WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 8, Number 5, Year 2026
DOI: https://doi.org/10.62051/ijcsit.v8n5.03
Journal homepage: https://wepub.org/index.php/IJCSIT/index

The Foundation of the All-Round Security of Intelligent Vehicles is Digital Security

Yixin Zuo [1], Jianming Li [2], Ru Tian [2,*], Fan Zhang [2]

[1] CATARC Huacheng Certification (Tianjin) Co., Ltd., China
[2] China Auto Information Technology (Tianjin) Co., Ltd., Tianjin, China
*Corresponding Author: tianru@catarc.ac.cn

ABSTRACT

As intelligent vehicles evolve from AI-enabled tools to intelligent entities with autonomous interaction capabilities, security boundaries are no longer confined to traditional mechanical protection, but extend to the all-domain scenario where data flows, algorithm operations, network communications and location services interweave and coexist. Therefore, digital security technology serves as the core support for intelligent transformation and the technical cornerstone that underpins the all-domain security. In this context, digital security can empower the upgrading of traditional security systems and enable the leap from "passive protection" to "active prevention".

KEYWORDS

Intelligent vehicles; AI; Global Scenarios; Global security; Security Upgrades

1. INTRODUCTION

Digital security is one of the fundamental prerequisites for the interconnection and collaboration of industrial ecosystems. The core of the future development of automotive intelligence lies in the in-depth empowerment of AI technology. AI security acts as the "brain" of intelligent vehicles, not only continuously iterating multifunctional user experiences and new value propositions, but also serving as the core hub driving intelligent decision-making for vehicles; Connected security is the "neural network" that supports the operation of this "brain", and its stability and reliability are the key cornerstones for ensuring real-time information transmission and multi-system synergy, directly determining the effectiveness of the intelligent experience. Satellite systems, as the "sky-eye" of vehicle safety, precisely compensate for the limitations of traditional on-board perception in remote sections and complex road conditions, enabling comprehensive all-domain perception with no blind spots. Based on the security logic and functional positioning of these core components, this paper clearly categorizes the digital security system of intelligent vehicles into three core domains: AI security, connected security, and satellite security.

2. AI SECURITY – THE ANCHOR OF TRUST FOR INTELLIGENT AGENTS

The essence of automotive intelligence lies in the evolution from mechanical vehicles to intelligent integrated agents, and AI security serves as the prerequisite for this transformation. In the era of "AI defines the car", safety has upgraded from a basic need to a core competitiveness, whose depth determines product premium and ecological boundaries, and AI security is no longer a backend

technical concept, but a core value that users can perceive and experience, as well as an anchor for building human-vehicle trust. AI security directly determines whether users dare to use and love to use the intelligent functions of cars, and it is also the core barrier and value carrier of differentiated competition for automakers.

Automotive AI security is a comprehensive security system that is built on reliable infrastructure, drives the evolution of intelligent driving models through secure data loops, and ensures that the behaviors of intelligent agents are controllable and trustworthy within the framework of relevant ethics and governance norms. The core is to transform cars from traditional means of transportation into safe, reliable, and responsible "wheeled intelligent agents."

From an industry perspective, intelligent vehicle safety has extended from traditional physical protection to digital and intelligent domains, driving the safety system to evolve from passive protection to active early warning and autonomous risk avoidance, and the core driving force is the large AI safety model. The model precisely addresses the industry pain points of risk intelligence and cross-domain transmission in the AI era, builds a solid foundation with its powerful scenario prediction and offensive and defensive capabilities, and upgrades security from a static "armor" to an "evolutionary immune system" adapted to unknown risks with its continuously optimized evolutionary characteristics.

2.1. AI Security Risks in Specific Scenarios

AI Hallucination Risk: AI tends to misinterpret information in extreme environments, such as heavy rain or strong backlight. It may mistake guardrails ahead for a passable road and fail to respond to pedestrians crossing the street, showing no response to pedestrians crossing the road; In strong light at tunnel entrances and exits, it may also mistake red lights for yellow ones, increasing the risk of running red lights. The main issue is that the algorithms lack sufficient resilience. Insufficient training data is available for rare road conditions and complex lighting-shadow scenarios, making the models prone to misjudgment before they acquire adequate learning experience. The AI's decision-making logic is like a "black box", and drivers can't understand why it makes such a choice, making it hard to trust and difficult to find out the cause of problems [1].

