IEEE SA
STANDARDS ASSOCIATION

IEEE SA WHITE PAPER

AUTONOMOUS DRIVING ARCHITECTURE (ADA)

Enabling Intelligent, Automated, and Connected Vehicles and Transportation

Authored by

Autonomous Driving Working Group

IEEE

ACKNOWLEDGMENTS

Special thanks are given to the members of IEEE SA Autonomous Driving Working Group (ADWG) for their discussions, comments, and reviews.

The authors of this paper are as follows:

Boon Chong Ang, *Intel*
Marius Dupuis, *ASAM*
Yong He, *Futurewei*
Yu Huang, *Futurewei*
Shugang Jiang, *JOYNEXT*
Astha Kukreja, *IEEE Senior Member*
Subhadip Kumar, *IEEE Senior Member*
Hongyang Li, *Shanghai AI Lab*
Linda Lim, *UC Berkely*
Jiaqi Ma, *UCLA*
Rajesh Murthy, *GAPASK*
Gaurav Pandey, *Texas A&M University*
Scott Schnelle, *Waymo*
Jin Shang, *IEEE SA ADWG Vice Chair*
Dong Sun, *IEEE SA ADWG Chair*
Lei Sun, *TuSimple*
Huijie Wang, *Shanghai AI Lab*
Wei Wei, *Guangzhou University*
Zijiang Yang, *Synkrotron & IEEE SA ADWG Vice Chair*
Mohammad Yasin, *Tech Mahindra*

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA27287 979-8-8557-1166-0

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA DOCUMENTS

This IEEE Standards Association ("IEEE SA") publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the activity that produced this Work. IEEE and the Autonomous Driving Working Group (ADWG) expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the ADWG disclaim any and all conditions relating to: results; and workmanlike effort. This document is supplied "AS IS" and "WITH ALL FAULTS."

Although the ADWG members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE SA OR ADWG MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder.

This Work is published with the understanding that IEEE and the ADWG members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

AUTONOMOUS DRIVING ARCHITECTURE

ABSTRACT

As the automotive industry continues its rapid evolution toward autonomy, this document describes a prototypical Autonomous Driving Architecture (ADA) along with a promising application ecosystem. It comprehensively explores fundamental components within ADA, ranging from hardware and software stack layers to regulatory and ethical considerations.

- Trends and challenges: The document sets the stage by detailing prevailing trends shaping autonomous driving. It navigates challenges encountered in transformation, encompassing safety imperatives, regulatory complexities, cybersecurity concerns, and societal readiness.
- ADA: A focal point of the discussion, ADA delineates the hierarchical layers comprising hardware, software stack layers, infrastructure, services, and application interfaces. By proscribing their interplay, ADA's modular and scalable framework will promote the evolution of autonomous driving systems.
- Applications: Venturing into practical uses, the document explores diverse applications fostered by ADA's ecosystem, from immersive in-vehicle experiences to revolutionizing mobility.
- Innovative technologies: At the forefront of innovation, emerging technologies such as artificial intelligence and vehicle-to-everything (V2X) communication are considered as enablers for autonomous driving and smart cars.
- Regulatory and ethical considerations: The document navigates the regulatory terrain governing autonomous vehicles, such as safety standards, certification protocols, and legal frameworks.

In essence, this document offers a holistic view of ADA and its ecosystem, illuminating its vast potential and the challenges ahead in realizing the vision of autonomous mobility.

1. INTRODUCTION

Smart cars, like the proliferation of other digital products, will reshape the landscape of the global automotive and transportation industry into a new era of software-defined vehicles (SDVs). The automotive industry is undergoing an innovation process akin to the replacement of feature phones with smartphones. This transformation encompasses various aspects, including the shift from internal combustion engines to electric motors as the primary powertrain, the evolution from manual driving to autonomous driving, and the transition from individual car ownership and driving to embracing safe, convenient, and cost-effective travel services.

The new transportation industry integrates the automotive, IT, communication, transportation, and energy sectors. It has the potential to lead to a reversal of current leading companies and countries, resulting in a massive transfer and reconfiguration. This marks the crown of the global fourth industrial revolution.

At the same time, the software for smart cars encompasses a range of modern software, including real-time embedded firmware, cloud computing software, consumer software, simulation software, AI algorithms, and large-scale multi-agent collaborative system software. The complexity and criticality of smart car software underscore the imperative need to ensure the utmost safety, security, and reliability. The ramifications of software failures extend far beyond mere inconvenience, potentially posing life-threatening consequences, necessitating the adoption of advanced software engineering and testing methodologies to ensure rigorous validation.

This document targets declarations of ADA in the technologies, applications, and related issues. Its scope and methodology range from trends, layers, applications, and innovations to regulatory and ethical issues, consisting of software, hardware, data, AI (including deep learning models and large-scale models), applications, safety/security, laws, and social factors, etc.

2. TRENDS AND CHALLENGES OF THE AUTOMOTIVE AND TRANSPORTATION INDUSTRY

The automotive and transportation industry stands amid a transformative era where rapid technological advancements, evolving consumer preferences, and global challenges are reshaping the landscape. Technological innovations, such as autonomous vehicles, are redefining traditional notions of mobility. Connectivity and data-driven insights are revolutionizing the way vehicles operate and interact with their surroundings. The emergence of autonomous and intelligent vehicles, smart infrastructure, and the integration of digital platforms are reshaping business models and operational processes. Adapting to these technological disruptions while ensuring safety, security, and regulatory compliance poses a formidable challenge for industry stakeholders.

As the world embarks on this journey into the future, it becomes imperative to comprehensively examine the major trends and challenges that define the trajectory of this crucial sector.

2.1. TRENDS

The industry is undergoing a profound transformation driven by several key trends. This white paper explores the following major trends shaping the future of this industry and the challenges that accompany them.

