Computer Life (CPL) ISSN: 1819-4818
DELIVERING QUALITY SCIENCE TO THE WORLD

Research and Development of High Pressure Common Rail ECU Based on Functional Safety Standard

Jian Xiong [a], Hong Gu [b, *]

School of Control Science and Engineering, Dalian University of Technology, Dalian 600015, China

[a]cd_xj@163.com, [b]guh@dlut.edu.cn

Abstract: The hardware circuits and monitoring strategies of the monitoring unit for high pressure common rail ECU were designed and developed, which mainly focused on query and response monitoring strategy of the three-level monitoring architecture. The model of monitoring strategy was built and simulated by using Matlab/Simulink tool, the codes were generated automatically by using Real-Time Workshop tool, the generated codes were optimized by using the tool chain and development process according to ISO 26262, and finally the test verification was conducted on a high pressure common rail diesel engine. The results showed that the monitoring unit could effectively inspect the fault of CPU and make the decision in time. Accordingly, the stability of high pressure common rail system improved greatly.

Keywords: Functional safety, Common rail system, Electronic control unit, System monitor

1. INTRODUCTION

With the development of automotive electronics technology, The wide range of electronic products. And the complexity is increasing, System failure, Components such as failure of functional safety The problem is getting worse[1].Automotive electronics industry so the latest road Vehicle Functional Safety International Standards 26262.ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of electrical and/or electronic (E/E) systems within road vehicles. It adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

Safety is one of the key issues of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering. Development and integration of these functionalities will strengthen the need for safe system development processes and the need to provide evidence that all reasonable system safety objectives are satisfied.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and

processes. System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process. Although ISO 26262 is concerned with functional safety of E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered. ISO 26262:

a) provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases; b) provides an automotive-specific risk-based approach to determine integrity levels Automotive Safety Integrity Levels (ASIL)];

c). Uses ASILs to specify applicable requirements of ISO 26262 so as to avoid unreasonable residual risk;

d). Provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;

e). Provides requirements for relations with suppliers.

Functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and by the management processes.

Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses the safety-related aspects of development activities and work products.

Functional safety standard (ISO26262) is based upon a V-model as a reference process model for the different phases of product development. ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities. Systems and their components released for production, or systems and their components already under development prior to the publication date of ISO 26262, are exempted from the scope. For further development or alterations based on systems and their components released for production prior to the publication of ISO 26262, only the modifications will be developed in accordance with ISO 26262. ISO 26262 addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of E/E safety-related systems. ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

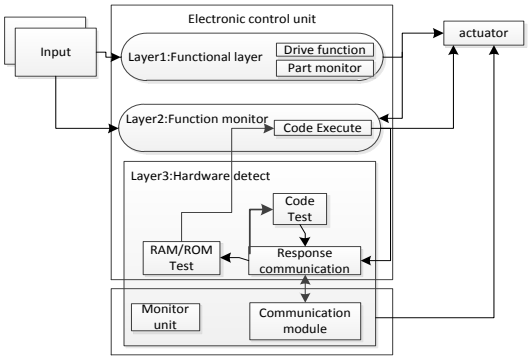
The hardware signal requirements in the IS O 26262 standard include the key Redundancy design of sensor signals, independent shutdown of critical output signals Path, the main control microprocessor and other Sichuan. This study draws lessons from Math Works introduced ISO 26262 standard base the model of the reference development process, the main control microprocessor to achieve monitoring ECU development.

2. HIGH-PRESSURE COMMON RAIL SYSTEM MONITORING FUNCTION ARCHITECTURE

Based on the requirements of safety monitoring of diesel common rail system, set Took a three-tier monitoring structure (see Figure 1), through the monitoring content Layered to meet the requirements of fail-safe at the hardware / software level.

2.1 hardware failure safety strategy

High-pressure common rail ECU (Electronic Control Unit) used Two independent CPU, the main CPU (Function Chip, below Referred to as FC) to complete the input signal acquisition check, the output signal control System, data memory access and other functions, monitoring CPU (Monitoring module, hereinafter referred to as MM) to complete the running status of the FC Real-time monitoring, diagnosis of its own memory, diagnostics of drive-level shutdown paths Off and control functions. Two CPU monitor each other, any one problem, can trigger the reset of the entire system and turn off the output stage, Achieve fail-safe.



