AIMOTIVE™

aiDrive™ SAFETY REPORT

June 2020

Table of contents

Executive summary

Safety is the very core of automated driving technology. Every ADAS or automated driving solution deployed is created to avoid or mitigate accidents and save lives. To this end, safety engineering is a central element of everything we do. This document details the measures we take, from software design, development, testing and deployment to ensure the safety of everyone around us, and our team, when developing aiDrive, the company's modular and intelligent automated driving software stack.

Over the last few years vital work has been done in developing automotive standards to increase the safety of automated driving solutions. The traditional ISO 26262 standard has been augmented with SOTIF (ISO 21448) to address the novel challenges that have arisen during the deployment of ADAS and automation solutions. This document details how the considerations of these standards are vital to the safe operation of AImotive and how they are implemented from the earliest phases of development to deployment on public roads.

Using an example functionality the document details the considerations pertaining to sensor setups, software architecture, continuous integration – continuous deployment development and public road testing. Beyond adhering to the above-mentioned standards, AImotive has created unique, industry leading development pipeline that relies on aiSim™. Our in-house developed simulator has been purposely designed to support the validation and verification of automated driving systems.

The document also details the legal requirements of, and internal policies that define our approach to public road testing. The collection of both training and testing data is also examined in connection to these. Safety features already deployed in aiDrive, such as sensor diagnostics are also presented.

Finally, we have highlighted a series of issues that will define the ongoing advancement of safety-critical automated driving features: hardware platforms, sensor evaluation, OTA updates and cybersecurity. While these are aspects that AImotive takes into consideration every day, they are complex questions, the solutions to which will require global collaboration of industry stakeholders.

If you still want to learn more about our safety practices check out our blog, or contact us at info@aimotive.com.

1. Scope

AImotive delivers a modular product portfolio that enables affordable, level-agnostic automated driving and helps OEMs and automotive suppliers to engineer scalable automated driving solutions.

This document is part and includes the results of AImotive's safety activities, from analysis through development to verification and validation actions. It provides an overview of our safety approach to developing automated driving (AD) and the safety activities we perform at AImotive to ensure that our aiDrive™ AD software suite operates with the highest level of safety, while minimizing avoidable risks. With this safety report, we intend to share our path to safety with our partners and stakeholders to foster open communication, transparency, and common understanding.

2. Objective

AImotive provides an AI-powered ecosystem composed of the aiDrive™ and aiSim™ software suites and the aiWare™ neural network accelerator IP.

aiDrive™, our modular automated driving (AD) software empowers OEMs and Tier1 suppliers to build an automated driving strategy relying on the industry-leading evolution of AD features for the mass market, from assisted driving to autonomy.

While AImotive continuously tests its AD software on closed test tracks and public roads in various countries, AImotive does not aim to build an outright autonomous mobility service. Rather, we envision the gradual adaption of AD technology through iincremental ADAS and AD feature evolution (and ODD expansion) from series production passenger cars to utility vehicles.

At AImotive, we have always believed that safety is the most critical element of automated driving. We take every possible measure both to make the aiDrive™ suite as safe and reliable as possible, and to prepare our test vehicle fleet operations for the safest possible road testing.

This document largely relies and builds on the work we have done and delivered in collaboration with various automotive industry players since AImotive was formed in 2015. While the technologies and processes described in this document mainly demonstrate the current capabilities of our automated driving system, aiDrive™, forward-looking statements are also made at certain points of the report.

2.1 DOCUMENT OVERVIEW

THIS DOCUMENT WILL COVER THE FOLLOWING MAIN TOPICS.

We begin by describing the concept of an SAE L2+ automated driving system that enables highway driving, which will serve as our guideline throughout this report. The section will detail a selected sensor system, the best of our automated driving technologies as manifested in aiDrive™, and the expected functional behavior and operation domain of such a system.

We continue by detailing our approach to software development, that is, how and in what framework we develop and test aiDrive™; how we use our simulation ecosystem aiSim™ to improve the quality and safety of our AD software up to the point that it is worth hitting public roads for testing.

The following section will cover how we customize and operate our test vehicles for AD systems, with special emphasis on the participants and the strict process of road testing and subsequent evaluation. We also elaborate on the various safety features of aiDrive™, which guarantee that the product itself is immanently safe and reliable.

Additionally, we outline further safety specific activities that support overall development and testing processes. We also present the relevant safety standards and industry guidelines that are continuously considered in our product development.

Finally, we discuss the current challenges and perspectives of automated driving as seen by AImotive.

We welcome feedback and comments on this document
info@aimotive.com

3. System concept

In this section, we provide an overview of an example AD system that AImotive is developing, so that the subsequent discussions on approaches, processes, and measures can be better understood and put into context.

3.1 PURPOSE OF THE AUTOMATED DRIVING FUNCTION

As the aiDrive™ AD software suite is modular and scalable, various AD functions and solutions can be built using its components at different levels of automation for varied operational domains. They can range from specific ADAS functions (like lane keeping or adaptive cruise control) through low-speed autonomous valet parking to more complex driving tasks like highway driving.

In this report, we take one concurrent and substantial use case that heavily drives our SW development, to build the discussion and reasoning around it.

The purpose of the example AD function is to enable SAE L2+ hands-free in-lane driving between specific sections of given highways under well-defined operational conditions. If the boundary conditions are met (as detailed in Operational domain), the AD system – containing the AD application SW logic – can manage all dynamic driving tasks (steering, acceleration, deceleration, lane change, signaling intentions) under human supervision.

The AD system is expected to run on automotive embedded hardware platforms like the Nvidia Drive AGX.

3.2 SENSOR SYSTEM

aiDrive™ perceives the real 3D, 360-degree environment around the vehicle through a range of state-of-the-art, automotive-grade but affordable, mass-production sensors, which allow for safe automated driving.

3.2.1 SENSOR SYSTEM REQUIREMENTS

Our extensive studies and analyses in the field of sensor technologies have revealed numerous basic requirements towards a sensor system suitable for the highway AD system in question, namely:

- Line of sight: >150 m (to support a safe vehicle stopping distance)
- Rear-view: detection of traffic approaching from the rear > 90 m for safe lane change maneuvers

AImotive's technical implementation involves assigning as many diverse sensor types and sensor modalities as possible to the above requirements to maximize the safe and reliable operation of our AD software.

3.2.2 SENSOR SYSTEM DESIGN

AImotive test vehicles are equipped with a diverse, redundant, synchronized, and calibrated sensor set.

The different AD solutions and use cases that can be realized with aiDrive™ require different sensor setups; from the various possible implementations, the following concentrate on an optimal and affordable selection of sensors.

Different sensors provide different ranges of benefits and they can complement each other's weak points. The aiDrive™ sensor system for L2+ highway driving is designed with a primary emphasis on cameras, as visual perception conveys the most information about the traffic environment. However, cameras cannot provide direct measurement of distance and speed which can be supplied, for example, by radars. Therefore, for safety and redundancy reasons, and for wider operation domain coverage, our reference L2+ implementation also uses radars and LiDARs in a complementary fashion for robust sensor fusion.

When planning a new or improved ADAS or AD system, we collect requirements for perception and the supporting sensor system based on the general system concept, including the Operational Design Domain (ODD), the maximum limits of road geometry, worst case assumptions about the environment, or realistic capabilities of sensors and processing algorithms. Here we can rely on our extensive experience founded in our internal

R&D and customer projects, as well as on the relevant international standards (ISO, UN ECE, NCAP, and so on). For L2+ Highway Assist, we have analyzed, for example, ISO 22839 for emergency braking, ISO 15622 for ACC, or ISO 17387 for lane change decision aid system requirements.

Based on the collected requirements, we specify an optimal sensor system, and we analyze both the individual sensors, as well as the complete sensor setup, as detailed below.

The development teams involved in the ADAS or AD feature development examine various types and makes of sensors in parallel from various aspects like sensor manufacturer, technical capabilities, placement, orientation, field of view (FoV), and so on. Our sensor experts check the detection distances in all the specified environmental conditions to verify that the proposed sensor setup can fulfil the general line of sight requirements. They also study further technical characteristics of individual sensor, such as lens distortion, angular resolution, maximum frame rate, or sensor data quality. We also test the position, orientation, and field-of-view of each sensor by emulating the sensor on virtual vehicles in our simulation tool, aiSim™, to exclude uncovered areas or blind spots.

FIGURE 1.
Exported aiSim frame showing front cameras of different FoVs.
The example shows that with cameras of narrower FoV, lane markings and guardrails cannot be detected in the full width of the ramp.

Based on the collected requirements, a set of simulation scenarios are also selected on which the full, proposed sensor setup is tested in aiSim™ to verify how the original sensor setup would perform in certain edge cases.

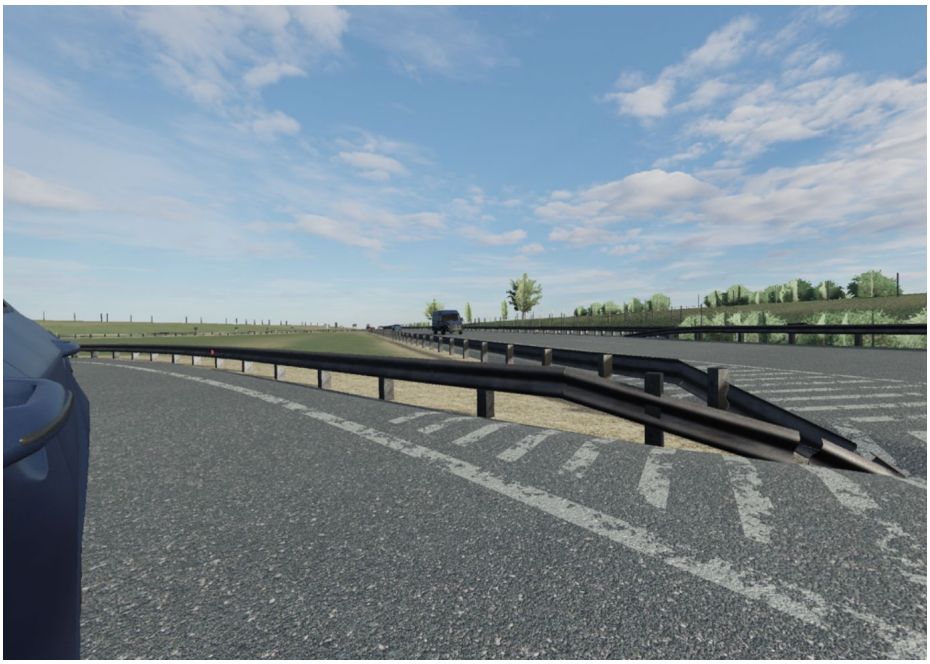


FIGURE 2.
An example scenario of merging onto a highway with a backward-looking side camera. Backward-looking wide-angle cameras allow detecting both the current merge lane and the surrounding lanes with vehicles traveling in them, which is vital in a highway merge scenario.

