IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 April 2024, accepted 21 May 2024, date of publication 24 May 2024, date of current version 3 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3404958

RESEARCH ARTICLE

Highly Redundant Safety Scheme and Its Experimental Validation for the Electronic-Controlled Pneumatic Braking System of Commercial Vehicle for Autonomous Driving

HANWEI BAO, KEYU WANG, XIAOXU WEI, YI CHENG, MINGMING ZHAO, AND GANGYAN LI

School of Mechanical and Electrical Engineering, Wuhan University of Technology, Wuhan 430070, China

Corresponding author: Gangyan Li (gangyanli@whut.edu.cn)

This work was supported by Hubei Province Key Research Program which cooperated with the SMC Corporation under Project 2022BAA077 and Project 20221h0530.

ABSTRACT With the relentless progression in autonomous driving and chassis control technologies, the safety requirements for commercial vehicle braking systems have intensified. Ensuring the safety and reliability of these systems during operation has become crucial. This study focuses on the automatic pressure regulating in commercial vehicles. To meet the evolving demands and safety standards of autonomous driving and chassis control technologies, this study incorporates theoretical methodologies including relevant standards and fault tree analysis. The research systematically categorizes and assesses failure modes of the automatic regulating valve, proposing a concept and framework for ensuring high redundancy safety. Validating the correctness and feasibility of the high redundancy safety scheme for the automatic regulating valve was accomplished through fault injection methods. Results indicate that the high redundancy safety scheme effectively diagnoses and manages faults, thereby guaranteeing the valve's pressure regulation capability even under fault conditions. This approach provides invaluable insights into the safety and reliability design for commercial vehicles and their components, offering essential theoretical underpinnings for the progression of autonomous driving and chassis control technologies in commercial vehicles.

INDEX TERMS Automatic pressure regulating valve, commercial vehicles, fault tree analysis, fault injection testing, high redundancy safety.

I. INTRODUCTION

With the rapid evolution of autonomous driving and chassis control technologies, commercial vehicle braking systems are undergoing a significant transformation to-wards enhanced electronic integration. This shift, while advancing the technological frontier, also introduces amplified challenges in terms of reliability and safety. As such, safeguarding the operational safety and reliability of these braking systems has emerged as an imperative task.

In response to these complexities, scholars globally are primarily adopting advanced analytical methodologies, such as fault tree analysis and failure mode and effects analysis. These approaches meticulously dissect and examine the causes, modes, and impacts of failures within different components of the system. This analysis serves as a foundation for optimizing and improving system designs. Pan et al. [1] examined the causes of faults in automotive differentials,

The associate editor coordinating the review of this manuscript and approving it for publication was Guillermo Valencia-Palomo.

establishing a fault tree model for these components. Their analysis produced a fault spectrum for automotive differentials, providing methods for their design, fault diagnosis, and maintenance. Popovic et al. [2] proposed a reliability analysis method for automotive powertrain systems based on Failure Mode, Effects, and Criticality Analysis (FMECA). They assessed the failure modes and associated risks within the system, providing a basis for reliability design. Chen et al. [3] applied Fault Tree Analysis (FTA) techniques to electronic com-ponents, elaborating on methods for fault tree analysis of these components. Their approach included manual construction, qualitative, and quantitative analysis of fault trees. Through this analysis, potential failure causes were identified, primary failure reasons were scrutinized, and corresponding preventive measures were suggested. Lee et al. [4] introduced an automated Failure Mode and Effects Analysis (FMEA) tool and developed a Simulink simulation model for an electronic fuel injection system. They employed the Simulink model to perform simulation analysis of this automated FMEA tool. The simulation results indicated that, compared to traditional FMEA analysis tools, this tool could automatically analyze causal relationships between failure modes and effects, thereby generating FMEA reports automatically. Aized T [5] conducted a potential failure analysis during the design and manufacturing process of automotive leaf springs. They utilized Failure Mode and Effects Analysis (FMEA) to evaluate 42 potential failures that could occur within automotive leaf springs. They determined high-potential failures based on four scoring criteria: severity, occurrence rate, detectability, and Risk Priority Number (RPN)Zhou et al. [6] focused on proposing a novel hybrid approach to effectively assess failure modes in vehicles during operation. Xu et al. [7] explored the complex field-circuit coupling system of permanent magnet synchronous motors in electric vehicles, discussing fault forms, diagnostic methods, and the current state of research. Xiong et al. [8] discussed various faults in battery systems, such as sensor, actuator, short circuit, overcharge/over-discharge, connection, inconsistency, insulation, and thermal management system failures. They analyzed causes and effects related to sensors, batteries, components, and actuators, exploring the existence of faults in electric vehicle battery systems along with diagnostic methods. Naranje et al. [9] utilized the Design Failure Mode and Effects Analysis (DFMEA) method to identify and analyze potential failure modes in Electrically Converted Vehicles (ECVs) and their impact on vehicle operation. They studied potential failure modes in electrical and mechanical systems like batteries, electric motors, and transmissions, evaluating their severity, occurrence probabilities, and detectability. Xie et al. [10], [11] summarized the latest advancements in automotive functional safety design methodologies. This encompassed functional safety analysis, assurance, cost optimization in safety perception, and safety-critical multi-function scheduling. Addressing safety-critical systems like Advanced Driver Assistance Systems (ADAS) and autonomous vehicles, they discussed the introduction of redundancy in system architecture and proposed an innovative analytical framework.

