Conceptual Design of Functional Safety of Motor Control System Based on ISO26262

Dafang Wang¹, Peng Song¹, Zexu Xu¹, Guanglin Dong¹ and Hui Wei¹

¹ School of Automotive Engineering, Harbin Institute of Technology, Cultural West Road, Weihai, China

Abstract. This paper carries out the conceptual design of motor control system based on the standard of functional safety ISO 26262 for new energy vehicle. First, the paper introduce the main contents of the concept phase of ISO 26262. Then, the paper complete the item definition, hazard analysis and risk assessment of motor control system, and determine the functional safety goal and functional safety requirements.

1 INTRODUCTION

Automotive electronics technology has become one of the most innovative technologies in the automotive field. As the complexity and integration of automotive electrical and electronic systems continues to increase, the risk of systematic failures and random hardware failures may be inherently increased [1].

In recent years, functional safety has attracted more and more attention by automaker. Since the official release of IEC 61508 by the International Electrotechnical Commission in 2000, the standards of IEC 61511 for process industries, the standards IEC 62061 for machinery, and the standards IEC 61513 for nuclear industry have been successively introduced, the international standard system of functional safety has been gradually formed. However, IEC 61508 originating in the industrial sector does not fully apply to the automotive industry [2].

In order to ensure the safety of functions, the International Organization for Standardization (ISO) issued the international standard ISO 26262 of automotive electronic and electrical system functional safety, which provided guidance for the work process and management process related to functional safety in the whole life cycle [3]. ISO 26262, as functional safety standards, consists of the following parts, vocabulary, management of functional safety, concept phase, product development at the system level, product development at the hardware level, product development at the software level, production and operation, supporting processes, Automotive Safety Integrity Level (ASIL) -oriented and safety-oriented analyses and guideline on ISO 26262 [4], as shown in figure 1.

Motor Control System (MCU), as the core of the electric drive system, plays a crucial role in controlling the running state of the electric vehicle, such as the

starting and running of the electric vehicle, the advance and retreat speed, the climbing strength and so on. Therefore, the research of motor control system is of great significance in the background of the rapid development of new energy vehicle and the expansion of pure electric vehicle market.

In this paper, we take the development of motor control system as an example, to introduce the design and development of the third part of the ISO 26262 (the concept phase).

1.Vocabulary			
2.Management of functional safety			
3.Concept phase	4.Product development at the system level		7.Production and operation
	5.Product development at the hardware level	6.Product development at the software level	
8.Supporting processes			
9.ASIL-oriented and safety-oriented analyses			
10.Guideline on ISO 26262			

Figure 1. An overview of ISO 26262.

2 CONCEPTUAL DESIGN OF MOTOR CONTROL SYSTEM

The concept phase of functional safety is the beginning of safety lifecycle. Its purpose is to derive functional safety requirements from safety goal and assign them to the preliminary architectural elements or external measures of related items. The main activities in this phase are shown in Table 1.

* Corresponding author: {wdflcjl, talensong}@163.com, xuzexu49@163.com

Table 1. An overview of the concept phase.

Clause	Objectives
5. Item definition	1) To define and describe the item, its dependencies on and interaction with the environment and other items. 2) To support an adequate understanding of the item so that the activities in subsequent phases can be performed.
6. Initiation of the safety lifecycle	1) To make the distinction between a new item development and a modification to a existing item. 2) To define the safety lifecycle activities that will be carried out in the case of a modification.
7. Hazard analysis and risk assessment	To identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.
8. Functional safety concept	To derive the functional safety requirements from the safety goals, and to allocate them to the preliminary architectural elements of the item, or to external measures.

2.1 ITEM DEFINITION

The main function of motor control system is to convert the electric energy stored in battery into the electric energy required to drive the motor to control the running state of the motor, that is, the control of the motor torque.

Motor control system is based on the hardware circuit with embedded software and algorithms to achieve effective control of the motor. The software part mainly includes the writing of the low-level code and the architecture of the upper-level logic. The two complement each other and form a complete control algorithm. The input terminals of motor control system is the target torque based on the pedal, which have a corresponding curve between the pedal and the torque. The target torque corresponding to the depth of the pedal is transformed into the current vector to allocate the current to achieve the maximum torque control.

Motor control system is a closed loop system. The actual value is close to the target value and better response and follow the change state of the motor by adjusting of the feedback. The change in the magnitude of the torque on the inverter is the turn-on and turn-off time of the bridge arms. With the change of the torque, the current vector will also change, so the synthesized voltage vector will be different. The action time of each vector can be calculated, and the microcontroller will update and adjust in real time according to the time calculated by the algorithm.

The main components are the following parts.

1) Control module, including the corresponding hardware circuit and control strategy. The hardware

circuit mainly includes the microprocessor, the monitoring circuit, the hardware protection circuit and the communication circuit. The control strategy is mainly the software realization of the motor control algorithm.

2) Power conversion module, including power devices (MOSFET or IGBT), driving chip, driving resistance and capacitance, and so on. It can change the control signal from the microprocessor to the drive signal of the inverter, and realize the control of the voltage of the motor.

2.2 HAZARD ANALYSIS AND RISK ASSESSMENT

According to the characteristics of the automotive electronics, ISO 26262 defines Automotive Safety Integrity Level (ASIL). There are four levels of Automotive Safety Integrity Level, which are A, B, C and D, of which ASIL A is the lowest level, and ASIL D represents the highest level. The ASIL level determines the security requirements of the system. The higher the ASIL level, the higher the security requirements for the system.

