our design deliverables. The results of the analyses are part of the functional safety deliverables and feed into the safety sign-off process (see subsection 1.4.1).

Our quality management system considers International Automotive Task Force 16949 [11] and International Organization for Standardization (ISO) 9001 [12]. In addition to our development processes, we incorporate and integrate Global Software Process Improvement and Capability dEtermination (SPICE) compliance. The integration of safety and quality engineering into our product development process encourages traceability of documentation and helps all engineers understand the purpose and role of the activities needed for a safe design.

1. System safety

1.2. Safe design and development

In the initial phase of a project, we draft a preliminary safety concept that lays out how we will make our product meet our safety, quality, and reliability objectives, following the 12 safety principles from SAFAD. The safety concept is a blueprint for our design and engineering efforts. In our processes and design, we follow state-of-the-art methods for functional safety, and conduct both scenario-based testing and statistical safety testing to achieve a high level of safety [4] [13].

1.2.1. Functional safety

The automotive functional safety standard ISO 26262 aims to ensure the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of [electrical and/or electronic] systems" [13]. This standard provides time-tested rigorous methods and serves as a viable foundation from which safety considerations for AVs will evolve [13]. Our processes and products undergo external review and ISO 26262 certification by industry-leading experts and partners. Functional safety work products include the functional safety assessment and safety mitigations. They contain four specific parts and supplemental documents:

1. The ***item definition*** specifies the system and its boundaries. In our case, the item is the AV (see chapter 2) and its operating environment (see chapter 3). The item definition captures functions, maneuvers, weather conditions, road layouts, operational speeds, and human interactions. It sets out the scope, depth, and detail for the safety analysis. We perform regular updates of the item definition to capture design decisions and system changes.
2. The ***HARA*** systematically analyzes the consequences of AV system malfunctions that could result in hazards in realistic worst-case scenarios. The HARA rates risks by severity, exposure, and controllability level, resulting in automotive safety integrity levels (ASILs). Higher ASILs warrant increasingly rigorous requirements for the implementation and validation of proposed hazard mitigation and prevention measures of the system, software, and hardware. The HARA yields a set of functional safety goals for addressing hazards. We translate functional safety goals into functional safety requirements for subsystems and components using requirement decomposition. The HARA also influences the SOTIF analyses (see subsection 1.2.2).
3. We ***design*** the system so that it addresses functional safety goals. The design balances the hardware and software redundancy needed to perform a wide range of complex functions autonomously with systems engineering practices that favor simplicity.
4. We create a ***functional safety validation plan*** to ensure that the design meets functional safety goals. The plan ties in lower-level testing of software and hardware with vehicle-level validation. This also allows us to reflect on and verify the intention and implementation of the functional safety concept before finalizing the design.

The functional safety requirements we develop and validate at the initial stages of a project remain applicable through the life of the product. We manage the system specification for consistency with system design and documentation so that safety assessments and safety mitigations remain valid and appropriate.

1. System safety

We implement both qualitative and quantitative approaches as part of our safety framework.

1.2.2. SOTIF

SOTIF originated from the ISO 26262 committee's understanding that being free from electrical and electronic malfunctions does not mean that a system is free from hazards. The SOTIF committee [4] recognized that the design and assessment of a more complex driver-assisted system needs to account for the system's performance in and suitability for its environment.

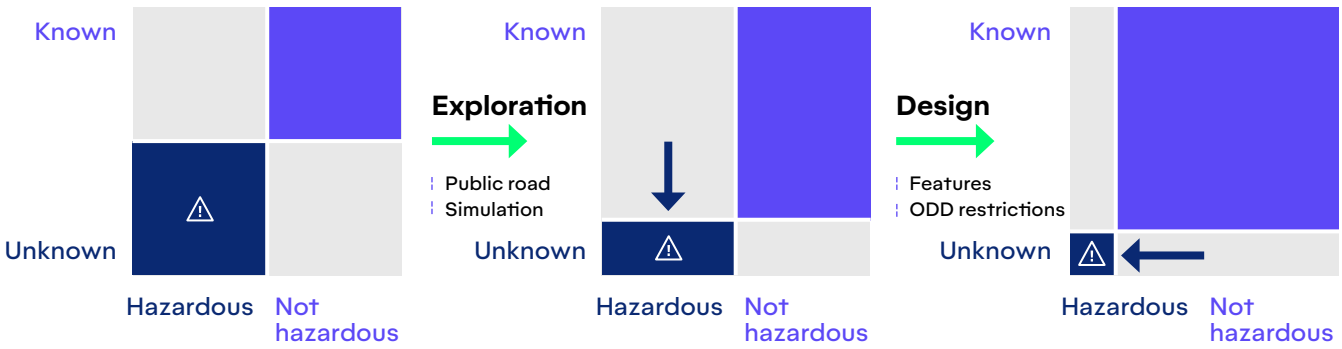
For AVs, this additional assessment is important due to the numerous actions that the system continually performs. Unlike the functional safety standard ISO 26262 [13], the existing SOTIF guidance [4] is not yet an official ISO standard[5]. It focuses primarily on SAE Autonomy Level 1 and 2 systems and does not prescribe a detailed process and deliverables for higher levels of automation. We incorporate guidance from experts[6] to ensure that our processes and deliverables continue to appropriately reflect the spirit of SOTIF and up-to-date industry practices.

The SOTIF guidance [4] divides all possible scenarios into four categories: (1) known, not hazardous; (2) known, hazardous; (3) unknown, hazardous; and (4) unknown, not hazardous. The goal of SOTIF activities is to minimize the unknown, hazardous area by (i) moving the boundary from unknown to known, and (ii) moving the boundary from hazardous to not hazardous (see Figure 4). We move the boundary from unknown to known through exposure of the AV system to new scenarios. This occurs iteratively, via public road testing (with a safety driver until fully validated) and simulation (see section 1.3). We move the boundary from hazardous to not hazardous via either new technical solutions that become part of the design, or modifications of the operational limits (i.e., ODD restrictions).

The SOTIF guidance [4] permits either a qualitative or a quantitative approach to evaluate SOTIF, without expressing a preference. Each approach has strengths and weaknesses when applied to AVs. The qualitative approach assesses robustness to corner cases of the AV system and its operating envelope. The quantitative approach assesses resilience through randomized testing.

We implement both qualitative and quantitative approaches as part of our safety framework. We build a robust system and assess both its functionality and any failures (see subsection 1.2.2.1). Our qualitative assessment includes test cases for known scenarios (see subsection 1.2.2.2). Our quantitative assessment centers around mileage accumulation on public roads to demonstrate statistically that unknown, hazardous scenarios are sufficiently rare (see subsection 1.2.2.3).

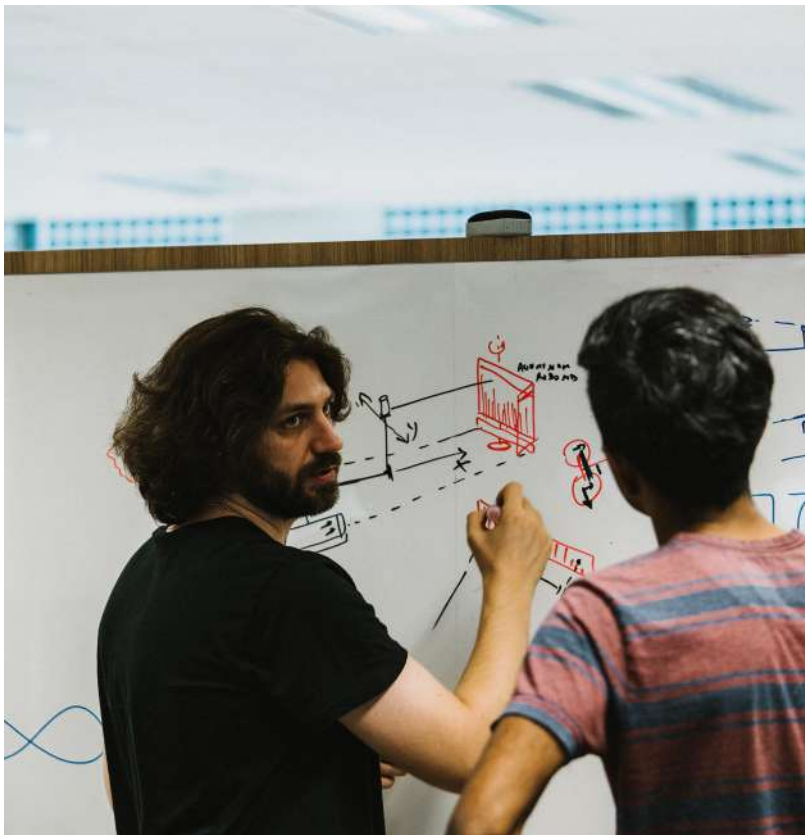
FIGURE 4: THE SOTIF PROCESS, ILLUSTRATING THE OVERALL OBJECTIVE OF MINIMIZING THE RATE OF OCCURRENCE OF UNKNOWN, HAZARDOUS SCENARIOS (BASED ON [4])



5. ISO/PAS 21488 [4] is a Publicly Available Specification and anticipated to become an International Standard

6. This includes guidance from internationally recognized automotive safety assessors

1. System safety



1.2.2.1. SOTIF assessment

The SOTIF process begins with an analysis founded on the HARA method. In contrast to functional safety, the SOTIF HARA identifies and assesses scenarios for which limits in functionality (as opposed to malfunctions) may lead to a hazard. Like a functional safety HARA, the SOTIF HARA rates hazards by severity, exposure, and controllability to produce SOTIF goals that inform subsystem and component SOTIF requirements.

1.2.2.2. Scenario-based testing for SOTIF

Scenario-based testing for SOTIF aims to build confidence in the AV system capabilities beyond the absence of malfunctions. This testing covers SOTIF goals and occurs on a closed course or in simulation. We establish passing criteria for scenario-based testing based on a specification of the appropriate driving behavior, including novel formal methods and processes that translate engineering judgment into a behavior specification to ensure consistent passing criteria and transparency, reproducibility, and scalability of our scenario-based testing activities (see section 5.2). We further recognize that partners and consortia can provide important support to discussions about appropriate driving behavior for AVs and to our internal processes for establishing passing criteria for driving behavior (see section 5.3).

Our approach to testing builds confidence that the AV can safely navigate a world that is random and diverse.

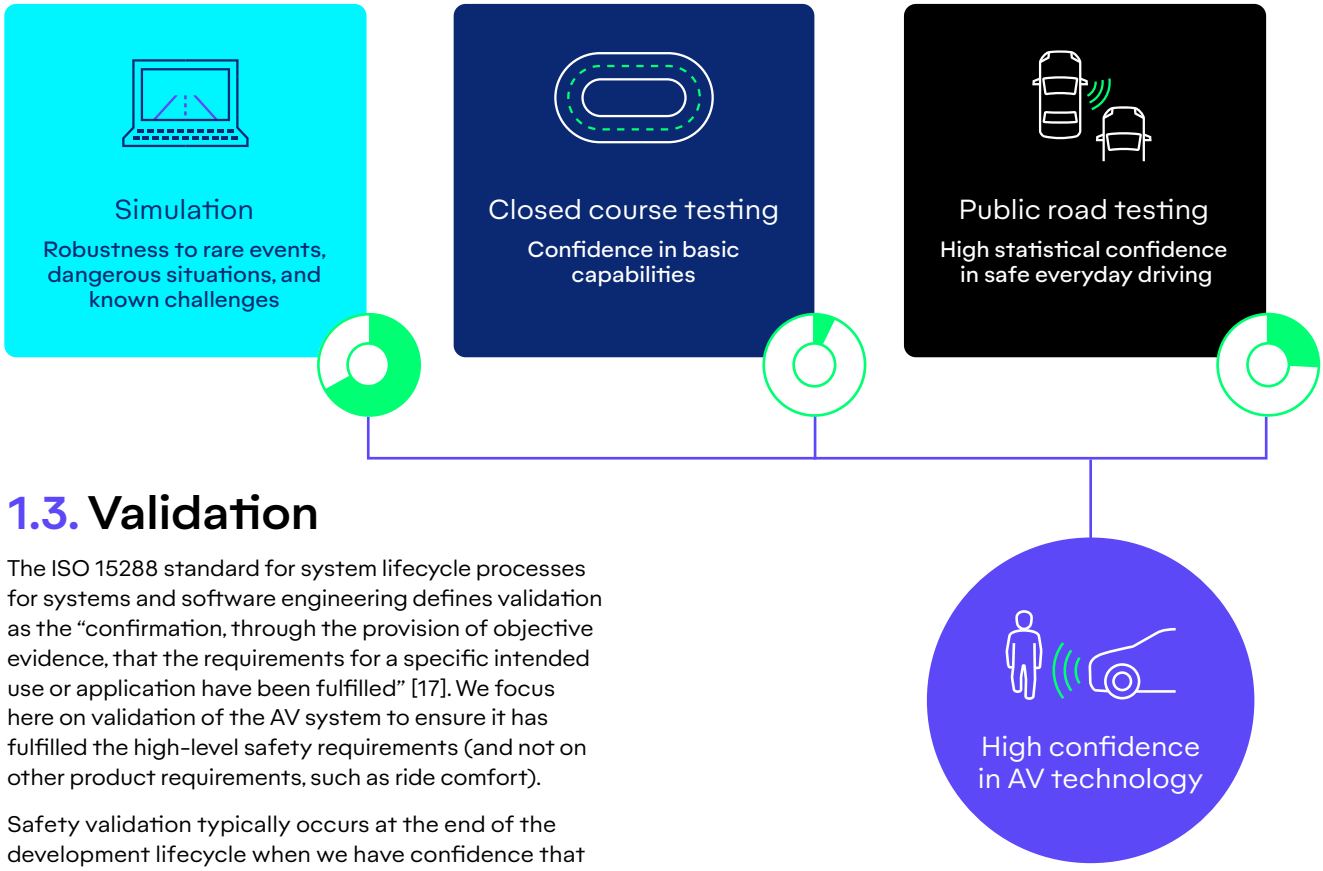
1.2.2.3. Statistical safety testing

One key challenge of AV development is that the real world is random and diverse, and this makes potential scenarios innumerable [18]. Consequently, confidence in our capabilities in known scenarios is only meaningful in conjunction with an understanding of the frequency of unknown scenarios in the ODD of the AV. Statistical safety testing accumulates mileage to establish whether the occurrence of unknown hazardous scenarios lies below an acceptable threshold. We carefully review any incidents that occur during this mileage accumulation to assess the incident's cause and any impact on the system.