Research on redundant safety measures is relatively limited. The common approach involves utilizing failure analysis and fault analysis to identify components or structures within a system that are most prone to failure. These analyses aid in con-ducting quantitative assessments to ensure the system's safety and reliability. The redundant requirements derived from these analyses serve as the foundation for redundant design. Wang et al. [12] implemented a dual-redundancy electronic steering system for vehicles, comprising two similar sets of controller modules, sensor modules, and actuator modules. Through appropriate redundant management mechanisms, it achieves heightened safety performance. Klomp et al. [13] addressed issues concerning autonomous driving, such as path tracking and vehicle motion control. They used differential braking to achieve redundant steering. Simulation results demonstrated that differential braking can offer heterogeneous redundancy, ensuring safe steering in the event of a steering system failure in autonomous vehicles. Kissai et al. [14] investigated a novel method ensuring safety through complementarity among diverse chassis systems. They employed optimization-based control allocation algorithms to find optimal control logic for complementing chassis systems. Results indicated that one system can take over control from another in the event of system failure, showcasing high fault tolerance and reconfigurability in control logic. Mi et al. [13] addressed safety concerns in wire-controlled steering systems by proposing a du-al-redundant wire-controlled steering system. They built an experimental system and validated it through fault injection tests, demonstrating the system's ability to operate normally in the event of a single electrical system failure. Habn et al. [15] presented a fault diagnosis method for differential braking systems, employing empirical model-based open-loop estimation, robust estimation, and adaptive estimation techniques for fault diagnosis. Simulation results showcased effective fault diagnosis of the differential braking system, enhancing vehicle active safety. Bao et al. [16], [17], [18] designed an electronically controlled air pressure braking system with an automatic pressure regulating valve for commercial vehicles targeted at driving automation. Through comparative structural analysis via simulation and experiments, they verified that the electronically controlled, human-independent decoupling structure of the automatic pressure regulating valve effectively enhances braking safety and reliability, meeting both commercial vehicle braking requirements and the needs of autonomous driving. Bansal A [19] developed the Synergistic Redundancy (SR) system architecture, offering a verifiable safety solution for complex physical systems like advanced intelligent driving vehicles.

The study focuses on the electronically controlled pneumatic braking system's automatic pressure regulating valve in commercial vehicles. In an effort to align with the rapidly

evolving demands of autonomous driving and chassis control technologies, while simultaneously upholding stringent safety standards, the research leverages theoretical methodologies such as fault tree analysis and relevant industry standards. This approach facilitates a detailed classification and assessment of failure levels in the automatic regulating valve. Furthermore, the study pioneers a novel concept and framework for high redundancy safety, meticulously validating its feasibility and precision through fault injection methods. The findings affirm that the high redundancy safety strategy proficiently diagnoses and rectifies faults, thereby ensuring the valve's robust pressure regulation capability, even amidst malfunction scenarios. This groundbreaking high redundancy safety paradigm for the automatic pressure regulating valve, within the realm of electronically controlled pneumatic braking systems in commercial vehicles, illuminates new pathways for enhancing the safety and reliability designs of commercial vehicle components. It lays a solid foundation, offering pivotal theoretical support for the continuous progression of autonomous driving and chassis control technologies in the commercial vehicle sector.

This article focuses on the research of the electronic controlled pneumatic pressure regulating valve for commercial vehicles. In order to meet the development requirements and safety standards of autonomous driving and chassis domain control technology, it combines relevant standards and theoretical methods such as fault tree analysis to classify and assess the failure levels of the automatic pressure regulating valve. It proposes the concept and solution of high-redundancy safety and verifies the correctness and feasibility of the high-redundancy safety solution for the automatic pressure regulating valve through fault injection. The results show that the high-redundancy safety solution for the automatic pressure regulating valve can effectively diagnose and handle faults, ensuring the pressure regulating capability of the valve under faulty conditions. The proposed high-redundancy safety solution and concept for the electronic controlled pneumatic pressure regulating valve of commercial vehicles can provide ideas for the safety design and reliability design of commercial vehicles and their components, and provide a theoretical basis for the development of autonomous driving and chassis domain control technology in commercial vehicles.

II. THE AUTOMATIC PRESSURE REGULATING VALVE AND ITS FAULT STATES

A. ELECTRONIC-CONTROLLED PNEUMATIC BRAKING SYSTEM OF COMMERCIAL VEHICLE

The primary feature of the braking system in commercial vehicles designed for autonomous driving is the addition of an automatic braking mode. This mode aims to alleviate the driving tasks and pressures on the driver, thereby enhanced safety, stability, and smoothness in the braking process of commercial vehicles. Furthermore, it prioritizes the comfort of both the driver and passengers.

The Electronic-Controlled Pneumatic Braking System of Commercial Vehicle enhances the pressure adjustment method by integrating electronic control with pneumatic operation, thereby augmenting the existing functionalities of the human-controlled pneumatic braking system. This system incorporates high-precision sensors to facilitate automatic braking, effectively adapting to the evolving demands of autonomous driving and intelligent braking systems. As depicted in Figure 1.

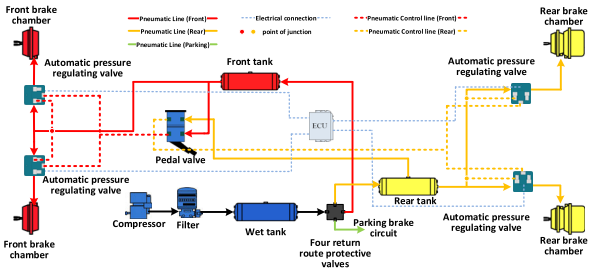


FIGURE 1. Schematic of the electronic-controlled pneumatic braking system of commercial vehicle.

B. THE CONCEPT OF AUTOMATIC PRESSURE REGULATING VALVE AND ITS HIGH REDUNDANCY SAFETY

As depicted in Figure 2, the Automatic Pressure Regulating Valve serves as the core pressure regulation component in the commercial vehicle's electronically controlled pneumatic braking system, playing a pivotal role in ensuring vehicle safety. Apart from fulfilling the fundamental braking functions in commercial vehicles, the automatic pressure regulating valve must also possess high safety and reliability standards. This ensures that the braking system of commercial vehicles maintains adequate braking capabilities even in the event of a single-point failure.

