actuators

MDPI

Article

Electro-Mechanical Brake System Architectural Design and Analysis Based on Functional Safety of Vehicles

Jing Peng [1], Tong Wu [1,*], Liang Chu [2], Jin Rong [1], Xiaojun Yang [1] and Yang Meng [1]

[1] Key Laboratory of Automotive Power Train and Electronics, Hubei University of Automotive Technology, Shiyan 442002, China; p3ng@huat.edu.cn (J.P.); 202311206@huat.edu.cn (J.R.); 2020900727@huat.edu.cn (X.Y.); 202211123@huat.edu.cn (Y.M.)
[2] Department of Automotive Engineering, Jilin University, Changchun 130015, China; chuliang@jlu.edu.cn
* Correspondence: wut@huat.edu.cn; Tel.: +86-15608748895

Abstract: Electro-mechanical brake (EMB) systems have garnered significant attention due to their distributed architecture. However, their signals from the brake pedal to the wheel-end actuators (WEAs) are transmitted electrically, meaning that any fault in EMB systems can severely impair the braking performance of vehicles. Consequently, the functional safety issues of EMB systems are the primary limitation of their widespread adoption. In response, this study first introduced the typical architectures of EMB and evaluated the automotive safety integrity level (ASIL) that must be achieved. Based on this, an EMB system architecture that satisfies functional safety standards was proposed. To accurately analyze the main factors affecting the probabilistic metric for hardware failures (PMHF) of the architecture, the failure rate of WEAs is further discussed. Specifically, a Markov chain was employed to define the operating states of the WEA matrix. The availability of each operating state was assessed based on the fault-tolerant control strategy. Finally, the failure rates of critical EMB parts, particularly the WEA matrix, were calculated. The results indicate that the unavailability of the WEA matrix is 9.244×10^{-3} FIT. Furthermore, the PMHFs of the EMB system for each safety goal are 6.14 FIT, 5.89 FIT, and 6.03 FIT, respectively, satisfying the ASIL-D requirements.

Keywords: electro-mechanical brake (EMB); functional safety; fault tolerance; actuators; fault tree analysis; Markov chain

check for updates

Citation: Peng, J.; Wu, T.; Chu, L.; Rong, J.; Yang, X.; Meng, Y. Electro-Mechanical Brake System Architectural Design and Analysis Based on Functional Safety of Vehicles. *Actuators* **2024**, *13*, 346. https://doi.org/10.3390/act13090346

Academic Editor: Cristina Morel

Received: 15 August 2024
Revised: 2 September 2024
Accepted: 4 September 2024
Published: 9 September 2024

1. Introduction

With the rapid iteration of autonomous driving, the demands for the precise control, functional integration, and shared hardware of vehicles have garnered significant attention in wire-controlled chassis [1]. Brake-by-wire (BBW) stands out as a crucial subsystem for driving safety, making it an indispensable way to facilitate advanced autonomous driving.

BBW systems can be categorized into two main types based on their structural scheme: electro-hydraulic brake (EHB) systems and electro-mechanical brake (EMB) systems. EHB systems are generally composed of main control units (MCUs), a hydraulic control unit (HCU, including hydraulic brakes, ABS/ESC solenoid valve modules, and electric boosters), sensors, power supplies, and communication buses, which are illustrated in Figure 1 [2]. The braking process is controlled by the MCU, which receives electrical signals from the brake pedal, interprets the driver's braking commands, and directs the HCU accordingly.

EMB systems generally comprise five principal components: MCUs, wheel-end actuators (WEAs), sensors, power supplies, and communication buses, which are illustrated in Figure 2 [3]. EMB systems rely on electro-mechanical integrated actuators installed at the wheel end to replace hydraulic calipers and provide a braking force. Hence, the complex hydraulic components between the brake pedal and the brake actuators are eliminated, with the WEAs being controlled through electrical signals instead of hydraulic pressure. Furthermore, a distributed braking system is constructed by integrating each WEA into a

WEA matrix, thereby facilitating easier and more flexible integrated chassis control. Consequently, EMB systems are widely recognized as the most promising braking system for intelligent electric vehicles.

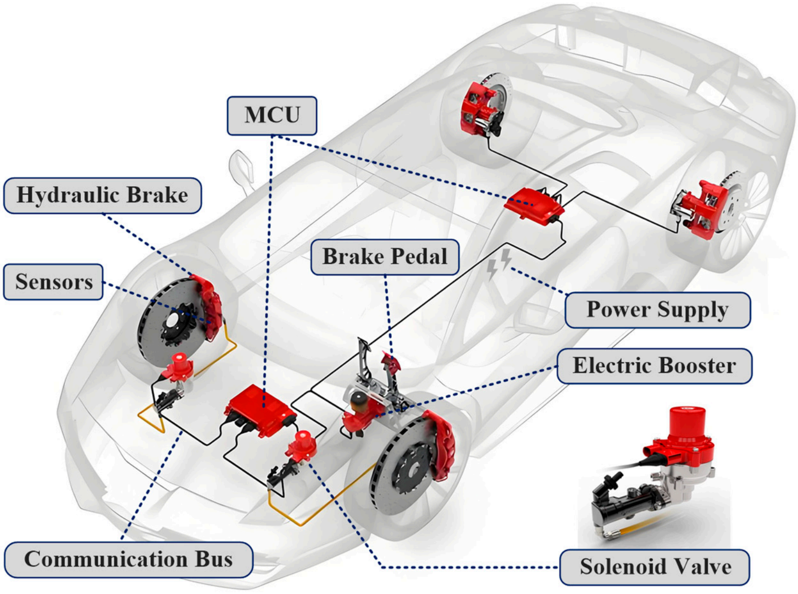


Figure 1. Overall scheme of EHB systems.

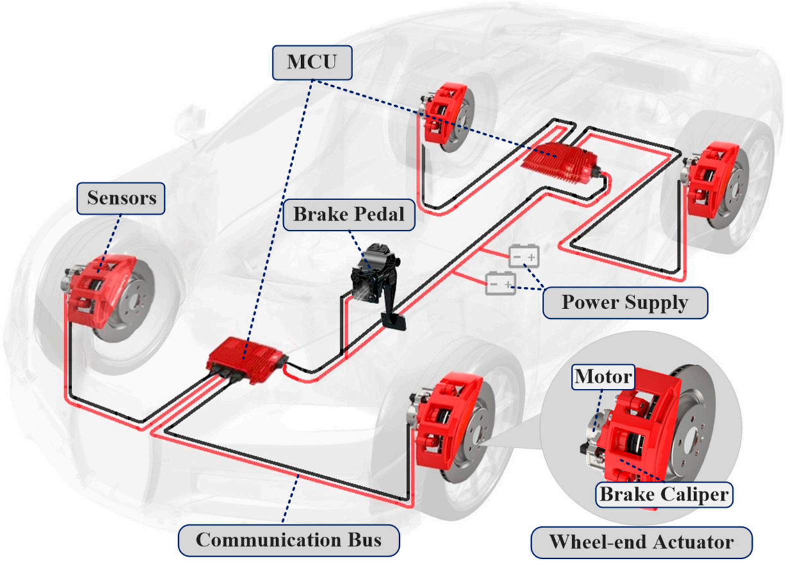


Figure 2. Overall scheme of EMB systems.

In contrast, technical schemes of EHB systems are relatively mature. The braking safety control (BSC) system introduced by BYD and the NBooster system developed by NASN both maintain a backup mode with pure mechanical connections and integrate external redundancies, including power and communication backups. These enhancements ensure that EHB systems fully meet the requirements of Level 2 of autonomous driving.

As for EMB systems, they are currently in the vehicle testing phase, with promising advancements indicating a strong potential for future mass production. In June 2022, Jiongyi Electronic Technology released the intelligent drive-by-wire chassis with a self-developed EMB system for automatic driving and claimed to achieve mass production in 2025 [4]. EMB systems eliminate mechanical backups and introduce redundancies such as controller and actuator backups, aiming to meet the requirements of Level 3 and higher levels of autonomous driving. Due to the absence of mechanical connections between the brake pedal and the WEA, any component fault within the EMB systems presents a potential failure risk. This failure is manifested through the actuator's inability to respond to brake commands promptly and accurately, leading to issues such as loss of braking, unintended braking, braking deviation, and braking skidding or even drifting. These issues severely endanger driving safety. Therefore, the functional safety challenges faced by EMB systems are the primary bottleneck restricting their large-scale application.

Functional safety issues refer to the system's inability to perform its functions correctly due to faults, which can lead to potential safety risks [5]. These faults may occur intermittently or permanently throughout the system lifecycle and can result in equipment damage, personal injury, or even life-threatening situations. Therefore, it is essential to ensure the system can still operate safely or enter a safe mode after failures to prevent harm. To ensure the functional safety of electrical and electronic (E/E) systems for road vehicles, the international organization standardization (ISO) has issued the ISO 26262 standard. The standard provides a reliable functional safety development process that spans the entire lifecycle of vehicles. The process starts with the concept development and progresses through system, hardware, and software developments, ultimately leading to verification and validation [5–10].

Since the standard release, scholars and enterprises have conducted related studies following the outlined processes. Regarding the definition of functional safety concepts, Fang Y. et al. [2] defined the functional safety concept for BBW systems, designed an EHB system hardware architecture with three redundant lines, and verified its reliability to meet functional safety requirements. Li C. et al. [11] defined a functional safety-compliant BBW system architecture and conducted a detailed analysis of its requirements. Chen Yang, et al. [12] defined the E/E architecture of a road traffic light system based on ISO 26262 and established the functional safety goals for this system. For the EMB system architecture, Li J. et al. [13] provided a hardware structure and designed a braking force control strategy for EMB systems based on the Fuzzy PID algorithm. Li C. et al. [4] summarized the configurations and typical EMB architectures, highlighting the characteristics of the schemes. Li Y. et al. [14] designed an EMB system architecture, allocating a monitoring strategy of three-layer control model for the architecture and conducted hardware-in-the-loop (HIL) tests for verification. For the system architecture analysis, Soltanali H. et al. [15] analyzed the safety of intelligent braking systems and explored the potential hazards of system functions with a fuzzy fault tree and Bayesian network model. Famfulik J. et al. [16] proposed a model of system architecture reliability calculation and validated this model through simulations and tests. For the system architecture verification, Wu X. et al. [17] studied the failure modes of a BBW system based on fault tree analysis (FTA) and designed hardware redundancy measures. Chao Huang, et al. [18] designed the hardware architecture of a steer-by-wire system (SBWs) based on functional safety concepts and conducted analyses using state transition diagrams and the FTA. Through literature research, it was found that previous studies on EMB system architecture have made remarkable progress in technical safety requirements (TSR) analyses, but there is a lack of study on the interdependencies of each component, especially of the WEA, which can affect the definition of EMB system failure. Hence, it is necessary to further explore fundamental events leading to EMB system failure, thereby providing critical data support for the functional safety verification of EMB systems.

To solve these issues, this study proposes an EMB system architecture, further analyzing and validating the architecture based on functional safety methods, as shown in Figure 3. Specifically, typical EMB system architectures are investigated. Safety goals (SGs) for EMB systems are set and the TSR for components are assigned. Second, an EMB system hardware architecture satisfying the TSR is proposed. Then, the hardware architecture and application software framework are analyzed, and the fault-tolerance control strategy is established for further analyses. On these bases, the top events leading to EMB failure are analyzed, the WEA matrix operating states are evaluated, and the WEA matrix availabilities are determined. Finally, the EMB system architecture is verified.

