Chain vol. 1, no. 1, pp. 2–45, 2024
DOI: 10.23919/CHAIN.2024.000006
ISSN 2097-3470
CN 10-1915/TB
Perspective

CHAINS: CHAIN-based fusion safety system framework for intelligent connected vehicle

Shichun Yang[1,2], Bin Sun[1], Haoran Guang[1], Rui Wang[1], Bowen Zheng[1], Weifeng Gong[1], Yu Wang[1], Yi Shi[1], Zexiang Tong[1], Lisheng Zhang[1], Kaiyi Yang[1], Xinhua Liu[1,3], Yaoguang Cao[4,5,✉], Jun Li[6], and Yunpeng Wang[1]

[1] *School of Transportation Science and Engineering, Beihang University, Beijing 100091, China*
[2] *Innovation Center of New Energy Vehicle Digital Supervision Technology and Application for State Market Regulation, Beijing 100091, China*
[3] *Imperial College London Ringgold standard institution - Dyson School of Design Engineering, London SW7 2AZ, UK*
[4] *Research Institute for Frontier Science, Beihang University, Beijing 100091, China*
[5] *State Key Lab of Intelligent Transportation System, Beijing 100091, China*
[6] *School of Vehicle and Mobility, Tsinghua University, Beijing 100084, China*

Received: 26 December 2023
Revised: 6 January 2024
Accepted: 19 January 2024
Online: 15 February 2024

KEYWORDS

CHAIN,
fusion safety,
X-shaped development process,
safety brain

ABSTRACT

Intelligent connected vehicles, as the focus of the global automotive industry, are currently at a critical stage of large-scale commercialization. However, during the development process of vehicles from mechanical systems with limited functions to mobile intelligence with complex and multiple functions, the issues of functional safety, cybersecurity, and safety of the intended functionality are the main challenges of the industrialization of intelligent connected vehicles, including multiple safety risks such as hardware and software failures, insufficient performance in edge scenarios, cyber-attacks and data leakage. In this paper, the safety and security issues of intelligent connected vehicles, the challenges posed by emerging technology applications, and related solutions are systematically reviewed and summarized. A fusion safety system framework with the safety cube as the core of protection and control is proposed innovatively based on a field-vehicle-human safety interactional model, realizing stereoscopic, deep, and comprehensive safety protection through end-cloud collaboration. Meanwhile, an X-shaped fusion safety development process based on CHAIN is proposed. Through the empowerment of digital twin and AI technologies, it could approach interaction between physical entities and digital twin models and the automation of the development process, thereby satisfying the demands of fusion safety system design, intelligent development, rapid delivery, and continuous iteration. The fusion safety system framework and X-shaped development process proposed in this paper can provide important insight into intelligent transportation vehicles and systems' safety and security design and development.

Address correspondence to caoyaoguang@buaa.edu.cn

有科出版 YOUKE PUBLISHING
EXCLUSIVELY AVAILABLE VIA IEEE Xplore

1 Introduction

The era is witnessing an unprecedented disruptive transformation in the automotive industry, with autonomous driving and telematics technologies at the core of this revolutionary wave. Intelligent connected vehicles (ICVs) are next-generation vehicles that utilize advanced technologies involving chips, big data, and artificial intelligence, facilitating highly effective, safe, comfortable, and energy-efficient driving.

Leading vehicle-producing countries are accelerating the industrialization of ICVs, progressively providing licenses in regulations and policies [1]. Germany passed the *Act on Autonomous Driving* in 2021, which permits L3 vehicles to operate nationwide and permits L4 vehicles to function under specific conditions [2]. Automotive manufacturers are enabled to apply for relevant qualifications from the German government. *Occupant Protection Safety Standards for Vehicles Without Driving Controls*, adopted by the U. S. National High Way Traffic Safety Administration (NHTSA) in March 2022, provides a regulatory framework for deploying autonomous vehicles without steering wheels and pedals [3]. The European Union issued *Uniform Procedures and Technical Specifications for the Type-Approval of the Automated Driving System (ADS) of Fully Automated Vehicles* in August 2022, marking the world's first regulation to allow the registration and sale of vehicles of L4 and above [4]. In November 2023, China issued the *Guidelines for the Safety of Autonomous Vehicle Transportation Services (Trial)*, permitting L3 and L4 autonomous driving vehicles to engage in passenger and freight transportation in designated areas and delineating explicit accident liabilities [5]. Following nearly a decade of rapid development, ICVs are now at the dawn of large-scale commercial applications.

However, safety concerns represent the most significant challenge to the mass commercialization of ICVs. Driven by multidimensional cutting-edge technologies, automobiles have gradually evolved from mechanical systems with limited functions to mobile intelligence with composite functions. The highly complex intelligent driving cyber-physical systems face the risk of multiple software and hardware failures; the intelligent driving system in edge scenarios may suffer from insufficient design of intended functions; and multi-level network access may trigger malicious attacks on vehicles and privacy leakage problems. These raise the issues of functional safety, cybersecurity, and safety of the intended functionality (SOTIF) for ICVs. Furthermore, there is an interconnectedness and mutual influence among these three safety categories. The safety of vehicles is no longer confined to the traditional domains of passive and active safety. Under the complex and diverse new challenges, it is urgent to review and study the security of ICVs deeply and systematically. Meanwhile, the rapid development of new technologies such as artificial intelligence (AI) algorithms and large models and their application in the automotive field present a series of new challenges to the safety of ICVs.

With the rapid development and fusion of the internet, big data, and AI, the automobile is being promoted to transform from a vehicle to an intelligent terminal. Cyber hierarchy and interactional network (CHAIN) is proposed as one of the digital solutions to break through the efficient and cross-discipline control of ICVs [2, 3]. CHAIN is an open architecture that integrates and designs data, algorithms, and users to maximize the potential of data. CHAIN has a cloud-based multi-level structure and "physical entity-virtual model" mapping interactions to satisfy the demands of multi-scale and multi-dimensional modeling. The CHAIN architecture has excellent realism and real-time capability and is promising to provide more complete digital solutions and promote industrial upgrades and transformation of ICVs.

This paper comprehensively analyzes the three categories of safety issues and the emerging challenges faced by ICVs and discusses the existing methods and their limitations. In response to the difficulty of single safety methods in addressing multiple security challenges, this study innovatively proposes a novel intelligent connected vehicle safety protection framework, integrating the concept of fusion safety. This framework is based on the field-vehicle-human safety interaction model and edge-cloud collaboration, directing the future development of safety protection for ICVs. Additionally, this research introduces, for the first time, a CHAIN-based [6, 7] X-shaped fusion

safety development process. This process facilitates interaction between physical entities and their virtual twin models, effectively meeting the needs of ICVs in terms of safety design, intelligent development, rapid deployment, and continuous iteration. The fusion safety design methodology proposed in this paper provides valuable guidance for the safety design and development of ICVs.

The remainder of this paper is organized as follows. In Section 2, we discuss safety & security issues and challenges for ICV. Section 3 presents existing methods and techniques for safety & security. Section 4 discusses fusion safety for ICVs, including the concept, framework, and development process of Fusion Safety. Conclusions and perspectives are presented in Section 5.

2 Safety & security issues and challenges for ICVs

Safety, as a fundamental attribute of automobiles, has been accompanying the development process of automobiles over time. Before applying intelligence and connectivity technologies in vehicles, the focus was on passive and active safety. Nowadays, information technology has made rapid development and deep integration with the automobile industry, promoting the accelerated evolution of automobiles in the direction of intelligence and internet connectivity. Figure 1 presents the development of the vehicle electronics and safety. On the one hand, the basic attributes of the automobile have transformed from a mechanical system to a mechatronic system and to a cyber-physical system with the addition of internet connectivity and intelligence attributes. The control of vehicles has shifted from human drivers to human-machine co-piloting and is further evolving towards complete autonomous driving. Additionally, the boundary of vehicle control has expanded from individual vehicles to multiple vehicles and further integrated vehicle-road-cloud systems. On the other hand, there have been significant changes from hardware to software for the vehicle. In terms of hardware, the electrical and electronic architecture (E/E architecture) of vehicles changed from a distributed control architecture to a domain-centralized architecture and will further develop into a central computing architecture in the future. Automotive chips have also evolved from early 8-bit processors to 64-bit processors and then to the multi-core processors currently used in autonomous driving systems. In terms of software, automotive software architecture has changed from signal-driven architecture to service-oriented and has experienced the development of Non-AUTOSAR to Classic AUTOSAR and then to Adaptive AUTOSAR. Accompanied by the gradual increase in software complexity, the automated driving software architecture has also evolved from a modularized solution to the current end-to-end solution. AI technology has been widely applied in the autonomous driving system.

Over the past decade, automobiles have rapidly undergone the developments above, with the pace and scale of evolution surpassing the previous 100 years of automotive history. Accompanying this rapid development are a series of safety & security challenges, including issues of functional safety, SOTIF, and cybersecurity. To clarify, "safety" in this paper refers to the prevention or mitigation of hazards arising from accidents, including SOTIF or functional failures, while "security" denotes the protection against malicious attacks that may originate from hackers or similar threats. As vehicles evolve from single-function mechanical systems to intelligent carriers with multiple attributes, their safety implications become increasingly rich, facing more complex and diverse safety challenges. this paper focuses on elaborating new issues encountered in functional safety, cybersecurity, and safety of intended function faced by ICVs. Traditional safety issues are not extensively discussed in this paper.

2.1 Functional safety

With the development of automotive electronics technology and increasing functionality, the complexity and number of electronic control units (ECUs) on the vehicle are increasing, resulting in a significant increase in the probability of systematic failures and random hardware failures in electronic control systems [8]. At the same time, the new intelligent functions often require coupling and linkage of multiple controllers to achieve. Therefore, if a controller fails, the consequences will not only affect the realization of the module's

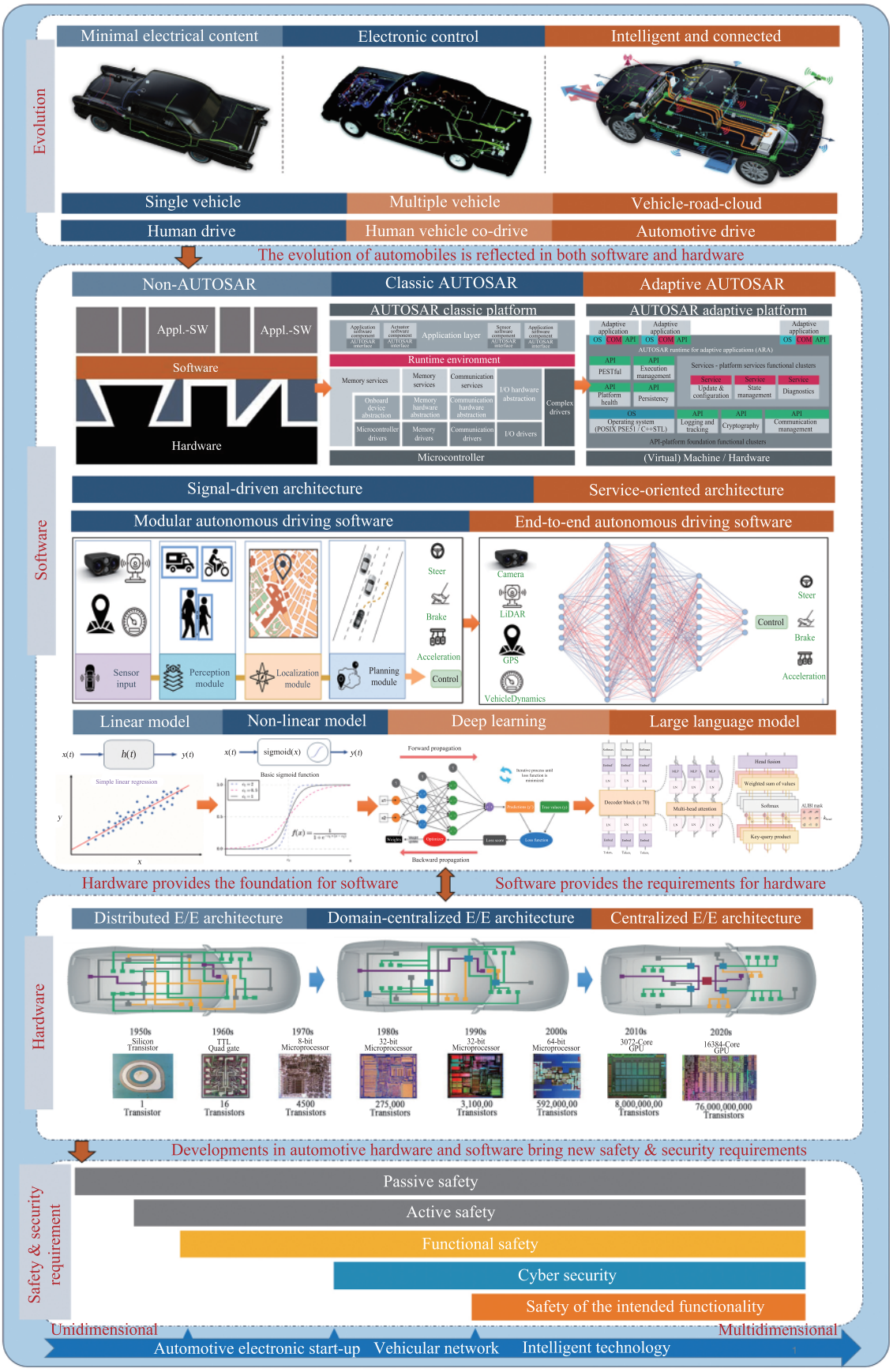

Figure 1 The development of vehicle electronics and safety.

function but also further extend to the whole system and even affect the driver's life.

Functional safety has emerged to address the safety issues caused by such hardware and software failures. Functional safety refers to the absence of unreasonable risk due to hazards caused by the malfunctioning behavior of Electrical/Electronic (E/E) systems [9]. Functional safety in automobiles mainly addresses the risks caused by hardware and software failures in the vehicle's E/E systems. For example, the failure of the EHB's (Electric Hydraulic Brake) software may result in incorrect power delivery to the value and pump motor, reducing braking effectiveness and significantly increasing the risk of an accident.

To cope with the above failures that may occur in automobiles and to standardize the design and development process of functional safety for ICVs, a functional safety standard for electrical and electronic systems that meets the requirements of the automotive industry was compiled by the Technical Committee on Road Vehicles (ISO/TC22) based on IEC 61508 in 2011, named ISO 26262 [10]. The ISO 26262 series defines the Automotive Safety Integrity Level (ASIL) based on the Safety Integrity Level (SIL) from IEC 61508, which contains five levels from QM to D. ASIL is composed of three parameters together: severity (S), exposure (E), and controllability (C), which improves operability for vehicle engineers. To address the need for functional safety development and analysis of high-computing power, complex controllers, and autonomous driving algorithms, the ISO organization released a revised version in 2018. The new standard forms a separate requirement for functional safety development for semiconductors. At the same time, requirements and descriptions for a Fail-Operational System (FOS) have been added to the Fail-Safe System, which is crucial for the development of functional safety for autonomous driving systems.

In recent years, with the changes in vehicle E/E architecture, as well as the further development of intelligence and network connectivity, the functional safety design analysis and development process based on ISO 26262 has encountered some new challenges.

The new generation of E/E architecture means new system and controller architectures. After the Distributed E/E architecture, automotive E/E architectures are moving towards Domain-Centralized E/E architecture and Domain Fusion E/E architecture. The evolution is driven by the continuous improvement in the integration level of controllers, particularly in the field of autonomous driving [11]. A typical autonomous driving domain controller will contain multiple heterogeneous compute units such as CPUs, DSPs, APUs (BPUs), etc., and can run multiple operating systems and perform multiple complex tasks simultaneously. This makes the verification and monitoring of functional safety more complicated, having the trend of multi-dimensional and multi-level and putting forward higher requirements for functional safety development and design.

Vehicle-road-cloud collaboration allows devices outside the vehicle to participate in the control link. The new generation of vehicle E/E architecture introduces cloud computing and V2X, which means the vehicle can connect and communicate with the road infrastructure and other traffic participants, including pedestrians. In this working environment, many out-of-vehicle devices or nodes will be deeply involved in the vehicle's perception, decision-making, control, and other automated driving tasks, providing more comprehensive information for the vehicle or undertaking part of the computation and data processing. However, these devices and nodes are mainly developed and produced by third-party enterprises or organizations and are not directly linked to the vehicle's design process. Therefore, this collaborative approach introduces new functional safety risks to the vehicle. The scope of functional safety analysis of this type of question has gone beyond the boundaries of traditional vehicle functional systems [12]. To realize comprehensive and reliable functional safety in the environment of vehicle-road-cloud collaboration has aroused the attention of the industry, and there is an urgent need to develop new methods and technologies to address this new risk of functional safety.

The black-box nature of artificial intelligence (AI) algorithms creates new challenges for functional safety. Traditionally, functional safety has been designed primarily through hardware and software to ensure that automotive systems remain safe in the face of

abnormal conditions. However, with the rise of AI technology, more and more functions in automotive systems, especially autonomous driving perception and decision-making, rely on complex machine learning and deep learning models. Traditional functional safety analysis methods are difficult to apply directly to AI models. While functional safety analysis methods are usually based on well-defined rules and strict system architectures, AI models are characterized by autonomous learning and adaptability, and their internal decision-making processes are complex to explain [13, 14]. As a result, understanding the behavior of models for functional safety analysis becomes complex and challenging. Methods such as failure mode and effect analysis (FMEA) often struggle to manage models' interpretability, robustness, and ability to handle uncertainty effectively. This leads to a limited comprehensive understanding of the potential risks of the models and the limitations of traditional means in assessing the safety of AI models. Therefore, in the new generation of intelligent vehicle systems, functional safety analysis methods applicable to AI models must be innovatively developed to ensure that these models can operate safely and reliably in various complex scenarios, which is also a key challenge facing the automotive industry with the convergence of AI.

Over the past 20 years, functional safety has accompanied the development of automotive E/E systems along the way and made remarkable progress, providing a reliable framework and laying the cornerstone for the safe development of the industry. However, with the continuous development of technology and the increasing complexity of automotive systems, functional safety is facing new challenges. Therefore, further in-depth research is needed to adapt to the continuous evolution of emerging technologies and systems to ensure that automobiles will still be able to operate safely and reliably in the future.

2.2 Cybersecurity

Emerging communication and intelligence technologies have led to substantial progress in automobile electronic control systems. Consequently, the automobile has transcended its erstwhile status as a self-contained entity. It has evolved into a mobile terminal endowed with communicative capabilities and a discernible degree of autonomous decision-making functionality. The ICVs can connect and transmit information to other vehicles, roads, clouds, and people, make judgments, and execute decisions based on the information collected and transmitted. However, while this brings more convenience and better experience, it also introduces cybersecurity threats, such as cyber-attacks and theft of sensitive data. Therefore, besides functional safety, cybersecurity has become a necessary concern in the automotive field. Ensuring that the automotive network communication process is normal and that the data is in a state of effective protection and legitimate utilization is the goal of cybersecurity in ICVs. The following section will introduce cybersecurity issues, the development of standards and regulations, and some new challenges of ICVs.

The cybersecurity threats faced by ICVs mainly originate from the automobile's internal and external communication networks. The cybersecurity problems of internal automobile communication are mainly in the following aspects. First, the in-vehicle network is used for information interaction between ECUs, domain controllers, and in-vehicle gateways inside the vehicle [15, 16]. Sensing, decision-making, and control data rely on the in-vehicle network for transmission. A cybersecurity attack on the in-vehicle network will seriously affect the vehicle's function. Attackers can directly or indirectly access the in-vehicle network through the diagnostic interface, USB, Bluetooth, Wi-Fi, and other interfaces. As a typical in-vehicle network protocol, the CAN bus lacks a security protection mechanism, and the open channel has the potential risk of malicious eavesdropping and illegal message injection. Back in 2013, Charlie Miller and Chris Valasek hacked the Toyota Prius through OBD [17]. In addition, many researchers have attacked vehicle infotainment systems by accessing malicious devices to interfere with the driver's decisions [18]. Nowadays, with the development of smart cockpits, a large number of assistive functions of the vehicle are integrated into it and controlled through smart vehicle computers. The latest upstream report shows increased automotive cybersecurity attacks triggered by third-party apps [19]. External automotive communications include vehicle-

to-vehicle, vehicle-to-infrastructure, vehicle-to-cloud, vehicle-to-user device, and vehicle-to-satellite communications. Many of these communication processes have cybersecurity risks. Attackers may be able to disrupt the movement of a vehicle and cause traffic congestion by jamming, eavesdropping, tampering, or falsifying information in the communication channel. For example, in 2015, two well-known hackers, Charlie Miller and Chris Valasek, successfully compromised a Jeep Liberty through a remote attack, sending unauthorized messages to interfere with its steering and braking functions, controlling the vehicle to deviate from the direction of travel, and ultimately run into an incline, resulting in an emergency for 1.4 million related Chrysler Corporation models recall [20]. Albouq and Redericks impersonated vehicle nodes and pretended to have the best routes between source and target nodes, deceiving other nodes in the network and realizing the black hole attack [21]. In addition, an attacker can affect the vehicle navigation through GPS spoofing attacks [22], causing the vehicle to deviate. In summary, the attackers may hack into a vehicle through its internal and external interfaces to gain access to information on the vehicle and interfere with its functionality.