The high redundancy safety concept of the automatic pressure regulating valve involves adding backup components, implementing redundancy measures, establishing fault prediction, control switching, and recovery mechanisms. It also maintains independence among multiple separate components and sensors. This ensures that in the event of a primary system failure, the backup system can take over operations, maintaining high performance and availability. This approach counteracts single-point failures, ensuring stable system operation and safety.

C. THE FAULT STATES OF THE AUTOMATIC PRESSURE REGULATING VALVE AND THEIR SAFETY IMPLICATIONS

The electronically controlled pneumatic braking system's automatic pressure regulating valve receives signals directly from the controller during operation. It executes pressure adjustment tasks designated by the controller and concurrently feeds back the output pressure signal to the controller. The automatic pressure regulating valve might encounter the following fault states during its operation:

(1) Loss of electronic control functionality in the automatic pressure regulating valve.

TABLE 1. Fault states and safety impact of the automatic pressure regulating valve.

Fault ID	Fault Name	Driving Condition	Safety Impact of the Fault	ASIL Level
1	Loss of Electronic Control Functionality	Vehicle in Motion	Unable to Control Braking Electronically	D
2	Loss of Electronic Control Functionality	Vehicle at Standstill	Vehicle at Standstill	QM
3	Inability to Switch Braking Circuit	Vehicle in Motion	Unable to Control Braking Electronically	D
4	Inability to Switch Braking Circuit	Vehicle at Standstill	Vehicle at Standstill	QM
5	Insufficient Braking Force Output from Electronic Control	High-Speed Travel	Excessive Braking Distance or Excessive Rapid Braking Release	D
6	Insufficient Braking Force Output from Electronic Control	Low-Speed Travel	Excessive Braking Distance or Excessive Rapid Braking Release	C
7	Excessive Braking Force Output from Electronic Control	High-Speed Travel	Excessive Braking, Vehicle Forced Stoppage, or Inability to Release Brakes	D
8	Excessive Braking Force Output from Electronic Control	Low-Speed Travel	Excessive Braking, Vehicle Forced Stoppage, or Inability to Release Brakes	A

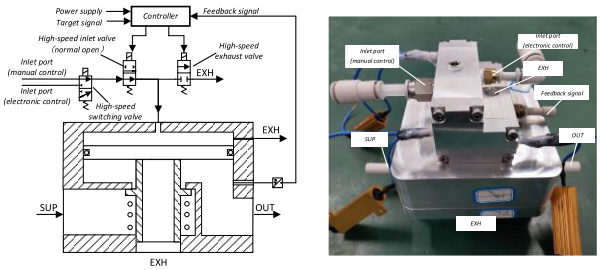


FIGURE 2. Schematic and physical structure of the automatic pressure regulating valve.

The electronic control functionality of the automatic pressure regulating valve primarily relies on continuous actions of the high-speed intake valve and high-speed exhaust valve. The controller generates the necessary control signals based on the difference between the outlet gas pressure of the automatic pressure regulating valve and the target braking pressure, enabling electronic control. Loss of electronic control functionality would impede the ability to achieve electronic pressure regulation.

(2) Inability to switch the braking circuit.

The switching between manual control of the braking circuit and electronic control relies on the action of the high-speed switching valve. The high-speed switching valve defaults to connecting the manual control braking circuit and, when powered, connects to the electronic control braking circuit. In the event of the inability to switch between braking circuits, the system will only be capable of manual control braking.

(3) Insufficient braking force output from electronic control.

The reasons for insufficient braking force output from electronic control are com-plex and can stem from various sources such as faults in the pressure sensor, high-speed solenoid valve, and others. During vehicle braking, insufficient braking force output from electronic control may result in excessively long braking distances or failure to complete braking. During the release of braking in the vehicle, insufficient braking force may lead to excessively rapid braking release.

(4) Excessive braking force output from electronic control.

During vehicle braking, excessive braking force output from electronic control can lead to the vehicle braking excessively, forcing the vehicle to come to an abrupt stop. During the release of braking, excessive braking force output from electronic control may prevent the vehicle from releasing the brakes.

ISO 26262 standard defines Automotive Safety Integrity Levels (ASIL), providing the fault states and safety impact of the automatic pressure regulating valve as indicated in Table 1 below.

III. FAULT TREE ANALYSIS OF THE AUTOMATIC PRESSURE REGULATING VALVE AND HIGH REDUNDANCY SAFETY REQUIREMENTS

A. FAULT TREE ANALYSIS OF THE AUTOMATIC PRESSURE REGULATING VALVE

Regarding the four higher ASIL-level faults associated with the automatic pressure regulating valve, using a fault tree analysis to consider them as top events, identifying component failures leading to the failure of the automatic pressure regulating valve. The fault tree analysis is shown in the figure 3 and figure 4.

Through fault tree analysis, the component failures corresponding to the four highest ASIL-level fault states of the automatic pressure regulating valve are presented in Table 2. The failures of the automatic pressure regulating valve mainly involve the high-speed switching valve, high-speed intake valve, high-speed exhaust valve, and pressure sensor. The primary fault modes of the pressure sensor include sensor supply voltage failure and sensor output signal failure. As for the high-speed solenoid valve, the primary fault modes encompass valve core sticking, electromagnetic coil short-circuit, and electromagnetic coil open-circuit failures.

TABLE 2. Component failure states of the automatic pressure regulating valve.