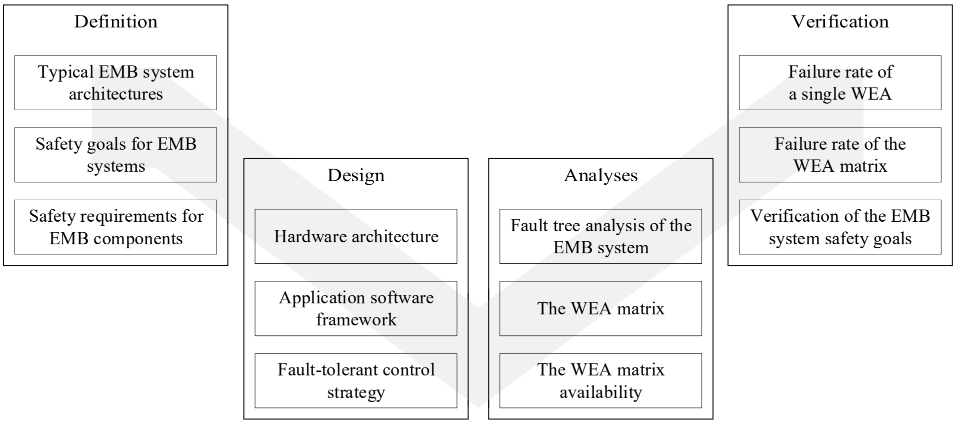

Definition
Typical EMB system architectures
Safety goals for EMB systems
Safety requirements for EMB components
Design
Hardware architecture
Application software framework
Fault-tolerant control strategy
Analyses
Fault tree analysis of the EMB system
The WEA matrix
The WEA matrix availability
Verification
Failure rate of a single WEA
Failure rate of the WEA matrix
Verification of the EMB system safety goals

Figure 3. Main work of this study.

The main contribution of this study is to propose a method for calculating the failure rate of WEA matrix based on Markov chain (MC) and fault-tolerant control (FTC) strategy. Firstly, the failure rate of a single WEA was calculated based on the FTA method. Secondly, a MC is established, and the operating states of the WEA matrix are further analyzed. On this basis, the FTC strategy is built, and experiments are carried out under WEA failure modes. Thus, the unavailable states of the WEA matrix are determined by comparing the experimental results with the SGs. Finally, the failure rate of the WEA matrix is obtained. Hence, the above detailed analyses facilitate the precise calculation of the EMB system failure probability and the functional safety assessments.

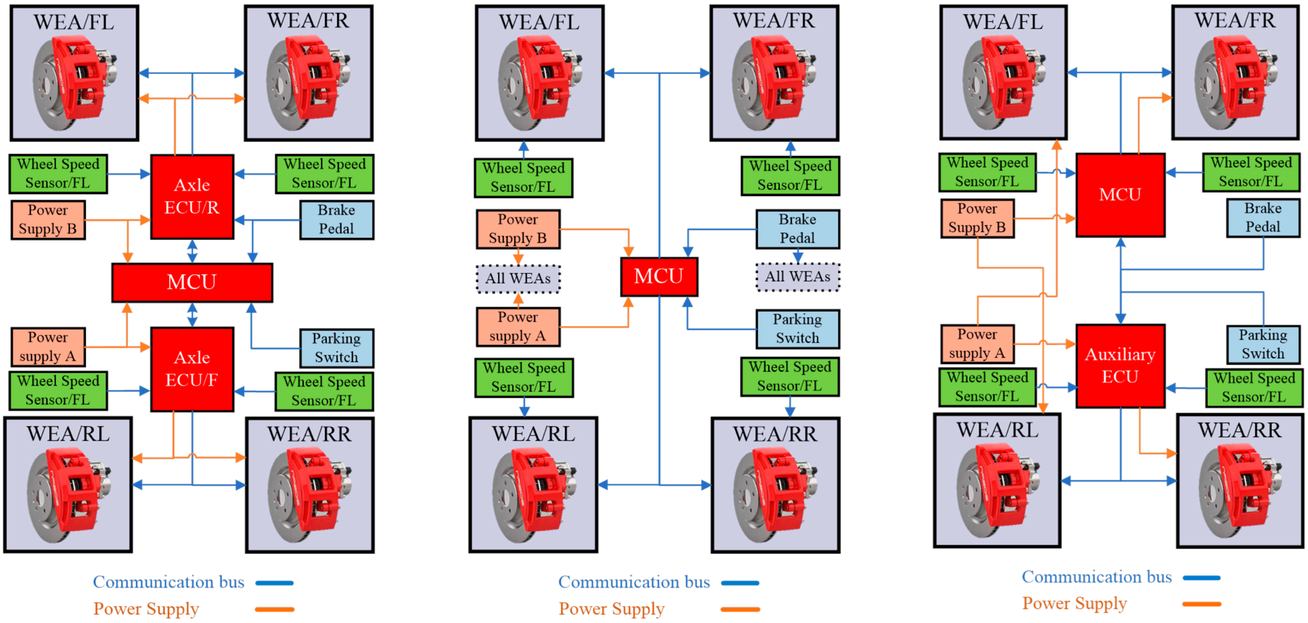
The remaining sections of this study are organized as follows: Section 2 presents a preliminary discussion on the typical EMB system architecture, defining the concept of EMB systems. Section 3 designs the hardware architecture, application software framework and control strategy of EMB systems. Section 4 provides detailed analyses of the EMB system architecture and the WEA matrix. Section 5 verifies that the proposed EMB system architecture satisfies the SGs. Section 6 concludes this study.

2. Concept Definitions of EMB Systems

2.1. Typical EMB System Architectures

EMB systems generally comprise five principal components as shown in Figure 2. The sensor components are tasked with sampling the driver's braking signals and vehicle status information. The MCU interprets the braking demands, determines the target braking force of each wheel, and executes fault diagnosis (including fault detection, fault isolation, and fault quantification) and FTC [19]. The WEA, which is an electromechanical integrated scheme, includes a servo motor, transmission mechanism, conversion mechanism, caliper, and actuation control unit (ACU). The ACU receives target braking force commands from the MCU and manages the WEA accordingly. Moreover, the power supply furnishes electrical energy to EMB systems, while the communication bus enables information exchange among the components. Based on the controller arrangement, three typical EMB system architectures are illustrated in Figure 4.

The architecture shown in Figure 4a employs a combination controller with an MCU and two axle-controlled electronic control units (ECU), offering the strongest redundancy performance with a relatively high cost. Figure 4b uses a single MCU with the brake pedal directly connected to the four WEAs. It provides poor residual capability after the MCU failure while reducing cost. Figure 4c uses an MCU and an auxiliary ECU as controllers, balancing controller redundancy with cost efficiency.



(**a**) MCU + Axle ECU (**b**) MCU + Pedal-direct (**c**) MCU + Auxiliary ECU

Figure 4. Typical EMB system architectures.

For the power supply and communication bus (comm. bus) the layout forms include "X", "H", and full redundancy. The "X" circuit coordinates braking allocation more effectively, enhancing vehicle stability during single-circuit failures, though its complex wiring increases maintenance difficulty. The "H" circuit employs a same-side redundancy design, simplifying the system structure but significantly affecting vehicle stability if a single-side circuit fails. In summary, the layout forms of each scheme are presented in Table 1.

Table 1. Conclusion of the schemes.

Scheme	Main Controller	Power Supply	Comm. Bus
(a)	MCU + Axis ECU	"H" circuit	"H" circuit
(b)	MCU + Pedal-direct	Full redundancy	"X" circuit
(c)	MCU + Auxiliary ECU	"X" circuit	"H" circuit

2.2. Safety Goals for EMB Systems

Hazard Analysis and Risk Assessment (HARA) is a systematic method for identifying, assessing, and controlling potential hazards and risks. The SGs of EMB systems can be established, and the functional safety requirements for EMB system components can be formulated to prevent accidents or mitigate injuries and enhance system reliability based on HARA. This study refers to the SAE J2980 and NHTSA 812574 standards [20,21], utilizing the hazard and operability study (HAZOP) method to analyze the failure behaviors of EMB systems and their hazards to vehicles. The results are shown in Table 2.

Table 2. Hazard analyses of EMB systems.

EMB Systems Failure Mode	Hazard Event (Vehicle Level)
Loss of braking, insufficient braking	H1: Deterioration of vehicle braking capability (longitudinal)
Unintended braking, brake lock, over-braking	H2: Unintended vehicle deceleration (longitudinal)
Insufficient braking, brake lock, over-braking	H3: Braking deviation, skidding or drifting (lateral, yaw)

This study follows the ISO 26262 standard, determining the ASIL corresponding to the identified hazard events through a quantitative analysis of severity, exposure, and controllability. Severity (S) is categorized into four levels based on the potential harm of the hazard event. Exposure (E) is also divided into four levels according to the frequency of the hazard event occurring in the operational scenario. Controllability (C) is similarly classified into four levels based on the likelihood that the driver can regain control of the vehicle after the hazard event occurs. Additionally, the ASIL is further classified into four levels: A, B, C, and D, with level D representing the highest risk and requiring the strictest safety design requirements.

Table 3 provides an example of the ASIL assessment for the hazard event "H1: Deterioration of vehicle braking capability" under a scenario where the vehicle is driving on a highway at 100~130 km/h.

Table 3. ASIL assessment for Hazard Event 1.

Hazard Event	Operating Scenario	Potential Risk	Risk Assessment			ASIL
H1	Vehicle is driving on a highway at 100–130 km/h	Collision with the front vehicle	Severity S3 Fatal injury	Exposure E4 Frequently occurs	Controllability C3 Hard to control	D

Based on the ASIL assessment, the SGs corresponding to each hazard event are further established according to SAE J2980 and relevant European regulations [4,20] and the strictest limits are adopted, as shown in Table 4.

Table 4. The SGs of EMB systems.

Hazard Events	Safety Goals	ASIL
H1	SG1: Avoid mean fully developed deceleration (MFDD) below 5.15 m/s^2 during vehicle operation	D
H2	SG2: Avoid a maximum unintended deceleration exceeding 2.44 m/s^2 during vehicle operation	D
H3	SG3: Avoid lateral displacement of the vehicle body exceeding 1.20 m due to the EMB system failure during vehicle operation	D

In summary, if the EMB system architecture can simultaneously meet the SGs (SG1, SG2, and SG3), it is considered capable of safe operation under the expected conditions.

2.3. Safety Requirements for EMB Components

Satisfying the functional safety requirements (FSR) of each component is essential for achieving the overall functional SGs of EMB systems, and further allocating the technical safety requirements (TSR) to each component provides guidance for system architectural design. According to the ISO 26262 and NHTSA standards [7,21], fifteen FSR and TSR for EMB systems are derived based on the failure mode and effects analysis (FMEA), as detailed in Table 5.

Table 5. FSR and TSR of EMB components.

