Development of the safety diagnosis system for VCU of pure electric vehicle

Zhao Yongqiang\textsuperscript{1}, Zhao kaicheng\textsuperscript{2}, Li Chang\textsuperscript{2} and Li Xiang\textsuperscript{2}

\textsuperscript{1} College of Automotive Engineering, Jilin University, 142 Renmin Street, Changchun, China
\textsuperscript{2} China FAW Group Corporation, 1 New Hongqi Street, Changchun, China
zhaoyongqiang1@faw.com.cn, zhaokaicheng@faw.com.cn, lichang@faw.com.cn, lixiang10@faw.com.cn

Abstract. Perfect safety monitoring system is the guarantee of vehicle safety. In this paper, through functional safety analysis and FMEA analysis, a pure electric vehicle safety monitoring system is developed, which can diagnose possible faults in real time, monitor software operation problems, and take appropriate fault handling strategies and safety mechanisms to ensure the safe and reliable operation of vehicles.

1. Preface
In recent years, with the rise of new energy vehicles, especially after the popularization of pure electric vehicles, the four-wheel drive system is not only the original mechanical structure, which is composed of multiple parts, transfer case, transmission shaft and sometimes differential lock [1]. In the electric four-wheel drive system, especially in the pure electric vehicle, the four-wheel drive structure is simpler, and the transmission mechanical structure can be avoided. In electric four-wheel drive, a driving motor is a power source. Although the mechanical structure of the electric four-wheel drive vehicle is much simpler, with fewer parts, it does not mean that the electric four-wheel drive has no disadvantages. Compared with the traditional mechanical four-wheel drive, the stability and reliability of the electric four-wheel drive electrical system have disadvantages under various working conditions. [2] If any part of the system fails, these failures may cause problems in the operation of the whole system. The general failure causes the performance of the vehicle to decline or fail to start, and the serious failure causes the major safety accident [3]. This requires that in the process of pure electric vehicle operation, the operation status should be monitored in time, the operation status should be judged correctly, the faults should be found as soon as possible and the corresponding measures should be taken, so as to ensure its high performance and reliability, improve operation efficiency and prolong service life of automobile [4]. Therefore, it is necessary to develop an efficient and suitable safety diagnosis system for pure electric vehicles.

2. Vehicle safety diagnosis and analysis

2.1. Power system structure of pure electric vehicle
The pure electric vehicle power system studied in this paper is a dual motor system, whose structure is shown in Figure 1. It is mainly composed of motors, reducer, power battery, charger, electronic stability system and corresponding control units. The motor drive system is a full-time four-wheel
drive system, with a set of motor drive system arranged at the front axle and a set of motor drive system arranged at the rear axle. The torque between axles can be dynamically distributed by VCU, but the left and right wheels on one axle cannot be controlled by independent torque distribution. In view of the safety of electric system, the safety strategies are formulated through the analysis of FMEA and functional safety.

![Figure 1. Power system structure of pure electric vehicle.](image)

2.2. FMEA analysis
The failure mode and effect analyze of electronic control system can be done in two sides.

First, analyze the failure mode and effect of the electronic control system based on the function. All the functions should be analyzed in this way, the more we know about the system, the deeper analyze we can do. Some complex electronic control systems often contain multiple levels of functions, and failure analysis should be carried out on the functional requirements of each level. It should be noticed that in addition to the basic functional requirements, the serviceability and assemblability requirements of electronic control system should also be analyzed. Taking VCU for example, the range to analysis is shown in Figure 2, including sensors, actuators connect to VCU, and signals related to power system, high voltage system, chassis system and comfort system which interact with VCU.
Second, analyze the historical failure. The case of historical failure can come from two aspects. One is the failure of the system itself, which has happened before, as shown in Figure 3. The other is the failure of the corresponding electric control system of other vehicles. In the process of FMEA analysis, the failure causes and preventive and detection measures of the above two historical failures should be fully evaluated to ensure that the historical failures will not occur again.

Figure 2. FMEA Boundary Diagram.

According to the risk assessment of the two aspects, the corresponding measures are formulated. As shown in Figure 4, that we take one function requirement for example for lack of space.

Figure 3. History Failure Analyze.