Fault Component	Fault State
High-Speed Switching Valve	Short Circuit, Open Circuit in Electromagnetic Coil Sticking Valve Core in High-Speed Solenoid Valve
High-Speed Intake Valve	Short Circuit, Open Circuit in Electromagnetic Coil Sticking Valve Core in High-Speed Solenoid Valve
High-Speed Exhaust Valve	Short Circuit, Open Circuit in Electromagnetic Coil Sticking Valve Core in High-Speed Solenoid Valve
Pressure Sensor	Power Supply Failure Output Signal Failure

TABLE 3. High redundancy safety requirements for the automatic pressure regulating valve.

Fault State	Driving State	ASIL Level	Redundancy Safety Requirements
Loss of Electronic Control Functionality	Vehicle in motion	D	Implement functional checks, establish redundancy schemes to ensure emergency braking can be achieved through manual control.
Inability to Switch Braking Circuit	Vehicle in motion	D	Monitor the switching valve and establish redundancy schemes to ensure the braking circuit can switch properly.
Insufficient Braking Force Output in Electronic Control	High-Speed Travel Low-Speed Travel	D C	Monitor the intake and exhaust valves and establish redundant pressure regulation schemes.
Excessive Braking Force Output in Electronic Control	High-Speed Travel	D	Monitor the intake and exhaust valves, and establish redundant pressure regulation schemes.

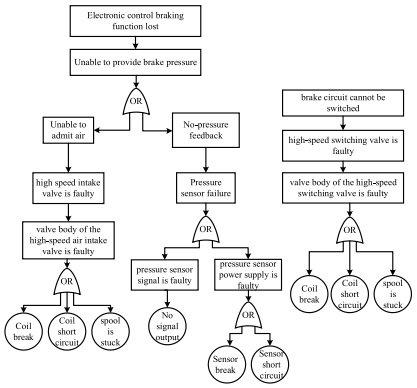


FIGURE 3. Fault tree analysis of loss of electronic control functionality and inability to switch braking circuit.

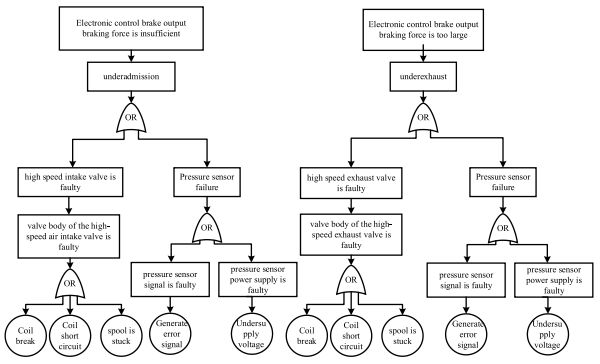


FIGURE 4. Fault tree analysis of insufficient or excessive braking force output in electronic control.

B. HIGH REDUNDANCY SAFETY REQUIREMENTS FOR THE AUTOMATIC PRESSURE REGULATING VALVE

Based on the four higher ASIL-level fault states of the automatic pressure regulating valve and the types of component failures causing these fault states, the corresponding high redundancy safety requirements for each fault state are presented in Table 3.

IV. AUTOMATIC PRESSURE REGULATING VALVE HIGH REDUNDANCY SAFETY MECHANISM

A. HIGH REDUNDANCY SAFETY SCHEME FOR AUTOMATIC PRESSURE REGULATING VALVE

Each of the high-speed switching valve, high-speed intake valve, and high-speed exhaust valve features a dual solenoid coil structure, enhancing operational reliability. The electromagnetic forces generated by the two coils collectively act on the armature and main valve core. In case of a short circuit or open circuit fault in one coil, single-coil pressure adjustment can be achieved, enhancing its reliability. Additionally, primary pressure sensors and redundant pressure sensors are placed at the outlet of the automatic pressure regulating valve. If the primary pressure sensor malfunctions, the system switches promptly to the redundant pressure sensor to ensure proper pressure detection and feedback. Current within the dual coils of the high-speed switching valve, high-speed intake valve, and high-speed exhaust valve is monitored for anomalies solenoid coil short circuits, open circuits, and valve core sticking faults. The redundancy safety scheme of the automatic pressure regulating valve is depicted in Table 4.

TABLE 4. Redundancy safety scheme of automatic pressure regulating valve.

Faulty Components	Fault States	Redundancy Safety Scheme
High-speed switching valve	Short circuit of electromagnetic coil Open circuit of electromagnetic coil Stuck valve core of high-speed solenoid valve	Check the drive signal of the high-speed switch valve and perform checks for circuit interruption, short circuit, and valve core jamming. Implement dual-coil redundancy for the high-speed switch valve to enhance reliability and ensure the ability to switch to manual control for braking.
High-speed intake valve	Short circuit of electromagnetic coil Open circuit of electromagnetic coil Stuck valve core of high-speed solenoid valve	Check the drive signal of the high-speed intake valve and conduct tests for circuit interruption, short circuit, and valve core jamming. Implement dual-coil redundancy for the high-speed intake valve to enhance reliability and ensure pressure build-up through electronic control.
High-speed exhaust valve	Short circuit of electromagnetic coil Open circuit of electromagnetic coil Stuck valve core of high-speed solenoid valve	Check the drive signal of the high-speed exhaust valve and conduct tests for circuit interruption, short circuit, and valve core jamming. Implement dual-coil redundancy for the high-speed exhaust valve to enhance reliability and ensure pressure control through electronics.
Pressure sensor	Power supply failure Output signal failure	Check the output signal of the pressure sensor and establish dual-pressure sensor redundancy to enhance reliability.

B. AUTOMATIC PRESSURE REGULATING VALVE HIGH REDUNDANCY SAFETY HANDLING MECHANISM

To ensure better response to various fault states, the Automatic Pressure Regulating Valve features three operational modes: normal electronic control braking mode, redundant braking mode, and manual control braking mode. Each mode is designed to address different fault conditions.

(1) Normal Electronic Control Braking Mode: The Automatic Pressure Regulating Valve operates without any faults, receiving signals from the controller and adjusting braking pressure through electronic control.