2.1.1. SOFTWARE: ARISE OF A SOFTWARE-DEFINED VEHICLE

SDVs mark a significant trend in the automotive industry. Vehicles are no longer purely mechanical; they are becoming increasingly intelligent with sophisticated software governing various aspects. This trend includes the development of advanced driver assistance systems (ADAS) and autonomous driving (AD) capabilities, OTA capability, vehicle-cloud computing collaboration, etc., highlighting the industry's journey toward a future where vehicles are not only electric but also intelligent and capable of autonomous operation.

Software-defined vehicles not only bring intelligence such as ADAS/AD's AI and algorithms but also use the complex software on the complex hardware to implement most conventional vehicle functionalities, such as cockpit, smart chassis, power domain (BMS/VCU), body domain, etc. In addition, OTA capability and function/application updates in the vehicle life cycle need the new in-vehicle software layers, such as the vehicle operating system (VOS) and application.

Software-defined systems empower vehicles to optimize performance dynamically, leveraging real-time data and user preferences. This optimization spans adaptive engine management, efficient energy utilization in electric vehicles, and dynamic adjustments to driving conditions, which culminate into a driving experience characterized by heightened efficiency, responsiveness, and sustainability.

2.1.2. HARDWARE: FROM DISTRIBUTED TO CENTRALIZED

The traditional automotive architecture, characterized by numerous electrical control units (ECUs) distributed throughout the vehicle, is undergoing a profound transformation. This shift involves transitioning towards a centralized computing platform or HPC, where the functions and capabilities of multiple ECUs are consolidated into a unified, centralized system; then, automakers can simplify the architecture, reducing the number of ECUs and associated wiring.

As vehicles become increasingly reliant on software for their operations, a centralized architecture provides a unified framework for implementing features such as connectivity, autonomous driving, and over-the-air updates. This consolidation not only simplifies the vehicle's electrical system but also enhances efficiency by facilitating seamless communication between different vehicle systems/components.

Centralized computing architectures offer scalability and adaptability, allowing for easier incorporation of future technologies and functionalities. As automotive technology continues to evolve, having a flexible and scalable platform is essential for seamlessly integrating new features, addressing security concerns, and ensuring compatibility with evolving industry standards.

2.1.3. ECOSYSTEM: IN-VEHICLE EXTENDS TO MULTI ECOSYSTEMS

With the ADAS/AD functionalities and new software and hardware, an electric smart car is not only a safe and efficient form of mobility but also an energy center and computing center. The fleet vehicles will work closely with smart cities and transportation, smart grid, smart data center with AI, etc. The vehicle ecosystem is extended into more ecosystems, and more innovations and new markets emerge.

2.1.4. AI: FROM SMALL MODELS TO A UNIFIED LARGE MODEL

As time goes on, the AI techniques in autonomous driving gradually evolve. It is seen that the multiple small models to handle various problems in perception, prediction, localization, and planning, etc., have evolved, such as bird's eye view (BEV) and transformer network, 3D occupancy network (OccNet), and world model, etc. In the

meantime, since large-scale language models (LLMs) make breakthroughs in AI with the emergent technologies of commonsense knowledge and reasoning, an end-to-end solution with a unified large model is being considered. However, energy efficiency and sustainability are crucial factors in the design and operation of autonomous vehicles. Overreliance on computational-heavy models like LLMs could indeed pose challenges in terms of energy consumption, especially in resource-constrained environments such as electric vehicles.

2.2. CHALLENGES

While these trends promise a more sustainable, connected, and intelligent future for the automotive and transportation sector, they also present unique challenges that need to be addressed for successful implementation.

2.2.1. ESCALATING SOFTWARE COMPLEXITY

As vehicles become more reliant on software for operations, the complexity of software development increases exponentially. The integration of features such as infotainment, ADAS, and autonomous driving demands sophisticated software solutions. Managing this complexity poses a challenge for automakers, requiring robust development processes and frameworks to help ensure the reliability and performance of the software-defined systems. The failure of one module can potentially impact the performance of the entire system, emphasizing the need for robust interconnectivity.

Ensuring that software remains up-to-date, secure, and compatible with evolving technologies requires continuous testing and validation of software. Simulating real-world scenarios and edge cases and ensuring the resilience of software to unforeseen circumstances are challenges that automakers need to address comprehensively. Collaboration between different teams, including hardware and software engineers, becomes critical to achieve a cohesive and integrated software-defined system.

2.2.2. DATA-DRIVEN SOFTWARE DEVELOPMENT

The automotive industry is experiencing a paradigm shift towards data-driven software development. This entails collecting vast amounts of data to enhance intelligence, train artificial intelligence (AI) models for advanced driver assistance (AD/ADAS), improve telemetry and diagnostics, and enhance user experiences. Effectively harnessing and managing this data becomes crucial for the success of automotive software initiatives, necessitating the development of robust data infrastructure and analytics capabilities.

Achieving interoperability and standardization in data formats and protocols is crucial for seamless collaboration within the automotive ecosystem. As the volume of data grows exponentially, ensuring a scalable and efficient storage infrastructure becomes critical, and the vast amounts of data collected pose challenges related to security and privacy. Data-driven software development allows vehicles to become more intelligent by leveraging historical and real-time data. This data includes information on engine performance, driving behavior, and system health. Analyzing telemetry data facilitates proactive diagnostics that enable manufacturers and service providers to identify issues early, improve reliability, and optimize vehicle performance.

2.2.3. SAFETY AND SECURITY IMPERATIVES

The paramount concern in the automotive industry is the safety of occupants and other road users. In addition, in the current vehicle digitalization era, functional safety, safety of the intended functionality (SOTIF), cybersecurity, and data privacy become the key vehicle quality and safety elements. There are two parts to autonomous vehicle (AV) safety—mechanical system safety and electronic and electrical (E/E) system safety. E/E safety for vehicle platforms is defined by ISO 26262-1 [4][1] and for conventional vehicles is defined by SAE J3061 [7].

