IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 December 2023, accepted 1 January 2024, date of publication 4 January 2024, date of current version 22 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3349964

RESEARCH ARTICLE

Longitudinal Functional Safety Analysis and Algorithm Design of Traffic Jam Pilot

LEI HE[1], JUNYI CHEN[1], XIUCAI ZHANG[1], JUN LI[2], AND JINGQUAN TIAN[2]
[1]State Key Laboratory of Automotive Simulation and Control, Jilin University, Changchun, Jilin 130022, China
[2]China First Automobile Works Group Corporation Ltd., Changchun, Jilin 130000, China

Corresponding author: Jun Li (lijun9@faw.com.cn)

This work was supported in part by the Project on Quantitative Development and Measurement Technology Research of Expected Functional Safety Based on Vehicle-Cloud Collaboration under Grant 20220301012GX, and in part by the Project on Research and Development of Intelligent Vehicle Key Technologies and Industrialization Projects Based on New Energy Vehicles under Grant TC210H02S.

ABSTRACT In recent years, autonomous driving technology has been developing rapidly, but there is still a certain gap from commercial production, in which the safety issue is one of the important factors. In the working of most companies and colleges, the Traffic Jam Pilot (TJP), serving as a prototypical Level 3 autonomous driving function, has predominantly focused on functional implementation and enhancement, prioritizing functional completeness and user comfort. However, the aspect of functional safety in the system has received comparatively less attention. To guarantee the safety of the driver's life and property, it is essential to consider the functional safety aspect regarding automobile operation after system function failure. In this paper, according to the functional safety development process and related regulations in ISO 26262, the functions and operation environment of the TJP system are defined in detail, and the longitudinal function is taken as an example to be developed following the functional safety process and verified by simulation. Simulation verification results show that the control algorithm is safe and reliable, and can ensure the safety and stability of the vehicle during operation. The research in this paper further explores the combination of functional safety and high-level automated driving function, providing some ideas for their practical application in industry.

INDEX TERMS Vehicle, longitudinal control, functional safety, fault tree analysis, TJP.

I. INTRODUCTION

With the continuous improvement of the economic level of the population, the number of vehicles is also increasing. People travel more conveniently, but the traffic jams are getting more serious. Traffic jams increase people's commuting time and reduce the comfort of people's travel [1].

The function of the TJP system is to help the driver steer the vehicle during traffic jams, reducing the time and fatigue of driving the vehicle and improving driving comfort and safety [2].

The TJP system is an L3 autonomous driving function [3]. Some car manufacturers (e.g., Audi [4], Mercedes-Benz [5]) had also proposed research and development programs for models with TJP functionality, but due to legal and technical reasons, this functionality could only be used in certain countries and regions. Many researchers have also made efforts to make this technology better.

Binlin Yi et al. explored the relationships and effects between physiological responses, situational factors, and takeover criticality when drivers use the TJP function [6]. Peng Guo et al. proposed a new algorithm for the automatic generation of self-driving test scenarios to assist in the verification of TJP functions [7]. Echeto et al. proposed a population model considering self-driving vehicles to simulate low-speed vehicles and their interactions with the vehicle in front of them and performed a simulation analysis in a traffic congestion scenario [8]. Zhang et al. proposed an open-source dataset full of congestion scenarios, which contained some congested roads and highways in China, and this dataset was

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaojie Su.

subjected to scenario parameterization and driving behavior analysis, which helped in the development and validation of TJP [9]. Wei et al. developed a control framework using onboard radar sensors and vehicle-to-vehicle (V2V) communication to realize automatic vehicle following in both longitudinal and transverse directions, which was demonstrated to have a good following effect through simulations and experiments [10].

Following the definition of the L3 autonomous driving function, it is imperative that before requesting the driver to control the vehicle, the autonomous driving system ensures the vehicle's ability to operate normally and safely or bring it to a secure stop at the roadside. The development of features such as the TJP system has brought about more complex electrical and electronic architectures and functional complexity [11]. Currently, researchers are mainly focusing on the implementation and enhancement of TJP system functions, but less consideration has been given to the security issues caused by the complexity of the system. The safety issues of autonomous driving can be categorized into passive safety, functional safety, anticipatory functional safety, behavioral safety, and information security [12]. The International Organization for Standardization has respectively published ISO 21448 and ISO 26262 for guidance on intended functional safety and functional safety [13], [14].

Functional Safety encompasses the prevention of risks from system failures and stochastic hardware malfunctions. ISO 26262 as a comprehensive document for guiding functional safety practices, extends its applicability to all stages of the lifecycle of safety-related systems consisting of electrical, electronic, and software elements that provide safety-related functions. Many scholars had done a lot of research in the field of functional safety in conjunction with ISO 26262. Lu and Chen proposed a system hardware architecture framework that combined fault tree vulnerability analysis with hardware architecture to discover solutions that met ISO 26262 security requirements and overhead constraints while generating Failure Mode, Effects, and Diagnostic Analysis (FMEDA) reports [15]. Marcos et al. provided a well-established design methodology for battery management systems (BMS) for lithium batteries in electric vehicles, following the ISO 26262 process from conceptualization to functional verification [16]. Huang and Li combined ISO 26262 and the technical report from the National Highway Traffic Safety Administration (NHTSA) to propose a faulty operation architecture for linear steering systems, which improved the safety and reliability of automotive steering systems [17]. Guo et al. summarized the latest developments and trends in functional safety design methodologies for vehicles through the analysis, design, optimization, and operation phases [18]. Xia et al.applied the functional safety analysis method for failure analysis and hazard identification in adaptive cruise control (ACC) system to obtain safety goals, Automotive Safety Integration Level (ASIL) level, and derive safety constraints, and safety requirements [19]. In addition to the work of the researchers mentioned above, ISO 26262 is also used in other areas, such as automotive software development [20], power supply systems [21], robotic drives [22], design of the brake-by-wire [23], risk quantification for driving scenarios [24], and test scenario generation [25].

The main work of this article is:

(1) Combine functional safety with the L3 autonomous driving function, which facilitates the subsequent improvement of the safety of the autonomous driving function.

(2) Define the functional and operational domains of the TJP system and propose a corresponding architecture.

(3) Conduct Hazard Analysis and Risk Assessment (HARA), Failure Mode and Effect Analysis (FMEA), and Fault Tree Analysis (FTA) analyses for longitudinal functions to obtain longitudinal safety requirements.

(4) Simulate the failure scenarios using fault injection and verify the results.

The remainder of the manuscript is described as follows. In Section II, the TJP system is defined to obtain functional components, operating conditions, and system structure. HARA is used to analyze longitudinal functions to identify hazardous events in Section III. In Section IV, the security objectives acquired in the preceding section undergo decomposition utilizing the security analysis methodology, and the corresponding security requirements are extracted and assigned to their respective modules. A Simulink / CarSim model is constructed to validate the aforementioned algorithm in Section V, and the conclusion is presented in Section VI.

II. TJP SYSTEM DEFINITION AND ANALYSIS

A. TJP SYSTEM FUNCTION DEFINITION

The role of the TJP system is to take control of the vehicle when driving on a highway or expressway and encountering congested conditions within the designated operational parameters known as the Operational Design Domain (ODD). During such circumstances, the system autonomously follows the vehicle ahead, executing tasks such as starting, stopping, and advancing. Consequently, the driver is relieved of the need to attend to road conditions and can direct their attention towards non-driving activities. However, it is important to note that the driver is required to regain control of the vehicle within a specified timeframe upon receiving a takeover request from the system. Between the time the system sends a takeover request and the time the driver takes control of the vehicle, the system continues to control the vehicle. The system is specifically designed for use in traffic congestion situations, with a maximum operating speed ranging from 40-60 km/h.