(2) Redundant Braking Mode: In the event of a failure in electronic control, the redundant backup scheme takes over to address such faults. It involves substituting redundant backup components for the faulty ones to ensure the integrity of the braking function.

(3) Manual Control Braking Mode: In this mode, if the electronic control failure cannot be addressed by the redundant backup, the system switches to manual control. The high-speed solenoid valve reverts to its default state, and braking is manually controlled to facilitate the braking process.

The paper considers only single-point failures. The redundant safety handling mechanism of the automatic pressure regulating valve is shown in Table 5.

V. THE EXPERIMENTAL VALIDATION SYSTEM FOR THE HIGH-REDUNDANCY SAFETY SCHEME OF THE AUTOMATIC PRESSURE REGULATING VALVE

For the experimental validation system, components were selected based on the high-redundancy safety scheme of the automatic pressure regulating valve in the commercial vehicle's electronic-controlled pneumatic braking system. Combining redundant safety software and hardware circuit boards, the high-redundancy safety test system for the automatic pressure regulating valve was assembled, as depicted in Figure 5.

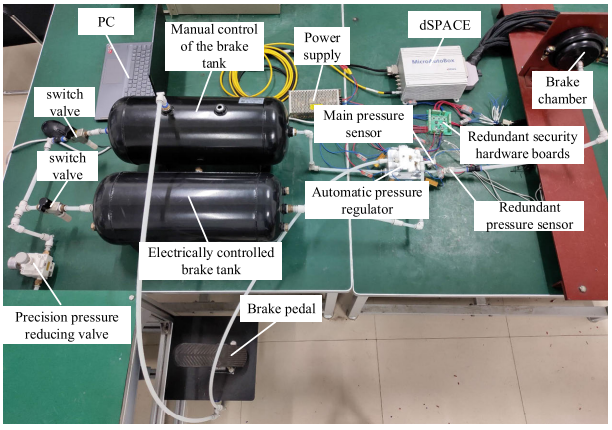


FIGURE 5. High redundancy safety test system for automatic pressure regulating valve.

In this paper, MATLAB/Simulink software is used to build the control algorithm and fault injection algorithm model, The dSPACE is used as the controller, and the action of automatic pressure regulating valve is controlled by redundant safety hardware circuit. The test system includes manually controlled braking tanks and electronically controlled braking tanks. The manually controlled braking tank is connected to the brake pedal, enabling pedal-controlled braking. The high-speed solenoid valve of the automatic pressure regulating valve operates in a dual-coil mode, powered independently by redundant safety hardware circuit boards, allowing single-coil control regulation if one coil fails. Pressure sensors (main and redundant) are installed at the outlet

TABLE 5. Redundant safety handling mechanisms of the automatic pressure regulating valve.

Fault Status	Fault Handling Approach	Operating Mode	Warning Signal
Primary Pressure Sensor Fault	Switch to Redundant Pressure Sensor	Redundant backup braking mode.	Prompt the driver to conduct timely fault diagnosis and repair.
Single Coil Failure in High-Speed Switching Valve	Increase the drive voltage to achieve single-coil braking.		
Single Coil Failure in High-Speed Inlet Valve	Increase the drive voltage to achieve single-coil braking.		
Single Coil Failure in High-Speed Exhaust Valve	Increase the drive voltage to achieve single-coil braking.		
Sticking Failure of High-Speed Switching Valve	Switch to manual control braking.	Manual control braking mode.	Remind the driver to engage in braking promptly.
Sticking Failure of High-Speed Intake Valve	Switch to manual control braking.		
Sticking Failure of High-Speed Exhaust Valve	Switch to manual control braking.		

of the automatic pressure regulating valve to measure and provide feedback on the gas pressure.

VI. EXPERIMENTAL VALIDATION OF HIGH REDUNDANCY SAFETY MEASURES FOR AUTOMATIC PRESSURE REGULATING VALVES

A. MAIN AIR PRESSURE SENSOR FAULT INJECTION TEST

The pressure sensor fault injection test for the high redundancy safety scheme of the automatic pressure regulating valve mainly includes no signal output fault, output drift fault, and output gain change fault.

(1) No signal output fault: Setting the feedback signal of the main pressure sensor to zero.

(2) Output drift fault: Adding a pressure value of 0.1MPa to the feedback signal of the main air pressure sensor.

(3) Output gain change fault: Amplifying the feedback signal of the main air pressure sensor by 1.2 times

When setting the target pressure of the automatic pressure regulating valve to 0.7MPa with a step signal, the fault injection was applied to the main pressure sensor, resulting in the curve shown in Figure 5. Upon diagnosing a fault in the main pressure sensor, the redundant safety system generates a fault indication signal, and subsequent pressure regulation will rely on the redundant pressure sensor. As depicted in the right figure, despite changes in the feedback pressure value from the main pressure sensor, the outlet pressure of the automatic pressure regulating valve remains at the target pressure of 0.7MPa.

B. SINGLE COIL FAILURE FAULT INJECTION TEST

When the input and output voltage levels align, diagnosing pin outputs a high voltage, indicating normal operation of the solenoid coil. If the input is low while the output shows a high-impedance state (a high resistance value), the diagnosing pin outputs a low voltage, demonstrating an open-circuit fault in the solenoid coil. If the input is high and the output is low, indicating a short-circuit fault in the coil, the chip triggers an overheating protection, cutting off power to the circuit. Simultaneously, the diagnosing pin outputs a low voltage.

The solenoid valve design of the automatic pressure regulating valve is a dual-coil structure, with each coil independently driven by redundant safety hardware. With the target pressure set at 0.7MPa and the automatic pressure regulating valve functioning normally, maintaining a stable outlet pressure, the pressure response curve of the automatic pressure regulating valve is shown in Figure 7 after disconnecting one coil of the high-speed solenoid valve.