As part of cybersecurity, data security cannot be overlooked. The software and hardware critical information of the vehicle itself, the personal privacy of drivers and passengers, and the sensitive data in the external environment of the vehicle may all become the target of attackers. The software and hardware information of the vehicle encompasses inherent attributes such as the VIN code, as well as data collected and processed by sensors during operation, including vehicle speed, acceleration, and other pertinent parameters. The development of intelligent cockpits has led to the collection of more frequent and varied data about the personal privacy of drivers and passengers, such as faces, voices, and driving habits. Sensitive data of the vehicle's external environment include license plates and faces of traffic participants that are collected when sensed by autonomous driving technologies. There is not only data directly associated with the subject but, more importantly, sensitive content that is mined from multiple data types and thus inferred. It is conservatively estimated that ICVs can generate 1–10 TB of data per day, with complex data types covering structured data sets, text, audio, video, trajectory, and images, etc., involving subjects such as drivers, other people in the cockpit, traffic participants, and the automobile manufacturer. In addition, automotive cloud platforms also have data security issues. Due to the substantial value of data encompassed within cloud platforms, these platforms may become targets for attackers aiming to acquire vehicle data and breach vehicular control systems illicitly. In 2018, Tesla was exposed to the hacking of its cloud server account, and a significant amount of sensitive data was leaked, including telemetry data, map information, and vehicle maintenance records [23]. In 2023, Toyota was exposed to several sensitive data leaks, including telemetry data, map information, and vehicle maintenance records, due to misconfigurations in its cloud environment [24]. The importance of data security is not only reflected at the individual level but also lies in its far-reaching impact on national security and social stability. However, the various data leakage and illegal utilization incidents that have emerged in recent years have significantly reduced the public's confidence in the data security of ICVs and seriously hindered the development of ICVs.

The issues above have prompted widespread attention, leading several countries and organizations to progressively formulate cybersecurity standards and regulations for ICVs over the past decade. These initiatives serve to standardize the design and management processes of cybersecurity. For example, the European Union initiated a standard for E-Safety Vehicle Intrusion Protected Applications (EVITA) in 2008 to standardize the design and management of cybersecurity throughout the life cycle of ICVs based on the four requirements of operability, safety, privacy, and finance. EVITA protects the network components in the security architecture according to four requirements. In addition, Europe has also proposed relevant standards such as PRESERVE and OVERSEE, etc. In 2016, SAE released the world's first vehicle cybersecurity standard, J3061, which refers to the V-model and proposes safeguarding automotive cybersecurity throughout the entire automotive lifecycle in terms of risk assessment and management, product development, operation/maintenance, and process auditing.

The U. S. SAE and the ISO began jointly developing the international standard *Road Vehicles – Cybersecurity Engineering* (ISO/SAE21434) in 2018. ISO/SAE21434 is the first international standard for constructing automotive cybersecurity, marking that a reliable cybersecurity guarantee mechanism has become an essential attribute of future automotive products. In January 2021, the first global mandatory cybersecurity standard for automobiles was adopted. In January 2021, the world's first mandatory automotive cybersecurity regulation, UNECE WP.29 R155, was released, which requires vehicles to pass both the cybersecurity Management System Certification (CSMS) and the Vehicle cybersecurity Type Approval (VTA). The former mainly requires OEMs to develop cybersecurity management processes during the complete life cycle of the vehicle, and the latter reviews the implementation of specific work in cybersecurity development to ensure that the vehicle's cybersecurity protection technology covers the entire life cycle of security. In terms of data security, the EU's *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications*, released in January 2020, categorizes personal data in telematics according to its sensitivity and proposes the principle of data minimization to ensure that vendors and data users only collect personal data that is relevant and necessary for processing, to ensure the security and confidentiality of the data. The above standards and regulations have ensured the cybersecurity of ICVs to a certain extent and improved the standardization of cybersecurity in the design and use of vehicles. Still, many new challenges have emerged by introducing more cutting-edge intelligent and connected technologies.

The advent of sophisticated and novel attacks poses challenges to the communication infrastructure of automotive networks. Some studies have shown that attackers with a high level of experience in automotive network communication protocols and understanding of vehicle functions may design more complex attacks and utilize artificial intelligence methods to generate more covert network attacks [25], significantly increasing the difficulty of attack detection. In addition, new types of vulnerabilities may be introduced by the gradually updated hardware and software systems of ICVs, and some new types of attacks based on unknown vulnerabilities may bypass the protection of rule-based firewalls or intrusion detection systems.

The development of foundation models also brings new challenges to automotive cybersecurity. Firstly, foundation models with deep feature mining capability and reasoning ability can mine deep and sensitive information from the massive amount of data related to ICVs. As a result, even data that has been desensitized may be exploited by foundation models to portray user profiles or predict human or vehicle behaviors [26]. This poses new challenges for the data security and privacy protection of ICVs. Second, the existing encryption during internal and external communication of ICVs usually uses pseudo-random passwords, which may be violently broken by foundation models supported by large-scale data and significant computational resources. It will lead to severe problems in access and authentication, and static protection systems will face the risk of failure.

With the advancement of low earth orbit (LEO) satellites such as Starlink and XingYun, vehicular satellite Internet has become a potential communication method for automobiles. However, some satellite internet communications use brand-new network protocols, and their communication behavior and content are difficult to monitor. This results in the vehicle-sensitive data being able to be transmitted to any designated place via satellite Internet. At the same time, attackers can gain control of the autonomous driving system and manipulate the vehicle driving behavior via satellite Internet. This also poses new challenges to traditional cybersecurity.

To sum up, ICVs still face serious cybersecurity threats. Many research institutions, enterprises, and government agencies actively promote the construction of automotive cybersecurity systems. Compared to cybersecurity issues in the IT domain, the cybersecurity landscape of ICVs exhibits significant disparities across threat origins, attack repercussions, security design constraints, standards, and regulations. With the continuous integration of new technologies in ICVs, emerging issues in novel cybersecurity pose ongoing challenges. Traditional techniques and methods in cybersecurity may prove insufficient to meet the evolving security

requirements introduced by these advancements. Therefore, it remains imperative to place continued emphasis on automotive cybersecurity.

2.3 SOTIF

Advanced intelligence systems, such as automated advanced driver assistance systems or self-driving systems in vehicles, may still face situations where they do not work correctly in the intended manner when there is no functional failure in the system, which can lead to potential dangers [27]. In March 2018, Uber's self-driving car accidentally struck and killed a pedestrian in the United States. The pedestrian was crossing a section of road that was not directly illuminated by streetlights, and the sensing system, in the absence of a malfunction, interpreted the pedestrian information captured as unknown objects, vehicles, and bicycles in the first six seconds of the collision [28]. In March 2020, Volvo announced a worldwide recall of nearly 740,000 vehicles involving nine models on sale due to the Autonomous Emergency Braking System (AEB) not effectively recognizing objects in some scenarios, resulting in the AEB not functioning correctly in the intended operating scenario [29]. In June 2020, a Tesla Model 3 in autopilot mode crashed directly into an overturned truck, mistakenly identifying the truck as a white cloud.

To address such issues, the concept of SOTIF was proposed, and the International Organization for Standardization (ISO) was the first to publish ISO 21448：2019 in 2019 to standardize the development and design of SOTIF, followed by a revised version, ISO 21448：2022, in 2022. In contrast to its predecessor, the 2022 version extends its application to encompass all levels of automated driving, providing specific clarifications on the Hazard Model and introducing the Operation Phase of the system [30].

SOTIF issues arise due to system performance constraints that prevent the practical realization of the intended functionality or due to reasonably foreseeable human misuse [31]. The root causes of these problems are manifold, such as encountering unknown scenarios where the system is unable to perceive the environment accurately or where the functional modules or algorithms within the system may lack the necessary robustness, making it difficult to maintain stability under complex and changing operating conditions [32]. The hardware performance and algorithmic performance of the system directly affect the SOTIF. There are a series of problems and challenges for the SOTIF in edge scenarios, design operation domains, human-machine interaction, and testing and verification [33].

The unpredictability of edge scenarios poses problems and challenges. Real-world driving scenarios are an infinite collection of rare, extreme, or never-before-experienced edge scenarios. The unpredictability of these scenarios leads to the impossibility of exhausting all possibilities at the beginning of the system's design, and exhaustive testing and validation at the later stages of development becomes very challenging [34]. It isn't easy to exhaustively test and validate all possible scenarios, and the system still encounters edge scenarios that cannot be safely dealt with during operation. Edge scenarios expose the lack of system performance, which causes SOTIF problems. The sensing system of an autonomous driving system is limited under specific conditions, such as bad weather and insufficient light, leading to insufficient understanding of the surrounding environment around the system, directly affecting vehicle safety [35]. For the decision-making system, the system is unable to make safe and reasonable decisions promptly due to the complex and variable uncertainty of the upstream information caused by sensor errors, unusual road conditions, and sudden emergencies [36]. For the control system, it is impossible to ensure that the decision-making commands can be executed effectively and rapidly in different scenarios, and the lack of real-time and follow-ability of the control system in the face of unexpected situations may lead to vehicle destabilization.

Determining the Operational Domain of Design (ODD) poses problems and challenges. The ODD describes the applicable scenarios and operating conditions of an automated driving system, including a range of factors such as geographic location, weather conditions, traffic conditions, road types, etc., as well as a variety of complexities and uncertainties that the system is capable of handling [37]. Designing the operational domain is critical to the safe operation of the system. However, the boundaries of the ODD are

difficult to define clearly and precisely, which may result in the system unintentionally operating in conditions that are not appropriate, thus compromising safety. Another issue is the dynamic change of ODD; the design operational domain may change over time, such as the implementation of new traffic regulations, irreversible degradation of the system hardware due to time (hardware aging), and the update of urban planning. The system needs to adapt to the ODD's dynamic change and update and validate the ODD as it changes. Monitoring the design operational domain and determining whether the system is operating within the design operation domain directly affects the system's performance. Establishing an efficient real-time data acquisition and analysis system is essential. However, there is a lack of practical techniques and methods to quantitatively assess the deviation of the actual operating conditions from the design operation domain, and it is not possible to reasonably determine the relationship between the actual operating scenarios and the design operation domain.

The complexity of human-machine interaction poses problems and challenges. Human-vehicle cooperative driving conditional automatic driving will continue to exist for a period. The human-machine two sides need to reach a consistent understanding of the driving task in a particular scenario to carry out close, deep interaction and different people's habits and behavioral patterns lead to the human consciousness and behavior being difficult to predict [38]. In addition, even if the same driver faces the complexity of the working conditions due to the fluctuation of their brain load, such as attention distraction or comprehension of the scenario, it is straightforward to lead to misuse. In some emergency scenarios, personnel misuse will directly cause safety accidents. SOTIF Human misuse is also an essential concern for the SOTIF. With the increased system complexity, this problem is more prominent in human-machine interaction. The effectiveness of human-machine interaction is based on a person's full knowledge of the system. However, the complexity of system functionality often increases the difficulty of HCI design, making it challenging to ensure that the driver and passenger fully understand each system function. This complexity can also lead to incorrect expectations of the driver and passenger about the system and incorrect assumptions about how the system is designed to interact, which creates direct or indirect misuse of the intended functionality and increases the safety risk [39].

SOTIF encounters problems and challenges in testing and validation. One of them is insufficient scenario coverage. Testing needs to cover as many road and traffic conditions as possible in a limited time, especially safety-critical edge scenarios, so efficiently generating edge scenarios is a hot research topic in the testing field, i.e., how to design relatively rare or unique driving scenarios within a limited testing time [40] to ensure that the system can operate safely under various extreme conditions. To solve the problem of insufficient scenario coverage requires innovative approaches, including model-based scenario generation, data-driven scenario generation, and the application of digital twin technology, to cover the various challenges of the system more comprehensively. Secondly, the testing of human-machine interaction, different behavioral patterns, cultural differences, etc., are difficult to quantify in testing for simulation testing. Human-machine interaction testing requires considering the complex interactions between the driving system and the driver, including language differences, cultural differences, and behavioral habits. Accurately modeling and evaluating these factors in testing is essential to ensure that the system can operate safely in real-world road conditions. Meanwhile, the system's handling of uncertainty, including sensor errors, environmental transformations, and algorithmic uncertainty, should also be considered in the testing process to ensure that the system can still maintain safety under uncertain conditions [41]. The fourth is the validation of the residual risk of unknown scenarios. Since unknown scenarios cannot be predicted in advance, it is difficult for the validation process to cover all possible unknown situations. Traditional validation methods are usually based on previous experience and data from known scenarios, making it difficult to consider the complexity and variability of unknown scenarios comprehensively. Meanwhile, the definition of reasonable risk in SOTIF is ambiguous, and the definition of reasonable risk varies depending on the environment, regulations, and even the understanding

of different people, which increases the subjectivity and complexity of validation [42].

The application of AI technology brings new challenges. Autonomous driving systems apply a vast array of artificial intelligence technologies, from perception to decision-making. Regarding perception, such as convolutional neural networks are used to process image data to detect and recognize targets. Decision-making, such as end-to-end decision-making methods and deep learning methods, are employed to directly map the original input data to the output control commands, forming an end-to-end learning framework. Artificial intelligence technology improves the intelligence of autonomous driving and realizes a more human-like decision-making process, thus better adapting to various driving scenarios [43]. However, it also brings a series of problems, one of which is the limitation of datasets. AI models are usually based on a large amount of training data, which cannot exhaust all the possibilities relative to the actual scenarios. Models may produce uncertain predictions in the face of unseen situations, leading to the SOTIF problem [44]. Second, the process is not interpretable: complex AI models such as deep learning are often considered "black boxes", making it difficult to explain the model's decision-making process and affecting the feasibility of model validation and regulation. Thirdly, the unreliability of the output: when training the model, the data distribution used in the model may differ from that of the actual application, leading to conceptual bias [45]. The bias between the data distribution exposed during training and the data distribution in real applications makes the model output unreliable in the face of factual scenarios. Fourth, the effectiveness of algorithm generalization ability. Migration learning and continuous learning have been proposed as solutions to cope with the "long-tail problem" of scenarios. However, the introduction of new scenario data may bring new security risks. This may lead to fluctuations or even severe degradation of model performance in new scenarios, thus affecting the security of the system.

Along with the intelligent development of automobiles, the new issue of SOTIF has been derived [46], and the development of the ISO 21488 standard marks an essential step in SOTIF, which standardizes the development process of SOTIF of a system. However, compared with functional safety, the concept of SOTIF is relatively new, and it is still challenging to propose clear, quantitative standards and means of prevention and control, as is done for functional safety issues. Many related types of research are still in the preliminary exploration stage, and the concrete application of SOTIF into practice still faces many urgent problems [47].

2.4 Interrelations of the safety & security issues

From the application perspective, the work on functional safety (FuSa), cybersecurity (CS), and SOTIF is currently viewed as independent domains. However, from the problem perspective, as shown in Fig. 2, these three categories of safety issues demonstrate mutual influence and tight coupling [48]. Functional safety is the foundation for achieving SOTIF and cybersecurity. A failure in functionality can lead to a decline in system performance or expose vulnerabilities in cybersecurity. For instance, in August 2023, doctoral students from the Technical University of Berlin, in collaboration with independent researcher Oleg Drokin, successfully bypassed the MCU-Z AMD Security Processor (ASP) of a Tesla Model 3 through physical contact with the Infotainment and Connected Electronic Control Unit (ICE) board, using voltage fault injection. This enabled unrestricted access to the Tesla vehicle, including unlocking paid features [49]. Concurrently, malicious cyber-attacks can pose threats to functional safety. For example, attackers can incapacitate vehicle ECUs by overloading them with redundant information through intrusions into the vehicle's internal network, leading to excessive consumption of ECU resources. The SOTIF of the system relies on real-time and reliable sensor data. Cyber-attacks can affect SOTIF by altering sensor data, such as injecting previous video streams into the perception system through replay attacks, causing errors in road marking recognition. The functional safety of the system may depend on the correct implementation of SOTIF. Design flaws in SOTIF or failure to consider all possible usage scenarios can threaten functional safety or cybersecurity. For example, limitations in system performance can lead to inadequate defenses

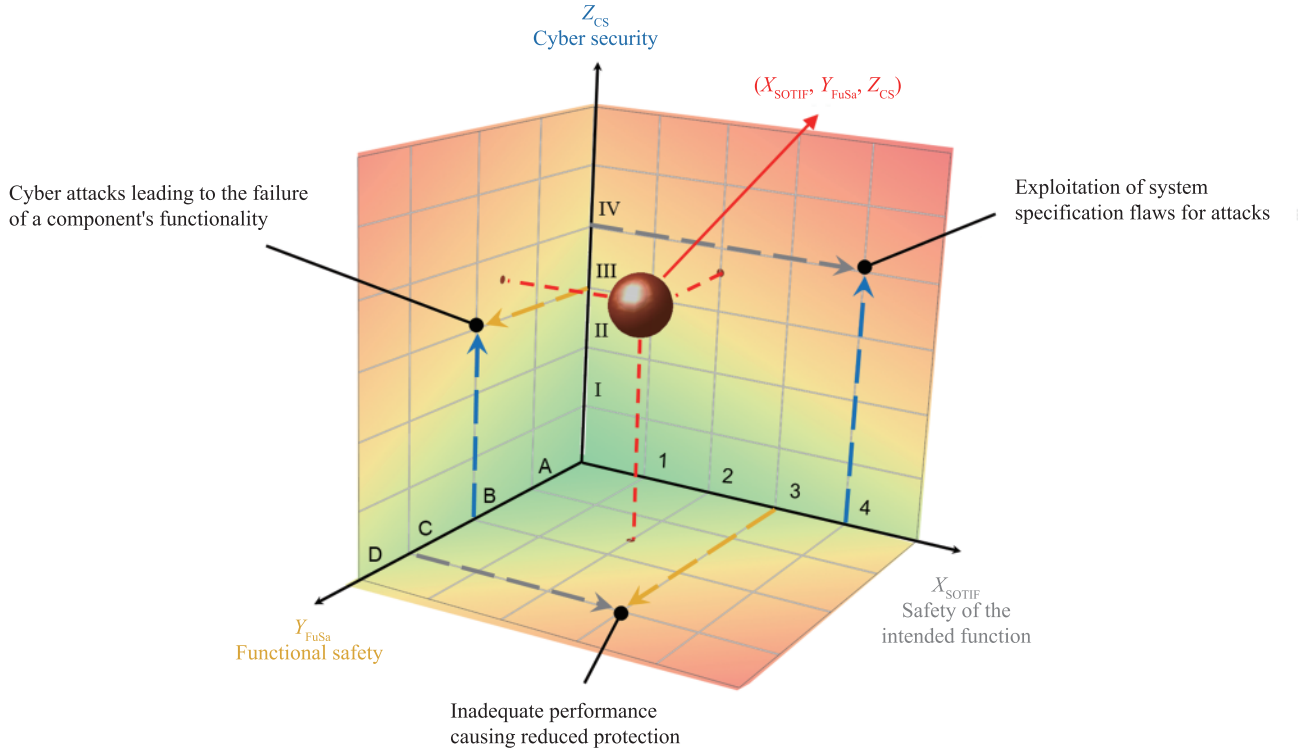

Figure 2 Interrelation of safety & security.

against specific cyberattacks, resulting in cybersecurity issues.

From the perspective of international standards, the connections and distinctions among the three categories of safety—functional safety, network and data security, and expected functional safety—are reflected through ISO 26262, ISO/SAE 21434, and ISO 21448, respectively. Each standard encompasses common areas such as management, concept development, system design, hardware development, software development, validation, verification, etc. However, there are differences in the specific content descriptions. For example, in the concept design phase, both functional safety and SOTIF undertake a crucial activity called Hazard Analysis and Risk Assessment (HARA), which involves analyzing and identifying hazardous events and setting safety goals to prevent and mitigate these events, avoiding unreasonable risks. In contrast, cybersecurity performs Threat and Risk Assessment (TARA), identifying threat scenarios and assessing risks based on the impact of damage and the feasibility of attacks. Furthermore, each domain has different focal points, and each area's work is usually relatively isolated. In functional safety, analyzing design concepts or system architecture and considering technical measures is essential. In cybersecurity, considerations extend beyond safety to financial, operational, and privacy aspects (SFOP). Additionally, discussing cybersecurity strategies requires specific system specifications, such as communication methods, data exchange, asset location and type, and updates during post-development operations. In SOTIF, numerous issues related to advanced technologies, such as safety challenges posed by autonomous driving and artificial intelligence, are involved. Addressing these potential safety issues requires complex and comprehensive analysis, covering unknown potential hazardous scenarios, driver misuse, insufficient specifications, and inadequate performance. Moreover, compared to ISO 26262 and ISO/SAE 21434, ISO 21448 is relatively new. It faces a series of challenges in practical application, including the standard for quantitative assessment of risks related to SOTIF.

The mutual influences among the three aspects of safety introduce higher complexity and uncertainty into the safety design of ICVs. The interplay between functional safety, cybersecurity, and SOTIF significantly increases the complexity of the overall system design. ICVs must not only meet traditional functional

safety requirements but also address issues arising from cybersecurity and SOTIF. During system design, testing, and verification, it is necessary to consider safety issues across multiple dimensions and layers, involving expertise from various fields, thus making the overall development process more intricate. Furthermore, the lack of explicit interconnection mechanisms among these three safety aspects adds to the complexity. Measures for functional safety may impact cybersecurity, while requirements for SOTIF may need to be considered within the framework of information network security. This potential lack of clarity introduces uncertain variables in system design. Additionally, SOTIF involves advanced technologies like artificial intelligence and machine learning, with the system's efficacy dependent on the correct functioning of these technologies. However, these new technologies may introduce novel risks related to functional safety and cybersecurity, such as attacks on or misusing models. The introduction of new technologies increases overall system uncertainty. Therefore, it is imperative to systematically study these three categories of safety issues to deeply understand their interrelationships, identify commonalities and intersections, and thereby develop more comprehensive and effective safety methods and techniques.

3 Existing methods and techniques for safety & security

With the rapid development of intelligent and connected technologies in the automotive industry, the industry is also conducting parallel research on functional safety, cybersecurity, and the SOTIF of ICVs. At present, many countries have carried out a lot of work on intelligent connected vehicle safety in terms of regulations, standards, and technology research and development. This paper summarizes the existing methods and technologies of functional safety, cybersecurity, and SOTIF of ICVs, as in Fig. 3, and analyzes the bottlenecks and problems that may exist in the existing methods and technologies when facing the new challenges of ICVs.