According to the risk assessment of the two aspects, the corresponding measures are formulated. As shown in Figure 4, that we take one function requirement for example for lack of space.
2.3. Functional safety analysis

After FMEA analysis of the system, the complete reliability of the electronic control system cannot be guaranteed. Based on ISO26262 functional safety standard, this paper continues to analyze the vehicle functional safety.

According to the ISO26262 functional safety standard, firstly, determine the analysis object of the electronic control system, such as FMEA analysis, including sensors, actuators, power system signals, high-pressure system signals, chassis system signals, etc.

Through the FMEA failure analysis and brainstorming in front, find out the hazards that directly or indirectly lead to personal injury. For each hazard, according to the ISO26262, evaluate the severity (S), probability of occurrence (E), and degree of control (C) under various operation conditions, and complete the risk assessment. Obtain safety objectives and ASIL level [5]. Due to space limitation, the analysis processes are not introduced, and the analysis results are directly given in this paper, as shown in Table 1. Develop corresponding functional safety requirements for each functional safety goal, as shown in Figure 5.

Table 1. Safety Goals of VCU.

| No.  | Safety Goal                                                                 | ASIL |
|------|-----------------------------------------------------------------------------|------|
| SG01 | The unintentional acceleration or deceleration controlled via VCU must be avoided | C    |
| SG02 | When accelerating from stand, the driving direction of the vehicle must be consistent with the driver's request | B    |
| SG03 | The gear P must not be deactivated if there is no driver request             | C    |
| SG04 | Fire must be avoided                                                         | C    |
| SG05 | High voltage electric shock controlled via VCU must be avoided               | C    |
The unintentional acceleration or deceleration controlled via VCU must be avoided.

FSR_01.01:
The signal of accelerator pedal position shall be correctly available with tolerance of 2%.

FSR_01.02.01:
The signal of accelerator pedal position 1 shall be correctly available with tolerance of 2%.

FSR_01.02.02:
The signal of accelerator pedal position 2 shall be correctly available with tolerance of 2%.

FSR_01.02.03:
The speed and direction from ESP shall be correctly available with tolerance of 2km/h.

FSR_01.03.01.01:
The signal of brake pedal 1 shall be correctly available.

FSR_01.03.01.02:
The signal of brake pedal 2 shall be correctly available.

FSR_01.03.02.01:
The signal of main cylinder pressure shall be correctly available.

FSR_01.05.01.01:
When ACC is active, the VCU torque request shall be in accordance with ACC torque request.

FSR_01.05.02.01:
When CRBS is active, the VCU torque request shall be in accordance with CRBS torque request.

FSR_01.06:
The VCU torque request shall avoid causing unintentional acceleration or deceleration.

3. Safety measure

Through FMEA and functional safety analysis, a three-layer safety monitoring mechanism is developed. The basic structure is shown in Figure 6.

The three layer safety concept represents the state of the art method and comprises:

1. **L1**: diagnostics for sensors and actuators to ensure reliable input information and execution of commanded actions.

2. **L2 monitoring**: process monitoring functions based on redundant backwards calculation from actuator status to be compared with redundant driver request.

3. **L2’ diagnostics**: all input for process monitoring must be redundantly diagnosed in L2’.

4. **L3 processor monitoring**: various tests to ensure proper operation of the controller hosting the L2’.

**Figure 5.** Functional safety requirements analysis.

**Figure 6.** The three layer safety concept.
3.1. The first layer: fault diagnosis and treatment
The possible faults and safety problems of pure electric vehicle power system can be divided into three categories: sensor or actuator faults, assembly faults, and communication faults. Any one of these faults is the hidden danger of pure electric vehicle, which needs timely diagnosis and treatment. Table 2 gives a detailed description of three types of pure electric power system faults and hazards.

