Research on Testing Method of Fault Injection for Motor Controller

Bin Wang¹, Zezhong Zhang¹*, Kai Ma¹, Xin Huang¹, Fang Wang¹ and Bo Li¹
¹China Automobile Technology Research Center Co., Ltd, Tianjin, China

*Corresponding author email: zhangzezhong@catarc.ac.cn

Abstract. According to the ISO 26262 standard, the fault injection test in the R&D verification stage can clearly show the stability or safety response ability of the Unit Under Test in the face of various faults or extreme conditions. This paper introduces the safety state mode of the motor drive system for electric vehicles, analyzes the possible fault forms of the Motor Controller Unit, builds a power hardware-in-the-loop test platform and carries out fault injection test by taking the motor rotation fault as an example. The results show that the fault injection test method proposed in this paper is an effective means to verify the functional safety of the electric drive system.

Keywords: Fault injection; MCU; Functional safety; Motor Drive System; Power HIL.

1. Introduction
For energy saving and global warming prevention, the automotive industry is transitioning from fuel powered vehicles to electric vehicles. There are more and more electrical and/or electronic (E/E) systems in one electric vehicles. Meanwhile, with the trend of increasing technological complexity, software content, and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures. Safety is one of the key issues in the development of road vehicles[1][2]. The ISO 26262 series of standards are an automotive specific standard that focuses on functional safety aspects for E/E systems for production vehicles, which was launched in 2011, and updated in 2018. In the west, it is imperative for Original Equipment Manufacturers (OEMs) and supplies to strictly follow these guidelines for functionally safe E/E systems. By contrast, many OEMs and supplies in China have begun to have specific functional safety requirements for MCU, BMS, and VCU, etc[3]. Especially, the GB/T 39086-2020 Functional safety requirements and testing methods for battery management system of electric vehicles is the first functional safety standard for electric vehicles in China[4]. Besides, the GB/T XXXXX—XXXX Functional safety requirements and testing methods for drive motor system of electric vehicles is the second standard, which is currently in the drafting stage. Although, functional safety technology is still in its infancy. These relevant standards and regulations are forcing OEMs and suppliers to increase investment in vehicle safety.
The E-motor Drive system (EDS), as the key powertrain system of electric vehicles. Being part of EDS, the motor control unit (MCU) is safety related electronic control units due to the severity of the accidents/incidents that could result if the MCU is not functional as intended. Compared with traditional fuel vehicles, EV has a shorter development period and has problems such as insufficient experience. The introduction of hundreds of volts of high-voltage electricity and flammable large-capacity batteries makes its functional safety more important. At present, EV still experience controller damage, loss of control of the vehicle, and battery fire caused by failures of the MCU from time to time.
The insecurity of electric vehicles comes from high voltage, high torque, high speed and other aspects. It is necessary to prevent the vehicle from causing unexpected acceleration and deceleration, or damage to components caused by over voltage, over current, and over heating, which endangers the safety of passengers. Therefore, it is necessary to conduct a comprehensive assessment of the safety of the EV based on the three powers (battery, motor, and electronic control). According to the ISO 26262-12:2018 standard, the fault injection technique is a very useful verification method of testing and verification for safety-related systems\cite{1}.

The purpose of this paper is to introduce the safety state mode of the EDS, analyze the possible fault model of the MCU, develop test case, and implement fault injection tests based on a power-level hardware-in-the-loop (Power HIL) test bench.

2. Working Principle and Fault Type of MCU

The working principle of EDS is shown in Figure 1. The signal or power output of MCU interacting with the outside world includes CAN bus, motor temperature signal line, motor speed signal line, DC bus, UVW phase line, KL30, KL15, and cooling system, etc.

![Figure 1. Working principle of EDS.](image)

According to the working principle diagram, the fault caused by abnormal external connection can be deduced. In addition, the fault caused by abnormal logic input/output of controller software drive/protection functions (such as active discharge, Active short circuit mode, freewheeling, etc.) should also be considered. Based on the above factors, the fault types of MCU are summarized as shown in Table 1.

| Fault Type | Description |
|------------|-------------|
| High voltage intermittent connection | Communication signal out of limit |
| High voltage over voltage/under voltage | The communication signal is open/short |
| Low voltage over pressure/under pressure | Motor torque anomaly |
| Low voltage open circuit | Resolver open/short/abnormal |
| Cooling system anomaly | Motor temperature sensor open/short/abnormal |
| Communication node/signal loss | Wake up signal wire open/short/abnormal |
| High voltage busbar/three-phase overcurrent | Collision signal hard wire open/short/abnormal |
| Motor phase current imbalance | High voltage interlock signal hard wire open/short/abnormal |
| Motor excitation-loss | System ASC/Freewheeling abnormal |
| Motor phase line open/short/intermittent connection | Motor/controller grounding disconnect/intermittent connection |
| Motor shaft gets stuck instantly | Abnormal active discharge of system |

Taking high voltage fault as an example, the DC bus of MCU comes from the battery pack, which is connected to IGBT through the main relay and converted into three-phase AC output to the motor. The possible high-voltage faults include: DC bus and three-phase line open/short circuit caused by poor contact of main relay or connector; high or low output voltage of battery pack caused by BMS fault or ambient temperature. In addition, in terms of MCU security mechanism, when collision or shell
removal is detected, the active discharge will occur. If the logic of such safety mechanism has loopholes, it may also cause danger to the passengers or maintenance personnel.

