2020-01-0085 Published 14 Apr 2020

Safety Development Trend of the Intelligent and Connected Vehicle

Fuquan Zhao, Hong Tan, and Zongwei Liu Tsinghua University

Citation: Zhao, F., Tan, H. and Liu, Z., "Safety Development Trend of the Intelligent and Connected Vehicle," SAE Technical Paper 2020-01-0085, 2020, doi:10.4271/2020-01-0085.

Abstract

Automotive safety is always the focus of consumers, the selling point of products, the focus of technology. In order to achieve automatic driving, interconnection with the outside world, human-automatic system interaction, the security connotation of intelligent and connected vehicles (ICV) changes: information security is the basis of its security. Functional safety ensures that the system is operating properly. Behavioral safety guarantees a secure interaction between people and vehicles. Passive security should not be weakened, but should be strengthened based on new constraints.

In terms of information safety, the threshold for attacking cloud, pipe, and vehicle information should be raised to ensure that ICV system does not fail due to malicious attacks. The cloud is divided into three cloud platforms according to functions: ICVs private cloud, TSP cloud, public cloud. The transmission side classifies three APNs based on usage: enterprise-owned APN, public network APN, and public network customized APN. The vehicle end ensures information security through the vehicle firewall, border firewall, PKI password system, key management, and security chip.

In terms of functional safety, ICV function security needs to systematically consider factors such as vehicle, system and architecture. ISO 26262 design flow, AUTOSAR software architecture and perceptual information fusion are fully discussed in this section.

In terms of behavioral safety, the driving mode change of the Level 3 ICV changes the driver's responsibility. Identify driving patterns to ensure that the driver can take over and clearly communicate driver responsibility as a prerequisite for safety. In the design and evaluation, it is necessary to consider the vehicle dimension, transition dimension and driver dimension to systematically guarantee vehicle behavior safety.

In terms of passive safety, ICVs significantly reduce accidents. This can reduce some of the passive security configuration, but the reduction means integration rather than cancellation. New interior layout and constraints require the integration of passive safety and travel cabin. Active and safe sensors make passive safety intelligent. Passive safety is transformed into a combination of hardware and software

In response to changes in the connotation of automotive safety of the ICV, a new research and development concept for enterprises covering six parts was proposed. A new research development architecture for enterprises covering four parts at the same time was proposed.

Introduction

The road traffic safety situation around the world is serious. Over 3,700 people die on the world's roads every day and tens of millions of people are injured or disabled every year. Annually about 63,000 people are killed and 226,000 people are injured in road traffic accidents in China [1]. And the number of annual road traffic deaths on the world's roads has reached 1.35 million [2]. Traffic accident casualties can cause hundreds of millions of economic losses. Blincoe presented the results of an analysis of motor vehicle crash costs in the United States in the year 2000 that the total economic cost of motor vehicle crashes in 2000 was $230.6 billion [3].

Many studies have shown that intelligent and connected vehicles(ICVs) can avoid lots of road accidents. ICVs will save 13,099 lives and reduce 34,848 injuries in China in 2030[4,5]. Because of the huge socioeconomic impacts of ICVs, many enterprises are devoting themselves to relevant businesses [6].

The interconnection between the vehicle and the outside world is connected, which is mainly reflected in the data of the inside and outside of the vehicle through the end, the tube and the cloud [7]. It realizes cloud-end integration of integrated computing and services. However, once the vehicle is connected to various service facilities in the external environment, there is a series of security risks. From the physical contact the vehicle's controlled area network (CAN) bus to Bluetooth and Wifi without physical connection, it is a possible attack portal for attackers to control the steering, acceleration, braking and the engine of the vehicle [8, 9, 10]. Two white-hat hackers broke into Chrysler's vehicle networking system 'Uconnect' and sent commands to the system to start various functions of the vehicle remotely[11]. Li illustrated how to

launch successful attacks through the controlled area network (CAN) bus, electronic control units (ECUs), and in-vehicle infotainment system[12]. There is a possibility of malicious attacks on the Internet of Vehicles that provide business model innovation and travel services. Information safety is the foundation of vehicle safety for intelligent and connected vehicles.