| Table 2. Power system fault and hazard analysis of pure electric vehicle |
|---------------------------------------------------------------|
| **Fault category** | **Fault name** | **Fault phenomena and hazards** |
| Sensor or actuator faults | Accelerator pedal failure | Accelerator pedal sensor fault, accelerator pedal signal inaccurate. |
| | Brake pedal failure | Brake pedal sensor fault, brake signal inaccurate. |
| | Water pump failure | Water pump line fault; water pump fault, water pump cannot work. |
| | PTC failure | PTC line fault, PTC fault, PTC cannot work or cannot stop working. |
| | Water valve failure | Water valve line fault, water valve body fault. |
| Assembly faults | Battery system failure | Sensor fault, power supply fault, over temperature fault, over voltage fault, single high voltage fault, high voltage insulation fault, etc. Leakage of electricity, fire, explosion, failure to apply high voltage. |
| | Motor system fault | Sensor fault, power supply fault, over temperature fault, over speed fault, over / under voltage fault, torque abnormality, etc. Limit output torque, unable to drive. |
| | Shift signal failure | Sensor fault, stuck fault, over / under voltage fault, vehicle cannot shift. |
| | ESC system failure | ABS Error, ESP Error, ASR Error, EPB Error, YRS Error. Body stability affected. |
| Communication faults | Communication faults | Checksum fault, liver counter fault, time out fault, note lost, Invalid failure of key signal, Bus off. |

According to the above analysis, taking PTC fault as an example, VCU controls PTC operation through PWM signal. For PTC working failure, it can be divided into:

1. Hard wire failure: short circuit to ground, short circuit to electricity, open circuit.
2. PTC failure, including high voltage component failure and low voltage component failure.

If PTC is working all the time, the temperature will continue to rise, causing fire and serious harm. At this time, there are two measures for PTC to stop working. One is to disconnect the high voltage, the other is to disconnect the low voltage power supply of PTC, which only affects the battery heating, and the vehicle can still be driven, which has a small impact compared with the first measure. Therefore, in the product design stage, the PTC low-voltage power supply is arranged behind the VCU controllable relay, as shown in Figure 7.
PTC always working, VCU controls the relay to cut off the low-voltage power supply of PTC to ensure the safety of the whole vehicle.

![PTC control circuit](image)

**Figure 7.** PTC control circuit.

### 3.2. Second layer: function monitoring

The second layer mainly monitors the basic functions of the first layer according to the functional safety requirements. According to the functional safety goals, it mainly includes torque monitoring, temperature monitoring, command set inspection, etc. When abnormal conditions are found, develop troubleshooting and remedial measures.

Taking torque monitoring as an example, its source is a functional safety requirement, as shown in FSR_01.06.02 of Figure 5. The following is a description of FSR_01.06.02.

#### Table 3. FSR_01.06.02

| Parameter                              | Description                                                                                           |
|----------------------------------------|-------------------------------------------------------------------------------------------------------|
| ASIL                                    | C(C)                                                                                                  |
| Allocation                              | VCU                                                                                                   |
| Fault tolerant time interval            | 500ms                                                                                                 |
| Warning operation                       | The driver shall be warned by a red warning light. The driver shall immediately drive the car to a safe place and stop it. Further driving with this degradation is not possible. |
| Degraded operation                      | DO_15: Degraded operation – torque calculation limited by a safety function. This degraded operation shall be activated if ERR_19 (accelerating torque request too high) or ERR_20 (recuperating torque request too high) is detected (see Figure 10). Allocation of related timers: tq_lim_rec_int = [2 s] tq_lim_int = [60 s] |

#### 3.2.1. DO_15: Degraded operation – torque calculation limited by a safety function.

The torque request shall be calculated by a complex normal function and monitored by a less complex (and thus easier to implement in a corresponding ASIL) safety mechanism (SM). The purpose of the safety mechanism is to define boundaries for the normal function, in which the calculation shall stay in the current driving situation. If the calculation from the normal function violates the calculation of the safety function, then the value calculated by the safety function shall substitute the value calculated by the normal function (see Figure 8 and Figure 9).
3.2.2. Recovery. This degraded operation shall only be acceptable for a short time (recovery time interval). The system shall recover from this degraded operation, if the normal function calculation returns to the safe margin given by the SM within the defined recovery time interval (see Figure 8). If the error in the calculation remains over the recovery time limit, no recovery is possible and the VCU shall transfer to the safe state (VCU outputs 0 Nm) within the degraded operation time interval (see Figure 9).

3.2.3. Triggering events. This degraded operation DO_15: Degraded operation – torque calculation limited by a safety function shall be activated in the following cases:

- Failure of the torque calculation function (“ERR_19: Acceleration too high” OR “ERR_20: Deceleration too high”).