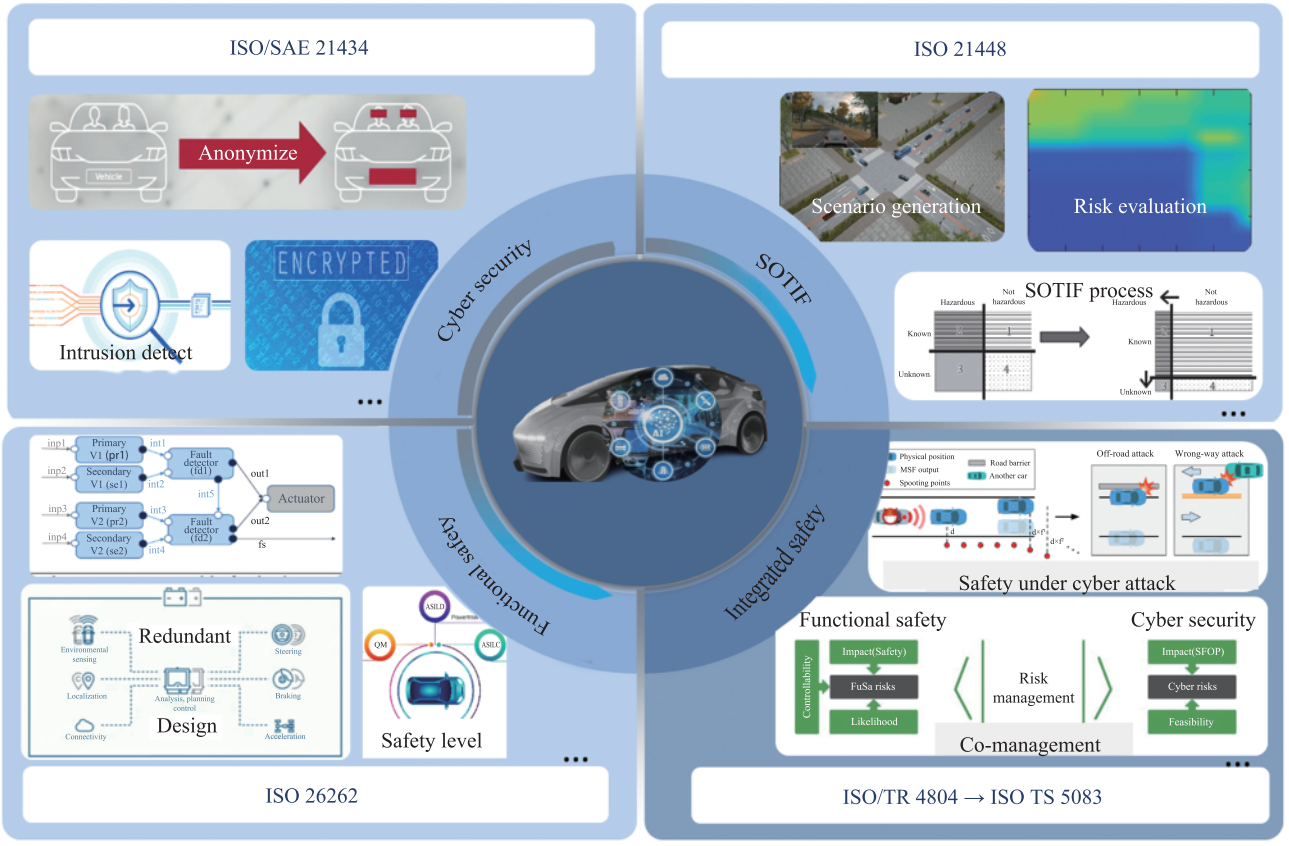

Figure 3 Existing safety technologies and associations.

3.1 Methods and techniques for functional safety

Functional safety emphasizes designing safety mechanisms correctly and reasonably to avoid risks or mitigate hazards. Currently, the functional safety research of ICVs focuses on the vehicle's electronic and electrical (E/E) system, concerned with the abnormal behavior of the vehicle function after the failure of E/E components and the possible harm.

Since the *Road Vehicle functional safety* release in 2011, many industry organizations and enterprises have continuously enriched the content of functional safety based on the ISO 26262 standard and related practices. Many scholars have also researched the functional safety of ICVs [9]. It covers power functions such as the vehicle's battery management system (BMS) [50], drive motor [51], chassis functions such as electric power steering (EPS) system [52] and electronic stability control [53], autonomous driving functions such as forward collision warning (FCW) and adaptive cruise Control (ACC) system [54], and related autonomous driving controllers and microchips [55]. Although functional safety standards and research results focus on different ICV systems, their ideas on functional safety analysis, verification, and evaluation all follow functional safety methods and activity processes.

The functional safety method covers the whole automotive system design, development, and operation process, mainly including functional safety design, fault diagnosis & fault tolerance control, and functional safety testing.

3.1.1 Functional safety design

Functional safety analysis of automotive systems is the key to the functional safety design process. Safety analysis methods mainly include failure mode effect and diagnostic analysis (FMEDA), failure mode and effect analysis (FMEA), and fault tree analysis (FTA). These methods start with failure mode analysis and assess its impact on the overall system or process. However, these methods rely on expert experience or large amounts of prior data and may not be able to cover all failure modes fully. The hazard analysis methods mainly include Hazard and Operability Analysis (HAZOP), Signal Error Factor Analysis (SEFA), and System-Theoretic Process Analysis (STPA), which are analyzed respectively from the functional, architectural, and system theory levels to explore the impact of different threats on system failure. Some scholars have combined several analysis methods above to deal with the highly integrated and complex E/E systems of ICVs. Reliability refers to the capability of ICV systems to perform their functions successfully under specified conditions, effectively complementing functional safety. Reliability can be quantitatively analyzed by the Markov model and Monte-Carlo simulation [56], and possible failure points of the system can be analyzed by simulating failure modes.

In addition to safety analysis, some studies introduce validation at the early design stage to verify the feasibility of design optimization before proceeding to cost design optimization. If design optimization is not feasible, designers can avoid unnecessary design work. If feasible, designers can reduce the design burden by using validation results as a basis [57]. In Refs. [58, 59], the design optimization of safety development cost, hardware cost, and resource consumption cost for safe automotive applications is studied.

The system should inherit the safety requirements of safety analysis output and implement various protection mechanisms. In Ref. [60], a redundant Autonomous Vehicle Control (AVC) Module Strategy is proposed. The main idea is to design a redundant control module, which can be controlled and protected when the vehicle fails. Safety requirements are also observed in hardware and software design. In the hardware design, attention should be paid to the electrical independence between the functional and safety mechanism circuits and the physical independence between the redundant designs. Functional safety protection should be carried out in software design and implementation; for example, defensive programming should be adopted [61], and input types and boundary values should be checked [62]. Forward recovery or backward recovery is used in case of failure [63]. In software, memory protection for critical safety functions [64], time protection, and sequential monitoring of tasks [65] are also effective functional safety methods in the design stage.

Each analysis method has its advantages and limitations and is often used in combination to meet the

functional safety requirements of systems. It is often necessary to consider factors such as the complexity of the system, the data required, the resources available, and the time.

3.1.2 Fault diagnosis & fault tolerance control

Functional safety monitors the operational process and focuses on the design process. When a failure occurs, the functional safety mechanism is activated. The functional safety mechanism is divided into fault diagnosis and fault tolerance control. Fault diagnosis refers to the analysis of the location, type, and duration of the fault after the fault occurs to obtain the severity of the fault. Fault diagnosis is divided into three methods: model-based, signal-based, and learning-based [66]. The model-based method uses filters or observers to estimate the parameters and states of the control system, analyzing the residual sequence with the estimated values and the actual values of the system, through which the fault information of the system can be obtained [62]. In reality, most systems are nonlinear, and the system robustness is compromised under the influence of external disturbance and noise. The established model is usually simplified because of the calculation requirements, which can reduce the difficulty of fault diagnosis and tolerance control but cannot reflect the actual system fault degree and location. The signal-based fault diagnosis method uses signal models, such as correlation function and spectrum, to analyze measurable signals directly and extract features such as amplitude, frequency, variance, and phase to identify and evaluate the state of the system [67]. When a system with a complex structure fails, the learning-based method extracts fault features through pattern recognition, expert systems, neural networks, deep learning, and other ways according to the knowledge of related faults. The diagnostic technology based on learning has universality and anti-interference ability, but its computation is also more extensive, which will be limited by the controller's performance. A variety of methods are often combined to achieve the classification of motor faults. For example, a heuristic feature selection method is used to analyze the motor current features, and the sampled current signal is used as the SVM input signal after the Stockwell Transform (ST). Finally, the actual motor fault category is obtained through machine learning [68].

Fault tolerant control (FTC) refers to taking appropriate measures based on fault diagnosis to ensure that the system enters the safe mode in the case of faults (sensors, actuators, or other system components) and completes the specified tasks as far as possible. Fault-tolerant control methods are generally divided into Passive fault tolerant control (Passive FTC) and Active fault tolerant control (Active FTC). Passive FTC adopts a robust controller with a fixed structure to ensure that the system is not sensitive to faults and does not depend on fault diagnosis results. However, this method is only applicable to a limited set of faults, and the risk of failure is high in extreme cases [69]. Active FTC compensates the system's control parameters or changes the controller's structure according to the fault diagnosis results after the fault occurs. The former is used when the fault can be isolated, estimated, and not severe. When the fault cannot be estimated or serious, the compensation control is no longer applicable. In this case, isolation of the fault loop is needed, and the system control loop should be reconfigured. When there are redundant parts or loops in the system, the fault tolerance mechanism can be realized by switching; when a specific part of the system fails, isolating the parts and the spare parts without fault are connected to the control loop. Sensors, actuators, controllers, and communication buses are all suitable for this fault tolerance method, such as the open phase fault and the open switch fault in the driver of the two-three-phase permanent magnet synchronous machine. However, the effect of fault-tolerant switching is closely related to the speed of fault diagnosis and location accuracy [70]. Too long diagnosis time or positioning errors will cause fault-tolerant switching failure. The past and current state of the system can also be used to predict the future output for Active FTC. For example, the model predictive control can effectively adjust the system performance failure by minimizing the error between the reference signal and the predicted system output [71].

3.1.3 Functional safety testing

Functional safety testing is also the key to functional safety. Functional safety testing involves hardware, software, and systems. Fault injection testing is a testing session required for every type of testing that

aims to introduce a fault into software, hardware, or system and analyze its response. Fault injection testing checks whether functions implemented in a fault-tolerant manner fail and also analyzes the behavior of non-fault-tolerant functionalities when they fail due to specific faults. The vehicle operating conditions and test cases are designed according to the hazards of the vehicle and the functional safety standards of the system under study before the fault injection test program execution. Then, the functional safety is integrated and verified using simulation, hardware-in-the-loop, vehicle-in-the-loop, and other experimental methods. The design of fault injection methods and test cases is the key to verification. Failure modes that violate security goals are derived from security analysis methods. These failure modes are simulated by designing use cases and injecting manually or through automated scripts into the software, hardware, or system operation. The software, hardware, or system execution process is then analyzed to see if it meets expectations, i.e., if the security mechanisms are implemented correctly. "Correctly" should include functional performance, accuracy, and temporal behavior. Many studies deal with parameter uncertainty in verification computations and correlation analysis based on Monte-Carlo and Markov models [72] for more efficient and faster test verification.

As ICVs continue to develop, functional safety technologies are being refined. The development and validation of safety-critical vehicle components through functional safety guidance can enable the development of safety-related elements, such as E/E and software, to meet the requirements of functional safety. However, it is worth noting that the information state and physical functions of ICVs are coupled with each other, and many problems cannot be solved by relying on functional safety alone, such as functional failure under edge scenarios and cyber-attack scenarios mentioned in Section 2. Meanwhile, the collaborative safety assessment and safety response of SOTIF and cybersecurity are also needed under failure scenarios to realize the overall effective safety of the vehicle.

3.2 Methods and techniques for cybersecurity

With the development of automotive technology, vehicle systems no longer mean just the traditional combination of mechanical and electrical components but also involve software and network connectivity. Therefore, protecting automotive cybersecurity has become a crucial task. The objective of automotive network security protection is to ensure the security of automotive network communication and guarantee that data remains in a state of adequate protection and lawful utilization, particularly in the context of the increasingly intelligent and interconnected trends in modern vehicles. This Section introduces regular automotive cybersecurity technologies.

3.2.1 Assessment and analysis methods for cybersecurity

The primary method for cybersecurity of ICVs is threat analysis and risk assessment (TARA). TARA provides the basis for positive cybersecurity development and security vulnerability repair. TARA identifies the possible risks of the vehicle/system and determines its risk level, which provides the basis for positive cybersecurity development and security vulnerability remediation. TARA is the missing link in the previous vehicle development, and it can be carried out at all stages of the vehicle's whole life cycle. For example, the cybersecurity risk of the whole vehicle is identified in the concept stage, which serves as an input to the cybersecurity concept of the whole vehicle. Vulnerabilities are analyzed in the post-development stage to determine the risk level of the vulnerabilities, which guides the subsequent vulnerability disposal. In the published version of ISO21434, TARA is mainly divided into seven steps: asset identification, threat scenario identification, impact rating, attack path analysis, attack feasibility level, risk determination, and risk disposal decision. In recent years, researchers have proposed improvements based on the existing TARA. The contribution of text [73] shifts the focus from procedural adjustments to quantitative recommendations, aiming to improve the risk matrix and, thus, the objectivity of the assessment. Vogt et al. [74] proposed a comprehensive TARA methodology for cooperative intelligent transport systems (C-ITS) that includes ICVs, combining qualitative and quantitative threat modeling and risk scoring tools to provide flexibility in asset assessment for any C-ITS.

The data security analysis of ICVs should start from

data classification and grading for data security. Data classification and grading can effectively improve the efficiency and robustness of data security technology. Qualitative classification and grading methods based on parallel classification and hierarchical classification are obviously difficult to meet data security needs. Scholars in Ref. [75] have already transformed the data classification problem into a multi-label classification problem, thus reducing the difficulty of data classification and improving end-to-end processing. In addition to the data from attributes, statistical characteristics, and the user's subjective feelings, the proposed quantitative sensitivity model and algorithm are also effective data classification methods [76].

3.2.2 Cybersecurity protection methods

Conventional technologies for automotive cybersecurity include encryption, authentication and privacy protection, intrusion detection, and emergency response. They ensure that automotive network communications are secure and regular, and that sensitive data is not leaked through active detection and passive constraints. The details regarding data security will be elaborated in Section 3.2.3.

Encryption methods in the communication process and cloud data storage can ensure the confidentiality of data in telematics and prevent sensitive information from leaking. Common encryption methods are symmetric encryption and asymmetric encryption.

Symmetric encryption algorithms involve both parties using the same key to encrypt and decrypt data during communication or data processing, which has the advantage of breakneck encryption speed and is suitable for the encryption and decryption process of large-volume data. Still, its security is not as good as asymmetric encryption algorithms, and the key management is complex. conventional symmetric encryption algorithms are DES, 3DES, TDEA, Blowfish, RC2, RC4, RC5, IDEA, AES, and so on. Asymmetric encryption algorithms have a pair of public and private keys; the information encrypted with the public key can only be decrypted with the corresponding private key; similarly, the information encrypted with the private key can only be decrypted with the corresponding public key. The advantage of asymmetric encryption is its high security and relatively easy key management; its disadvantage is that it is slow and suitable for small data volume encryption and decryption or data signature. Common asymmetric encryption algorithms include RSA, elliptic curve cryptography (ECC), etc.

Since some vehicular network uses open channels and the deployment of secure communication mechanisms is not comprehensive, once a vehicle malicious node or device gets access to the in-vehicle network or inter-vehicle network, it may eavesdrop on the private data of other vehicles or attack the whole system of the vehicular network by sending malicious messages, which may lead to traffic accidents. In addition, the leakage of sensitive information may even threaten the road traffic system and national security. Therefore, authentication and privacy protection must be considered in the Telematics architecture. The standard approaches are Public Key Infrastructure (PKI)-based authentication [77] and privacy protection [78], Identity-based cryptographic authentication and privacy protection [79], Pseudonym-based authentication and privacy protection [80], and Group Signature-based authentication and privacy protection [81], blockchain-based authentication and privacy protection [82].

Unlike passive cybersecurity protection methods such as authentication and data encryption, intrusion detection in vehicular networks is the proactive detection of data, communication messages, etc., to look for possible malicious attacks and intrusions so that appropriate measures can be taken in time to prevent damages caused by such activities such as blocking the access of malicious nodes to the network to prevent further damages caused by them. More research has been done on intrusion detection for in-vehicle and VANETS. An intrusion detection system (IDS) can be categorized into host-based IDS and network-based IDS regarding application objectives [83]. Host-based IDS monitors specific nodes and local hosts. Network-based IDS monitors network status and data transmission in wired or wireless networks [84]. From the deployment perspective, IDS can be categorized into centralized and distributed deployment IDS. Centralized deployment of IDS is usually deployed in the in-vehicle gateway or VANETs in the RSU and other locations, with unified detection of the entire network between the nodes of the communication process. The distributed deployment of

IDS is in the network of all nodes, or part of the important ones are deployed in the IDS [85]. The IDS can also be divided into rule-based IDS and learning-based IDS. Rule-based IDS sets rules through a priori knowledge to form a database of signatures of various intrusions, and detection is realized by matching the input model's information with the intrusion rules' information in the database [86]. Learning-based IDS is to build a machine learning or deep learning model based on existing data to build a learning model and then use the model to detect anomalies in the network [87]. Typically, when the IDS detects a malicious intrusion, it takes several emergency response measures, such as disconnecting the malicious ECU in the CAN bus from the bus as proposed in Ref. [88]. These emergency response measures target network nodes, VANETs, or in-vehicle networks. The infrastructures with centralized IDSs also have some emergency response measures after detecting the malicious nodes in the network, such as revoking their legitimate certificates, informing their identity information to other vehicles, or lowering their trust value, etc., to quarantine the malicious nodes, to prevent the malicious vehicles from continuing to attack the network. In addition, emergency response mechanisms for malicious packets are often deployed in the in-vehicle network. When abnormal communication packets or packets are detected, retransmission or overwriting of malicious packets can be used to restore the damaged functions of ICVs in a short period. In short, intrusion detection and emergency response should complement each other. To realize active protection of cybersecurity in the vehicle network, both fast and accurate intrusion detection and efficient emergency response methods are needed.

3.2.3 Data security technologies

Data accompanies the entire process of the vehicle, with complex, heterogeneous, complex flow, sensitive range, and user-based characteristics; from the perspective of the entire life cycle of the data, it is conducive to clarifying the source and destination of the data, as well as the required security protection technology. Generally, data will go through the process of data collection, data transmission, data storage, data processing, data exchange, and data destruction, and each stage will face corresponding risks. The basic principles of data security protection technology should be to ensure that in-vehicle processing, accuracy range application, default non-collection, and desensitization are met. This series of principles provides a foundation for the security of vehicle data and, at the same time, poses a challenge for a comprehensive response to data security. Comprehensive protection is provided from the perspective of the entire life cycle of data, covering data asset grooming, sensitive data identification, data encryption, desensitization, data destruction, and other important technologies.

Data asset grooming is generally centered around knowledge graph technology, which utilizes the knowledge graph inference function to identify new subjects and new relationships of vehicle data. In particular, the prominent visualization effect is more effective for data grooming of ICV data assets. The EVKG [89] encapsulates essential EV-related knowledge, including EV adoption, electric vehicle supply equipment, and electricity transmission network, to support decision-making related to EV technology development, infrastructure planning, and policymaking by providing timely and accurate information and analysis. In a word, data asset grooming from the perspective of data security is an essential foundation for subsequent identification and desensitization of sensitive data.

Sensitive data identification and desensitization are the focus of data processing. On the one hand, there are sensitive data specified in laws and regulations, such as face and license plate information collected inside and outside the vehicle that can identify individuals, and sensitive personal information, such as voiceprints, fingerprints, heart rhythms, etc., collected from the driver and passengers in the cockpit; on the other hand, the high-dimensional and hidden relationships between data have the risk of Membership Inference Attacks and Linkage Attack, such as speculating on the latitude and longitude of the state authorities and the personal information of the passengers through the linkage of an external database with the vehicle trajectory data. Currently, the use of neural networks [90], heuristic algorithms, information theory [91], and other methods to mine sensitive data has significant results.

Specific identification and desensitization efforts are carried out in the form of data, e.g., structured data,

text, image data, audio data, and trajectory data, and have applications in healthcare, finance, military, and government agencies. Structured datasets have quasi-identifiers and sensitive attributes, and unlike quasi-identifiers that can be intuitively recognized as sensitive data, sensitive attributes often need to be identified in conjunction with background knowledge and external databases. In addition, quantifying sensitivity based on sensitive identification is also the main identification idea. Among them, information entropy is a vital sensitivity identification index, as well as TF-IDF and other statistical features, which, to a certain extent, can react to the sensitivity of the data. The sensitivity of image data is more intuitive, but the difficulty is to realize image encryption under the premise of maintaining usability. The sensitivity of track data [92] is reflected in semantic features and geographic location privacy, and the identification and decryption process has high requirements for real-time accuracy. The sensitivity of audio data is reflected in both voiceprint features and audio content [93].

Sensitive data processing has been well-established in other fields, focusing on classical cryptography schemes and privacy-preserving data mining. These techniques have not only been intensively researched in the academic field but also have demonstrated strong results in practical industrial applications. In structured datasets, the desensitization strategies of FPE [94] and hash function [95] are generally adopted for direct identifiers. On the other hand, sensitive attributes are dominated by privacy-preserving data mining. Privacy-preserving data mining can be classified into randomization, anonymization, and cryptography-based. The classical algorithms based on anonymization are *k*-anonymity, *l*-diversity, and *t*-closeness. However, it is still difficult to fully protect against background knowledge attacks, as well as the lack of applications in ICV. Cryptography-based privacy protection methods for data mining are secure multi-party computation, homomorphic encryption, differential privacy, and secret sharing or homomorphic secret sharing. Among them, differential privacy [94] does not change the statistical characteristics with the change of a single piece of data and has better security against inference attacks; Homomorphic encryption [96] has a high balance between privacy protection and data utility due to its "computable but invisible" property and can be applied to both structured datasets and unstructured audio and video data.