No.	Component	Functional Safety Requirement	Technical Safety Requirement
01	Sensor	Detect the accuracy of brake pedal signals	Design dual-channel brake pedal signals
02	Sensor	Detect the accuracy of wheel speed signals	Design four-component wheel speed sensors
03	MCU	Switch to backup link after system failure	Design dual-component main controller
04	MCU	Parse driver's brake signals	Design dual-channel human–machine interface (HMI)
05	MCU	Ensure communication between dual main controllers	Design dual-channel star coupler
06	MCU	Diagnose the rationality of sensor signals	Assign sensor inputs to dual-channel ADC
07	MCU	Ensure the communication among signals	Set J1587 bus interface

Table 5. *Cont.*

No.	Component	Functional Safety Requirement	Technical Safety Requirement
08	MCU	Monitor and distribute the battery voltage	Set power distribution module
09	Comm. bus	Ensure message transmission and reception	Set four-component FlexRay to control WEAs
10	Comm. bus	Ensure communication between dual-channel controllers	Set dual-component LIN bus
11	Power supply	Ensure power supply to all components	Set dual-component power unit
12	WEA	Ensure normal voltage of actuator module	Set power management module
13	WEA	Normally receive commands from MCU	Set bus interface
14	WEA	Control the action of execution motor	Set PWM module and power stages
15	WEA	Provide motor control inputs	Set braking force, motor speed, and motor current sensor

3. Architectural Design of the EMB System

3.1. Hardware Architecture

Based on the concept definitions of EMB systems, a hardware architecture that satisfies the TSR described in Section 2.3 is shown in Figure 5. The EMB system primarily consists of a brake pedal, a parking brake switch, dual MCUs, four WEAs, dual power supplies, and multi-channel communication buses including CAN, LIN, and FlexRay.

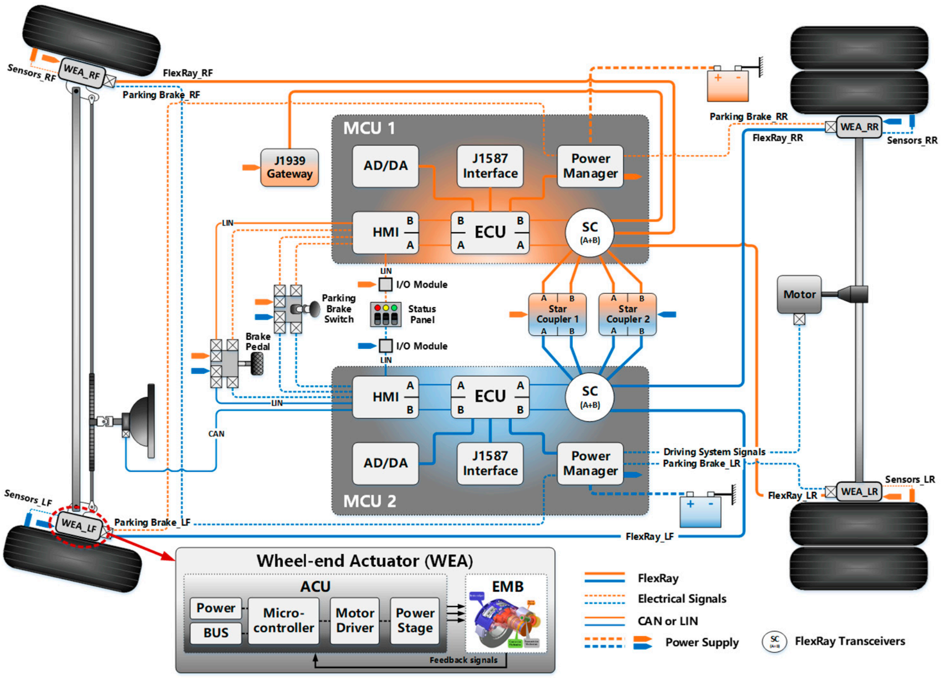


Figure 5. The EMB system architecture.

3.1.1. Sensors

The sensor components are responsible for collecting driver's operation signals and vehicle information and transmitting them to the MCU. Specifically, the sensor components include a brake pedal sensor, wheel speed sensors, braking force sensors, motor speed sensors, and motor current sensors (integrated within the ACU), as shown in Figure 6. The signals sampled by the brake pedal sensor and wheel speed sensors are transmitted in real time to the MCU via communication buses, ensuring the immediate parsing and monitoring of braking demands. Braking force sensors measure the axial thrust output from the motor to the caliper, typically using piezoresistive sensors, which are suitable for the harsh braking environment at the wheel-end and offer excellent durability and reliability. Additionally, the braking force signals are cross-checked with the pedal sensor, providing a heterogeneous hardware redundancy. Motor speed sensors provide motor speed signals, which are cross-checked with the rotor position sensors installed at the rear of the motor to estimate the motor speed, serving as an algorithm redundancy. Finally, the motor current sensors integrated within the ACU sample the real-time motor current information.

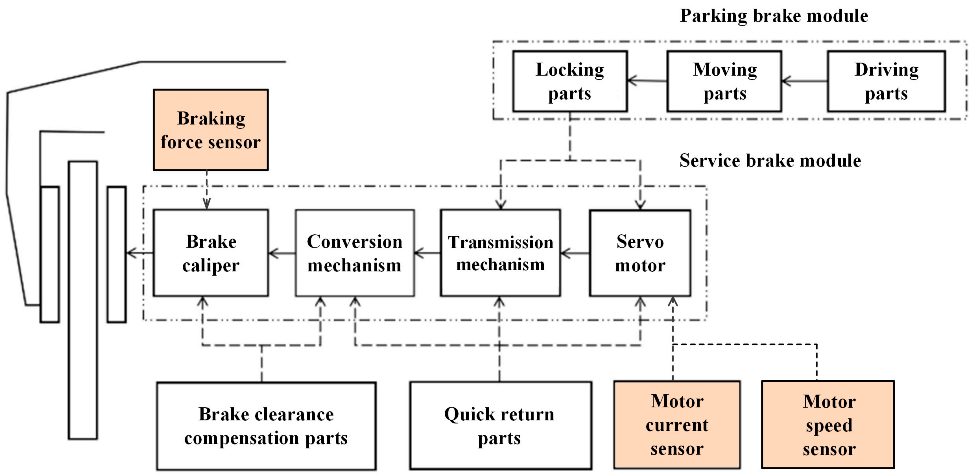


Figure 6. Sensor components.

3.1.2. MCUs

Each MCU consists of dual ECUs, several bus interfaces following the SAE-J1587 standard, FlexRay transceivers that satisfy high-speed, high-reliability, and high-redundancy requirements, some analog-to-digital/digital to analog (AD/DA) modules, a human–machine interface (HMI), and a power manager. The MCU is responsible for processing sensor signals and calculating the target braking force in each WEA. It also implements the fault diagnosis and FTC strategy. When an MCU fails, the other can immediately take over and brake the vehicle.

3.1.3. WEAs

The WEA is an electro-mechanical integrated scheme composed of an ACU, a servo motor, a conversion mechanism, a transmission mechanism, and a brake caliper. The servo motor provides braking energy to the EMB. The transmission mechanism amplifies the torque output from the motor and inputs it into the conversion mechanism. The conversion mechanism converts the rotational torque into the linear thrust and acts on the friction lining, which ultimately clamps the brake disc to generate a clamping force. The ACU, consisting of a micro-controller, two motor drivers, and two power stages, is responsible for receiving the target braking force from the MCU and operating each WEA. The architecture of the WEA is shown in Figure 7.

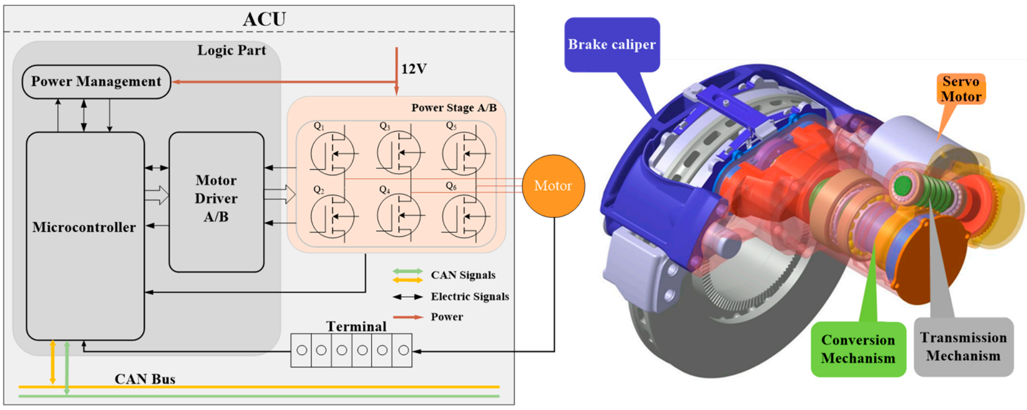


Figure 7. Architecture of the WEA.

Furthermore, a distributed braking system is constructed by integrating each WEA into an WEA matrix. Due to the matrix, it is possible to ensure the residual braking ability after a WEA failure by reconstructing the braking force in the remaining healthy actuators based on the FTC.

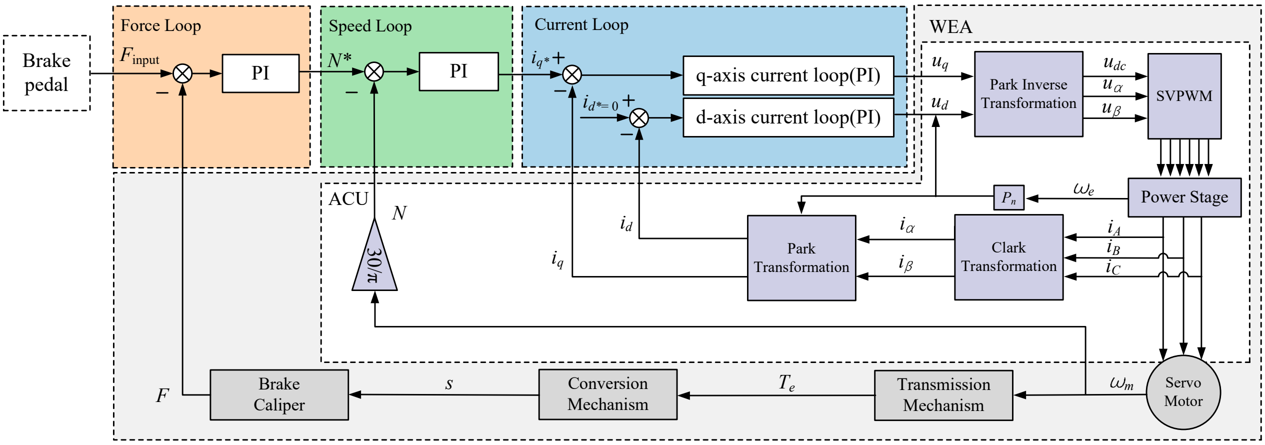
3.1.4. Power Supplies and Communication Buses

The EMB system uses dual power supplies to provide braking energy to each WEA in an “X” circuit. The communication buses including controller area network (CAN), local interconnect network (LIN) and FlexRay. The brake pedal and parking brake switch communicate with the MCU via the CAN. Since the CAN cannot meet the high transmission rate, synchronicity, FTC, and flexibility requirements of autonomous driving and wire-controlled chassis, communication between both MCUs, as well as between the MCUs and WEA, is conducted through the FlexRay.