A sensor setup can be accepted only if they fulfill the individual sensor requirements, and the given edge scenarios can be solved safely by aiDriveTM in a consistent and confident way using the proposed sensors.

Based on such detailed analyses, AImotive test vehicle used for verifying L2+ highway functions are equipped with a set of eight cameras, partly inside the vehicle, partly mounted on the outside of the chassis. Radar and LiDAR devices are also mounted to the front and the rear of the chassis.

Apart from cameras, AImotive uses GPS and IMU sensors for enhancing localization during L2+ highway driving and relies on basic vehicle motion data (wheel speeds, steering wheel angle) received over the CAN bus of the vehicle.

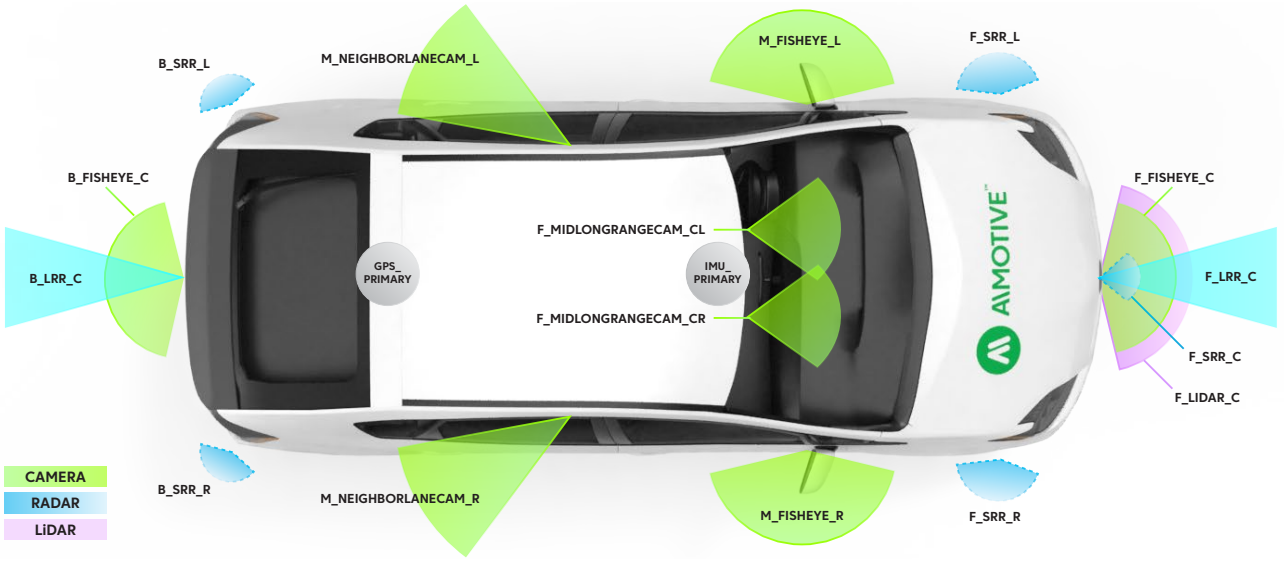


FIGURE 3. *Example test vehicle sensor setup for L2+ highway driving*

More specifically, the following types of sensors are included:

- Front: Cameras with medium field of view (FoV) in a stereo setup and a wide FoV (fisheye) camera
  AImotive prefers using a forward-facing stereo camera pair as one supports diverse and robust perception techniques:
  - *Stereo depth map for vision-based distance estimation*
  - *Generic obstacle detection based on stereo depth map*
  - *3D lane detection for enhanced modeling of the road surface and structure*
- Side: a pair of fisheye and narrow neighbor-lane cameras
- Back: fisheye camera
- Front and rear long-range radars
- Short-range corner radars
- Front LiDAR (optional)
  LiDARs, together with HD maps, can offer a parallel perception stack to extend the capabilities and provide the redundancy required when moving to SAE Level 3.
- Access to wheel speed and steering wheel angle information over CAN
- IMU information
- Global position information from GPS

aiDrive™'s sensor management component reads and synchronizes input from this multitude of live sensors, as temporal synchrony of sensors and proper timestamping of data acquired are crucial for safe automated driving. This component also monitors and diagnoses their operation, as detailed in Sensor diagnostics.

Apart from live sensors, we use SD maps enhanced with in-house annotation layers (containing lanes and road edges, and traffic signs and traffic lights) as offline sources of information for smooth navigation.

3.3 AIDRIVE™ SW ARCHITECTURE FOR SAFETY

From a functional perspective, AImotive's aiDrive™ software suite can be divided into five main building blocks – engines –, each responsible for a specific key component of self-driving technology. These components reflect a natural flow of processing, understanding, and reacting to the environment. AImotive carries out active research and development in the fields of technologies related to these components.

Each engine is divided into modules responsible for select processes. Certain modules rely on AI for improved perception and decision-making performance, while others utilize formal algorithms throughout the system to ensure safety.

- **Perception Engine,** *responsible for handling sensor data, detecting and classifying objects, and interpreting the environment*
  In the heart of the aiDrive™ Perception Engine, we use various AI-based detectors in parallel (2D bounding boxing, semantic segmentation, 2D and 3D lane detectors, stereo depth estimator). AI-based detectors process the input from either the same or different cameras, to meet the strict redundancy requirements of reliable camera-based perception. The Perception Engine also manages processing radar and LiDAR sensor data.

- **Location Engine,** *responsible for providing precise vehicle location, orientation, velocity, and acceleration (so-called ego-motion) information of the ego-vehicle at every moment*
  Ego-motion is a crucial input for various AD features like precise object tracking, motion planning, reliable vehicle control, as well as yaw and pitch correction for the moving vehicle chassis, or on-the-fly sensor calibration.
  AImotive utilizes both vehicle dynamics-based odometry (using GPS, IMU, wheel speed and wheel angle data of standard sensors available on the market), as well as visual odometry algorithms for its ego-motion implementation.

- **Fusion Engine,** *responsible for fusing the individual static and dynamic detections into a complete model space*
  The Fusion Engine has a hierarchical architecture. A range of abstraction functions create a 3D model of the road surface, the detected lanes, and the drivable area within. Extended Sensors produce parallel sensor-level abstractions (defining low-level object tracks). Model Space Fusion implements a multi-layer, sensor-agnostic fusion of all information provided by the preceding layers to create an accurate and complete 360° model of the static and dynamic environment around the vehicle.

- **Motion Engine,** *responsible for deciding the right behavior and trajectory for the vehicle*
  Taking into account planned route information and predicted object movements, it decides the behavior and the driving trajectory for the vehicle to follow, while considering traffic rules and culture, as well as situation-specific operation modes.

- **Control Engine,** *responsible for operating the vehicle through low-level actuator commands*
  The Control Engine calculates the longitudinal and lateral control actions required to drive the vehicle along the planned trajectory, then transforms them into proper actuator commands and transmits them towards the vehicle's control interfaces.
  In AImotive's reference implementation, a separate DBW Unit provides the actual physical interface between the vehicle and the aiDrive™ compute platform.

The following figure illustrates these engines and their main sub-components.

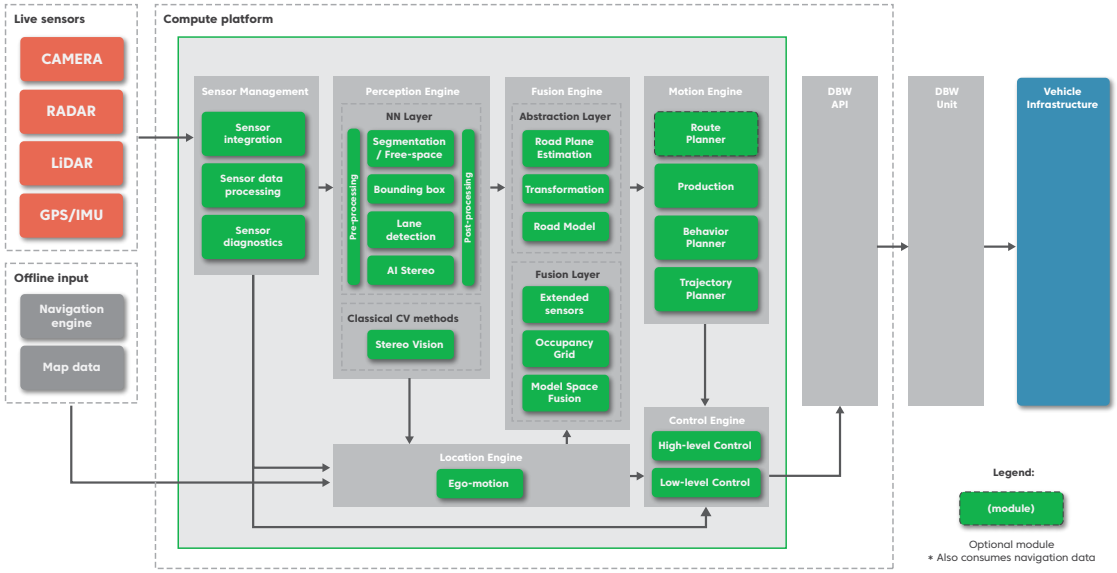


FIGURE 4. *A high-level overview of aiDrive™ building blocks*

aiDrive™ has a proprietary execution framework for the SW modules that – relying on a single application configuration – handles strict and hierarchical scheduling of module executions and reports any violations.

3.4 MODELING FUNCTIONAL BEHAVIOR

We can summarize the expected functional behavior of an L2+ highway AD function along the following lines:

- Full-range adaptive cruise control (ACC) and lane keeping function (LKF), including traffic jam assistance (TJA), in the range of 0 to 130 km/h
- Autonomous (unsupervised) lane change, including highway merge and exit maneuvers
- Automatic route planning and speed limit obedience
- Collision avoidance and emergency braking for both classifiable and unclassifiable obstacles, including stationary objects

- Obeying applicable traffic rules (speed limit, lane delimiters, keeping to the right)
- Detection of system degradation including sensor deterioration or misalignment, to allow smooth control handover to the driver if needed, or to reach a well-defined safe state when automated driving is no longer possible and there is no handover

We consider a number of factors when defining the expected functional behavior model of the vehicle equipped with the selected AD function. These aspects are – but not limited to – the operational domain, traffic rules, safety, and user experience considerations. For these subjective rules, we apply a machine-interpretable, formal definition of the expected behavior to be able to model traffic situations in our simulation environment and to reduce the uncertainty of their interpretation.