Algorithmic Discrimination Risk: AI exhibits “bias” issues, which are evident in automotive applications. For example, facial recognition demonstrates a low success rate on drivers with darker skin tones. Elderly drivers speak slowly and have indistinct pronunciation, and voice commands are often misrecognized, making it impossible to use the vehicle normally; At intersections, AI may consistently prioritize yielding to larger vehicles while delaying evasive actions for cyclists and pedestrians, particularly riders with disabilities. The root cause is that the training data is "biased", with too few samples of special groups and niche traffic participants; And the algorithm doesn't take "fairness" into account; it only pursues overall accuracy without considering whether the user experience of different groups is balanced [2].

Risk of Capability Malfunction: In-vehicle AI may suddenly malfunction and execute unanticipated actions that cannot be mitigated in a timely manner. For example, on a familiar route, the autopilot may suddenly misidentify the right-turn lane and execute an aggressive lane change; An emergency should give way to pedestrians, but if there are both pedestrians and cyclists at the same time, it may jam or choose to crash into the guardrail instead of slowing down; Some in-vehicle infotainment systems may incorrectly increase volume or adjust seating positions due to misinterpreted voice commands. The core issue is the model's poor adaptability and inability to handle complex scenarios it has never seen before, such as extreme weather and sudden accidents; Additionally, the AI’s objective rules are poorly defined, leading to ambiguous prioritization in complex situations. Coordination with vehicle hardware also contains vulnerabilities, preventing the termination of anomalous commands..

The Problem Of Illegal Abuse: AI technology may be exploited to inflict harm, such as hacking in-vehicle cameras and voice systems, surreptitiously recording drivers' facial data, communications and driving trajectories, and leveraging such data for fraudulent activities; Using AI to make fake vehicle diagnosis reports, modifying fault data, and tricking consumers into buying problematic used cars; More critically, adversaries may embed backdoors in vehicle systems, forging radar signals to mislead autopilot, misrepresenting brake failures as normal operation, and even remotely controlling vehicles to trigger malicious braking or acceleration.This is because the information protection of in-vehicle AI is inadequate and sensitive data is not encrypted; Third-party navigation and diagnostic plugins have not checked for security issues and are vulnerable to malicious programs; Single-factor authentication, such as passwords or basic facial recognition, can also be bypassed using AI-forged images.

External Attacks And Threats: In-vehicle AI is vulnerable to being attacked by outsiders to "seize power", directly affecting driving safety. For example, someone can trick the AI into misting "No entry" for "U-turn allowed" by sticking special stickers on traffic signs; Send malicious instructions via Internet of Vehicles and Bluetooth to hijack the route planning of self-driving cars and lead them to remote areas; Attackers may also use jamming devices to disrupt cameras and radars, causing AI to falsely perceive a clear path ahead and resulting in collisions; The AI makes fake voice commands and plays them in the car to trick the voice assistant into opening the car door and starting the engine. The technical flaw is that the sensors are not protected against this "trick" and have not been trained for such attacks; The Internet of Vehicles is loosely protected, making it easy for outsiders to break in; AI can't quickly identify abnormal signals either, and attack instructions can be executed smoothly.

2.2. Security Requirements and Technology Trends

As an emerging technology, AI has prompted the development of standardization frameworks both domestically and internationally to ensure its secure deployment. Internationally, In December 2023, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) released ISO/IEC42001:2023 "Information technology - Artificial intelligence Management System" Management system provides a framework and guidance for organizations to establish, implement, maintain and continuously improve a responsible and trusted AI management system; ISO also released ISO/PAS 8800:2024 Road vehicles - Safety and artificial intelligence in December 2024, becoming the world's first systematic specification for automotive AI safety. Geely Automobile has obtained its first AI safety certification covering the entire lifecycle of requirements analysis, data management, verification testing, deployment and operation. Regulation (EU) 2024/1689 on artificial intelligence (AI Act) classifies AI systems deployed in or associated with autonomous vehicles that impact driving and passenger safety as high-risk AI systems, which may be deployed only if they meet stringent requirements. These requirements include risk mitigation mechanisms, high-quality datasets, activity logging, comprehensive documentation, transparent user disclosures, human oversight, and robust performance in terms of reliability, accuracy and cybersecurity.

Although regulations and standards on AI security at home and abroad are not yet complete, AI security urgently needs leading security requirements.

