Functional Safety Design of Four-Wheel Independent Brake System on Electric Vehicle

Jingming Zhang*, Yunshuang Zhang and Guoxing Li

School of Automotive Engineering, Harbin Institute of Technology at Weihai, Weihai 264209, China

*Corresponding author e-mail: Whjingming@163.com

Abstract. The fault trees are set up to analyse the five failure modes of wire controlled four-wheel independent brake system on electric vehicle. The hardware redundancy is designed. The control strategy with ASIL D is established. The method of joint simulation of CarSim and MATLAB/Simulink is adopted. After fault injection, the simulation tests are carried out under the conditions of wire brake. It shows that the system has reached the ASIL D from analyses.

1. Introduction

Automotive wire controlled brake system has the advantages of simple structure, stable work and high functions such as ABS. Nowadays, the electronic control equipment is important for automobile brake. So it is imminent to improve its functional safety [1]. The design based on the ISO 26262 is a trend in the current automotive industry. However, the specific analysis on the failure modes and corresponding countermeasures are still limitation in the concept stage of functional safety. Many researchers have made great contribution on the study of the control strategy of the four-wheel independent brake system [2, 3]. However, it is necessary to establish a control strategy that meets the requirements of the functional safety basing on the normal four-wheel brake control strategy. That is achieved through the detection and diagnosis of the various structural faults of the brake system.

2. Functional safety requirements of four-wheel independent brake system

2.1. The Structural analysis of brake system

The hydraulic linear control four-wheel independent brake system, which includes brake pedal module, the wheel brake module, the central controller, the communication network, the power supply module and so on, is studied in this paper. The power of the four wheels can be controlled by four channels. The structure of the brake system is shown in Figure 1.

2.2. Risk analysis and risk assessment

Different effects on the driver and the vehicle are considered, rating method ASIL is applied to evaluate damage degree when the brake system fails in different failure modes and conditions [4]. The brake conditions are city, high speed, tunnel and ice surface road. The failure modes include brake deviation, brake failure, spontaneous braking, brake error and brake retardation. The ASIL grade is evaluated through SAE J2980, as shown in Table 1.
From the above analysis, the highest grade of functional safety under various driving conditions and failure modes is selected to define the safety integrity grade of the vehicle, so the functional safety requirements of the brake system can reach ASIL D. Allocating the whole ASIL D to the subsystems or components. If the subsystems or components are all reach ASIL D, the whole system can also reach ASIL D.

**Table 1.** ASIL grades under various brake failure modes and working conditions

| Failure modes      | Effect of failure            | City | High speed | Tunnel | Ice surface |
|--------------------|------------------------------|------|------------|--------|-------------|
| Brake deviation    | Out of control in the direction | D    | D          | C      | B           |
| Brake failure      | No brake                     | D    | D          | C      | B           |
| Spontaneous braking| Suddenly decelerate or stop  | C    | C          | B      | B           |
| Brake error        | Velocity abnormity           | D    | D          | C      | C           |
| Brake retardation  | Brake delay                  | D    | D          | B      | A           |

2.3. Analysis of the failure cause of brake system

Fault tree analysis can be used to analyse the cause of failure concretely [5]. According to the fault tree analysis of the brake deviation, which is shown in Figure 2, the reasons of brake deviation are got, as shown in Table 2.
### Table 2. Analysis of reasons for braking deviation

| Failure position       | Specific reasons                          |
|------------------------|-------------------------------------------|
| ECU                    | ECU fault                                 |
| communication network  | communication network fault               |
| wheel brake module     | a. Malfunction of wheel brake controller  |
|                        | b. Malfunction of Hydraulic device        |
|                        | c. Malfunction of Wheel speed sensor      |
|                        | d. Brake fault                            |

In the same way, the fault tree analysis method is used to analyse the brake failure, the spontaneous brake, the brake error and the brake delay. According to the analysis of five failure modes, we can know that the mistakes of brake pedal module, wheel brake module, ECU module, power supply module and communication network module may cause danger to vehicle.

