Functional Safety Concept Design of Pure Electric Vehicle Controller Based on Iso26262

Jingbo Wu, Jiakai Liu

Henan University of Science and Technology, Luoyang, Henan 471000, China

Keywords: Functional safety, Iso26262, Vehicle controller, Conceptual design

Abstract: Aiming at the potential safety hazard of the controller of EV,based on the advantages of iso26262road vehicle functional safety standard in dealing with the safety problems of vehicle mounted electronic and electrical system,the functional safety concept design of EV controller is completed to reduce the residual risk of vehicle controller and improve the operation stability and safety of EV.

1. Introduction

In the face of the more complex electrical system compared with the traditional automobile,the Automotive OEMs can only realize the basic functions,and the safety related problems have not been paid attention to and solved.How to ensure the safe operation of the pure electric vehicle electrical system systematically and normatively,and how to guarantee the personal and property safety of the drivers and passengers,is an urgent task for the Automotive OEMs .The implementation of iso26262 can make the on-board electrical system avoid potential risks in the product design stage,and reduce the recall and complaint events caused by safety problems.

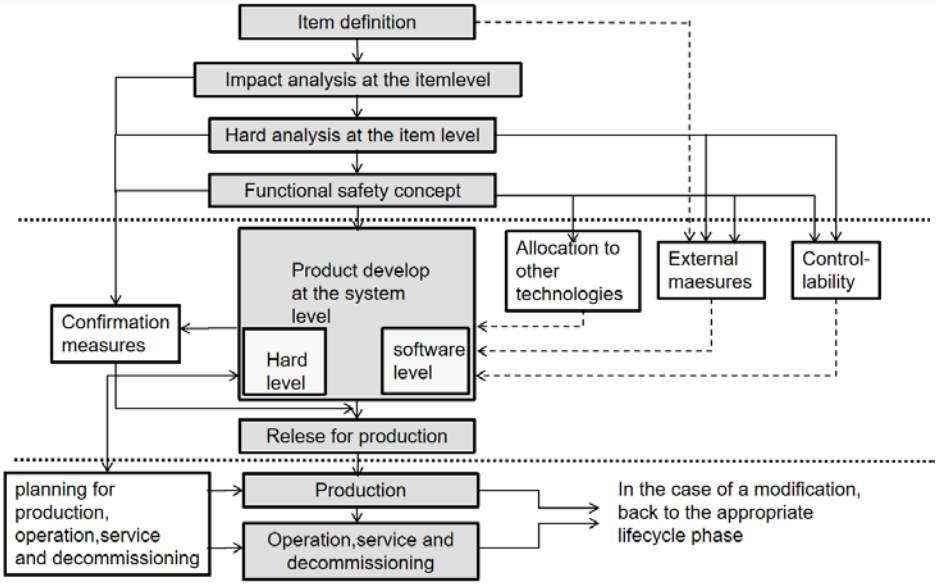

Fig.1 Safety Management Lifecycle

2. Introduction to Functional Safety Standards

The functional safety standard provides the relevant requirements and specifications for the safety development of automotive electrical systems in the safety lifecycle,and ensures the reliability and safety of products by improving process quality,organizational maturity and product quality. In each sub stage of the development process in line with functional safety,the required design input,work content and work results are clearly defined,and in principle,the organizational structure of functional safety management is relatively independent of the design team,which is specially responsible for the planning and coordination of safety activities and functional safety approval review, so as to reduce the system failure caused by human factors.Functional safety

  DOI: 10.25236/iwmecs.2020.036

standard provides a risk assessment method of “ASIL”,and reduces the risk caused by random failure of hardware by adding safety mechanism,so that the residual risk of the system is within the acceptable range[1].

3. Concept Design of Function Safety of Vehicle Controller

3.1 Project Definition

The functional requirements, operational requirements and boundary conditions of the vehicle controller need to be clarified first in the functional safety concept formulation stageThe project definition is the first stage of the development process. A clear and complete description and definition of the project will enable the participating developers to have a deeper understanding and understanding of the product and establish a clear product concept to successfully complete the follow-up process during the life safety cycle[2].

The whole vehicle controller is the core control component of electric vehicle. Its main responsibility is to analyze the driver's demand, monitor the running state of the vehicle in real time, coordinate the BMS,MCU and other control units, and realize the functions of power management, power up and down management, CAN bus communication management, energy feedback management, vehicle equipment management and fault diagnosis and processing.