2.2.1. AI Offense-Defense Confrontations Escalate from Digital Space to the Physical World

Intelligent car AI attack and defense have broken through the boundaries of the digital space and escalated into direct attacks against the physical world. Traditional digital attacks are evolving into novel threats that disrupt on-board sensors via physical media (e.g., sound, light and electromagnetic signals), directly triggering fatal hazards such as vehicle loss-of-control incidents. It is imperative to construct an endogenous-exogenous coordinated defense system and prioritize the development of a series of supporting key technologies. Develop recognition technology for cross-modal adversarial

attacks to detect behaviors that cooperatively deceive multiple sensors; Overcome the generation and defense challenges of physical-world adversarial attacks and achieve native defense to enhance the robustness of models in real-world environments; Identify and remediate vulnerabilities in sensor fusion algorithms, optimize fusion strategies to counter such composite attacks, and ultimately establish comprehensive protection capabilities to address emerging physical security threats.

2.2.2. Ensuring the security and trustworthiness of the entire AI research and development chain is crucial

The security of in-vehicle AI systems extends to the upstream and downstream supply chains, and security risks penetrate and spread along the upstream core links such as open-source data and pre-trained models, and the vulnerability of a single component may cause systemic failures. To address this trend, security capabilities need to be embedded throughout the entire R&D and integration process. Focus on developing detection and defense technologies for targeted data poisoning to ensure that training data is feasible from the source; Develop an identification and isolation system for model fine-tuning backdoors to prevent malicious features from being triggered after deployment; Develop security audit standards for third-party model components, create automated audit tools for in-vehicle scenarios, and build a full-chain security defense line.

2.2.3. AI security goes beyond the technical realm and is deeply integrated with social governance

AI security for smart cars has become a social governance issue that integrates law, standards and ethics, and new risks drive full coverage of laws, regulations and industry standards. Compliance and privacy protection capabilities need to be integrated at the algorithm design stage, and legal standards need to be transformed into enforceable technical checkpoints. Focus on developing an AI review platform adapted to in-vehicle scenarios to integrate automated ethical review and compliance verification capabilities; At the same time, tackle privacy compliance technologies such as lightweight federated learning and dynamic encryption to meet strict regulatory requirements while ensuring data availability and achieve effective synergy between technical solutions and social governance goals.

2.3. Connected Security – The Pillar of Global Interconnection

Connected security refers to the security system tailored for the "person-vehicle-road-cloud-satellite" all-domain interconnection scenario of intelligent vehicles, upgrading the vehicle network from a single communication link to an all-domain interconnection security hub, and through the synergy of technology and management, ensuring reliable vehicle positioning, reliable instruction transmission, timely emergency response, and preventing risks such as cyber attacks, data leaks, and malicious intrusions. Meanwhile, strictly complying with cross-border data compliance and security management requirements, it constitutes a comprehensive security domain with full controllability over positioning, communication, data and control in complex connected vehicle environments. Its strategic value has gone beyond mere technical protection and has become a prerequisite for the industrialization of intelligent connected vehicles and the implementation of smart city transportation. The core is to upgrade the vehicle network from a single communication link to an all-domain connected security hub, ensuring reliable positioning, reliable instructions and timely emergency response of vehicles in the all-domain connected environment, and ultimately achieving all-dimensional security and controllability of the vehicle network in complex connected scenarios [3].

(1) Application scenarios

According to the classification of communication subjects, automotive connected vehicle security can be divided into two major scenarios: traditional automotive network security and V2X security.