Both the operational definition of unknown hazardous scenarios and the appropriate threshold remain areas of active discussion within the industry and society [14] [15] [16].

1. System safety

FIGURE 5: WE LEVERAGE THREE TEST SETTINGS TO OBTAIN THE HIGHEST POSSIBLE CONFIDENCE IN THE SAFETY OF OUR AVS. THE SHADED CIRCLE SEGMENTS QUALITATIVELY ILLUSTRATE THE APPROXIMATE AMOUNT OF TEST DRIVING THAT EACH TEST SETTING REPRESENTS



1.3. Validation

The ISO 15288 standard for system lifecycle processes for systems and software engineering defines validation as the "confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled" [17]. We focus here on validation of the AV system to ensure it has fulfilled the high-level safety requirements (and not on other product requirements, such as ride comfort).

Safety validation typically occurs at the end of the development lifecycle when we have confidence that we completed the design according to subsystem safety requirements. Safety validation occurs after a stable software release and hardware configuration have undergone substantial testing, improvement, and verification during development. Until the completion of safety validation and sign-off on safety (see subsection 1.4.1), we operate with a trained safety driver when testing AVs on public roads.

Our aim for safety validation activities is to demonstrate that the AV is safe enough for fully self-driving operation on public roads. These activities include scenario-based testing on known scenarios and statistical safety testing. At a minimum, we aim for "a positive risk balance of the automated driving solution compared to the average human driving performance" [5], with high statistical confidence. We may sharpen this target as operational scope, technology, and safety expectations evolve.

Safety validation occurs in three main test settings outlined in Figure 5 and described in the following subsections: simulation, closed course proving grounds, and public roads. These individual test settings have distinct strengths and limitations. Our validation approach integrates the three test settings to leverage the strengths of each and collectively address their respective limitations.

1. System safety

1.3.1. Simulation

Simulation testing uses a virtual environment to evaluate AV software across a large number of scenarios. For safety validation we aim to reduce the risk of uncovering high-impact AV deficiencies in the real world. Doing so involves optimizing the coverage of the scenario space, setting appropriate pass/fail criteria for our tests, and using appropriate levels of simulation fidelity. With simulation testing we can:

- Test scenarios that are too dangerous to test in the real world;
- Precisely control all inputs and settings, leading to repeatable tests;
- Efficiently expose the AV system to many scenarios; and
- Randomize inputs to search for unknown, hazardous scenarios.

These capabilities allow us to use simulation both for scenario-based testing and as a complement to statistical safety testing on public roads. Simulation, however, relies on models that only approximate the physical world. Moreover, extrapolating AV performance in the real world from controlled tests remains difficult without a precise understanding of the frequency at which the tested scenarios occur in the ODD [5].

Simulation testing encompasses a wide range of methods, including basic replay of data collected in the real world on the AV software (open-loop software reprocessing), testing of the AV software in an artificially created virtual environment (software-in-the-loop, or SIL), and testing of the AV software in an artificial environment but on the hardware that it runs on (hardware-in-the-loop, or HIL) [5]. Our approach to SIL testing varies based on relevance to the features and the risk associated with a scenario. For example, SIL scenarios that deal with the detection of and response to pedestrians may involve detailed sensor simulation, since the perception system and its sensors are highly relevant to detecting pedestrians, and because of the severe consequences of any pedestrian collisions in the real world. A scenario involving loss of control due to slippery road surfaces may instead make use of high-fidelity vehicle dynamics and road surface models.

As a prerequisite to testing an AV on public roads with a safety driver (Stage I), we perform comprehensive simulation testing that includes both open-loop software reprocessing of sensor data to evaluate any regressions in the perception system and SIL testing to ensure the safe performance of the planning and controls software.

Before operating an AV prototype with a human AV steward (Stage II), we perform two additional types of simulation testing. First, we perform reprocessing and analysis of data surrounding key events observed during public road testing. This includes ODD-specific data collected using AV systems released for Stage I testing. Second, we perform HIL testing of safety-critical subsystems as part of our functional safety goal validation (see subsection 1.2.1). This includes fault injection testing following functional safety practices to further evaluate the robustness of our systems to faults [13]. Where appropriate and feasible, we complement these simulation tests with SIL and/or HIL simulation of European New Car Assessment Programme (NCAP) scenarios and NHTSA pre-crash scenarios that apply to the ODD, and SIL scenarios constructed from situations we encountered during past public road testing.

1. System safety

1.3.1. Simulation cont.

The scope and number of simulation tests we conduct prior to the release of a fully self-driving AV (Stage III) increases relative to the earlier stages. Open-loop software reprocessing for regression testing and for analysis of events observed during public road testing continues, and HIL testing expands in scope. We consider several evaluations and additions for SIL testing:

- Scenarios derived from AV safety requirements and AV behavior definitions;
- Relevant scenarios from external sources like NCAP [19], NHTSA's pre-crash typology [20], and Pegasus [21];
- Scenarios derived from the variation of static ODD elements (e.g., road configurations); and
- Dynamic scenario generation to search for system weaknesses and (previously) unknown, hazardous scenarios.

Due to its scalability, simulation testing for Stage III includes the largest amount of test driving compared to closed course and public road testing (see Figure 5).

1.3.2. Closed course testing

Closed course environments allow us to conduct controlled tests in specific, well-formulated scenarios and address scenario-based testing needs, including to:

- Evaluate the AV in a real physical environment;
- Test the AV without posing any risk to the general public;
- Test key AV capabilities in standard scenarios;
- Repeatably test interactions that may only occur rarely on public roads;
- Validate simulation models; and
- Train safety drivers to safely operate the AV.

However, closed course testing has certain limitations:

- It can be practically challenging to stage highly complex scenarios that the AV might encounter on public roads (e.g., a scenario involving numerous vehicles at a large intersection);
- Not all tests are repeatable or scalable;
- Closed course testing often uses props as stand-ins for real people, but the movement of real people may be less predictable; and
- The frequency at which scenarios tested in closed course occur in the intended ODD of the AV may be unknown (due to lack of scenario-specific driving data).

We use closed course testing primarily to ensure that the AV meets specific requirements and to manage AV system exposure to rare and potentially dangerous scenarios. By doing so, we gain confidence in the capabilities of the AV and in some elements of its broader ecosystem (e.g., human-machine interactions).

The extent of closed course testing we perform depends primarily on the development stage. As a prerequisite for public road testing with a safety driver (Stage I), our AVs undergo closed course testing to assess their autonomous behavior and performance. This includes consistent object detection and maneuvers ranging from basic to more complex.

We expand closed course testing prior to allowing AV prototype operation with a human AV steward (Stage II). The tests extend to include more AV behavior testing and extensive testing of safety-critical systems (e.g., a fallback system; see section 2.2). These tests follow and meet existing standards for functional safety goal validation [13]. We also conduct external tests developed specifically for emergency braking systems by the NCAP [19].

The extent of closed course testing may increase in scope prior to the release of an AV for a fully self-driving taxi service in a defined ODD (Stage III). For example, for this stage we may systematically evaluate requirements for all parts of the AV stack, for vehicle interfaces, and for any other ecosystem elements.

1. System safety

Public road testing is a key pillar of the statistical safety testing activity for safety validation.

1.3.3. Public road testing

Public road testing exposes the AV to scenarios that it encounters during everyday driving. Public road testing is a key pillar of statistical safety testing for safety validation. Driving real-world miles in our ODD allows us to evaluate whether the rate of unknown hazardous scenarios is sufficiently low. Key strengths of public road testing are:

- The ability to make statistical inferences about safety and risk; and
- The possibility of encountering unanticipated or complex scenarios not represented in other test settings.

Two aspects of public road testing complicate its utility for statistical validation.

First, unlike during closed course and simulation testing, we do not control the selection of scenarios the AV might encounter during public road testing. Most miles of public road testing involve known scenarios that the AV can handle (i.e., known, not hazardous scenarios). New scenarios are rare and decrease in frequency as the technology matures. Serious events involving human drivers (on a per mile driven basis) are relatively infrequent. To obtain statistical confidence that the AV is safer than a human driver, public road testing alone would require very high mileage. A RAND study indicated that it would take a 100-car AV fleet, driving 24 hours a day and 365 days a year, more than 400 years to show a lower rate of fatal collisions than human drivers [22].

Second, our operational processes for all public road tests focus on ensuring that the safety driver takes over driving control well before any safety-critical events occur (see section 3.2). This is positive for safety in general, but it is a limitation for statistical validation—because we are unable to directly observe how the AV system would have responded to a potentially safety-critical scenario if the safety driver were not present.

Our public road test strategies aim to minimize these limitations while retaining the strength of the test setting. First, we conduct public road testing for validation in a statistically representative manner. We accumulate miles to encounter driving scenarios in conditions that are consistent with the intended ODD and we avoid biasing the testing (e.g., towards lower traffic density or more favorable times of day).

Second, we use appropriate metrics to statistically evaluate the safety performance of our AVs. Those metrics include leading measures (also known as surrogate safety metrics), such as incidents prevented by the safety driver, near-collisions, violations of certain driving rules, and other notable events that may identify unknown, hazardous scenarios [23]. We can then use mathematical modeling to help characterize the uncertainty about more serious events (i.e., lagging measures) based on statistical observations of more frequent events [24].

Third, we evaluate takeover events to assess the AV behavior that would have occurred if the safety driver had not taken over. Our methods include reprocessing of log data, expert review of system metrics and processes, and scenario recreation in simulation. We also conduct empirical evaluations of the reliability of processes to classify takeovers [25].

Fourth, we leverage our understanding of AV system designs to better evaluate the data obtained during public road testing. We use a novel application of shadow mode testing to assess the safety performance of certain subsystems. Shadow mode testing is a method in which the system under assessment is unable to actuate any controls but logs its activation commands. Conventional shadow mode testing occurs while a human performs the driving task and typically focuses on evaluating unneeded activations such as brake requests when there is no actual obstacle (i.e., false positives) [26]. However, we use shadow mode testing to evaluate a subsystem (e.g., a fallback system) while the AV itself performs the driving task. Additionally, we detect possible false negative activations as well as false positive activations of the safety feature under test. False negatives occur if the safety feature does not activate in a situation that requires it. We carefully review safety driver takeovers to identify potential false negatives. Conducting public road testing in this manner can provide better information about safety performance than a purely black-box statistical evaluation and can increase confidence in the system's overall safety.

1. System safety

The diversity of our sites gives us a unique ability to continually improve our AV systems.

1.3.4. Iterative testing and continuous improvement

We view validation activities as an integral element of development. Scenario-based testing and statistical safety testing may result in the discovery of deficiencies. We review whether we will address any deficiencies via new functionality or other improvements to the AV system. We may also conduct statistical safety testing activities that focus on specific subsystems (e.g., shadow mode testing) alongside the development of other parts of the AV to accumulate statistical data about different subsystems and inform further development.

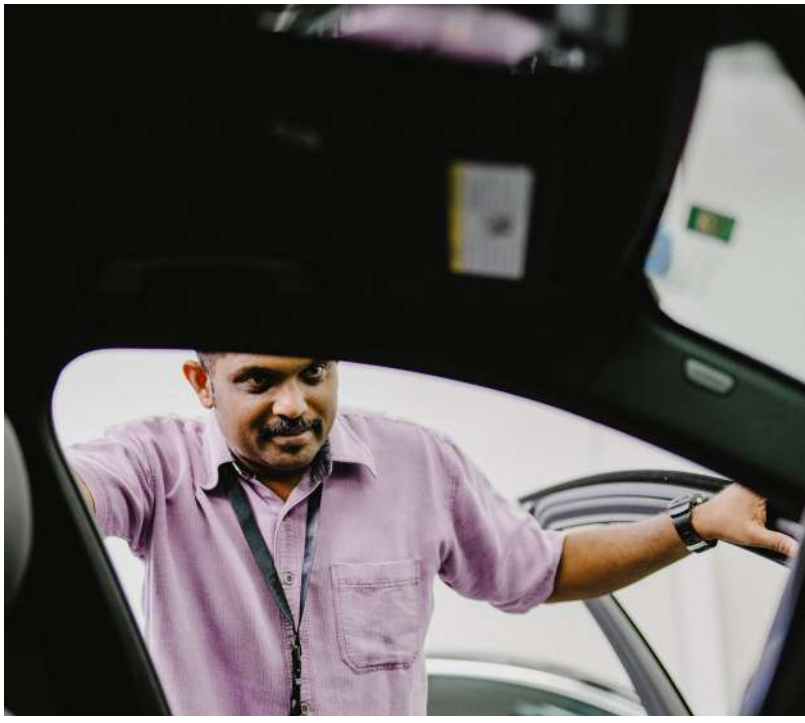
During our public road testing, we have encountered a wide range of objects and events globally. For example, our Singapore test site exposes AVs to left-side driving, dense urban environments, and monsoon weather conditions [27]. In Las Vegas, our AVs have witnessed gridlock, sandstorms, creatively dressed pedestrians, and erratic jaywalkers [28]. In Pittsburgh, we have tested our AVs in snow, sleet, and fog. In Boston, our AVs have witnessed seagulls [29], articulated buses [30], and "Boston left turns" [31]. The diversity of our sites gives us a unique ability to continually improve our AV systems.

