System-Level Functional Safety Testing of MCU Based on Power-HIL

Bin WANG, Kai MA, Xin HUANG, Shan REN and Fang WANG
China Automobile Technology Research Center Co., Ltd, Tianjin, China
*Corresponding author

Keywords: Functional safety, POWER-HIL, MCU, E-motor emulator, Fault injection.

Abstract. “Electrification, interconnection, sharing and intellectualization” are the inevitable trend of the future development of the automobile industry. In recent years, most OEMs begin to attach importance to developing the EV/HEV/PHEVs. Being part of powertrain of the vehicle, the motor control unit 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. Therefore, functional safety (Fusa) related with E/E systems is becoming a key factor in the EV/HEV/PHEVs. According to the ISO26262 standard, this paper develops different test cases and test scenarios for system-level functional safety test & validation of MCU based on Power-level hardware-in-the-loop.

Introduction

For energy saving and global warming prevention, EV/HEV/PHEVs are indeed seen as a promising trade-off between the necessary reductions in emissions and fuel consumption and the ever increasing demand for driving pleasure and vehicle performance[1].

New energy vehicles generally use high-power permanent magnet synchronous motor (PMSM) and motor control unit (MCU). As the core system of the EV/HEV/PHEVs, the e-motor Drive System (PMSM & MCU), is safety related electronic control units (ECU) due to the severity of the accidents/incidents [2].

With the trend of increasing technological complexity, software content, there are increasing risks from systematic failures and random hardware failures. ISO 26262 standard derived from IEC 61508 standard is an automotive specific standard that focuses on functional safety aspects for E/E systems for production vehicles.

Nowadays, many domestic OEMs in China have begun to have specific functional safety requirements for MCU, BMS and TCU, etc. Especially, MCU is qualified for ASIL-C or ASIL-D compliance from various suppliers. The focus of functional safety is on the dangers that can originate in E/E systems on a vehicle level. However, how to verify functional safety is very important. According to the ISO26262 standard, fault injection test, error guessing test, and stress test are highly recommended for the validation of the technical safety requirements [3].

Power-level hardware-in-the-loop (Power-HIL) is a kind of powerful tool of fast evaluation, function development, fault injection and performance-durability testing for MCU. It can be used to do the three-phase short/open circuit, temperature, stall, demagnetization, sensor and mechanical fault tests, etc., which are difficult or dangerous to test by real e-motor and dyno. The purpose of this paper is to develop different test cases and test scenarios for system-level functional safety test & validation of MCU based on Power-level HIL.

What is Power-HIL

Power-HIL is a powerful tool of fast evaluation, function development, fault injection and performance-durability testing for MCU, which is mainly composed of battery simulator, e-motor emulator and related HIL [4,5,6].

1) Virtual motor, parameterized configuration of analog permanent magnet synchronous motor, induction motor and switched reluctance motor;
2) The software and hardware of the MCU are used to test and verify the performance of the power level.
3) Load/durability test and high accelerated life test;
4) Quickly evaluate and test the performance and reliability of the software and hardware of the MCU.
5) Fault injection (e.g. injection of three-phase line short circuit and circuit break, motor temperature, motor blockage, current and torque), overrun, speed overrun, sensor fault, motor impedance change, demagnetization, mechanical fault, etc.

Electromagnetic behavior of the PMSM is described by the following parameters:

\[
\psi_d = L_d \cdot i_d + \psi_{PM} \tag{1}
\]

\[
\psi_q = L_q \cdot i_q \tag{2}
\]

\[
u_d = R_S i_d + L_d \frac{d}{dt} i_d - \omega_L q_i q \tag{3}
\]

\[
u_q = R_S i_q + L_q \frac{d}{dt} i_q + \omega_L d_i d + \psi_{PM} \tag{4}
\]

- \(\psi_d, \psi_q\): flux linkages
- \(\psi_{PM}\): flux of PMSM
- \(p\): number of pole pairs
- \(R_S\): ohmic stator resistance

**MCU Function Safety Analysis**

Functional safety development follows the process of V-model. ISO 26262 deals with entire product life cycle i.e. design and development, verification and validation, production, operation, service and decommissioning. The right side of V-model is the integration, verification and the safety validation. Key steps during product development to achieve functional safety are shown in Figure 2[7].
According to ISO 26262, the development process of functional safety of motor controller, including item definition, Hazard Analysis and Risk Assessment (HARA), safety goal (SG), functional safety concept (FSC), functional safety requirements (FSR), technical safety requirements (TSR), and safety analysis, etc.