Based on reinforced supervision and management, proposing a method of data encryption to meet the requirements of anonymization is also a practical approach, which involves gradually reducing data availability, thereby leading to data destruction. The clock factor is added to the image encryption, and the image decryption result is unavailable when the preset value is reached [97].

3.2.4 Cybersecurity testing

Cybersecurity testing includes compliance testing and vulnerability discovery testing. Compliance testing refers to verifying whether the security policies of various components and related functions of telematics meet the requirements under the guidance of security specifications or testing standards; vulnerability discovery testing refers to analyzing and detecting the possible vulnerabilities in Telematics systems by using various technical methods to assess the security of the whole system. Commonly used vulnerability discovery testing technology methods mainly include vulnerability testing, penetration testing, and fuzz testing. Vulnerability testing aims to scan for vulnerabilities in the system and even utilize exploratory testing and more aggressive testing to break, bypass, or tamper with security protections to find weak points in the system. Penetration testing is mainly the process of detecting the presence of security issues in telematics and in-vehicle networks and their applications and data using various vulnerability discovery techniques and attack methods. Fuzz testing is attacking the telematics systems and functions with data or signals to see if the systems or functions will react abnormally, thus exposing vulnerabilities that can be exploited. The framework for testing cybersecurity in ICV is still immature, and the related technology is still in the research stage.

This section summarizes the standard methods and techniques of cybersecurity, which are used to solve some of the cybersecurity problems described in Section 2. However, the existing methods still have the problem of inapplicability and mismatch for the rapidly developing ICV. In particular, under the trend of increasing vehicle intelligence and communication capabilities,

cybersecurity, there is a growing correlation between functional safety, cyber safety, and intended functional safety. A single cybersecurity protection method may make it difficult to address the above new challenges.

3.3 Methods and techniques for SOTIF

ISO 21448 provides a complete set of methods and guidelines for the development and design of SOTIF, and the standard uses the "V-model" to describe the flow of development activities for SOTIF. Compared to functional safety and cybersecurity standards, SOTIF clearly defines some specific steps in its process, including identifying potential functional deficiencies and triggers, assessing known and unknown scenarios, and assessing SOTIF results [98]. Among them, potential functional deficiency and trigger condition identification aim to analyze the planning algorithms, sensors, actuators, and environmental conditions and foreseeable misuse in the autonomous driving system to identify the trigger conditions that may lead to a hazardous event. Unknown scenarios assessment is the most challenging issue, which focuses on confirming that the residual risk from unknown scenarios meets the acceptance criteria through many long-term tests. In the SOTIF achievement evaluation, the standard lists methods and criteria for assessing the SOTIF but lacks clear quantitative criteria [99].

There are three basic principles for the design of SOTIF technologies: system performance enhancement, functional degraded use, and driver takeover. On the one hand, system performance enhancement can fundamentally solve the problem of system performance limitations and insufficient design specifications [100]; on the other hand, based on the infinity of real-world scenarios, it ensures the safe operation boundaries of the system by defining clear design operation domains [32], and once exceeding the design operation domains of the system, it is necessary to carry out performance degradation and use; when the system is degraded and used, the driver and passenger, as the only subject with independent judgment and action ability in the vehicle, play an essential role in ensuring the SOTIF of the system [101]. Based on the above three principles, the critical technologies for the SOTIF will be divided into system design, system testing and verification, and system operation safety [102].

The technology of SOTIF for system design involves environment sensing technology, decision planning technology, and human-machine interaction technology. The hardware level of environment sensing technology includes utilizing multiple sensors, including millimeter-wave radar, camera, and LiDAR, to obtain comprehensive and multidimensional environmental information [103]. At the algorithmic level, heterogeneous sensor data are fused, and the data are cross-analyzed and integrated to enhance the system's ability to understand the scene [104]. In the fusion process, the confidence and accuracy of different sensors are considered, giving higher weight to the high-reliability sensors, which has weakened the influence of other less powerful sensors. In addition, the perception must react adequately to so-called edge cases, such as overexposure of the sensed image or unexpected and potentially dangerous traffic situations. In other words, the perception system has to be extremely robust to environmental sensing [105] and still be able to perceive and understand the environment correctly in case of data anomalies. For decision planning, the industry has mainly adopted rule-based techniques that apply to regular scenarios and have shown good performance in specific scenarios, such as Baidu's Apollo [106]. Numerous researchers have also researched data-driven decision planning-based algorithms, such as end-to-end decision planning [107], where the algorithmic models have been trained to show good performance for test scenarios. However, both model-based and data-driven algorithms are a simple integration of decision planning for a single scenario and cannot meet the requirements of advanced autonomous driving. The core challenge of high-level decision-making algorithms lies in understanding and reasoning about driving scenarios [108]. Advanced autonomous driving requires a decision-planning technique that can cope with different scenarios, especially with a strong generalization ability for extreme scenarios. Like a good human driver, it can understand and reason about complex driving scenarios and extract valuable information to make the right maneuvers and navigate the environment well, regardless of the encountered situation [109]. Of particular note,

the timeliness of decision-making is critical when responding to emergencies, and responding quickly and generating appropriate safety strategies, including emergency response behavior selection and real-time path planning, is essential to ensure that a vehicle can be driven safely in uncertain or dangerous situations. Emergency response behavior selection can be implemented using a finite state machine (FSM) algorithm that maps emergencies and corresponding behavioral rules to states and transfers of the FSM [110]; for real-time path planning, the key is the prediction of the movement of other traffic participants, Shao et al. propose a self-aware trajectory prediction method [111], which achieves online by combining a self-awareness module and a two-stage training performance evaluation to cope with possible scenarios where the expected functionality is insufficient. Similarly, human-machine interaction is an important concern in the SOTIF, on the one hand, to avoid safety problems caused by foreseeable human misuse, and on the other hand, to perform a safe transfer of driving rights when the system is downgraded for use. To avoid human misuse, the system cognition and operation ability of the driver and passengers can be improved by increasing the training of the driver and passengers; in addition, it is necessary to improve the design of the system human-machine interface (HMI), combining the visual, auditory, tactile and other sensory interactions through the graphical user interface (GUI) technology, the intelligent voice interaction technology, and the multi-modal interaction technology to improve the intuitiveness and comprehensibility of the HMI. When the system sends a takeover request to the driver, the system should adopt an effective feedback mechanism according to the driver's status to help the driver return to the driving task in time. It is possible to recognize driver fatigue and distraction state and assess emotional state through the technology of multi-dimensional comprehensive monitoring of vision, hearing, touch, and smell, and strengthen HMI feedback through enhanced display technology, intelligent voice interaction technology and haptic virtual display technology, etc., to help the driver understand the driving environment quickly and make driving decisions promptly [112]. Furthermore, the utilization of brain-computer interface technology represents an exploratory approach to enhancing SOTIF. A positive correlation between cerebral oxygen and the driving risk field is discovered in the literature [113]. Passengers' electroencephalography (EEG) signals are analyzed to distinguish between emergency and non-emergency situations in literature [114]. Both pieces of research illustrate the potential to enhance driving safety by considering humans' perception of driving risk.

Testing and verification play a crucial role in ensuring the SOTIF. For SOTIF testing of perceptual systems, diverse test cases are generated using a high-coverage test-set generation method with basic scenarios [115]. For SOTIF testing of decision planning systems, the dynamic adaptive design and optimization experiment (ADOE) approach is divided into scenario-based and mileage-based tests [116]. Through an adaptive approach, scenario-based testing focuses on quickly identifying scenarios that challenge the decision-making system in a complex logical scenario space. In contrast, mileage-based testing constructs various interactive driving models in a simulation environment to mimic actual traffic conditions and evaluates the system's performance in a natural traffic flow. In addition to independent testing of the perception and decision-making systems, testing and validation of the process from the perception system to the decision-planning system involves the use of error-injection-based reinforcement testing to generalize the error results produced by the perception system and to test the robustness of the decision-planning system through the error-injection method [117].

To ensure the SOTIF in system operation, performing real-time driving safety risk assessment is extremely important. Real-time driving safety risk assessment involves a variety of techniques, including temporal logic-based assessment techniques, which assess the risk based on temporal metrics such as time-to-collision (TTC) and time-headway (THW) [118]; physical model-based assessment techniques, which assess the driving safety risk of vehicles by simulating the vehicle's kinematics and dynamics behavior [119]; collision probability-based assessment techniques, which performs driving safety risk assessment by calculating the probability of all potential collision trajectories [120];

and statistical learning-based assessment techniques, including traditional machine learning, deep neural networks, and deep reinforcement learning, which predicts risk through big data analysis [121]. In addition, artificial potential field (APF) models are used to build driving risk fields to assess safety risks in dynamic environments [122]; safety force field-based approaches utilize the concept of physical forces to assess safety distances and collision risks; and entropy-based risk assessment techniques deal with system stochasticity and uncertainty by calculating the entropy value of a system's state to assess risk [123]. The comprehensive application of various technologies and algorithms is set to become a trend [124], aiming to achieve a more holistic and precise assessment of vehicular safety risks. For the SOTIF in system operation, in addition to real-time risk assessment, the importance of emergency response should not be neglected. Feng et al. proposed an active collision avoidance strategy based on the uncertainty of pedestrian motion [125], which realizes fast and accurate planning of optimal paths to respond to emergencies in complex road environments.

With the development of cutting-edge technologies such as autonomous driving and artificial intelligence, the concept of SOTIF has been derived, becoming a new safety concept independent of functional safety and cybersecurity. Although the ISO 21448 standard provides a series of guidelines and methods, there remains a gap in its practical implementation and application. Meanwhile, SOTIF technology is still in the early stages and has not yet been well developed. The application of artificial intelligence and deep learning in the field of autonomous driving not only raises concerns about SOTIF itself but also has a profound impact on the methods and techniques of functional safety and cybersecurity [126].

3.4 Integrated design for safety

When contemplating the safety design of future ICVs, it is important to recognize the integrated and interdependent relationship among functional safety, cybersecurity, and SOTIF. The interconnection of different categories of safety risks has gained attention, leading to the release of ISO/TR 4804：2020 by the International Standards Organization in 2020. This standard focuses on the safety of autonomous driving systems and integrates it with cybersecurity. ISO/TS 5083 has introduced cybersecurity considerations in the design, validation, and confirmation methods of autonomous driving. Additionally, the ISO/IEC DTR 5469 and ISO 8800 standards, currently under development by the International Standards Organization, attempt to combine vehicle functional safety with artificial intelligence technologies. Beyond these standards, the analysis of the relationship between cybersecurity and safety in the field of autonomous driving is discussed in the 2019 whitepaper titled *Safety First for Automated Driving* (SaFAD). This publication elucidates the impact of cybersecurity on functional safety and SOTIF. Researchers are also exploring the fusion of various safety technologies. Suo et al. [127] present a novel approach, combining hazard analysis and risk assessment (HARA) with threat analysis and risk assessment (TARA) analyses. Martin et al. [129] proposed a workflow based on the Safety Pattern, which considers both functional safety incidents and information security incidents as a safety pattern. Research on various safety coupling issues is a significant engineering challenge, and its scope extends beyond the automobile domain. Dotsenko et al. [130] introduce a method for enterprise security management. This methodology introduces an additional ecological safety management unit, fostering mutual coordination among cybersecurity, functional safety, and other safety facets within its purview.

In general, the interconnectivity of various safety issues has begun to be noticed, with some corresponding international standards currently in the drafting stage and preliminary research foundations established in related fields. However, it is crucial to note that no unified standard or methodology encompasses all three categories of safety issues.

3.5 Limitations of existing methods and techniques

As automotive electronic and electrical systems become increasingly complex, functional safety, the earliest proposed concept, has relatively matured in its methods and technologies. However, the development of ICVs has led to significant expansion in the definition and boundaries of vehicles. Traditional functional safety

methods and technologies are insufficient to address the novel issues brought about by new technologies. For example, the development of vehicle-cloud collaborative technologies has shifted important functionalities to the cloud. Traditional functional safety primarily focuses on the vehicle system itself, often neglecting the security of cloud systems. The failure of cloud-side system functionalities may result in the inability of ICVs to receive critical traffic information in real-time, thereby increasing safety risks. Simultaneously, with the application of big data and large models in the automobile industry, emerging cybersecurity issues

Table 1 Summary of Existing Techniques for Safety & Security

Category	Means	Technical description	Typical approaches
Functional safety	Risk analysis	Analyze failure modes and assess their impact on the entire system or process.	FMEDA, FMEA, FTA, SEFA, HAZOP
	Fault diagnosis	Analyze the position, type, and duration of faults occurring after a failure to determine the severity of the fault.	Model-based [62], signal-based [67], and learning-based [68]
	Fault tolerance control	Drawing on the results of fault diagnosis, implement appropriate measures to ensure that the system, in the event of a fault (sensor, actuator, or other system components), transitions into the corresponding safe state and endeavors to fulfill specified tasks to the best extent possible.	Passive FTC [69] and Active FTC [70, 71]
	Redundancy design	In critical areas where the system plays a pivotal role in task completion, introduce multiple redundant functional channels or components performing the same function to ensure the system continues to operate normally in the event of a failure.	Redundant control modules [60], defensive programming [61], memory protection [64], and time protection [65]
	Early validation	Introduce functional safety verification in the early stages of development to avoid unnecessary design work or alleviate the design burden during later optimization phases.	Fast functional safety verification [57] Safety cost verification [58, 59]
	Fault injection testing	Introducing faults into the software, hardware, or system and analyzing their responses.	Artificial fault injection [52] Markov model [72]
Cybersecurity	Cybersecurity assessment	Identifying security risks in-vehicle networks and data.	TARA Enhanced TARA [73, 74] Data classification and categorization [76]
	Encryption	Encrypting essential data to ensure the confidentiality of information.	Symmetric encryption and asymmetric encryption [78, 79]
	Certification	Verifying the identity of communication nodes to ensure their authenticity and integrity.	PKI [77] Identity-based [80] Group signature [81] Blockchain [82]
	IDS	Detecting potential network attacks and malicious activities on automotive networks and systems, and implementing defensive measures.	Rule-based IDS [86] Learning-based IDS [87]
	Data anonymization	Employing specific strategies for data protection, and preventing attacks related to external database connections or background knowledge.	*k*-anonymity *l*-diversity [108] *t*-closeness Differential privacy [91] Homomorphic encryption [95]
	Data desensitization	De-identifying data that directly identifies individuals.	FPE encryption [161] Hash function [93]
	Network security testing	Verifying whether automotive components, systems, and the entire vehicle comply with regulations and identifying potential vulnerabilities.	Compliance testing Vulnerability scanning testing

(Table 1 Continued)

Category	Means	Technical description	Typical approaches
SOTIF	Sensor fusion	Through algorithmic synthesis, diverse sensor data, including cameras, radar, and lidar, is processed comprehensively to obtain more accurate and comprehensive environmental information as well as object detection results.	3-D object detection [128] Real-time multi-object tracking [131] SSD [132]
	Rule-based decision and planning	Make decisions and plans based on predefined rules and logic.	Baidu Apollo EM motion planner [106] Finite state machine（FSM）[110]
	Data-driven decision and planning	Rely on extracting information and patterns from large real-world data, establishing a mapping between input data and decision planning results.	End-to-end decision and planning [133] Self-aware trajectory prediction method [111]
	human-machine interface optimization	Enhance the interaction experience between users and the system, making the system more user-friendly, efficient, and user-centric.	Enhanced display technology [134] Intelligent voice interaction technology [135] Haptic virtual display technology [136]
	Test scenario generation	Design and simulate various environments and conditions reflecting real-world driving scenarios to assess and validate the system's performance.	Scenario-based Testing [115] Mileage-based Testing [116]
	Error injection-based testing	Introduce errors or anomalies into the system intentionally to evaluate its robustness and error-handling capabilities.	Enhanced testing based on error injection [117]
	Real-time driving safety risk assessment	Continuously monitor and analyze the vehicle's operational environment and status information to identify potential safety risks in real-time.	Assessment technology based on physical models [119] Assessment technology based on collision probability [137] Risk Assessment Based on Security Entropy [123] Risk Assessment Based on Artificial Potential Field [122]
Integrated Safe Design	Threats joint analysis	Quantify and decompose threats across multiple domains, drawing attack trees.	Integrated analysis of HARA and TARA [127]
	Development process optimization	Integrate and optimize the workflows of different security engineers to enhance collaboration.	Normalization of Security Issues [129]

such as large-scale data mining, model-based data encryption, and the processing of remote uncontrolled information are becoming increasingly apparent. These problems become more challenging due to the vehicle's limited computing power, storage resources, and cost considerations. Hence, there is a need to reassess and address these emerging cybersecurity issues to adapt to the specific requirements and challenges of ICVs. Compared to functional safety and cybersecurity, the concept of SOTIF is the latest to be introduced. Despite the growing recognition of the importance of SOTIF, this field still lacks a mature, quantifiable methodology and technology, with no clear solutions. This implies that the actual implementation of SOTIF concepts still faces significant gaps.

While there has been some research on the interconnection of different types of safety issues, the study of composite safety problems often involves the combination of only two types of safety issues. There is a lack of a comprehensive, systematic framework that unifies the consideration of all three types of safety. This isolated research approach and technology are challenging to address the increasingly complex safety requirements of ICVs effectively.

4 Fusion safety for ICVs

In facing the complex and uncertain interconnections

of these three types of problems, developing a high-dimensional, integrated security approach based on three categories of safety technologies and methods is necessary. This involves not only the fusion at the technological level, such as data sharing, comprehensive assessment, and integrated protection, but also the integration of development processes and toolchains to adapt to the future's complex and variable security protection requirements.

This section first expounds on the concept of integrated security from four dimensions and then introduces a theoretical framework model for field-vehicle-human safety interaction. Based on this theoretical framework model, a potential integrated security system framework is proposed. Lastly, a new security design and development process that supports rapid development and continuous iteration is designed based on CHAIN to meet future complex and dynamic security needs.

4.1 The concept of fusion safety

Fusion Safety is a high-dimensional security concept developed from functional safety, cybersecurity, and SOTIF. Fusion Safety is not a mere aggregation and integration of these three safety categories but an organic, systematic, and multi-layered fusion. In Fig. 4, the relationship between safety and security is akin to a Möbius strip, representing the dual aspects of the same concept. Their interdependence and close connection render them an inseparable whole. From a dynamic development perspective, safety and security are intertwined and spiral upwards in their evolution, continuous and boundless, analogous to the shape of a Möbius strip and the infinity symbol in mathematics. The close integration of Safety and Security forms the core concept of Fusion Safety.

Surrounding this core concept, Fusion Safety integrates and intercommunicates across four dimensions: value, process, toolchain, and information. At the process level, the fusion concept encompasses concept definition, system design, testing, verification, and production, comprehensively considering all three safety types at every stage. At the toolchain level, the unification and collaboration in areas like code generation, model development, test calibration, and simulation platforms provide robust support for Fusion Safety. At the information level, the seamless integration and fusion of data collection, mining, transmission, and integration maximize and enhance data value. Finally, at the value level, the design philosophy of Fusion Safety extends beyond the direct safety of vehicles and humans to play a pivotal role in promoting societal and ecological values, aiming to foster coordinated, symbiotic development in these areas.

The fusion of these four dimensions creates a closely linked ecosystem. Value creation drives the development of the entire process, which is supported and realized by the toolchain. The toolchain, in turn, adds value to data, benefiting the entire system. Ultimately, the value of this data further promotes and shapes value creation, forming a closed-loop interactive system. In the design philosophy of Fusion Safety, each dimension is interconnected and interdependent, collectively enhancing the overall safety and efficacy of the system.

4.2 Framework for fusion safety protection system

Based on the concept of Fusion Safety and guided by the field-vehicle-human safety interaction model, a "Safety Brain System" aimed at Fusion Safety is proposed, as illustrated in Fig. 5. A field-vehicle-human safety interaction model is proposed to thoroughly consider the complex driving scenarios faced by ICVs within the Fusion Safety design. This model comprehensively and hierarchically depicts the multi-dimensional characteristics of driving scenarios and the dynamic interactions between different factors within the Field. In the model, "Field" includes both the physical space and the cyber space, corresponding to the physical world and the data-constructed virtual world. At the same time, "Human" refers not only to the driver but also to the passengers in the vehicle. The field-vehicle-human safety interaction model serves as the foundation and input for the design of the Safety Brain System. The protection system is divided into the primary Safety Brain System and cloud collaboration [138]. The Safety Brain System provides real-time safety protection, while the cloud offers intelligent remote protection, ensuring Fusion Safety through end-cloud collaboration.