1.3.5. Collaboration

Our experience in validating AV safety will likely lead to new approaches and methods. We recognize the importance of collaborating on this work to accelerate the development and release of AV technologies. We contribute to industry-leading standards to reduce the work required for others to determine how to validate the safety of their products. In addition to our collaboration with industry peers on SAFAD, we actively collaborate with certification experts, simulation providers, and non-profit research organizations to develop the theory and tools that enable AV validation.

1.4. Safety Readiness

The Safety Readiness assessment is the structural evaluation of the safety of the AV, touching on all aspects of the safety lifecycle and AV ecosystem. The Safety Readiness assessment provides confidence in the strength of our system safety work, including safe design and validation. It considers the many aspects of ecosystem safety, ranging from how we write software to how we verify our operational processes, and confirms that we have conducted all aspects of our safety process. It examines technical documents, processes, external reviews, and testing results to ensure the AV system meets the defined criteria, culminating in a safety sign-off.



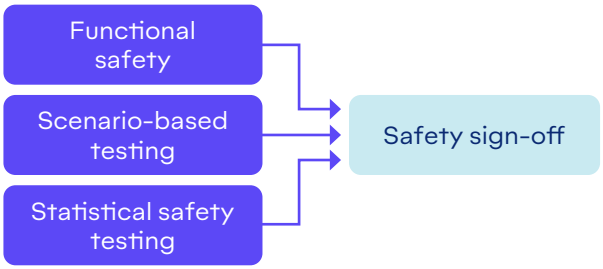
1. System safety

1.4.1. Safety sign-off

We have devised a rigorous safety sign-off process that forms the backbone of the Safety Readiness assessment of our AV (see Figure 6). Our safety sign-off process applies to the release of an AV system in a defined ODD for self-driving operation. It considers the functional safety of the AV system and evaluates whether scenario-based testing and statistical safety testing adequately demonstrate the absence of unreasonable risk from known or unknown hazardous scenarios.

Our validation framework includes activities in different test settings that collectively address the functional safety, scenario-based testing, and statistical safety testing dimensions of our safety sign-off process. Figure 7 summarizes the role of each validation test setting in support of these three dimensions.

FIGURE 6: MOTIONAL'S SAFETY SIGN-OFF PROCESS

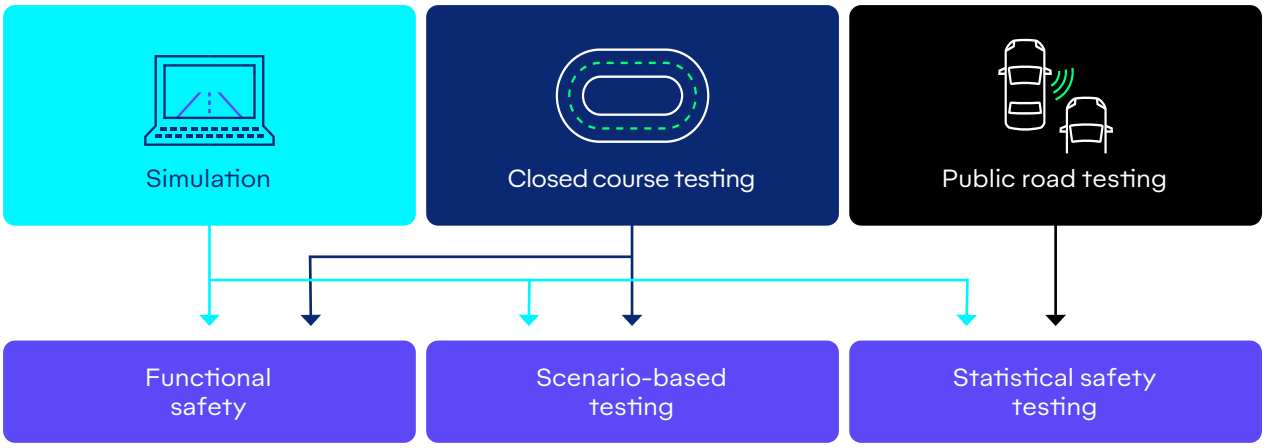


1.4.2. Data-driven, phased sign-off approach during development

While Motional's safety and validation assessment framework supports our formal release of a mature product, we have also implemented processes to support safe testing on public roads during earlier stages of development. We use a phased approach to determine whether our AV system is ready for safe operation on public roads within our ODD and under the supervision of a safety driver. This Road Release Process has clear passing criteria and sign-off gates that include code reviews, testing across extensive simulation scenarios, and a multi-phase closed course assessment. We examine the results of each phase prior to moving to the next phase. If a release passes the sign-off gate that allows it to proceed to public road testing, we start testing on a small scale. We review the data and results from this small-scale testing prior to proceeding to larger scale safety driver-supervised public road testing.

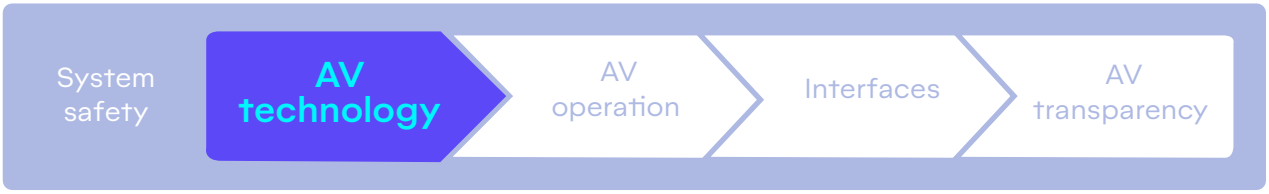
As a further safety measure, our Red Button process and operational procedures (see section 3.2) ensure that we can respond quickly and appropriately if any issues arise on or off the road. ■

FIGURE 7: RELATIONSHIP BETWEEN THE THREE PILLARS OF SAFETY SIGN-OFF AND THE VALIDATION TEST SETTINGS FROM SECTION 2.2



2. AV technology

2. AV technology

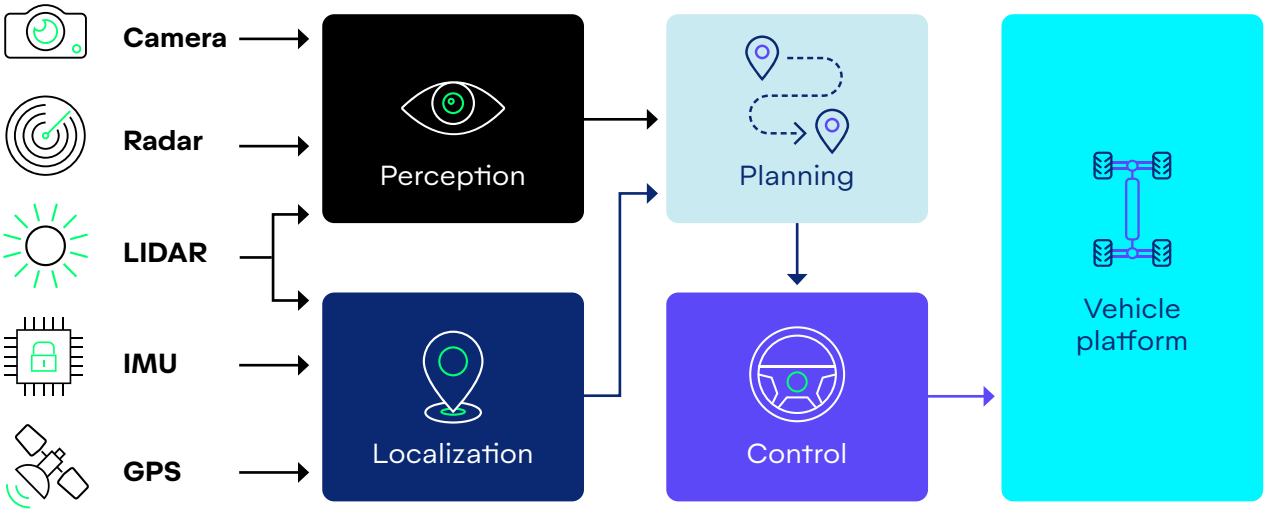


This chapter covers core components of our system that are key to safety. These components include the technical capabilities of perception, localization, mapping, planning, and control as well as the technical fallback system and vehicle platform. We will highlight some of the systems we are developing to improve our real-world capabilities and dive into promising innovations we build in-house.

2.1. Object and event detection and response

AV subsystems primarily responsible for object and event detection and response include the perception, localization, planning, and control systems (see Figure 8). These subsystems help the AV sense its surroundings, determine the AV's location relative to the road and other objects, detect and classify different types of road users (e.g., pedestrian, vehicle, bicycle) and potential hazards, and determine and follow a safe path.

FIGURE 8: HIGH-LEVEL DIAGRAM OF OUR CORE AV SYSTEM ARCHITECTURE (FALLBACK SYSTEMS NOT SHOWN)



2. AV technology

2.1. Object and event detection and response cont.

To support our safety and performance goals, we use multiple sensor modalities and algorithmic approaches to provide robustness and redundancy. For example, we use multiple sensor types as each type has strengths and weaknesses in detecting and classifying objects in the surrounding environment. We process the data flowing from those sensors in multiple ways, including deep learning-based approaches and geometric approaches. We represent our surroundings using world models that identify and classify objects that the AV needs to navigate carefully, as well as world models that affirmatively identify free space as safe areas for driving. We use multiple methods to determine the right path for the AV to follow. Ultimately, this careful consideration and combination of multiple methods enables us to build a system that is safer and more capable than one built on any individual technology.

2.1.1. Sensors and perception

We design the suite of sensors on the vehicles to be redundant in case of failure and complementary for increased awareness. To ensure consistent sensor quality across our fleet, we have put in place sophisticated quality checks, calibration setting processes, and maintenance and cleaning procedures.

Our sensor suite currently consists of multiple sensor types covering a 360-degree field of view at short and long ranges, including radar, light detection and ranging (LIDAR), and cameras, as well as other supplemental sensors. We have chosen to use these three primary types for 360-degree coverage to balance the strengths and weaknesses of each. For example, radar provides excellent range as well as direct measurement of object speed relative to the AV. This makes radar extremely effective at detecting moving vehicles. However, automotive radars historically have difficulty distinguishing stopped objects from stationary background objects like metal guard rails. Similarly, camera-based vision systems provide exceptional ability to classify objects and can help distinguish a pedestrian from a pedestrian-shaped object such as a mailbox. However, vision systems have historically been less accurate at estimating the precise location of objects in three-dimensional space, compared to ranging sensors like LIDAR or radar.

We use multiple methods to build a system that is safer than one built on any individual technology.

To maximize object detection and classification performance in a variety of environmental conditions, we currently take advantage of the strengths of all three primary types. However, the capabilities and performance of sensors, both in terms of hardware capabilities and data processing methods, are improving quickly. For example, we have used data collected during our public road testing to develop increasingly capable and efficient object classification using LIDAR data. Expanded capabilities of individual sensor types strengthen and simplify the work of building a high-performance, safe, and robust perception system, and our choices will evolve with changes in sensing technology.

2. AV technology

2.1.1.1. Sensor positioning and aiming

Positioning and aiming of the sensors are critical to ensure the AV has full view of its surroundings. We position sensors so that their field of view overlaps with neighboring sensors (see Figure 9) to provide multiple sources of information about the environment. We also consider the perspective of sensors relative to one another, to ease the downstream task of comparing sensor measurements from different sensor types.