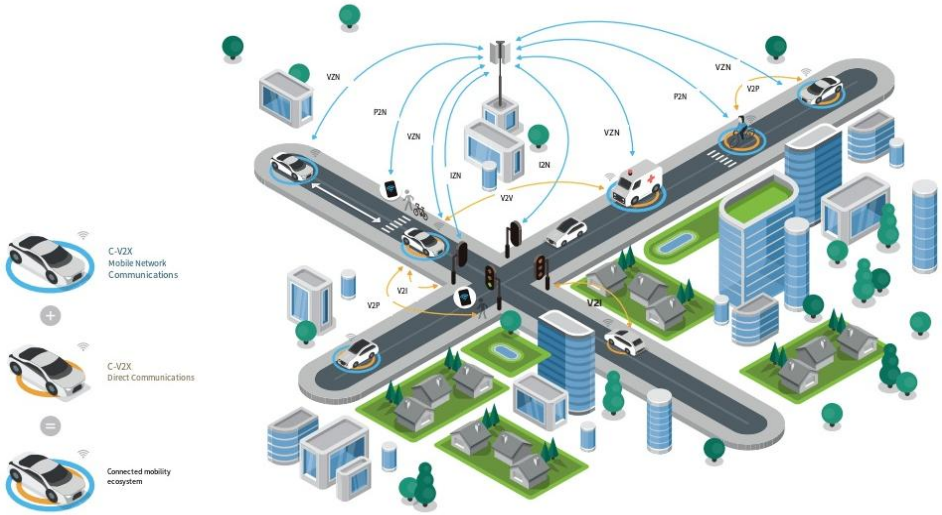

Figure 1. Intelligent transportation systems for future cities

Automotive cybersecurity scenarios refer to application scenarios that rely on multi-layer defense architectures and encryption technologies to protect the internal electronic systems, data transmission links, and control modules of vehicles from illegal intrusions and attacks, ensuring the safety of core driving functions.

A V2X security scenario refers to an application scenario that, based on trusted communication protocols and data verification mechanisms, enables cross-agent secure data interaction between vehicles and between vehicles and roadside devices to prevent false information interference.

(2) Security requirements and trends

The requirements for automotive connected security are specified in multiple national standards. GB 44495-2024 "Technical Requirements for Information Security of Complete Vehicles" requires enterprises to identify key risks, implement effective control measures, and ensure that the system has the ability to resist attacks and obtain evidence. It specifies that vehicle internal and external communications must incorporate encryption, tamper-proofing, and anti-replay capabilities during data transmission. GB 44496-2024 "General Technical Requirements for Automotive Software Upgrade" stipulates the management system requirements for automotive software upgrade, as well as technical requirements and test methods for vehicle software upgrade functions such as user notification, version number reading, security protection, preconditions, battery power guarantee, and failure handling [4-5].

To achieve mutual identity authentication between communicating parties in V2X security, the national standard system has established a multi-level architecture covering communication protocols, equipment requirements, security specifications, and test methods. GB/T 45315-2025 "Technical Requirements and Test Methods for Vehicle-mounted Information Interaction Systems Based on LTE-V2X Direct Communication" specifies vehicle-grade environmental adaptability, communication performance and test methods for vehicle-mounted terminals (OBUs). Key communication performance indicators, including transmission power, reception sensitivity, and antenna gain, must meet specified thresholds. The standard also mandates support for multi-channel bandwidth configuration and GNSS positioning, with a positioning accuracy of ≤5 meters in an open environment. GB/T 33577-2020 "Information Security Technology - Cybersecurity Guidelines for Automotive Electronic Systems" requires V2X systems to implement identity authentication, data encryption and intrusion detection to prevent man-in-the-middle attacks and data tampering.

3. SUMMARY

Entering the new era of intelligent development, digital application scenarios continue to expand, and the coverage and protection boundaries of digital security are constantly broadening, and various new types of cyber risks and data security risks keep emerging. Traditional security protection technologies and control models are difficult to adapt to the new development situation, forcing the digital security protection system to accelerate iteration and upgrade. In the face of increasingly complex cyber security situations and diverse digital application demands, the future digital security industry will witness comprehensive technological innovation and gradually advance into cutting-edge fields such as quantum-secure encryption, vehicle-cloud collaborative all-domain protection and intelligent self-learning active defense. Build an active, intelligent and integrated security defense architecture based on cutting-edge technology, continuously consolidate the security foundation of the digital industry, comprehensively enhance risk identification, early warning analysis and emergency response capabilities, and build a solid security barrier for the steady development of the digital economy.

REFERENCES

[1] Wang, Y. (2026). New trends in automotive intelligence: From single-point breakthrough to system victory. Automotive Horizons, (5), 3.

[2] Lu, J. (2026). Development path and prospect of intelligent technology for new energy vehicles. Automotive Knowledge, 26(5), 19–21.

[3] Feng, Y., Bao, J. N., Zhou, Y. Z., et al. (2025). Application status and trends of AI technology in the development of passive safety performance for intelligent vehicles. Intelligent Manufacturing, (6), 14–20.

[4] Cheng, Y. (2025). AI adversarial offense and defense in intelligent vehicle cybersecurity. Auto Pictorial, (12), 56–58.

[5] Tang, C. J., & Liu, C. (2025). Threats and protection of intelligent vehicle cybersecurity. Auto Art, (12), 44–46.