FIGURE 5. *Example scenario of an exit lane occupied by traffic jam.*

Based on these aspects, we have created and maintain an exhaustive set of traffic scenarios, pre-defined traffic situations that describe the functional behavior of the ego-vehicle and that of other traffic participants, with designated pass criteria. These cover the complete expected function range of the AD system (including, for example, ACC, LKF, lane change, highway exit and merge, traffic jam assist) modeled both in various real-world and generic simulated locations.

Scenarios are defined based on functional safety requirements, on real-world situations that AImotive's fleet of test vehicles encounter, or that are deduced from the EURO NCAP test protocols and NHTSA road accident databases.

These unique traffic scenario descriptions are then used for AD function verification and validation in our simulation environment, aiSim™, permutated with road types, speed range, and environmental conditions, resulting in thousands of possible, distinct test cases.

3 Test Steps

	Critical	Action	Expected result
#1	-	Switch ON aiDrive system.	aiDrive system is running.
#2	-	Vehicle_02 passenger car is ahead of Ego vehicle. Vehicle_04 minivan and Vehicle_01 pickup are in the adjacent lane in the right. Vehicle_03 passenger car is on the exit lane; v_rel = 0 km/h	Ego remains between lane lines, unless lane change intended. *Lane keep* Ego maintains target speed when on unblocked path. *Speed change*
#3	-	Vehicle_02 execute lane changing maneuver to the right AND vehicle_04 execute lane changing maneuver to the left simultaneously.	aiDrive recognize vehicle_02 and vehicle_04 vehicles' intention. Ego vehicle maintains safe distance from vehicle_04. Ego maintains safe following distance to other vehicles. *Safety gap* Ego does not collide with vehicles or objects. *Collision* Ego reaches target destination of scenario. *Travel distance*

FIGURE 6. *Example definition of actions and results of a scenario*

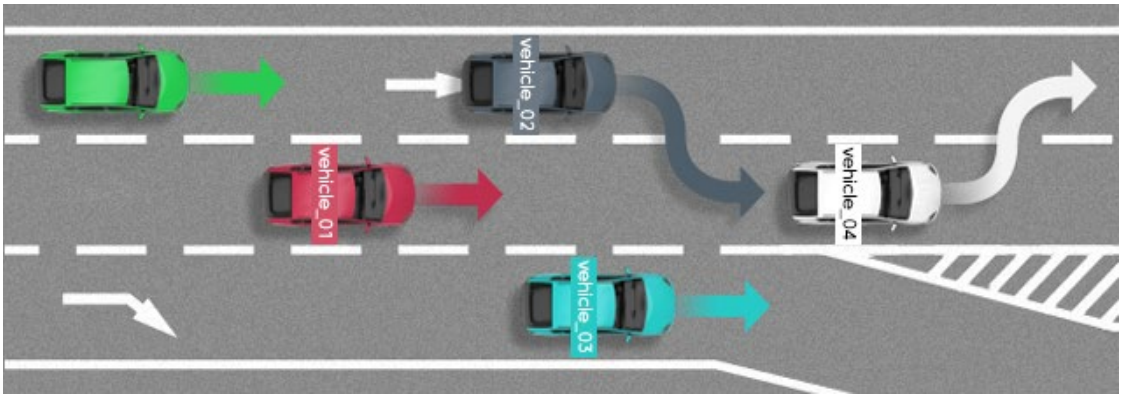


FIGURE 7. *An example scenario of congested highway traffic*

Regarding the used AD system elements, we create comprehensive requirement specifications with the same rigor and detail. For AI-based perception functions, we also specify the requirements for the training data set precisely, considering the aspects of the use-cases, the possible objects of the operation domain, and the precision requirements of the annotation.

3.5 OPERATIONAL DOMAIN

The Operational Design Domain (ODD) describes the specific conditions in which the AD system is expected to operate, with regard to, for example, environmental conditions, road

or traffic conditions, geographical area, time of day, and so on. ODDs also help to define specific scenarios for verification both in simulation and on physical roads.

The considered AD function aims at providing in-lane driving actions in a typical, pre-determined, geofenced highway environment.

Compared to other AD vendors, there is no need for pre-mapping the selected geographical area; commercial maps are suitable.

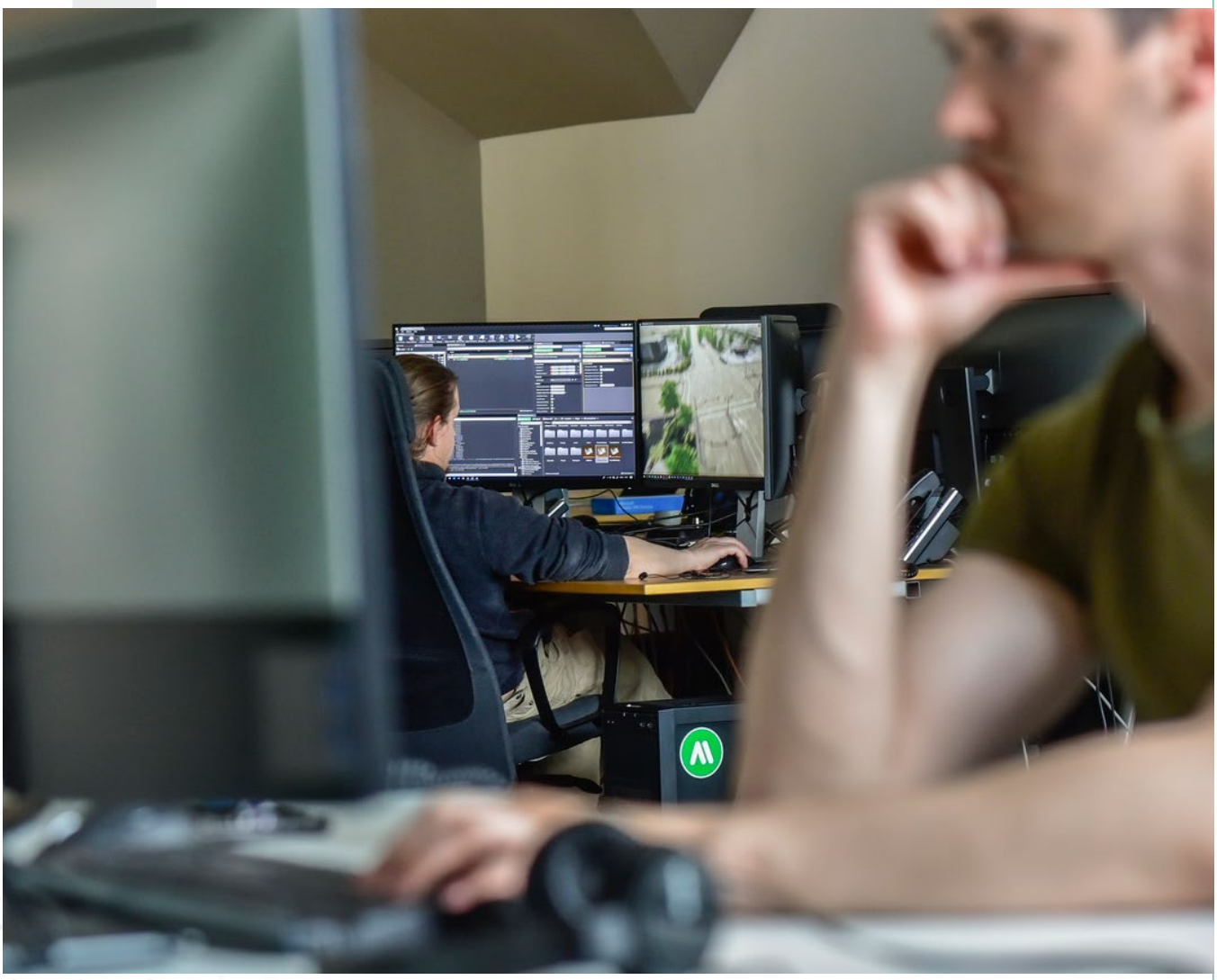
The ODD for the AD function in focus can be broken down into the following inherent practical conditions:

- Applicable to public highway roads with at least 2 lanes in the same direction and proper, visible lane markings throughout the route
  Road definitions are based on the applicable road standards for the supported regions, as well as field analyses and experience (recordings, measurements, and annotations) at testing locations in the USA, France, and Japan.
- Lanes for oncoming traffic delimited by barriers
- Normal weather conditions: including clear or cloudy sky, light snow, light rain, light fog
- Driver supervision on activation
  The driver enables the function when the car is already traveling on the highway, and there is no imminent dangerous traffic situation surrounding the car.
- Adjacent vehicles traveling in the same major direction as the ego vehicle (vehicles coming from the opposite direction are filtered out)
- Minimal object classes to detect: passenger vehicle, truck, motorcycle

FIGURE 8.
Currently, it is the responsibility of the Safety Driver and the operator to ensure that these conditions are met continuously during road testing. If any of them deteriorates, they deactivate the AD function.

4. Approach to software development

At AImotive, we foster a safe and sustainable software development culture, which approach entails numerous aspects, from the rigorous selection of our colleagues through various elements of the SW development environment to diverse verification and validation processes.



Our approach follows general, established automotive guidelines; we pursue extensive compliance with the Automotive SPICE Process Reference Model or with the applicable parts of automotive safety standard ISO26262:2018 Road vehicles — Functional safety. We apply strict risk mitigation strategies at every stage of development.

The following sections detail how we address these complex challenges in software development.

4.1 SW DEVELOPER RECRUITING

At AImotive, we build on people who create value and unleash their potential. Our strict SW developer recruiting process contributes to building a team with high level technical expertise and safety awareness.

We use rigorous interview techniques for all applicants, ensuring top-notch knowledge of the required programming language and implementation techniques.

We also put a large emphasis on retaining employees to ensure their experience with the AD system is maximally utilized and can be transferred to new members of the teams.

4.2 SW DEVELOPMENT FRAMEWORK

At AImotive, we employ a complex framework for SW development and testing activities, so that deficiencies or wrong design decisions are discovered as early in the development process as possible.

This framework is composed of the following main elements:

- **C++** programming language for scalability, portability, and performance, optimal for resource-intensive applications such as AD systems.
  The chosen implementation for the aiDrive™ function is developed in C++.
- Coding style: A derivative of Chromium C++ coding style and enforced using Clang-format
  For automotive compliance, we also follow a stricter protocol: we use a subset of **AUTOSAR C++14** guidelines.
- Source code management in **Git**
  The source code of the developed aiDrive™ software suite is stored in Git repositories, together with supporting information (build configuration, embedded documentation, data files). Git allows fast and distributed source code management, resulting in a more error-resistant system with a small overall footprint.
  Git ensures that branching and merging facilities are available for all repositories.
- Code review in **Gerrit**
  The implementation deemed complete by the developer is submitted to the Gerrit code review system. In the code review system, the implementation is reviewed by peers during the code review process, which also includes reviewing the SW design. The initial implementation can thus be updated and resubmitted potentially several times based on review findings. The person who accepts the code change must check consistency with the task description and the code review checklist.
- **Jenkins** build automation system for Continuous Integration (CI)
  Jenkins is also closely integrated with Gerrit, allowing automatic feedback and control mechanisms about the code quality of a given change based on build results. These mechanisms ensure that the proposed source code change successfully compiles and links on all target platforms (e.g., Windows, Linux, or Nvidia Drive PX/AGX), or the code change does not impair automated simulation tests.