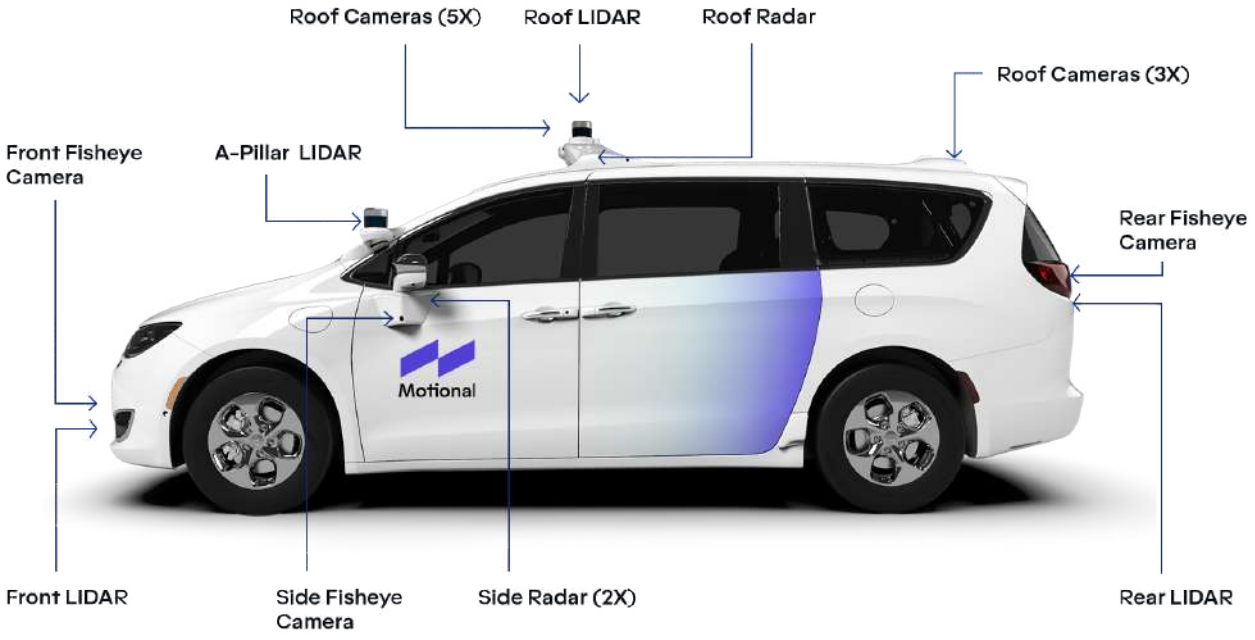
We use data collected from public road testing to verify our sensor placement provides effective sensing performance, maximizes long-range visibility, and minimizes blind spots. Experience with operation of a public fleet has also taught us practical considerations, such as selection of sensor locations that will minimize damage or disruption from regular vehicle use. Additionally, our sensor system includes features to maintain high performance during adverse conditions such as dust clouds and precipitation.

2.1.1.2. Sensor data fusion

Our sensor data fusion system combines sensor inputs according to the strengths of each sensor to build a world model of moving and stationary items around the AV. For example, our sensor data fusion system combines range and speed information from the radar system with classification and location information from the vision and LIDAR systems to enable us to conclude that a fast-moving motorcycle is approaching the AV. By comparing multiple methods of detecting an object, we gain confidence about our model of the world. If we receive contradictory information from our sensors, our algorithms consider the right approach to safely reconcile these differences. For example, if we are unsure whether we are observing a bicycle or a pedestrian, we may choose to treat the object as if it could be either. We also keep track of areas potentially hidden from our sensors' sight, which allows us to take some extra precautions for a possible object we cannot yet see.

In the event of a failure of an individual sensor that perceives a part of the world surrounding the AV, other sensors continue to provide information about that part of the world. We design the sensor network and data connections to minimize the impact of any larger system failure. These designs evolve continuously, especially between development stages I, II, and III, and optimization remains an area of active research.

FIGURE 9: EXAMPLE SENSOR LAYOUT OF ONE OF OUR PLATFORM VEHICLES (CHRYSLER PACIFICA)



2. AV technology

2.1.1.3. Machine learning

Machine learning enables improved vehicle performance through reliable road user identification and classification. We conduct leading research in the field of deep learning. Our PointPillars research and nuScenes dataset make invaluable contributions to the safety and robustness of AV systems [8] [32].

PointPillars is a novel deep network trained on LIDAR point clouds. Designed for both accuracy and speed, PointPillars yielded state-of-the-art detection and runtime performance on benchmark tests (see Figure 10). By providing fast object detection and classification on large data sets, PointPillars dramatically improves the performance and capability of LIDAR data processing which in turn provides a better view of the world the AV navigates.

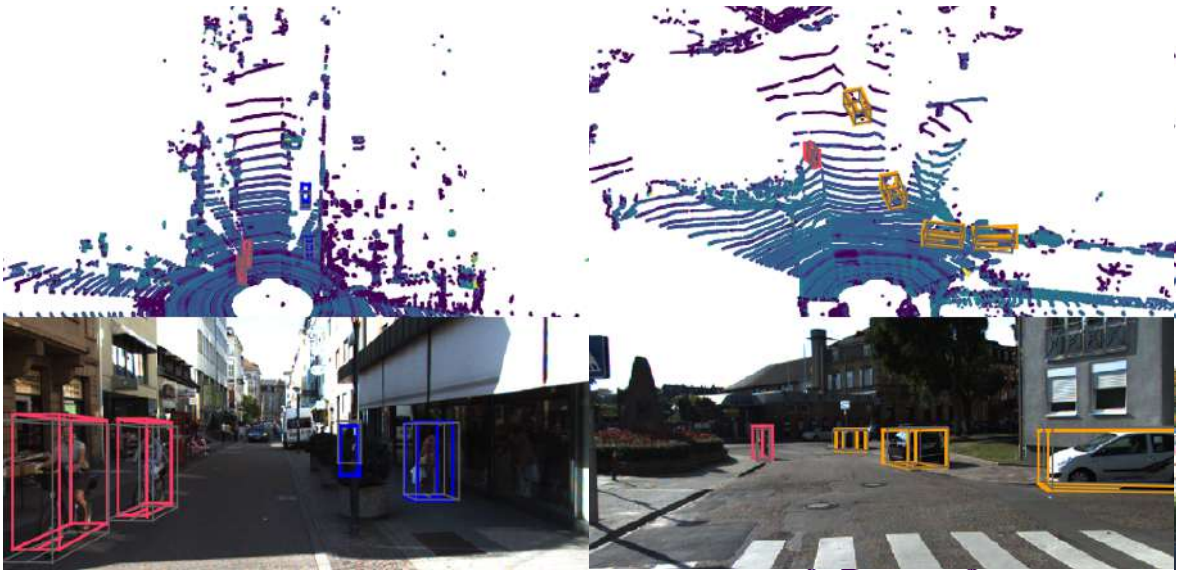
In March 2019, our team released nuScenes. The first publicly available dataset of its kind, nuScenes is a collection of 1,000 real-world street scenes that inform and help advance the machine-learning models that ultimately enable the creation of safe AVs.

FIGURE 10: QUALITATIVE ANALYSIS OF POINTPILLARS DETECTION RESULTS, SHOWING A BIRD'S-EYE VIEW OF THE LIDAR POINT CLOUD (TOP) AS WELL AS THE THREE-DIMENSIONAL BOUNDING BOXES PROJECTED INTO THE IMAGE FOR CLEARER VISUALIZATION [32]

An industry first for scale and sophistication, nuScenes provides data collected through public road testing in Singapore and Boston. The street scenes consist of meticulous hand annotations of millions of photos and data points from our AVs' full sensor suites. The data set delivers unique and challenging urban driving situations, including both left-side and right-side driving.

In 2020, nuScenes became more robust with the additions of nuScenes-LIDARseg and nuImages. nuScenes-LIDARseg is the industry's first dataset with LIDAR segmentation annotations, adding one of 32 point-level labels, such as a car, bicycle, or pedestrian, to the LIDAR points of 40,000 keyframes. This resulted in 1,400,000,000 annotated LIDAR points. Our nuImages dataset, which is the largest commercial offering of its kind, comprises 93,000 images. It complements nuScenes' three-dimensional nature through annotations with approximately 800,000 two-dimensional bounding boxes, instance segmentation masks for objects and two-dimensional segmentation masks for background classes. The team behind nuImages mined for difficult images to generate a dataset with numerous edge cases and challenging driving conditions.

At the time of the publication of our VSSA, more than 9,000 researchers and more than 389 scientific papers have used nuScenes data. Across the industry, many organizations followed suit in releasing their own data, generating a collective body of shared knowledge and progressive research.



2. AV technology

Our published research and datasets make invaluable contributions to the safety and robustness of AV systems.

2.1.2. Localization and positioning

Object detection and path planning rely on the AV's understanding of its physical location and orientation, including relative to the immediate surroundings and road infrastructure. The localization system uses range-based sensors to create a detailed data impression of the vehicle's surroundings. The system compares this information with a pre-made, high-resolution map to pinpoint the vehicle location. Combined with a global positioning system (GPS) unit, inertial sensors, and the vehicle's odometry data (from the wheel rotations), this system yields highly reliable and accurate localization and positioning of the AV.

2.1.3. Maps

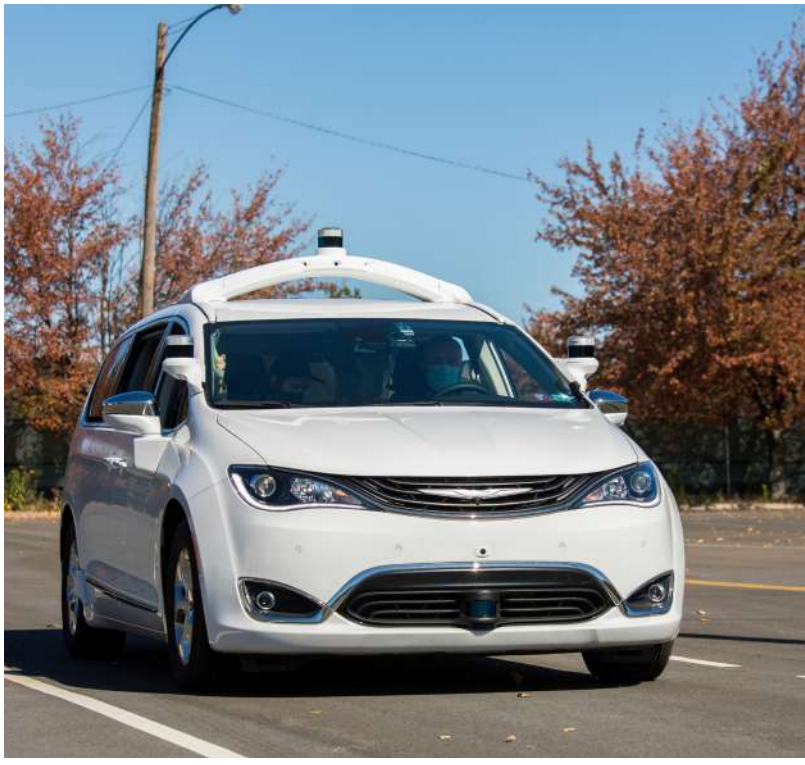
We generate detailed maps of public roads and closed course test areas for our AVs to orient themselves and navigate from point to point. The map includes layers of information on lanes and intersections, which provides context to localization and detected objects. We regularly update our maps to capture changes, and our maps are capable of dealing with dynamic elements (e.g., construction zones).

2.1.4. Path planning

The path planning system builds a map of multiple possible paths for the AV to consider based on sensor fusion and localization system output (e.g., location of pedestrians, cyclists, and other vehicles relative to the AV). The planning algorithm rapidly evaluates properties of these paths to select the best path according to our evaluation framework, which includes safety, traffic laws, common driving practices, and driving preferences (see section 5.2).

2.1.5. Vehicle control

The planning system communicates the path to the control module, which translates the path into precise actuator control messages. The control module contains a vehicle dynamics model that uses real-time information about vehicle state and location based on onboard sensors, such as inertial measurement unit (IMU) and odometry sensors. The dynamic model ensures stable and smooth execution of a desired path. Our control systems also consume information about the vehicle path relative to objects and other road users, which provides another opportunity to verify the planned path.



2. AV technology

2.2. Fallback systems

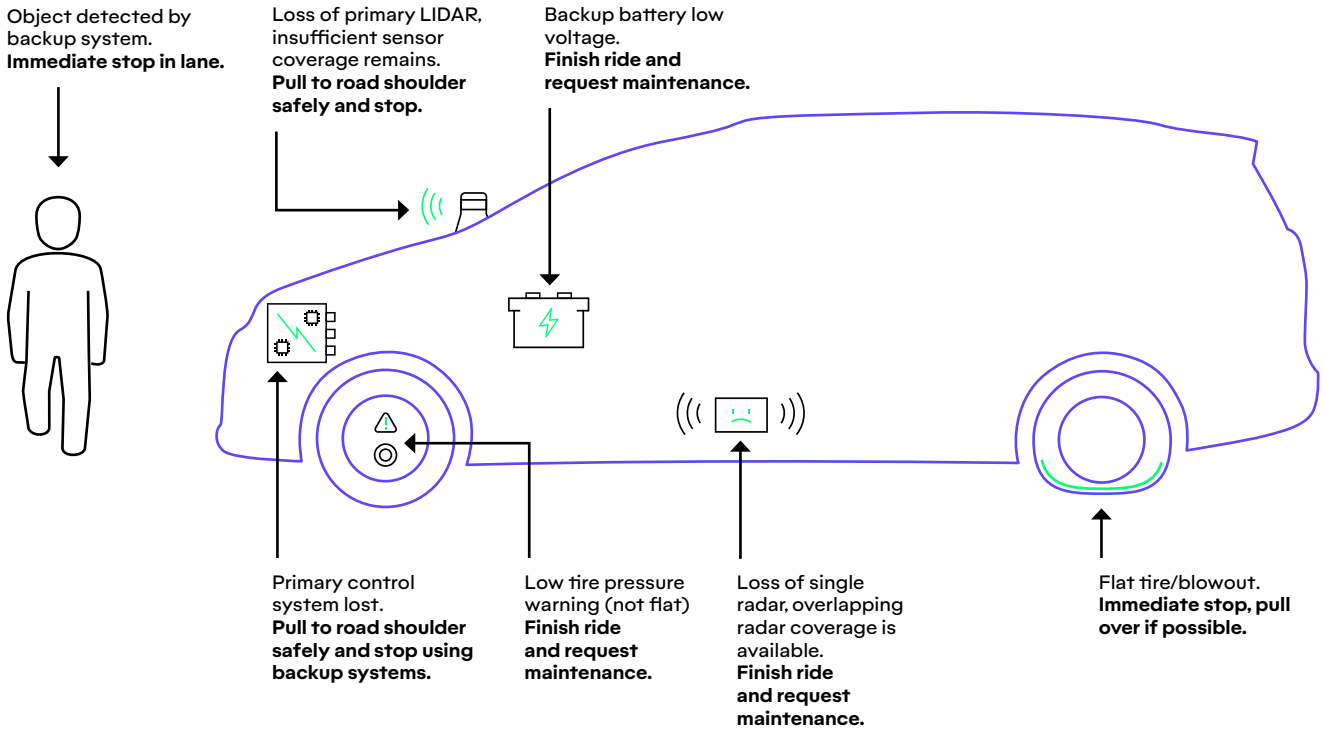
Any system (especially a complex system operating in a dynamic environment) can experience faults. A fault is an "abnormal condition that can cause an element or an item to fail" [13]. Examples include a sensor failure, a software module experiencing an unexpected error or a bug, or a communication failure. Our AV system includes a system monitoring capability to detect and respond to such faults in a safe and effective way, resulting in a robust overall AV system.