The TJP system encompasses various functional states, including (1) standby state, (2) overtaking state, (3) degradation control, and (4) activation state. These states are described as follows:

Standby state: When the TJP system is inactive, it assesses the driving environment against the ODD. If the driving

TABLE 1. TJP system functions.

Function	Functional Description
Longitudinal Function	(1) Automatically maintain a specified distance from the preceding vehicle within the defined margin of error. (2) Automatically maintain a designated speed consistent with the leading vehicle within the established tolerance. (3) Automatically execute stop-and-start maneuvers while following the vehicle ahead. (4) When encountering a new target vehicle, automatically perform target transition and appropriately decelerate. (5) When the preceding target vehicle exits, automatically execute the target transition and accelerate accordingly. (6) Upon recognizing environmental speed limit information (including map data or traffic flow information), automatically implement speed restrictions.
Lateral Function	(1) Compute the lateral control trajectory based on navigation information and regulate the lateral turning angle through the heading angle or lateral displacement output. (2) Automatically uphold the function of lateral trajectory alignment within a specified tolerance. (3) Automatically adapt the lateral alignment offset of the vehicle following the curve radius. (4) Automatically adjust the lateral alignment offset based on the risk of the vehicle deviating from the adjacent lane. (5) Automatically fine-tune the lateral trajectory deviation using feedback from lateral execution and environmental variations.
Monitoring Function	Automatically monitor the driver's status and execute corresponding countermeasures according to the monitoring results. (1) When the driver's status is detected as heavy fatigue or long distraction time, the TJP system is not entered. (2) When the TJP is activated and the driver's condition is assessed as severe fatigue or prolonged distraction, the TJP's operational duration is shortened and proactively activates its alarm system. (3) When the driver monitoring system detects the TJP's activation, it introduces a delay before initiating its alarm system.
Alarm Function	When the system detects a specific collision hazard, it autonomously assesses the level of risk and notifies the driver through varying degrees of warning signals.
Safe Collision Avoidance	(1) The TJP system is designed to prevent any collisions occurring within the ODD to mitigate potential liability incidents involving the vehicle, which encompasses the avoidance of collisions with other vehicles, pedestrians, cyclists, and various obstacles located ahead of the vehicle. (2) The collision avoidance procedure entails decelerating to a complete stop within a specified speed range while simultaneously alerting the driver.

conditions do not meet the ODD criteria, the system prevents the driver from activating TJP and provides clear explanations without interfering with their normal driving. Conversely, if the driving environment satisfies the ODD, the system appropriately prompts the driver to activate TJP.

Overtaking state: While in the system activation state, the TJP system monitors the accelerator pedal and steering wheel. If the driver applies pressure to the accelerator pedal (with the pedal opening of 2%-5%) or turns the steering wheel (with a torque exceeding 1.5 N·m-2 N·m), it is interpreted as

an intention to overtake longitudinally or laterally. In such cases, the system relinquishes control and returns it to the driver.

Degraded control: When the system detects that the vehicle's operating environment lies beyond the predetermined ODD range or encounters a system failure, the TJP system endeavors to maintain control of the vehicle to the best of its ability. Simultaneously, it promptly alerts the driver to take over. Should the driver fail to regain control within the specified timeframe, considering the system's low operating speed, the system autonomously brakes the vehicle and brings it to a safe stop at the side of the road.

Once the system monitors the vehicle operating conditions to meet the ODD, the driver gains the ability to activate the TJP system. Subsequently, the system assumes control and carries out a range of driving tasks, encompassing environment perception, behavioral decision-making, lateral and longitudinal motion control, feedback regulation, alarm displays, and more. Further information regarding these functionalities is provided in Table 1.

B. DEFINITION OF OPERATIONAL DESIGN CONDITIONS

The Operational Design Condition (ODC) refers to the anticipated operating conditions during the system's design phase, encompassing elements such as the ODD, vehicle status, driver condition, and more [26], [27]. The ODC of the TJP system is outlined in Table 2.

C. SYSTEM CONFIGURATION ARCHITECTURE

To complete the system functions mentioned above, the TJP architecture should be as shown in Fig. 1. The TJP system is an L3 autonomous driving system, when the system detects that the operating environment meets the ODD, the driver will be reminded to turn on the TJP function through the Human Machine Interface (HMI) interface, and at this time, the TJP system will take over the vehicle instead of the driver and control the vehicle for traveling.

After the system function is turned on, the sensors installed on the vehicle acquire the driving environment, road signs, vehicle status and other data, which are processed by the algorithm and passed to the planning system. The planning system performs task decision-making and path planning to generate a motorable trajectory. The planned information is passed to the downstream controller, which outputs the acceleration, steering angle and other information, and ultimately realises the control of the vehicle, and so on, and so forth, to realise the driving task.

When the system function is turned on but detects that the operating environment will not satisfy the ODD, the driver will be reminded through the HMI interface to notify the driver to take over the vehicle within a certain period, returning the control of the vehicle to the driver.

This framework serves as the basis for subsequent work and provides the basis for subsequent analysis and improvement.

TABLE 2. TJP system operational design condition.

Classification	Explicit description
ODD	-Vehicle speed below 60km/h -Clear traffic signs, and traffic lights -No toll booths -No slopes, tunnels -No temporary construction sections -High visibility and good road adhesion conditions -Highways or urban expressways with opposite physical separation -Clear lane lines -No pedestrian crossing -No two-wheelers
Driver Status	-Driver in the driver's seat and seat belt fastened -Conscious head or body movements -or blink
Vehicle status	-Door closed -Vehicle is trouble-free -Vehicle not in reverse -Clear vehicle position information

TABLE 3. ASIL ratings.

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

III. HAZARD ANALYSIS AND RISK ASSESSMENT

A. HAZARD ANALYSIS AND RISK ASSESSMENT

HARA as a comprehensive safety analysis methodology at the vehicle level, is primarily employed during the conceptual development stage to identify and analyze potential hazardous events, as well as determine the corresponding ASIL ratings and safety objectives.

HARA comprises four distinct steps:

(1) Analysis of scenarios and identification of hazards;
(2) Categorization of hazard events;
(3) Evaluation of severity, exposure, and controllability;
(4) Determination of the ASIL rating.