3.2. Application Software Framework

According to the requirements of ISO 26262, fault-tolerant design (FTD) should be represented as a hierarchical structure illustrating the interactions of its elements. Hence, this study developed an application software framework for the EMB system that includes the modules of functional implementation, function monitor, controller monitor, and FTC strategy.

Specifically, the functional implementation layer is responsible for controlling the WEA and ensuring the rapid response, precise tracking, and stable maintenance of the clamping force. This layer typically adopts a closed-loop cascade control architecture characterized by “clamping force–motor speed–motor current”, as shown in Figure 8 [22–24].



* represents the target value.

Figure 8. The closed-loop cascade control architecture.

The function monitor layer is responsible for the real-time monitoring of the actual clamping force from each WEA, comparing it with the braking commands sent by the MCU to accurately determine the operating states of the WEA matrix. The function monitor layer typically employs a lockstep architecture, as shown in Figure 9 [25–27].

The controller monitor layer consists of a monitor chip and programs within the MCU. The chip periodically queries the program. Once receiving an incorrect answer, it will resend the same question to the program and activate the fault counter. To detect latent failures in the monitor chip, the program periodically sends the chip an incorrect answer to test its functionality.

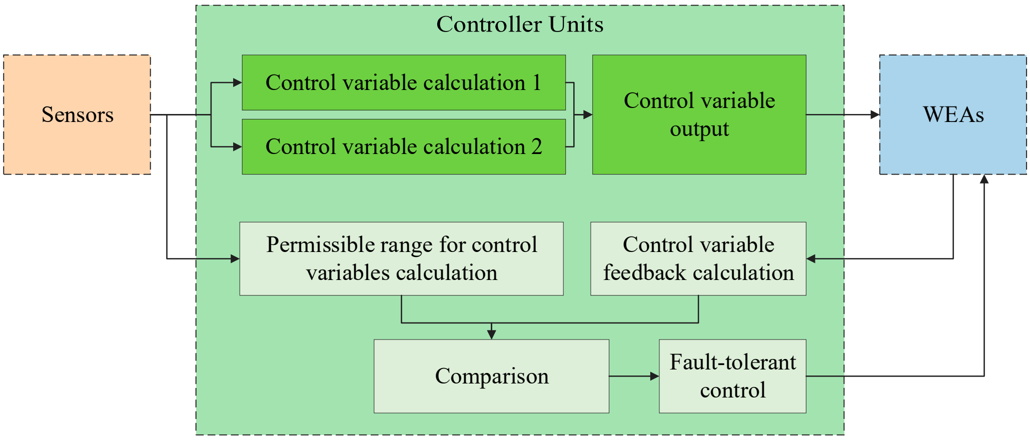

Controller Units
Sensors
Control variable calculation 1
Control variable calculation 2
Control variable output
WEAs
Permissible range for control variables calculation
Control variable feedback calculation
Comparison
Fault-tolerant control

Figure 9. The lockstep architecture.

3.3. FTC Strategy

The FTC is to reconstruct the braking force in the remaining healthy WEAs after a certain WEA fails, so that the vehicle has a residual braking ability to stop stably. Hence, the FTC strategy consists of two parts: the braking reconstruction rules and the reconstructed braking force calculations.

3.3.1. Braking Reconstruction Rules

Failed WEAs are in an unstable or uncontrollable state, so that the WEAs are not allowed to participate in braking reconstruction to avoid their further negative impact on vehicle dynamics regardless of the failure modes, and this is called "isolation". The braking reconstruction rules established in this study include a single WEA and double WEAs fail simultaneously, and they follow the "isolation" principle.

The failure modes can be categorized into four situations: failure of a single WEA, failure of WEAs on the same axle, failure of WEAs in diagonal positions and failure of WEAs on the same side, and their braking reconstruction rules are as shown in Figure 10.

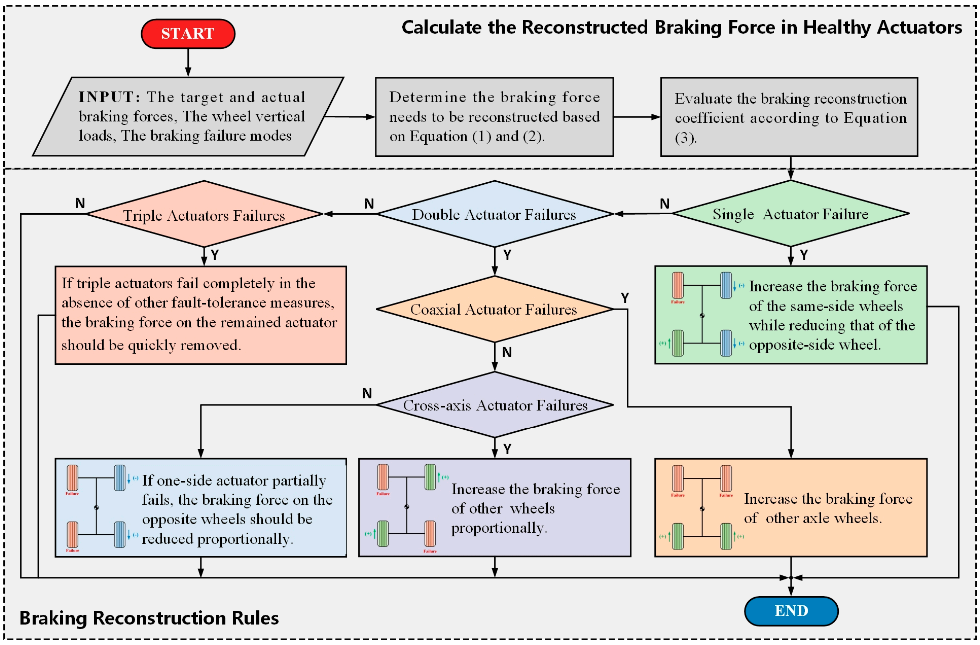

START
Calculate the Reconstructed Braking Force in Healthy Actuators
INPUT: The target and actual braking forces, The wheel vertical loads, The braking failure modes
Determine the braking force needs to be reconstructed based on Equation (1) and (2).
Evaluate the braking reconstruction coefficient according to Equation (3).
Triple Actuators Failures
Double Actuator Failures
Single Actuator Failure
N
Y
If triple actuators fail completely in the absence of other fault-tolerance measures, the braking force on the remained actuator should be quickly removed.
Coaxial Actuator Failures
Increase the braking force of the same-side wheels while reducing that of the opposite-side wheel.
Cross-axis Actuator Failures
If one-side actuator partially fails, the braking force on the opposite wheels should be reduced proportionally.
Increase the braking force of other wheels proportionally.
Increase the braking force of other axle wheels.
END
Braking Reconstruction Rules

Figure 10. The principle of FTC.

3.3.2. Reconstructed Braking Force

To fully utilize the ground adhesion, this section calculates the reconstructed braking force of the healthy WEAs based on wheel vertical loads according to the braking reconstruction scheme shown in Figure 10, and the complete failure of the left-front WEA is taken as example to verify the braking reconstruction rules.

First, we determine the failed WEA(s) and the lost braking force, and the braking force needs to be reconstructed as numerically equal to the total lost braking force.

Second, the braking force that needs to be reconstructed is allocated into healthy WEAs proportionally based on vertical load of the wheels where the healthy WEAs located in. Based on the braking reconstruction rules, the reconstructed braking force in healthy WEAs were as follows.

$$F_{recons,i} = F_{xd,i} \pm F_{recons} \cdot i_{recons,i} \leq F_{x\max,i} \tag{1}$$

where $F_{xd,i}$ is the target braking force in the failed WEA, i represents the position of the failed WEA, the sign is determined by the braking reconstruction rules, F_{recons} is the braking force that needs to be reconstructed, $i_{recons,i}$ is the reconstruction coefficient, and the $F_{x\ \max,i}$ represents the maximum braking force of the WEA.

Finally, to reflect the driver's intention as well as possible, the total braking force acting on the vehicle is not allowed to exceed the driver's expected braking force during braking reconstruction [28].

Above all, the principle of FTC is shown in Figure 10.

It should be noted that the FTC is also used to determine whether the braking and handling stability of the vehicle satisfy the established SG after the WEA's failure and to further assess the availability of the WEA matrix.

4. Analyses of the EMB System Architecture

In this section, the EMB system architecture is analyzed by the FTA to identify the minimal cut sets (MCSs) that lead to hazard events. Second, the operating states of the WEA matrix and their transition probabilities are analyzed based on the MC method. Finally, the residual braking ability under various operating states is tested using HIL tests based on the FTC strategy. By comparing the results with the established safety goals, the availability of the WEA matrix is evaluated.

4.1. FTA of the EMB System

To trace the causes of the EMB system failure back to components, the top events need to be analyzed. Exemplifying the established safety goal "SG1: Avoid MFDD below 5.15 m/s^2 during vehicle operation", the top event after system failure can be defined as "MFDD is below 5.15 m/s^2 during vehicle operation", as in the FTA of the EMB system illustrated in Figure 11.

It can be seen from Figure 11 that any failure of the components, such as the sensors, MCU, WEA, power supply, or communication components, may lead to system failure, which ultimately leads to the occurrence of the top event.

To determine the probability of the MCSs leading to the top event, FTAs for sensors, MCUs, WEAs, power supplies, and communication buses are required. However, since the failure probabilities of the sensors, power supplies, and communication buses can be referred from SN29500 and IEC 62380 [29], the further FTA will only focus on the MCUs and WEAs. MCU1 is taken as an example, as in the FTA shown in Figure 12.

As depicted in Figure 12, if one of the HMIs, AD/DA module, ECUs, J1587 interface, star couplers, or power manager fails, MCU1 will fail. Specifically, simultaneous failures of the dual-channel backups for the HMIs, ECUs, and SCs, as well as single-point failures in the AD/DA module, J1587 interface, or power manager, can all result in MCU1 failure.

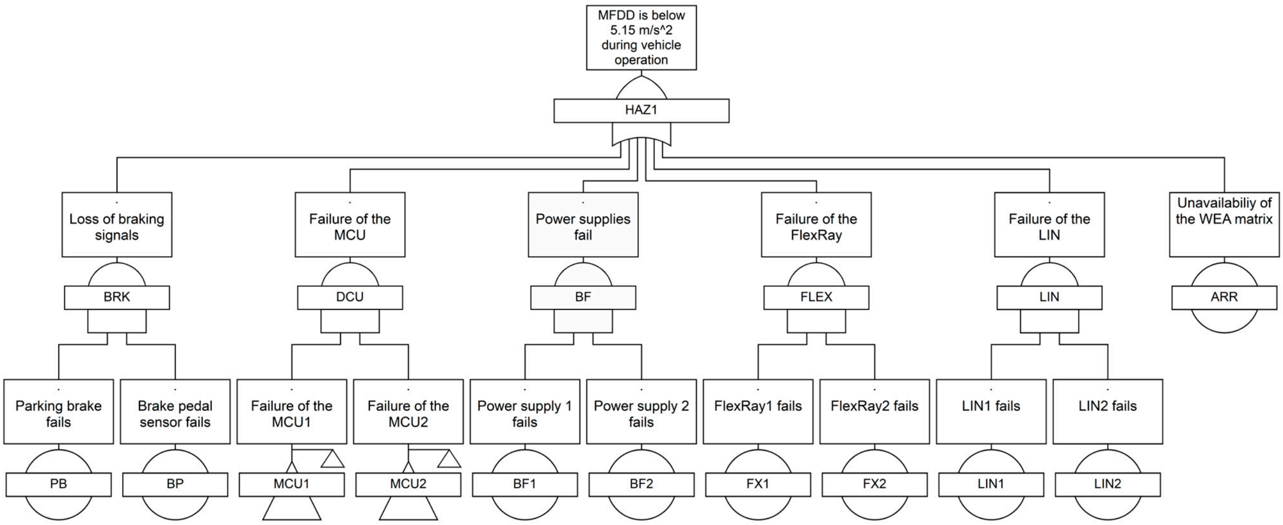


Figure 11. SG1 FTA of the EMB system.