We use tiers of failures according to criticality and urgency to manage the severity and system impact of failures (see Figure 11). These tiers range from issues that affect comfort only to critical system failures that trigger an immediate stop.

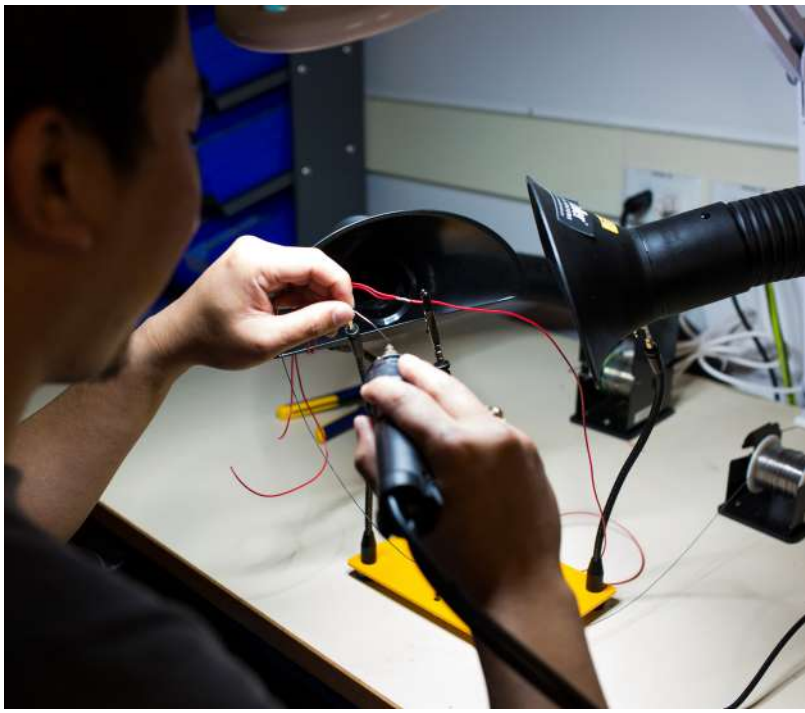
Diversity and redundancy are key principles for designing a robust system [13]. Completing a task in several different ways and comparing the results increases our confidence in the results. One example of this approach is our use of multiple sensor types to leverage their individual strengths and improve robustness.

Depending on the maturity of an AV system and the associated level of human supervision (i.e., development stage I, II, or III), we employ different strategies for fault detection and fallback. For AV testing prior to self-driving release (Stage I), the safety drivers and safety engineers serve as the primary fallback system. They monitor vehicle behavior, respond to system issues, and can quickly take control if AV performance does not match other road users' or our own expectations.

FIGURE 11: ILLUSTRATION OF TIERED FAILURES TO GUIDE APPROPRIATE SYSTEM RESPONSES



2. AV technology



2.2. Fallback systems cont.

For the prototype development stage (Stage II), we design a fallback system that aims to bring the vehicle to a stop if it detects a potential collision or a critical failure. The fallback system we use during the prototype development stage supplements the primary AV system by providing an additional mechanism for detecting and responding to potential obstacles. We train the AV stewards specifically to operate with this fallback system. The fallback system uses separate hardware, including power and network systems, to prevent any hardware failures from affecting both the primary and fallback systems.

As we progress to fully self-driving AV operation (Stage III), the AV's core capabilities provide the redundancy, fault monitoring, and fallback functionalities that enable safe operation without manual supervision. These functionalities enable the system to autonomously achieve a safe state in any failure situation, consistent with safety principles (see subsection 1.1.1). In Stage III, the AV's operational scope includes managing situations such as a vehicle platform hardware failure (e.g., a flat tire), a road condition outside of the AV's ODD (e.g., a sudden sandstorm or downpour), damage to one of the AV subsystems (e.g., a sensor or backup battery failure), or a rare and serious failure of the primary AV system (e.g., loss of localization). While teleoperator assistance and remote support (see subsection 3.2.4) may help resolve problems that arise during operation, they are not essential for safe operation of the AV.

Redundancy, fault monitoring, and fallback functionalities enable safe operation without manual supervision.

2.3. Vehicle platforms

Our AV systems operate on vehicle platforms from original equipment manufacturers (OEMs). Since these vehicle platforms are a key component that impacts AV safety and performance, our Safety Readiness assessment (see section 1.4) carefully considers the design of the vehicle platform and how our AV system integrates with it.

Our vehicle platform choices consider safety, capability, robustness, and vehicle maturity. We leverage advanced passive safety systems in our vehicle platforms to keep our passengers and operators safe. We use direct connections to the vehicle controllers to support the AV system's actuation requests, power, and communication needs. We ensure that our vehicles continue to comply with crashworthiness regulations after making modifications needed for the integration with the AV system. We strive to make the AV system as complementary as possible to the base vehicle.

2. AV technology

2.3.1. Vehicle integration

An ideal vehicle platform provides a comprehensive vehicle control interface, access to vehicle diagnostic data, actuator redundancy, and a suitable vehicle design. These features simplify our work to integrate AV systems with the base vehicle.

Precise and reliable software and hardware interfaces for the actuators (i.e., steering, braking, acceleration, gear shifting) enable the AV system to accurately control the vehicle, and to transition control to and from the safety driver, when present. Vehicle platforms that will operate without a safety driver also provide redundancy in any safety-critical systems. In a conventional human-driven vehicle, the driver can act as a backup. For example, the driver can manage a failure in the power-assisted brakes by applying additional force on the brake pedal. In a vehicle platform that will operate without a driver, redundancy in actuation, power, and network enables the AV system to cope with component failures.

We also consider practical requirements for the vehicle platform. Electrical and network systems need to support the computing demand from the AV system. The vehicle needs to have physical space to safely package and install system components while maintaining good weight distribution for performance and safety, including crashworthiness (see subsection 2.3.2). As we make design choices, we strive for continuous collaboration with the OEM to ensure optimal integration.

2.3.2. Crashworthiness

We work with the OEM to identify and plan the various locations on the vehicle to place our sensors and compute components. While evaluating a design, we review the local and federal regulations related to crashworthiness [33]. This may include the following:

- Federal Motor Vehicle Safety Standards;
- State inspections and registration requirements;
- Publicly available compliance tests; and
- Certified national and international industry standards.

We evaluate whether any regulatory requirements necessitate changes to the vehicle or its subsystems. We analyze the previously recorded test data from vehicle compliance tests to simulate forces and loads on our added components to ensure that the vehicle is safe. We also consider whether an application for an exemption is appropriate for any of the modifications.

We then build a prototype and conduct additional review of the AV system's physical implementation. The above standards and public documentation do not address certain aspects of physical routing of connections, placement of components, or final loading of the vehicle. We work closely with the OEM and adhere to their routing of wires around the vehicle frame, airbag components, and any special considerations of crash structures for protection of the vehicle occupants. Additionally, we employ independent parties to review and assess our vehicles throughout development. ■

3. AV operation

3. AV operation

Our approach to safety and validation extends beyond a single vehicle. It encompasses the entire AV ecosystem, which includes the environment where the AV operates, AV operators, and fleet operations.

3.1. ODD

The ODD "describes the specific operating domains in which an [AV] is designed to function with respect to roadway types, speed range, lighting conditions (day and/or night), weather conditions, and other operations constraints" [30]. The ODD provides requirements for the AV without specifically stating how to develop the AV or how to handle a situation. We create the ODD definition along with the initial safety work products (see subsection 1.2.1), although it may evolve over time. The high-level categories of ODD that we consider include static geographic elements and dynamic environmental elements [34].

Our AV system is geo-fenced, which means that we control static geographic elements by including or excluding them in our mapped routes. The constraints and maneuvering capabilities of the AV affect the static geographic elements of the ODD. Static geographic elements include the following:

- **Speed:** AV upper speed limits restrict the AV to specific roads. The AV does not operate autonomously on roads with a speed limit in excess of the AV's speed limit;
- **Intersections:** for example, three-way stop, traffic lights, roundabouts, and filter lanes;
- **Lane types:** for example, one way, bidirectional, roads with dividers; and
- **Physical infrastructure:** for example, tunnels, bridges, school zones, and bicycle lanes.

Unlike static geographic elements, which are fixed properties of geographical locations, dynamic environmental elements change over time. Therefore, we cannot control for them by specifying where the AV may operate. Instead, we rely on thresholds, operational processes, or other criteria to determine when the AV has reached its dynamic environmental ODD limits and to safely stop operation when this occurs. Examples of dynamic environmental elements include:

- Weather, visibility, and road conditions (e.g., intensity of rain, fog, smoke, or snow, accumulated amount of snow or foliage, oil spills); and
- Road configurations that can change over time (e.g., construction zones, lane closings).

Making use of HARA and SOTIF analysis, we evaluate ODD elements and identify permutations that may be difficult for the AV to handle. We manage these permutations by either adding functionality to the AV to strengthen our capability under those conditions, or by excluding the permutation from operation until we establish confidence. For example, we may consider whether the AV should handle driving on highways at night when light level falls under a specific threshold.

3. AV operation

3.2. AV operators

Human supervision is important to our testing strategy during all three development stages, as well as the ongoing improvement of our AVs. Our trained, attentive human operators provide a flexible and highly capable fallback to our AV systems during development.

We routinely review our operational practices to ensure continued operational safety and effectiveness, and we adhere to local and national regulations relating to the health and safety of our AV operators. For example, during the COVID-19 pandemic we installed plexiglass dividers between AV operator seats and we perform frequent, thorough disinfection.

In addition to AV operators who directly interact with the AV, vehicle engineers and the broader development team provide remote monitoring and support of the fleet. Across the entire company, we foster a culture of safety.

TABLE 1: AV OPERATOR ROLES AND RESPONSIBILITIES

Title	Works with	Seat location	AV-Human Role Summary	
Safety driver	Safety engineer or Safety operator	Driver seat	Interface	No display or simple unobtrusive display, steering wheel, accelerator pedal, brake pedal, vehicle control keys
			Responsibilities	Monitor environment and take over vehicle control if necessary
Safety engineer	Safety driver	Front passenger seat	Interface	Display with engineering view, vehicle control keys, keyboard/touchpad
			Responsibility	Monitor AV system in code testing scenarios, instruct driver takeover if necessary
Safety operator	Safety driver	Front passenger seat	Interface	Display, vehicle control keys
			Responsibility	Monitor AV system, monitor passenger experience
AV steward	None	Front passenger seat	Interface	Display with simplified AV steward view, E-Stop, comfort stop, vehicle control keys
			Responsibility	Monitor environment and AV system, initiate stopping procedure if necessary

3. AV operation

All safety drivers, safety engineers, safety operators, and AV stewards receive training in defensive driving techniques, have clean driving backgrounds, and have excellent knowledge of road conditions and rules.

3.2.1. Individual AV operator roles

All safety drivers, safety engineers, safety operators, and AV stewards receive training in defensive driving techniques, have clean driving backgrounds, and have excellent knowledge of road conditions and rules. We use a staged testing strategy with different roles and expectations of human operators (see Table 1). We keep individuals in these roles informed of updates and changes in the software they are supervising through release notes, stand-up meetings, and hands-on experience with the software during closed-course testing.

We instruct safety drivers to proactively take control of the vehicle if they are uncomfortable in a driving situation or foresee an unsafe situation. We train our safety drivers to remain vigilant, to be responsible for the vehicle behavior even in autonomous mode, and to take over if they are in doubt [7]. We carefully avoid incentives for our safety drivers to avoid takeovers, and we account for the nature of takeovers (e.g., precautionary, safety-critical) in our internal analyses of AV performance. Safety engineers assist safety drivers during engineering testing of the AV system on public roads or a closed course. During pilot rides for ride-hailing customers, and demo rides (that emphasize rider experience rather than testing of newer engineering builds), safety operators assist the safety driver by monitoring both the AV system and the passenger experience.