Electric traction system is used to provide electric traction to the vehicle and to charge the included battery using the on-board charger. The hazards which are caused by malfunctioning behavior of E/E safety-related systems are the basis for the risk assessment and for the ASIL and safety goal determination step of ISO 26262. The following Figure 3 is system block diagram for MCU with functional safety from Infineon[8].

![Figure 3. System Block diagram for MCU with FuSa.](image)

The table 1. & 2. are some safety goals for e-motor drive system and functional safety requirements for MCU, respectively. The functional safety concept of the MCU is based on the E-Gas 3-layer architecture. The level 1 is the functional level, which contains all control function which is required for operation and controlling of the E-motor. The level 2 is function monitoring, which ensures the correctness of the functional level regarding violation of the defined safety goals. The level 3 is controller monitoring, which ensures that a safe operation of the function monitoring level is possible [9,10,11].

Table 1. Safety goals for e-motor drive system.

<table>
<thead>
<tr>
<th>No</th>
<th>Safety Goal</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG1</td>
<td>Avoid unintended deceleration torque.</td>
<td>ASIL C</td>
</tr>
<tr>
<td>SG2</td>
<td>Avoid unintended acceleration torque.</td>
<td>ASIL C</td>
</tr>
<tr>
<td>SG3</td>
<td>Avoid unintended high voltage.</td>
<td>ASIL B</td>
</tr>
<tr>
<td>SG4</td>
<td>Avoid overheating of e-motor drive system.</td>
<td>ASIL A</td>
</tr>
</tbody>
</table>

Table 2. Functional safety requirements about ASIL C.

<table>
<thead>
<tr>
<th>No</th>
<th>Description of requirements about ASIL C</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSR1</td>
<td>The current sense chain should ensure the correctness of the stator current signal.</td>
</tr>
<tr>
<td>FSR2</td>
<td>Resolver sensing chain shall ensure the correctness of the rotor position and motor speed signal.</td>
</tr>
<tr>
<td>FSR3</td>
<td>CAN sensing chain shall ensure the correctness of the vehicle speed from HCU/VCU.</td>
</tr>
<tr>
<td>FSR4</td>
<td>Inverter's HV connector(s) shall integrate interlock</td>
</tr>
</tbody>
</table>
Test Case Development

The requirements for functional safety system testing of automotive electronic control units are defined in detail in ISO 26262. Table 3 shows methods of integrating test cases. The development of test cases requires the writing of test cases for each FSR corresponding to the TSR, such as FSR1: The current sense chain should ensure the correctness of the stator current signal. Corresponding TSR1: In order to check the plausibility of the motor phase current detection chain, all three phase currents should be independently tested. TSR2: Range check—after the start mode is completed and before the start mode is turned off, the three-phase current sense chain should be detected for out of range failure. TSR3: plausibility check—the plausibility check of the three-phase current sense chain should be carried out, that is, if the sum of the actual currents of the three phases exceeds the maximum allowable error, the plausibility check fault should be detected. For different technical TSR, the following methods are usually used to generate test cases.

Table 3. Method of integrating test cases.

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Analysis of requirements</td>
<td>++</td>
</tr>
<tr>
<td>1b Analysis of external and internal interfaces</td>
<td>+</td>
</tr>
<tr>
<td>1c Generation and analysis of equivalence classes for hardware-software integration</td>
<td>+</td>
</tr>
<tr>
<td>1d Analysis of boundary values</td>
<td>+</td>
</tr>
<tr>
<td>1e Error guessing based on knowledge or experience</td>
<td>+</td>
</tr>
<tr>
<td>1f Analysis of functional dependencies</td>
<td>+</td>
</tr>
<tr>
<td>1g Analysis of common limit conditions, sequences, and sources of dependent failures, see ISO 26262-9:2018, Clause 7</td>
<td>+</td>
</tr>
<tr>
<td>1h Analysis of environmental conditions and operational use cases</td>
<td>+</td>
</tr>
<tr>
<td>1i Analysis of field experience</td>
<td>+</td>
</tr>
</tbody>
</table>

— “++” indicates that the method is highly recommended for the identified ASIL;
— “+” indicates that the method is recommended for the identified ASIL;

Test Results and Analysis

The safety state of the motor controller generally includes two control modes related to the inverter, one is a freewheel (FW) and the other is an active short circuit (ASC) [12]. Both safety modes ensure that the electronic control system can safely release the kinetic energy of the vehicle without causing damage to the inside of the vehicle when the vehicle is out of control. The coasting mode generally ensures that the inverter of the power system works in the state of stopping the inverter, that is, for the classical three-phase six-bridge structure, all the IGBTs are turned off, so that the motor works as if it is in an open state, as shown in the following Figure4 [12].