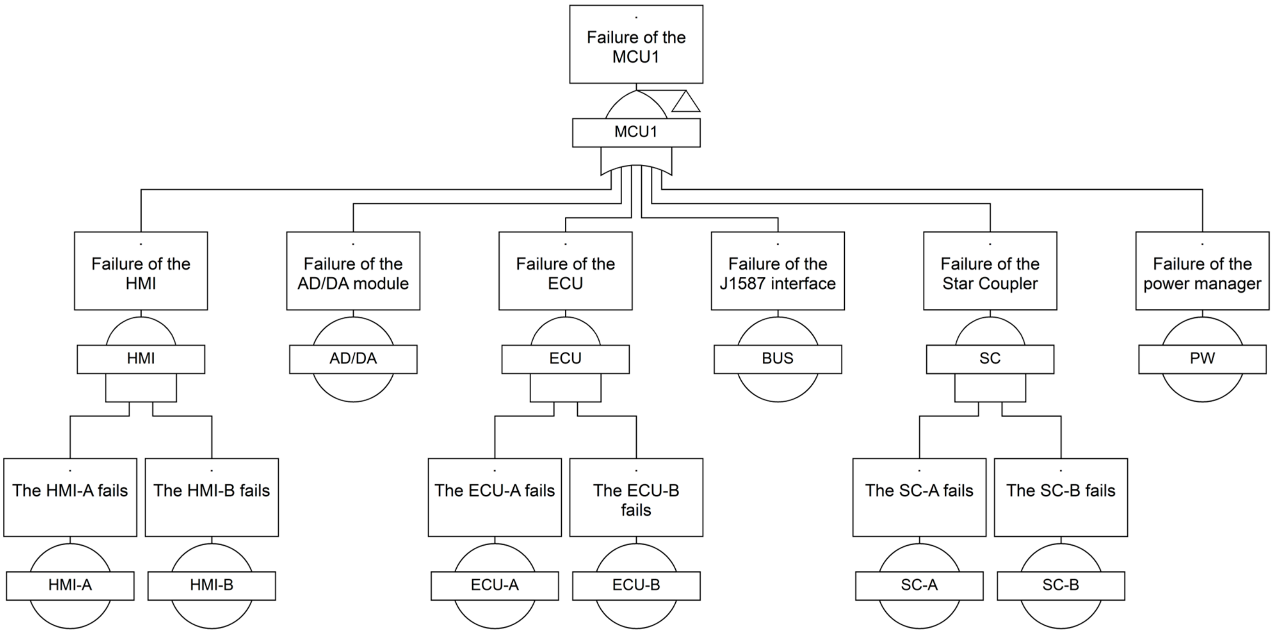
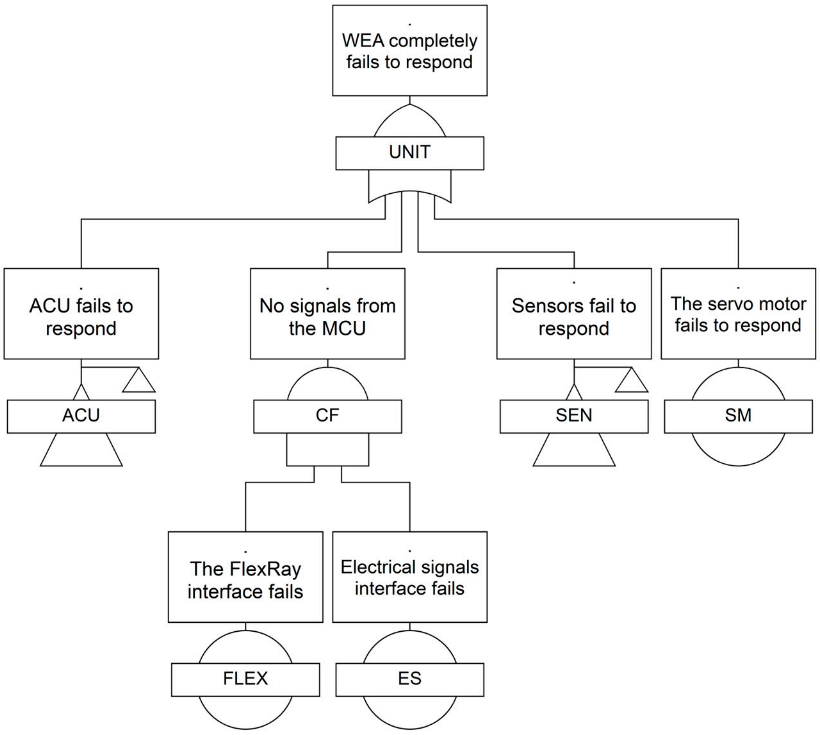


Figure 12. FTA of the MCU.

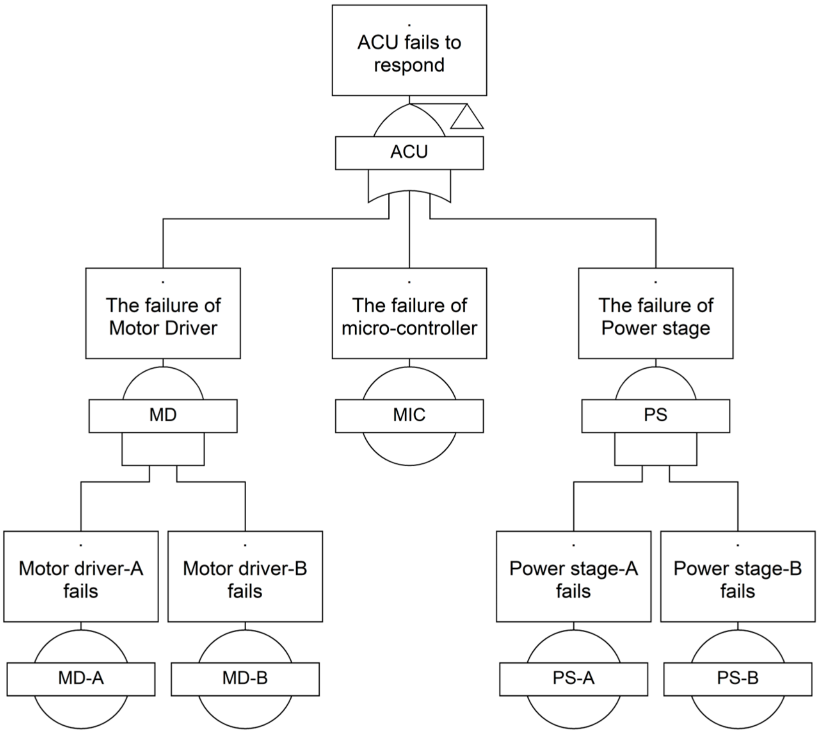
Moreover, the FTA of WEA is illustrated in Figure 13.

As illustrated in Figure 13a, the WEA failures encompass ACU non-responsiveness, inability to receive MCU signals, sensor non-responsiveness, and servo motor non-responsiveness. If both the FlexRay interfaces and the electrical signal interfaces fail simultaneously, the WEA will be unable to receive MCU signals. Additionally, the events of "ACU fails to respond" and "sensor fails to respond" require further decomposition. From Figure 13b, "ACU fails to respond" may be attributed to failures in the motor drive module, micro-controller, or power stage. Figure 13c indicates that "sensor fails to respond" may result from the absence of braking force signals, motor speed signals, or motor current signals.

In summary, the MCSs which leading the MCU1 and WEA failures are quantitatively analyzed. Furthermore, the failure probability of the MCU and WEA can be obtained [9].

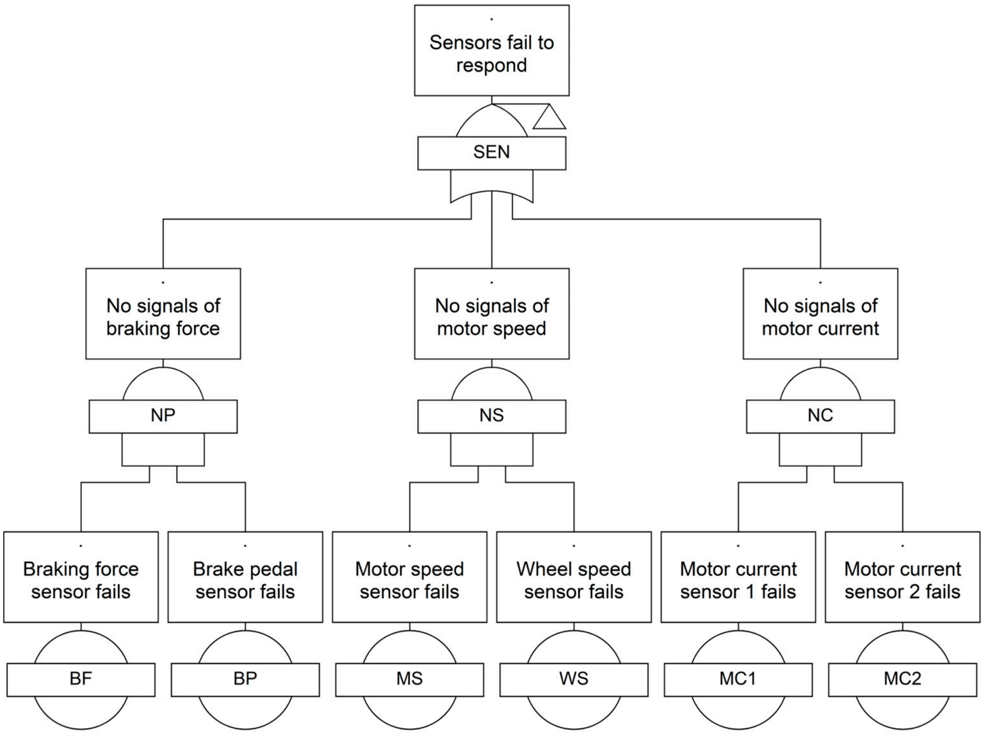

WEA completely fails to respond
UNIT
ACU fails to respond
ACU
No signals from the MCU
CF
Sensors fail to respond
SEN
The servo motor fails to respond
SM
The FlexRay interface fails
FLEX
Electrical signals interface fails
ES

(**a**) FTA of the failure "WEA completely fails to respond".



(**b**) FTA of the failure "ACU fails to respond".