2.2 Software Failure Security Policy

The software architecture is divided into three layers according to the basic principle of monitoring functions.

1) The first level includes the realization of the basic control functions of high-pressure common-rail engines, such as fuel injection timing and fuel quantity control, and common rail pressure control. The diagnosis and processing of the input signal is also part of the monitoring functions, including the accelerator pedal signal, crankshaft and camshaft signals, coolant temperature signal. Once the above signal fails, the system will perform a homecoming function.

2) The second level mainly implements monitoring of engine output torque. According to the relevant parameters in the first layer to calculate the required torque, the actual output torque, etc., when the actual output torque is greater than the safety limit torque, the monitoring function triggers an error response, limiting the injector and the fuel pump output, so that limit torque output to ensure the vehicle is in a safe state.

3) The third layer includes the check of the FC hardware environment, the self-diagnosis of the monitoring unit, and the monitoring strategy between the two CPUs. The hardware environment check includes real-time communication between FC's program flow and instruction test, memory and timer monitoring, A/D analog-to-digital conversion module, and communication module

monitoring, such as MM and FC. When the fault occurs and the accumulated number of times is reached, the shutdown will be performed. Output and reset operations ensure the safety of the entire high pressure common rail system.

3. MONITORING FUNCTION HARDWARE DESIGN

3.1 Overall hardware framework

The monitoring function hardware schematic is shown in Fig. 2. It mainly includes SPI communication circuit (FC' is master, MM is slaver) and reset shutdown circuit. FC' and MM use XC'.2785 and XC'.866 chips, respectively. The hardware design mainly realizes the following functions: 1) The FC and MM can reset each other; 2) The FC and MM can communicate with each other through the SPI interface in real time; FC' sends the monitoring result to the MM; 3) The output level Shutdown and enable control. FC' and MM both have their own SPI module, only need to configure the chip, and then connect according to the pins shown in Figure 2.

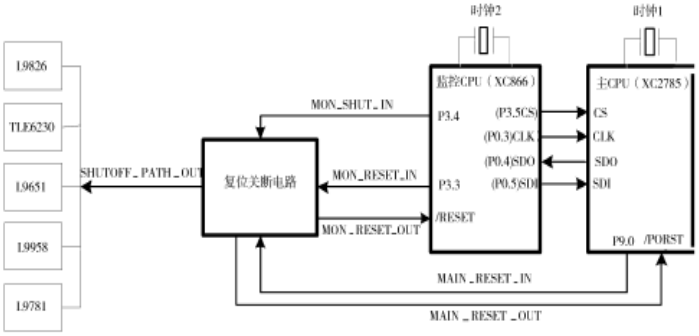


Figure 2 Hardware Features of Monitoring Functions

3.2 Mutual reset and output stage shutdown circuit

Mutual reset and output stage shutdown circuit In order to achieve safety monitoring, ensure that the monitoring unit responds to the error correctly and timely, monitoring unit design should consider the reset and shutdown requirements. The design of the reset shutdown circuit is shown in Figure 3.

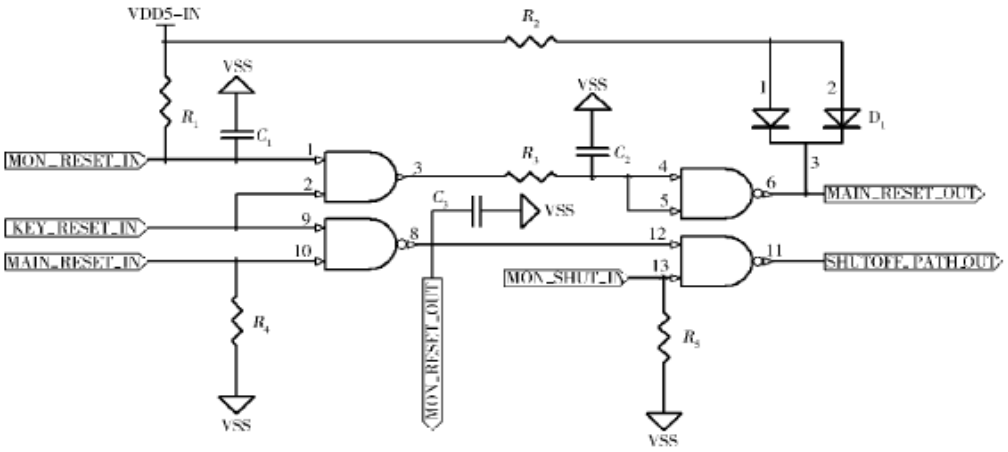


Figure 3 reset shutdown circuit

The circuit can achieve the following functions:

1) The main CPU can reset the monitoring CPU. When monitoring CPU operating errors, MAIN RESET IN will be set low and MON RESET OUT will also be set accordingly, triggering the monitoring CPU reset.