![Figure 4. Inverter status in coasting mode.](image)

The active short circuit mode generally makes the high side IGBTs or the low side IGBTs of the motor inverter work in the closed state, and the remaining side IGBTs works in the off state, so that the motor works in the short circuit state, as shown in the following Figure5 & Figure6.
Normally, the driving motor system operating in the coasting mode, the output torque of the motor is zero, the motor and the power supply (battery pack) have no energy flow when the motor rotates at a low speed, the motor shaft is free to slide, and the friction is gradually stopped. However, when the PMSM is at a high speed, high back EMF is generated. In the meantime, the inverter becomes a rectifier, and the motor charges the battery. If the charging current is too large, or the battery SOC is too high, the EMF may cause the battery to be out of control.

General speaking, when the motor enters the safe state at high speed, it will enter the ASC state, and make the motor work in the short circuit state. Therefore, the braking torque of the motor will gradually reduce the motor speed to zero. However, it is necessary to ensure that the active short-circuit current of the motor does not cause thermal runaway of the battery system within a specified time. Fortunately, it is easy to meet this requirement. The next consideration is when the electric drive system will be activated into safe mode. Generally, according to HARA analysis and scenario analysis, safety goals will be obtained, FSR will be obtained from SG, and technical security requirements will be obtained. For specific TSR and export test cases, specific test cases can often be obtained.

The test is generally used for fault injection, stress testing, limit testing, and the like. This paper lists the test results and analysis process of different types of faults in some electric drive systems:

**Speed Sensor Failure**

The motor speed sensor generally uses a resolver. In the drive motor system, the resolver is mounted on the rear end cover of the motor, the output signal is analog, and it is highly susceptible to high-frequency current interference. The resolver receives an error signal, which may result in incorrect decoding due to vector control of the speed. The strong dependence of the signal, the wrong speed signal can easily cause the control torque to oscillate, and even the torque reversal occurs, which is not allowed to occur. The way to avoid this situation is that the functional safety strategy needs to be effectively implemented. The signal loss occurs in the following diagram. The yellow, red, and blue lines in the Figure 7 represent the motor line voltage, the resolver SIN signal, and the motor phase current. The test condition is that the motor speed is 6000 rpm, and output torque is 100 N.m, fault injection of resolver may lead to motor damage. The test result is that the MCU enters the ASC state within 300 us after the fault occurs.
Motor Temperature Signal is Abnormal

Abnormal motor temperature signal generally indicates that the measured motor temperature is in an unreasonable interval or an unreasonable change interval. For example, if the motor over temperature generally indicates that the motor temperature is higher than 150 °C, the motor temperature is too high, which may cause thermal loss of the motor or insulation failure. Loss of magnetism can cause a sudden drop or even complete loss of motor torque. Additionally, insulation failure can cause a short circuit in the motor or a short circuit in a high voltage system. Unreasonable changes in motor temperature, such as abnormal motor temperature jumps, the reliability of the temperature acquisition value is greatly reduced, affecting the decision-making result of the electric drive on the output torque, and the result is to interfere with the driver's manipulation of the vehicle. Figure 8, is electronically controlled response after abnormal motor temperature. The blue line and green line indicate DC current, and AC current, respectively. And the orange line indicates the DC bus voltage. It can be seen that after the motor temperature abnormality occurs at high speed, the electric control enters the ASC mode, and there is no energy exchange between the battery end and the motor end. Figure 9 is current runaway after motor loss of magnetism.

As shown in the Figure 10 below, the motor speed does not change during the test. When the motor overheats at low speed, the motor torque becomes zero, no phase current is output, and the coasting mode is entered. The red and blue lines represent the q-axis and d-axis currents, respectively, and the black lines represent the electromagnetic torque.
Figure 10. The motor overheats at low speed and then returns to normal temperature.

At the same time, in Figure 10, it can be seen that the power reduction occurs at 25s~35s, which is also the self-protection strategy of the system when the motor temperature is relatively high.

Summary

In this paper, the Power-HIL is a e-motor emulator (EME), which has powerful functions of on-line modification of e-motor parameters and MCU fault injection. It can change such parameters as motor flux linkage parameters under the working state of the motor controller, and inject motor resolver faults, phase-to-phase short circuit/open circuit, temperature sensor faults, and rotor faults, etc. in real time. This kind of test items are generally difficult to complete on the traditional dyno bench, so the power-HIL equipment which actually expands the dimension of electric control test and coverage of test regulations, and is an effective test method for functional safety test verification of the motor controller.

Acknowledgement

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