Figure 8 shows the results of the single-coil fault injection test for the high-speed intake valve and high-speed exhaust valve of the automatic pressure regulating valve, with the target pressure set as a sinusoidal signal with a frequency of 0.5Hz, an amplitude of 0.35MPa, and a bias of 0.35MPa.

According to Figures 7 and 8, it's evident that when a single-coil fault occurs in the automatic pressure regulating valve, its electromagnetic force is reduced, the magnetic field coverage is reduced, the overall solenoid valve spool action is delayed, so that its pressure regulation performance is affected, resulting in pressure fluctuations. However, it can still achieve pressure regulation, ensuring the vehicle's basic braking or degraded braking functionality.

C. VALVE CORE STICKING FAULT INJECTION TEST

The valve core sticking fault injection test is implemented through redundant safety software. Figure 6 represents the electromagnetic coil currents of the high-speed solenoid valve, both during normal operation and when the valve core is stuck, collected by the redundant safety hardware circuit board of the automatic pressure regulating valve. Utilizing software, the input to the valve core sticking fault diagnosis

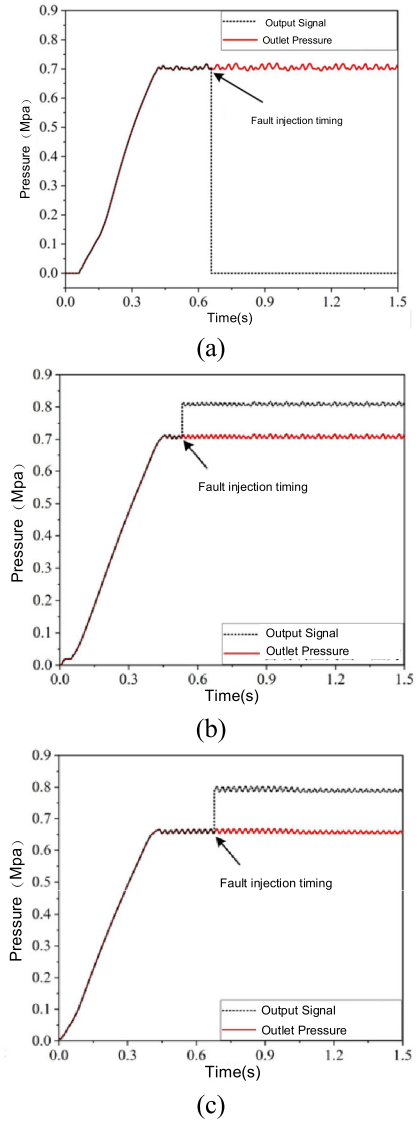


FIGURE 6. Step target pressure main air pressure sensor fault injection test (a) No signal output fault (b) Output drift fault (c) Output gain change fault.

module of the high-speed solenoid valve is switched from the coil current during normal operation to the coil current when the valve core is stuck, thus injecting the fault. The valve core sticking fault diagnosis module receives different current signals, generates distinct fault codes, and completes the transition of the braking mode.

Using software, the electromagnetic valve's coil current is switched from the normal operational state to the coil current when the valve core is stuck, effectively injecting the valve core sticking fault. In the valve core sticking fault injection test for the three types of solenoid valves in the automatic pressure regulating valve, the results are shown in Figure 9. When the valve core sticking fault occurs, the automatic pressure regulating valve automatically switches to manual control braking mode. The driver presses the brake pedal,

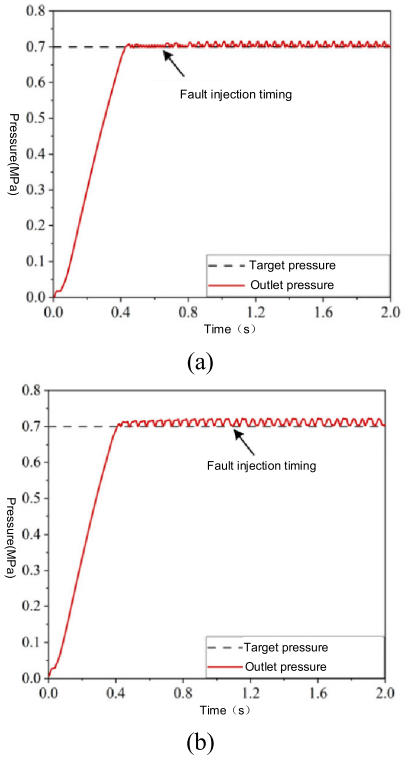


FIGURE 7. Step target pressure single coil fault injection test (a) Intake valve single coil fault injection (b) Exhaust valve single coil fault injection.

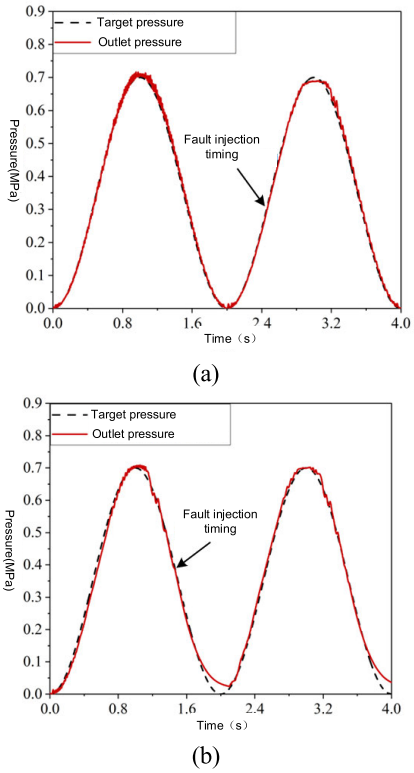


FIGURE 8. Sinusoidal target pressure single coil fault injection test (a) Intake valve single coil fault injection (b) Exhaust valve single coil fault injection.