- **Black Duck** open source audit to monitor legal and license aspects
- Static code analysis with **Helix QAC** system, running overnight on the aiDrive™ codebase checking compliance with the selected subset of AUTOSAR C++14 guidelines
- Dynamic code analysis: Low-level code execution analysis with tools like **Valgrind** and **Address Sanitizer** to detect memory management and threading bugs, as well as **CUDA-MEMCHECK** for GPU code analysis
  The CI pipeline also runs regular, higher-level dynamic code testing on all units in aiDrive™, compliant to ISO 26262 recommendations. For details, see General safety approach and activities.
- Requirements and specifications management in the **codeBeamer** ALM platform, qualified to support development in accordance with the requirements of ISO26262 (up to ASIL D)
- Unit tests and integration tests managed in **Google Test** and **Cantata**
- Documentation inside the code in the format of Doxygen-compatible comments and informative naming conventions
  The purpose and operation of classes and functions, parameters, non-trivial design and implementation aspects are to be documented in the code as inline comments.

Developers have access to the same hardware-software execution environment that is used in the test vehicles, so that they can perform initial testing on their developer workstation with results relevant and comparable to what actual vehicle tests could produce.

4.3 SW DEVELOPMENT PIPELINE

Software development and validation at AImotive are carried out according to agile principles. In its core lies an iterative, test-driven development pipeline relying on large-scale simulation and real-world testing.

At AImotive, we have a deep understanding of how simulation for automated driving works as we have achieved a unique combination of developing software for automated driving (aiDrive™) and a purpose-built, automotive simulation ecosystem (aiSim™).

Our long history of developing these two products in close cooperation has confirmed our stance that simulation offers huge advantages over real-world testing with regard to efficiency, repeatability, scalability, or the ability to test corner cases.

The diagram below provides a model of the system as a controlled process, with interfaces and feedback loops. While supporting agile operation, the below development pipeline also maps to the elements of the V-cycle, so that we can apply the requirements of ISO26262 to safety-relevant components.

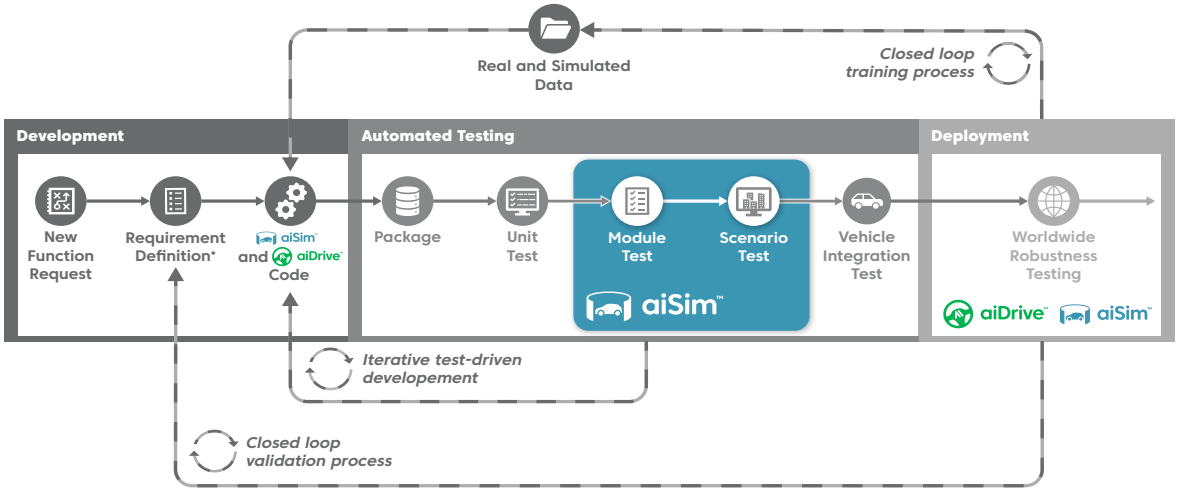


FIGURE 9. *Software development pipeline*

The pipeline guarantees that each participant of the SW development and testing processes – from the SW developer to the safety driver – contributes to the overall safety of the AD system, keeping all safety implications of engineering decisions under strict supervision.

The pipeline heavily relies on AImotive's proprietary simulation application, aiSim™, and the supporting ecosystem, involving mass-scale simulation testing and a series of feedback loops and checkpoints. In essence, aiSim™ acts as a safety barrier by allowing only mature SW builds onto public roads. New functions are tested on thousands of proprietary and standard (for example, Euro NCAP) scenarios in modeled real-world locations before road tests.

Simulation testing enables on-the-spot evaluation of the end-to-end AD SW stack, to validate perception, fusion, planning, and decision-making algorithms governing virtual vehicle behavior in distinct simulated traffic scenarios, with automatic behavioral evaluation criteria like safety distance, lane keeping, speed of reaction to events, and so on.

THE PROCESS INVOLVES THE FOLLOWING MAIN STEPS:

1. New feature or function requests (coming either from Partners or from internal stakeholders) are analyzed to define the feasible operation domains and the related use cases for the given function.

2. Based on the operation domain and use case definitions, functional, performance, and safety requirements are formulated to cover all possible aspects and to meet all relevant standards and common-case scenarios.

3. Requirements can evoke the following development activities:
   - *aiDrive™ algorithm development*
   - *New scenario definitions (to be fed into aiSim™ for simulator testing)*
   - *aiSim™ and related toolchain development*
   - *Real-world and augmented training data preparation and collection*

4. Based on the requirement set and algorithm design, a complete test suite is defined (consisting of a range of scenarios).

5. The new aiDrive™ algorithms undergo a strict code review process (managed in the Gerrit code review framework).

6. If the new algorithms pass the code review, they are merged into the protected feature SW branch, and a new SW package is generated.

7. The aiDrive™ SW package is verified through the following, subsequent phases:

    7.1 Unit Test, testing a confined part of an algorithm
    7.2 Module Test, testing high-level blocks (engines) of aiDrive™ separately in aiSim™, like perception, fusion, decision making, or control
    7.3 Scenario Test, testing the full aiDrive™ SW stack in simulated scenarios
    7.4 Vehicle Integration Test, testing the SW package in test vehicles either on closed test tracks (when required) or on public roads once aiSim™ testing phases have deemed the SW mature enough

    Vehicle Integration Tests always require a safety driver and an operator on board. The results of the given test phases are analyzed for possible faults or regressions and are fed back to SW development for possible SW corrections or modifications.

8. Once the SW package shows sufficient maturity and passes Vehicle Integration Test, the SW branch is merged to the Master branch then a Release Package is created.

9. The Release Package undergoes heavy robustness testing, including the following activities:
    - Public road vehicle tests in headquarter and satellite offices (for example, in the USA) Recordings from public road robustness tests also serve as a basis for new, annotated training data for aiDrive™ NN algorithms.
    - Large-scale simulator testing (against thousands of scenarios on a weekly basis Robustness tests also serve as a means of validation for the original assumptions laid in the requirements or can reveal corner cases not covered in the original requirement set.

This robust approach is backed with a complex and scalable, simulation-based ecosystem, described in detail in the following sections.

4.3.1 PRINCIPLES OF CONTINUOUS INTEGRATION AND TESTING

As illustrated by the above, AImotive applies rigorous, multi-step testing processes for its AD software to provide evidence that the developed SW complies with the initial functional safety requirements.

Our Continuous Integration methodology is defined by traditional functional safety engineering and accelerated by our aiSim™ framework, according to the following aspects:

- Compile on multiple platforms and compilers
- Apply maximum warning level, handling warnings as errors

- Run regression sets regularly (containing a comprehensive set of traffic scenarios)
- Define traffic scenarios in a formal, machine-interpretable way
- Analyze real-world examples (accident statistics, test drive experience) as the base of possible traffic scenarios
- Apply strict success criteria for simulated scenarios, with warnings and safety gaps
- Validate AI continuously through NN benchmarking and confidence reporting and calibration

4.3.2 SIMULATION TESTING ECOSYSTEM

In the heart of our testing activities lies our simulation testing backend, an AImotive-proprietary system that allows for the creation of custom test sets (suites) from pre-defined traffic scenarios, and running these in the aiSim™ simulator with aiDrive™ automated vehicle SW.

The following figure illustrates the basic components of the system:

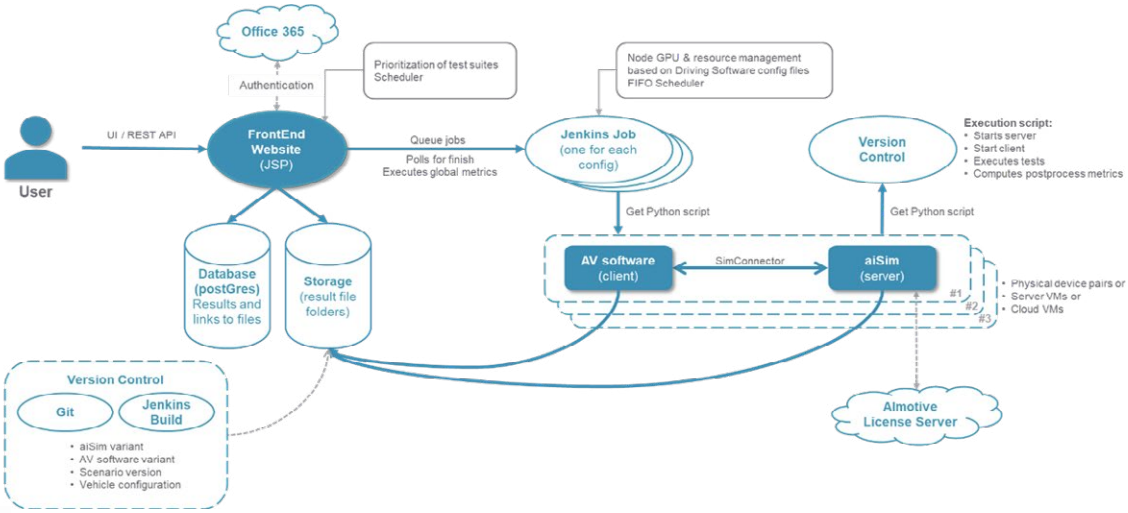


FIGURE 10. *The components of the simulation testing backend*

The heart of the system is a dedicated Jenkins server, with a related front-end website, complemented with a database of test scenarios (test sets) and their various manifestations, test cases (defined by different condition variables). Individual test scenario definition JSON files are stored in Git, in a scenario repository.