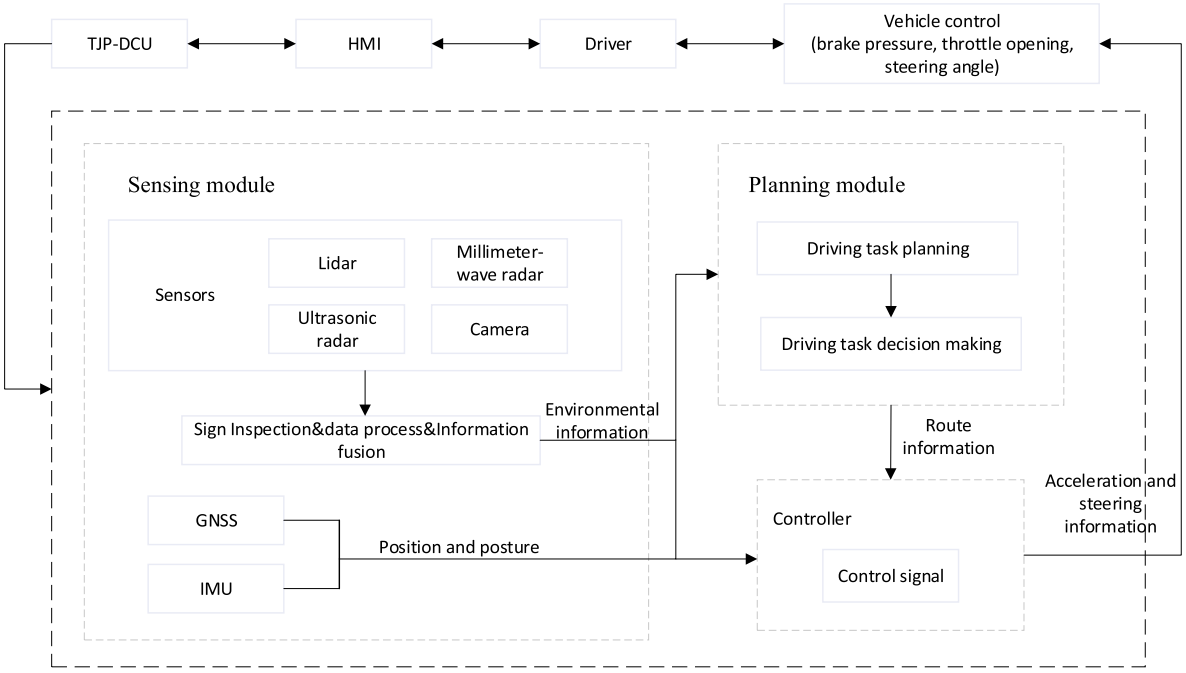

FIGURE 1. TJP system architecture.

Hazard and Operability Analysis (HAZOP), a prevalent technique for hazard identification in industrial and power systems, can be used to accomplish the corresponding aspects of step (1) mentioned earlier. This method employs suitable guide words (e.g., reverse, excessive, etc.) to envision abnormal manifestations of system functionality and can be employed to examine the operation of pertinent components at the vehicle-wide level [28].

The hazards stemming from abnormal system functionality vary across different driving scenarios and are scrutinized by assuming the aberrant operation of the relevant component and combining it with specific driving scenarios during the risk assessment.

ISO 26262 introduces the concept of ASIL in conjunction with vehicle characteristics, which can be assessed using three parameters as follows:

Severity (S): This parameter measures the extent of injury caused by the hazard to individuals. The severity rating should be determined based on professional medical evaluation or deduced from past crash data [29], ranging from S0 (minimal severity) to S3 (severe severity) in sequential order.

Exposure (E): Exposure refers to the probability of encountering hazardous conditions. The exposure rating ranges from E0 (low probability) to E4 (high probability) in ascending order of occurrence likelihood.

Controllability (C): Controllability assesses the ability of personnel involved in the hazard to take preventive measures and avoid harm. The controllability rating is categorized from C0 (easy control) to C3 (difficult control) based on the level of control required.

The greater the functional safety risk associated with the system, the more elevated the safety requirements and ASIL rating become. Consequently, the demands for design methodologies, testing approaches, safety techniques, performance indicators, development processes, and audit confirmation also intensify. In the case of functional abnormalities about the relevant item, its S/E/C must be assessed, followed by the derivation of the corresponding ASIL rating. The correlation between various S/E/C ratings and ASIL ratings is illustrated in Table 3. It is worth noting that "QM" denotes quality management, signifying that this functionality does not impact safety, and the development process should comply with the requirements of quality management assurance.

B. LONGITUDINAL HARA ANALYSIS

Based on the longitudinal functions of the TJP system defined in the previous section, the above methodology is applied to analyze and obtain the corresponding security objectives as follows:

Function 1: Automatically maintain a specified distance from the preceding vehicle within the defined margin of error. Automatically maintain a designated speed consistent with the leading vehicle within the established tolerance. Automatically execute stop-and-start maneuvers while following the vehicle ahead. When encountering a new target vehicle, automatically perform target transition and appropriately decelerate. When the preceding target vehicle exits, automatically execute the target transition and accelerate accordingly.

Function 2: Upon recognizing environmental speed limit information (including map data or traffic flow information), automatically implement speed restrictions.

TABLE 4. Longitudinal function HARA table.

Serial number	guide words	Functional Abnormalities	Potential Hazards	Driving Scenes	Hazardous Events	S	E	E value basis	C	C value basis	ASIL	Security Objectives	Number
01	excessive	Provides excessive acceleration	The excessive longitudinal force causes failure to maintain a good distance from the car in front	This vehicle is traveling on highways or urban expressways with opposite physical separation at 40km / h	Rear-ending with the car in front at a higher speed	3	4	Drivers encounter almost every time they drive	3	It is difficult for the driver to take over the driving task for a short period	D	The proportionality between the gas pedal and the distance to the vehicle in front should be reasonably controlled	Safe-1
02	Lost	Suitable acceleration not provided	Acceleration loss can not follow the front car distance in time	Id.	Causing rear-end collisions	3	4	Id.	3	Id.	D	Id.	Safe-2
03	Reverse	Provides the opposite of actual acceleration, such as braking	Acceleration reverse can not follow the car in time	Id.	Id.	3	4	Id.	3	Id.	D	Id.	Safe-3
04	Stagnant	The stagnant acceleration provided is a fixed value	Throttle lag causes acceleration not to keep up with the distance of the car in front	Id.	Causing loss of the following vehicle	0	4	Id.	3	Id.	QM		Safe-4
05	Not required but provided	Provides acceleration when the vehicle does not need it	Excessive longitudinal acceleration leading to increased vehicle speed	Id.	Rear-ending the car in front	3	4	Id.	3	Id.	D	Unanticipated provision of acceleration should be prevented	Safe-5
06	Time delay	Provides acceleration too late	Failure of the vehicle following due to late provision of acceleration	Id.	Rear-end collision	3	4	Id.	3	Id.	D	Vehicle collisions caused by untimely acceleration should be prevented	Safe-6
07	Premature	Premature provision of acceleration	Prematurely providing acceleration does not maintain the correct distance from the vehicle in front	Id.	Rear-ending the car in front	3	4	Id.	3	Id.	D	Prematurely provided acceleration should be prevented from causing a vehicle collision	Safe-7

C. SAFETY OBJECTIVES

Upon synthesizing the preceding analyses, the summary of the safety objectives is shown in Table 6.

The similar objectives in the above safety objectives are combined to obtain the combined safety objectives in Table 7.

IV. SECURITY REQUIREMENTS DECOMPOSITION AND ANALYSIS

ISO 26262 recommends two safety analysis methodologies: Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA). These methods employ distinct approaches, with FTA being a top-down analysis method. FTA initiates from the top event that violates the safety objective, progressively decomposing it downward to analyze potential causes leading to the top event and identify the corresponding bottom events [30]. Conversely, FMEA operates as a bottom-up analysis method, assuming the failure of bottom-level functions and subsequently propagating the analysis layer by layer to ascertain if the outcome conflicts with the safety objective [31]. Both approaches complement each other, enabling comprehensive system analysis [32].

TABLE 5. Environmental identification HARA table.

Serial number	guide words	Functional Abnormalities	Potential Hazards	Driving Scenes	Hazardous Events	S	E	E value basis	C	C value basis	ASIL	Security Objectives	Number
08	Lost	Loss of recognized environmental information	Ignoring environmental speed limits	This vehicle is traveling on highways or urban expressways with opposite physical separation at 40km / h	Speeding	3	4	Drivers encounter almost every time they drive	3	It is difficult for the driver to take over the driving task for a short period	D	Loss of perceptual information should be prevented	Safe-8
09	Lost	No braking	Resulting in no reduction in vehicle speed	This vehicle is traveling on highways or urban expressways with opposite physical separation at 40km / h	Speeding	3	4	Drivers encounter almost every time they drive	3	It is difficult for the driver to take over the driving task for a short period	D	Brakes should be prevented from being lost when speed limit information is recognized	Safe-9
10	Reverse	Same as function 1											Safe-10
11	Stagnant	Same as function 1											Safe-11
12	Not required but provided	False recognition of deceleration information	False recognition of a deceleration message causes braking	Id.	Speed mismatch	3	4	Id.	3	Id.	D	Misinformation should be prevented from interfering	Safe-12
13	Time delay	Braking too late	Causes slow speed reduction of the vehicle	Id.	Speeding	3	4	Id.	3	Id.	D	Late braking should be prevented from causing vehicle collisions	Safe-13

TABLE 6. Summary of safety objectives.