The vehicle-edge "Safety Brain" encompasses three

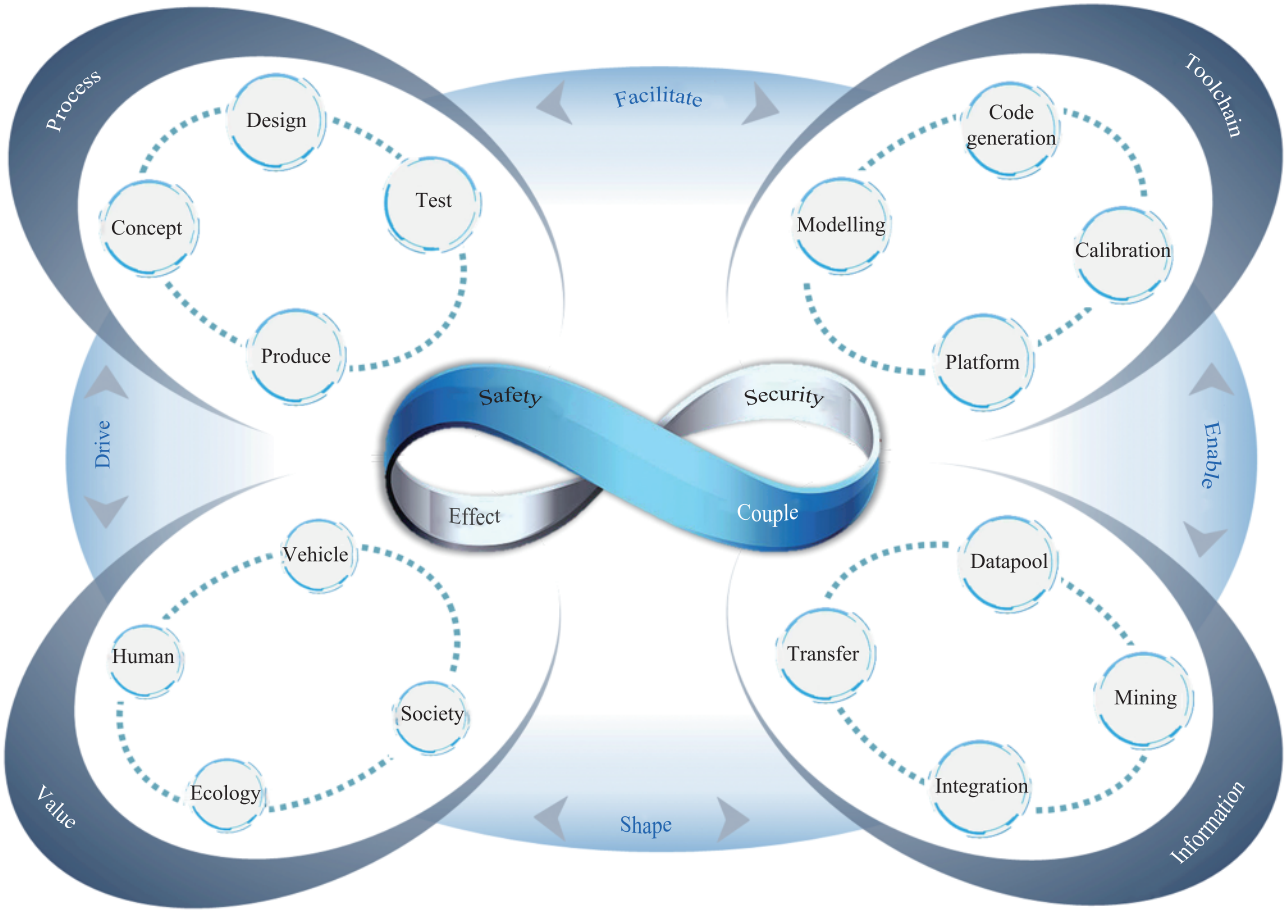

Figure 4 Concept and design of fusion safety.

key functional modules: monitoring, assessment, and prevention & control. The monitoring module implements real-time global safety risk monitoring, utilizing multi-fusion sense technology and overall perception to capture information about vehicle status and the external environment. The assessment module quantitatively evaluates the vehicle's Fusion Safety status in real-time based on data from the monitoring module, involving risks of functional failure, performance degradation, and cybersecurity. It performs an integrated assessment of Fusion Safety risks based on independent analysis of these factors. The prevention and control module, based on assessment results, generates Fusion Safety strategies and implements protective measures to ensure Real-time Vehicle-edge Protection.

The cloud acts as an information and strategy processing center, equipped with Safety Risk Alert capabilities, recording (Critical Scenario Record) and analyzing (Scenario Reasoning and Analysis) critical scenarios. Utilizing its big data storage and high-performance computing capabilities, the cloud optimizes safety strategies [139] to ensure optimal safety performance of the entire system. The cloud is capable of providing Remote Intervention Control when necessary [140], serving as a redundancy plan for vehicle-edge protection. The Safety Brain enables ICVs to adapt dynamically to complex and variable traffic environments. End-cloud collaboration not only enhances the vehicle's safety protection capabilities but also strengthens its ability to respond to external safety risks, thus realizing a comprehensive, integrated Fusion Safety management system.

4.2.1 Field-vehicle-human safety interaction model

The field-vehicle-human safety interaction model is proposed to comprehensively understand and address the complex safety challenges in the environment around ICVs. The environment, vehicle, and humans interact, forming a complex system that collectively determines the system's safety. The field-vehicle-human

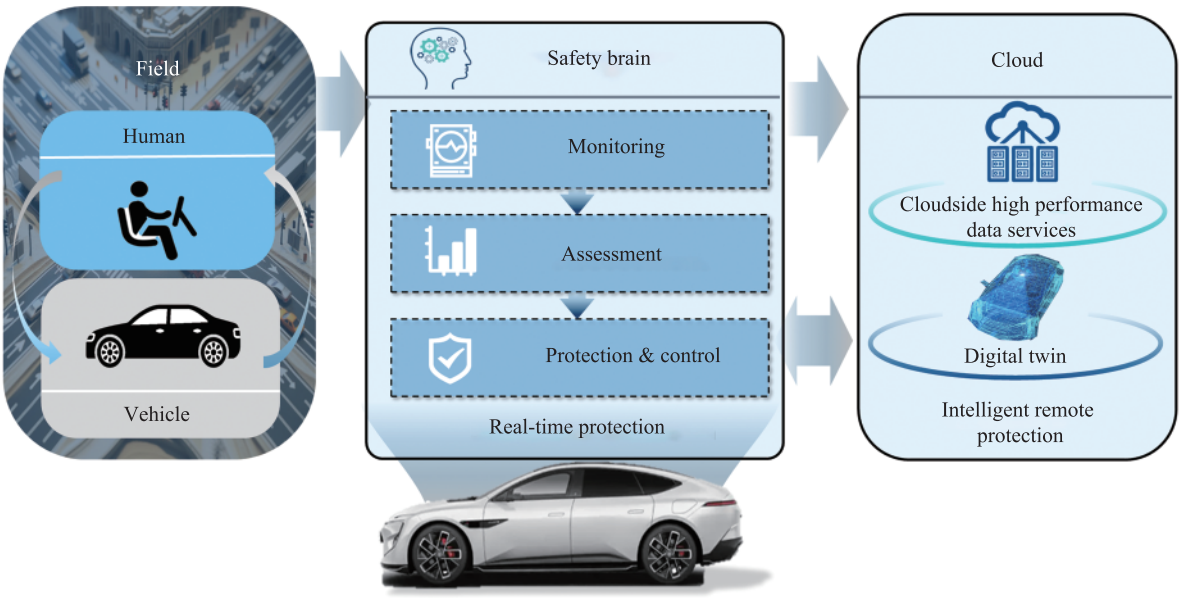

Figure 5 Fusion safety system framework.

model allows for a systematic analysis of the interactions between these three components, thereby more thoroughly identifying and addressing potential safety risks. As shown in Fig. 6, the field in the field-vehicle-human safety interaction model is divided into physical space and cyber space. Physical space includes the natural domain and the traffic domain, where the natural domain encompasses natural environments like weather, climate, and lighting, and the traffic domain includes traffic elements such as infrastructure, traffic signals, traffic flow, and road conditions [141]. Cyber space is categorized into near-field and far-field communication domains based on communication distance, where the local communication domain [142] primarily refers to the information domain created through short-distance communication methods such as V2X and mobile communication with the vehicle, and the global communication domain refers to the information domain that involves long-distance data exchange with the vehicle through satellite communication. Physical space and cyber space, surrounding the microsystem of vehicles and humans, collectively form a macro-system for safety interaction.

In the field-vehicle-human safety interaction theory, safety risks are considered due to the system state, which we define as "Safety Potential Energy". This concept draws from the idea of potential energy in physics, which describes the likelihood and severity of potential safety risks in a given system state. The level of Safety Potential Energy depends on the interaction of various factors, specifically in the physical space through "energy" transformations representing interactions [143] and in the cyber space through data exchange representing the influence between different elements. Both energy transformation and data exchange affect the system's state, influencing changes in safety potential energy. If the safety potential energy exceeds the safety margin of the system under study, safety risks may evolve into hazardous events, leading to systemic safety collapse. In the field-vehicle-human safety interaction model, the vehicle and human form an intelligent entity capable of cognition, decision-making, and action, considered as the microsystem in field-vehicle-human, with the surrounding field forming the macro-system. The macro-system and microsystem interact through energy transformation and data exchange. Within the microsystem, the interaction between vehicles and humans is reflected in the complementary role in driving tasks, with human attributes divided into personal, intrinsic, and extrinsic characteristics. Personal characteristics include age, gender, race, etc.; intrinsic characteristics cover physiological and psychological features like reaction ability, cognitive ability, attention, etc.; extrinsic characteristics represent driving takeover ability, decision-making ability, driving style, etc., directly influencing vehicle-human interaction. In

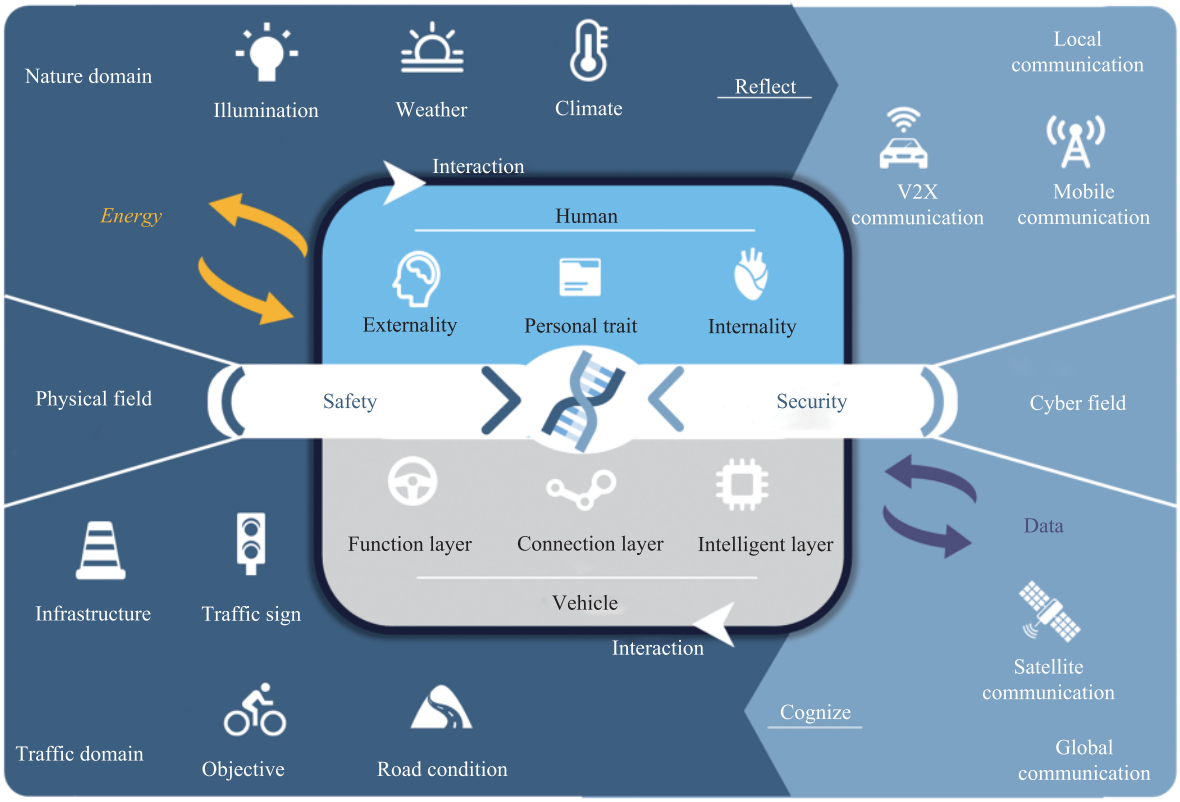

Figure 6 Field-vehicle-human safety interaction model.

terms of the vehicle, it is divided into three levels: the functional layer, including basic functional modules such as the power system, steering system, and braking system; the intelligent layer, including advanced functional modules like the intelligent cockpit and ADAS system [144]; and the connectivity layer, consisting of the vehicular network made up of CAN/FD, LIN, Ethernet, etc. [145], responsible for data transmission between different layers.

4.2.2 "Safety brain" system

Monitoring module. The "Monitoring" module integrates various sensory methods such as vision, hearing, and touch to monitor and assess the safety risks of ICVs comprehensively. It considers unsafe factors caused by natural environments, such as adverse weather conditions [146], potential risks in traffic conditions, such as congestion and accident-prone areas, and safety hazards that may arise during vehicle-cloud communication (Fig. 7). Additionally, the module focuses on the safety state of the vehicle itself, including the reliability of the vehicle's essential systems, the performance of advanced intelligent systems, and the security of onboard network communications. The status of drivers and passengers, including their behavioral intentions [147] and potential erroneous operations, are also crucial monitoring points as they significantly impact vehicle safety. By real-time monitoring and analysis of this multifaceted information, the module comprehensively perceives potential threats, monitors global safety risks, and provides information support to other parts of the system to ensure safe vehicle operation.

Assessment module. The "Assessment" module, building upon the risk information provided by the "Monitoring" module, further identifies and analyzes sources of safety risks, including unsafe conditions in the field, unsafe states of the vehicle, and unsafe behaviors of humans (Fig. 8). The unsafe conditions in the field encompass severe weather in the natural domain, intricate traffic scenarios in the traffic domain, and either packet loss of vital traffic information or cyber-attacks in the informational domain. Concerning the vehicle, unsafe states arise from malfunctions at the function layer, connectivity disruptions at the

communication layer, and performance insufficiencies at the intelligence layer. Beyond mere misuse related to SOTIF, human unsafe behaviors extend to disregarding safety alerts, thereby increasing the risk to functional safety and engaging in actions threatening cybersecurity, such as connecting virus-infected devices to the vehicle. It conducts an in-depth analysis of safety risks due to functional failure [148], SOTIF risks, and cybersecurity risks from network attacks. This module is not limited to assessing individual safety risks but also considers the occurrence of multiple safety risks simultaneously to evaluate potential safety risks comprehensively. After separately assessing the three categories of safety risks, it conducts a joint analysis of the concurrent multiple safety risks and their composite harmful impacts, revealing their potential interplay and combined effects. Combining the vehicle's level of safety risk response capability, it quantitatively assesses the vehicle's Fusion Safety risk state.

Prevention and control module. Based on the results from the "Assessment" module (Fig. 9), the "Prevention and Control" module addresses various identified safety protection needs, including protection against functional failure, performance degradation, and network attack safety protection [149]. It solves strategies within the designed safety strategy space, generating a tiered combination of safety protection strategies (Strategy Portfolio). This module elevates traditional singular protective measures to a more comprehensive defensive level, transitioning from passive to active adaptive protection, thus constructing a safety prevention and control system that is in-depth, highly adaptive, and integrates multiple safety measures. The core of this module lies in its ability not only to respond precisely to a specific category of safety risk but also to dynamically adjust protection strategies in real-time according to various compound safety protection needs, adapting to the ever-changing safety environment. This comprehensive approach to safety prevention and control enhances the vehicle system's ability to withstand safety risks and strengthens the safety resilience of the entire macro-traffic system.

4.2.3 Edge-cloud collaboration

In the safety protection system of ICVs, digital twin technology plays a key role [150]. Digital twins create a virtual model of a physical entity in the cloud, simulating the system interrelations and risk evolution mechanisms of the actual physical space world. Advanced data exchange protocols and real-time data

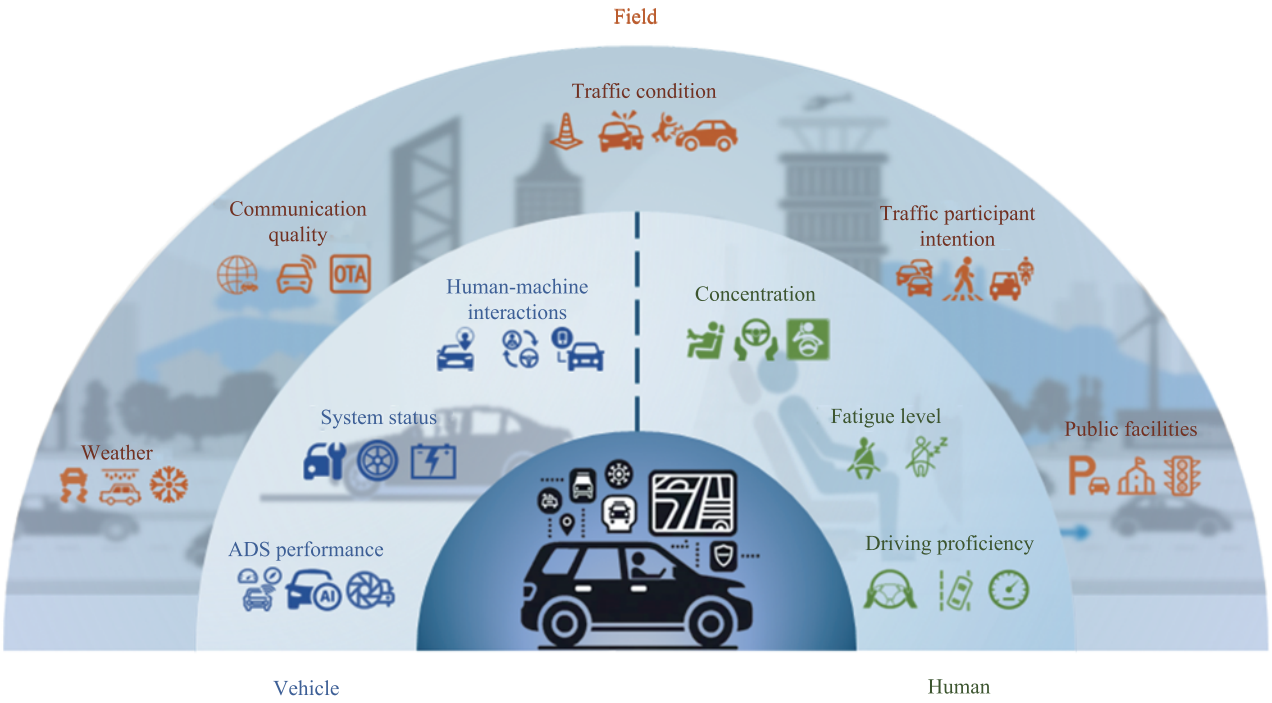

Figure 7 Monitoring module of the safety brain.

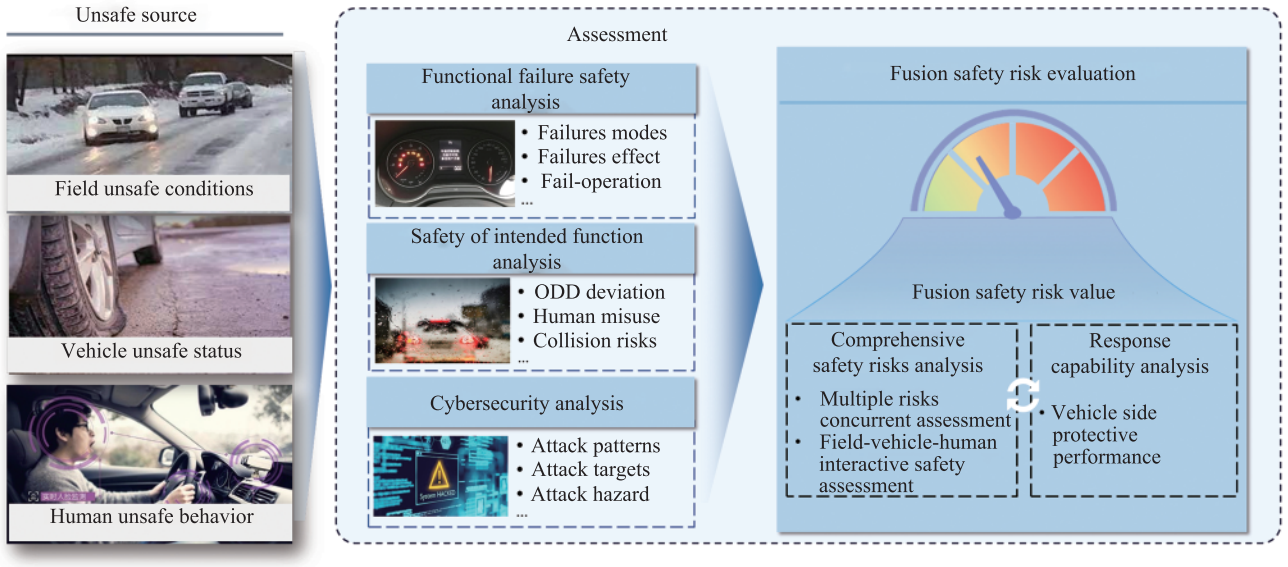

Figure 8 Assessment module of the safety brain.