3. Fault Response of MCU

On the basis of ensuring the safety of the whole vehicle and the passengers, the fault response of the MCU should be reasonable and appropriate. It is not allowed to blindly pursue the safety and stop the vehicle to cause panic in the vehicle or affect the convenience of vehicle maintenance, so as to avoid "excessive response". Generally speaking, the fault response of MCU can be divided into four classifications, as shown in Table 2.

| Classification | System stage |
|----------------|--------------|
| 0              | Normal operation without derating |
| 1              | The controller recognizes the fault information and uploads the alarm, and does not perform derating |
| 2              | The controller recognizes the fault information, uploads the alarm and performs derating (including zero torque mode) |
| 3              | The controller recognizes the fault information, uploads the alarm and executes the shutdown (including ASC and freewheeling modes) |
| 4              | The controller recognizes the fault information and uploads the alarm, performs the shutdown and carries out the active discharge |

Among them, level 0 ~ 4 represents the severity of the fault, the more serious the fault, and the higher the response level. The fault recovery mode of the MCU also has an important impact on the safety of the whole vehicle and passengers, especially in case of the MCU shutdown, the untimely recovery and startup may lead to the driver's misjudgment of vehicle out of control, which is very dangerous. Therefore, it is not allowed to resume operation until the maintenance is completed after the serious fault (such as collision) occurs. The classification of fault recovery mode is shown in Table 3. According to the development logic, the more serious the fault, the higher the level of fault recovery.

| Classification | System stage |
|----------------|--------------|
| 1              | After the fault is eliminated, the controller automatically dissolves the fault response |
| 2              | After the fault is eliminated, the fault response removed after stopping and restarting |
| 3              | Failure recovery is not allowed. Repair and replacement of parts by repair shop is required |

4. Safety Status of Electric Drive System

The safety state of electric drive system can be divided into four categories:

- Active short circuit mode (ASC)

In the active short circuit mode, the IGBT short circuit the three-phase AC lines of the motor and cuts off the DC channel at the same time. This is a mode that prohibits the operation of the electric drive system when the fault level is high, and is also conducive to the isolation of high voltage parts. If the motor still rotates during the active short-circuit period, a back electromotive force will be formed in the three-phase short circuit circuit, and the braking torque will be generated to gradually reduce the motor speed. The magnitude of the generated back electromotive force changes with the change of the motor speed, as shown in Figure 2.
It can be seen from Figure 2 that if the ASC is entered at a low speed, a large and unstable braking torque will be generated, causing the vehicle to brake suddenly and affecting the driver’s judgment. Therefore, when formulating strategies, many OEMs restrict the entry into ASC conditions at low speeds.

- **FreeWheeling**
  In the freewheeling mode, IGBT is in the off state, that is, the motor three-phase line and DC bus are disconnected from each other. During the freewheeling period, the motor still relies on inertia to continue to rotate, unless the driver actively intervenes to brake or decelerates by driving resistance. Compared with the active short-circuit mode, freewheeling cannot make the vehicle slow down, so the freewheeling mode is mostly implemented under the condition that the low-speed mode is not applicable to the ASC mode.

- **Limp-home mode**
  When the controller detects the fault of sensor and other electronic components, it starts the standby control loop according to logic, and runs the vehicle with low power until the maintenance is normal.

- **Derating mode**
  In derating mode, when a certain index exceeds the limit value (such as temperature signal) when the vehicle is running, but it is still within the acceptable range of vehicle control, the controller will reduce the power according to the actual working conditions, and generally speaking, the controller can resume operation after the indicators are normal. Derating mode is a safe state between ASC and limp mode.

5. **Fault Injection Test Method**
For the development of vehicle electrical system, the test and verification methods of V model include: Model-in-the-Loop (MIL) test, Software-in-the-Loop (SIL) test, Processor-in-the-Loop (PIL) test, Hardware-in-the-Loop (HIL) test, system level and vehicle level test. The power level hardware-in-the-loop (Power HIL) test should be used for fault injection test of component level MCU.

