Development of ECU Hardware for EPS Conforming to Functional Safety (ISO26262)

T. ITO

The automotive safety standard ISO26262 (Functional Safety) was established in 2011, making compliance imperative for EPS, a main product of JTEKT. I will therefore introduce actual case examples of the application of functional safety within recent development of ECU hardware for EPS, with a focus on the newly added quantitative analysis of the fault of electronic components, and the development process that has been created.

***Key Words**: functional safety, ISO26262, hardware, process*

1. Introduction

The automotive safety standard ISO26262 (Functional Safety) was established in 2011, making compliance imperative for EPS, a main product of JTEKT. We have implemented the application of functional safety within the development of ECU hardware for EPS, an example of which has been provided in this report. Of the basic vehicle functions of driving, turning and stopping, EPS is an important vehicle component which bears the task of "turning". Malfunctions in EPS in particular may lead to dangerous situations while driving, and as such it is necessary in the development of EPS to apply ASIL-D (described hereafter), the highest of all functional safety levels. Functional safety development of automotive components can be divided into system development, hardware development and software development. For system development and software development, the development process is being defined and improved through Automotive SPICE activities, and as such this report will describe ECU hardware development with an expanded range of application in functional safety compliance. This description will focus mainly on the newly added quantitative analysis of the failure in components.

2. ASIL level of EPS

ASIL levels are determined by combinations of the three indices shown in **Table 1** with the classifications defined within these indices.

As shown in **Fig. 1**, ASIL level is determined as the most stringent ASIL-D when each index is at its highest classification, and decreases ASIL level as the classifications of each index decrease.

As seen in the following example, each index is at its highest classification for EPS, thus the ASIL of EPS is determined as ASIL-D, the most stringent level of the functional safety standard.

- Severity: EPS malfunction has the potential to lead to vehicle behavior unintended by the driver: S3
- Exposure: It is necessary to take into consideration straight driving, during which EPS malfunctions occur very frequently: E4
- Controllability: EPS output error greatly interferes with vehicle operation: C3

Table 1 Indices of ASIL determination

Index	Classification
Severity	4 classifications S0 (Low) through S3 (High)
Exposure	5 classifications E0 (Low) through E4 (High)
Controllability	4 classifications C0 (Easy) through C3 (Difficult)

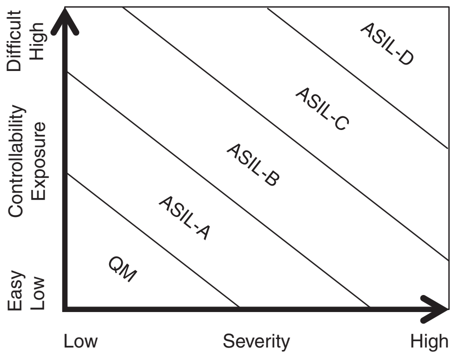

Fig. 1 Relationship of each index with ASIL

3. Requirements for functional safety compliance in ECU hardware development

ECU hardware for EPS is arranged as shown in **Fig. 2**.

This report defines mainly the following two items for compliance with functional safety in hardware development.

①Safety design which defines safety goals

②Quantitative analysis at failure of electrical hardware components

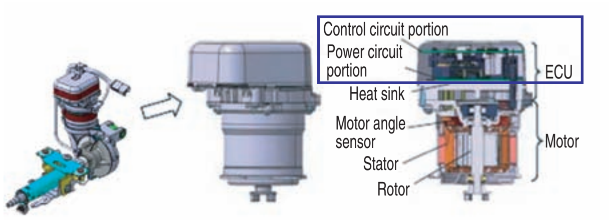

Fig. 2 Structural drawing of ECU/motor

3. 1 Safety design which defines safety goals

To verify the achievement of vehicle-level safety goals defined by automakers, it is necessary to follow the v-model of functional safety. As shown in **Fig. 3**, the v-model is development which ensures traceability from the safety goals up to hardware and software development.

More specifically, we narrow down safety goals into the functional safety requirements/concept (FSR/FSC) of the concept phase and the system-level technical safety requirements/concept (TSR/TSC), and implement safety design at the hardware and software levels by inputting the technical safety requirements/concept (TSR/TSC). The detailed hardware-level process, which is the subject of this report, is explained in the hardware design process of **Chapter 4**.

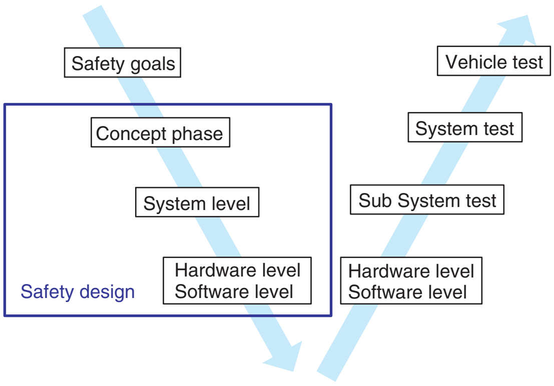

Fig. 3 V-model of compliance with functional safety

3. 2 Quantitative analysis at failure of electrical hardware components

In the conventional development method, FMEA at electronic component failure was conducted at the qualitative level. In contrast, the functional safety standard requires FMEDA to be conducted as a quantitative hardware analysis at electronic component failure, and evaluations of the following two items.