Advanced driver assistance systems (ADAS), automated driving features, and more in-vehicle intelligent functions offer immense potential to enhance road safety. However, unlike traditional vehicle software, they also company with complex software operations in an environment with many dynamic variables. Any failure in the software or cybersecurity defenses could lead to accidents and harm to people, property, and the environment; malicious attacks can compromise privacy, cause financial losses, disrupt operations, and compromise safety. Therefore, advanced features and innovations have to be accompanied by rigorous safety assessments. Integrating safety into the design and development process helps to ensure that innovative technologies are not only groundbreaking but also reliable and secure.

The safety and security challenges in the connected automotive era are not obstacles but imperatives that define the responsible evolution of the industry. Automakers should embrace a culture that prioritizes safety and cybersecurity over preliminary function, investing in technologies, processes, and collaborations that ensure vehicles are not just innovative and connected but safe and secure for everyone on the road.

[1] Numbers in brackets correspond to the sources listed in Section 7.

2.2.4. AI MODEL'S PROBLEMS

Autonomous driving is an application of AI in complex driving scenarios. It is regarded as a "long tailed" problem with scarce data collected for corner cases. Though the data closed-loop is taken as the solution, how to get the valuable data efficiently is still open, and the cost to annotate the data for supervised training of the model is still large. In the field of autonomous driving, training large models presents unique challenges compared to tasks like natural language understanding and general image recognition, in which the pretrained model and fine-tuning framework of the foundation model are not grounded yet.

On the other hand, a balanced approach is needed, where energy-efficient algorithms and models are prioritized alongside small language models (SLMs) and LLMs. For example, using lightweight perception and control algorithms combined with LLMs for high-level decision-making could reduce computational requirements while maintaining performance. Furthermore, advancements in hardware acceleration, optimization techniques, and edge computing may also help mitigate energy consumption concerns associated with LLMs.

3. AUTONOMOUS DRIVING ARCHITECTURE (ADA)

3.1. REQUIREMENTS

Based on autonomous driving's requirement of full stack software, and in response to the trends of central computing hardware and the integration of vehicle-cloud, as well as the emerging technologies like AI large models, a refined definition of the overall architecture for autonomous driving is established and can be considered as the vehicle operating system (OS) or vehicle AD-OS. This involves optimizing and clearly defining conceptual boundaries—expanding, iterating, and refining the roles of modules within each layer, including hardware, infrastructure, services, and application.

3.1.1. REVIEW OF CURRENT SYSTEMS

Today's automotive E/E (electric/electronic) architecture can be divided into different domains, such as infotainment, chassis, body control, and AD. The infotainment system typically employs Linux or commercial off-the-shelf general-purpose operating systems, while chassis and body controls utilize the standard AUTOSAR CP (classic platform).[2] AUTOSAR AP (adaptive platform),[3] as a foundational software platform, primarily provides the

[2] Available at https://www.autosar.org/standards/classic-platform.
[3] Available at https://www.autosar.org/standards/adaptive-platform.

basic operating environment for the entire vehicle, but it lacks safety, real-time frameworks, and services. SOAFEE, some open source, and vendors define the vehicle or automotive OS architecture, but that definition primarily focuses on overall structure with less detailed descriptions of components.

3.1.2. KEY REQUIREMENTS FOR ADA

The key requirements for ADA are as follows:

- **Open architecture:** The boundaries have openness and a clear development interface. It enables easier integration with external systems, hardware, and software, thereby achieving greater flexibility, interoperability, and scalability. It also has the potential to attract more developers and partners to participate in the development, driving the advancement and innovation of autonomous driving technology.
- **Hierarchical decoupling:** The use of hierarchical decoupling architecture not only makes the software function independent of the underlying specific hardware, but also divides the complex system into various levels with clear functions, reduces the complexity of the system, increases the security, reliability, maintainability, portability and scalability, and improves the development efficiency. It is flexible to achieve “performance-oriented” and “cost-oriented” differentiated product needs, and better support different technical routes.
- **Safety and security:** Considering the construction of security systems from an overall perspective, functional safety, SOTIF, security, and data privacy are organically integrated into the entire process of product design, development, production, operation, and maintenance. The security technology of hardware and software is used to create a full-stack internal security system, improve the versatility and flexibility of security policies, and consider the performance and cost of products.
- **AI and large model (LM):** Explore and give play to the role of AI and LM in improving the perception, understanding, and decision-making ability of intelligent driving system, intelligent cockpit, and other aspects of the vehicle. Using AI and LM requires data closed-loop, automatic annotation, and scene construction.
- **Vehicle-to-infrastructure/vehicle-cloud computing:** V2X (vehicle-to-infrastructure/person/vehicle/cloud) helps the AD have redundant perception, global planning, and more service-oriented architecture (SOA) cross-domain applications. The extra computing is needed while the vehicle lacks the full AD hardware/software/algorithm, and the vehicle-cloud (edge) collaborative computing architecture is

proposed based on real-time and reliable communication in the decentralized, distributed, disaggregated networks for specific applications or scenarios.

3.2. AUTONOMOUS DRIVING ARCHITECTURE (ADA)

3.2.1. OVERVEIW OF ADA

The high-level framework of ADA is described in Figure 1.