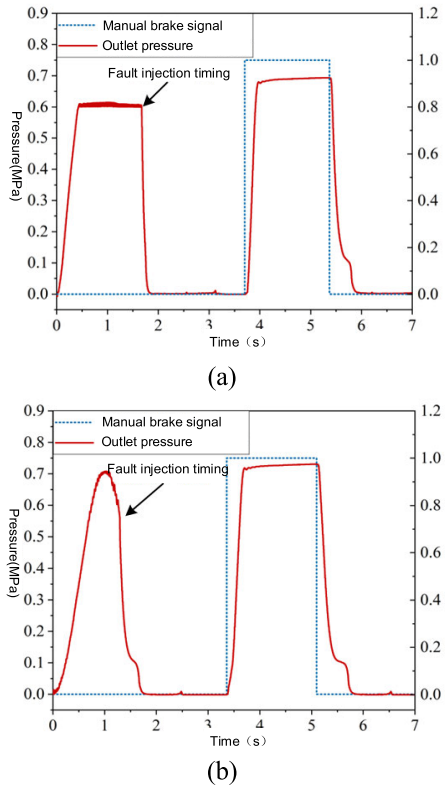


FIGURE 9. **High-speed solenoid valve core sticking fault injection test (a) Step target pressure (b) Sinusoidal target pressure.**

allowing the gas in the manual braking reservoir to swiftly enter the braking chamber, completing the manual emergency braking procedure.

VII. DISCUSSION

In this study, we conducted an in-depth analysis of the fault types and safety levels associated with the automatic pressure regulating valve. This analysis facilitated the development of targeted high-redundancy safety measures to address specific faults. To validate these measures, we established an experimental system and carried out fault injection tests. These tests focused on scenarios such as main pressure sensor faults, single-coil sticking faults, and single-coil failure faults. The outcomes of these tests provide compelling evidence that the high-redundancy safety scheme for the automatic pressure regulating valve robustly maintains its pressure regulation capabilities. These findings lay a significant theoretical groundwork for the advancement of high-redundancy safety systems within the realms of autonomous driving and chassis systems.

VIII. CONCLUSION

This article is aligned with the evolving needs of autonomous driving, centering on the design and validation of a high-redundancy safety scheme for the automatic pressure regulating valve utilized in commercial vehicle electronic pneumatic braking systems. The primary objective is to develop a high-redundancy safety solution tailored for the automatic pressure regulating valve, ensuring its compatibility and effectiveness in the forthcoming advancements of commercial vehicle electronic pneumatic braking systems. Building upon this work, the project team will venture into the exploration of high-redundancy safety architectures specific to commercial vehicle electronic pneumatic braking systems. This exploration will be informed by the high-redundancy safety framework established for the automatic pressure regulating valve and will encompass the development of corresponding high-redundancy safety control methodologies. Such advancements are anticipated to lay a substantial theoretical groundwork, contributing significantly to the progression of high-redundancy safety in the domains of autonomous driving and chassis systems.

ACKNOWLEDGMENT

The authors would like to thank Gangyan Li, Xiaoxu Wei, Yi Chen, Keyu Wang, and Mingming Zhao of Wuhan University of Technology for their support and help with this study.

REFERENCES

[1] Y. W. Pan, Q. Y. Yu, and F. Wang, "Failure analysis of automotive differential based on the fault tree," *Adv. Mater. Res.*, vols. 1049–1050, pp. 871–874, Oct. 2014.

[2] P. Popovic, G. Ivanovic, R. Mitrovic, and A. Subic, "Design for reliability of a vehicle transmission system," *Inst. Mech. Eng., Part D, J. Automobile Eng.*, vol. 226, no. 2, pp. 194–209, 2012.

[3] Y. Chen, X. Q. He, and P. Lai, "The application of fault tree analysis method in electrical component," in *Proc. 20th IEEE Int. Symp. Phys. Failure Anal. Integr. Circuits (IPFA)*, Jul. 2013, pp. 658–661.

[4] D. Lee, D. Lee, and J. Na, "Automatic failure modes and effects analysis of an electronic fuel injection model," *Appl. Sci.*, vol. 12, no. 12, p. 6144, Jun. 2022.

[5] T. Aized, M. Ahmad, M. H. Jamal, A. Mahmood, S. U. U. Rehman, and J. S. Srai, "Automotive leaf spring design and manufacturing process improvement using failure mode and effects analysis (FMEA)," *Int. J. Eng. Bus. Manag.*, vol. 12, Jul. 2020, Art. no. 1847979020942438.

[6] W. Zhou, Z. Qiu, S. Tian, Y. Liu, L. Wei, and R. Langari, "A novel hybrid approach for risk evaluation of vehicle failure modes," *Sensors*, vol. 21, no. 2, p. 661, Jan. 2021.

[7] X. Xu, X. Qiao, N. Zhang, J. Feng, and X. Wang, "Review of intelligent fault diagnosis for permanent magnet synchronous motors in electric vehicles," *Adv. Mech. Eng.*, vol. 12, no. 7, Jul. 2020, Art. no. 168781402094432.

[8] R. Xiong, W. Sun, Q. Yu, and F. Sun, "Research progress, challenges and prospects of fault diagnosis on battery system of electric vehicles," *Appl. Energy*, vol. 279, Dec. 2020, Art. no. 115855.

[9] V. Naranje, H. Javed, S. Anjum, and H. M. A. Hussein, "Failure modes and effects analysis (FMEA) for electric converted vehicle," in *Proc. Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE)*, Mar. 2023, pp. 444–449.

[10] G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng, and R. Li, "Recent advances and future trends for automotive functional safety design methodologies," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5629–5642, Sep. 2020.