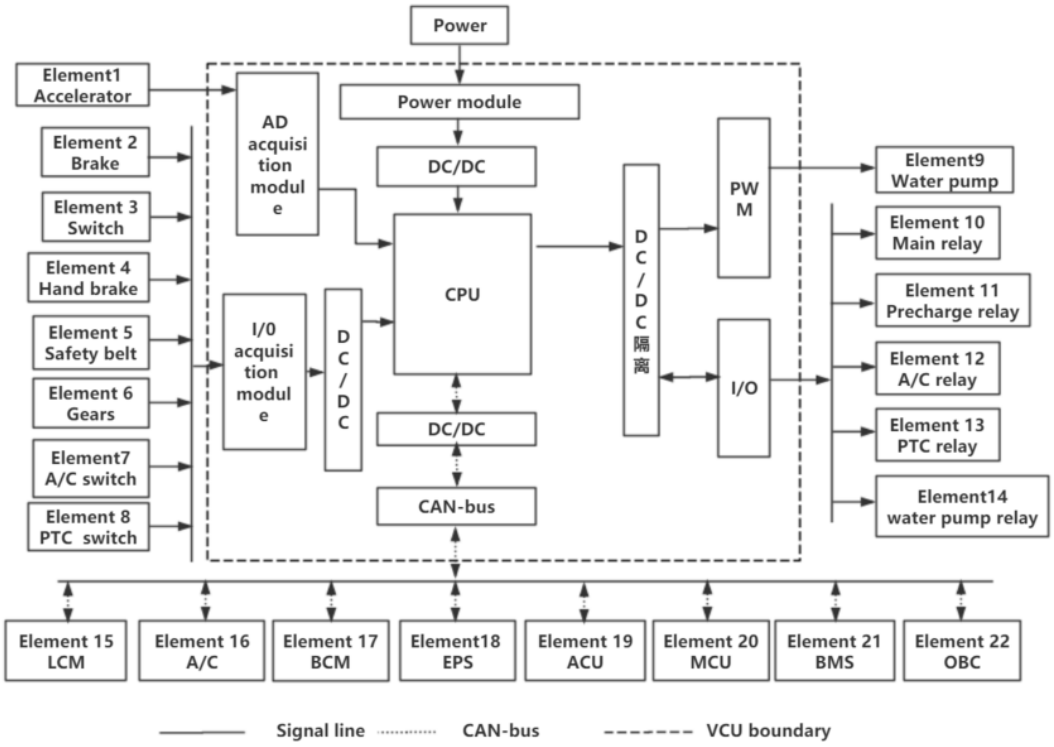

Fig.2 Functional Framework and Boundary of Vehicle Controller

3.2 Hazard Analysis and Risk Assessment

The main work of hazard analysis and risk assessment is to identify the whole vehicle class hazards caused by product failure and classify the vehicle safety integrity grade according to the standard. This section takes the power management function as an example to carry out the whole vehicle controller hazard analysis and risk assessment work[3].

3.2.1 Determination Ofasil Levels

Analysis the influence of vehicle controller failure on vehicle level , and whether the result of scene analysis is a hazard event or not. After completing the vehicle hazard identification of the vehicle controller failure, it is necessary to determine the vehicle safety integrity grade (A utomobile safety integrity levers,ASIL) of the identified risk. ASIL classification reference three

indicators: exposure, severity and controllability[4].

When the three indexes of vehicle class hazard event exposure, severity and controllability are determined, different ASIL levels will be assigned according to the above three indexes: QM,A,B,C,D, the ASIL A is the lowest safety level, the ASIL D is the highest safety level, and the QM is not related to safety.

3.2.2 Security Objective Confirmed

For the hazard event >QM the safety completion grade of the vehicle, at least one safety target should be set up for it, so that the vehicle can enter the safety state in time when the system fails, and avoid the occurrence of the hazard event. Similar safety targets can be synthesized as a safety target, but post-synthetic safety targets should inherit the highest vehicle safety completion level of the synthesized safety targets. Table 1 is the safety target after the vehicle controller power management confirmation.

Tab.1 Functional safety objectives of power management

Vehicle Class Hazard	ASIL grade	Security objectives
Large or small vehicle acceleration	ASILB	Avoid unexpected deviations from VCU torque commands
Vehicle lost acceleration	ASILC	Avoid unexpected interruptions to VCU torque commands
…	…	…

3.3 Concept Development for Functional Security

After completing the hazard analysis and risk assessment, it is necessary to formulate the functional safety concept of the whole vehicle controller according to the obtained safety objectives, formulate the corresponding functional safety requirements, and assign each subsystem to the preliminary architecture of the system, so as to provide the theoretical basis for the software and hardware development meter test of the whole vehicle controller.

In order to achieve the established safety goal, it is necessary to put forward the corresponding functional safety requirements for each safety goal and assign the corresponding ASIL grade, so as to facilitate the subsequent development of the vehicle controller to add the safety mechanism for each hazard event. To ensure that the random risk caused by the vehicle controller failure is reasonably avoided in the design process.As shown in Table 2, this paper, based on the initial architecture of the vehicle controller, completes the functional safety requirements formulation and A SIL grade distribution of each functional safety target.