①Evaluation of the hardware architectural metrics

- Hardware failure coverage calculated for each safety goal

②Evaluation of safety goal violations due to random hardware failures

- Probability of hourly safety goal violations calculated for each safety goal

To enable the calculation of the latter item, we added to the conventional qualitative FMEA the component failure rate and the diagnostic coverage by the safety mechanism, as shown in **Fig. 4**. In quantitative FMEA, the component failure rate is a value determined by the type and size of the component as well as environment temperature, and the diagnostic coverage of the safety mechanism is determined by the detection method of the safety mechanism.

These items have been integrated in ⑧ and ⑨ of the hardware design process listed in **Chapter 4** and standardized.

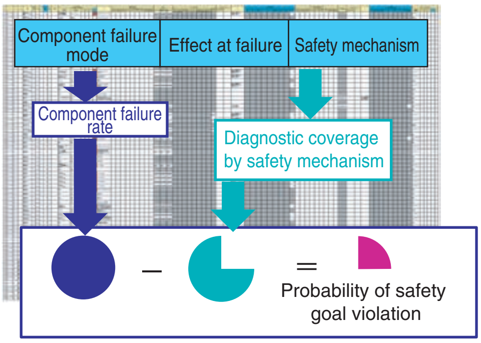

Fig. 4 Conceptual drawing of constant FMEA

4. Creation of hardware design process

Figure 5 shows the hardware design process compliant with functional safety that we have created.

The following explains the contents for implementation defined for each process.

①Hardware architecture design

- Input system architecture and design hardware architecture.

②Hardware safety analysis

- Input system safety analysis and implement safety analysis of hardware architecture.

③Hardware safety requirements (HSR) and hardware/software interface (HSI)

- Input technical safety requirements (TSR)/technical safety concept (TSC), and define hardware safety requirements (HSR) and hardware/software interface (HSI) through hardware safety analysis. This includes the safety mechanism and FTTI (fault tolerant time interval).

④Detailed hardware design

- Input hardware safety requirements (HSR) and hardware/software interface (HSI) and implement circuit design.

⑤Hardware design verification (qualitative)

- Implement FMEA at the electronic component level for circuits designed within the detailed hardware design, and verify whether safety design has been achieved on a comprehensive scale regarding safety requirements.

⑥Component failure rate/Component failure ratio (quantitative)

- Input components used in hardware and standards for failure rate calculation, and calculate the failure rate and failure ratio of each component.

⑦Diagnostic coverage by safety mechanism (quantitative)

- Calculate diagnostic coverage by the safety mechanism which detects the failures of each component.

⑧Evaluation of hardware architectural metrics (quantitative)

- Add component failure rate/component failure ratio and diagnostic coverage by safety mechanism to electronic component-level FMEA to create FMEDA. From FMEDA, calculate the single-point fault metric (SPFM) and latent fault metric (LFM) for each safety goal, and conduct evaluations.

⑨Evaluation of safety goal violations due to random hardware failures (quantitative)

- From FMEDA, calculate the probabilistic metric for random hardware failures (PMHF) for each safety goal, and conduct evaluations.

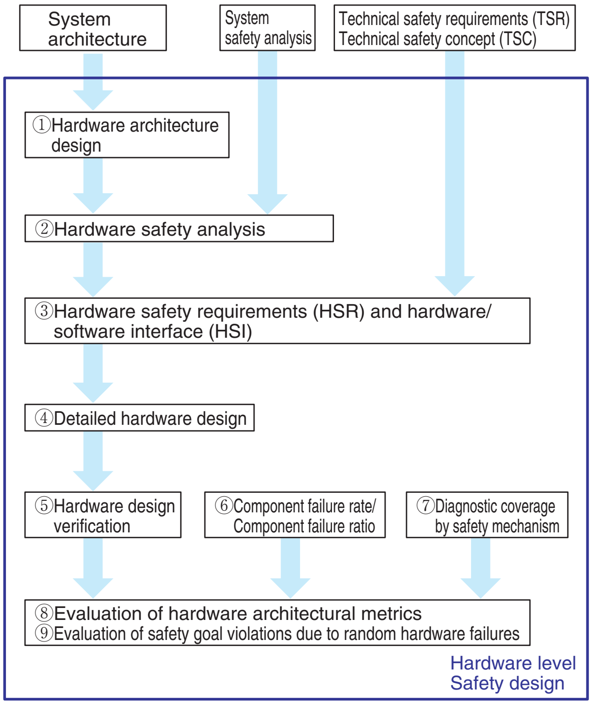
System architecture
System safety analysis
Technical safety requirements (TSR)
Technical safety concept (TSC)
①Hardware architecture design
②Hardware safety analysis
③Hardware safety requirements (HSR) and hardware/software interface (HSI)
④Detailed hardware design
⑤Hardware design verification
⑥Component failure rate/Component failure ratio
⑦Diagnostic coverage by safety mechanism
⑧Evaluation of hardware architectural metrics
⑨Evaluation of safety goal violations due to random hardware failures
Hardware level Safety design

Fig. 5 Hardware design process

5. Conclusion

We have achieved the creation of a hardware development process for EPS that is compliant with functional safety, and furthered product development. We will hereafter continue activities for improvement and, in non-EPS hardware components as well, deploy and standardize the hardware design process which we have created.

T. ITO*

* *Electronics Engineering Dept.1, Steering Systems Operations Headquarters*