Intelligentization is mainly reflected in two aspects of automatic driving and human-computer interaction[7]. In terms of automatic driving, there is no doubt that computers are fast, consistent and precise. They will be programmed to avoid risky driving and will not be impaired by alcohol, fatigue, and other stressors. However, it is foolhardy to assume that their decisions would be flawless [13]. Google driverless car caused an accident due to a mistake in the automatic driving decision system [14]. Tesla acknowledged that the algorithm to detect obstacles and apply automatic braking is still imperfect [15]. And software can contain as many as 20-30 defects for every 1000 lines of code[16]. The function of the intelligent and connected vehicles do not necessarily work as expected. functional safety is an important part of vehicle safety for intelligent and connected vehicles.

In terms of human-computer interaction, current human-computer systems are rapidly evolving. Many design decisions have not yet been made [17]. For the first time in history, the automation system will become the controlling body of the vehicle, and the driver may become a "bystander" of vehicle control. When the automatic driving system is running, the driver needs to trust the system. Ekman proposed a design example for human-computer interface (HMI) to promote driver trust in automated driving systems [18]. Liu has established an objective method to assess driver's steering comfort, including posture comfort and operational comfort [19]. Behavioral safety is a secure interaction between the intelligent and connected vehicle driver and the driving system.

Many studies have confirmed that active safety can significantly reduce accidents, even zero collisions [4]. But zero collisions and zero casualties are completely different. There may be casualties due to passenger restraint problems in the car, even if there is no vehicle collision. Therefore, in order to achieve a good vision of zero casualties, it is necessary not only to vigorously develop active safety functions, but also to invest passive safety as the last "defense line". On the other hand, with the in-depth development of intelligent active security technology, new demands are placed on passive safety technology. For example, when the passive safety is active, the passenger's posture, location, and attention to driving are very different from those of traditional vehicles. Undoubtedly, the development of intelligent and connected vehicles brings opportunities for technological upgrading and innovation to passive safety.

In general, information safety, functional safety, behavioral safety, and passive security need to be considered when designing and evaluating vehicle safety for intelligent and connected vehicles. This is a complete assessment framework.

This paper is organized as follows. The next section describes the importance of vehicle safety. Following that, methods are introduced to ensure information safety, functional safety, behavioral safety, and passive safety of intelligent and connected vehicles. The final section provides the countermeasures for enterprise to research and development the vehicle safety.

The Importance of Vehicle Safety in China

Safety is always the focus of consumers. In China, the first factor of concern for consumers to buy a car is safety. Consumers are highly sensitive to the safety technology and safety brands. On the surface, the Chinese consumers do not seem to believe in advertising about the safety of an automotive product. In fact, they are greatly affected by the advanced advertisement and are willing to pay for the vehicle safety. The core reason is that the Chinese consumer mixes the safety and quality of the automotive product. They believe that car quality is good if the safety is good enough. Meanwhile, Chinese consumers have low tolerance for small brands. Their satisfaction for low-level safety vehicle model has declined year by year and satisfaction for high-level safety vehicle model has increased significantly. All functions could be remove except safety function when designing a vehicle for consumers. In addition to consumers, the Chinese government is particularly concerned with the safety factors such as battery safety, data safety and so on because of the public safety and social stability.

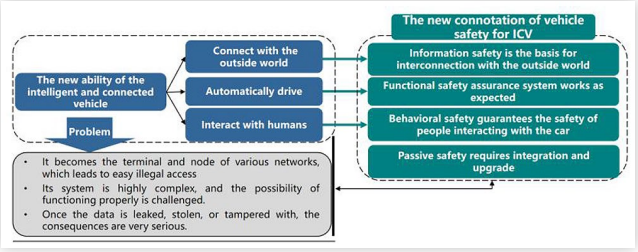
The technical research and development of Chinese vehicle manufacturer are determined by focus of consumes. The focus of Chinese vehicle manufacturer on vehicle safety is generally passive safety because Chinese consumers are more sensitive to passive safety than active safety. A part of Chinese vehicle manufacturers pay more attention to vehicle safety technology only to the results of C-NCAP. For reasons of cost, safety technology is also marketed as a vehicle configuration. In general, Chinese Vehicle manufacturers' awareness of safety technology has not risen to the level of system technology, and has not raised the development of safety technology to the height of improving vehicle performance (such as improving handling, etc.). Vehicle manufacturers have insufficient reserves for future safety technologies, such as battery safety for new energy vehicles, software security for intelligent networked vehicles, and data security. China's automobile brands and parts companies have made great progress, and whether they can occupy the commanding heights in the future depends largely on how safe they are, because safety is the biggest core of the brand.

