

System Design Process in Compliance with ISO26262 Using Model-Based Design

Hiroki SAGAMI* Shinji HIRONAKA*
Ryoji MORI* Takuyuki MUKAI*

ABSTRACT

It is necessary for automotive electrical and/or electronic systems to conform to the functional safety standard ISO 26262. ISO 26262 stipulates the implementation of Processes and the creation of Work Products in order to prove safety. However, ISO 26262 is based on a V-model development process, and the definition of structures and requirements at the design stage affects whether or not there is an increase in person-hours across the course of the development as a whole. The research discussed in this paper therefore focused on the system design stage, an upstream process, and formulated a system design process that conforms to ISO 26262 using model-based design as a means of controlling increases in person-hours. As a result, a process was formulated that makes it possible to implement processes conforming to ISO 26262 and create Work Products as a series of procedures, in addition to accurately defining structures and requirements by means of models.

1. Introduction

The functional safety standard ISO 26262 (Fig. 1) officially came into effect in November 2011⁽¹⁾. This standard seeks to ensure safety through the reduction of potential risks associated with automotive electrical and/or electronic systems to allowable levels. In order to conform to this functional safety standard, it is necessary to implement a development process and create Work Product (WP)s that provide theoretical proof of safety as specified in the standard.

However, because there are numerous requirements to be met in order to conform to the standard, there are concerns that the person-hours involved in development will increase in comparison to developments conducted prior to its issuance. In addition, the basis of ISO 26262 is a V-model development process, and waterfall development featuring stage-by-stage design and verification is fundamental to the process⁽²⁾. As Fig. 2 shows, in a V-model development process, the further upstream the design stage is, the further downstream verification becomes. Given this, the accuracy of design more strongly affects the amount of

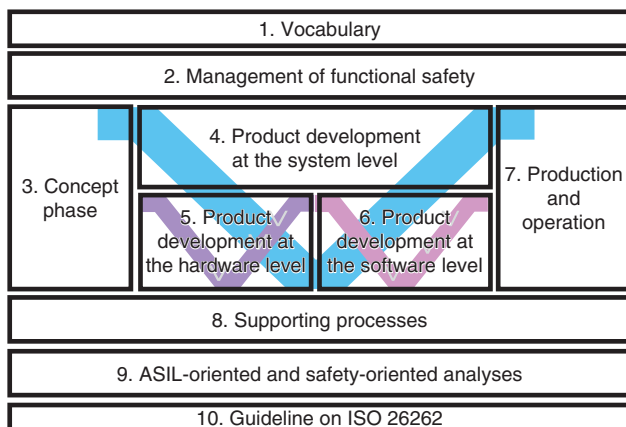


Fig. 1 Overview of ISO 26262

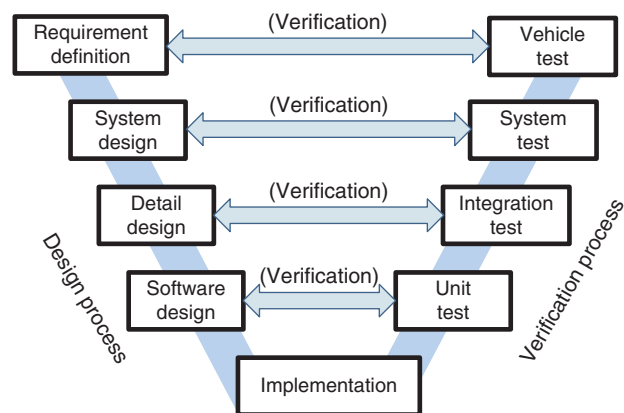


Fig. 2 General V-model development process

* Automobile R&D Center

rework that will be required the more upstream the design process is, and this is ultimately linked to increased person-hours. Against this background, determining how to control the increases in person-hours that are predicted to result from conforming to the standard is an issue for the future development of electrical and/or electronic systems.

The research discussed in this paper therefore focused on the system design stage, an upstream process of the V-model development process (corresponding to ISO 26262 Part 4), and developed an ISO 26262-compliant system design process using model-based design as a means of addressing the issue.

2. Goals of Development of Process

Figure 3 shows an overview of ISO 26262 Part 4. Part 4 of the standard stipulates the implementation of a V-model development process at the system level. The clauses that relate specifically to the design stage are Clauses 6 and 7. The focus of Clause 6 is the specification of the technical safety requirements, and it stipulates the definition of concrete methods of reducing potential risks in systems to help to ensure safety based on system characteristics. The focus of Clause 7 is system design, and it stipulates the definition of the system structures necessary for the realization of the technical safety requirements defined in Clause 6.

As indicated in Chapter 1 above, in order to conform to ISO 26262, it is necessary to implement the development process and create the WPs stipulated by the standard. Determining how to link the implementation of the development process and the creation of the WPs is an important factor in attempting to conform to ISO 26262 while at the same time controlling increases in person-hours.