Figure 13. *Cont.*


Sensors fail to respond
SEN
No signals of braking force
No signals of motor speed
No signals of motor current
NP
NS
NC
Braking force sensor fails
Brake pedal sensor fails
Motor speed sensor fails
Wheel speed sensor fails
Motor current sensor 1 fails
Motor current sensor 2 fails
BF
BP
MS
WS
MC1
MC2

(**c**) FTA of the failure "sensors fail to respond".

Figure 13. FTA of the WEA.

4.2. Analysis of the WEA Matrix

If the WEA fails and the residual braking ability of the vehicle cannot satisfy the requirements of safety goals under the effect of FTC, it is considered that the WEA matrix is unavailable. The unavailability of the WEA matrix will also lead to the occurrence of hazard events. Hence, further analysis of the operating states and failure modes of the WEA matrix is needed. Since WEA fails in random ways, it is hard to analyze the operating states based on FTA. Therefore, this section uses the MC to analyze the operating states and calculate the transition probabilities between each state. The MC can address the system's multi-state relationships and temporal dependencies, effectively compensating for the limitations of FTA. Assuming the WEA matrix is composed of four WEAs, six operating states are defined as follows:

- S_0: All WEAs are operating normally.
- S_1: A single WEA has completely failed.
- S_2: Dual WEAs on the same side have completely failed.
- $S_{2.5}$: Dual WEAs on the same axle or diagonal position have completely failed.
- S_3: Triple WEAs have completely failed.
- S_4: All WEAs have completely failed.

According to the operating states of WEA matrix, the transition between two states is defined as follows:

- T_1: Transition from the state S_0 to S_1.
- T_2: Transition from the state S_1 to S_2.
- $T_{2.5}$: Transition from the state S_1 to $S_{2.5}$.
- T_3: Transition from the state S_2 or $S_{2.5}$ to S_3.
- T_4: Transition from the state S_3 to S_4.
- T_5: Transition from the state S_1 to S_3, S_2 to S_4 or $S_{2.5}$ to S_4.
- T_6: Transition from the state S_0 to S_2.
- T_7: Transition from the state S_0 to $S_{2.5}$.
- T_8: Transition from the state S_0 to S_3 or S_1 to S_4.

- T_9: Transition from the state S_0 to S_4.

  In summary, the WEA matrix is analyzed based on the MC, as shown in Figure 14.

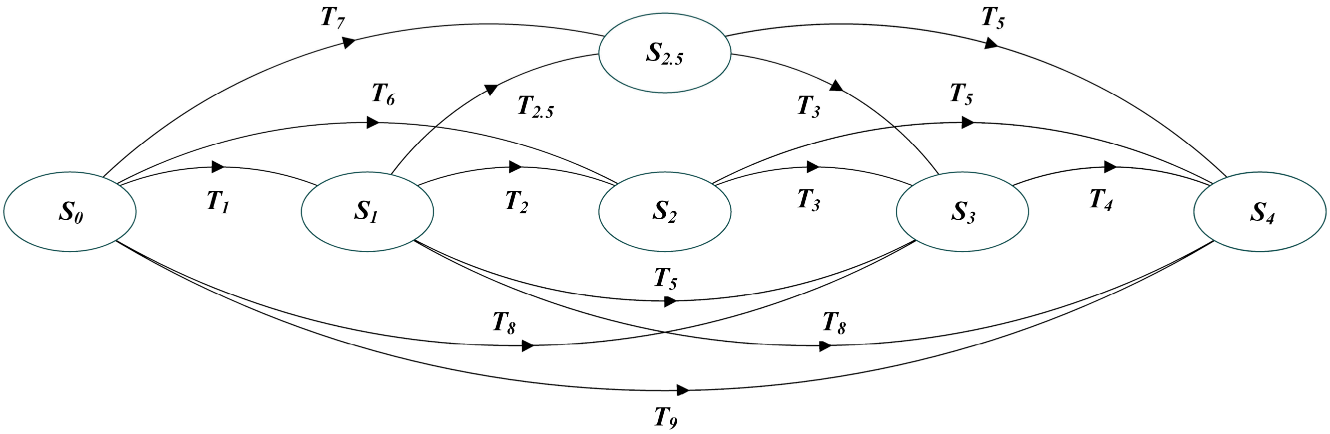


Figure 14. Markov chain of the WEA matrix.

In Figure 14, each ellipse represents an operating state of the WEA matrix, and the curved arrows indicate the permitted transitions between these states. Assuming λ, α, β, and γ, respectively, represent the probabilities of a single WEA, dual WEAs, triple WEAs, and all WEAs failing completely. We further assume that the transitions between states are irreversible; that is, WEAs do not have self-repair capability. Hence, the transition probabilities between those operating states are shown in Table 6.

Table 6. Transfer probabilities between operating states of the WEA matrix.

Transition	Transition Probability	Transition	Transition Probability
T_1	4λ	T_5	α
T_2	λ	T_6	0.33α
$T_{2.5}$	2λ	T_7	0.67α
T_3	2λ	T_8	β
T_4	λ	T_9	γ

4.3. Analysis of the WEA Matrix Availability

The braking performance will be weakened when the WEA fails. To determine the availability of the WEA matrix, the previously mentioned FTC strategy and the self-developed EMBs HIL test platform (Figure 15) are used to analyze the operating states of the WEA matrix except S_0 in this section.

From Figure 15, it can be seen that the platform consists of an upper computer, a WEA matrix, a rapid prototype controller, and DC power. The specific details are as follows:

1. The upper computer is responsible for model compilation, program flashing, data acquisition, and test control.
2. The rapid prototype controller is used for replacing the MCU, and it consists of the NI PXIe-1082 chassis, the NI PXIe-8840 motherboard, and the CAN boards. Its function is to execute the compiled FTC strategy and to facilitate communication with the WEA matrix via the CAN bus, while simultaneously handling data exchange with the upper computer through the local area network (LAN).
3. The WEA matrix consists of four WEAs, namely the WEA left front, left rear, right front, and right rear.
4. Two DC power supplies are responsible for powering the WEA matrix.

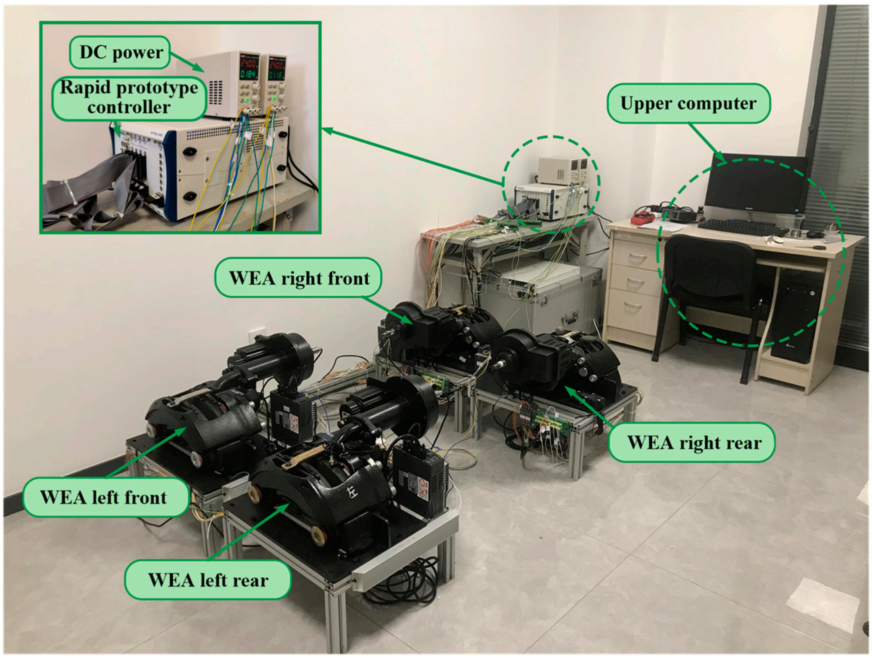
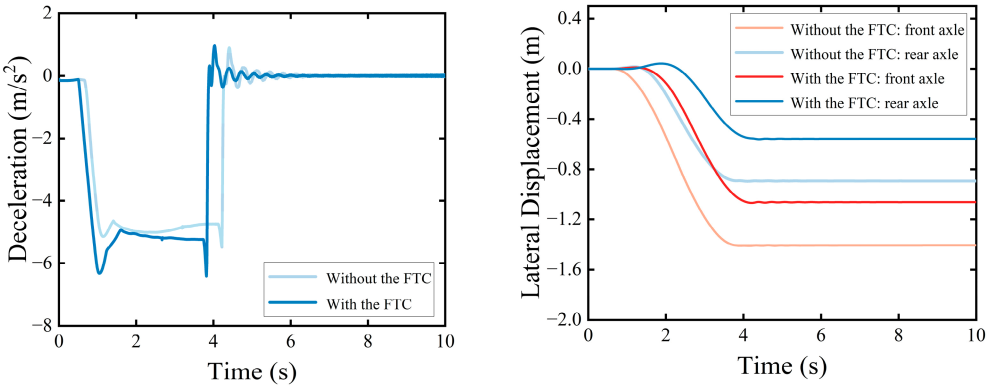


Figure 15. EMB system HIL test platform.

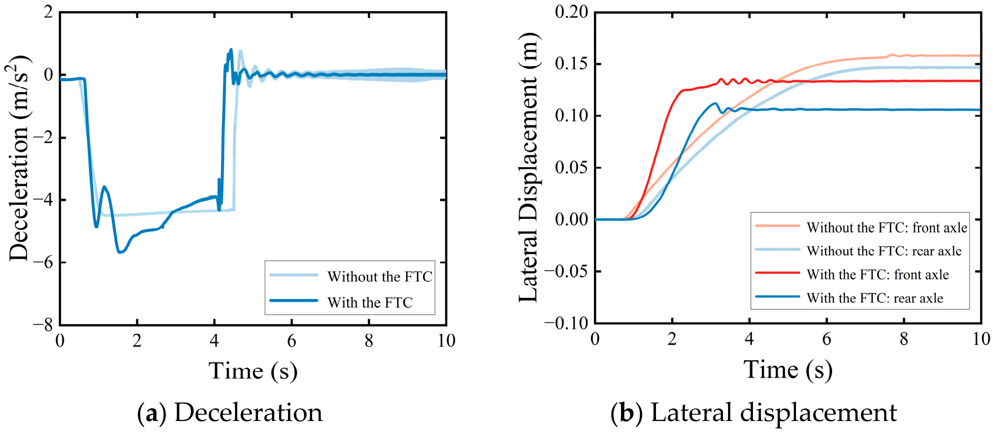
The working principle of the HIL test platform is as follows: Firstly, the rapid prototype controller runs the FTC strategy corresponding to the test conditions to determine the target braking force for each WEA. These target braking force signals are transmitted to the ACU via the CAN bus. The ACU then manages the operation of each WEA and generates braking force according to the closed-loop cascade control architecture mentioned in Section 3.2. Subsequently, the braking force output by each WEA is conveyed to the rapid prototype controller via the CAN bus and sent to the upper computer through the LAN. The vehicle dynamics model running in the upper computer calculates the vehicle state signals and displays, along with WEA status information (such as motor speed, torque, and current), on the human–machine interface (HMI).

Referring to GB12676-2014 [30], the vehicle is set to full braking in a straight and horizontal lane at an initial velocity of 60 km/h with a friction coefficient of 0.85. The deceleration and lateral displacement of the front and rear axles are selected as indicators, and the results are shown in Figures 16–18.