Safety is always the focus of technology. Vehicle safety is actually a kind of tactic. The strategy is embodied in tactics and the tactics serve the strategy. The electrical vehicle and the intelligent and connected vehicle are China's national strategic development direction. For the government and public society, the most important things need to be considered first is how to avoid the explosion of the battery of the electrical vehicle and how to design the complex safety system for the intelligent and connected vehicle. Therefore, Safety is not only a strategic support, but also a direction of strategic decision-making. Enterprises should fully recognize the importance of the vehicle safety.

The New Connotation of Intelligent and Connected Vehicle

Electricization, connecting and intelligence enable the vehicle to generate a large amount of data on vehicle sates and road environment. The intelligent vehicle uses the laser radar, millimeter wave radar, camera, V2X to collect the internal and external information for logical judgment of the data, to provide warning information to the driver before the collision occurs or the system automatically takes measures. ICVs have the ability to automatically drive, connect with the outside world, and interact with humans. The ICV system is open and becomes the terminal and node of various networks, which leads to easy illegal access. Its system is highly complex, and the possibility of functioning properly is challenged. Once the data is leaked, stolen, or tampered with, the consequences are very serious. In general, the data-driven ICV is not a stand-alone system, and ensuring the safety of ICVs will be a huge challenge. Information safety is the foundation of its safety, ensuring that car-side, pipe-side, cloud for computing and storage of information is secure. The focus of information safety is cloud/pipe/end system design, vehicle data security design, and data transmission security design. Functional safety ensures the normal operation of the active safety functions of the system as expected, sensing, making decisions and executing as expected. Functional safety focuses on redundant sensing system design, vehicle/software/hardware full-area management design, and hardware and software layered design. Behavioral safety guarantees a safe interaction between people and vehicles, ensuring that the driver can take over when the system expects the driver to take over. The focus of attention is on driver status recognition, driving pattern recognition, and driver task communication. In addition, passive safety is the last line of defense for vehicle safety. ICVs will bring new opportunities and challenges to the development of passive security. The focus of passive safety is the upgrade of existing traditional passive safety, integration with intelligent travel cockpit, and integration with active safety. In general, the ICV needs to consider four categories of safety including functional safety, information safety, behavioral safety, and passive safety in order to ensure a high level of safety, as shown in Fig 1.

FIGURE 1 The new connotation of the vehicle safety for the ICV



Information Safety

In terms of information safety, cloud operation centers, pipe-end mobile communication, and vehicle-end key equipment are important concerns for information safety of ICVs. Hackers may attack sensor vulnerabilities through external environments, may attack the car network through physical contact interfaces, short-range communications, and may also attack mobile communications between the car and the cloud. Therefore, it is necessary to raise the threshold for information attacks in the cloud, pipe end, and car end. This will ensure that the ICV system will not be invalidated by malicious attacks.