### 3. The functional safety of the four-wheel independent brake system

In order to achieve the functional safety of the four-wheel independent brake system to ASIL D, two sets of ASIL B working system combined with monitoring algorithm are designed. When one system is broken, it is converted to standby ASIL B system to ensure the safety of brake.

The brake pedal is set up with two angular displacement sensors and a hydraulic pressure sensor. The safety integrity level of the angular displacement sensor is ASIL A, and the hydraulic pressure sensor is ASIL B. The low grade architecture elements allocated here must be independent. That can be expressed as ASIL D = ASIL B + ASIL A (D) + ASIL B (D). The wheel speed sensor, control system, power supply and communication network are all decomposed, that is, ASIL D = ASIL B (D) + ASIL B (D). ECU and brake controllers can be considered as a control unit.

### 4. Functional safety simulation of four-wheel independent brake system

#### 4.1. Simulation model

The B-Class vehicle model is built in the CarSim. The parameters such as mass, geometric size and aerodynamic characteristics are retained. There are 27 freedoms in vehicle which parameters are shown in Table 3. The preview optimal control model is used. Then the following modifications are made to the model:

1. The drive system was disconnected and the initial speed is set with actual requirement;
2. Independent suspensions and disc brakes are selected;
3. The four wheel brake system is selected with no brake force. The required brake force is provided by the formulated brake control strategy;
4. The four wheel steering system is selected. Then the path is set in the simulation.

The brake system with functional safety is designed. Then the model of ASIL D is obtained, which is as shown in Figure 3. It also includes a calculation module of deceleration, two calculation modules of vertical load of four wheel, two calculation modules of brake force module and a system diagnosis module, which is used to diagnose the signal of system and select the correct signal of output. In CarSim model, the brake pressure of four wheels is input signal. The longitudinal acceleration, the lateral acceleration and the speed of the four wheels are the output signals.

There may be a fault in one position, and may be a lot of faults in multiple positions at the same time when the vehicle is braking. According to ISO 26262, the condition with a fault in one position is analysed in this paper. In order to make contrast tests, the failure vehicle that is no functional safety design with fault, the test vehicle that is functional safety design with fault and the normal vehicle without fault are set up. The conditions of the simulation in this paper are right front wheel speed sensor signal error with braking in straight line. The road adhesion coefficient is 0.8, the initial speed is 65 km/h, the braking speed is 0.15 g, and the simulation time is set to 20 s. Before the simulation, the faults are input to system.
Table 3. Vehicle parameters

| Parameter                        | Value  | Unit  |
|----------------------------------|--------|-------|
| vehicle weight                   | 1231   | kg    |
| sprung mass                       | 1111   | kg    |
| unsprung mass of front axle      | 60     | kg    |
| unsprung mass of rear axle       | 60     | kg    |
| inertia of the wheel's moment    | 0.6    | kg.m² |
| vehicle’s height of C.G.         | 0.515  | kg.m² |
| sprung mass’s height of C.G.     | 0.540  | m     |
| unsprung mass’s height of C.G.  | 0.28   | m     |
| wheelbase                        | 2.6    | m     |
| distance between the C.G. and front axle | 1.026 | m |
| tread of front wheel             | 1.481  | m     |
| tread of rear wheel              | 1.486  | m     |

Figure 3. ASIL D simulation model of four wheel brake

4.2. Signal error of speed sensor on right wheel

Signal error of speed sensor on right wheel, which is multiplied by a sinusoidal signal on the original signal, is injected into model that with braking in straight line. The results of simulation are shown in Figure 4, Figure 5 and Figure 6.