The AV steward operates the vehicle without a safety driver on mature AV prototype systems (Stage II). The role of the AV steward is to monitor the environment and AV performance. Like safety drivers, AV stewards receive training to expect the unexpected and have experience in driving manually and operating AVs. The AV steward sits in the passenger seat and interacts with the AV through various interfaces (see Table 1). AV operation with only an AV steward (i.e., no safety driver) takes place in vehicles that have primary and fallback systems (see section 2.2) specifically designed to ensure robust and safe operation, and occurs only after extensive validation of the system (see section 1.3). If the AV steward observes an issue (through audible alarm and/or displayed on the screen), or encounters a scenario that is outside the ODD, the AV steward can use an emergency stop (E-Stop) or a comfort stop to halt the vehicle, depending on the nature of the issue.

7. A safety driver takeover disengages the vehicle from autonomous mode and returns it to manual mode.

3. AV operation

3.2.2. Safety culture

At Motional, we work hard to maintain a culture of safety. We articulate this with our policy that anyone can press the metaphorical "Red Button", referring to the typical red button available to immediately halt machinery or robotics. Our metaphorical Red Button applies not only to public road operation, but also to any activity that could carry or identify risk (e.g., a workshop, simulation, or closed course testing).

If anyone, from a newly hired safety operator to a senior executive, believes that an operation may be unsafe or unreasonably risky and decides to raise a Red Button issue, our policy is to pause the affected operation, gather the proper stakeholders, evaluate the safety and risks, and make any necessary short- or long-term changes. Our Red Button process empowers all employees to take active ownership of safety. This process highlights the value we place on a thoughtful and safety-conscious culture.

Our safety culture extends to work expectations for AV operators. Our testing staff comprises motivated, experienced, serious, well-trained professionals. However, we recognize that there are limits to human attention and therefore we design our testing schedule so our AV operators can reasonably deliver their best performance. We also encourage and train our AV operators to monitor their own mental state and fatigue levels and to decline to operate a vehicle if they do not feel they can do so safely. We provide no incentives to drive more hours and no penalties for declining to drive.

Our Red Button process empowers all employees to take active ownership of safety.

We perform our testing in teams of safety drivers paired with a safety engineer or operator, which provides an opportunity for the two to help each other maintain focus and ensure mutual accountability. The self-driving operation with a single AV steward will use short trips and low overall testing volume to limit any risk of the AV steward being unable to adequately supervise the vehicle.

As we develop testing plans for increasingly reliable systems that need less and less supervision or intervention, the ability of our testing staff to reliably maintain focus is an integral consideration in our test design. Currently, we mainly use human factors, such as shift length, two-person teams, time of day, and mandatory breaks to maintain reasonable expectations for the attention that our AV operators can provide. As we continue to scale our testing operations, we are evaluating and implementing various technical tools to maintain and monitor AV operator attention, such as gaze monitoring and intermittent interaction prompts.

As part of our safety culture, we also provide the initial training and ongoing learning and development curriculum described below.

3. AV operation

We continuously develop the skills of our testing employees by providing advanced practice and training on topics like defensive driving skills.

3.2.3. Personnel and training

It is important that we find the right candidates for the AV operator roles. We seek out good defensive driving skills, an excellent driving record, great observation skills, and an ability to handle unexpected situations. Our hiring process includes interviews, closed course driving tests, and background and drug screenings.

Training for all AV operators includes three main parts: (1) instructor-led classroom learning and assessment, (2) a hands-on in-vehicle mentoring and performance assessment, and (3) self-directed and instructor-led continuing education and assessment. This training protocol helps ensure that all testing personnel have a thorough understanding of the vehicle and AV system behavior as well as experience operating AVs on a closed course before proceeding to public road testing.

The training also includes material on defensive driving, driving etiquette, proper procedures for systems checks and corresponding documentation, and incident response plans (see section 3.3). While much of the material is uniform across our testing sites, we include site-specific content as needed (e.g., materials on local traffic laws or road features). Our accredited learning management system provides traceability in the training regimen [35].

Following training for new AV operators, we continue to develop the skills of our testing employees by providing advanced practice and training on topics like defensive driving skills. Less formally, we keep our drivers and all testing personnel informed and encourage them to improve their knowledge and skills in frequent stand-up meetings to discuss vehicle behaviors, changes, procedures, and best practices. While we have the highest confidence in our testing personnel, we also have strict disciplinary procedures to address behaviors that do not conform to our policies and safety guidelines.

3.2.4. Remote vehicle monitoring and assistance

We use a fleet management system that monitors vehicles individually and as a fleet, performs centralized dispatch, and manages software versions and updates (see also section 4.2). Today, cloud-based vehicle control focuses on the dispatch level, defining a route or destination and directing the AV to proceed when ready under normal autonomous operation. We may add additional remote assistance to help with object classification when the AV is stopped, propose a safe path, or provide other inputs to assist the AV in navigating an unusual situation. No commands that are critical to ensuring safe real-time vehicle operation come via a remote connection.

We do not currently allow direct remote real-time operation of the AV because of the following challenges:

- Maintenance of reliable wireless connections;
- The dynamic nature of difficult on-road situations;
- Signal latency between the vehicle on the road and a remote operator; and
- The need for increasingly rigorous cybersecurity standards.

We will continue to track progress in resolving these challenges to direct remote operation and revise our approach to remote assistance accordingly.

3. AV operation

3.3. Incident response and management

In addition to system and operational safety, we recognize our incident response and management program as a critical component of overall AV fleet safety (see Figure 12).

Two foundational elements underpin our incident response and management program. First, our safety culture includes extensive training and development of AV operators to prevent incidents and includes the Red Button process to proactively investigate and address potential issues. Second, our incident response and management program emphasizes involvement of appropriate internal and external stakeholders in our processes for responding to incidents.

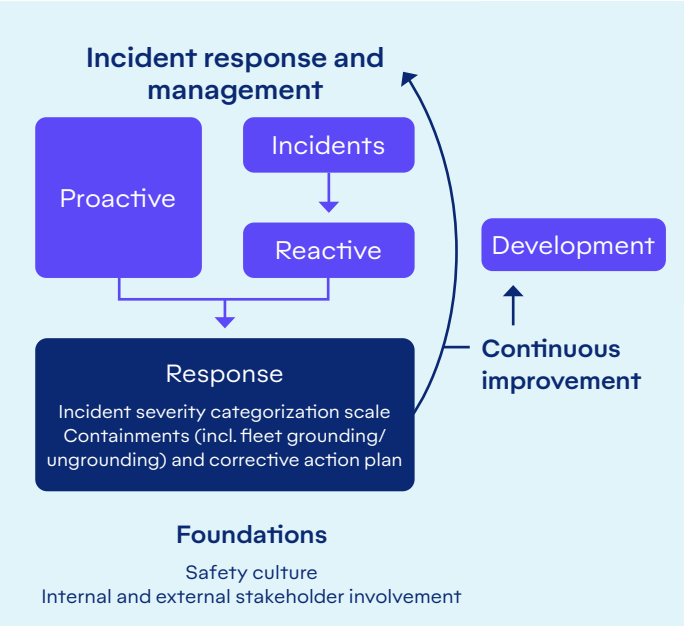
Our incident response and management program encompasses both proactive processes to respond to safety-critical issues we may identify (e.g., through the Red Button process) and reactive processes to respond to potential incidents involving our AVs. These processes use an incident severity categorization scale as a systematic method for assigning severity to an issue or incident based on the probability and consequences of different potential outcomes. Leveraging this common scale, we can react appropriately from an operational, information-sharing, and timeliness perspective.

A proactive issue or reactive incident triggers containment measures that may result in vehicle and/or fleet grounding. Once grounded, we do not redeploy a vehicle into our fleet until we complete an ungrounding process across all affected vehicles. The ungrounding process begins with a corrective action plan and concludes when we demonstrate the implementation of a solution that addresses the hazard and after we determine that the vehicle(s) is/are safe to return to service.

Our business, fleet, and AV technology constantly evolve as both the AV ecosystem and levels of market preparedness mature. As the technology develops, we continually learn and adapt through a robust, post-incident feedback loop. This feedback loop ensures that we periodically review our incident response and management program and revise it with our partners to keep it state-of-the-art. The feedback loop also supports our efforts to continuously improve our technologies to maximize safety (see subsection 1.3.4). By capturing learnings from each incident and feeding them back into development, we ensure that processes continue to evolve alongside the AV ecosystem.

An example of continuous evolution alongside partners is our regular collaboration with first responders in the markets in which we operate. These partnerships consistently prove to be mutually beneficial in multiple ways. For example, we introduce first responders to our vehicles and provide education on AV technology. This enables responder teams to better understand how to respond safely to an incident involving an AV. Furthermore, regular collaboration allows us to build a product that meets stakeholder needs. In this example, first responder feedback is a critical component of developing technologies that not only recognize emergency vehicles and personnel, but that are also able to respond appropriately. Finally, information exchange with external partners improves safe deployment of AVs by enabling the development and evolution of standard operating procedures. ■

FIGURE 12: OVERVIEW OF OUR INCIDENT RESPONSE AND MANAGEMENT



4. Interfaces

4. Interfaces

While navigating roads and providing rides, an AV interfaces with many entities, including passengers, pedestrians, and other vehicles. The AV also interfaces with data systems used to monitor the fleet from a command center, provide remote customer assistance, and provide remote technical assistance to the AV.

These interfaces enable the AV to effectively and efficiently complete typical tasks and are also important to the overall safety of the AV operation. For example, passengers may need to safely stop the vehicle during their ride if an unexpected issue arises. We also use data retrieved from an AV during development to improve performance and safety. However, these important interfaces can make vehicle software vulnerable, and protecting against malicious intent is therefore also part of safe AV development and operation.

4.1. Passenger and road user interface

We strive to provide a safe and pleasant journey while building confidence in the AV and trust among passengers and surrounding road users. We achieve this through effective communication during the journey in the vehicle. In our on-road pilots, our safety operators handle this communication since they explain how the AV interacts with the world around it.

We strive to provide a safe and pleasant journey while building confidence in the AV.

In a fully self-driving AV, the communication will occur via systems within the vehicle, such as tactile buttons, cameras, and touchscreen passenger displays paired with audible feedback. The tactile buttons in the AV allow the passengers to request a stop or call a supervisor working remotely in a command center. The passenger displays provide instructions to the passenger for pick up, safety during the ride, and drop off. These displays have an easily understood interactive visualization of the route and the immediate surroundings to show the passengers a simplified view of what the AV is detecting. We are also exploring communication of intention and function to other road users using motion-based, visual, and/or audible technologies.

We work with local law enforcement and first responders to help them understand where and how our vehicles operate. Currently, our AV operators handle all necessary interaction with law enforcement and first responders. We are actively researching the inclusion of best practices from first responders in the design of our AVs. This collaborative partnership further aims to ensure that local law enforcement and first responders know how to interact with our AVs.

4. Interfaces

4.2. Cybersecurity

Our safety and cybersecurity teams work together to design and build AVs that will operate safely even in the presence of malicious actors. We have established engineering processes that help us consistently and proactively discover and address cybersecurity threats. We base our cybersecurity processes on publications from numerous public authorities and industry organizations[8]. Besides standards organizations, we collaborate with security experts across industry and academia to evolve our processes and evaluate our AVs.

Central to our efforts is our AV security development lifecycle (SDL) [36]. This SDL prescribes security activities and practices that find and address threats and vulnerabilities via methods tailored to each development phase. Our SDL framework supports hardware and software components we develop and guides us in how we specify, select, and include components we source from third parties.

For hardware, the SDL ensures we define security requirements early, adapt our goals as projects evolve, and review security at defined touchpoints, including via techniques like penetration tests. The SDL further helps us understand the threats relevant to individual components and the implications of integrating those components into our AV system. In particular, we use a threat analysis and risk assessment framework inspired heavily by an industry-leading threat modeling framework [37] that asks the following questions:

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

8. Specifically, NHTSA, the Automotive Information Sharing and Analysis Center [49], the British Standards Institution [54], ISO [40], the National Institute of Standards Technology [58] [59], SAE [55], SAFECode [52], and the Safety Critical System Club [51].

We have established engineering processes that help us consistently and proactively discover and address cybersecurity threats.

For software, the SDL covers similar ground. However, the SDL as applied to software further includes standard practices among software companies that develop high-quality, secure software. We threat-model all our AV systems and perform a risk analysis for each threat. While defining mitigations for threats we cannot accept or avoid, we identified four key measures we consider broadly effective in securing self-driving systems:

- Secure boot, which ensures devices will run only untampered firmware provided by the vendor;
- Device identity and authentication, which ensures that we can soundly identify devices at runtime and the entities that may configure or update them;
- Secure communications, which prevent device data traveling between system nodes from being forged or altered;
- Secure updates, which ensure we can counter improved attacks and fix newly discovered problems without human intervention per vehicle or device.

In addition to these measures, we use tools that allow us to automate enforcement of coding standards [38] while also checking for common issues identified in the Common Weakness Enumeration framework [39]. Modern compilers come with sanitizers we use during code testing to dynamically detect memory corruption, memory leaks, and undefined behaviors.

The SDL helps us quickly identify risks so that we can design, specify, and implement mitigating security features, including for third-party components. We track common vulnerabilities and exposures in third-party packages to promptly roll out mitigating measures. To further ensure sufficient security protection in third-party components, we specify penetration testing for supplied software. We will also begin to require suppliers to adhere to ISO 21434 [40] once released.