The ICV information safety needs to consider the cloud, pipe-end, and vehicle-end for systematic information safety design. The cloud platform of ICV is divided into three cloud platforms according to functions: ICV private cloud is used to ensure application security; telematics service provider cloud is used to ensure host security; public cloud is used to ensure physical security. The three cloud platforms are responsible for authentication and rights management, secure transfer storage, access control and security auditing. They are an important part of cloud security. The pipe end is divided into three kinds of access point names (APN) based on the purpose: the enterprise self-use APN is a dedicated line to the back of the car factory, providing functions such as remote control and status detection. The public network APN connects to the Internet from the carrier side and supports Internet infotainment applications. The public network customized APN is only used directly for the new energy national standard platform. Three APNs perform real-time monitoring and operation management on the pipe end. The vehicle end ensures information security through four means: vehicle firewall, border firewall, key management, and safety chip. The vehicle firewall is used to ensure the safety of the vehicle network and the security of data communication. The border firewall is used to ensure data isolation inside and outside the car. Key management is used to prevent network packets from being tampered with. The safety chip guarantees the security of the vehicle end information from the hardware side.

Before the program is written, the system needs to sign and authenticate it. Then, the data plaintext is converted into ciphertext by an encryption algorithm for storage. In the program use phase, it is first necessary to check the program signature based on the security chip before decrypting it. Signature authentication is used to avoid forgery, and keys are used to avoid stealing, both of which are essential components of data security. In addition, special security chips and secure encryption algorithms need to be considered during design.

The public key infrastructure (PKI) cryptosystem is used to build a multi-layer defense system with security defense combined with hardware and software. The certificate center supports the issuance of identity certificates to external devices such as vehicle controllers, backgrounds, and diagnostic devices. The Over-the-Air (OTA) consists of a firmware version management platform, a FOT server, a vehicle terminal, and a key server. The key server plays the role of key generation, user authentication, and key management. During the OTA file transfer process,

the firmware version management platform responsible for version compilation and version release needs to obtain the key from the key server KMS and encrypt and sign the upgrade file. Then upload the encrypted upgrade file to the FOT server. The FOT server is responsible for the release of the version, the configuration of the update and the push of the upgrade package. After the vehicle terminal downloads the file from the FOT server, it needs to obtain the key and signature from the key server KMS. The upgrade file is detected, verified, and decrypted based on the obtained key and signature. The key server plays the key generation of the network transmission file, and the role of the vehicle terminal through the user authentication key authorization is an indispensable part of the data network transmission.

Functional Safety

In terms of functional safety, intelligent and connected vehicles need to systematically consider the factors such as vehicle integration and calibration, the ICV system and system architecture from top to bottom, as shown in Fig 2. At the system architecture level, the safety of the communication architecture and control architecture needs to be considered. At the vehicle integration and calibration level, it is necessary to consider not only the hardware integration of the vehicle, but also the integration of the intelligent control system. The system architecture and vehicle integration and calibration are all designed to support the safety of the intelligent and connected system. At the intelligent and connected system level, sensing, decision making and execution need to be considered. The functional safety of sensing needs to consider the environment sensing layer, data acquisition layer and information fusion layer. The environment sensing layer includes laser radar, millimeter wave radar, camera, map, roadside unit, etc. The information fusion layer is used to realize the complex information required for pedestrian, obstacle and vehicle identification, scene reconstruction, and precise positioning.

The information sensed by the ICV sensor needs to be fused to cover the entire scene. Various types of sensors may fail. The radar may not work on the metal bridge. Ultrasonic radar cannot detect children wearing sweaters. The camera cannot recognize targets in some situations, such as large roundabouts without lane lines. On the other hand, ICVs require a complementary set of sensor technologies to perceive enough distance information. The distance of the ultrasonic radar is 4 meters, the perceived distance of the optical camera is 80 meters, and the sensing distance of the laser radar is 200 meters. For the transmission of perceptual information over 200 meters, V2X technology needs to be developed. Therefore, ICVs require a complementary set of sensor technologies and the ability to fuse multiple sensor-aware information.

In order to ensure functional safety, it is required to carry out layer-by-layer security design from the vehicle level to the system level to the software level based on ISO 26262. In this way, the risk of functional failure can be systematically avoided. At the vehicle-level safety design, hazard and risk analysis is required to confirm safety target standards. The core purpose of this layer is to confirm the safety requirements of the vehicle. In the system-level safety design, the requirements for vehicle safety are assigned to the requirements of each subsystem. The core purpose is to allocate requirements to subsystems. In the hardware and software level security design, the technical security requirements should be derived based on the safety requirement. The core purpose of this layer is to validate hardware and software security design specifications.