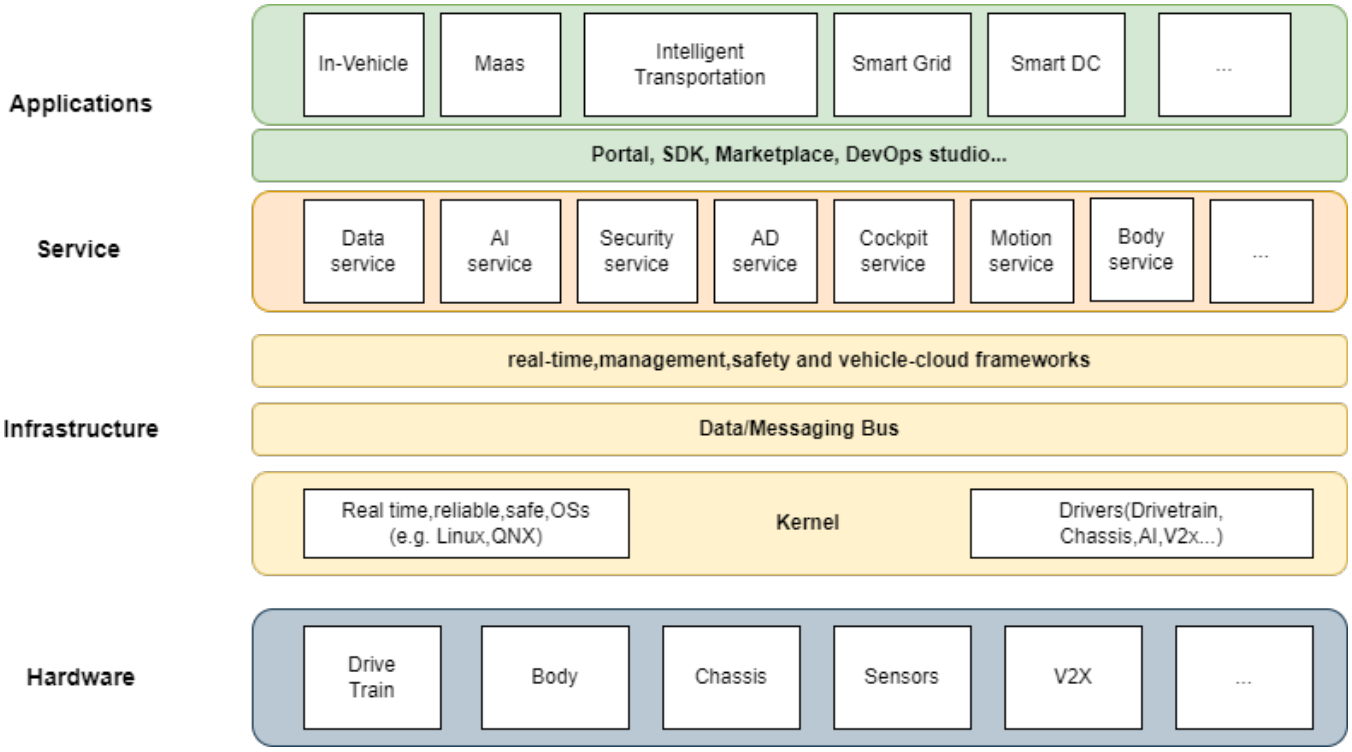

FIGURE 1: Autonomous Driving Architecture (ADA)

ADA defines the new and clear layers and their boundaries of hardware and full software stacks, and supports HPC hardware, AD/ADAS application integration, SOA/SDV application, and ecosystems. ADA includes a hardware layer, an infrastructure layer, a service layer, and an application support layer (as shown in Figure 1). It also shows the architecture of the VOS (infrastructure and service layers) in the AD domain, which can be extended to an in-vehicle domain, the decoupling of hardware from software, and application decoupling from VOS. VOS layers clearly describe the inside modules that can come from different industry chains.

- **Hardware layer:** This layer includes the physical components of the vehicle, such as chassis, drivetrain, sensors, and actuators. More importantly, it includes the computing hardware platforms for AD/ADAS used to process the data from the sensors and control the vehicle's movements.
- **Infrastructure layer:** This layer includes a real-time, reliable, and safe operating system kernel, BSP/Drivers, middleware for communication and messaging and data bus systems, real-time and safety frameworks, etc.
- **Service layer:** This layer provides the common services such as AI services for AI and LM frameworks, data services for the data closed-loop process, security for network security and data privacy, V2X services, etc., It also provides the specific services for AD systems providing AD's perception/planning/control common functions and services. While considering in-vehicle operating systems including other domains, the service layer will be extended to include the cockpit, chassis, body, and power control.
- **Application interface layer:** This layer provides interfaces, tools, and develop studio that enable developers to create applications and services for the autonomous driving system. It includes a portal for accessing the system's features and settings, a marketplace for purchasing and downloading apps and services, an SDK for developing custom applications, and a test studio for testing and validating new features and functions.

3.2.2. HARDWARE LAYER

The hardware layer includes physical sensors and actuators that are located on chassis, driver unit, and body. The AD/ADS hardware platform may have multiple different numbers of hysteresis chips such as AI chips, general computing, MCUs, safety chips, etc. ADA defines a unified hardware architecture to cover SAE L2-L4 (SAE J3016 [6]) with different sensors, actuators, and hardware architectures that have different chip providers, and need the corresponding VOS to support the heterogeneous distributed hardware architecture.

3.2.3. INFRUSTRUCTURE LAYER

The common and generic layer includes the operating system kernel, data and message bus, and functional frameworks.

- **Operating system kernel:** A real-time, reliable, and secure operating system kernel is the cornerstone of the autonomous driving system. The operating system kernel is primarily responsible for managing the hardware resources of the vehicle and providing basic support for processes, threads, memory, network, and security for upper-layer software. In a heterogeneous distributed hardware architecture, different units load kernels with different functional safety levels: AI computing units have a functional safety level of QMASIL-B; the supporting general computing units have a functional

safety level of QMASIL-B; the supporting control units have a functional safety level of ASIL-D. This may require the design of multiple kernels with different safety levels or a single kernel that supports applications with different functional safety levels.