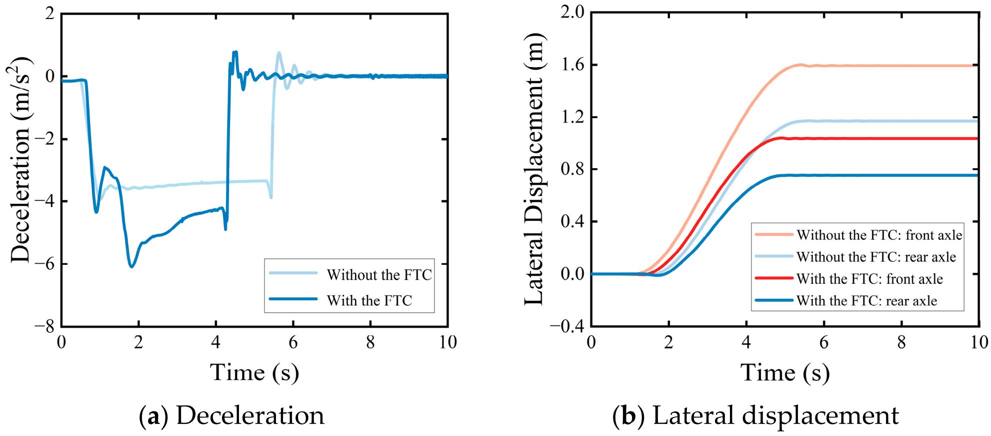
(**a**) Deceleration (**b**) Lateral displacement

Figure 16. Left front WEA completely fails.



(**a**) Deceleration (**b**) Lateral displacement

Figure 17. Front axle WEAs completely fail.



(**a**) Deceleration (**b**) Lateral displacement

Figure 18. Diagonal WEAs completely fail.

4.3.1. Left Front WEA Completely Fails

From Figure 16, when the left front WEA completely fails under the fault-tolerant strategy, the vehicle's maximum deceleration is approximately 6.41 m/s^2, and the lateral displacement of the front and rear axles are −1.06 m and −0.59 m, respectively.

4.3.2. Front Axle WEAs Completely Fail

From Figure 17, when the front axle WEAs completely fail under the fault-tolerant strategy, the vehicle's maximum deceleration is approximately 5.72 m/s^2, and the lateral displacement of the front and rear axles are 0.13 m and 0.10 m, respectively.

4.3.3. Diagonal WEAs Completely Fail

From Figure 18, when the diagonal WEAs completely fail under the fault-tolerant strategy, the vehicle's maximum deceleration is approximately 6.13 m/s^2, and the lateral displacement of the front and rear axles are 1.13 m and 0.78 m, respectively.

We further calculate the MFDD and compare the lateral displacement of the vehicle body under the test cases, as shown in Table 7.

Comparing the results in Table 7 with the safety goals in Table 4, the lateral displacement of vehicle body was notably suppressed with the application of FTC. It can be verified that the safety goals "SG1", "SG2", and "SG3", mentioned in Section 2.2, are satisfied in these three operating states. This ultimately indicates that the vehicle's braking and handling stability meet regulatory requirements.

Table 7. Test results of the braking performance.

No.	WEA Matrix Operating States	MFDD (m/s^2) Without the FTC	With the FTC	Lateral Displacement of Vehicle Body (m) Without the FTC	With the FTC
1	Left front WEA completely fails	4.72	5.41	−1.40/−0.95	−1.06/−0.59
2	Front axle WEAs completely fail	4.23	5.27	0.16/0.14	0.13/0.10
3	Diagonal WEAs completely fail	3.85	5.62	1.60/1.19	1.13/0.78

Furthermore, according to the above FTC strategy, if the "WEAs on the same side" and "triple or all WEAs" fail completely in the absence of other fault-tolerance measures, the braking force on the remained WEA(s) should be quickly removed to ensure stability, and the vehicle will completely lose its braking ability. Hence, the aforementioned operating states do not satisfy the safety goals and pose potential risks to the vehicle, such as drifting, collisions, or even rollover.

Above all, the WEA matrix is considered available only in the following operating states:

S_0: All WEAs are operating normally.

S_1: Only one WEA has completely failed.

$S_{2.5}$: Dual WEAs on the same axle or diagonal position have completely failed.

Conversely, the WEA matrix is considered not available in the following states:

S_2: Dual WEAs on the same side have completely failed.

S_3: Triple WEAs have completely failed.

S_4: All WEAs have completely failed.

5. Verification of the EMB System Architecture

This section verified the proposed EMB system architecture from bottom to top. Specifically, the probabilities of the top events leading to WEA failure are determined based on the FTA of the WEA. Second, according to analysis of WEA matrix availabilities, the steady-state probabilities for each unavailable state of the WEA matrix and its failure rate are calculated. Finally, the ASIL of the EMB system architecture is verified by comparing its probability metric for random hardware failures (PMHF) with the requirements of ISO 26262.

5.1. Failure Rate of a Single WEA

To further determine the steady-state probability of the WEA matrix entering an unavailable state, it is necessary to analyze the failure probability of the WEA firstly. Hence, this section takes the event "WEA completely unresponsive" as an example for analyzing, and the MCSs of the fault tree depicted in Figure 13 are identified, as shown in Table 8.

Table 8. MCSs of the WEA fault tree.

No.	MCS	No.	MCS
1	MIC (Microcontroller)	5	MC1, MC2 (Motor Current Sensor)
2	SM (Servo Motor)	6	FLEX, ES (FlexRay, Electrical Signal Line)
3	MD-A, MD-B (Motor Driver)	7	MS, WS (Motor Speed, Wheel Speed Sensor)
4	PS-A, PS-B (Power Stage)	8	BF, BP (Braking Force, Brake Pedal Sensor)

Subsequently, the frequency of the MCSs within unit time is recorded as the hardware failure rate, with units of FIT (10^{-9} h^{-1}) [9]. The failure rates of the related electronic components are referenced in [29] and listed in Table 9.

Table 9. Hardware failure rate of the WEA.

No.	Component	Failure Rate (FIT)	No.	Component	Failure Rate (FIT)
1	FlexRay	100	7	Braking Force Sensor	50
2	Electrical Signal Line	100	8	Brake Pedal Sensor	100
3	Motor Driver	300	9	Motor Speed Sensor	100
4	Microcontroller	50	10	Wheel Speed Sensor	100
5	Power Stage	150	11	Motor Current Sensor	100
6	Servo Motor	10			

On this basis, assuming the probability of the top event caused by the MCS is Q_0, there is

$$Q_0 \approx 1 - \prod_{j=1}^{k} (1 - Q_j) \approx \sum_{j=1}^{k} Q_j \tag{2}$$

where k is the number of MCS; Q_j represents the probability of all events of the jth MCS simultaneous occurring. Furthermore,

$$Q_j = \prod_{i=1}^{m_j} q_i \tag{3}$$

where m represents the number of events contained in the MCS j, and q_i denotes the probability of the event i.

From Figure 13a and Tables 8 and 9, the probability of the top event "WEA completely fails to respond" is Q_0 = 21.5 FIT.

5.2. Failure Rate of the WEA Matrix

According to the analysis, the probability λ of a single WEA being completely unresponsive is numerically equal to Q_0. Assuming that the WEAs do not have self-repair capabilities, there is a relationship between the probability α, β, and γ,

$$\gamma \ll \beta \ll \alpha \ll \lambda_0^2 = 4.62 \times 10^{-7}\text{FIT} \tag{4}$$

Generally, the values of α, β, and γ are extremely minor, and it can be approximated that the corresponding events are nearly impossible. Based on the transition probabilities shown in Table 6, the state transition matrix of the MC in Figure 14 is defined as follows,

$$P = \begin{bmatrix} 1-4\lambda & 4\lambda & 0 & 0 & 0 & 0 \\ 0 & 1-3\lambda & 3\lambda & 0 & 0 & 0 \\ 0 & 0 & 1-2\lambda & 2\lambda & 0 & 0 \\ 0 & 0 & 0 & 1-\lambda & \lambda & 0 \\ 0 & 0 & 0 & 0 & 1-\lambda & \lambda \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

where the element P_{ij} represents the probability of the transition from state i $(0 \le i \le 6)$ to state j $(0 \le j \le 6)$.

When the MC reaches a steady state, the steady-state probabilities π for each state S_i should satisfy the following equation:

$$\pi P = \pi \tag{5}$$

Additionally, the normalization condition also must be met, which is as follows:

$$\begin{cases} \pi_0 + \pi_1 + \pi_2 + \pi_{2.5} + \pi_3 + \pi_4 & = 1 \\ \pi_0(1 - 4\lambda) & = \pi_0 \\ \pi_0 4\lambda + \pi_1(1 - 3\lambda) & = \pi_1 \\ \pi_1 3\lambda + \pi_2(1 - 2\lambda) & = \pi_2 \\ \pi_1 3\lambda + \pi_{2.5}(1 - \lambda) & = \pi_{2.5} \\ \pi_{2.5}\lambda + \pi_3(1 - \lambda) & = \pi_3 \\ \pi_3\lambda + \pi_4 & = \pi_4 \end{cases} \tag{6}$$

Combining Equations (5) and (6), the steady-state probabilities for each operating state in the MC are as follows:

$$\pi = \begin{bmatrix} 0.9998 & 2.149 \times 10^{-4} & 7.705 \times 10^{-9} & 1.541 \times 10^{-8} & 1.243 \times 10^{-12} & 2.673 \times 10^{-17} \end{bmatrix}$$

Based on the analysis of the WEA matrix, it is known that the state "S_2: Dual WEAs on the same side have completely failed, S_3: Triple WEAs have completely failed, S_4: All WEAs have completely failed" will lead the WEA matrix to be unavailable. Therefore, the unavailability Q of the WEA matrix is the sum of the steady-state probabilities of S_2, S_3, and S_4; that is,

$$Q = \pi_2 + \pi_3 + \pi_4 = 7.705 \times 10^{-9} \tag{7}$$

assuming that the failure rates of the components are constant, and the failure time follows an exponential distribution. Additionally, according to ISO 26262 [8], we set the life time of the EMB system at 10,000 h. The relationship between the unavailability and the failure rate of the WEA matrix is

$$Q(t) = 1 - e^{-\lambda t} \tag{8}$$

In summary, the failure rate of the WEA matrix is λ = 9.244 × 10^{-3} FIT.

5.3. Verification of the EMB System Safety Goals

Enhancing system reliability by reducing the random failure of each component, thereby decreasing the occurrence of hazardous events, is the pursuit of functional safety development. Therefore, the PMHF is the main criterion for assessing the ASIL of EMB systems. The correspondence between the PMHF and the ASIL is listed in Table 10 according to ISO 26262 [9].

Table 10. Targets PMHF of the ASIL.

ASIL	PMHF
A	<1000 FIT
B	<100 FIT
C	<100 FIT
D	<10 FIT

Furthermore, the failure rates of electronic components associated with the MCUs, sensor components, communication buses, power supplies, and the WEA matrix are presented in Table 11 [29].

Table 11. Hardware failure rate of EMB components.