In order to ensure functional safety, the architecture is designed after describing the security requirements from the system. The security requirements are thus assigned to software components for encoding and integration. In the end, verification at all levels is needed, as shown in Fig 3. During the design phase, platform security requirements need to be described to identify new security requirements. The architecture is designed based on security requirements. Further, the architectural security requirements are assigned to the application software. There must be no interference between different software components. The software component code is integrated. Then the ECU code is completed. After completing the above design phase, it entered the testing phase. The developer tests the software components and then integrates all the modules. Checking the integration is essential. The next step is to test the software and ECU. After completing the above work, test and verify the whole system.

Behavioral Safety

The L2 is partially automated and is controlled most of the time by the driver and part of the time by the ADAS system. The main controller of L2 is the driver. L3 is conditionally automated and the main controller becomes the system. Most of the time is controlled by the system and part of the time is taken over by the driver. The driver only needs to accept the takeover request from the system under certain circumstances. In order to cope with this change, clear driver responsibility is the basis for ensuring safety. First of all, autonomous driving must ensure that the current driving mode can be identified unambiguously at any time. Only in this way can there be no

FIGURE 2 Factors that need to be considered in the functional safety

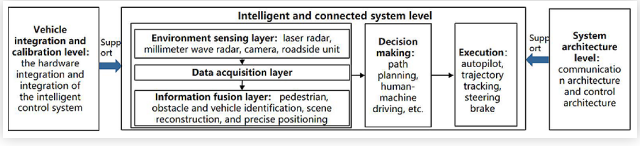


FIGURE 3 Functional safety design process

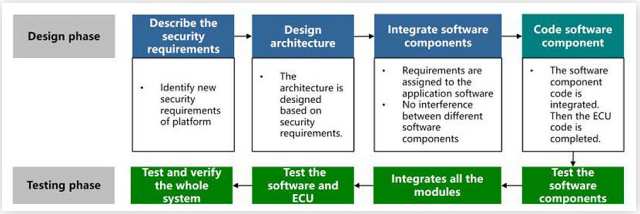
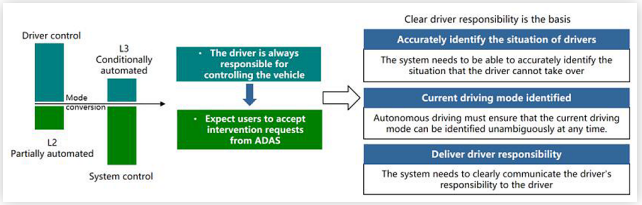


FIGURE 4 Change in driving mode changes driver responsibility



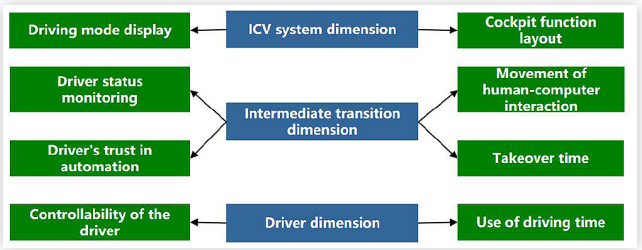
situation in which the driver and the system compete for control. Before the system makes a takeover request, the system needs to be able to accurately identify the situation that the driver cannot take over. If it is confirmed that the driver's status can take over the control of the vehicle, the system needs to clearly communicate the driver's responsibility to the driver, as shown in Fig 4.

In this interaction process, if the interaction pressure given to the driver by the system is too large, the driver will be fatigued and anxious. Similarly, if the interaction pressure is too small, it will make the driver feel bored. Proper interaction pressure allows the driver to be in the best state of excitement. Control is the transition from the system to the driver. Therefore, it is necessary to design and evaluate behavioral safety from three dimensions, including the ICV system dimension, the intermediate transition dimension, and the driver dimension, as shown in Fig 5. In the dimension of the system, the driving mode display and the cockpit function layout need to be considered. In the dimension of the intermediate transition, the driver status monitoring, the driver's trust in automation, the movement of human-computer interaction, and the takeover time should be considered. In the driver dimension, it is necessary to consider the controllability of the driver and driving time.