- **Data and message bus:** Data and message bus modules are used to coordinate and manage communication between various components of the vehicle. They provide unified communication interfaces and protocols to ensure that different components in the vehicle can exchange data and events conveniently. Through middleware and message bus, it achieves efficient data sharing and collaborative work within the vehicle, including intra-process, inter-process, cross-kernel, cross-CPU, inter-board, and even cross-vehicle-to-cloud unified communication mechanisms.
- **Functional frameworks:** In response to the safety and productization common requirements generated by intelligent driving, designing and implementing a generic framework module to meet these common requirements is the basis for ensuring real-time, safe, scalable, and customizable intelligent driving systems. In addition, with the gradual realization of advanced intelligent driving applications and the widespread application of large models in intelligent driving, faced with more complex and diverse scenarios, the powerful computing and storage resources of the cloud (or edge) can be utilized through the vehicle-to-cloud computing framework. The algorithms and models in the cloud can be further advanced to more complex and advanced decision-making and planning under vehicle regulations. Therefore, the frameworks include a real-time framework, vehicle-cloud collaborative computing framework, and safety framework.
- **The real-time framework** relies on communication middleware to provide customizable data interfaces and a real-time data processing framework. The real-time framework ensures decoupling and reliable communication among algorithm applications and hardware platforms. It supports the topological relationships of data flow nodes for different intelligent driving applications and algorithms. Considering system performance and functional safety requirements, different flow nodes are deployed to specific AI acceleration units, computing domains, security domains, etc. Tasks can be scheduled and allocated based on factors such as task priority, real-time requirements, and resource availability to ensure that various functional modules are scheduled and executed reasonably according to their priority and timing requirements. The real-time framework needs to meet the requirements for the autonomous driving system to operate in real-time with safe and stable operation in complex traffic environments.
- **The vehicle-cloud collaborative framework** achieves real-time and safe vehicle-cloud collaborative

integration between intelligent connected vehicles and cloud edge computing, etc. The vehicle-cloud collaborative framework needs to provide reliable data transmission and synchronization mechanisms to ensure the efficiency and accuracy of data transmission and synchronization between the vehicle and the cloud. It also allocates and assigns the computing works to vehicle and cloud, respectively, based on latency, application, vehicle hardware, etc.

- **The safety framework** provides a series of functional safety mechanisms, including real-time monitoring of hardware devices, operating systems, applications, system resources, etc. When relevant faults or abnormal states are detected, the safety framework needs to respond and report to prevent faults from spreading and affecting the operation of the entire system, and decisions are made and processed by the framework according to system configuration. A complete safety framework also includes safety backup functions for the control unit, providing mechanisms for system fault degradation and fault-tolerant operation while meeting the functional safety requirements of the control unit ASIL-D. The uncertainty and unexplainable characteristics of AI and large models also require the safety framework to provide corresponding safety detection mechanisms and failure-safe functions, which can increase heterogeneous redundancy algorithms for AI and large models.

3.2.4. SERVICE LAYER

The service capabilities layer provides essential functions and support for the autonomous driving system. As intelligent driving technology develops, AI large models, data security, and network security become increasingly crucial. Comprehensive requirements for information security services and data closed-loop services are needed. The basic and common services also need to be scalable, continuously evolving, and innovative to meet the challenges and demands of intelligent driving technology. The functional service layer includes autonomous driving services, intelligent cockpit services, chassis and body services, data services, safety services, connected services, AI services, etc.

A framework in autonomous driving could be end-to-end or modular style. *End-to-end* systems generate control signals directly from sensory inputs. Control signals can be the operation of the steering wheel and pedals (throttles and brakes) for acceleration/deceleration (even stop) and turning left/right. There are three main approaches for end-to-end driving—direct supervised deep learning, neuro evolution, and deep reinforcement learning. LLMs-based methods usually belong to this category.

Modular systems are built as a pipeline of multiple components connecting sensory inputs to actuator outputs. Key functions of a modular ADS are regularly summarized as perception, localization and mapping, prediction, planning and decision making, and vehicle control, etc.

Recently BEV perception has been the most active perception direction in autonomous driving. After BEV, the 3D occupancy network is coming to the forefront in the perception domain of the self-driving field.

Large models play a crucial role in the business solutions for autonomous driving. Small models are designed to run in real-time on the client side, such as the vehicle itself, with limited computing resources. On the other hand, large models are run on the server/cloud side, without the real-time constraint, using powerful computing resources. Large models often handle more extensive data input and generate more results compared to small models on the client side. The performance achieved by large models sets a performance "ceiling" for small models, and they serve two main purposes as follows:

- **AI services:** To support the end-to-end (e2e) or modular AD systems, there are some typical AI functions to serve. An e2e neural network model could infer the vehicle trajectory or the control signal of the brake, the throttle, and the steering wheel. A modular pipeline provides some perception functions like 2D/3D obstacle detection and tracking, lane/boundary detection and tracking, traffic light detection and classification, etc. A localization module could use Neural Network (NN) models for motion estimation, visual odometry estimation, Simultaneous Localization and Mapping (SLAM), etc. A prediction module could infer the obstacle's motion or trajectory based on interaction modeling. A planning module provides the vehicle's trajectory based on an understanding of surrounding obstacles, the road (lanes and boundaries), the targeted destination, traffic rules, as well as efficiency and convenience. Data unification is important to build a general model for different vehicles with different sensor configurations. Virtual sensor is a technique in transferring data to a predefined virtual sensor, either camera, LiDAR, or radar; novel view synthesis is tailored to keep the consistency of sensor data in each modality. To support the data closed-loop and iterative upgrades of autonomous driving systems, it is crucial to implement smart data selection, automatic data annotation, safety-critical scenario detection, and generation in simulation-based model verification before real road testing. If LLMs are integrated into the autonomous driving platform, the instruction tuning method or the text-augmented multi-modal method can leverage the common knowledge and reasoning capabilities in the LLMs.
- **Data services:** Based on the algorithm architecture, the data flow can be categorized as end-to-end or modular pipelines. In the e2e system, usually the output could be fed to the controller or directly to the

end actuator (i.e., brakes, throttle, steering wheel). For the controller, the input data is the vehicle trajectory from the planner. For the actuator, the data changes to wire control signals for brakes, throttle, and steering. Either e2e or modular systems requires the same input from sensors, like cameras, LiDARs, radars, GNSS, IMU, and map (navigation map or HD map), etc. In modular systems, this input goes into the perception module and localization module, the output from the perception and localization module includes the vehicle location and orientation, and obstacles information (3D location on the road) and road information (lanes, boundaries, traffic lights, and signs, etc.), fed into the prediction and planning modules. The output from planning and the result from the controller should be the same as the e2e system mentioned previously. When the data unification is performed, sensor data is converted to the transformation space before feeding into the trained model. To support the data closed-loop, simulation data is also generated for model validation. If LLMs are integrated, a text prompt is utilized to provide clues from LLMs.