2) The monitoring CPU can reset the main CPU. When the monitoring chip detects a failure, the monitoring CPU sets MON RESET Ilk low.

The MAIN RESET OUT connected to the main CPU reset pin is also pulled low, triggering the main CPU reset.

3) The monitoring chip can independently turn off the output stage. When a fault is detected, the monitoring CPU de-asserts the UT SHUT UT pin so that SHUTOFF PATH is pulled low and UT finally turns off all output stages connected to it.

4. MONITORING UNIT SOFTWARE DESIGN

4.1 monitoring unit self-diagnosis function

Because MM monitoring of FC depends on its own running loop environment, so it is necessary to check its own hardware environment (RAM/ROM Etc.) Self-diagnosis content includes:

1) During the initialization phase or per After the reset operation, MM will execute a complete ROM area Check, by checking the current Checksum (checksum) and records Checksum match, in order to determine whether the ROM is normal;

2) In each communication process, it is necessary to enter the used RAM area. Check once. By performing read and write operations on it, if positive true read and write indicates RAM is normal, otherwise reset operation will be performed and check again.

4.2 Monitoring unit inquiry/response strategy

Each monitoring cycle, the MM sends 16 different queries via a virtual random signal generator (algorithm implementation), transfers to the FC' through the SPI port, waits for the FC' to make a clear response to each inquiry, inquiry/response Communication monitoring is shown in Figure 4.

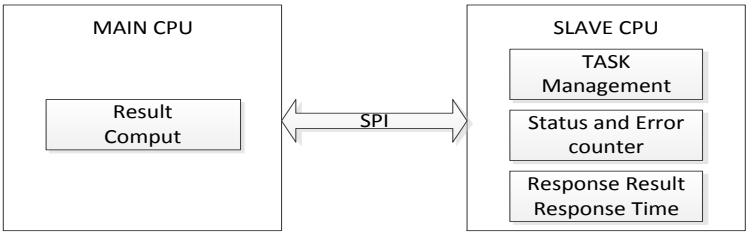


Figure 4 Illustration of pass response communication monitoring

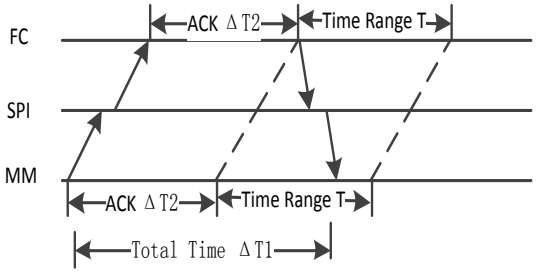


Figure 5 response communication timing diagram

The MM sends a random inquiry to the FL and starts the timer T1. When the FL reception is completed, the timer T2 is started immediately, and then the answer result is calculated and sent according to the inquiry. When the transmission is finished, the T2 stops counting, and the time difference of T2 is T: is the response time. When the MM reception response is completed, T1 stops timing and sends a reception interrupt request. At this time, the time difference ΔT of T1 is the entire communication time. Its response communication timing chart is shown in Figure 5.

The response verification includes the verification of the response time and results, and the inquiry/response monitoring flow chart is shown in Figure 6. When ΔT2<= ΔT1<=ΔT2+T, it means that the response time is reasonable (On time). When ΔTl < T2, it means that the time is too early (Too early). When ΔT1> ΔT2 +T, it means that the time is too short. Too late; indicates that the response is True when the response is consistent with the expected rule, and False otherwise.