The front-end web site enables the creation and execution of test suites, either automatically (e.g., when developers commit a code change) or on demand.

When launching a test suite, the website passes the test suites to the Jenkins server (with aiDrive™ and aiSim™ hosted on a separate machine). Through these automated processes, thousands of scenarios can be run within an hour.

The results are stored on a dedicated server share and can be viewed by developers on the front-end website. They include not only the results of all scenario runs but any information vital for the benchmarking of the AD system, including sensor inputs, software states, actuator commands, and so on.

This cloud-based database is accessible to our development teams and partners. Beyond visualizing important statistics such as pass rates, various filters help engineers sift through the data to get meaningful insight into the causes of failed scenarios.

4.3.3 CERTIFIED TOOL FOR AUTOMOTIVE DEVELOPMENT

For automotive SW development, the ISO 26262 standard strongly recommends product safety qualification for the tools and applications that are used in the development process.

The objective of ISO 26262 tool qualification is to ensure that software tools are suitable for use in developing safety-related items, such as, driver assistance or automated driving software.

AImotive is strongly committed to these guidelines, and has pursued a Trusted Tool certification for aiSim™ (of Tool Confidence Level 3). This means that aiSim™ can reliably be used as a development tool for safety-directed systems, such as automated driving software. This provides evidence that aiSim™ can be part of an AD SW verification pipeline up to ASIL D development.

4.3.4 SCENARIOS AND SIMULATION TEST SUITES

Scenario testing is one of the most vital elements of simulation. The internal front-end website allows developers to define complex test suites based on a wide range of scenario definitions for various purposes, e.g., to test the operation of a new SW algorithm or function, or for general regression tests.

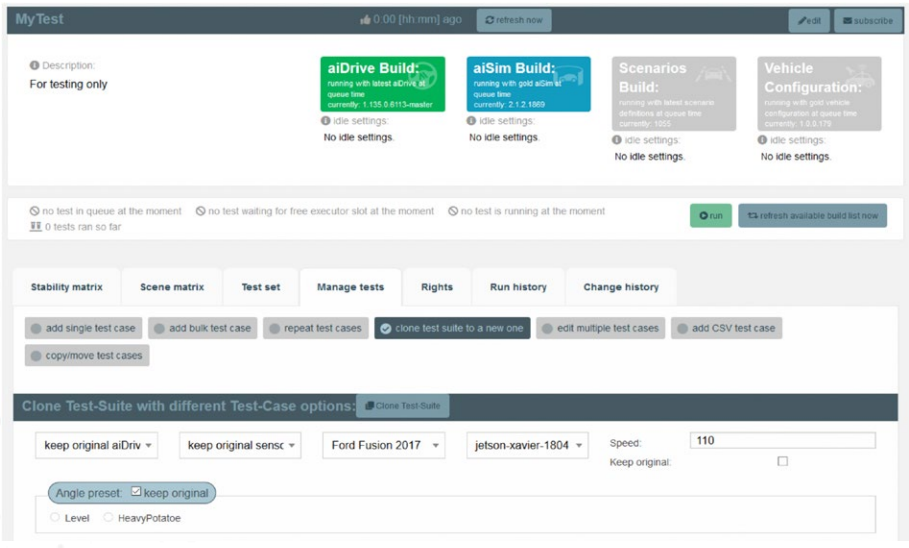


FIGURE 11. *Excerpt from a test suite definition page*

We apply a flexible scenario definition format that supports defining certain parameters or parameter ranges only when compiling a specific test suite. This allows for more flexible and varied test suites with fewer base situations resulting in more runtime alterations.

This adjustable scenario framework also helps fulfill the complex scenario definition criteria of EURO NCAP compatible testing. Currently, we cover over 90% of EURO NCAP ACC and LKA testing protocols in our simulation testing.

We define the automatic evaluation criteria of expected results for the following behavioral aspects, for example:

- Lane keep (distance from lane separators)
- Safety gap to the vehicle ahead
- Speed change
- Collision
- Overtake
- Acceleration or jerk
- Oscillation
- Uninterrupted travel distance in AD mode

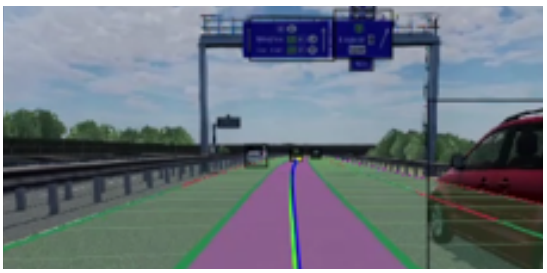


FIG. 12. *aiDrive driving on a simulated highway*

Our carefully engineered scenario set and strict evaluation criteria also ensure that our AD software is constantly tested on interesting, risky, or even dangerous situations. Many of these are difficult or impossible to properly test in the real world, either because they are too dangerous, or because of extremely limited repeatability.

4.3.5 GRANULAR APPROACH TO MODULE TESTING THROUGH AISIM™

Beyond a vast library of scenarios and a wide range of test possibilities, more can still be done to extract the full potential of simulation testing. Running the full self-driving stack in the simulator provides the most important feedback; however, the root of a problem is not always apparent.

This is where module testing comes in. Modules are smaller sections of the SW stack responsible for well-defined tasks. In aiSim™, any of these modules can be replaced with ground truth data (GT) provided by the simulator, recorded sensor data from field tests (so-called readback tests), or the real output of a preceding SW module, as shown in the figure below.

If all but one module is replaced, the performance of the single running module can be checked automatically against a reference output, and logging or visualization can provide insight into the operation of the module.

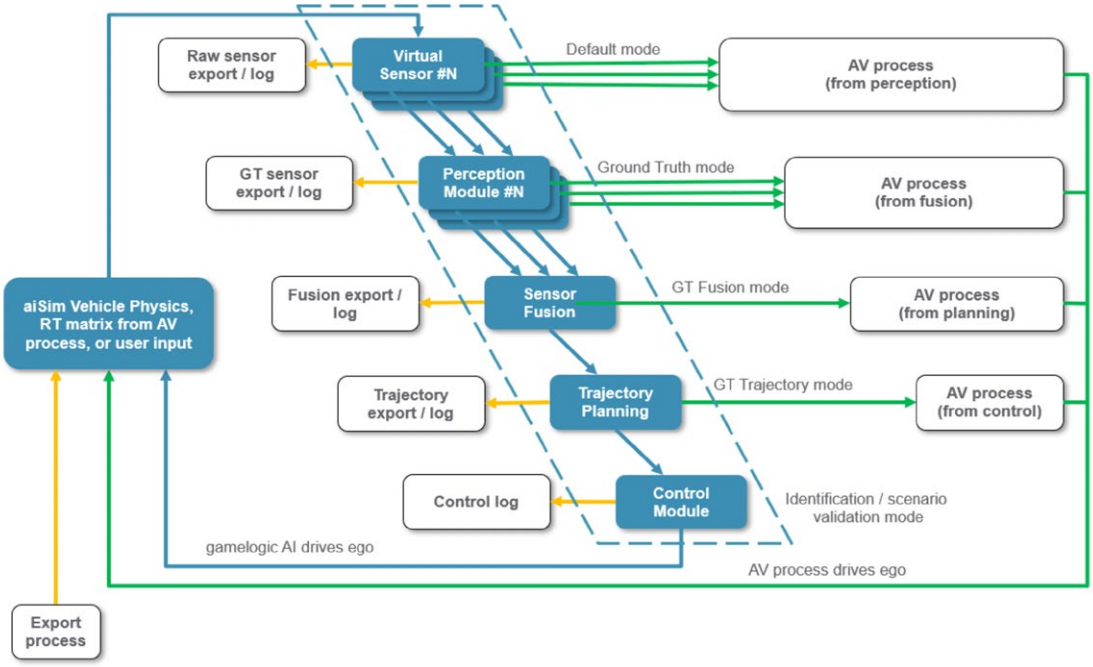


FIGURE 13. *Module testing modes in aiSim™*

This setup allows for testing a module both independently from the effects of preceding modules, as well as including effects such as simulated sensor noise, fault injection, stress testing, or ODD coverage. This flexible testing environment supports the early assessment of the module's performance and discovery of SW module malfunctions or deteriorations from the expected behavior.

4.3.6 NN BENCHMARK

aiDrive™ uses AI-based deep learning (DL) methods – neural networks (NNs) – for computer vision (CV) in the aiDrive™ Perception Engine. In recent years, neural networks have been proven to be far superior to traditional, hand-crafted CV methods in terms of detection accuracy, reliability, and scalability.

AImotive is continuously evaluating the detection quality of its NNs used in aiDrive™ according to a standardized benchmarking process, whereas both the datasets used for testing and the team responsible for benchmarking are strictly separated from the data and teams responsible for NN development and training. The requirements for the training and verification data sets are specified precisely, considering the aspects of the use-cases, the possible objects of the operation domain, and the precision requirements of the annotation.

The following main performance measures are applied:

- Semantic segmentation: Mean intersection over union (IoU) for the different object classes over classified pixels

- Depth: Relative error with 80% and 90% confidence intervals
- Object detection: Area under precision-recall curves (AuC)
- Lane detection: Precision-recall curves for clustered lane marking polylines

FIGURE 14. *Segmentation ground truth (left) and detection data (right) in parallel*

4.4 ROADWORTHINESS

The final checkpoint for a new SW feature before it is allowed to be tested in live automated driving is a well-defined regression test in simulation, as part of the overall Scenario Test phase. The regression test set contains a wide range of test cases for stable AD SW features.

The regression tests include, for example, the following types of test cases:

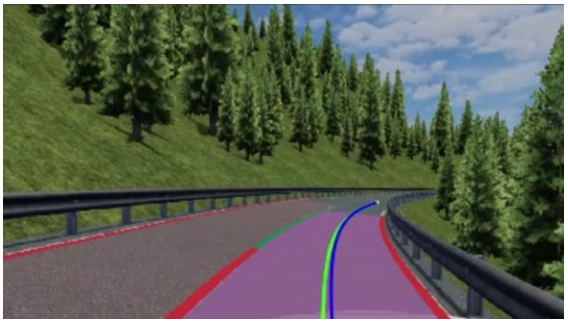


FIGURE 15. *aiDrive running on a simulated curved track*

- Performance testing in extreme artificial scenes like steep curves or highly banked road sections for verifying lateral control
- EURO NCAP brake tests for static or dynamic objects for verifying longitudinal control
- Free-ride with random traffic situations on simulated US and Hungarian highway tracks to verify the overall behavior of the complete AD SW

Test results are evaluated according to the following criteria:

- There are no errors in the test runs (no scheduling errors or errors due to scarce computing resources).
- There are no safety-critical failures that would need attention, e.g., collision or unintended lane departure.
- There are no failed test cases (scenarios); that is, pass criteria not fulfilled.