When the speed of the failure vehicle is reduced to 0 km/h at about 10.8 second, the brake distance is 98.37 m, which is shorter than normal vehicle and test vehicle. The maximum lateral displacement is 4.4 m, which deviates from the predetermined orbit. In 0 s to 10.8 s, the lateral acceleration fluctuates from -0.065 g to 0.03 g. After full brake, lateral acceleration changes in the range of ±0.0002 g.
Figure 4. The brake distance when the signal of speed sensor on right wheel is error

Figure 5. The lateral displacement when the signal of speed sensor on right wheel is error

Figure 6. The lateral acceleration when the signal of speed sensor on right wheel is error
The data of the test vehicle and the normal vehicle are exactly the same. Because the system has activated the spare sensor of wheel speed which makes the system is restored to normal after detecting the fault. The speed of the test vehicle is reduced to 0 km/h and the brake distance is 109.25 m at about 12 s. The maximum lateral displacement is $2.25 \times 10^{-5}$ m, which has a good ability of keeping predetermined orbit. In 0 s to 12 s, the lateral acceleration fluctuates in the range of $\pm 0.00003$ g. After full brake, lateral acceleration changes in the range of $\pm 0.0002$ g.

4.3. **ECU error**

The brake pressure on right wheel is multiplied by a sinusoidal signal, which is an example of ECU error. When the fault is injected into the test vehicle and failure vehicle, the brake distance, lateral displacement and lateral acceleration of three vehicles are shown in Figure 7, Figure 8 and Figure 9.

The data of the test vehicle and the normal vehicle are exactly the same. The speed of the test vehicle is reduced to 0 km/h and the brake distance is 109.25 m at about 10.8 s. The speed of the failure vehicle is reduced to 0 km/h and the brake distance is 90.5 m at about 10.1 s. Both the time and distance of test vehicle are shorter. The calculated brake pressure is bigger with ECU error.

The maximum lateral acceleration of the failure vehicle has reached 0.1 g because of the change of the brake pressure, resulting in a great reduction in stability. During the braking time, the maximum lateral displacement of the fault vehicle is 5.5 m, which deviates from the predetermined track.

![Figure 7](image1.png)

**Figure 7.** The brake distance with ECU error

![Figure 8](image2.png)

**Figure 8.** The lateral displacement with ECU error

![Figure 9](image3.png)

**Figure 9.** The lateral acceleration with ECU error
It is known from the above analysis, the failure vehicle without functional safety design has great errors in the brake distance, lateral distance and lateral acceleration. In addition, the stability is reduced because of a large lateral displacement, which increases the driving risk. But the test vehicle with functional safety design has good fault-tolerance ability. It can ensure the stability of brake efficiency in time when hardware or software is error.

5. Conclusion
The purpose of this paper is to improve the reliability of the brake system on electric vehicle. The four-wheel independent brake system that controlled by wire is studied in a view of functional safety. First, the functional safety requirements are put forward. Then the brake system with functional safety is designed. Joint simulation of CarSim and MATLAB/Simulink is carried out. Results show that indexes of the four-wheel independent brake system meets the functional safety requirements are exactly agreement with the normal vehicle. The results show that the brake system designed on electric vehicle in this paper meets the requirements of ASIL D.

References
[1] G. Ressler, Application of System Safety Engineering Processes to Advanced Battery Safety, J. Sae International Journal of Engines. 4 (2011) 1921-1927.
[2] B. Wang, R. Sun, W. Yong, Research on Vehicle Stability Control Strategy on Varying Road Surface, J. Automobile Technology. 5 (2012) 17-20.
[3] B. Li, Vehicle Yaw Dynamics through Combining Four-wheel-steering and Differential Braking, J. Transactions of the Chinese Society for Agricultural Machinery. 39 (2008) 1-4.
[4] C. Takahashi, A 16nm FinFET Heterogeneous Nona-Core SoC Supporting Functional Safety Standard ISO26262 ASIL B, J. IEEE Journal of Solid-State Circuits. 99 (2016) 1-12.
[5] R. Dardar, B. Gallina, A. Johnsen, et al, Industrial Experiences of Building a Safety Case in Compliance with ISO 26262, J. IEEE International Symposium on Software Reliability Engineering Workshops. IEEE Computer Society. (2012) 349-354.