4. Interfaces

4.2. Cybersecurity cont.

We have a cybersecurity lab staffed by expert automotive penetration testers. Our lab annually tests our AV systems, and we design our security processes for continuous improvement based on internal and external teachings. Our combined cybersecurity practices lead to increasingly robust AV products.

We have developed monitoring and incident response processes (see section 3.3) specific to cybersecurity. We regularly practice these processes using tabletop exercises and training to make sure all stakeholders understand our processes. We ensure protocols remain best-in-class by treating these as dynamic processes that continually evolve alongside the AV and cybersecurity ecosystems. To enable continuous improvement, we record and feed back any cybersecurity incidents discovered on the road through our incident response and management or through the Road Release process.

We are committed to cybersecurity practices that align with industry and support our mission of delivering a safe and secure AV. We are seeking formal ISO 21434 certification upon its release. We are working with an external auditor who has attested that our SDL framework complies with the standard as currently drafted.

4.3. Data management

Our AVs generate and log large amounts of data from their sensors and software. The data represent a critical interface between the AVs and our broader ecosystem that we must manage securely and efficiently. Our data management strategy supports the following safety-related objectives:

- Record and retain data around novel and technically interesting scenarios observed on the road, on our closed course test facilities, and in simulation to identify and address issues and to continuously learn and improve vehicle safety and performance;
- Provide information on serious road incidents to relevant authorities; and
- Share data to encourage collaboration, advance research and technology, and improve safety across industry and the wider academic community.

A fleet of AVs generates valuable data that inform design decisions to continuously make our vehicles safer and better performing. To be able to use data to improve our systems, we must take care to maintain the integrity of the vehicle data we log. We offload data from dedicated storage devices on each AV using purpose-built hardware and software, which verifies log integrity, generates metadata, and provides a complete and encrypted upload to our private storage servers and clouds (see Figure 13). To further ensure the integrity of our data, we limit access to enumerated individuals using personal electronic credentials; a strictly limited number of employees have read-write access to aspects of our storage servers. A larger number of employees have read-only access and high-speed internal connections to vehicle data. This allows real-world performance of our AVs to drive internal development and testing across our teams.

A fleet of AVs generates valuable data that inform design decisions to continuously make our vehicles safer.

4. Interfaces

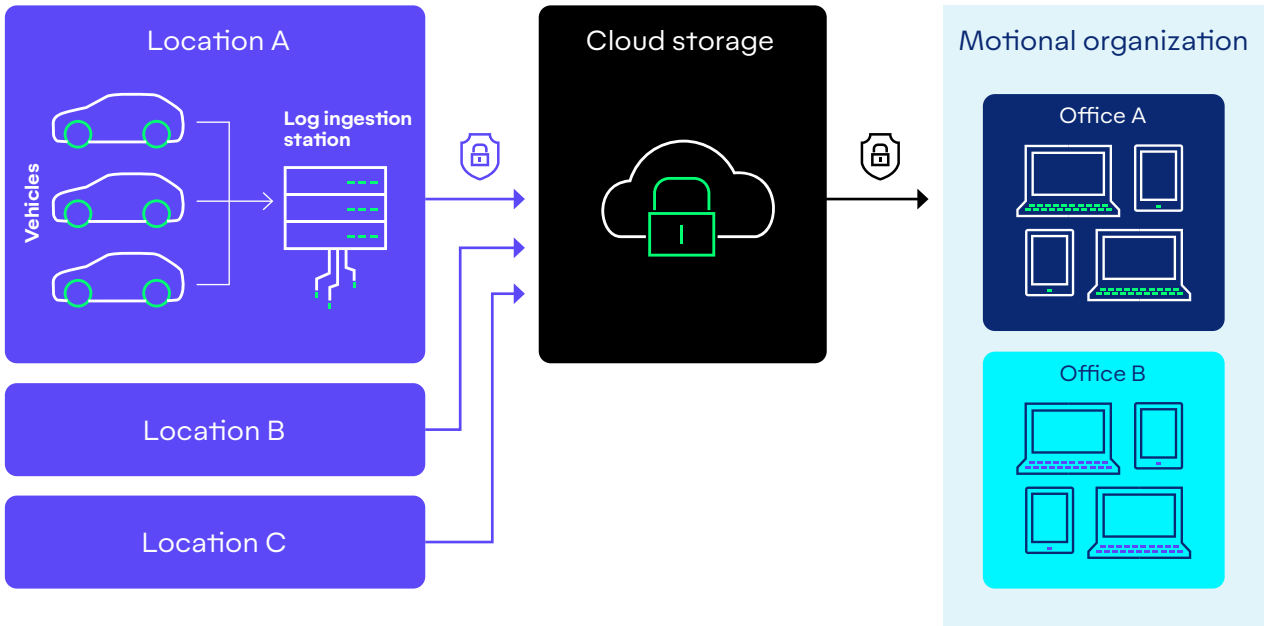
4.3. Data management cont.

In the context of the large volume of data that our AV fleets generate, certain slices of data are more valuable than others. Therefore, we optimize our data storage around incidents that help us improve our systems and/or may require review by authorities. Retaining slices of log data at full resolution allows us to internally reconstruct and investigate events to determine and address the causes, including:

- Incidents resulting in a collision or near-collision;
- Safety driver takeovers;
- Activations of the fallback mechanism (including false positive activations in shadow mode, as described in subsection 1.3.3);
- Missed or late detections of other road users;
- Rare or unusual road users and decor (e.g., costumes, extreme vehicle modifications);
- Unexpected maneuvers performed by road users; and
- AV behavior that is subjectively concerning to an AV operator.

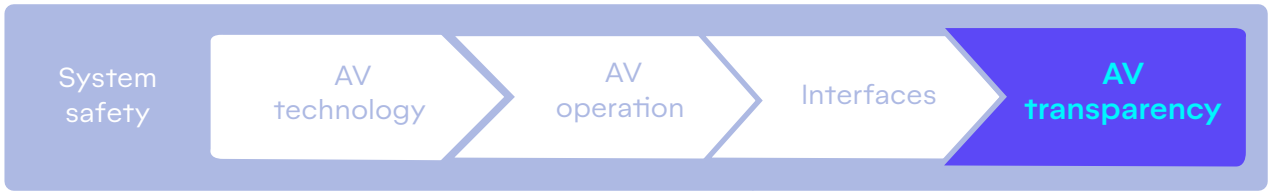
To help identify the most interesting slices of log data, AV operators flag events in real time based on feedback from the safety driver, on events that occur in traffic, and on monitoring of AV software behavior and metrics. We also use algorithms to automatically detect interesting events for investigation. The logs from these events enable us to learn from experience and create a comprehensive library of simulation scenarios to test new algorithms and software (see subsection 1.3.1). ■

FIGURE 13: OUR DATA PIPELINE



5. AV transparency

5. AV transparency



We believe that developing a safe self-driving taxi service requires developing not only robust technology, but also robust support and trust with passengers, regulators, and the public. Having conducted the first public self-driving taxi trial, our relationship with communities goes back to the earliest days of our AV technology development. We encode our goals of delivering a trustworthy and transparent self-driving taxi service in our technical approach to building a safe AV.

5.1. Public education

We work closely with city officials and non-governmental organizations that focus on safe mobility and with passengers to show them our operations and demonstrate our AVs.

Our extensive public deployment in Las Vegas provides us with a significant primary research testbed for understanding public and passenger perception of AVs, and offers a channel for conducting educational and collaborative campaigns directly for members of the public. We have provided more than 100,000 rides in Las Vegas, with 98% of riders rating their experience as five out of five stars. We have also hosted self-driving taxi ride demonstrations in Boston, Singapore, and Pittsburgh for city officials, non-governmental organizations, passenger focus groups, and first responders.

Our dialogue with the public engages those with limited mobility, including blind and low vision people and the elderly [41]. We believe that public demonstrations and open dialogue with passengers are critical parts of shaping our self-driving taxi product in a manner that truly benefits our communities.

Our team is committed to developing trust in our AV technology through transparency. As such, in addition to this VSSA, we have shared information with the public, including an open-source dataset (see subsection 2.1.1.3) and the public release of SAFAD. Moreover, our approach to compliance with the rules of the road emphasizes transparency of our AV behavior definition.

We believe that public demonstrations and open dialogue with passengers are critical parts of shaping our self-driving taxi product.

5. AV transparency

We believe that open discussion among government institutions, the general public, and industry players will ultimately lead to the safest possible deployment of AVs.

5.2. Rulebooks for federal, state, and local laws

We are committed to complying with all applicable international, federal, state, and local laws in locations where we operate. In particular, we are committed to complying with the rules of the road and their local nuances to the greatest extent possible. Because traffic laws, as currently written, are not suitable for AV interpretation, we developed the Rulebooks approach to encode rule compliance. We use this framework to design AV behavior in a way that explicitly considers the rules of the road and the priority between these rules [9]. This formal framework offers an approach with the following key strengths:

- Explainable and unambiguous: rules are explicit and the degree of violation of a rule is measurable;
- Traceable to decision-making: the framework allows humans to understand why an AV makes any given driving decision;
- Internally consistent: the framework specifies the priorities among rules in an internally consistent way across all scenarios the AV may encounter in its ODD; and
- Scalable: one can adapt the rules and the hierarchy according to the local rules of the road.

The process of formalizing rules and developing priority is complex. Therefore, we believe it is the collective responsibility of the general public, government, and AV industry to agree on a set of behavior rules for AVs.

5.3. Standards collaboration

Our collaboration with industry partners and government institutions helps shape the technology landscape through the publication of research papers and international standards. For example, we played an instrumental role in the creation of Singapore's Technical Reference 68 (TR 68) for AVs [10]. This work reflects a collaboration between industry, academia, and government organizations to create a balanced guideline. In Las Vegas, we work closely with the Regional Transportation Commission of Southern Nevada to align with the transportation needs of the local public. SAFAD represents a collaboration between industry competitors to agree on an appropriate framework for AV safety and form the foundation of a broadly accepted standard. Motional is also working with a broad range of government and industry stakeholders to develop a new standard that defines minimal assumptions and scenarios for models of safe AV behavior [42].

We recognize that open discourse with society to develop standards results in increased governance and administration of safety assessments. The authorities, in turn, recognize that the deep knowledge required for effective regulation is primarily available from the AV companies. We strongly believe that open discussion among government institutions, the general public, and industry players will ultimately lead to the safest possible deployment of AVs. Where possible, we continue to take opportunities to share our experience and thoughts about safety, as well as encourage dialogue among industry stakeholders. ■

Glossary

Term	Definition
Actuator	A mechanical vehicle component that controls motion (e.g., braking pedal, steering wheel, throttle)
Automotive Safety Integrity Level (ASIL)	"One of four levels to specify the item's or element's necessary ISO 26262 requirements and safety measures to apply for avoiding an unreasonable risk, with D representing the most stringent and A the least stringent level" [13]
Autonomous Vehicle (AV)	A driving system consisting of software, hardware, and a vehicle platform that can autonomously perform the driving task without the help of a human driver (SAE Autonomy Level 4 or 5); also known as self-driving car, self-driving vehicle, driverless car, driverless vehicle, autonomous driving system, highly automated vehicle, highly automated driving system
AV ecosystem	The broad system that enables a self-driving taxi service, including the AV technology itself, ODD, fleet operations, and human interactions with the AVs
AV steward	A trained human AV operator sitting in the passenger seat with responsibility to monitor the environment and AV system and to take over using the E-Stop button if necessary
AV system	The hardware and software system that enables an AV's self-driving operation; also known as autonomous or driverless system, highly automated driving system
AV technology	The software algorithms, hardware components, subsystems, interfaces, and architecture needed to build an AV
Collision (motor vehicle)	A motor vehicle incident involving contact between the motor vehicle and another road user or obstacle; also known as a motor vehicle crash, accident
Comfort stop	The action of coming to a stop smoothly in a non-emergency situation that aims to avoid discomfort of the AV operators and passenger (as opposed to E-Stop below)
Common vulnerabilities and exposures	A list of "publicly known cybersecurity vulnerabilities" [43]
E-Stop	An emergency stop button that allows a human inside the AV to command a hard brake in the event of an emergency (as opposed to comfort stop above)

Glossary

Term	Definition
Failure Mode and Effects Analysis (FMEA)	"A method designed to (i) identify and fully understand potential failure modes and their causes, and the effects of failure on the system or end users, for a given product or process; (ii) assess the risk associated with the identified failure modes, effects and causes, and prioritize issues for corrective action; and (iii) Identify and carry out corrective actions to address the most serious concerns" [44]
Fault	An "abnormal condition that can cause an element or an item to fail" [13]
Fault Tree Analysis (FTA)	"A deductive procedure used to determine the various combinations of hardware and software failures and human errors that could cause undesired events (referred to as top events) at the system level" [45]
Functional safety	The "absence of unreasonable risk due to hazards caused by malfunctioning behavior of [electrical and/or electronic] systems" [13]
Hardware-In-the-Loop (HIL)	The testing environment in which "target software is executed on target hardware, whereas the hardware outputs influence the hardware inputs" [5]
Hazard	A "potential source of harm caused by malfunctioning behavior" [13] or other inadequate behavior
Hazard Analysis and Risk Assessment (HARA)	A "method to identify and categorize hazardous events of items and to specify safety goals and ASILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk" [13]
Human-machine interface	The interface between our AV and humans (both operators and passengers) which commonly consists of a display and functional keys
Incident severity categorization scale	A scale of severity of an incident based on several criteria reflecting the probability and consequence of different outcomes
Item definition	A key functional safety deliverable which sets out the functionality of the item under assessment
Lagging and leading measures	Leading measures are "proxy measures of driving behaviors correlated to safety outcomes"; lagging measures are "actual safety outcomes involving harm" [23]
Operational Design Domain (ODD)	"The specific operating domains in which an [AV] is designed to function with respect to roadway types, speed range, lighting conditions (day and/or night), weather conditions, and other operations constraints" [34]
Red Button process	A company process that allows any employee to pause operations out of safety concerns and trigger immediate stakeholder review of the issue