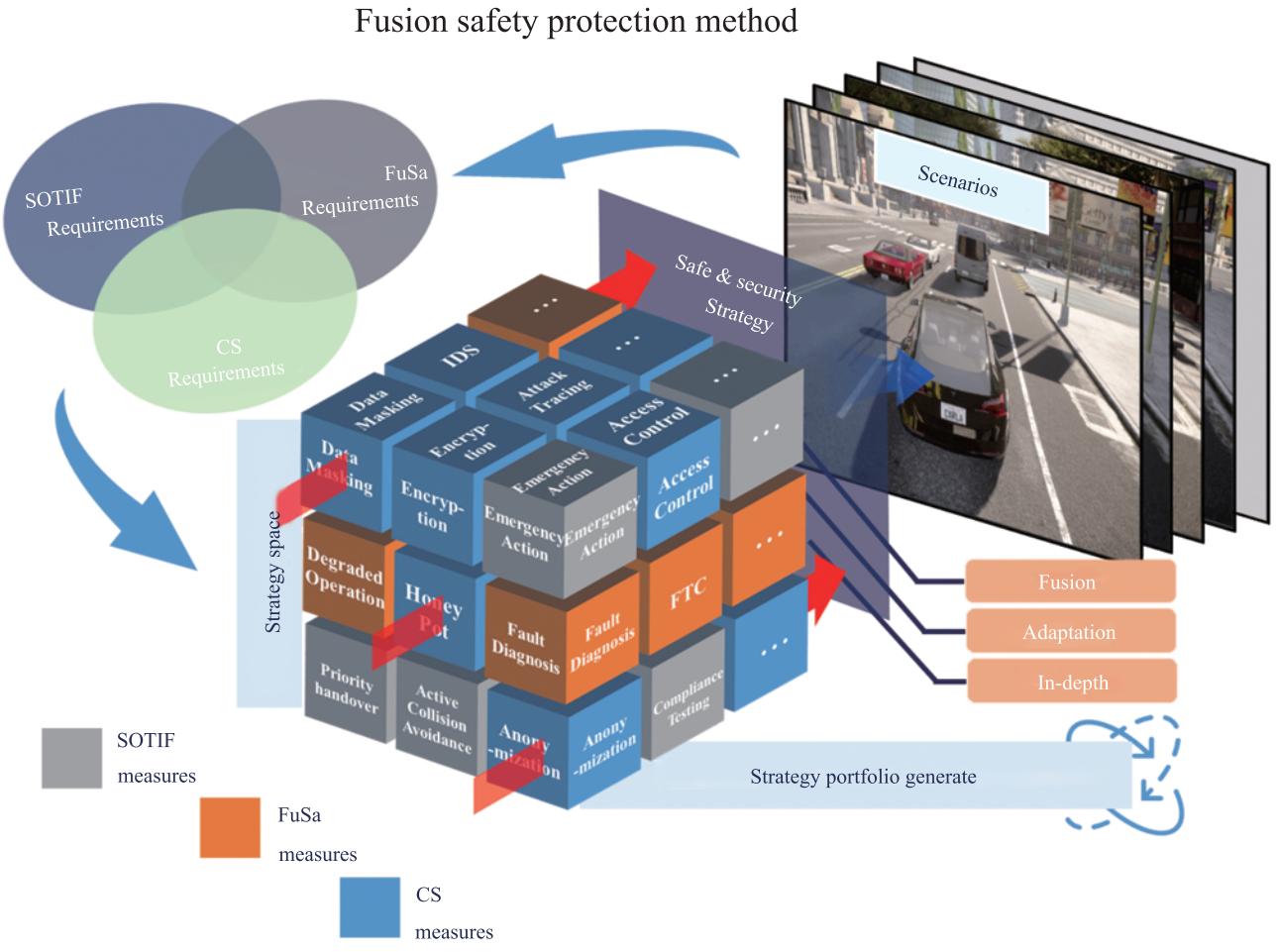

Figure 9 Protection & control module of the safe brain.

processing frameworks are employed for real-time data synchronization between the physical entity and its virtual model. This framework encompasses immediate collection and transmission of vehicle data,

ensuring timeliness and accuracy. In this manner, data is efficiently obtained from the vehicle's sensing system, including but not limited to speed, location, and environmental information. After immediate processing, the real-time collected data, including data cleaning, normalization, and feature extraction, is used for real-time monitoring of vehicle performance and predicting safety states. Additionally, when potential safety risks are detected as uncontrollable, the cloud can perform remote diagnostics and intervention through the digital twin model and even remotely control the vehicle in emergencies to prevent accidents [151]. Recording high-risk safety-critical scenarios and analyzing synchronized data makes it possible to trace and analyze the scenarios of safety incidents, infer the causes of safety risks, and thereby provide a basis for optimizing future preventive measures. Combining historical data with real-time monitoring data, the cloud collaboration platform can deduce optimal safety strategies through algorithms based on large-model analysis and, through OTA (Over-The-Air) technology, continuously optimize these strategies on the vehicle edge to adapt to the ever-changing driving environment and conditions.

Through edge-cloud collaboration (Fig. 10), the "Safety Brain" system leverages the complementary advantages of both the vehicle-edge and cloud systems. The vehicle edge focuses on real-time data collection and rapid response, while the cloud provides robust data storage, analysis capabilities, and superior computational power [152]. The protection system can execute highly real-time monitoring and protection while possessing the ability to self-evolve through learning and experience accumulation. This dual functionality ensures that the system can react to immediate risks and address new safety challenges through self-iteration and continuous learning.

4.3 X-shaped fusion safety development process

4.3.1 Fusion safety development process

In the era of traditional fuel vehicles, the development cycle of a vehicle product typically spanned 5 to 6 years, with German brands taking about 5 to 7 years, while Japanese brands reduced this cycle to about four years by introducing parallel development models [153]. Entering the era of new energy vehicles, this development cycle has been further shortened to approximately 36 months. Some new automotive manufacturers have even reduced this period to 9 to 12 months. As the automotive industry fully enters the era of ICVs, development cycles are expected to compress further. On the other hand, the diversity and variability of user demands necessitate a focus on continuous iteration and rapid updating of in-vehicle product development to promptly meet customer needs [154]. Shorter development cycles and rapid functional iterations inevitably lead to insufficient safety testing and validation time, thereby increasing safety risks. In the rapid iteration and upgrading of ICVs, a major challenge in safety design and development is effectively addressing unknown or insufficiently understood scenarios [155]. Scenarios not considered during design and encountered during operation can lead to new safety issues, necessitating swift responses and timely functional upgrades.

Currently, the mainstream development model adopted in automotive electronics and electrical systems development is the V-model, with the left side of the V representing the design phase and the right side representing the testing phase [156]. The V-model delineates different software development and testing stages with well-defined documents and test cases. However, its relative rigidity and linearity pose challenges in dealing with changes and flexibility [157]. Additionally, the sequential execution model of the V-model leads to extended delivery cycles, failing to meet the demands for rapid delivery and continuous iteration of ICVs. Since all testing is concentrated in the latter stages of the project, issues identified during testing are complex to rectify promptly, increasing the risk of delays. The linear structure of the V-model is not flexible enough to rapidly deliver and iterate in response to frequently changing requirements.

In the software development field, new development processes like CI/CD (Continuous Integration/Continuous Delivery) have emerged [158]. CI/CD, by automating code integration and deployment, enhances software delivery speed and quality, but its automated processes may introduce potential security risks that require appropriate safeguards. Containerized

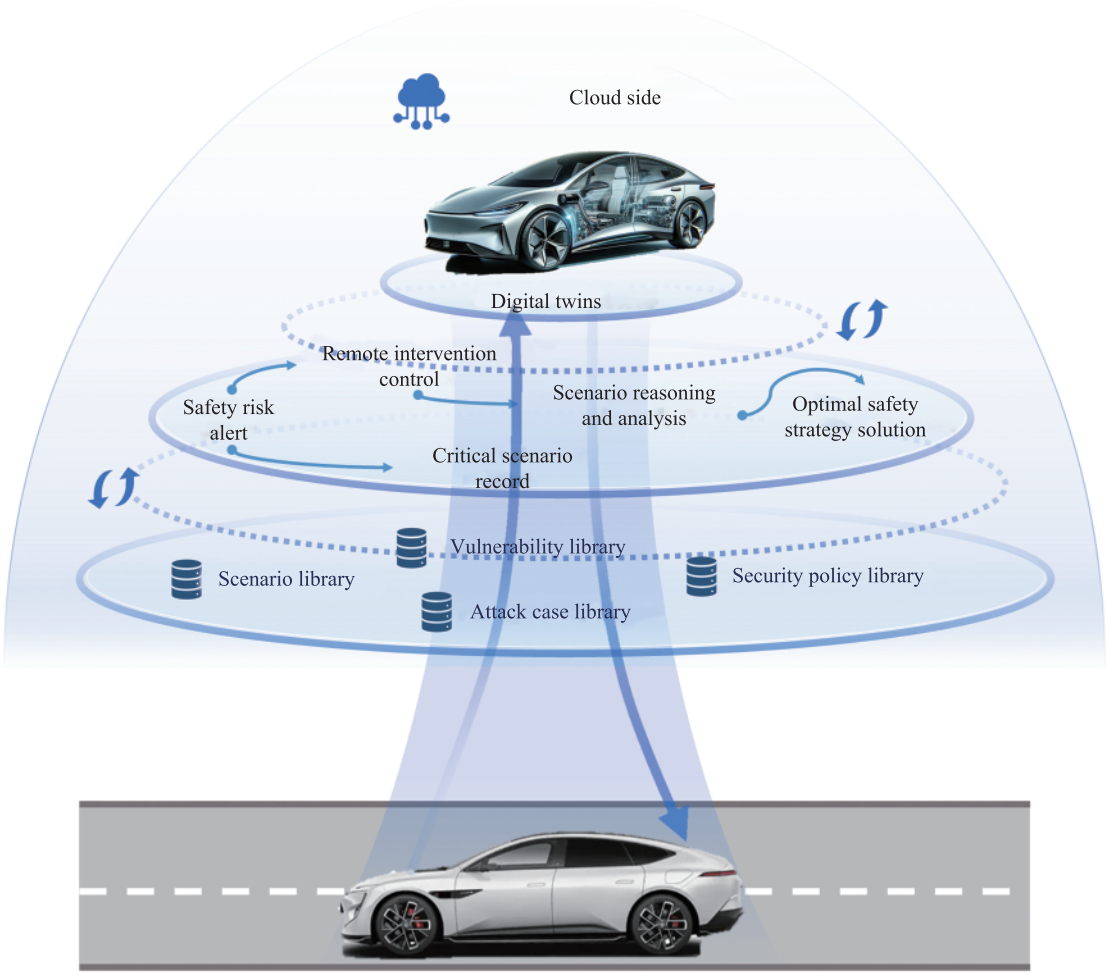

Figure 10 End-to-cloud collaboration for fusion safety system.

development processes use container technology (such as Docker) [159] to package applications and their dependencies into portable containers, thereby improving development, testing, and deployment consistency and efficiency. However, in containerized environments, isolation between containers is achieved through the container runtime and operating system. Despite many security measures, improper configuration can lead to security vulnerabilities between containers. Moreover, if a component in a containerized environment fails, it can impact the availability of the entire application.

A comprehensive analysis reveals that traditional development processes like the V-model, with their rigid workflows, lack sufficient speed and continuous integration capabilities to meet the rapid and changing development needs of ICVs. New development processes in the software field, while enabling rapid delivery, struggle to ensure product safety and reliability. A new type of safety design and development process is urgently needed to meet the new challenges of ICV safety and fulfill the demands of Fusion Safety, encompassing functional safety, cybersecurity, and SOTIF. This paper proposes an X-shaped development process based on CHAIN, as shown in Fig. 11.

The CHAIN architecture is presented as one of the digital solutions to the interconnection of open complex giant systems [6, 7]. As an interactive multi-layer collaborative network architecture, CHAIN possesses powerful generalization capabilities and universality in facing complex dynamic system challenges, enabling the design, development, rapid deployment, and system iteration of ICVs' Fusion Safety.

The X-shaped development process integrates physical space and cyber space development processes, retaining the traditional V-model while mapping

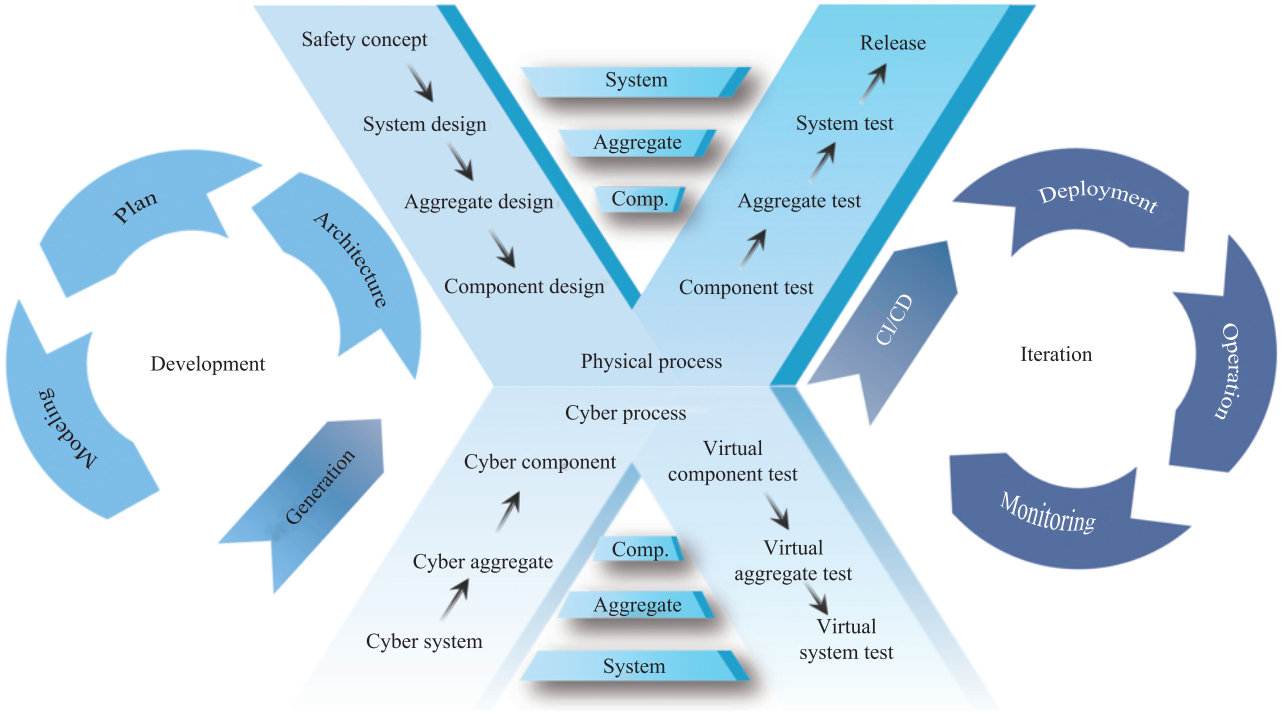

Figure 11 X-shaped fusion safety development process.

complex design and development processes from physical space to cyber space based on digital twins. This approach accelerates product delivery while ensuring design development rigor and compliance. In the physical process, for system, integration, and component levels, the left side of its V-model includes system concept, system design, aggregate design, and component design. In contrast, the right side encompasses component testing, aggregate testing, system testing, and release. In the cyber space, cyber system, cyber aggregate, and cyber components construction are performed for elements according to physical space, followed by the creation of high-fidelity virtual testing environments.

The physical and cyber processes interact during the design and testing phases in the X-shaped development process, enhancing development efficiency and reliability. On the one hand, in the physical process, after completing the system requirements, design, aggregate design, and component design, it can directly connect to the testing process in the cyber space, conducting functional and performance validation of cyber components, cyber assemblies, and cyber systems; on the other hand, after constructing cyber systems, cyber assemblies, and cyber components in the cyber space, hardware-in-the-loop and whole vehicle-in-the-loop testing and validation can be directly conducted in the physical space. Interactive design and development across Physical and cyber spaces significantly improve the efficiency of the Fusion Safety development model. Additionally, cross-testing and validation across Physical and cyber spaces enhance system safety and reliability.

In the fusion safety design and development process, the importance of the system's overall development and iteration cannot be overlooked. In the design and development phase, comprehensive consideration of planning, modeling, generation, and architecture is required, followed by interaction between the physical and cyber processes to achieve safer and smarter development design. After the product release phase, it's still necessary to focus on product deployment, operation, and safety monitoring, as well as achieve continuous integration and delivery through CI/CD, supporting rapid iteration of product functions.

This paper innovatively proposes a CHAIN-based X-shaped fusion safety development process, as presented in Fig. 11. The X-shaped development process is an advanced safety design method for ICVs, mirroring and integrating the two V-models of physical

and cyber worlds through an interactive multi-layer collaborative network architecture. Combining digital twin and artificial intelligence technology, it achieves collaborative development between physical space and cyber space, effectively shortening development cycles and significantly improving the efficiency of Fusion Safety system development while enhancing system safety and reliability through cross-testing and validation in physical and cyber processes. The X-shaped development process has the following features:

(1) Digital Twin: The proposed fusion safety development model encompasses both the physical space and the cyber space, constructing a V-model in both parts and connecting the two processes, breaking through the two development workflows, and realizing interactive development between physical space and cyber space. Starting from the physical V process end, it not only points to the physical space testing end but also to the cyber space's testing end. Starting from the virtual development end of the cyber world, it can point to the virtual testing end of the cyber space and the actual physical world's testing end. By bridging the development processes of the physical space and the cyber space, the system's development time is considerably shortened, development and testing costs are reduced, and a large number of physical and simulation cross-tests further ensure system safety [160].

(2) Rapid Delivery and Continuous Iteration: The proposed fusion safety development process combines the characteristics of new development processes across disciplines, designing corresponding development processes on both the development and testing sides, ensuring rapid delivery and continuous iteration. On the development side, from the system, aggregate, and component levels, a plan-modeling-generation-architecture development structure is designed, integrating the development processes of physical space and cyber space, and shortening the time cost of system development from an architectural perspective. On the testing side, considering the operation phase, a deployment-operation-monitoring-CI/CD iterative process is designed and integrated into the testing ends of Physical and cyber space, ensuring continuous iteration and upgrade after system release [161].

(3) Enhanced Safety: First, the process combines Physical and cyber space, allowing complex and costly design development and testing validation steps involved in functional safety, cybersecurity, and SOTIF to be directly conducted in cyber space. Additionally, digital twins can expand and enrich edge scenarios and new attack types and reduce safety risks due to difficulties obtaining test samples and insufficient testing validation. In addition, the proposed fusion safety development process incorporates the traditional V-model [162], ensuring the rigor and completeness of the development process. The fusion safety development model, in both the physical space and the cyber space, is based on the V process architecture, with each stage having clearly defined tasks and objectives. Clear stage divisions clarify the tasks and roles of each stage, ensuring system safety and security [163]. Since the V-model requires establishing clear links between the design and testing phases, issues can be discovered and fixed early in the development process, reducing the cost of finding issues in later stages. Moreover, the traditional single-dimensionality safety development process cannot satisfy the rapid development of ICVs. In contrast, the three types of safety in the X-shaped development process are coupled in models, data, and scenarios at each stage. Developing and designing according to the X-shaped development process can address some fusion safety issues.

(4) Intelligence: The proposed fusion safety development architecture adopts a digital twin development process that integrates physical space with cyber space. In cyber space, the latest deep-learning algorithms can be modularly integrated. By cleaning and analyzing vast amounts of system data and extracting core features, targeted models for cyber systems, aggregates, and components are constructed, ensuring high fidelity of test and validation in cyberspace. Additionally, generative AI algorithms can be applied to generate many simulation test cases specifically for different scenarios, creating comprehensive testing strategies to test and verify the functionality of cyber components, aggregates and systems. Furthermore, the X-shaped development process adopts an automated development process throughout the entire development and

iteration cycles, enhancing development efficiency significantly.

The new safety development architecture proposed in this paper, while designed for ICVs, also has application value and significance in other domains. For example, in the context of web applications, mobile applications, and embedded systems, adopting this new safety development architecture can ensure system safety and reliability while shortening the delivery cycles and achieving rapid iteration. Additionally, the proposed new safety development architecture is not limited by project scale and is applicable to development processes for projects of various sizes. This new safety development process allows new safety components or modules to be expanded according to different development needs, offering substantial flexibility to other development projects. Each safety component within it is relatively independent and replaceable, allowing for modifications or replacements according to specific requirements. Moreover, this new safety development architecture can be easily integrated into different development tools and integrated development environments (IDEs), supporting new extensions to various development luggage and requirements.

4.3.2 AI-enabled fusion safety development process

Artificial intelligence applications provide a powerful development tool for the fusion safety development process. For instance, AI can be used for automated business analysis, scientifically planning project schedules, accurately assessing development progress, optimizing resource allocation, and balancing development time [164]. In empowering the fusion safety development model, as shown in Fig. 12, AI is mainly reflected in the following aspects.

In database construction, AI can automatically collect, store, and utilize data from various sources, including driving scenario databases, safety event databases, vehicle malfunction databases, driver behavior databases, and user feedback databases [165]. AI facilitates the mining of interrelated features between databases, further summarizing development laws. AI has advantages in data anonymization and encryption, strengthening user privacy and data security [166]. Through Natural Language Processing (NLP), AI can extract essential user requirements and accurately depict user profiles, thereby enhancing the directionality and effectiveness of product development.

In modeling fusion safety development architecture, AI automatically creates and updates views of large and complex models, aiding developers in better understanding and analyzing the structure and internal mechanisms of the fusion safety system. With automated vulnerability mining, AI can uncover potential security risks in the architecture, identify the root causes of risks, and determine appropriate safety measures. During model creation, AI can rapidly auto-generate model code [167], reducing development time and minimizing the risk of human errors.

In terms of testing and validation, AI can automate repetitive testing tasks such as functional testing, performance testing, and regression testing, thereby improving testing efficiency and coverage. By analyzing historical test data and identifying critical issues in the testing process, AI helps develop more effective testing strategies [168]. With extensive safety events and data, AI technology can automate the generation of test cases for critical scenarios, enhancing the efficiency of system testing and validation. Additionally, AI's in-depth test results analysis can uncover security vulnerabilities and update the system promptly to fix bugs, enhancing system safety.