Security target number	Content Description	ASIL rating
Function 1	Longitudinal control	
SG-1	Provides excessive acceleration	D
SG-2	Acceleration not provided	D
SG-3	Provides the opposite of actual acceleration, such as braking	D
SG-4	The acceleration hysteresis provided is a fixed-value	QM
SG-5	Provides acceleration when the vehicle does not need it	D
SG-6	Provides acceleration too late	D
SG-7	Premature provision of acceleration	D
Function 2	Identify environmental speed limits and perform deceleration	
SG-8	Recognized environmental information is lost	D
SG-9	No braking	D
SG-10	Reverse deceleration (acceleration)	D
SG-11	Deceleration stall	D
SG-12	Deceleration without recognition of deceleration information	D
SG-13	Too late recognition or too late deceleration	D

A. SECURITY ANALYSIS

By leveraging AutoFTA, an FTA is conducted, focusing on the top event, SG-01, which deviated from the security objectives in Table 7, as depicted in Fig. 2.

The meaning of each event in the fault tree is as follows:

Top event: unintended longitudinal movement of the whole vehicle

TABLE 7. The combined table of security objectives.

Security target number	Description of security objectives	Security target level	Source of security objectives
SG-01	Collisions caused by unintended longitudinal movement of the vehicle should be avoided	D	SG-1, SG-2, SG-3, SG-5, SG-6, SG-7, SG-8, SG-9, SG-10, SG-11, SG-12, SG-13.

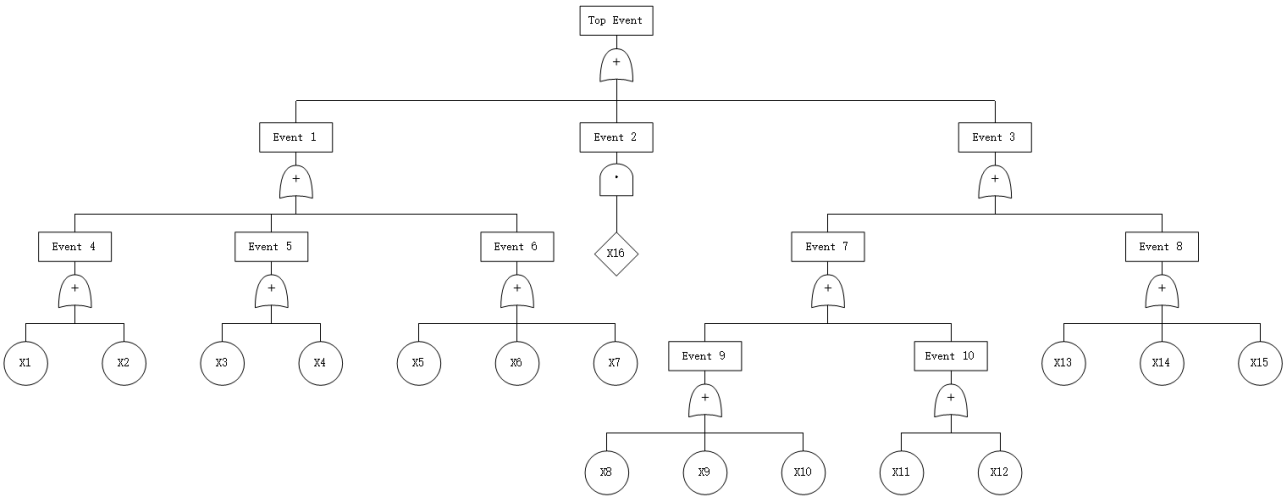

FIGURE 2. Safety target SG-01 fault tree analysis.

Event 1: Unanticipated acceleration request from Domain Controller Unit (DCU)

Event 2: Unexpected actuation of the drive/brake system

Event 3: Input error causing unintended acceleration/ braking

Event 4: Unintended acceleration due to improper handling of the sensing module

Event 5: Unintended acceleration due to improper handling of the decision module

Event 6: Unintended acceleration due to improper handling of the control module

Event 7: Sensor error causing unintended acceleration/ braking

Event 8: Driver unintended trigger acceleration

Event 9: The environment sensor incorrectly determines the surrounding environment/the state of the vehicle.

Event 10: Vehicle status sensor incorrectly determines vehicle status

X1: The perception algorithm fusion processing error

X2: The perception algorithm outputs the wrong static target information

X3: The perception algorithm outputs the wrong dynamic target information

X4: The decision algorithm outputs the wrong desired trajectory

X5: The decision algorithm outputs too large tracking curvature

X6: The control algorithm outputs the reverse acceleration command

X7: The control algorithm outputs excessive acceleration command

X8: LIDAR generates error point clouds

X9: Camera detection error

X10: Millimeter wave radar misjudges obstacles

X11: GNSS/IMU misjudges vehicle position

X12: The wheel speed sensor incorrectly calculates the vehicle speed

X13: Driver unintentionally depresses accelerator pedal/brake pedal

X14: Driver unintentionally activates the shift command

X15: Driver incorrectly turns on TJP

X16: Omitted events

Following the completion of FTA, two failure modes associated with control-related components are selected for analysis using the FMEA method. The outcomes of this analysis are presented in Table 8. It is essential to conduct an FMEA analysis for each type of failure observed in the system's relevant items, thereby iteratively enhancing the safety mechanism and supplementing the safety requirements.

After conducting FTA analysis, the failure mode of some relevant items is taken as an example and analyzed using the FMEA method, and the results are shown in Table 8. For each form of failure of relevant items in the system, FMEA analysis should be conducted to gradually

TABLE 8. FEMA of selected relevant items.

Relevant items	Security Objectives	Failure performance	Potential Risks	Response measures
LIDAR	Accurate generation of point cloud maps	Signal Noise	Impact on subsequent functions such as feature extraction and target recognition	Appropriate filtering algorithms are used
		Special scene signal output error	Inability to accurately judge the environment around the system	Multi-sensor deployment
		Error extraction for vehicle status	Inability to correctly obtain and use the current status of the vehicle	Add status extraction checks
Control	Capable of accurate control	The output control information is unstable	Poor vehicle control	Enhanced robustness of algorithms
		Error in the output control information	Wrong control of the vehicle	Add algorithm result verification

TABLE 9. Typical functional security requirements.

Functional safety requirement number	Functional safety requirement description	ASIL rating	Distribution
FSR-01	Environment-aware sensors should correctly identify and output environmental information	D	LIDAR Millimeter wave radar
FSR-02	The vehicle status sensor should correctly identify and process the output vehicle position, speed, attitude, etc.	D	GPS/IMU Wheel speed sensors, etc.
FSR-03	The sensing module should correctly receive and process the data from each sensor and correctly output the sensing information	D	DCU sensing module
FSR-04	The decision module should correctly receive and process the sensing results from the sensing module and correctly output the reference trajectory	D	DCU Decision Module
FSR-05	The control module should correctly receive and process the result data from the sensing module and the decision module, and output a reasonable horizontal and Longitudinal motion control law	D	DCU control module
FSR-06	The drive/brake system should correctly receive and process and output the longitudinal motion control from the DCU	D	Drive System Braking System

improve the safety mechanism and supplement the safety requirements.