Once a software feature branch has satisfied these criteria in regression testing, a public road test can be scheduled.

When starting an AD session in a test vehicle, we also use an elaborate, rigorous checklist for evaluating the overall conditions of the AD system and the SW application.

4.5 EDUCATION FOR SAFETY AWARENESS

4.5.1 INTERNAL

At AImotive, we are committed to continuous enhancing of the competencies of our development staff, also including safety awareness. We believe that beyond educating our staff in safety-relevant fields and aspects, our choice to employ the most skilled and devoted engineers in various professional fields also contributes to the overall safety and reliability of AD system that we develop.

Our training framework consists of the following elements:

- Internal training programs in general SW development areas
- Regular safety training to ensure employees are aware of the safety-relevant aspects of the everyday work
- Monthly R&D seminars to showcase the latest cutting-edge research and development results
- AImotive Academy: Selected extensive training programs in fields like AI or GPU programming

4.5.2 PUBLIC

In parallel with our internal research and development activities, we are immersed in a number of joint studies and analyses with our Clients and Business Partners to reveal the safety aspects of AD technologies.

As we are continuously learning and revealing new facets of the complex field of automated driving, we also feel responsible and obliged to educate the broader public on the advancement of AD technologies, their possibilities, related considerations, and limitations, especially with regard to safety. For these purposes, we maintain the **AImotive Blog** and a **Medium channel** where we regularly publish articles by our distinguished experts.

These efforts come to light, for example, as **insight** into our testing approach, or in a recent Medium **article** that elaborates the possibilities and limitations of using AI and simulation in automated driving systems.

5. Test vehicle fleet and operations

aiDrive™ is continuously tested on AImotive's fleet of test vehicles. The company holds testing licenses in various countries and locations, including Hungary and the states of California and Nevada in the USA.

aiDrive™'s autonomous valet parking solution has been showcased in Hungary, the US, and Japan, while our solutions have also proven themselves on closed courses in Asia. Limited tests of solutions for select urban driving features began around Budapest in 2019.

We have dedicated engineering groups, with the following responsibilities related to our fleet,

- Vehicle Integration: Customizing production vehicles for our testing purposes, equipping them with the necessary sensors and compute platforms
- Embedded Systems: Producing embedded Drive-By-Wire (DBW) HW module and SW layers so that AD SW can control test vehicles in a safe and monitored way
- Safety Drivers: Skilled and qualified professional drivers

5.1 TEST DRIVERS AND OPERATORS

Test vehicles are always operated by two people:

- **The Safety Driver** is responsible for executing the dynamic driving task (DDT) while operating the vehicle manually, and for supervising vehicle behavior while it is in autonomous mode.
  They are trained, professional drivers capable of taking over vehicle control in critical situations, that is, when the AD SW fails to issue proper actuation requests towards the vehicle infrastructure.
  They are also responsible for giving the final vote over merging feature SW branches to the Master branch, as they are the most authentic source of information about the reliability of a given SW package.
  All AImotive safety drivers are experienced, automotive test engineers.
- **The Operator** manages and supervises the vehicle compute platform and the aiDrive™ AD SW running on it (through a dedicated debug view showing live streams of data about the main components of the system).
  Peripheries (keyboard) can be directly connected to the compute platform, or the operator can use a separate workstation (notebook) to connect to the vehicle computer.
  Operators also manage the recording, labeling notable events during the AD driving session for later analysis. They can also warn the Safety Driver of critical SW status or behavior, which should invoke a driver override on one of the applicable vehicle control interfaces (VCI), e.g., a steering movement or pressing the brake or accelerator pedal.
  Developers also have the possibility to join the test drives as spectators if necessary, for example, to check the operation of their SW features under real-life circumstances.

Safety Drivers go through a rigorous training program in their first weeks at AImotive. They have to participate in and successfully pass defensive and technical driver training in order to operate AImotive test vehicles in autonomous mode:

- **Defensive training:** Can be held either internally, and/or external automotive training can be accepted (for example, BMW B1, B2, C1, Daimler, Nordschleife training, etc.). The defensive training focuses on driving skills and reflexes: low speed, high-speed maneuvers, and vehicle handling on the limit. After the training, an “Evaluation sheet” is filled in that contains a driving skill profile for each safety driver.
  Additionally, in Hungary, an official exam is compulsory for drivers conducting public road testing, a generic Driving Aptitude Test held by the Hungarian National Transport Authority; the same as for ambulance drivers. This exam focuses on the reaction time, monotony tolerance, and the decision-making abilities of drivers. After successful completion of this exam, the name of the participating safety driver is reported to the Hungarian Government by AImotive.
- **Technical training:** The in-house technical training focuses on the safe operation of AImotive test vehicles during AV software testing, covering the safety concept and safety features of AImotive self-driving cars like diagnostic features, disengagement (driver override) possibilities, DBW limitations, and error handling.

- **Refreshment sessions:** AImotive holds 1-day driver skill refreshment sessions for its safety drivers every 6-8 weeks on closed test tracks, with set exercises and final evaluations.

5.2 TEST VEHICLE MODIFICATION

The Vehicle Integration group is responsible for modifying and customizing the test vehicles for AImotive's AD SW testing purposes, equipping them with the necessary compute platform, sensors, actuators, connections (cables, switches, and so on).

They also test the successful integration of the system with:

- Dedicated tools for the different subsystems (for example, sensor calibration)
- Executing aiDrive™ on the whole integrated system in shadow mode (without actuation)

5.2.1 SENSOR SETUP AND CALIBRATION

AImotive selects sensor suppliers based on rigorous criteria for harsh automotive use cases and ODDs, defined by our experts in the Sensors group.

For automated driving, sensors have to be accurately calibrated to the vehicle's coordinate system. AImotive utilizes a proprietary framework and algorithms for performing intrinsic and extrinsic camera and other sensor calibration.

However, during vehicle operation, previously performed offline calibration may deteriorate slightly due to vibration and other external effects. For the stable operation of the sensor perception systems, we also use on-the-fly techniques to compensate for these effects or at least detect and report an excessive misalignment which cannot be further tolerated.

5.2.2 COMPUTE PLATFORM AND ADDITIONAL ELEMENTS

AImotive uses cutting-edge compute platforms that provide the maximum computational performance power with efficiency.

For research and development purposes, we use custom-built computers, optimized for demanding in-vehicle usage (e.g., with special housing, power supply, and cooling) and equipped with a range of top Nvidia GPUs (GTX 1080/RTX 2080).

Also, we are continuously testing the performance of aiDrive™ on the latest commercially available automotive-grade platforms such as the Nvidia Drive PX or Drive AGX. Additionally, we are eagerly exploring new possibilities for development on production-purpose, automotive-grade HW platforms with our partners like Renesas.

We are also actively experimenting with ways to integrate our neural network accelerator HW IP, aiWare™, into a possible SoCs and to run aiDrive™ on them.

We rely on special, in-house developed HW elements for triggering and synchronizing the full sensors set.

5.2.3 VEHICLE CONTROL

The AD system has two main components from a vehicle control perspective:

- AD software – aiDrive™ – running on the vehicle compute platform, which provides actuation request towards vehicle control interfaces (VCIs)
- Embedded Drive-By-Wire hardware and firmware element acting as a control gateway and safety barrier towards the vehicle infrastructure

aiDrive™ requires access to and actuation on the following main vehicle control interfaces:

- Lateral control (steering)
- Longitudinal control (acceleration, braking, gear shift)
- Electronic parking brake
- Turn signal
- Hazard light

In our prototype test vehicles, these interfaces are spliced by the Vehicle Integration Team; the exact method depends on the given vehicle and the type of the interface. However, all manipulated VCIs preserve the parallel possibility of manual control actions – so-called driver override – taken by the Safety Driver.

For production vehicles, we expect OEMs to provide a standardized DBW-compatible actuation and control system – as part of the general vehicle infrastructure – for the AD SW to access the respective VCIs.

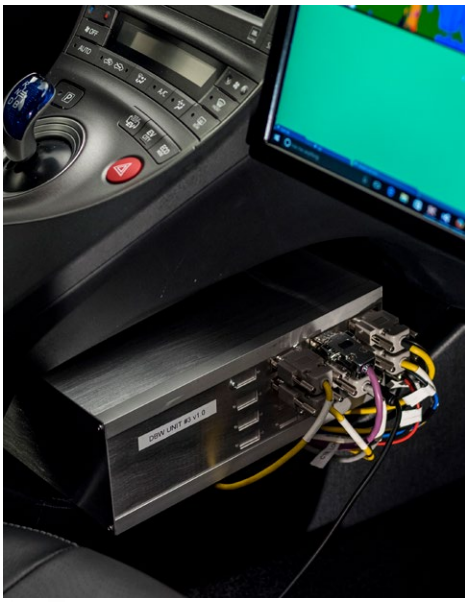
5.3 SAFETY LIMITS THROUGH DBW

In AImotive's reference implementation, communication with the vehicle infrastructure is implemented by a dedicated, development-purpose HW element, the Drive-By-Wire (DBW) Unit, and related SW components, to provide safe and reliable control of AD test vehicles.

Currently available production vehicles do not include standard drive-by-wire interfaces for single, unified communication channels; therefore, the respective analog or digital interfaces have to be accessed separately.

However, we put maximum emphasis on the demand that modifications do not corrupt the original control and safety mechanisms of the vehicle.

The DBW System is responsible for providing an actual physical interface between the vehicle and the aiDrive™ compute platform, to control the vehicle's actuators based on the output of aiDrive™. It is also responsible for keeping the vehicle in a safe state by:



- Applying safety limits for actuation commands
  These set a threshold for steering and deceleration commands commands to ensure that a trained safety driver can take back control of the vehicle without exiting the lane in critical situations. Safety limits are calibrated on closed test tracks and are stored in the DBW Unit's firmware.
- Allowing driver intervention
- Managing critical error handling procedure upon AD system failure, to move the vehicle into a safe state

The main component of the DBW System is a separate HW unit, the DBW Unit, with proprietary firmware.

5.4 VEHICLE CYBERSECURITY

To avoid any harm to the public or property as a result of a cyber-attack, AImotive guarantees the security of test vehicles through the following means

- Limited physical access to the test vehicle, with strict control over the keys and to the vehicle compute platform
- The AD SW is stored on a removable HW drive of the vehicle compute platform, so that operators do not and cannot modify the base image of the computer
- No wireless access points to the AD SW.