- **Security services:** Security services encompass data security, network security, AI security, etc., providing application information security services for the intelligent driving system. This establishes a comprehensive lifecycle security protection mechanism for vehicle data and personal privacy, guarding the intelligent driving system against unauthorized access, tampering, and destruction. It employs various protection measures based on data security classification, which implement comprehensive control over data throughout its lifecycle. This includes establishing a classification and grading mechanism for data, encrypting sensitive personal information, providing secure data transmission channels, and anonymizing personal information outside the vehicle. It also covers integrity protection and confidentiality protection for the on-board computing platform, as well as identity and access control. Additionally, it includes security management and isolation for intelligent driving applications and communication, such as transmission security between the intelligent driving domain and other in-vehicle network nodes, V2X nodes, and the cloud. Access control, encryption protection, and monitoring between different domains within the on-board intelligent computing platform and with actuators are also covered. The safety framework ensures the security of AI models by providing encryption and model integrity verification methods, preventing adversarial sample attacks and model tampering. It establishes an attack detection engine based on AI and large models, along with corresponding detection signature libraries, and applies them in real-time to AI interfaces or large model libraries.
- **Vehicle-cloud services:** The V2I module enables communication between the vehicle and surrounding infrastructure. This allows vehicles to exchange data, communicate with other vehicles, share traffic

information, and receive cloud-based control signals. Real-time perception or decision-making information from external elements like traffic lights and other vehicles can be integrated through connected services and data flow frameworks. Connected services provide functions such as remote monitoring, data uploading, and command issuance for intelligent driving systems. The cloud obtains real-time traffic information, vehicle status, location, sensor data, etc., and sends commands to the vehicle through data analysis, enabling remote control, collaborative operations, global management, and more.

- **AD services:** These services provide algorithm components/model libraries that users can use directly or in combination to form different functions within the intelligent driving system. They mainly support the efficient development of intelligent driving algorithms, providing decomposable and reconfigurable algorithm modules and atomic component libraries for intelligent driving applications. It includes algorithms for environment perception, fusion positioning, decision planning, and motion control, enabling the vehicle to operate autonomously or with reduced driver intervention.
- **Cockpit services:** The cockpit module focuses on user interfaces and interactions with the vehicle. It includes components such as the infotainment system, dashboard, head-up display, and human-machine interface (HMI). The cockpit functional services provide generic models, including large-scale language models, which, through real-time analysis of the driving environment data and natural language commands, questions, and conversations from the driver and passengers, better understand the driver's intentions and needs. This enables drivers and passengers to interact with the vehicle more conveniently and intelligently, enhancing the driving experience.
- **Chassis and body services:** These services involve monitoring, controlling, and optimizing the chassis (including suspension, braking system, etc.) and body (including doors, sunroof, lights, etc.) of the vehicle through intelligent electronic control systems and sensors. This aims to enhance driving safety, comfort, and performance. It includes features like chassis suspension adjustment, electric seat adjustment, automatic switch control, and active safety systems (such as anti-lock braking, electronic stability control, etc.). These advancements contribute to the development of the automotive industry towards intelligence, connectivity, safety, and comfort.

4. APPLICATIONS

4.1. IN-VEHICLE APPLICATIONS

ADA provides the interface for application integrations and developments. These applications can have different levels of autonomous driving functions, be extended to more SOA applications across domains, and provide additional convenience and safety.

4.1.1. ADAS/AD (L1-L4)

Based on ADA, ADAS/AD application can be easily developed and integrated by several steps: defining or choosing hardware including chips, sensors, actuators, vehicle body, etc.; defining application topology by using framework; plugging the algorithms and defining messages, or configuring the services to use, etc. The highly efficient and independent platform's behaviors show the advantages of ADA and VOS.

4.1.2. SOA/CROSS-DOMAINS (IVI, BODY, CHASSIS, POWER)

Service-oriented architecture (SOA) is widely used in intelligent driving systems. SOA contains the Service Provider and Consumer, and communication across multi-domains. The change from signal to service makes the applications be developed in their domain and do not need the changes in other domains, such as the Power domain can rely on the map or ADAS output service to have better emission control.

Application developers can carry out cross-domain functional communication through SOA-based services, which are used to support the application layer to interact with IVI, body actuators, power management, and other services.

4.2. ECOSYSTEM

The smart mobility application ecosystem signifies a transformative wave in the transportation landscape, where a constellation of digital applications converges to redefine how we move, connect, and experience urban mobility. At its essence, this ecosystem encompasses a diverse array of applications designed to streamline, enhance, and personalize various facets of transportation, ranging from daily commutes to logistics and beyond.

4.2.1. SMART CITY

The smart mobility apps ecosystem may be highly based on ADA and Vehicle OS, SDV/SOA applications, etc., and could be integrated into mobility as a service (MaaS) Platforms, such as ride-sharing apps, car rental apps,

parking apps, navigation apps, represents a paradigm shift towards a more connected, efficient, and user-centric transportation system. By leveraging digital technologies, these applications empower individuals, businesses, and cities to navigate the complexities of urban mobility while fostering sustainability, accessibility, and an overall improved quality of life. This ecosystem is not merely a collection of apps but a catalyst for the evolution of transportation into a seamlessly integrated, intelligent, and interconnected network that offers benefits as well, for example, enhanced convenience, urban planning advancements, real-time information, optimized resource utilization, cost-effective solutions, and environmental sustainability.