Passive Safety

Passive safety is not a "sunset industry." One thing that can be confirmed is that passive safety technology at present cannot meet the new demands of the future. ICVs and traditional cars have great differences in the time when passive safety works, passengers' posture, location, attention to driving, etc. Undoubtedly, the development of intelligence poses a great challenge to the passive safety constraint system, but it also brings opportunities for technology upgrade and innovation to passive safety. Passive safety is still the last line

FIGURE 5 Design and evaluate behavioral safety from three dimensions



of defense for ICVs. One thing to know is that zero collision and zero injury are two different things. Intelligent functions can greatly reduce collisions, but passengers in the car may be injured due to restraint problems even if there is no vehicle collision. The realization of the beautiful vision of zero casualties will be a small number of collisions in the future combined with the perfect passive safety, as shown in Fig 6.

The passive safety technology of ICVs has three main development directions, as shown in Fig 7. First, some passive safety configurations will be reduced. The rapid development of active safety technology has the greatest benefit of reducing a large number of casualties, so some passive safety configurations can be reduced. But the reduction does not mean cancellation, but further integration. Second, passive safety is integrated with active security. Due to the intelligence brought by various types of sensors, passive safety has the ability to judge and execute in advance. Pre-passive safety technologies represented by pre-tensioned seat belts and pre-airbags have been developed. Third, passive safety needs to be effectively integrated with the cabin because automatic driving changes the position and direction of the restraint. Travel cabin integration represented by wrapped airbags and individual restraint systems is the development direction. Currently, the occupant restraint system is a uniform standard installation location, which improves safety through installed airbags and safety belts. In the future, the higher-level self-driving cars will be on the road, and the cockpit like the "living room" will make the seat arrangement more flexible. In order to meet the passenger's demand for comfort and convenience, the seat space will be more spacious. But this flexibility and spaciousness make the passive safety solution more

FIGURE 6 ICV poses a great challenge and opportunities to the passive safety

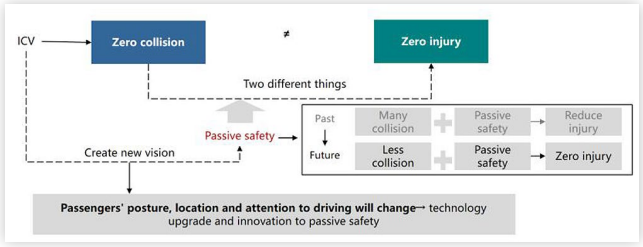
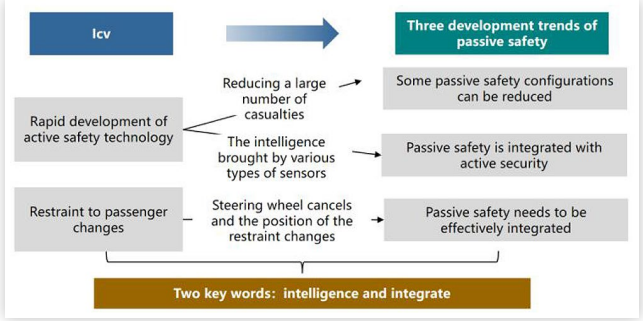


FIGURE 7 The passive safety technology has three development directions



complicated. A variety of seat positions and integrated safety systems need to be considered. Applicability to different body types and age occupants can be improved by independently controlling each airbag and adapting the size of the airbag. Personalization has become the key word for the development of passive safety constraint systems in the future.