B. FUNCTIONAL SAFETY REQUIREMENTS EXTRACTION

Functional safety requirements are the meticulous delineation of safety objectives, wherein the overarching safety objectives at the vehicle level are allocated to individual architectures. Drawing upon the safety analysis depicted in Fig. 2 and Table 8, the functional safety requirements are extracted and reasonably assigned, as presented in Table 9. To achieve the security goal of ASIL D, each module should meet ASIL D. Considering the cost, technology, etc., according to ISO 26262 Part IX, which points out the ASIL level decomposition, redundant architecture can be used, i.e., using different chips and algorithms to improve security.

The L3 level of autonomous driving function cannot be taken over by the driver immediately when the system fails, so Fail-Operational should be implemented, i.e., the vehicle can still run until the vehicle stops or the driver takes over the vehicle after the system fails. The architectures used to achieve Fail-Operational guarantee include primary/secondary control architecture, dual-core lock-step architecture, NooM architecture, etc. Considering the usage scenario and cost control, this paper adopts an approximate

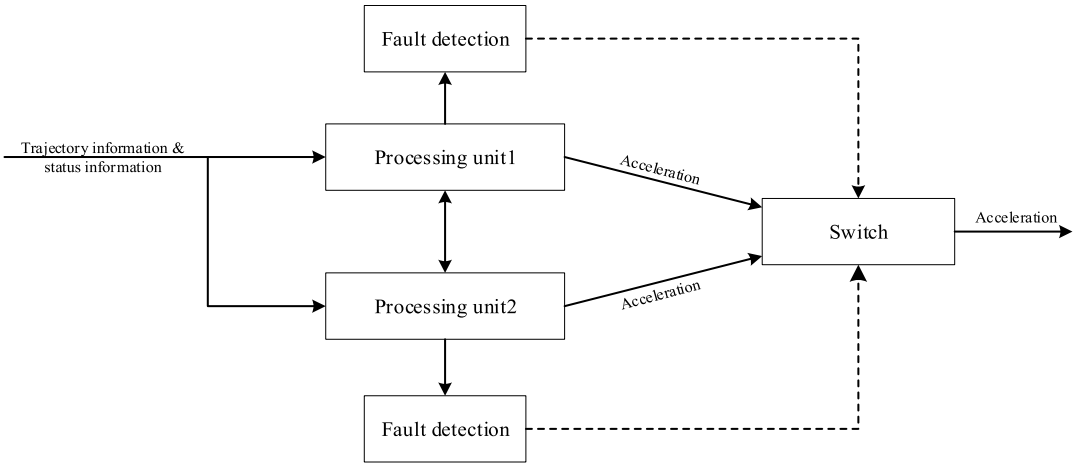

FIGURE 3. DCU security architecture.

TABLE 10. Control module software security requirements.

Software Security Requirement Number	Software Security Requirements Description	ASIL rating	Distribution
SSR-01	The longitudinal control software algorithm should correctly accept the result data from the sensing and decision modules	B(D)	Processing unit 1 Processing unit 2
SSR-02	The longitudinal control software algorithm should correctly calculate a reasonable amount of acceleration control based on the reference trajectory and the state of the vehicle	B(D)	Id.
SSR-03	The longitudinal control software algorithm should correctly output acceleration control to the drive/formulation system	B(D)	Id.

architecture of 2oo2 architecture for the control module: 1oo2D architecture, as shown in Figure 3. Different manufacturers or classes of chips should be used in different processing units to ensure the security of the hardware.

For the control module, the software should be designed after securing the hardware. According to the control logic in Fig. 3, the software security requirements are obtained as shown in Table 10.

V. DESIGN AND VERIFICATION OF LONGITUDINAL CONTROL FUNCTION

A. ALGORITHM INTRODUCTION

As science and technology evolve, so do the control algorithms used for vehicles. Wang Shaohua et al. combined neural networks with sliding mode control to propose a new control strategy to improve the longitudinal control performance of smart vehicles [33]. Guo Jinghua et al.established a corresponding longitudinal vehicle model for the vehicle nonlinearity and parameter uncertainty problem and proposed an adaptive control system to improve the longitudinal tracking performance of the vehicle [34]. Lu and Bi proposed a longitudinal brain control method based on human behavior and vehicle dynamics for disabled people who cannot use their limbs to drive vehicles, which can accurately enable drivers to control their vehicles and ensure the safety of driving [35].

The PID control algorithm has the characteristics of simple and effective, fast response speed, etc., which is widely used in engineering, and many researchers have studied it, the related theories are more mature, and the control effect is stable and effective. Yang et al. proposed a control method combining deep reinforcement learning and a PID controller in the cooperative adaptive cruise control (CACC) function to achieve automatic PID weight adjustment, which resulted in a significant reduction in the stabilization time of the vehicle queuing system [36]. Kebbati et al. used genetic algorithms (GA-PID) and neural networks (NN- PID) two methods to realize adaptive PID control and thus accomplish the longitudinal control task [37]. Yang and Lin used fuzzy PID as a longitudinal tracking controller in trajectory tracking control to control the motor torque and braking pressure and accomplish the longitudinal tracking task [38]. Li et al. proposed a longitudinal dynamics model for an autonomous vehicle and compared the control effects of various PID controllers [39].

The PID control algorithm adjusts the control effect by adjusting the size of the proportional coefficient Kp, the

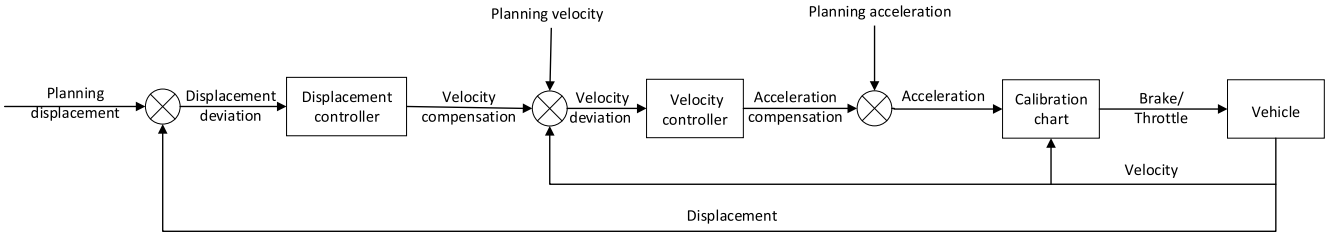

FIGURE 4. Double closed-loop PID control diagram.

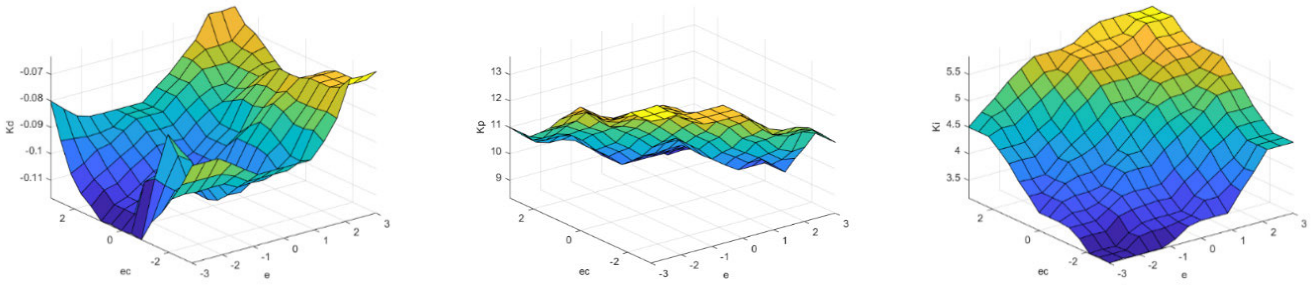

FIGURE 5. Input-output relationship diagram.

integral coefficient Ki, and the differential coefficient Kd, where: the role of Kp is to adjust the deviation of the system proportionally; the role of Ki is to enable the system to eliminate the steady-state error; and the role of Kd is to reduce the overshooting and the regulation time, and to improve the dynamic performance of the system.