4.2.2. ENERGY AND EMISSION UNDER INTELLIGENT VEHICLES

Smart driving cars can also contribute to energy conservation and emission reduction, for instance:

- By analyzing traffic conditions and real-time data to optimize routes, select the most efficient routes and driving speeds, avoiding traffic congestion and unnecessary waiting, thereby reducing vehicle energy consumption and exhaust emissions.
- By optimizing acceleration and braking processes and implementing energy recovery techniques to reduce energy loss and decrease vehicle energy consumption.
- By monitoring the condition and performance of vehicles, providing timely maintenance recommendations, ensuring vehicles are in their best condition, reducing energy waste, and prolonging the lifespan of vehicles.

Smart cars typically rely on pure electric power as their energy source. In the event of natural disasters causing disruptions to the power system, they can also serve as a backup power supply or as a virtual grid plant for the grid, supporting the operation of small electrical devices.

4.2.3. MOBILE COMPUTING CENTER

The computing center is an integral component of smart cars. In addition to utilizing the computing power and resources of the computing center, smart cars can also serve as edge computing nodes, performing computing center tasks during their idle periods. This dual role makes smart cars a versatile computing platform. By harnessing the computing power and resources of the computing center, smart cars can engage in complex data processing and analysis, enabling more intelligent driving experiences and services. Moreover, when not in use, smart cars can contribute their idle resources to the computing center, providing computational capabilities for other tasks and further enhancing resource utilization efficiency.

5. INNOVATIVE TECHNOLOGIES

5.1. ARTIFICIAL INTELLIGENCE (AI)

Deep learning recently has been extended to the prediction and planning module, as the data-driven solution to replace the rule-based method. Large-scale language models (LLMs) have had remarkable success with emergent capabilities of commonsense knowledge and reasoning. However, explainability and safety of AI models are still open, and how to evaluate the AI models is critical.

5.1.1. LARGE LANGUAGE MODEL (LLM)

Foundation models are a form of generative artificial intelligence (generative AI). On a technical level, foundation models are enabled by transfer learning and scale. Foundation models usually follow that a model is pre-trained on a surrogate task and then adapted to the downstream task of interest via fine-tuning.

World models explicitly represent an autonomous agent's knowledge about its environment. The main use cases are pure representation learning, planning, or learning a policy in the world model (neural simulator). For world model and traffic behavior simulation, multi-modal language models can be built with a training dataset of sensor-text-action data (with the help of LLMs) to generate reasonable and realistic predictions.

An obvious perspective on applying LLMs for autonomous driving is that LLMs can serve as the decision-making "brain." Various tools within the autonomous vehicle ecosystem, including the perception module, localization module, and in-cabin monitor, function as the vehicle's sensory "eyes." Additionally, the vehicle's actions and controller function as its "hands," executing instructions derived from the LLM's decision-making process.

5.2. DATA CLOSED-LOOP

The key to data closed-loop building is the source of data. The data-driven models or algorithms applied to solve autonomous driving tasks are the base.

It can be formulated as follows: capturing data from the vehicle, selecting valuable data, annotating them, training/finetuning the expected model, validating and deploying the target model to the vehicle etc., constitute a data closed-loop for autonomous driving.

As a platform, the data closed-loop should include both the client vehicle end and server cloud, implementing

data collection and preliminary screening at the vehicle side, mining based on some machine learning strategy (such as active learning) in the cloud side database, automatic tagging, model training and simulation testing (simulation data might also join model training), and model deployment back to the vehicle side. Data selection/screening and data labeling/annotation are key modules that determine the efficiency of the data closed-loop.

Data selection is divided into two ways: one is online style, where the trigger mode for data collection is set on the human-driven vehicle, which can collect the required data most economically; another is the database model; in addition, in cases where there is a significant lack of data for known scenarios or targets, a “content search” mode can also be set on the vehicle or server side to search for similar object, scene or scenario data to enhance the diversity of training data and the generalization of the model.

Based on the data selection and annotation output, the training platform can adopt reasonable methods to absorb these incremental data. Among them, active learning is the most common method, which can efficiently use these valuable data.

5.3. SAFETY AND SECURITY

Considering the construction of the safety system from the whole of the automatic driving system, it is still not clear for AI and LM’s safety and security architectures, and AI/LM continuously evolve.

Research on safety technologies with reliable redundancy design, multi-layer and diversified monitoring schemes, fail-operable or fail-de-escalation safety modes, scene library construction, and test evaluation are all part of the integrated security strategy. The risk caused by insufficient design and limited performance of the automatic driving system in the hazard scenario is controlled within a reasonable and acceptable range. To comprehensively ensure network security, research focuses on the construction of a secure and trusted environment, an in-depth defense system, network security monitoring, and elastic engineering based on endogenous security. This approach addresses risk identification and vulnerability, security protection, security detection, security response, and rapid recovery. For the entire lifecycle of data, a comprehensive technical system of data security is built, centered on the processes of data collection, transmission, storage, processing, provision, disclosure, deletion, and destruction.

6. REGULATORY AND ETHICAL CONSIDERATIONS

The rapid advancement of autonomous driving technology necessitates a thorough examination of regulatory and ethical frameworks to ensure safety, privacy, equity, and accountability. The architecture of AVs is inherently complex, involving diverse components like sensors, algorithms, and connectivity systems. As these vehicles move closer to widespread deployment, regulatory bodies, and ethical guidelines need to evolve to address emerging challenges.