![Figure 8. Torque calculation error – recovery from degraded operation DO_15.](image)

![Figure 9. Torque calculation error – transition to the safe state.](image)
Torque calculated by normal function
Entry:
delete timer tq_lim_rec_int
delete timer tq_lim_int

DO_15: Degraded operation-torque calculation limited by a safety function
Recovery possible
Entry:
Start timer tq_lim_rec_int
Start timer tq_lim_int

Timer tq_lim_rec_int

DO_15: Degraded operation-torque calculation limited by a safety function
Recovery not possible

Timer tq_lim_int

Safe state-no torque requested by VCU

Figure 10. Safety mechanism for torque calculation function.

3.3. Third layer: Monitoring the health status of functional controllers and monitoring microcontrollers
For the functional controllers and the monitoring Microcontrollers, we should always monitor their health status ensure the normal operation of L1 and L2 layers. The main monitoring contents are shown in Figure 11.

Figure 11. Processor monitoring in function controller and monitoring unit.

Processor monitoring level 3 in function controller:
1. RAM-Check: Complete RAM-Check in the initial phase.
2. ROM-Check: Complete ROM-Check in the background.
3. ROM-Check Level 2: Cyclic Check all xx seconds.
4. RAM-Check Level 2: redundant storage of all internal values.
5. Verification of functional behavior in the pre-phase.
6. Verification of the right SW-version.
7. Monitoring of process flow.
8. Permanent data communication between Monitoring Controller to screening the communication.

Processor monitoring level 3 inheres monitoring unit:
(1) RAM-Check: Complete RAM-Check in the initial phase.
(2) ROM-Check: Complete ROM-Check in the background.
(3) Verification of functional behavior in the pre-phase.
(4) Verification of the right SW-version.
(5) Permanent data communication between Main Controller to screening the communication.

If the test fails, enter the failure mode. According to the failure handling measures, the vehicle enters the safe state.

4. Offline and after sales Safety Design
Under the normal mode of vehicle, the vehicle safety can be guaranteed through the above safety mechanism and fault handling measures. But in the process of production and sales, the high-voltage safety of electric vehicles is also crucial.

In the production line, in order to prevent electric shock, high voltage power on should be prohibited. Through the diagnosis service, add the offline mode, in which the vehicle cannot be powered on with high voltage. In the production process of the factory, the vehicle always keeps the offline mode, and after the offline, the vehicle is configured to the normal mode. Similarly, we define the maintenance mode and forbid high voltage power on, during maintenance at the maintenance station, the vehicle is changed to the maintenance mode to prevent the maintenance personnel from electric shock.

With the development of OTA technology, software updates frequently. If the high voltage is powered on, writing the software directly at this time may cause the battery to directly disconnect the relay, resulting in load rejection. After the software is written, the main positive relay and the main negative relay are directly closed, without precharge process, which may cause the relay to stick. Therefore, a safety mechanism should be developed. When the vehicle is in the state of high-voltage power on, the first step is to power off through the diagnosis service, otherwise the VCU should not respond to the write service.

By adding offline mode, maintenance mode, and swipe service limit, the vehicle and personnel are always in a safe state.

5. Conclusion
In this paper, through the safety analysis of pure electric vehicle power system, identify the possible faults and hazards, so as to design a perfect safety monitoring system, and formulate a reasonable fault diagnosis and treatment strategy. Through HIL test and road test verification, the safety diagnosis system of pure electric vehicle developed can identify vehicle faults in time and effectively, and adopt safe and effective fault handling strategies to ensure the safe and reliable operation of vehicles.

References
[1] Bian yaozhang. New energy technology of automobile [M]. Beijing: China Communications Press, 2003.
[2] Dou Yu. Study on motor fault tolerance control method of wheels drive vehicle[D]. Harbin: Harbin Institute of Technology, 2018.
[3] Zhang Peng, Zhang Junhong, Zhang Lin, Zhang Yan. Functional development of hybrid vehicle fault diagnosis [J]. Shanghai Auto, 2011, 01:16-19.
[4] Chen Qingquan, sun Fengchun, Zhu Jiaguang. Modern electric vehicle technology [M]. Beijing: Beijing Institute of Technology Press, 2002.
[5] ISO.: Road vehicles — Functional safety — Part 1-10. ISO/DIS 26262 (2011).