Glossary

Term	Definition
Road Release process	A company process that assesses the maturity of candidate AV systems prior to public road testing during development
Safe design	A design (of a system) developed using state-of-the-art processes which result in acceptably low risk
Safety concept	The "specification of the functional safety requirements, with associated information, their allocation to architectural elements, and their interaction necessary to achieve the safety goals" [13]
Safety driver	A trained human driver sitting in the driver seat of an AV with responsibility to monitor the environment and take over vehicle control from the AV if necessary
Safety engineer	A trained human AV operator sitting in the passenger seat with responsibility to monitor the AV system in code testing scenarios and instruct the safety driver to take over if necessary
Safety Of The Intended Functionality (SOTIF)	The "absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons" [4]
Safety operator	A trained human AV operator with a similar role to a safety engineer, but in the context of pilot rides for ride-hailing customers rather than engineering testing
Safety Readiness assessment	A structural evaluation of the safety of the AV, touching on all aspects of the safety lifecycle
Scenario-based testing	An AV testing practice focused on completing specific driving scenarios in simulation or on a closed course testing facility
Security Development Lifecycle (SDL)	A series of processes in software development that reduces security risks and vulnerabilities
Self-driving taxi	A taxi driven using AV technology instead of a human taxi driver; also known as AV taxi, autonomous taxi, driverless taxi, robotaxi
Shadow mode testing	A testing method in which the system under assessment is not able to actuate any controls but logs activation outputs
Society of Automotive Engineers International Autonomy Level (SAE Autonomy Level)	"Levels of driving automation" ranging from no automation (SAE Autonomy Level 0) to full automation (SAE Autonomy Level 5) [46]

Glossary

Term	Definition
Software-In-the-Loop (SIL)	A testing environment in which "partial target software is executed on prototypical hardware, whereas the software decisions influence the virtually generated stimulus" [5]
Statistical safety testing	An AV testing practice which aims to collect empirical evidence through statistically representative public road driving miles or simulation scenarios
Subsystem	A system that is part of a larger system
System safety	The combination of safe design and thorough validation and testing, tied together in a systematic and integral logical framework
Systems engineering	A field of engineering that covers the design and management of highly complex systems
Systems Theoretic Process Analysis (STPA)	"A relatively new hazard analysis technique based on an extended model of accident causation" [47]
Takeover	An event in which a human overrides the AV's command of the vehicle by assuming manual command of the vehicle controls; also known as disengagement, handover, or override
Validation	"Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled" [17]
Vehicle platform	The base vehicle, comprising mechanical and electrical systems, that hosts the AV technology
Verification	"Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled" [17]

Bibliography

[1] World Health Organization, "Global status report on road safety 2018," World Health Organization, Geneva, Switzerland, 2018.

[2] S. Singh, "Critical reasons for crashes investigated in the national motor vehicle crash causation survey," Report DOT HS 812 115. National Highway Traffic Safety Administration, Washington, DC, 2015.

[3] K. Spieser, K. B. Treleaven, R. Zhang, E. Frazzoli, D. Morton and M. Pavone, "Toward a systematic approach to the design and evaluation of automated mobility-on-demand systems: A case study in Singapore," in Road Vehicle Automation, (Lecture Notes in Mobility), G. Meyer and S. Beiker, Eds., Springer, 2014.

[4] International Organization for Standardization, "ISO/PAS 21448:2019: Road vehicles - Safety of the intended functionality," 2019.

[5] Aptiv; Audi; Baidu; BMW; Continental; Daimler; Fiat Chrysler; HERE; Infineon; Intel; Volkswagen, "Safety first for automated driving," 2019.

[6] U.S. Department of Transportation, "Automated driving systems 2.0 — A vision for safety," National Highway Traffic Safety Administration, 2017.

[7] National Science and Technology Council; U.S. Department of Transportation, "Automated vehicles 4.0 — Ensuring American leadership in automated vehicle technologies," National Highway Traffic Safety Administration, 2020.

[8] Motional, "nuScenes," 2020. [Online]. Available: https://www.nuscenes.org/. [Accessed 18 February 2020].

[9] A. Censi, K. Slutsky, T. Wongpiromsarn, D. Yershov, S. Pendleton, J. Fu and E. Frazzoli, "Liability, ethics, and culture-aware behavior specification using rulebooks," in International Conference on Robotics and Automation 2019, Montreal, PQ, 2019.

[10] Singapore Standards Council, "Technical reference 68 for autonomous vehicles," ICS 03.100.70; 43.020. Enterprise Singapore, Singapore, 2019.

[11] International Automotive Task Force, "IATF 16949:2016: Quality management systems standard," 2016.

[12] International Organization for Standardization, "ISO 9001:2015: Quality management systems — Requirements," 2015.

[13] International Organization for Standardization, "ISO 26262: 2018: Road vehicles - Functional safety," 2018.

[14] B. W. Smith, "Automated driving and product liability," Michigan State Law Review, vol. 2017, no. 1, pp. 1-74, 2017.

[15] P. Junietz , U. Steininger and H. Winner, "Macroscopic safety requirements for highly automated driving," Transportation Research Record, vol. 2673, no. 3, pp. 1-10, 2019.

Bibliography

[16] Federal Minister of Transport and Digital Infrastructure (BMVI), "Ethics commission - Automated and connected driving," 2017. [Online]. Available: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission-automated-and-connected-driving.pdf?__blob=publicationFile. [Accessed 20 February 2020].

[17] International Organization for Standardization, "ISO/IEC/IEEE 15288:2015: Systems and software engineering — System life cycle processes," 2015.

[18] Underwriter Laboratories Inc., "Proposed first edition of the standard for safety for the evaluation of autonomous products, UL 4600," [Online]. Available: https://edge-case-research.com/wp-content/uploads/2019/12/191213_UL4600_VotingVersion.pdf. [Accessed 19 February 2020].

[19] European New Car Assessment Programme, "Test protocol – AEB VRU systems," 2017. [Online]. Available: https://cdn.euroncap.com/media/26997/euro-ncap-aeb-vru-test-protocol-v20.pdf. [Accessed 19 February 2020].

[20] W. G. Najm, J. D. Smith and M. Yanagisawa, "Pre-crash scenario typology for crash avoidance research," Report DOT HS 810 767. National Highway Transportation Safety Administration, Washington, DC, 2007.

[21] Federal Ministry for Economic Affairs and Energy, "Pegasus research project," [Online]. Available: https://www.pegasusprojekt.de/en/home. [Accessed 19 February 2020].

[22] N. Kalra and S. M. Paddock, "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?," RAND Corporation, 2016.

[23] L. Fraade-Blanar, M. S. Blumenthal, J. M. Anderson and N. Kalra, "Measuring automated vehicle safety," RAND Corporation, Washington, D.C., 2018.

[24] A. Bin-Nun, A. Panasci and R. J. Duintjer Tebbens, "Applying Heinrich's Triangle to autonomous vehicles—Analyzing the long tail of human and artificial intelligence failures," in Third International Workshop on Artificial Intelligence and safety engineering, Virtual, 2020.

[25] K. A. Hallgren, "Computing inter-rater reliability for observational data: An overview and tutorial," Tutorials in quantitative methods for psychology, vol. 8, no. 1, pp. 23-34, 2012.

[26] W. Wachenfeld and H. Winner, "Virtual assessment of automation in field operation: A new runtime validation method," in Workshop Fahrerassistenzsysteme UNI DAS e.V., Walting, Germany, 2015.

[27] S. Ong, "At Singapore's test center, self-driving cars battle fake monsoons," IEEE Spectrum, 8 April 2019.

[28] A. Aupperlee, "Aptiv self-driving cars navigating Las Vegas Strip with Pittsburgh technology," AP News, 8 January 2018.

[29] A. Vaccaro, "The biggest challenge for self driving cars are Boston seagulls," Boston Globe, 7 February 2017.

[30] nuTonomy, "nuTonomy quarterly AV testing report - First quarter 2017," 2017.

Bibliography

[31] K. Iagnemma, "From Boston to Singapore: Deploying self-driving cars in the most complex urban environments," 20 January 2018. [Online]. Available: https://www.aptiv.com/newsroom/article/from-boston-to-singapore-deploying-self-driving-cars-in-the-most-complex-urban-environments. [Accessed 19 February 2020].

[32] A. Lang, S. Vora, H. Caesar, L. Zhou, J. Yang and O. Beijbom, "PointPillars: Fast encoders for object detection from PointClouds," in Conference on Computer Vision and Pattern Recognition, Long Beach, CA, 2019.

[33] National Highway Traffic Safety Administration, "Federal Motor Vehicle Safety Standards: Standard No. 135; Light vehicle brake systems," 2011, Washington, DC, 2005.

[34] National Highway Traffic Safety Administration, "A framework for automated driving system testable cases and scenarios," Report DOT HS 812 623. National Highway Traffic Safety Administration, Washington, DC, 2018.

[35] International Association for Continuing Education and Training, "Accredited providers list," [Online]. Available: https://www.iacet.org/resources/accredited-providers-list/. [Accessed 19 February 2020].

[36] Microsoft, "Microsoft SDL," [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/. [Accessed 17 April 2020].

[37] A. Shostack, Threat modeling: Designing for security, Indianapolis, IN: John Wiley & Sons, 2014.

[38] A. Ballman, "CERT C++ coding standard," Carnegie Mellon University, 2016.

[39] R. C. Seacord and R. Martin, "CERT C secure coding standard," Addison-Wesley Professional, 2009.

[40] International Organization for Standardization, "ISO/SAE DIS 21434: Road vehicles — Cybersecurity engineering (under development)".

[41] D. Etherington, "Lyft, Aptiv and the National Federation of the Blind partner on self-driving for low-vision riders," Tech Crunch, 8 July 2019.

[42] Institute of Electrical and Electronics Engineers, "IEEE 2846 WG," [Online]. Available: https://sagroups.ieee.org/2846/. [Accessed 19 March 2020].

[43] MITRE, "Common vulnerabilities and exposures," [Online]. Available: https://cve.mitre.org/index.html. [Accessed 20 February 2020].

[44] Effective FMEAs, "FMEA glossary of terms," [Online]. Available: http://effectivefmeas.com/uploads/Glossary_of_FMEA_Terms.pdf. [Accessed 20 February 2020].

[45] S. Pilot, "What is a Fault Tree Analysis?," Quality Progress, vol. 35. no. 3, pp. 120, 2002.

[46] SAE International On-Road Automated Driving (ORAD) committee, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," Document J3016_201806. SAE International, 2018.

Bibliography

[47] N. Leveson and J. P. Thomas, STPA handbook, Cambridge, MA: MIT, 2018.

[48] Institute of Electrical and Electronics Engineers, "IEEE 2851 WG," [Online]. Available: https://sagroups.ieee.org/2851/. [Accessed 11 July 2020].

[49] Information Sharing and Analysis Centers, "Auto-ISAC," July 2016. [Online]. Available: https://www.automotiveisac.com/best-practices/. [Accessed 19 February 2020].

[50] A. Longthorne, R. Subramanian and C.-L. Chen, "An analysis of the significant decline in motor vehicle traffic crashes in 2008," Report DOT HS 811 346. National Highway Traffic Safety Administration, Washington, DC, 2010.

[51] The Data Safety Initiative Working Group, "Data safety guidance version 3.0," Report SCSC-127. Safety Critical Systems Club, 2018.

[52] Software Assurance Forum for Excellence in Code, "Fundamental practices for secure software development," SAFECode, 2018.

[53] International Electrotechnical Commission, "IEC 61508-1:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems," 2010.

[54] British Standards Institution, "PAS 1885:2018: The fundamental principles of automotive cyber security," BSI Standards Limited, 2018.

[55] SAE International, "SAE J3061 Cybersecurity guidebook for cyber-physical vehicle systems," Document J3061_201601. SAE International, 2016.

[56] International Telecommunication Union, "Systems characteristics and compatibility of automotive radars operating in the frequency band 77.5 78 GHz for sharing studies," International Telecommunication Union, Geneva, Switzerland, 2015.

[57] National Highway Traffic Safety Administration, "Traffic safety facts 2016," Report DOT HS 812 115. National Highway Traffic Safety Administration, Washington, DC, 2018.

[58] D. Dodson, M. Souppaya and K. Scarfone, "Mitigating the risk of software vulnerabilities by adopting a secure software development framework (SSDF)," National Institute of Standards Technology, 2019.

[59] W. Newhouse, S. Keith, B. Scribner and G. Witte, "SP 800-181: National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework," National Institute of Standards Technology, 2017.

[60] World Economic Forum; Deepen AI; McKinsey & Company, "Safety pool," [Online]. Available: https://www.safetypool.ai/. [Accessed 19 February 2020].

[61] Consumer Technology Association, "Public groups area," [Online]. Available: https://standards.cta.tech/apps/group_public/. [Accessed 19 February 2020].