In a continuous system, the expression of the PID control algorithm is:

$$u(t) = Kp * e(t) + Ki \int_0^t e(t)dt + Kd \frac{de\,(t)}{dt} \tag{1}$$

In a discrete system, the expression for the PID control algorithm is:

$$u(t) = Kp * e(t) + KiT \sum_{j=0}^{k} e\,(j) + Kd \frac{e\,(k) - e\,(k-1)}{T} \tag{2}$$

In equation (2), e(t) is the input deviation, numerically the difference between the input and output quantities, k is the sampling sequence number, and T is the sampling time.

In the previous chapter, after extracting the safety requirements, a hardware redundancy architecture was derived in which different types of chips should be used. In this chapter, software redundancy design is required and in this paper, fuzzy PID and dual closed-loop PID control are used as longitudinal control algorithms for the vehicle.

It is worth mentioning that this paper focuses on functional safety analysis and the algorithms in this section are a simple validation of the previous chapters to ensure the completeness of the work. Due to the focus of the work and the consideration of efficiency, we choose the PID algorithm in this paper, and readers can also choose other algorithms if they are interested. At the same time, because of the reasons mentioned before, we have used an ideal system in this section, and have not considered the disturbances in the control process.

The double closed-loop PID control algorithm contains position and velocity loops, which retain the advantages of the traditional PID algorithm in terms of simple structure and rapid response, and at the same time improve the control effect, and its schematic diagram is shown in Fig. 4.

Fuzzy PID control combines fuzzy control with PID control to improve the robustness of the PID algorithm. Leveraging the Fuzzy toolbox in MATLAB, it is possible to set up the affiliation function and fuzzy rules by fuzzification. The inputs are determined by the rate of change of the speed deviation and the speed deviation, while the outputs yield the adjustments for Kp, Ki, and Kd.

The fuzzy PID control algorithm is expressed as:

$$u(t) = Kp' * e(t) + Ki' \int_0^t e(t)dt + Kd' \frac{de(t)}{dt} \tag{3}$$

In the equation (3):

$$Kp' = Kp + \Delta Kp$$
$$Ki' = Ki + \Delta Ki$$
$$Kd' = Kd + \Delta Kd$$

In this paper, the range of values of e and ec is:

$$\mathrm{e} \in (-3,\ 3), \mathrm{ec} \in -(3,\ 3)$$

The result after transforming the domain of fungible values into a fuzzy theoretical domain is:

$$\mathrm{e} \in (-3,\ -2,\ -1,\ 0,\ 1,\ 2, 3)$$
$$\mathrm{ec} \in (-3,\ -2,\ -1,\ 0,\ 1,\ 2, 3)$$

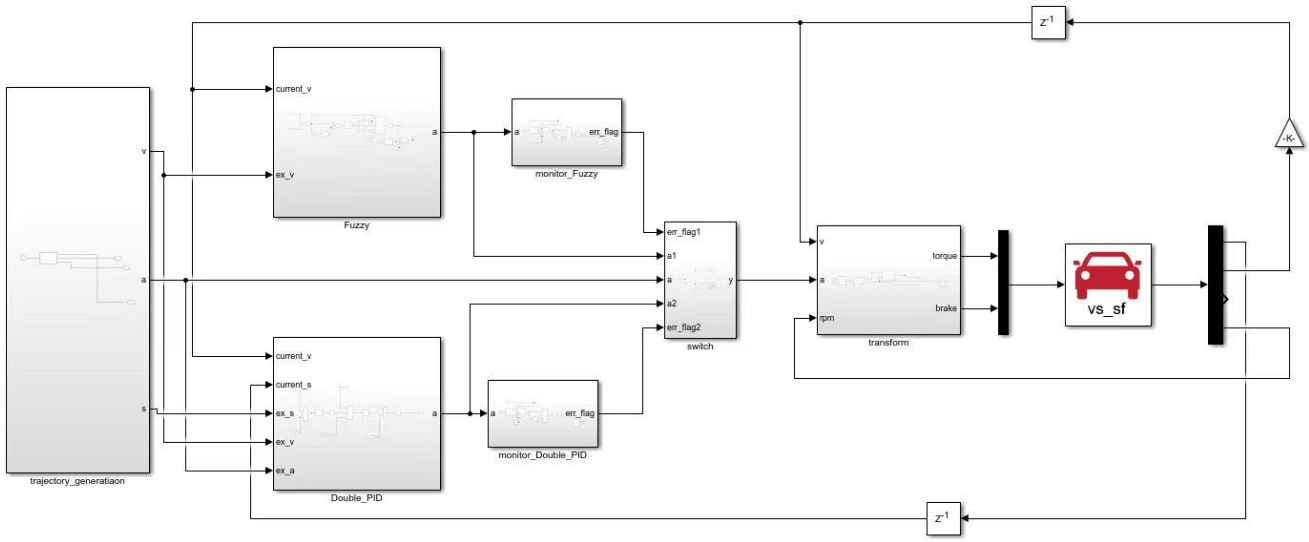

FIGURE 6. Joint simulation model.

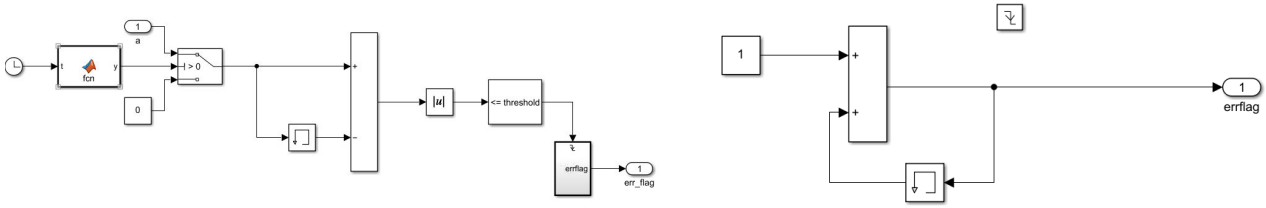

FIGURE 7. Monitoring module and falling edge trigger system.

The fuzzy theory domains of the output results ΔKp, ΔKi, ΔKd are:

$$\begin{aligned}\Delta Kp &\in (8, 9, 10, 11, 12, 13, 14)\\ \Delta Ki &\in (3, 3.5, 4, 4.5, 5, 5.5, 6)\\ \Delta Kd &\in (-0.12, -0.11, -0.10, -0.09,\\ &\quad -0.08, -0.07 - 0.06)\end{aligned}$$

The center of gravity method is used for defuzzification and the center of gravity method is formulated as:

$$Z0 = \frac{\sum_{i=0}^{n} uc(t)zi}{\sum_{i=0}^{n} uc(t)} \tag{4}$$

In the above equation, Z0 is the exact value obtained after defuzzification; uc is the value of affiliation before defuzzification; and zi is the value in the fuzzy control theory domain.

The final relationship between the input and output quantities is obtained in Fig. 5.

B. SIMULATION VERIFICATION

In this paper, Simulink/CarSim is used for joint simulation, and the simulation model is shown in Fig. 6.

The model implements the control algorithm mentioned before, after the planning module gives the corresponding trajectory, the control module can control the acceleration according to the information, and then control the corresponding throttle and brake pedal openings to control the vehicle's operation.