The Research and Development of Vehicle Safety for the ICV

In the past, vehicle safety focused only on active and passive safety inside the vehicle. But in the future, the coordinated development of the human-vehicle-environment trinity is a long-term mechanism to deal with road traffic safety, as shown in Fig 8. In terms of the human, it is necessary to educate the public about how to take over, drive, and ride an intelligent and connected vehicle. In terms of the vehicle, companies are building safer vehicle by enhancing technological innovation capabilities. At the same time, through the active and passive safety integration to protect the personal safety inside and outside the vehicle. More importantly, the significance of the environment in traffic safety is self-evident due to the interconnection of all things. The vehicle provides real-time information to the environment based on its network connection capabilities. At the same time, the intelligent traffic environment provides environmental data information for the vehicle, which makes intelligent vehicles run on intelligent roads. In one words, the traffic safety will take into account the three factors of human, vehicle and environment in future.

In response to the development trend of vehicle safety for intelligent and connected vehicles, enterprises should consider research and development(R&D) concepts, R&D architecture and R&D methods, as shown in Fig 9. In terms of research and development concept, the new concept that enterprises should adopt when designing vehicle safety include 6 aspects: ①considering consumer acceptance; ②integration of active and passive safety; ③covering all people including different ages and genders inside or outside of the vehicle; ④covering the whole process of collision including collision avoidance, collision protection, and post-collision rescue; ⑤covering all possible conditions of traffic accidents; ⑥covering all elements including human, vehicle and environment. In terms of research and development architecture, four types of vehicle safety should be systematically considered including information safety, functional safety, behavioral safety and passive safety. In terms of development methods, the development of vehicle safety products for ICVs needs to form an open development platform and system based on market, regulations and third-party evaluation. In addition, it is necessary to continuously iterate based on the user experience. The perfect vehicle safety product development system is the forward development from user to user. After fully combining market information, national compulsory regulations and third-party evaluation, the vehicle safety requirements of ICVs in the actual traffic environment are confirmed. Then, the vehicle safety target is decomposed step by step to the system components. After the design is completed, a set of subjective and objective evaluation system associated with the user needs to be established for vehicle safety products. The next most important thing is to iterate based on the user experience. Thereby, an open research and development system from user to user is realized. An open R&D system will drive the adoption of key safety technologies. This system is the core system for the safe driving of ICVs in the future.

In the past, companies that wanted to occupy the market only needed to have core technologies and superior products for vehicle safety. But in the future, if enterprises want to truly seize the smart security business in China, they will not only need core technologies and superior products, but also need to use resource combination capabilities to continuously innovate business models. In general, companies need to focus on improving strategic decision making, resource mix, and coordination. For foreign-funded enterprises, it is recommended to start with a systematic strategic layout of intelligent security services. It is necessary to fully authorize local technology innovation and resource advantages. At the same time, let innovative technology and business be brought to the forefront with fast execution. Enterprises can firmly grasp the huge opportunities in China's auto safety market.

FIGURE 8 The human-vehicle-environment trinity of road safety

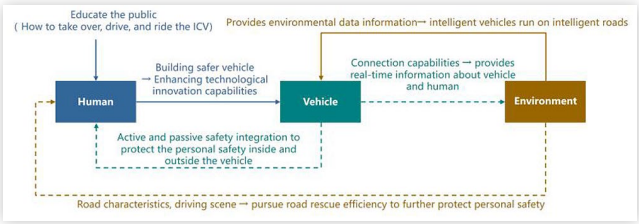
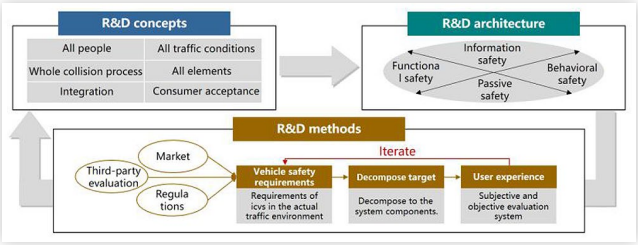


FIGURE 9 Research and development(R&D) concepts, R&D architecture and R&D methods of vehicle safety for intelligent and connected vehicles



References

1. Global Status Report on Road Safety 2018, Geneva: World Health Organization, 2018, Licence: CC BYNC-SA 3.0 IGO, available at https://www.who.int/violence_injury_prevention/road_safety_status/2018/en/, accessed 2018.