Power HIL test is an effective method for MCU fault injection test. In this way, the test equipment simulates the real operating environment of the unit under test (UUT), so that the UUT can work normally and the data can be read and record by the test equipment. With Power HIL, technical safety requirements (TSR) can be confirmed whether the safe mechanisms can detect faults, prevent or mitigate failures, and enables an item to achieve or maintain a safe state, with the specified fault tolerant time interval (FTTI) time[^1][^4]. This method can effectively reduce the test cost and improve the test efficiency. The principle of MCU power HIL bench is shown in Figure 3.
The core equipment of MCU power HIL test bench is the motor emulator. Different from the motor test bench, the speed and torque of the motor emulator are virtual values, and the high-voltage DC / AC side voltage is the real value. It can provide MCU with real load operation environment and speed regulation is faster and wider. It can also carry out high-voltage fault injection test without worrying about bench damage[10,11].

The following part takes the motor demagnetization fault as an example to test the fault injection of a certain type of MCU. Under certain conditions, the rotor magnetic material of permanent magnet synchronous motor will undergo irreversible demagnetization, which will lead to abnormal AC output power and affect the MCU's power control of vehicles. There are various reasons for rotor demagnetization, including high temperature and vibration. The MCU Power HIL test bench built in this paper replaces the real permanent magnet synchronous motor with a motor emulator. The motor simulator can be demagnetized by modifying the upper PMSM software parameters, so as to analyze the MCU response.

The test results of motor demagnetization fault injection are shown in the Figure 4. The test condition is 9000rpm, 50Nm, and the cooling system is 25°C.

![Diagram of MCU power HIL bench](image)

**Figure 3.** Principle of MCU power HIL bench.

**Figure 4.** Demagnetization fault injection test results.

It can be seen that the phase current output fluctuates when the speed remains unchanged after the fault injection, and the MCU still maintains the driving state without any protective action. If the demagnetization is serious, the output torque will be insufficient or even reduced to 0, which may affect driving safety.

## 6. Conclusion

In this paper, the fault injection test method of electric drive system is studied. The fault types and test methods of the MCU are described in detail. The test is based on the power level hardware in the loop test. The results show that it can be applied to the functional safety test of the drive system of EV. At the same time, no matter EV, HEV, FCV or traditional fuel vehicles, there will never be "absolute
Developers and testers need to constantly improve their technical ability and strive to solve 100% unsafe factors in the laboratory.

Acknowledgments
This research was financially supported by National Key R&D Program: ‘Technology Development of Vehicle Motor Drive System Based on Silicon Carbide Technology’, No. 2018YFB0104703

Reference
[1] ISO 26262:2018, "Road vehicles–Functional safety," International Organization for Standardization, second edition, 2018.
[2] Ludovic Pintard, Michel Leeman, and Abdelillah Ymlahi-Ouazzani, Jean-Charles Fabre, Karama Kanoun, and Matthieu Roy, "Using Fault Injection to Verify an AUTOSAR Application According to the ISO 26262", SAE Technical Paper, 2015-01-0272, 2015.
[3] Bin Wang, Kai Ma, Xin Huang, Shan Ren, Fang Wang, System-Level Functional Safety Testing of MCU Based on Power-HIL. Science and Engineering Research Center. Proceedings of 2019 4th International Conference on Automation, Mechanical and Electrical Engineering(AMEE 2019).Science and Engineering Research Center: Science and Engineering Research Center, 2019:8.
[4] GB/T 39086-2020, Functional safety requirements and testing methods for battery management system of electric vehicles
[5] Batchu, SriRamaChandraMurthy., "Functional Safety in Inverter Hardware", SAE Technical Paper, 2016-28-0166, 2016.
[6] Christiaens, S., Ogrzewalla, J., and Pischinger, S., "Functional Safety for Hybrid and Electric Vehicles," SAE Technical Paper, 2012-01-0032, 2012.
[7] Rajiv Kumar, ISO 26262 Hazard and Risk Assessment for Hybrid Powertrain, SAE Technical Paper, 2019-26-0107, 2019.
[8] Zhihong Wu, Ke lu, Yuan Zhu, Xiaojun Lei, and Liqing Duan, "Functional Safety and Secure CAN in Motor Control System Design for Electric Vehicles", SAE Technical Paper, 2017-01-1255, 2017.
[9] Shuai Li, Cheng Chang, and Huaca Zhao, "Functional Safety Development of E-motor Drive System for PHEV", SAE Technical Paper, 2015-01-0261, 2015.
[10] Horst Hammerer, Testing Power Electronics without an E-Motor Eduard Enderle, ATZelektronik worldwide, September 2015, Volume 10, Issue 5, pp 36–41
[11] Martin Heininger, Horst Hammerer, Testing Power Electronics According to ISO 26262, ATZelektronik worldwide, August 2015, Volume 10, Issue 4, pp 26–31
[12] SriRamaChandraMurthy Batchu, “Functional Safety in Inverter Hardware”, SAE Technical Paper, 2016-28-0166