The ASIL level is determined by three factors, which are severity, exposure and controllability. Among them, the severity represents an estimate of the potential harm in a particular driving situation, while the probability of exposure is determined by the corresponding situation. The controllability rates how easy or difficult it is for the driver or other road traffic participant to avoid the considered accident type in the determined operational situation.

ASIL classification rules as shown in Table 2. QM stands for Quality Management, which means that it is sufficient to develop a system or function according to a quality management system. The events of S0, E0 and C0 have no harm to drivers, pedestrians and vehicles, and therefore do not assess the ASIL level.

Table 2. ASIL determination.

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

The table can clearly identify the relationship between Automotive Safety Integrity Level and the degree of the risk. For the same potential risk, due to differences in the weather and road conditions of the country or region, as well as the habits of drivers and traffic participants, different Automotive Safety Integrity Level may be derived. The higher the ASIL level, the higher the security requirements for the system, and the

higher the cost to achieve this level. This means that the diagnostic coverage of hardware is high, the development process is strict, the corresponding development costs increase, the development period is extended, and the technical requirements is strict.

Before confirming the safety goals of motor control system, it is necessary to identify all of hazard events. Hazard analysis and risk assessment are performed for each hazard event, and safety goals of motor control system is confirmed at last.

For motor control systems, there are the following hazard events.

- 1) An unexpected increase of the motor output torque.
- 2) An unexpected reverse of the motor output torque.
- 3) Jitter of the motor output torque.

The Automotive Safety Integrity Level analysis process as shown in Table 3, Table 4, Table5.

Table 3. An unexpected increase of the output torque.

Hazard event	An unexpected increase of the motor output torque.	
Driving scene	Low speed, medium speed, high speed and driving on any road after starting the car.	
Severity	Instructions	Vehicle does not follow the intention of the driver and poses a threat to the lives of drivers, passengers and pedestrians.
	Value	S3
Probability	Instructions	It can happen in the current driving scene.
	Value	E4
Controllability	Instructions	The driver is in the car and cannot check and control the motor control system. It is not controllable.
	Value	C3
ASIL	ASIL D	

Table 4. An unexpected reverse of the output torque.

Hazard event	An unexpected reverse of the motor output torque.	
Driving scene	Low speed, medium speed, high speed and driving on any road after starting the car.	
Severity	Instructions	Vehicle does not follow the intention of the driver and poses a threat to the lives of drivers, passengers and pedestrians.
	Value	S3
Probability	Instructions	It can happen in the current driving scene.
	Value	E4
Controllability	Instructions	The driver is in the car and cannot check and control the motor control system. It is not controllable.
	Value	C3
ASIL	ASIL D	

Through the above analysis, we can determine the ASIL level of the three hazard events are ASIL D, ASIL D and ASIL B. Therefore, the ASIL level of motor control system should select the highest level of ASIL D.

The three hazardous events are all related to the driver's target torque, so we can confirm that the safety goal of motor control system studied in this paper is to prevent the torque that is not intended by the driver.

Table 5. Jitter of the motor output torque.

Hazard event	Jitter of the motor output torque.	
Driving scene	Low speed, medium speed, high speed and driving on any road after starting the car.	
Severity	Instructions	Vehicle does not move steadily according to the driving intention, and has a slight injury to the driver, the passenger and the pedestrian.
	Value	S1
Probability	Instructions	It can happen in the current driving scene.
	Value	E4
Controllability	Instructions	The driver is in the car and cannot check and control the motor control system. It is not controllable.
	Value	C3
ASIL	ASIL B	

2.3 FUNCTIONAL SAFETY CONCEPT

The objective of the functional safety concept is to derive the functional safety requirements from the safety goals, and to allocate them to the preliminary architectural elements of the item or to external measures.

In view of the safety goal of motor control system, this paper proposes the functional safety requirements as follows.

- 1) Motor control system should take measures to avoid generating torque that is not intended by the driver.
- 2) Motor control system should be able to detect the generation of torque that is not intended by the driver.
- 3) Motor control system should be switched to the safety state in time when the torque that is not intended by the driver is produced.

3 CONCLUSIONS

ISO 26262, as an international standard for the functional safety of automotive electronics and electrical products, provides new ideas and methods for research and development institutions and manufacturing companies in the field of vehicle. This paper finished item definition and hazard analysis and risk assessment for motor control system based on ISO 26262. And then, it determines the ASIL level of motor control system, proposes safety goal and functional safety requirements. It lays the foundation for the development of the work in the follow-up stage.d

REFERENCES

1. Liu Jiayi, Guo Hui, Li Jun, J., 2011. Shanghai Automotive, 2011 (10): 57-61, *The functional safety standard of automotive electrical and electronic systems ISO 26262*.
2. Ahistrom K, Torin J, Johannessen P, C., 2001. Engineering of Complex Computer Systems, 2001. Proceedings. Seventh IEEE International Conference on, 2001: 133-143. *Design method for conceptual design of by-wire control: two case studies*.
3. Simonot-Lion F. C., 2006. IEEE Symposium on Industrial Embedded Systems, IES'2006. *The design*

of safe automotive electronic systems: some problems, solutions and open issues.

4. ISO26262, 2011. *Road Vehicle Functional Safety*. Geneva IEC.