2. "The Ministry of Public Security of the People's Republic of China," Annual Report on Road Traffic Accidents of the People's Republic of China (2016), July 2017.
3. Blincoe, L.J., Seay, A.G., Zaloshnja, E. et al., "The Economic Impact of Motor Vehicle Crashes, 2000," United States, National Highway Traffic Safety Administration, 2002.
4. Kuang, X., Zhao, F.Q., Hao, H., and Liu, Z.W., "Assessing the Socioeconomic Impacts of Intelligent Connected Vehicles in China: A Cost-Benefit Analysis," *Sustainability* 11(12):3273, 2019.
5. Kuang, X., Zhao, F.Q., Hao, H., and Liu, Z.W., "Intelligent Vehicles' Effects on Chinese Traffic: A Simulation Study of Cooperative Adaptive Cruise Control and Intelligent Speed Adaption," in *Proceedings of the 21st IEEE International Conference on Intelligent Transportation Systems (ITSC) 2018*, Maui, HI, USA, November 4-7, 2018, 368-373.
6. Kuang, X., Zhao, F.Q., Hao, H., and Liu, Z.W., "Intelligent Connected Vehicles: The Industrial Practices and Impacts on Automotive Value-Chains in China," *Asia Pacific Business Review* 24(1):1-21, 2018.
7. Zhao, F.Q., Liu, Z.W., Hao, H., and Shi, T.Z., "Characteristics, Trends and Opportunities in Changing Automotive Industry," *Journal of Automotive Safety and Energy* 9(3), 2018.
8. Golde, N. et al., "Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications," NDSS, 2012.
9. Kleberger, P. et al., "Security Aspects of the In-Vehicle Network in the Connected Car," *Intell. Vehic. Symp. (IV)*, 2011.
10. Miller, C. and Valasek, C., "Adventures in Automotive Networks and Control Units," *DEF CON 21 Hacking Conf.*, 2013.
11. Miller, C. and Valasek, C., *Remote Exploitation of an Unaltered Passenger Vehicle* (Blackhat USA, 2015).
12. Li, X., Yu, Y., Sun, G. et al., "Connected Vehicles' Security from the Perspective of the In-Vehicle Network," *IEEE Network* 32(3):58-63, 2018.
13. Noy, I.Y., Shinar, D., and Horrey, W.J., "Automated Driving: Safety Blind Spots," *Safety science* 102:68-78, 2018.
14. Google, "Google Self-Driving Car Project Monthly Report - February, 2016," 2016, Online at https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-0216.pdf.
15. Yadron, D., Tynan, D.. "Tesla Driver Dies in First Fatal Crash While Using the Autopilot Mode," The Guardian, 2016, online at https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk.
16. Lonsdale Systems, "Software Quality Essentials," Online at http://lonsdalesystems.com/site/course/software_quality_essentials.php, 2016.
17. Tanelli, M., Toledo-Moreo, R., and Stanley, L.M., "Guest Editorial: Multifaceted Driver-Vehicle Systems: Toward more Effective Driving Simulations, Reliable Driver Modeling, and Increased Trust and Safety," *IEEE Transactions on Human-Machine Systems* 48(1):1-5, 2018.
18. Ekman, F., Johansson, M., and Sochor, J., "Creating Appropriate Trust in Automated Vehicle Systems: A Framework for HMI Design," *IEEE Transactions on Human-Machine Systems* 48(1), 2018.
19. Liu, Y., Liu, Q., Lv, C., Zheng, M., and Ji, X., "A Study on Objective Evaluation of Vehicle Steering Comfort Based on driver's Electromyogram and Movement Trajectory," *IEEE Transactions on Human-Machine Systems* 48(1), 2018.

Contact Information

Zongwei Liu
Lee Shau Kee Science & Technology Building
Tsinghua University, Beijing, China
liuzongwei@tsinghua.edu.cn

Acknowledgments

This research is supported by the National Natural Science Foundation of China (U1764265).

Definitions/Abbreviations

ICV - Intelligent and connected vehicle

R&D - Research and Development

APN - Access Point Name

ISSN 0148-7191