Tab.2 Functional safety requirements of vehicle controller

Security objectives	Number	Functional security requirements	ASIL level
	FSR1	Analog acquisition circuit to provide accurate signal	ASIL B
	FSR1.1	Analog acquisition circuit to provide accurate signal	QM(B)
	FSR1.2	Need to apply diagnostic and security mechanisms to check	ASIL B (B)
	FSR2	ECU to receive signals correctly and process and transmit torque signals correctly	B
	FSR2.1	ECU to properly connect signals and process and transmit torque signals correctly	QM(B)
	FSR2.2	Need to apply diagnostic and security mechanisms to check	ASIL B (B)
…	…	…	…

According to the established functional safety requirements, it is necessary to complete the safety architecture design of the whole vehicle controller as shown in figure 3, and draw the summary table of the safety requirements of the whole vehicle controller as shown in table 3 as the basis for subsequent development.

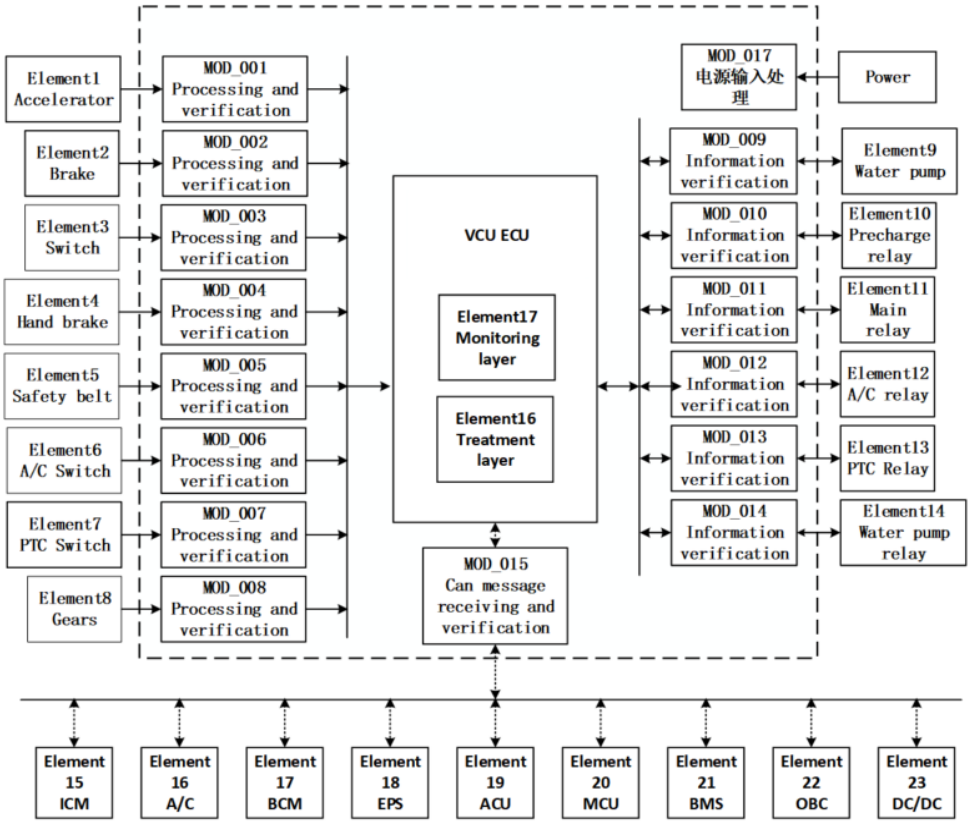

Fig.3 Safety Structure of Vehicle Controller

Tab.3 Functional safety requirements of vehicle controller

Relevant Item No.	Security requirements	Systems/subsystems	ASIL grade
MOD_001	Process accelerator pedal signal and verify	Analog data acquisition	C
MOD_002	Process brake pedal signal and verify	Switch collection	B
MOD_003	Process key switch signal and verify	Switch collection	C
…	…	…	…

4. Conclusion

On the basis of the requirements of the functional safety concept design of part 3 of the I SO26262 standard, from the relevant item definition, the HARA analysis is used to carry out hazard analysis and risk assessment of the potential failure of the vehicle controller, and the safety target and A SIL grade are formulated according to the impact of the failure at the vehicle level. According to the safety target and A SIL grade, the specific function safety requirements of vehicle controller are derived, and the safety architecture of vehicle controller is completed.

References

[1] ISO26262, Road Vehicles Functional Safety [S]. International standard: International Organizations for Standards, 2018.

[2] Oliver Koller, Robert Bosch. Automated ASIL Allocation and Decomposi-tion according to ISO26262, Using tne Example of Vehicle Electrical Systems for Automated Driving. Passeng. Cars-Electron. Electr.Syst, Vol.11,No.2,pp.123-130,2018.

[3] Volker Scheuch,Gerd Kaiser. A safe Torque Vectoring function for ele -ctric vehicle. World Electric Vehicle Journal, No.6, pp.731-740,2013.

[4] Anunay Krishnamurthy, Bastian Holderbaum. Functional Safety Concept of a H -ybrid Powertrain for a Heavy Duty Vehicle. ATZ Worldwide, No.09, pp.49-53,2018.