In addition, because the system-level design process is an upstream process in terms of the development as a whole, it is essential to identify and express a certain amount of necessary information. Test verification will be conducted at the system level in the processes downstream from system design following the development of hardware (HW) and software (SW) in order to realize the design. As a result, identifying information with a high degree of precision and making accurate determinations with regard to requirements and structures are also important in limiting

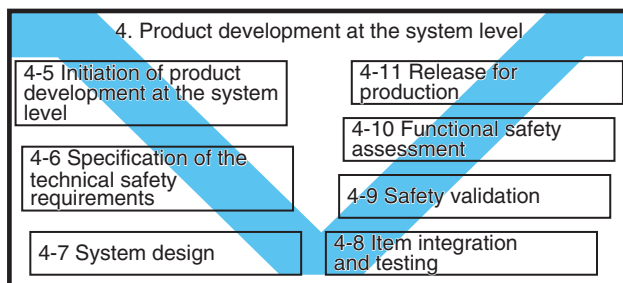


Fig. 3 ISO26262 Part 4

the amount of rework in later stages.

Based on the above considerations, the following goals were set for process development:

- (1) The development of a mechanism making it possible to directly reflect the information obtained as a result of the design process in the WP.
- (2) The development of a mechanism making it possible to accurately define requirements and structures related to functional safety at the system level.

3. System Design Process conforming to ISO 26262

3.1. Overview of Process

Model-based design (Fig. 4) was employed in order to implement the V-model development process stipulated by ISO 26262. Model-based design is an effective method for the efficient implementation of a V-model development process. Here, a model is defined as expressing the results of identification and organization of system information. The model expressing the system includes the system structures, the requirements demanded of the system, and the behavior of the system. System modeling languages (SysML) are among the methods available for the notation of the model⁽³⁾. In addition to making it possible to eliminate ambiguity and define the system at an early stage of the design process, the use of model-based design in which a model is employed in design also makes it possible to conduct verifications at an early stage through the use of the model in simulations. Hierarchization of the model also makes it possible to increase the detail of requirements and specifications in stages, helping to enable clear expression of the connections with upstream and downstream processes. Based on the above, the use of the method can be expected to control increases in person-hours by helping to eliminate ambiguities and oversights from system definitions, thus doing away with factors requiring rework.

During this development of an ISO 26262-compatible system design process, the hierarchy of system structures

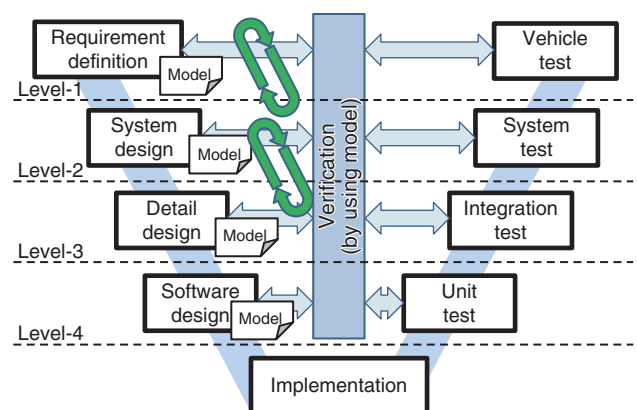


Fig. 4 V-model development process using model-based design

and requirements shown in Fig. 5 was defined in order to make it possible to express systems by means of models. SG are the safety goals necessary at the top level for the avoidance of hazardous events, and FSR are the functional safety requirements necessary at the concept level in order to realize the SG. TSR1 are the technical safety requirements defined as the methods of realizing the FSR, and TSR2 are further elaborations of these methods of realization of the FSR (this includes discrimination of HW and SW, allocation to elements, etc.). Figure 6 shows an example of the expression of a hierarchy using SysML.

The design process for structures and requirements at the system design level to help ensure conformity to ISO 26262 will be discussed below.

3.2. Process of Specification of Technical Safety Requirements

Technical safety requirements are defined as the concrete methods of realization of the functional safety requirements, the safety requirements at the concept level. Failsafe technologies and other concrete specifications are defined by further elaboration of the technical safety requirements. ISO 26262 stipulates that technical safety requirements should be defined with no oversights in order to help ensure that no hazardous events occur as a result of system failures.

Figure 7 shows the process of specifying technical safety requirements accurately and without oversights. In the explanation of the process that follows, it is assumed that the concept-level structures and the allocated FSR have already been defined as prerequisites, as shown in Fig. 7(a).