- Regulatory framework adaptation for safety and compliance—Regulatory frameworks must be adapted to ensure AVs meet stringent safety standards before hitting the road. This includes comprehensive testing protocols, certification processes, and continuous monitoring systems to detect and mitigate potential failures. Regulations should also mandate the interoperability of AV systems to enhance safety through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications.
- Ethical framework for decision-making algorithms—Ethical considerations should guide the development of AV decision-making algorithms, especially in scenarios involving moral dilemmas. Frameworks should promote transparency, accountability, and fairness in algorithmic decisions, ensuring that AVs do not perpetuate biases or inequality. Ethical guidelines should also address the allocation of liability in accidents involving AVs, balancing between manufacturers, software developers,
- Accountability mechanisms—To build public trust in AV technology, transparency and accountability mechanisms need to be implemented. This includes the disclosure of safety records, incident reporting mechanisms, and clear communication channels for public feedback. Regulatory bodies should have the authority to hold manufacturers and operators accountable for safety breaches or ethical violations.
- International collaboration on standards and practices—Given the global nature of the automotive industry, international collaboration is essential to harmonize standards and practices for AVs. This includes shared safety standards, ethical principles, and data protection regulations, facilitating cross-border operation of AVs and ensuring consistent safety and ethical considerations worldwide.

6.1. REGULATORY CHALLENGES

6.1.1. SAFETY AND SECURITY STANDARDS

Ensuring the safety and security of AVs is paramount, necessitating comprehensive standards and protocols. These standards are designed to mitigate risks, protect against cybersecurity threats, and help ensure the

reliability of AV systems under various operational scenarios. As AVs integrate deeply with societal infrastructure, the establishment of rigorous safety and security measures is essential to prevent harm to users and the public.

- Comprehensive testing and certification—AVs need to undergo extensive testing and certification processes before deployment. This includes simulation-based testing, closed-course testing, and real-world operational testing to verify system reliability and response under diverse conditions. Certification protocols should assess the vehicle's ability to handle emergency situations, system failures, and interaction with non-autonomous entities (e.g., pedestrians and non-AV vehicles).
- Cybersecurity measures—Cybersecurity is a critical component of AV safety, requiring robust protection mechanisms to safeguard against hacking and unauthorized access. Standards should mandate end-to-end encryption for data transmission, regular security audits, and the implementation of intrusion detection systems to prevent and respond to cyber threats.
- Fail-safe operation protocols—AVs should be equipped with fail-safe mechanisms that activate in the event of system failure. This includes redundant systems for critical operations, safe-stop procedures, and manual override capabilities. Ensuring vehicles can safely transition to a minimal-risk condition is essential for passenger and public safety.

6.1.2. DATA PRIVACY AND OWNERSHIP

As AVs collect and process vast amounts of data, ensuring the privacy and ownership of this data is a critical concern. Regulations must protect individual privacy rights while allowing for the beneficial use of data to improve AV functionality and traffic management. Balancing these needs requires clear guidelines on data handling, consent mechanisms, and user control over personal information.

- Clear data governance policies—Data governance policies must clearly define how data is collected, used, stored, and shared. This includes specifying the types of data collected, purposes for collection, and the entities with access to this data. Policies should enforce the principle of data minimization, ensuring that only necessary data is collected.
- Data security and anonymization—Protecting data security and privacy requires implementing strong encryption, access controls, and anonymization techniques. Sensitive information should be anonymized or pseudonymized to prevent the identification of individuals, especially in shared data scenarios or when used for traffic management and research.

6.1.3. AUTONOMOUS VEHICLE DECISION-MAKING

Driver accountability is also stressed in the Global Forum for Road Safety's 2020 [2] draught international standards on autonomous vehicle safety. The guidelines that are currently being developed state that drivers should be able to drive safely at all times, that they should resume control of the vehicle promptly and appropriately when asked to do so, that they should be familiar with the rules and regulations surrounding takeovers and what can be done while the vehicle is in automated mode, and that they should think about their abilities when using a shared driving system since some people might not be able to do so safely due to mental or physical limitations. It would appear that the AV manufacturer benefits from the asymmetry in responsibility for running the AV, while the driver bears a disproportionate share of the burden.

Drivers need to know what to do and what risks are involved for AVs to run safely on roadways. This is also necessary for the driver and vehicle to share responsibility in an accident. Liability and insurance frameworks will become less predictable if users give their approval to drive a vehicle when they have not been given all the necessary information or when it is known they will not pay attention. This makes the validity of their "consent" questionable in any post-accident litigation.

There is a tendency for the present policy discussion on autonomous vehicle certification and licensing to center on the vehicle rather than the driver. At the global level, a group within the UNECE known as the World Forum for Harmonization of Vehicle Regulations is attempting to come up with a system for the secure certification of AVs that adheres to the standards set by physical certification tests, real-world test drives, and audit procedures (GRVA 2019 [3]). Law Commission (2019) [5] states that the focus is currently on AV certification rather than AV drivers since the technology is still in its early stages of development. Creating a training system that works for all AV models is not going to happen overnight.

7. REFERENCES

The following sources have either been referenced within this paper or may be useful for additional reading:

[1] Cui, J. and Sabaliauskaite, G., On the Alignment of Safety and Security for Autonomous Vehicles. The Second International Conference on Cyber-Technologies and Cyber-Systems. 2017.

[2] Global Forum for Road Safety, UNECE Global Forum for Road Safety Eightieth Session, 3 March 2020. https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp1/ECE-TRANS-WP1-Informal_document-MARCH-2020-7e.pdf. (Accessed Nov 2023).

[3] GRVA (2019), Future certification of automated/autonomous driving systems. International Organization of Motor Vehicle Manufacturers (OICA).

[4] ISO 26262-1, Road Vehicles—Functional Safety.

[5] Law Commission, Scottish Law Commission (2019*) Automated vehicles: analysis of responses to the preliminary consultation paper*. https://www.scotlawcom.gov.uk/files/2815/6093/3787/Automated_Vehicles_-_Analysis_of_Responses_to_the_Preliminary_Consultation_Paper.pdf (Accessed Nov 2023).

[6] SAE J3016, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.

[7] SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571