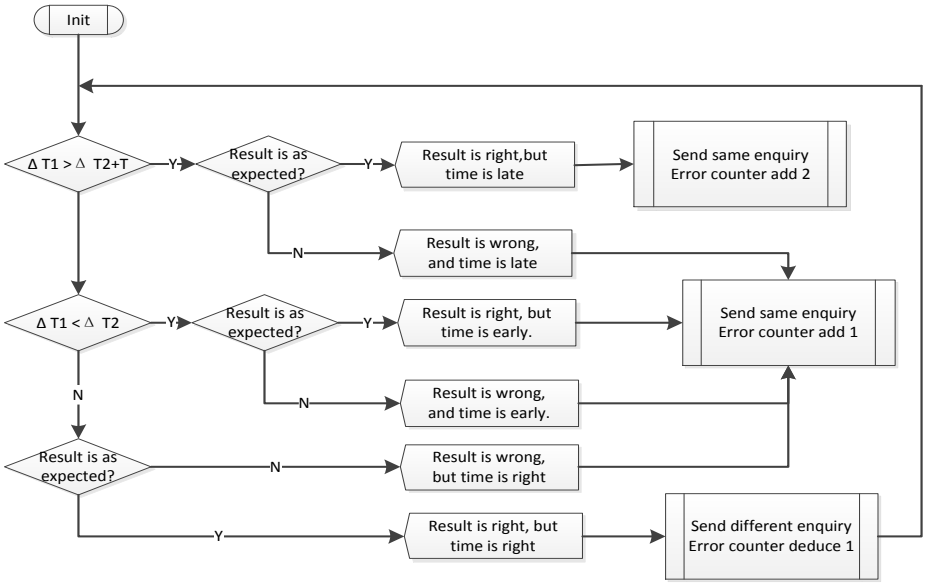


Figure 6 Flow chart of inquiry/response control

4.3 Error response mechanism

The monitoring chip needs a reasonable error response mechanism while implementing the monitoring function. In the MM software solution, three error response mechanisms are defined:

1) SPI communication error. During the initialization phase, if MM detects. The SPI signal level is incorrect, it will be initialized again if the level is still error triggers the error flag and stops at the boot loader. Active boot process) and report an error.

2) ROM/RAM error. Initialization stage, if MM checks If a fault in the ROM area or RAM area is detected, the corresponding error flag is triggered position and perform a reset operation.

3) Response verification error. If MM is within the specified period of time no response was received, or the received response was wrong, MM then send the same query request and error counter the value of MoCCom_ctErrMM increases. When the error counter exceeds the specified value, the MM shuts down the output stage and performs a reset operation on the FC.

5. CONCLUSION

The safe operation of the high pressure common rail ECU is the core of the normal operation of the entire engine. This study has designed the monitoring unit for the high pressure common rail ECU by using the tool chain provided by the Matlab/Simulink and the reference development process for IS 26262 Road Vehicle Functional Safety Standards. A three-layers monitoring system architecture was proposed. Finally, model simulation and experimental demonstration were completed.

The research results show that the monitoring unit can accurately identify the inquiry/response communication failures of the main CPU and perform the set safety objectives under different operating conditions, which greatly improve the safety of the entire high pressure common rail system and realizes the expected functions goal. The development process of the inquiry/response communication monitoring strategy can be used as a reference and can be used as a reference for the development of the entire monitoring unit. In addition, the hardware circuit as a basis for the realization of monitoring functions fully meets the design requirements and has universality.

REFERENCES

[1] International standard ISO 26262 Road vehicles — Functional safety —Part 1:Vocabulary

[2] International standard ISO 26262 Road vehicles — Functional safety —Part 2: Management of functional safety

[3] International standard ISO 26262 Road vehicles — Functional safety —Part 3: Concept phase

[4] .International standard ISO 26262 Road vehicles — Functional safety —Part 4: Product development at the system level

[5] International standard ISO 26262 Road vehicles — Functional safety —Part5 : Product development at the hardware level

[6] International standard ISO 26262 Road vehicles — Functional safety —Part : Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

[7] Ziqing Zhai.Achieving ASIL D for Microcontroller in Safety-Critical Drive-by-Wire System[c].SAE Paper 2009—0 O759.

[8] Zhao Junpeng. Electronically Controlled Diesel Engine Torque Monitoring Based on ISO 26262 Standard Strategy Research IJ]. Mechanical and Electrical Engineering, 2014(3): 376-372.

[9] Conrad M.Software Tool Qualification According to ISO 26262[C].SAE Paper 2011-01—1005.

[10] Conrad M，Munier P，Rauch F.Qualifying Software Tools According to ISO26262[C] MBEES，2010：117-128.