No.	Component	Failure Rate (FIT)	No.	Component	Failure Rate (FIT)
1	Pedal Sensor	100	6	Star Coupler	100
2	Parking Brake	50	7	AD/DA	200
3	Power Supply	500	8	J1587 Interface	100
4	HMI	150	9	Power Manager	300
5	MCU	200	10	WEA Matrix	9.244×10^{-3}

Based on Equations (2) and (3), it can be calculated that the PMHF for the safety goal "Avoid MFDD below 5.15 m/s^2 during vehicle operation" is 6.14 FIT. Similarly, the PMHF for the safety goals "Avoid a maximum unintended deceleration exceeding 2.44 m/s^2 during vehicle operation" and "Avoid lateral displacement of the vehicle body exceeding 1.20 m due to the EMB system failure during vehicle operation" are 5.89 FIT and 6.03 FIT, respectively. As shown in Table 10, the PMHFs of the EMB system for SG1, SG2, and SG3 are all lower than the targets required by ASIL-D. In summary, the EMB system architecture proposed in this study satisfies the ASIL-D requirements, and the functional safety of the system can be guaranteed under the expected operational conditions.

6. Conclusions

Functional safety is the main bottleneck restricting the large-scale application of EMB systems. To solve this issue, we propose an EMB system architecture and further analyze and validate it based on functional safety methods. Specifically, the top events leading to system failures are analyzed based on the FTA; the WEA matrix operating states are evaluated according to the established MC, and the WEA matrix unavailability is determined by the FTC strategy proposed in this study. Finally, the EMB system architecture is verified through comparing the PMHF with the limit of ASIL. The main conclusions are as follows:

1. The proposed EMB system architecture satisfies the safety concept, and each component in the system also satisfies the TSR.
2. The WEA matrix has six operating states, and these can be further categorized into three available states and three unavailable states. The unavailability of the WEA matrix is 9.244×10^{-3} FIT.
3. The PMHFs of the EMB system for each safety goal are 6.14 FIT, 5.89 FIT, and 6.03 FIT, respectively, and the system satisfies the ASIL-D requirements.

We will focus on improving the accuracy of the component failure rates, discovering the effect of the WEA scheduled maintenance on the availability calculation. Additionally, the vehicle road tests are considered in the future.

Author Contributions: Conceptualization, T.W. and L.C. conceptualized the study, focusing on the EMB system architectural design and analysis in accordance with the functional safety standards; methodology, T.W. and L.C. developed the methodology, including the FTA of the EMB system and the MC of the WEA matrix; software, J.P. was responsible for designing the software required for the simulations; validation, J.P. and T.W. validated the models and control strategies through various tests; formal analysis, J.P. conducted formal analysis of the simulation results; investigation, J.P. conducted investigations into the crucial parts of the EMB systems affecting the functional safety; resources, T.W. and L.C. provided necessary resources for the study; data curation, J.R. and X.Y. managed and curated the data obtained from the simulations; writing—original draft, J.P. prepared the initial draft of the manuscript, detailing the findings and methodologies; writing—review and editing, T.W. and J.P. reviewed and edited the manuscript to ensure clarity and accuracy; visualization, J.R. and Y.M. plotted graphs, tables, and diagrams to support the findings; supervision, L.C. and T.W. supervised the entire project and provided guidance; project administration, T.W. managed to ensure the project was completed on time; funding acquisition, T.W. and L.C. secured the funding to conduct the project. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Project of Central Guidance for Local Scientific and Technological Development of Hubei with Grant No. 2022BGE248, the Open Foundation of Key Laboratory of Automotive Power Train and Electronics (Hubei University of Automotive Technology) with Grant No. ZDK1202204, and the PhD Scientific Research Foundation of Hubei University of Automotive Technology with Grant No. BK202214.

Data Availability Statement: The data presented in this study are available in the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

EMB	Electro-Mechanical Brake
WEA	Wheel-End Actuator
ASIL	Automotive Safety Integrity Level
SG	Safety Goal
TSR	Technical Safety Requirement
PMHF	Probabilistic Metric for Hardware Failures
FIT	Failures in Time
FTA	Fault Tree Analysis
MC	Markov Chain
FTC	Fault-Tolerant Control
MCU	Main Control Unit
ACU	Actuator Control Unit
MCS	Minimal Cut Set

References

1. Gong, X.; Ge, W.; Yan, J.; Zhang, Y.; Gongye, X. Review on the Development, Control Method and Application Prospect of Brake-by-Wire Actuator. *Actuators* **2020**, *9*, 15. [CrossRef]
2. Fang, Y.; Wang, W.; Yang, C.; Zhang, Y.; Chen, Z. Brake-by-Wire Architecture Design and Analysis in Accordance with Functional Safety Standard. *Proc. Inst. Mech. Eng. Part D J. Automob. Eng.* **2023**, 09544070231185192. [CrossRef]
3. Schrade, S.; Nowak, X.; Verhagen, A.; Schramm, D. Short Review of EMB Systems Related to Safety Concepts. *Actuators* **2022**, *11*, 214. [CrossRef]
4. Li, C.; Zhuo, G.; Tang, C.; Xiong, L.; Tian, W.; Qiao, L.; Cheng, Y.; Duan, Y. A Review of Electro-Mechanical Brake (EMB) System: Structure, Control and Application. *Sustainability* **2023**, *15*, 4514. [CrossRef]
5. *ISO 26262-1:2018*; Road Vehicles—Functional Safety—Part 1: Vocabulary. International Organization for Standardization: Geneva, Switzerland, 2018.
6. *ISO 26262-1:2018*; Road Vehicles—Functional Safety—Part 2: Management of Functional Safety. International Organization for Standardization: Geneva, Switzerland, 2018.
7. *ISO 26262-1:2018*; Road Vehicles—Functional Safety—Part 3: Concept Phase. International Organization for Standardization: Geneva, Switzerland, 2018.
8. *ISO 26262-1:2018*; Road Vehicles—Functional Safety—Part 4: Product Development at the System Level. International Organization for Standardization: Geneva, Switzerland, 2018.
9. *ISO 26262-1:2018*; Road Vehicles—Functional Safety—Part 5: Product Development at the Hardware Level. International Organization for Standardization: Geneva, Switzerland, 2018.
10. *ISO 26262-1:2018*; Road Vehicles—Functional Safety—Part 9: Product Development at the Software Level. International Organization for Standardization: Geneva, Switzerland, 2018.
11. Li, C.; Zhang, J.; Hou, X.; Ji, Y.; Han, J.; He, C.; Hao, J. A Novel Double Redundant Brake-by-Wire System for High Automation Driving Safety: Design, Optimization and Experimental Validation. *Actuators* **2021**, *10*, 287. [CrossRef]
12. Schranner, F.S.; Misheni, A.A.; Warnecke, J. Deriving a Representative Variant for the Functional Safety Development According to ISO 26262. *Reliab. Eng. Syst. Saf.* **2021**, *209*, 107436. [CrossRef]
13. Li, J.; Jiang, Y. Variable Universe Fuzzy–Proportional-Integral-Differential-Based Braking Force Control of Electro-Mechanical Brakes for Mine Underground Electric Trackless Rubber-Tired Vehicles. *Sensors* **2024**, *24*, 2739. [CrossRef] [PubMed]
14. Li, Y.; Shim, T.; Shin, D.-H.; Lee, S.; Jin, S. Control System Design for Electromechanical Brake System Using Novel Clamping Force Model and Estimator. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8653–8668. [CrossRef]
15. Soltanali, H.; Khojastehpour, M.; Farinha, J.T.; Pais, J.E.D.A.E. An Integrated Fuzzy Fault Tree Model with Bayesian Network-Based Maintenance Optimization of Complex Equipment in Automotive Manufacturing. *Energies* **2021**, *14*, 7758. [CrossRef]
16. Famfulik, J.; Richtar, M.; Rehak, R.; Smiraus, J.; Dresler, P.; Fusek, M.; Mikova, J. Application of Hardware Reliability Calculation Procedures According to ISO 26262 Standard. *Qual. Reliab. Eng.* **2020**, *36*, 1822–1836. [CrossRef]

17. Wu, X.; Zhang, M.; Xu, M. Active Tracking Control for Steer-by-Wire System with Disturbance Observer. *IEEE Trans. Veh. Technol.* **2019**, *68*, 5483–5493. [CrossRef]
18. Huang, C.; Li, L. Architectural Design and Analysis of a Steer-by-Wire System in View of Functional Safety Concept. *Reliab. Eng. Syst. Saf.* **2020**, *198*, 106822. [CrossRef]
19. López-Estrada, F.-R.; Rotondo, D.; Valencia-Palomo, G. A Review of Convex Approaches for Control, Observation and Safety of Linear Parameter Varying and Takagi-Sugeno Systems. *Processes* **2019**, *7*, 814. [CrossRef]
20. *SAE Standard J2980*; Considerations for ISO 26262 ASIL Hazard Classification. SAE International: Warrendale, PA, USA, 2023.
21. Becker, C.; Arthur, D.; Brewer, J. *Functional Safety Assessment of a Generic, Conventional, Hydraulic Braking System with Antilock Brakes, Traction Control, and Electronic Stability Control*; National Highway Traffic Safety Administration: Washington, DC, USA, 2018.
22. Jo, C.; Hwang, S.; Kim, H. Clamping-Force Control for Electromechanical Brake. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3205–3212. [CrossRef]
23. Line, C.; Manzie, C.; Good, M.C. Electromechanical Brake Modeling and Control: From PI to MPC. *IEEE Trans. Contr. Syst. Technol.* **2008**, *16*, 446–457. [CrossRef]
24. Feng, C.; Ding, N.; He, Y.; Xu, G.; Gao, F. A Control Allocation Algorithm for Improving the Fail-Safe Performance of an Electric Vehicle Brake System. *SAE Int. J. Passeng. Cars—Electron. Electr. Syst.* **2013**, *6*, 134–143. [CrossRef]
25. Lee, J.; Oh, K.; Yoon, Y.; Song, T.; Lee, T.; Yi, K. Adaptive Fault Detection and Emergency Control of Autonomous Vehicles for Fail-Safe Systems Using a Sliding Mode Approach. *IEEE Access* **2022**, *10*, 27863–27880. [CrossRef]
26. Anwar, S.; Chen, L. An Analytical Redundancy-Based Fault Detection and Isolation Algorithm for a Road-Wheel Control Subsystem in a Steer-By-Wire System. *IEEE Trans. Veh. Technol.* **2007**, *56*, 2859–2869. [CrossRef]
27. Cao, X.; Tian, Y.; Ji, X.; Qiu, B. Fault-Tolerant Controller Design for Path Following of the Autonomous Vehicle Under the Faults in Braking Actuators. *IEEE Trans. Transp. Electrific.* **2021**, *7*, 2530–2540. [CrossRef]
28. Zhou, J.; Di, Y.; Miao, X. Single-Wheel Failure Stability Control for Vehicle Equipped with Brake-by-Wire System. *World Electr. Veh. J.* **2023**, *14*, 177. [CrossRef]
29. *SN 29500*; Failure Rates of Components Expected Values, General. SIEMENS: Munich, Germany, 2005.
30. *GB/T 12676-2014*; Technical Requirements and Testing Methods for Commercial Vehical and Trailer Braking Systems. Standards Press of China: Beijing, China, 2014.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.