In addition to the control module, monitoring modules are added, as shown in Fig. 7, to monitor the output results of the control module. When a significant error is monitored in the output, the falling edge trigger system is triggered, passing a signal to the switching module so that the switching module can switch the algorithm to ensure the safety of the system.

In the simulation verification, after the vehicle keeps 15 seconds of normal driving, the fault input is carried out, and the acceleration suddenly increases from 0.5m/s^2 to 5 m/s^2, simulating the situation of unintended acceleration of the vehicle. After injecting the fault, the detection module will detect the sudden change of acceleration, determine that the vehicle has a fault, set the fault flag to 1, and pass it to the switching module, after the switching module recognizes the fault flag, it will carry out switching of the control algorithm, the results are shown in Fig. 8. In Fig. 8, the red lines represent planning conditions and the blue lines represent vehicle operations.

We have conducted several simulation experiments and the results are consistent, which shows that the algorithm is stable and reliable. As shown in Fig. 8, when the vehicle has a sudden change in acceleration due to a fault, the system can quickly switch to the redundant control algorithm to effectively maintain control of the vehicle and ensure the driving stability of the vehicle.

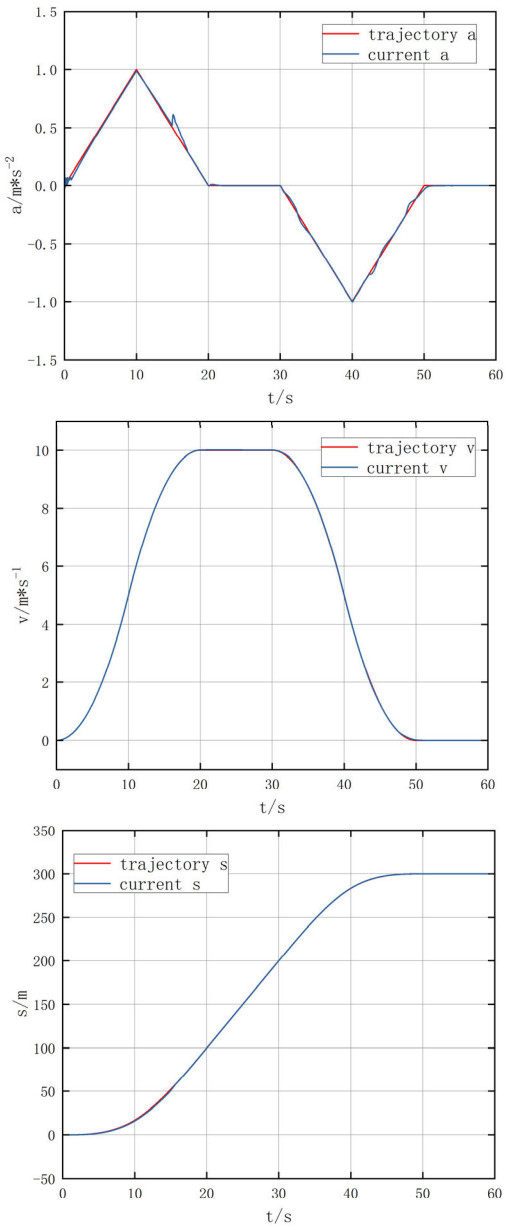

FIGURE 8. Comparison of route, speed, and acceleration.

VI. CONCLUSION

This paper is based on the functional safety development process and related regulations in ISO 26262. The functions and operating environment of the TJP system are defined in detail, and the longitudinal function is taken as an example, analyzed and designed according to the functional safety development process, and simulated and verified by the Simulink/CarSim simulation platform.

Firstly, the system is defined in detail to clarify the system functions, design operation conditions, system configuration and operation scenarios, etc. For the longitudinal functions of the system, hazard analysis and risk assessment are carried out according to the process in ISO 26262, the HAZOP method is used to find out the hazard events, the S/E/C levels of the hazard events are evaluated, the corresponding ASIL levels are further determined, the safety objectives are formed and summarize. After getting the aggregated safety objectives, the FTA and FMEA methods are used to decompose the safety objectives comprehensively, extract the safety requirements, and assign them, and to meet the safety requirements, the 1oo2D architecture is used to ensure the hardware safety. Fuzzy PID and double closed-loop PID control algorithms are used to ensure the safety requirements of the software, and Simulink/CarSim simulation models are built to verify the reliability of the algorithms using fault injection.

Simulation verification results show that the control algorithm is safe and reliable, and can ensure the safety and stability of the vehicle during operation.

REFERENCES

[1] Q. Li and S. Tian, "Environmental and social problems and countermeasures in transportation system under resource constraints," *Complexity*, vol. 2020, pp. 1–11, Dec. 2020.

[2] F. Plestan, J. Davins-Valldaura, S. Moussaoui, and G. Pita-Gil, "Sliding mode observer design for the road curvature estimation in traffic jam pilot system," in *Proc. 14th Int. Workshop Variable Struct. Syst. (VSS)*, Nanjing, China, Jun. 2016, pp. 302–307.

[3] S. M. Pampel, D. R. Large, G. Burnett, R. Matthias, S. Thompson, and L. Skrypchuk, "Getting the driver back into the loop: The quality of manual vehicle control following long and short non-critical transfer-of-control requests: TI: NS," *Theor. Issues Ergonom. Sci.*, vol. 20, no. 3, pp. 265–283, Jan. 2019.

[4] (Sep. 7, 2017). *Audi, Audi AI Traffic Jam Pilot*. Accessed: Oct. 25, 2023. [Online]. Available: https://www.audi-mediacenter.com/en/videos/video/footage-audi-a8-audi-ai-traffic-jam-pilot-3785

[5] (Dec. 13, 2021). *Brad Templeton, Mercedes Gets Approval for Traffic Jam Pilot, Where is Tesla*. Accessed: Oct. 25, 2023. [Online]. Available: https://www.forbes.com/sites/bradtempleton/2021/12/13/mercedes-gets-approval-for-traffic-jam-pilot-where-is-tesla

[6] B. Yi, H. Cao, X. Song, S. Zhao, W. Guo, and M. Li, "How to identify the take-over criticality in conditionally automated driving? An examination using drivers' physiological parameters and situational factors," *Transp. Res. F, Traffic Psychol. Behav.*, vol. 85, pp. 161–178, Feb. 2022.

[7] P. Guo and F. Gao, "Automated scenario generation and evaluation strategy for automatic driving system," in *Proc. 7th Int. Conf. Inf. Sci. Control Eng. (ICISCE)*, Changsha, China, Dec. 2020, pp. 1722–1733.

[8] J. Echeto, M. G. Romana, and M. Santos, "Swarm modelling considering autonomous vehicles for traffic jam assist simulation," in *Proc. 15th Int. Conf. Soft Comput. Models Ind. Environ. Appl. (SOCO)*, Burgos, Spain, 2021, pp. 429–438.

[9] Y. Zhang, C. Wang, R. Yu, L. Wang, W. Quan, Y. Gao, and P. Li, "The AD4CHE dataset and its application in typical congestion scenarios of traffic jam pilot systems," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 5, pp. 3312–3323, May 2023.

[10] S. Wei, Y. Zou, X. Zhang, T. Zhang, and X. Li, "An integrated longitudinal and lateral vehicle following control system with radar and vehicle-to-vehicle communication," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1116–1127, Feb. 2019.

[11] J. Bach, S. Otten, and E. Sax, "A taxonomy and systematic approach for automotive system architectures–from functional chains to functional networks," in *Proc. 3rd Int. Conf. Vehicle Technol. Intell. Transp. Syst.*, Porto, Portugal, 2017, pp. 90–101.