To enhance the capability of ICVs in dealing with unknown scenarios in real-world operations, it's essential to ensure that the developed systems have continuous optimization capabilities to improve generalization performance in various new scenarios. In recent years, the concept of continual learning has been proposed in artificial intelligence [169]. Continual learning methods enable accumulating new knowledge from new data, tasks, or environments without significantly forgetting previously learned knowledge. Integrating continual learning with the X-shaped development process can help vehicles update the fusion safety model in real time, allowing vehicles to make safer decisions in new scenarios based on the constantly updated knowledge base. Additionally, continual learning ensures that models maintain high performance in complex dynamic environments, which is crucial for ICVs to address safety risks in physical space [170]. Therefore, by introducing continual learning methods into the

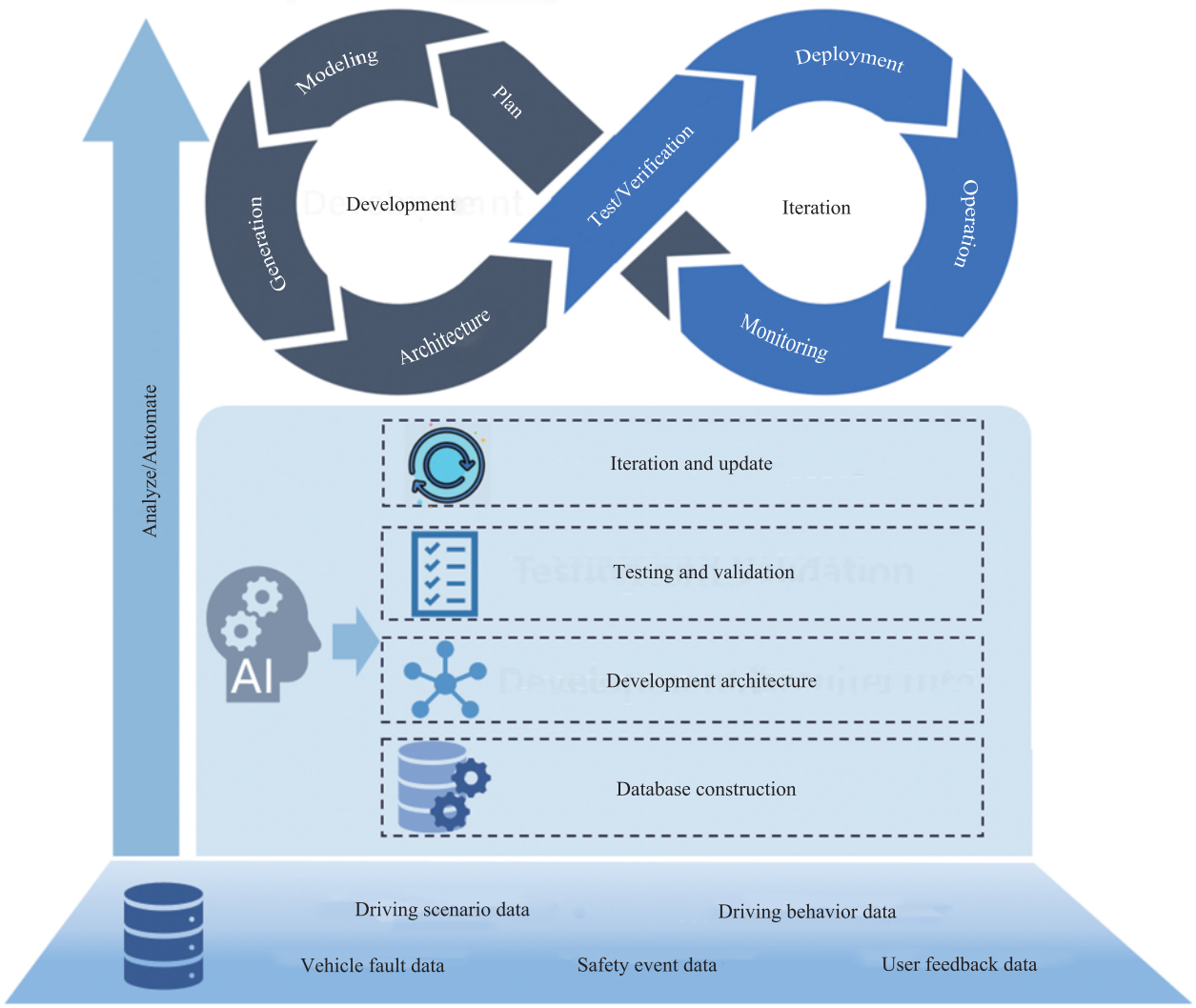

Figure 12 AI-enabled development process.

X-shaped development process, the self-optimization ability of ICV systems is enhanced, improving vehicle safety in unknown and complex scenarios to meet new requirements of functional safety, cybersecurity, and SOTIF.

5 Conclusions and perspectives

In summary, this paper firstly reviews the current issues and challenges of functional safety, cybersecurity, and SOTIF for ICVs. Then, the existing safety assessment, protection, and testing methods are summarized, and the limitations are also analyzed. Further, this paper proposes a fusion safety systematic framework based on CHAIN and introduces the concept of fusion safety, which is not only a technical merger but also involves the merge of four levels: process, toolchains, value, and information. Based on the concept of fusion safety, this paper further proposes a fusion safety protection framework for ICVs based on the field-vehicle-human safety interaction model and end-cloud collaboration, which systematically defines the future development direction of safety protection for ICVs. Innovatively, a CHAIN-based X-shaped fusion safety development process is presented, enabling the interaction between physical entities and digital twin models to meet the needs of ICV safety design, intelligent development, rapid delivery, and continuous iteration.

Based on the fusion safety concept, fusion safety protection system framework, and X-shaped fusion safety development process proposed in this paper, the safety ecology of ICVs can be further constructed. In

terms of hardware, various components such as chips, sensors, and actuators play a vital role in intelligent and internet-connected systems. These elements could be designed and developed based on fusion safety principles at the element level to contribute to the development of a foundational safety hardware platform, which serves as the foundation for vehicle-level safety. Additionally, by implementing fusion safety design and development at various vehicle system levels, Fusion Safety can be integrated into the entire automotive industry, thus forming a comprehensive ecological component supply chain. In terms of software, the operating system, basic software, and automotive development toolchain involved in the X-shaped fusion safety development process are crucial elements that will facilitate the creation of an integrated safety software development platform. The operating system provides a stable and safe foundation, ensuring application reliability and efficiency. Basic software acts as the middle layer, offering essential services and libraries. The automotive development toolchain, tailored specifically for the demands of ICVs, streamlines the entire development process from coding to testing.

This approach aims to construct a comprehensive and reliable safety protection system for ICVs from an industry-wide perspective, thereby enhancing the vehicles' ability to respond to safety risks and supporting the mass commercialization of ICVs. The fusion safety concept, fusion safety protection system framework, and X-shaped fusion safety development process can be further applied to intelligent transportation vehicles and systems.

References

[1] Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (European Commission), and European Commission, "Commission implementing regulation (EU)," Accessed: Mar. 1, 2024 [Online]. Available: http://data.europa.eu/eli/reg_impl/2022/1426/oj(Accessed in March, 2024).

[2] Federal Ministry for Digital and Transport, "Germany will be the world leader in autonomous driving," Accessed: Mar. 1, 2023 [Online]. Available: https://bmdv.bund.de/SharedDocs/EN/Articles/DG/act-on-autonomous-driving.html.

[3] NHTSA, "NHTSA issues first-ever proposal to modernize occupant protection safety standards for vehicles without manual controls," Accessed: Mar. 1, 2023 [Online]. Available: https://www.nhtsa.gov/press-releases/nhtsa-issues-first-ever-proposal-modernize-occupant-protection-safety-standards.

[4] European Union, "Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles (Text with EEA relevance)," Accessed: Mar. 1, 2023 [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/94bfefa8-24e9-11ed-8fa0-01aa75ed71a1.

[5] Ministry of Transport of the People's Republic of China, "Notice of the General Office of the Ministry of Transport on the issuance of the *Guide for Safety Services of Autonomous Vehicle Transport* (Trial Version)," Accessed: Mar. 1, 2023 [Online]. Available: https://xxgk.mot.gov.cn/jigou/ysfws/202312/t20231205_3962490.html.

[6] S. Yang, Z. Zhang, L. Zhang, H. Yu, K. Yang, and X. Liu, "CHAIN: Cyber hierarchy and interactional network," *Etransportation*, vol. 17, p. 100256, 2023.

[7] S. Yang, R. He, Z. Zhang, Y. Cao, X. Gao, and X. Liu, "CHAIN: Cyber hierarchy and interactional network enabling digital solution for battery full-lifespan management," *Matter*, vol. 3, no. 1, pp. 27–41, 2020.

[8] W. Deng, "Electrification and intelligent technology: The driving force of the future vehicle," *Journal of Automotive Safety and Energy Efficiency*, vol. 1, no. 3, pp.179–189, 2010.

[9] International Organization for Standardization, "ISO 26262:2018 (en) road vehicles–Functional safety," Accessed: Mar. 1, 2023 [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:iso:26262:-1:ed-2:v1:en.

[10] H. Y. Ji, S. C. Cui, C. Sun, and J. M. Zhang, "Understanding of vehicles functional safety development process based on ISO 26262," *Auto Electric Parts*, no. 7, pp. 57–59, 2016.

[11] W. Cao, Z. Zhu, J. Nan, X. Zhang, Y. Zou, and Y. Cui, "Combined LKA and DYC control for electric vehicle with a domain- centralized E/E architecture based on software-defined networking," *IEEE Transactions on Transportation Electrification*, in press, doi: 10.1109/TTE.2023.3320262.

[12] I. Llatser, A. Geraldy, G. Jornod, and Y. Yang, "Poster: Safe V2X communication for cooperative automated driving," 2023 IEEE Vehicular Networking Conference (VNC), Istanbul, Turkiye, 2023, pp. 163–164.

[13] A. Corso, R. Moss, M. Koren, R. Lee, and M. Kochenderfer, "A survey of algorithms for black-box safety validation of cyber-physical systems," *Journal of Artificial Intelligence Research*, vol. 72, pp. 377–428, 2021.

[14] J. Wang, Y. Li, Z. Zhou, C. Wang, Y. Hou, L. Zhang, X. Xue, M. Kamp, X. Zhang, and S. Che, "When, where and how does it fail? A spatial-temporal visual analytics approach for interpretable object detection in autonomous driving," *IEEE Transactions on Visualization and Computer Graphics*, vol. 29, no. 12, pp. 5033–5049, 2022.

[15] G. Qin, X. H. Dong, L. Yang, W. Wang, Y. Xu, and Y. Wang, "Research on secure FOTA upgrade method for intelligent connected vehicle based on new domain controller architecture," International Conference on Computer Communication and Network Security, Hohhot, China, 2022.

[16] A. Benslimane and J. Liu, *Intelligent and Connected Vehicle Security*, New York: River Publishers, 2022.

[17] P. Leijen and N. Kularatna, "Developing a monitoring system for Toyota Prius battery-packs for longer term performance issues," 2013 IEEE International Symposium on Industrial Electronics, Taipei, 2013, pp. 1–6.

[18] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive ethernet-based networks," *Vehicular Communications*, vol. 29, no. 100338, 2021.

[19] Upstream, "Automotive Cybersecurity & Data Management," Accessed: Mar. 1, 2023 [Online]. Available: https://upstream.auto/.

[20] C. Valasek and C. Miller, "Who's behind the wheel? Exposing the vulnerabilities and risks of high tech vehicles," Accessed: Mar. 1, 2023 [Online]. Available: https://trid.trb.org/view/1370158.

[21] S. S. Albouq and E. M. Fredericks, "Lightweight detection and isolation of black hole attacks in connected vehicles," 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, USA, 2017, pp. 97–104.

[22] J. Ying, Y. H. Feng, Q. A. Chen, and Z. Mao, "GPS spoofing attack detection on intersection movement assist using one-class classification," ISOC Symposium on Vehicle Security and Privacy (VehicleSec), San Diego, USA, 2023, pp. 1–8.

[23] S. Brady, "Tesla data breach affecting 75k people was 'inside job'," Accessed: Mar. 1, 2023 [Online]. Available:https://www.just-auto.com/news/tesla-data-breach-affecting-75k-people-was-inside-job/.

[24] J. Coker, "Toyota reveals data leak of 300,000 customers," https://www.infosecurity-magazine.com/news/toyota-data-leak-customers/(Accessed in March, 2024).

[25] J. W. Sun, T. W. Zhang, X. F. Xie, L. Ma, Y. Zheng, K. J. Chen, and Y. Liu, "Stealthy and efficient adversarial attacks against deep reinforcement learning," The Thirty-Fourth AAAI Conference on Artificial Intelligence, New York, USA, 2020, pp. 5883–5891.

[26] S. A. Abdelhameed, S. M. Moussa, N. L. Badr, and M. E. Khalifa, "The generic framework of privacy preserving data mining phases: Challenges & future directions," 2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt, 2021, pp. 341–347.

[27] T. Skibik, A. P. Vinod, A. Weiss, and S. Di Cairano, "MPC with integrated evasive maneuvers for failure-safe automated driving," 2023 American Control Conference (ACC), San Diego, CA, USA, 2023, pp. 1122–1128.

[28] A. Palffy, J. F. Kooij, and D. M. Gavril, "Detecting darting out pedestrians with occlusion aware sensor fusion of radar and stereo camera," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1459–1472, 2022.

[29] Carsales, "Volvo recalls 750,000 cars over AEB fault," Accessed: Mar. 1, 2023 [Online]. Available: https://www.carsales.com.au/editorial/details/volvo-recalls-750000-cars-over-aeb-fault-123425/.

[30] International Organization for Standardization, "The categories of ISO 13849-1," Accessed: Mar. 1, 2023 [Online]. Available: https://www.byhon.it/the-categories-for-iso-13849/.

[31] T. Munaro and I. Muntean, "Early assessment of system-level safety mechanisms through co-simulation-based fault injection," 2022 IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany, 2022, pp. 1703–1708.

[32] A. Peng, A. Netanyahu, M. K. Ho, T. Shu, A. Bobu, J. Shah, and P. Agrawal, "Diagnosis, feedback, adaptation: A human-in-the-loop framework for test-time policy adaptation," in Proceedings of the 40th International Conference on Machine Learning, Honolulu, Hawaii, 2023, pp. 27630–27641.

[33] N. Gerlin, E. Kaja, F. Vargas, L. Lu, A. Breitenreiter, J. C. Chen, M. Ulbricht, M. Gomez, A. Tahiraga, and S. Prebeck, "Bits, flips and RISCs," 2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), Tallinn, Estonia, 2023, pp. 140–149.

[34] X. Zhang, J. Tao, K. Tan, M. Töngren, J. M. G. Sanchez, M. R. Ramli, X. Tao, M. Gyllenhammar, F. Wotawa, N. Mohan, M. Nica, and H. Felbinger, "Finding critical scenarios for automated driving systems: A systematic mapping study," *IEEE Transactions on Software Engineering*, vol. 49, no. 3, pp. 991–1026, 2022.

[35] A. Adee, R. Gansch, and P. Liggesmeyer, "Systematic modeling approach for environmental perception limitations in automated driving," 2021 17th European Dependable Computing Conference (EDCC), Munich, Germany, 2021, pp. 103–110.

[36] J. De Villiers, G. Pavlin, A. Jousselme, S. Maskell, A. De Waal, K. Laskey, E. Blasch, and P. Cost, "Uncertainty representation and evaluation for modeling and decision-making in information fusion," *Journal for Advances in Information*

Fusion, vol. 13, no. 2, pp. 198–215, 2018.

[37] G. Pappalardo, R. Caponetto, R. Varrica, and S. Cafiso, "Assessing the operational design domain of lane support system for automated vehicles in different weather and road conditions," *Journal of Traffic and Transportation Engineering (English Edition)*, vol. 9, no. 4, pp. 631–644, 2022.

[38] T. Hirose, T. Sawaragi, H. Nomoto, and Y. Michiur, "Functional safety analysis of SAE conditional driving automation in time-critical situations and proposals for its feasibility," *Cognition, Technology & Work*, vol. 23, no. 4, pp. 639–657, 2021.

[39] X. Zhao, J. Sun, and M. Wang, "Measuring sociality in driving interaction," arXiv preprint arXiv:2306.13992, 2023, DOI: 10.48550/arXiv.2306.13992.

[40] M. Klischat, E. I. Liu, F. Holtke, and M. Althoff, "Scenario factory: Creating safety-critical traffic scenarios for automated vehicles," 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 2020, pp. 1–7.

[41] Y. Forster, F. Naujoks, and A. Keinath, "How many participants are required for validation of automated vehicle interfaces in user studies," *Information*, vol. 12, no. 10, pp. 410, 2021.

[42] K. Madala and M. Solmaz, *Scenario-Based Risk Quantification Approach for Assuring Safety in Autonomous Vehicles*, Illinois: SAE, 2023.

[43] D. Katare, D. Perino, J. Nurmi, M. Warnier, M. Janssen, and A. Y. Ding, "A survey on approximate edge AI for energy efficient autonomous driving services," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2714–2754, 2023.

[44] Z. T. Xu, R. Y. Wang, G. Balaji, M. Bundele, X. F. Liu, L. Liu, and T. Wang, "AlerTiger: Deep learning for AI model health monitoring at LinkedIn," in Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, New York, NY, United States, 2023, pp. 5350–5359.

[45] V. Negri, A. Mingotti, R. Tinarelli, and L. Peretto, "Uncertainty and lack of information affecting the training of machine learning algorithms for fault prediction of cable-Joints," 2023 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Kuala Lumpur, Malaysia, 2023, pp. 1–5.

[46] L. Zhang, Q. Zhang, L. Shen, B. Yuan, X. Wang, and D. Tao, "Evaluating model-free reinforcement learning toward safety-critical tasks," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 12, pp. 15313–15321, 2023.

[47] K. C. Han, P. S. Bo, and U. Michiel, *A Study on Estimation Tool of Occupant Injury Risk for Deriving Integrated Safety Scenarios*, Illinois: SAE, 2023.

[48] T. Terzimehić, S. Barner, Y. G. Dantas, U. Schöpp, V. Nigam, and P. Ke, "Safety-aware deployment synthesis and trade-off analysis of Apollo autonomous driving platform," 2023 IEEE 20th International Conference on Software Architecture Companion (ICSA-C), L'Aquila, Italy, 2023, pp. 309–316.

[49] A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "An overview of safety and security analysis frameworks for the internet of things," *Electronics*, vol. 12, no. 14, p. 3086, 2023.

[50] B. Li, Y. Fu, S. L. Shang, Z. Z. Li, J. F. Zhao, and B. Wang, "Research on functional safety of battery management system (BMS) for electric vehicles," 2021 International Conference on Intelligent Computing, Automation and Applications (ICAA), Nanjing, China, 2021, pp. 267–270.

[51] B. Li, X. C. Wei, and Y. Fu, "Research on functional safety of drive motor system for electric vehicle," 2021 International Conference on Artificial Intelligence and Electromechanical Automation (AIEA), Guangzhou, China, 2021, pp. 84–87.

[52] M. Park, H. C. Koag, and H. S. Ahn, "Functional safety improvement of electric power steering system by using electronic stability control system," 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE), Cairns, QLD, Australia, 2018, pp. 230–234.

[53] S. Chung and H. Lee, "Estimating desired yaw rate and control strategy analysis on developed air ESC system for performance evaluation," 15th International Conference on Control, Automation and Systems (ICCAS), Busan, Korea (South), 2015, pp. 2005–2010.

[54] Y. Tao, Y. Z. Li, and Y. H. He, "Research on methods of wamings for ADAS safety design method based on AHP," 2021 6th International Conference on Transportation Information and Safety (ICTIS), Wuhan, China, 2021, pp. 1332–1337.

[55] M. Yadav, D. Shankar, and T. Jose, "Functional safety for braking system through ISO 26262, operating system security and DO 254," 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 2020, pp. 1–8.

[56] M. Šik and J. Křivánek, "Survey of Markov chain Monte Carlo methods in light transport simulation," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 4, pp. 1821–1840, 2018.

[57] G. Xie, G. Zeng, Y. Liu, J. Zhou, R. Li, and K. Li, "Fast functional safety verification for distributed automotive applications during early design phase," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 5, pp. 4378–4391, 2017.

[58] Z. Gu, G. Han, H. Zeng, and Q. Zhao, "Security-aware mapping and scheduling with hardware co-processors for

flexray-based distributed embedded systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 10, pp. 3044–3057, 2016.

[59] G. Xie, Y. Chen, Y. Liu, Y. Wei, R. Li, and K. Li, "Resource consumption cost minimization of reliable parallel applications on heterogeneous embedded systems," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 1629–1640, 2016.

[60] C. B. S. T. Molina, J. R. De Almeida, L. F. Vismari, R. I. R. Gonzalez, J. K. Naufal, and J. Camargo, "Assuring fully autonomous vehicles safety by design: The autonomous vehicle control (AVC) module strategy," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Denver, CO, USA, 2017, pp. 16–21.

[61] A. A. J. Zumalde, J. M. Secall, and J. B. C. Junior, "Comparative analysis on the impact of defensive programming techniques for safety-critical systems," 2009 Fourth Latin-American Symposium on Dependable Computing, Joao Pessoa, Paraiba, Brazil, 2009, pp. 95–102.

[62] K. Liu, X. Z. Zhang, W. Q. Kong, G. Hou, M. Watanabe, and A. Fukuda, "Interpolation-based multi-core bounded model checking of HSTM designs," 2019 6th International Conference on dependable systems and their applications (DSA), Harbin, China, 2020, pp. 25–36.

[63] A. Tashakori and M. Ektesabi, "Fault diagnosis of in-wheel BLDC motor drive for electric vehicle application," 2013 IEEE Intelligent Vehicles Symposium (IV), Gold Coast, QLD, Australia, 2013, pp. 925–930.

[64] H. Volos, "The case for replication-aware memory-error protection in disaggregated memory," *IEEE Computer Architecture Letters*, vol. 20, no. 2, pp. 130–133, 2021.

[65] S. Fürst and M. Bechter, "AUTOSAR for connected and autonomous vehicles: The AUTOSAR adaptive platform," 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), Toulouse, France, 2016, pp. 215–217.

[66] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459–474, 1990.

[67] K. Indu and M. Aswatha Kumar, "Electric vehicle control and driving safety systems: A review," *IETE Journal of Research*, vol. 69, no. 1, pp. 482–498, 2023.

[68] M. Singh and A. G. Shaik, "Incipient fault detection in stator windings of an induction motor using stockwell transform and SVM," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 12, pp. 9496–9504, 2020.

[69] D. Du and Z. Li, "Passive fault-tolerant control for discrete parameter system," *IET Power Electronics*, vol. 16, no. 12, pp. 1969–1983, 2023.