- No possibility to modify the source code on the vehicle computer. Code must originate from our centralized and secure build system

5.5 HMI

The human-machine interface (HMI) of the AD system plays a crucial role in managing and monitoring the operation of the automated vehicles and in reacting to events:

The development-purpose HMI of our vehicle-level AD system is composed of the following elements:

- Compute platform HMI: external monitor with a debug aiDrive™ application window, complemented with a keyboard and embedded touchpad
- DBW control panel: allows interacting with DBW and enabling or disabling a self-driving session and showing the status of the respective vehicle subsystems through LEDs
  The DBW also provides audio signals in the case of AD-related events (activation/deactivation, driver override or failures).
- Self-drive panel: a small display mounted on the top of the dashboard indicating whether self-driving is active

5.6 ROAD TESTING

Even though simulation has countless advantages and can cater to various traffic situations and ODDs, it does have its limits. No matter how realistically a simulator can render the world or emulate physics, it still is not reality. Simulation can reduce the amount of real-world testing needed but cannot replace public road tests entirely. Without public road testing, the innovative solutions of AD technologies would never mature to a level where they are safe for public use.

Therefore, AImotive is testing aiDrive™ on real roads on a daily basis at several locations across multiple continents.

However, testing on public roads requires careful consideration and specific preparations to ensure safety. The following chapters provide an overview of the measures taken at AImotive to ensure the safety of our testing process.

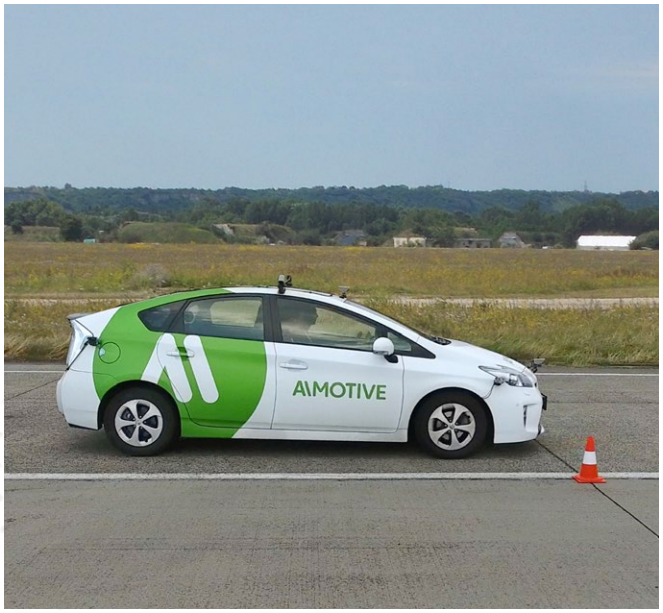
5.6.1 GENERAL ROAD-TESTING POLICY

Tests are performed according to the list of test cases derived from the functions supported, based on the experience of safety drivers, which is continuously extended with cases found during on-road testing.

In AImotive's general policy, road testing always requires human supervision while the AD system is performing the dynamic driving task.

We distinguish the following types of road testing:

- Closed test track
- Public roads for which we have a testing permit



5.6.2 CLOSED TEST TRACKS

We test new AD SW functions on closed test tracks in cases when the development team or the Safety Drivers judge the risk of affecting the normal flow of traffic on public roads unacceptable.

These include, for example:

- Early DBW and aiDrive™ function tests
- Measurements related to vehicle dynamics
- Functions involving sudden maneuvers, for example, Automatic Emergency Braking (AEB) according to EURO NCAP test protocol

5.6.3 PUBLIC ROADS

Once a new aiDrive™ functionality has successfully passed simulation – and if required, closed test track – testing, public road testing can commence.

Daily test drives on selected, pre-defined highway sections are performed to check aiDrive™

highway autopilot functions, such as lane keeping, adaptive cruise control, lane change/ overtaking, highway exit, and merge.

Currently, we are testing on the following highway sections:

- Hungary: M0, M3, M6, M5, M7
- Mountain View, California, USA: 101, 280

In-vehicle tests include testing the AD software on local highway sections under different circumstances, in different vehicles available from the fleet. For example, the same functionality may be tested with or without a radar sensor available in the vehicle.

New functions are first tested in detection-only mode (where possible), when actuations are disabled, while detections and the intentions of the vehicle are visualized and logged for evaluation of correct operation. During highway test drives, the whole test drive is logged automatically, with application screen recording and disengagements marked separately in the log.

Additionally, all functions on the Master SW branch undergo regular regression tests both in simulation and on public roads, to detect any subtle deviations in the behavior of existing AD functionalities.

During daily test drives, drivers test the system according to a testplan, where test cases are derived from the general concept and requirements. Test cases cover various functions under different curcumstances, which can be performed on known highway sections within a reasonable distance from the development center. New software versions are tested against this checklist, plus additional tests to validate the new functionality, as described in the requirements requesting the new functionality.

Operators can also mark challenging situations or notable events on the debug HMI of the AD SW, which can be used for later analysis, or they can be re-created as simulated scenarios to support the development and regression testing of the AD software.

5.6.3.1 ENSURING DRIVER AWARENESS DURING TEST DRIVES

Safety drivers are not allowed to operate the vehicle in self-driving mode for more than 90 minutes in a single session. After this session, the safety driver must rest at least for 30-minutes. The maximum time allowed in self-driving mode is 4 hours per day. Due to high traffic or difficult, dangerous traffic situations, this time frame can be reduced if deemed necessary by the Safety Driver or Operator on the spot.

5.6.4 EVALUATION OF FIELD TESTS

Logs and recordings of all road tests are processed automatically by a dedicated internal tool and their summary published on an internal website, providing comprehensive information, for example, about the traversed route on a map, the list and statistics of disengagements with reasons for disengagements and comments from the operators, or official test reports of Safety Drivers.

Disengagements are also visualized in clusters over a map, color coding the reasons for, and the number of disengagements in a selected area. This helps developers find and better understand challenging road sections identified during field testing. Recordings of application operation of all test drives are also available in the report.

Data from disengagements are then used for:

- Bug reporting for subsequent code correction
- Scenario creation for re-creating the conditions leading to the disengagement in simulation testing

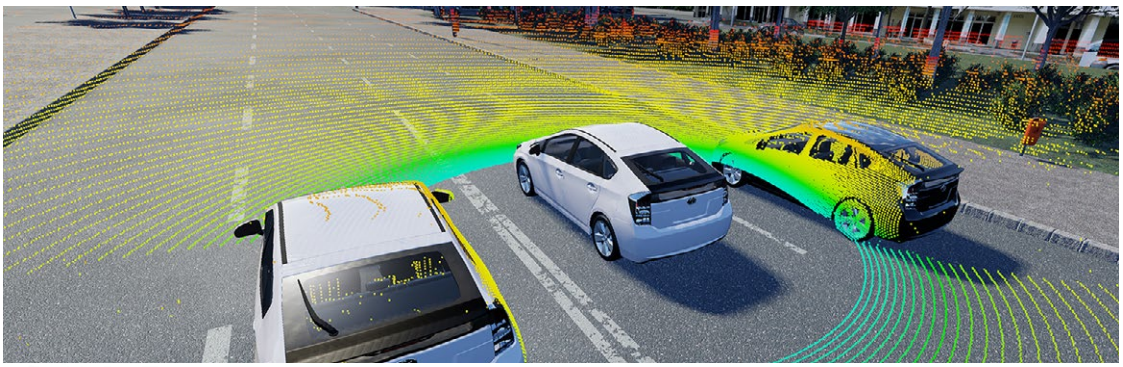
A new AD SW function can only be merged into the main codebase (Master branch) after the Safety Driver confirms that all previously reported bugs have been corrected and applicable test cases have been passed.

5.7 DATA COLLECTION

We collect data from test drives for the following main purposes:

- Recording raw sensor data and logging actual application operation for later analysis and automated tests
- Recording for annotation, to be used in NN training and verification/benchmarks

Our data collection and protection policy is in line with the European Union's GDPR regulations, and is available on our website.



5.7.1 RECORDING AND LOGGING

During test drives, aiDrive™ can record raw sensor input and the output of SW modules, in any combinations. These can be used to:

- Reproduce test drives in an office environment to analyze any anomalies experienced during the actual drive, using recorded sensor or SW module data
- Run aiDrive™ in automated tests using recorded raw sensor data (instead of simulated sensor data)

Issues detected during test drives are reviewed by the members of the Vehicle Test team, using the recordings and log files produced during the test drive. If any deviations are found, tickets are raised for developers, describing the issue and associating it to the specific segment of the recording created during the test drive.

Recorded raw sensor data are also an invaluable source for automated tests, as new aiDrive™ functionalities can thus be tested in our automated testing environment using real-world sensory data. Additionally, selected and representative tested locations are modeled in aiSim™, which allows for the comparison of AD SW behavior and performance on real-world and simulated versions of the same road section.

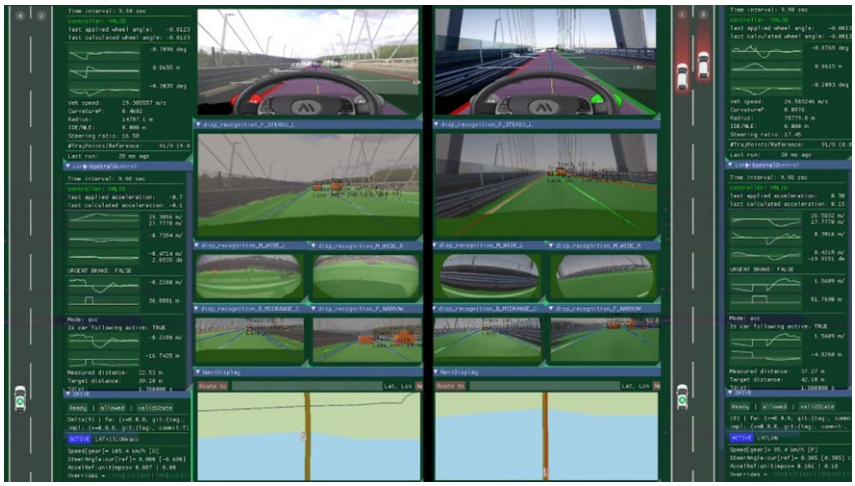


FIGURE 16. *aiDrive™ driving in a real and a simulated world*

5.7.2 DATA COLLECTION FOR ANNOTATION

Well-prescribed and quality data collection is indispensable for developing state-of-the-art neural networks to perceive and understand the environment around an AD vehicle.

For this purpose, Almotive applies several types of automated and manual data collection and annotation methods to provide the sufficient quality and quantity of training and verification material for our high-performance, real-time operating neural networks.