[12] W. He, Y. Zhang, P. An, and H. Chen, "Patent analysis review of automated driving vehicle safety technology," *SCIENTIA SINICA Informationis*, vol. 50, no. 11, p. 1732, Oct. 2020.

[13] *Road Vehicles Safety of the Intended Functionality*, Standard ISO 21448, International Standard Office, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/77490.html

[14] *Road Vehicles-Functional Safety*, Standard ISO 26262, International Standard Office, Geneva, Switzerland, 2018. [Online]. Available: https://www.iso.org/standard/68383.html

[15] K.-L. Lu and Y.-Y. Chen, "Safety-oriented system hardware architecture exploration in compliance with ISO 26262," *Appl. Sci.*, vol. 12, no. 11, p. 5456, May 2022.
[16] D. Marcos, M. Garmendia, J. Crego, and J. Cortajarena, "Functional safety BMS design methodology for automotive lithium-based batteries," *Energies*, vol. 14, no. 21, p. 6942, Oct. 2021.
[17] C. Huang and L. Li, "Architectural design and analysis of a steer-by-wire system in view of functional safety concept," *Rel. Eng. Syst. Saf.*, vol. 198, Jun. 2020, Art. no. 106822.
[18] J. Guo, G. J. Xu, J. J. Wu, L. Yang, and H. Deng, "The development and trend of vehicle functional safety," in *Proc. 6th Int. Conf. Smart Comput. Commun. (SmartCom)*, New York, NY, USA, 2021, pp. 470–480.
[19] X. Xia, W. Xi, H. Li, and Y. Wang, "Application and comparison of STPA and functional safety analysis in ACC system," in *Proc. 6th Int. Conf. Electromechanical Control Technol. Transp. (ICECTT)*, Chongqing, China, Feb. 2022, pp. 1085–1093.
[20] G. Xie, W. Wu, G. Zeng, R. Li, and S. Hu, "Risk assessment and development cost optimization in software defined vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3675–3686, Jun. 2021.
[21] P. Kilian, A. Köhler, P. Van Bergen, C. Gebauer, B. Pfeufer, O. Koller, and B. Bertsche, "Principle guidelines for safe power supply systems development," *IEEE Access*, vol. 9, pp. 107751–107766, 2021.
[22] L. Chen, D. Fan, J. Zheng, and X. Xie, "Functional safety analysis and design of sensors in robot joint drive system," *Machines*, vol. 10, no. 5, p. 360, May 2022.
[23] Y. Fang, W. Wang, C. Yang, Y. Zhang, and Z. Chen, "Brake-by-wire architecture design and analysis in accordance with functional safety standard," *Proc. Inst. Mech. Eng., D, J. Automobile Eng.*, Jul. 2023, Art. no. 15.
[24] E. de Gelder, H. Elrofai, A. K. Saberi, J.-P. Paardekooper, O. O. den Camp, and B. de Schutter, "Risk quantification for automated driving systems in real-world driving scenarios," *IEEE Access*, vol. 9, pp. 168953–168970, 2021.
[25] K. Meng, R. Zhou, Z. Li, and K. Zhang, "A quantitative approach of generating challenging testing scenarios based on functional safety standard," *Appl. Sci.*, vol. 13, no. 6, p. 3494, Mar. 2023.
[26] German Bundestag. (May 14, 2019). *Pegasus Research Project*. Accessed: Oct. 25, 2023. [Online]. Available: https://www.pegasusprojekt.de/en/about-PEGASUS
[27] E. Thorn, S. C. Kimmel, and M. Chaka, "A framework for automated driving system testable cases and scenarios," Dept. Transp. National Highway Traffic Safety Administration, Washington, DC, USA, Tech. Rep. DOT HS 812 623, 2018.
[28] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, "Hazard and operability (HAZOP) analysis. A literature review," *J. Hazardous Mater.*, vol. 173, nos. 1–3, pp. 19–32, Jan. 2010.
[29] J. Krampe and M. Junge, "Deriving functional safety (ISO 26262) S-parameters for vulnerable road users from national crash data," *Accident Anal. Prevention*, vol. 150, Feb. 2021, Art. no. 105884.
[30] M. Yazdi, J. Mohammadpour, H. Li, H. Huang, E. Zarei, R. G. Pirbalouti, and S. Adumene, "Fault tree analysis improvements: A bibliometric analysis and literature review," *Qual. Rel. Eng. Int.*, vol. 39, no. 5, pp. 1639–1659, Jul. 2023.
[31] J. Huang, J.-X. You, H.-C. Liu, and M.-S. Song, "Failure mode and effect analysis improvement: A systematic literature review and future research agenda," *Rel. Eng. Syst. Saf.*, vol. 199, Jul. 2020, Art. no. 106885.
[32] J. F. W. Peeters, R. J. I. Basten, and T. Tinga, "Improving failure analysis efficiency by combining FTA and FMEA in a recursive manner," *Rel. Eng. Syst. Saf.*, vol. 172, pp. 36–44, Apr. 2018.
[33] S. Wang, Y. Hui, X. Sun, and D. Shi, "Neural network sliding mode control of intelligent vehicle longitudinal dynamics," *IEEE Access*, vol. 7, pp. 162333–162342, 2019.
[34] J. Guo, Y. Luo, K. Li, and L. Guo, "Adaptive dynamic surface longitudinal tracking control of autonomous vehicles," *IET Intell. Transp. Syst.*, vol. 13, no. 8, pp. 1272–1280, Aug. 2019.
[35] Y. Lu and L. Bi, "Human behavior model-based predictive control of longitudinal brain-controlled driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1361–1374, Mar. 2021.
[36] J. Yang, W. Peng, and C. Sun, "A learning control method of automated vehicle platoon at straight path with DDPG-based PID," *Electronics*, vol. 10, no. 21, p. 2580, Oct. 2021.
[37] Y. Kebbati, N. Ait-Oufroukh, V. Vigneron, D. Ichalal, and D. Gruyer, "Optimized self-adaptive PID speed control for autonomous vehicles," in *Proc. 26th Int. Conf. Autom. Comput. (ICAC)*, Portsmouth, U. K., Sep. 2021, pp. 1–6.
[38] C. Yang and J. Liu, "Trajectory tracking control of intelligent driving vehicles based on MPC and fuzzy PID," *Math. Problems Eng.*, vol. 2023, pp. 1–24, Feb. 2023.
[39] R. Li, S. Deng, and Y. Hu, "Autonomous vehicle modeling and velocity control based on decomposed fuzzy PID," *Int. J. Fuzzy Syst.*, vol. 24, no. 5, pp. 2354–2362, Jul. 2022.

LEI HE received the Ph.D. degree from Jilin University, Changchun, China, in 2011. He is currently a Professor with the State Key Laboratory of Automotive Simulation and Control, Jilin University. He is the author or coauthor of numerous publications in the field of environmental awareness and vehicle control and also responsible for several state-funded intelligent driving modeling and simulation government projects.

JUNYI CHEN is currently pursuing the M.S. degree in automotive engineering with the State Key Laboratory of Automotive Simulation and Control, Jilin University, Changchun, China. His research interests include functional safety and trajectory planning.

XIUCAI ZHANG is currently pursuing the M.S. degree in automotive engineering with the State Key Laboratory of Automotive Simulation and Control, Jilin University, Changchun, China. His research interest includes V2X infrastructure-side multi-target detection.

JUN LI received the master's degree from Jilin University. He is currently a Senior Engineer with China First Automobile Works Corporation. His research interests include functional safety of power and chassis systems (vehicle failure behavior acceptance criterion).

JINGQUAN TIAN received the master's degree from Jilin University. He is currently an Assistant Engineer with China First Automobile Works Corporation. His research interests include intelligent cockpit, body comfort, and functional safety of vehicle-end internet connection.