[11] A. Frigerio, B. Vermeulen, and K. G. W. Goossens, "Automotive architecture topologies: Analysis for safety-critical autonomous vehicle applications," *IEEE Access*, vol. 9, pp. 62837–62846, 2021.

[12] T. Wang, J. Mi, Z. Cai, X. Chen, and X. Lian, "Vehicle dual-redundancy electronic steering wheel system," in *Proc. 5th Int. Conf. Mech., Automot. Mater. Eng. (CMAME)*, Aug. 2017, pp. 183–187.

[13] J. Mi, T. Wang, and X. Lian, "A system-level dual-redundancy steer-by-wire system," *Proc. Inst. Mech. Engineers, Part D, J. Automobile Eng.*, vol. 235, no. 12, pp. 3002–3025, Oct. 2021.

[14] M. Kissai, X. Mouton, B. Monsuez, D. Martinez, and A. Tapus, "Complementary chassis systems for ground vehicles safety," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, Aug. 26, 2018, pp. 179–186.

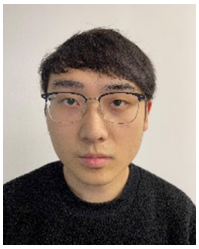
[15] J.-O. Hahn, S.-H. You, Y. Man Cho, S. Kong, and K. Il Lee, "Fault diagnostics in the differential brake control system using the analytical redundancy technique," in *Proc. 42nd IEEE Int. Conf. Decis. Control*, Dec. 2003, pp. 2276–2281.
[16] H. Bao, Z. Wang, X. Wei, and G. Li, "Study on the structural configurations and pressure regulation characteristics of the automatic pressure regulating valve in the electronically controlled pneumatic brake system of commercial vehicles," *Appl. Sci.*, vol. 11, no. 22, p. 10603, Nov. 2021.
[17] G. Li, X. Wei, Z. Wang, and H. Bao, "Study on the pressure regulation method of new automatic pressure regulating valve in the electronically controlled pneumatic brake systems in commercial vehicles," *Sensors*, vol. 22, no. 12, p. 4599, Jun. 2022.
[18] H. Bao, Z. Wang, X. Wei, and G. Li, "Analysis of pressure response characteristics and influencing factors of the automatic pressure regulating valve in electronic-controlled pneumatic braking system of commercial vehicle," *Fluid Power Syst. Technol.*, vol. 85239, Dec. 2021, Art. no. V001T01A008.
[19] A. Bansal, H. Kim, S. Yu, B. Li, N. Hovakimyan, M. Caccamo, and L. Sha, "Perception simplex: Verifiable collision avoidance in autonomous vehicles amidst obstacle detection faults," 2022, *arXiv:2209.01710*.

HANWEI BAO was born in Mengyin, Shandong, in March 1990. He received the bachelor's degree, in June 2012, the master's degree, in June 2015, and the Ph.D. degree in engineering from Wuhan University of Technology, in October 2022. He is currently a Postdoctoral Fellow with the School of Mechanical and Electrical Engineering, Wuhan University of Technology. Mainly engaged in theoretical and technical research in the fields of vehicle autonomous driving, domain control and intelligent braking, pneumatic transmission and control, led the research and development of an automatic pressure regulator for commercial vehicle electronic pneumatic braking system and its test equipment for driving automation, and proposed a precise, fast, and stable pressure regulator method that can be fully decouple. He has published more than ten SCI and EI articles on relevant content, applied for 13 invention patents (five international patents), and has authorized five invention patents (one international patent authorization).

KEYU WANG received the dual B.Sc. degree (Hons.) in mechanical engineering from Wuhan University of Technology, China, and the University of Birmingham, U.K., in 2021, and the M.Sc. degree (Hons.) in aeronautical robotics from the University of Bristol, U.K., in 2022. He is currently pursuing the Ph.D. degree with Wuhan University of Technology, focusing on the highly redundant safety control strategies for pneumatic brake systems and safety verification systems based on digital twin technology.

XIAOXU WEI received the Graduate and master's degrees from the School of Mechatronic Engineering, Wuhan University of Technology, in 2018 and 2022, respectively. His main research interests include automatic driving and intelligent braking.

YI CHENG was born in Shiyan, Hubei, in 1979. He received the bachelor's degree in mechanical design, manufacturing and automation from the Department of Logistics, Wuhan University of Technology, in 2004, and the master's and Ph.D. degrees in mechatronic engineering from Wuhan University of Technology, in 2007 and 2016, respectively. From 2007 to 2012, he was with Wuhan Youfin Automotive Electronic Control System Company Ltd., mainly engaged in research and development. He has published two articles and about 50 patents. Focusing on the field of automotive electronic braking system for nearly 20 years, he is good at vehicle control modeling and related algorithm development technology.



MINGMING ZHAO received the B.S. degree in vehicle engineering from Chongqing University of Technology, China, in 2020. He is currently pursuing the master's degree with the School of Automotive Engineering, Wuhan University of Technology, China. His research interests include the development of pneumatic brake systems and vehicle control aspects.

GANGYAN LI received the B.S. and M.S. degrees from Wuhan Automobile Polytechnical University (currently Wuhan University of Technology), Wuhan, China, in 1982 and 1985, respectively, and the Ph.D. degree from the School of Mechanical and Electronic Engineering, Wuhan University of Technology, in 2000. He was the Deputy Dean of the School of Mechanical and Electrical Engineering, Wuhan University of Technology, the Director of the Institute of Automotive Electronics and Information Integration Technology, and the Director of the Pneumatic Technology Center in SMC, Japan, Wuhan University of Technology, where he is currently a Professor with the School of Mechanical and Electrical Engineering. He has over 20 years of experience in pneumatic technology, CAN bus, and vehicle brake and steering. His current research interests include autonomous driving, domain control and intelligent braking, intelligent manufacturing and processing mechanism and equipment, and pneumatic transmission and control.