5.8 DISENGAGEMENT REPORT

Every year Almotive prepares reports of disengagements from public road tests for respective local authorities, where the company conducts public road testing.

A recent report to the Californian authority on year 2019 collects the unintended disengagements in autonomous mode while testing pieces of AD technology that meet the definition of SAE L2+ or above (for example, in lane change or merge maneuvers). These reveal a limited number of disengagements (a few dozen) over several thousands of overall driven miles.

6. aiDrive™ safety features

AImotive is committed to achieving automated driving safety that exceeds human capabilities on the overall AD system level, with our aiDrive™ AD software application at its heart.

6.1 SAFETY ON SYSTEM- AND PRODUCT-LEVEL

We believe that to reach and maintain a distinguished level of safety for the complete automated driving system, we must continuously analyze and improve on all aspects and components of the system.

Therefore, we apply processes and recommendations from standard ISO 26262:2018 Road vehicles – Functional safety, an automotive industry standard for functional safety, to identify, assess, and mitigate faults and hazards for the AD system. For details, see General safety approach and activities.

We also carry out stringent integration tests when all the components of the AD system (sensors, compute platform, auxiliary equipment) are installed on and inside a test vehicle.

On the product level, AImotive integrates various means of hardware and software diagnostics and failsafe functions to promote a high level of safety and to avoid hazards during the operation of the aiDrive™ software suite. Failsafe functions can be grouped into the following main areas:

- Failsafe functions for perception, including fields like sensor diagnostics, support for multiple sensor modalities, or the combination of various AI-based and classical computer vision methods in the same SW pipeline
- Failsafe functions for motion planning, including filtered trajectory and plausibility check, considering safety constraints evoked by internal and external environmental conditions
- Failsafe functions for vehicle control, monitoring vehicle status (including wheel speed, acceleration, yaw, pitch, and roll)

6.2 DIAGNOSTICS

6.2.1 SENSOR DIAGNOSTICS

aiDrive™ continuously monitors the operation of the sensor system so that it can promptly react to any sensor degradations or faults.

Sensor diagnostics cover the following main areas:

- Basic sensor health checks like sensor availability
- Arrival and quality of sensor data, to reveal, for example, sensor contamination, loss of focus, frame drop, or sensor freeze
- Sensor offset compared to the vehicle body
- Comparing localization algorithms using different types of sensor data (for example, GPS, IMU, or visual odometry)

Diagnostics information originating from these sources is processed by a dedicated sensor diagnostics SW module of aiDrive™, which communicates the reliability of the sensor system towards Low-Level Control.

6.2.2 SW MODULE DIAGNOSTICS

Diagnostics of aiDrive™ SW modules are interpreted and managed on the following levels:

- Monitoring runtime and latency of distinct SW modules and application threads
- During a self-drive session, the operator continuously monitors these values and can indicate the need for a driver override to the safety driver upon need.
- The Low-Level Control module supervises the overall self-drive session, the sensors system, and the output of certain SW modules (e.g., Trajectory, Motion planning), triggering a driver override request and disengagement upon serious deficiencies

6.3 FAILURE MODES

aiDrive™ SW or AD system failures are managed on the following main levels:

- The Low-Level Control module of aiDrive™ can detect serious and dangerous failures of the AD SW and can trigger a disengagement notifying the driver to take over control of the vehicle.
- The DBW Unit monitors the communication channels towards the vehicle control interfaces and can initiate a disengagement, for example, in the case of false or unsafe control requests, or when the connection towards the vehicle infrastructure is lost.
  In such cases, besides alerting the driver, the DBW Unit can keep or restore a “safe state” of the vehicle until the driver intervenes, holding the last valid steering trajectory value and decelerating the vehicle until a full stop if required.

The basic fallback mechanism returns control of the vehicle to the human driver, as on this level of automation, the driver still has the overall control and responsibility for the operation of the AD function and for the behavior of the vehicle.

7. General safety approach and activities

Stringent safety procedures help prevent unwanted anomalies, hazards, and damage to humans or transport infrastructure.

aiSim™ ISO 26262:2018

TÜVRheinland CERTIFIED

AUTOMOTIVE SPICE®

AImotive is committed to building and sustaining a healthy and visible safety culture that penetrates all the development and testing activities of the company.

As an essential guiding rope, we have formulated and are continuously evaluating and improving our processes and activities in the light of the automotive safety standard ISO 26262:2018 Road vehicles – Functional safety. The processes of our SW development pipeline are also adapted to adhere to the Automotive SPICE process reference model.

These approaches manifest, for example, in our thorough, multi-layer testing procedure, or in the following types of safety-related activities that we perform during the early stages of SW development:

- Definition of safety goals resulting from the Hazard analysis and risk assessment (HARA)
- Stipulation of safety requirements
- Analysis of new AD system or software
- Thorough and comprehensive expert review of all work products

Our applied dynamic testing methods also follow the principles laid out in ISO 26262, including:

- Requirement- and scenario-based testing
- SW module and system interface tests
- Fault injection tests in simulation
- Resource usage monitoring and testing, including stress testing of the AD system both in simulation and in test vehicles

We are also closely following the progress of the ISO 21448 Road vehicles — Safety of the intended functionality (SOTIF) standard, and apply its approaches, for example, in the practice of defining functional requirements in the form of traffic scenarios. SOTIF also places significant emphasis on simulation-based verification and validation, which plays a key role in our development and testing pipeline.

With the continuous extension of the ODDs and the included traffic scenarios, we are broadening proper situational awareness and the extent of the known and analyzed area (dangerous vs. not dangerous situations), while reducing the area of unknown but possibly hazardous events, to increase the safety of the intended AD function.

8. Compliance to legal regulations

AImotive pays close attention to all applicable legal regulations at every location where it operates, with special emphasis on locations where public road testing is carried out. We are obliged to the following legal regulations allowing testing permissions:

- California, US:
  - *California Code of Regulation:*
    Title 13, Division 1, Chapter 1, Article 3.7 Testing of Autonomous Vehicles
  - *California Vehicle Code 38750*
- Nevada, US: NEVADA REVISED STATUTES Chapter 482A
- Hungary: 5/1990. and 6/1990. (IV.12) KöHÉM statutes (on technical inspection and technical conditions of road vehicles)

9. Challenges and the way forward

In this section, we elaborate on some of the future challenges to the autonomous driving technologies and their safety aspects. Our goal is to foster open discussion and sharing of knowledge and ideas among stakeholders to pave the way to safer roads.

HARDWARE PLATFORMS FOR AUTOMATED DRIVING

Currently available mass production embedded HW platforms for ADAS or AD systems are limited both in terms of computing capabilities and efficiency for more resource-demanding AD functions and applications.

Almost all automated driving systems currently in development or production rely on commercial GPUs for image processing. Though they offer flexibility in programming, they consume too much power and produce a lot of heat, which makes them inapplicable for mass production automotive use.

In addition, neural networks – which are proliferating in AD applications – require a strikingly different approach to HW design and implementation. For this reason, we started to develop our own NN accelerator hardware IP, aiWare™, for maximum operational performance and efficiency.

We foresee the rise of new, modular, and distributed embedded HW platforms – through the collaboration of OEM, Tier 1s, and HW engineering hubs - dedicated to automated driving with much lower power consumption and with a high emphasis on efficient, real-time NN inference of high-resolution sensor inputs.

SENSOR EVOLUTION

We also expect the rise of more reliable, automotive-grade, high-definition sensors, as well as the emergence of new sensor technologies similar to imaging radar or the simultaneous detection of visible wavelengths and mid-infrared rays in cameras. All these are closely connected to the HW platforms that will be able to process their data, and allow for the more profound perception and interpretation of a vehicle's environment.

This will also facilitate the evolution of sensor fusion techniques, as no single sensor can cater to the complex requirements of automated driving.

DATA COLLECTION AND ANNOTATION

Efficient and scalable neural networks require a multitude of quality ground truth data both for training and verification. This poses ever higher requirements to data collection and annotation techniques, as currently, many of them mainly rely on manual effort.

We foresee the advent of more automated data collection and annotation technologies that will allow for faster NN training and verification and ODD/geographical area extension.

At AImotive, we will continue our research and implementation efforts in this field as well to strengthen the foundations of safe automated driving.

REGULATORY ASPECTS

Currently, there are no applicable regulations for the public use of self-driving systems in real-road traffic.

We expect that in the upcoming years, lively discussions and first attempts will unfold to put a regulatory fence around the first implementations of L3 and L4 AD systems in terms of applicability or moral aspects, such as liability and responsibility. Inevitably, we will be at the forefront of these discussions.

SIMULATION

We can clearly see the increasing importance of simulation in the verification of AD systems, as simulation is a major driving force behind ensuring the safety of automated driving.

One of the main questions that will need a firm answer is how to validate and further improve the realism of simulation; its representation of the actual world. This area involves both the visual representation, the quality of synthetic sensor data, and the physical vehicle models used in simulation. The closer simulation is to reality, the better the AD software can be tested in it, resulting in ultimately safer and more reliable automated driving technologies.

We also see the rising need for a standardized scenario definition language that allows for the exchange of scenarios between simulation applications. AImotive experts actively participate in a standardization endeavor for scenario definitions, OpenSCENARIO. OpenSCENARIO will allow industry players to bring the most out of their existing scenarios and other resources to make road transport safer for everyone.

CYBERSECURITY AND UPDATING THE AD SW

Automotive OEMs and their partners have to ensure that the best possible algorithms are available for users of a car throughout its lifetime. Continuous improvement of existing AD features, the introduction of new features, support of new ODDs or geographical regions require constant access to the AD SW and the possibility to update it over the air (OTA).

However, this raises serious cybersecurity concerns that the automotive industry will have to tackle and solve.

10. Conclusion

The above have detailed AImotive's approach to the safe development and testing of automated driving technologies.

Heavily relying on simulation improves testing AD software safety and reduces development times while allowing our team to manage resources effectively and focus on the most pressing areas of software development. Placing simulation as a safety barrier between development and real-world tests means that only reliable and mature versions of aiDrive™ are ever tested on public roads.

Our testing procedures rely on the knowledge and experience of our team supported by specific training for monitoring autonomous vehicles even at high speeds. Further guidelines, policies and rules ensure that our vehicles are road-ready, and our safety drivers are never fatigued or distracted. With two persons involved in testing, one is only ever monitoring road conditions, while the other reviews information from the self-driving system. Additional hardware safety barriers ensure that the self-driving software cannot transmit erratic behavior to the drive-by-wire system of the vehicle.

It is AImotive's belief that our development pipeline and the safety considerations and practices outlined in this report drastically improve the safety of autonomous vehicle testing everywhere and contribute to the creation of truly safe autonomous driving systems, operable in any location, any climate, at any time.

www.aimotive.com