[70] Z. Hu, F. Zhang, and Z. Wei, "Research on fault tolerant strategy and reliability of steering-by-wire," *International Journal of Modeling and Optimization*, vol. 6, no. 2, pp. 106, 2016.

[71] C. Huang, F. Naghdy, and H. Du, "Fault tolerant sliding mode predictive control for uncertain steer-by-wire system," *IEEE Transactions on Cybernetics*, vol. 49, no. 1, pp. 261–272, 2017.

[72] Y. F. Wang, Y. Huang, and X. F. Han, "Research on verification method of safety integrity level based on Monte-Carlo," 2021 3rd International Symposium on Robotics & Intelligent Manufacturing Technology (ISRIMT), Changzhou, China, 2021, pp. 181–184.

[73] Y. Wang, Y. Wang, H. Qin, H. Ji, Y. Zhang, and J. Wang, "A systematic risk assessment framework of automotive cybersecurity," *Automotive Innovation*, vol. 4, pp. 253–261, 2021.

[74] T. Vogt, E. Spahovic, T. Doms, R. Seyer, H. Weiskirchner, K. Pollhammer, T. Raab, S. Rührup, M. Latzenhofer, C. Schmittner, M. Hofer, A. Bonitz, C. Kloibhofer, and S. Chlup, "A comprehensive risk management approach to information security in intelligent transport systems," *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 4, pp. 39–58, 2021.

[75] X. You, Y. Zhang, B. Li, X. Lv, and J. Han, "VDIF-M: Multi-label classification of vehicle defect information collection based on seq2seq Model," In: Y. Yin, Y. Li, H. Gao, J. Zhang, eds., *Mobile Computing, Applications, and Services*, Cham Switzerland: Springer, 2019.

[76] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *ACM Computing Surveys (CSUR*), vol. 51, no. 3, pp. 1–38, 2018.

[77] A. Alrawais, A. Alhothaily, B. Mei, T. Song, and X. Cheng, "An efficient revocation scheme for vehicular ad-hoc networks," *Procedia Computer Science*, vol. 129, pp. 312–318, 2018.

[78] S. Du and G. Ye, "IWT and RSA based asymmetric image encryption algorithm," *Alexandria Engineering Journal*, vol. 66, pp. 979–991, 2023.

[79] Z. H. Meng and Y. Wang, "Asymmetric encryption algorithms: Primitives and applications," 2022 IEEE 2nd International Conference on Electronic Technology, Communication and Information (ICETCI), Changchun, China, 2022, pp. 876–881.

[80] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[81] C. Zhang, X. Xue, L. Feng, X. Zeng, and J. M, "Group-signature and group session key combined safety message authentication protocol for VANETs," *IEEE Access*, vol. 7, pp. 178310–178320, 2019.

[82] H. Tan and I. Chung, "Secure authentication and key management with blockchain in VANETs," *IEEE Access*, vol. 8, pp. 2482–2498, 2019.

[83] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, "Subject review: Intrusion detection system (IDS) and intrusion prevention system (IPS)," *Global Journal of Engineering and Technology Advances*, vol. 14, no. 2, pp. 155–158, 2023.

[84] I. Naqvi, A. Chaudhary, and A. Kumar, "A systematic review of the intrusion detection techniques in VANETS," *TEM Journal*, vol. 11, no. 2, pp. 900–907, 2022.

[85] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud," *Vehicular Communications*, vol. 12, pp. 138–164, 2018.

[86] A. Tomandl, K. P. Fuchs, and H. Federrath, "REST-Net: A dynamic rule-based IDS for VANETs," 2014 7th IFIP Wireless and Mobile Networking Conference (WMNC), Vilamoura, Portugal, 2014, pp. 1–8.

[87] M. Anand, S. P. Kumar, M. Selvi, S. S. Kumar, G. D. Ram, and A. Kannan, "Deep learning model based IDS for detecting cyber attacks in IoT based smart vehicle network," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023.

[88] S. U. Sagong, R. Poovendran, and L. Bushnell, "Mitigating vulnerabilities of voltage-based intrusion detection systems in controller area networks," Arxiv Preprint Arxiv:1907.10783, 2019, DOI: 10.48550/arXiv.1907.10783.

[89] Y. Qi, G. Mai, R. Zhu, and M. Zhang, "EVKG: An interlinked and interoperable electric vehicle knowledge graph for smart transportation system," *Transactions in GIS*, vol. 27, no. 4, pp. 949–974, 2023.

[90] H. Ahmed, I. Traore, S. Saad, and M. Mamu, "Automated detection of unstructured context-dependent sensitive information using deep learning," *Internet of Things*, vol. 16, p. 100444, 2021.

[91] M. Ashraf, S. Rady, T. Abdelkader, and T. F. Gharib, "Efficient privacy preserving algorithms for hiding sensitive high utility itemsets," *Computers & Security*, vol. 132, p. 103360, 2023.

[92] L. Yu, L. Liu, and C. Pu, "Dynamic differential location privacy with personalized error bounds," NDSS '17, San Diego, USA, 2017, pp. 1–15.

[93] H. Y. Khdier, W. M. Jasim, and S. A. Aliesawi, "Deep learning algorithms based voiceprint recognition system in noisy environment," *Journal of Physics: Conference Series*, vol. 1804, no. 1, p. 012042, 2021.

[94] Z.-L. Liu, C.-F. Jia, and J.-W. Li, "Research on the format-preserving encryption techniques," *Ruanjian Xuebao*, vol. 23, no. 1, pp. 152–170, 2012.

[95] X. Luo, H. Wang, D. Wu, C. Chen, M. Deng, J. Huang, and X. S. Hu, "A survey on deep hashing methods," *ACM Transactions on Knowledge Discovery from Data*, vol. 17, no. 1, pp. 1–50, 2023.

[96] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–35, 2018.

[97] Y. Wang, L. Wang, M. Dong, J. Tang, M. Sun, R. Wang, M. Hu, and H. Zhang, "Image encryption and decryption system with clock controlled destruction," 2022 International Conference on Image Processing, Computer Vision and Machine Learning (ICICML), Xi'an, China, 2022, pp. 90–93.

[98] A. Alsobeh, and A. Shatnawi, "Integrating data-driven security, model checking, and self-adaptation for IoT systems using BIP components: A conceptual proposal model," in Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23), San Diego, USA, 2023, pp. 533–549.

[99] Q. Song, E. Engström, and P. Runeson, "Industry practices for challenging autonomous driving systems with critical scenarios," *ACM Transactions on Software Engineering and Methodology*, in press, 2023, DOI: 10.1145/3640334.

[100] M. Wäschle, K. Wolter, K. Bause, M. Behrendt, and A. Albers, "Considering functional safety – Supporting the development of automated driving vehicles by the use of model-based systems engineering," 2022 17th Annual System of Systems Engineering Conference (SOSE), Rochester, NY, USA, 2022, pp. 275–280.

[101] L. Hu, X. Zhou, X. Zhang, F. Wang, Q. Li, and W. Wu, "A review on key challenges in intelligent vehicles: Safety and driver-oriented features," *IET Intelligent Transport Systems*, vol. 15, no. 9, pp. 1093–1105, 2021.

[102] D. Hulse and L. Irshad, "Using degradation modeling to identify fragile operational conditions in human- and component-driven resilience assessment," 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), Portsmouth, VA, USA, 2022, pp. 1–10.

[103] Y. Poledna, F. Reway, M. F. Drechsler, W. Huber, C. Icking, and E. P. Ribeiro, "An open-source high-level fusion algorithm in ROS for automated driving applications," 2022 10th International Conference in Software Engineering Research and Innovation (CONISOFT), San José Chiapa, Mexico, 2022, pp. 174–181.

[104] S. Y. Alaba and J. E. Ball, "Deep learning-based image 3-d

object detection for autonomous driving," *IEEE Sensors Journal*, vol. 23, no. 4, pp. 3378–3394, 2023.

[105] J. Breitenstein, J. A. Termöhlen, D. Lipinski, and T. Fingscheidt, "Systematization of corner cases for visual perception in automated driving," 2020 IEEE Intelligent Vehicles Symposium (IV), Las Vegas, NV, USA, 2020, pp. 1257–1264.

[106] H. Fan, F. Zhu, C. Liu, L. Zhang, L. Zhuang, D. Li, W. Zhu, J. Hu, H. Li, and Q. Kong, "Baidu Apollo EM motion planner," *arXiv preprint arXiv:1807.08048*, 2018, DOI: 10.48550/arXiv.1807.08048.

[107] C. Hu, H. Gong, and Y. He, "Data driven identification of international cutting edge science and technologies using SpaCy," *PLoS One*, vol. 17, no. 10, p. e0275872, 2022.

[108] T. Paul and K. Ueno, "Robust incremental logistic regression for detection of anomaly using big data," 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 2020, pp. 1167–1173.

[109] Y. Wang, J. Jiang, S. Li, R. Li, S. Xu, J. Wang, and K. Li, "Decision-making driven by driver intelligence and environment reasoning for high-level autonomous vehicles: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 10, pp. 10362–10381, 2023.

[110] M. Ammour, R. Orjuela, and M. Basset, "A MPC combined decision making and trajectory planning for autonomous vehicle collision avoidance," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 24805–24817, 2022.

[111] W. Shao, J. Li, and H. Wang, "Self-aware trajectory prediction for safe autonomous driving," 2023 IEEE Intelligent Vehicles Symposium (IV), Anchorage, AK, USA, 2023, pp. 1–8.

[112] J. Lu, Z. Peng, S. Yang, Y. Ma, R. Wang, Z. Pang, X. Feng, Y. Chen, and Y. Cao, "A review of sensory interactions between autonomous vehicles and drivers," *Journal of Systems Architecture*, vol. 141, p. 102932, 2023.

[113] H. Wang, X. Zhang, J. Li, B. Li, X. Gao, Z. Hao, J. Fu, Z. Zhou, and M. Atia, "Driving risk cognition of passengers in highly automated driving based on the prefrontal cortex activity via fNIRS," *Scientific Reports*, vol. 13, no. 1, p. 15839, 2023.

[114] J. Fu, X. Zhang, W. Yu, J. Li, M. M. Atia, H. Wang, C. Li, and Z. Hao, "Decoding passenger's EEG signals from encountering emergency road events," 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC), Macau, China, 2022, pp. 2214–2219.

[115] D. Humeniuk, F. Khomh, and G. Antoniol, "Ambiegen: A search-based framework for autonomous systems testing," *Science of Computer Programming*, vol. 230, p. 102990, 2023.

[116] S. Singhal, N. Jatana, K. Sheoran, G. Dhand, S. Malik, R. Gupta, B. Suri, M. Niranjanamurthy, S. N. Mohanty, and N. R. Pradhan, "Multi-objective fault-coverage based regression test selection and prioritization using enhanced ACO_TCSP," *Mathematics*, vol. 11, no. 13, p. 2983, 2023.

[117] G. Yang, M. Haque, Q. Song, W. Yang, and X. Liu, "Testaug: A framework for augmenting capability-based nlp tests," *arXiv preprint arXiv:2210.08097*, 2022, DOI: 10.48550/arXiv.2210.08097.

[118] D. Zhang, J. Sun, J. Wang, and R. Yu, "Real-time driving risk assessment based on the psycho-physical field," *Journal of Transportation Safety & Security*, vol. 16, no. 3, pp. 293–322, 2024.

[119] A. Fries, F. Fahrenkrog, K. Donauer, M. Mai, and F. Raisch, "Driver behavior model for the safety assessment of automated driving," 2022 IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany, 2022, pp. 1669–1674.

[120] O. De Groot, L. Ferranti, D. Gavrila, and J. Alonso-Mor, "Scenario-based motion planning with bounded probability of collision," *arXiv preprint arXiv:2307.01070*, 2023.

[121] M. M. J. Samodro, R. D. Puriyanto, and W. Caesarendr, "Artificial potential field path planning algorithm in differential drive mobile robot platform for dynamic environment," *International Journal of Robotics and Control Systems*, vol. 3, no. 2, pp. 161–170, 2023.

[122] A. Arun, "A novel road user safety field theory for traffic safety assessment applying video analytics," Ph.D. Dissertation, Queensland University of Technology, Brisbane, 2022.

[123] P. Franklin, "Risk assessment using information entropy," 2023 Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, USA, 2023, pp. 1–4.

[124] Z. Pang, Z. Chen, J. Lu, M. Zhang, X. Feng, Y. Chen, S. Yang, and Y. Cao, "A survey of decision-making safety assessment methods for autonomous vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 16, no. 1, pp. 74–103, 2023.

[125] J. Feng, C. Wang, C. Xu, D. Kuang, and W. Zhao, "Active collision avoidance strategy considering motion uncertainty of the pedestrian," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 4, pp. 3543–3555, 2020.

[126] A. Shoker, V. Rahli, J. Decouchant, and P. Esteves-Verissimo, "Intrusion resilience systems for modern vehicles," 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 2023, pp. 1–7.

[127] D. Suo, J. E. Siegel, and S. E. Sarm, "Merging safety and cybersecurity analysis in product design," *IET Intelligent Transport Systems*, vol. 12, no. 9, pp. 1103–1109, 2018.

[128] C. Lin, D. Tian, X. Duan, J. Zhou, D. Zhao, and D. Cao, "3d-DFM: Anchor-free multimodal 3-d object detection with dynamic fusion module for autonomous driving," *IEEE*

Transactions on Neural Networks and Learning Systems, vol. 14, no. 12, pp. 10812–10822, 2022.

[129] H. Martin, Z. Ma, C. Schmittner, B. Winkler, M. Krammer, D. Schneider, T. Amorim, G. Macher, and C. Kreiner, "Combined automotive safety and security pattern engineering approach," *Reliability Engineering & System Safety*, vol. 198, p. 106773, 2020.

[130] S. Dotsenko, H. Fesenko, O. Illiashenko, V. Kharchenko, V. Moiseenko, and L. Yermolenko, "Integration of security, functional and ecology safety management systems: Concept and industrial case," 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2020, pp. 470–474.

[131] S. Numan, E. Gordon, K. Klaus, and D. Kristina, "Multi-Sensor Data Fusion for Real-Time Multi-Object Tracking," *Engineering, Environmental Science, Computer Science*, in press, doi: 10.3390/pr11020501.

[132] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C. Y. Fu, A. C. Berg, "SSD: Single shot multibox detector," arXiv 2015, arXiv:1512.02325.

[133] M. Bojarski, D. D. Testa, D. Dworakowski, B. Firner, B. Flepp, P. Goyal, L. D. Jackel, M. Monfort, U. Muller, J. Zhang, X. Zhang, J. Zhao, and K. Zieba, "End to end learning for self-driving cars," ArXiv, 2016, vol. abs/1604.07316.

[134] C.-C. Wu, C.-W. Chen, C.-L. Lin, and C.-J. Yang, "Advanced organic light-emitting devices for enhancing display performances," *Journal of Display Technology*, vol. 1, no. 2, pp. 248–266, 2005.

[135] A. Jain, A. R. Kondapally, K. Yamada, and H. Yanak, "A neuro-symbolic approach for multimodal reference expression comprehension," *arXiv preprint arXiv:2306.10717*, 2023, DOI: 10.48550/arXiv.2306.10717.

[136] D. Wang, Y. Guo, S. Liu, Y. Zhang, W. Xu, and J. Xiao, "Haptic display for virtual reality: progress and challenges," *Virtual Reality & Intelligent Hardware*, vol. 1, no. 2, pp. 136–162, 2019.

[137] J. Kim and D. Kum, "Collision risk assessment algorithm via lane-based probabilistic motion prediction of surrounding vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 9, pp. 2965–2976, 2017.

[138] M. Nalini, "Intelligent devices, device management, and device security for cloud platforms," *Convergence of Deep Learning and Internet of Things: Computing and Technology*, Hershey, PA: IGI Global, 2023, pp. 1–22.

[139] L. Wang, Y. Ma, J. Yan, V. Chang, and A. Y. Zomay, "pipsCloud: High performance cloud computing for remote sensing big data management and processing," *Future Generation Computer Systems*, vol. 78, pp. 353–368, 2018.

[140] R. Beyar, L. Gruberg, D. Deleanu, A. Roguin, Y. Almagor, S. Cohen, G. Kumar, and T. Wenderow, "Remote-control percutaneous coronary interventions: Concept, validation, and first-in-humans pilot clinical trial," *Journal of the American College of Cardiology*, vol. 47, no. 2, pp. 296–300, 2006.

[141] B. Chen and H. H. Cheng, "A review of the applications of agent technology in traffic and transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 2, pp. 485–497, 2010.

[142] T. V. Nguyen, P. Shailesh, B. Sudhir, G. Kapil, L. Jiang, Z. Wu, D. Malladi, and J. Li, "A comparison of cellular vehicle-to-everything and dedicated short range communication," 2017 IEEE Vehicular Networking Conference (VNC), Turin, Italy, 2017, pp. 101–108.

[143] Y. P. Varshni, "Comparative study of potential energy functions for diatomic molecules," *Reviews of Modern Physics*, vol. 29, no. 4, p. 664, 1957.

[144] K. Reif, *Brakes, Brake Control and Driver Assistance Systems*, Weisbaden, Germany: Springer, 2014.

[145] G. M. Zago and E. P. De Freitas, "A quantitative performance study on CAN and CAN FD vehicular networks," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 5, pp. 4413–4422, 2017.

[146] Y. Almalioglu, M. Turan, N. Trigoni, and A. Markham, "Deep learning-based robust positioning for all-weather autonomous driving," *Nature Machine Intelligence*, vol. 4, no. 9, pp. 749–760, 2022.

[147] M. Liebner, M. Baumann, F. Klanner, and C. Stiller, "Driver intent inference at urban intersections using the intelligent driver model," 2012 IEEE Intelligent Vehicles Symposium, Madrid, Spain, 2012, pp. 1162–1167.

[148] M. A. Van Staalduinen, F. Khan, V. Gadag, and G. Reniers, "Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure," *Reliability Engineering & System Safety*, vol. 157, pp. 23–34, 2017.

[149] D. Zhang, G. Feng, Y. Shi, and D. Srinivas, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.

[150] Z. Lv, Y. Li, H. Feng, and H. Lv, "Deep learning for security in digital twins of cooperative intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16666–16675, 2021.

[151] I. Errandonea, S. Beltrán, and S. Arrizabalaga, "Digital Twin for maintenance: A literature review," *Computers in Industry*, vol. 123, no. 103316, 2020.

[152] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based big data storage systems in cloud computing: Perspectives and challenges," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 75–87, 2016.

[153] K. T. Arun, "Software defined vehicle demands R&D overhauling," Accessed: Mar. 1, 2023 [Online]. Available: https://hindujatech.com/blog/software-defined-vehicle-demands-r-and-d-overhauling.

[154] A. Bernard and A. Fischer, "New trends in rapid product development," *CIRP Annals*, vol. 51, no. 2, pp. 635–652, 2002.

[155] N. G. Leveson, *Engineering A Safer World: Systems Thinking Applied to Safety*, Cambridge: The MIT Press, 2016.

[156] Globe Newswire, "Intelligent vehicle E/E architecture research report, 2022," Accessed: Mar. 12, 2024 [Online]. Available: https://www.globenewswire.com/news-release/2022/09/13/2515252/0/en/Intelligent-Vehicle-E-E-Architecture-Research-Report-2022.html.

[157] Collimator, "Model based design overview for system development," Accessed: Mar. 1, 2024 [Online]. Available: https://www.collimator.ai/post/model-based-development.

[158] C. Singh, N. S. Gaba, M. Kaur, and B. Kaur, "Comparison of different CI/CD tools integrated with cloud platform," 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 7–12.

[159] Z. Kozhirbayev and R. O. Sinnott, "A performance comparison of container-based technologies for the cloud," *Future Generation Computer Systems*, vol. 68, pp. 175–182, 2017.

[160] F. Tao and Q. Qi, "Make more digital twins," *Nature*, vol. 573, no. 7775, pp. 490–491, 2019.

[161] J. Zhou, P. Li, Y. Zhou, B. Wang, J. Zang, and L. Meng, "Toward new-generation intelligent manufacturing," *Engineering*, vol. 4, no. 1, pp. 11–20, 2018.

[162] I. Gräßler, D. Wiechel, D. Roesmann, and H. Thiele, "V-model based development of cyber-physical systems and cyber-physical production systems," *Procedia Cirp*, vol. 100, pp. 253–258, 2021.

[163] S. Mathur and S. Malik, "Advancements in the V-Model," *International Journal of Computer Applications*, vol. 1, no. 12, pp. 29–34, 2010.

[164] D. Sjödin, V. Parida, M. Palmié, and J. Wincent, "How AI capabilities enable business model innovation: Scaling AI through co-evolutionary processes and feedback loops," *Journal of Business Research*, vol. 134, pp. 574–587, 2021.

[165] X. Zhou, C. Chai, G. Li, and J. Sun, "Database meets AI: A survey, 2020," Accessed: Mar. 1, 2024 [Online]. Available: https://dbgroup.cs.tsinghua.edu.cn/ligl/papers/aidb.pdf.

[166] S. A. Seshia, D. Sadigh, and S. S. Sastry, "Toward verified artificial intelligence," *Communications of the ACM*, vol. 65, no. 7, pp. 46–55, 2022.

[167] P. Pataranutaporn, V. Danry, J. Leong, P. Punpongsanon, D. Novy, P. Maes, and M. Sra, "AI-generated characters for supporting personalized learning and well-being," *Nature Machine Intelligence*, vol. 3, no. 12, pp. 1013–1022, 2021.

[168] S. K. Singh, S. Rathore, and J. H. Park, "Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721–743, 2020.

[169] D. Maltoni and V. Lomonaco, "Continuous learning in single-incremental-task scenarios," *Neural Networks*, vol. 116, pp. 56–73, 2019.

[170] M. Rubert and K. Farias, "On the effects of continuous delivery on code quality: A case study in industry," *Computer Standards & Interfaces*, vol. 81, p. 103588, 2022.