3.2.1. Definition of preliminary architectural assumption

The upper-level requirements (the concept-level

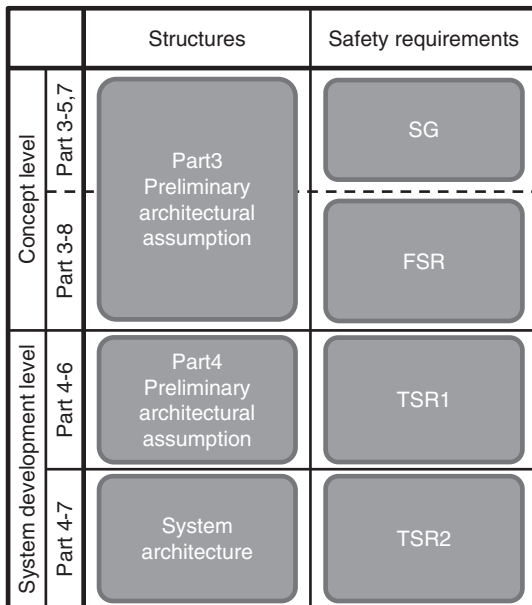


Fig. 5 Hierarchical definition of structures and requirements

requirements) are analyzed, and the methods of realizing the concept and the preliminary architectural assumption of the structures at the system level are defined [Fig. 7(b)].

3.2.2. Implementation of safety analysis

A safety analysis (e.g., FTA⁽⁴⁾, FMEA⁽⁵⁾, or HAZOP⁽⁶⁾) is conducted in relation to the preliminary architectural assumption, and any elements that might lead to violate safety goals, and the failure modes of those elements, are identified [Fig. 7(c)].

3.2.3. Definition of TSR1

TSR1 are defined as methods of helping to prevent the occurrence of hazardous events as a result of the failure modes of the elements identified in Section 3.2.2 and of realizing FSR, the upper-level requirements [Fig. 7(d)].

3.3. System Design Process

The purpose of system design is to determine the structures that will realize the technical safety requirements. In ISO 26262, in order to fulfill this purpose, it is necessary

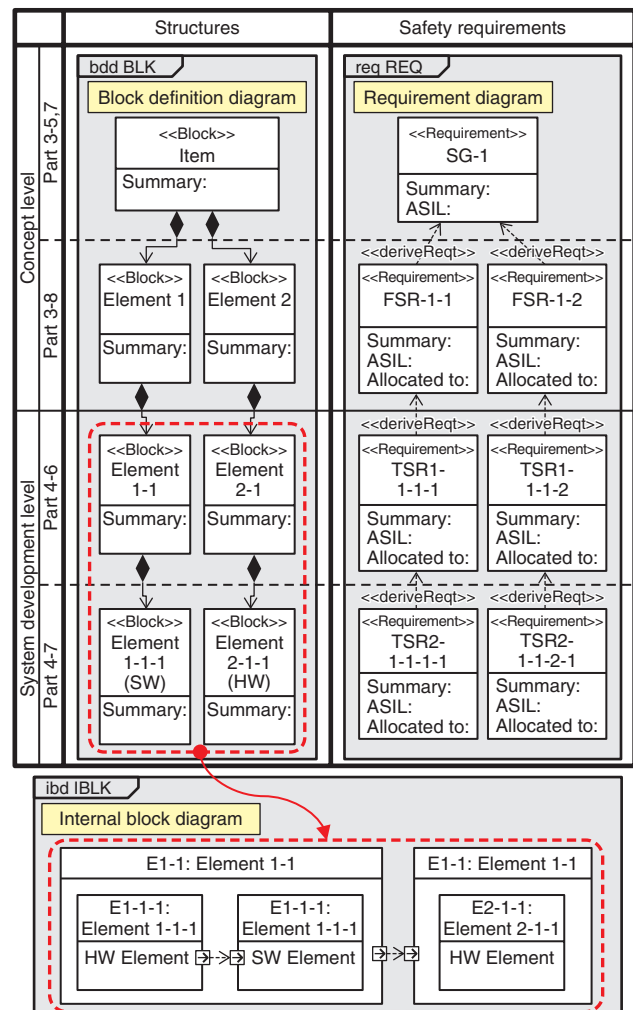


Fig. 6 Structure and requirement definition using SysML

to specify the elements that will realize the technical safety requirements, clarify the roles of HW and SW in realizing the technical safety requirements, and specify the interfaces between HW and SW elements.

A process of determination of structures, incorporating the above items, relating to the TSR1 defined in Section 3.2 will be discussed in this section (Fig. 8).

3.3.1. Definition of system architecture

An architecture that has been further elaborated in relation to the system requirements and preliminary architectural assumption defined in Section 3.2.1. up to the stage at which the roles of HW and SW are able to be specified is defined as the system architecture [Fig. 8(a)].

3.3.2. Implementation of safety analysis

A safety analysis of the system architecture defined in Section 3.3.1. is conducted, and elements of the system

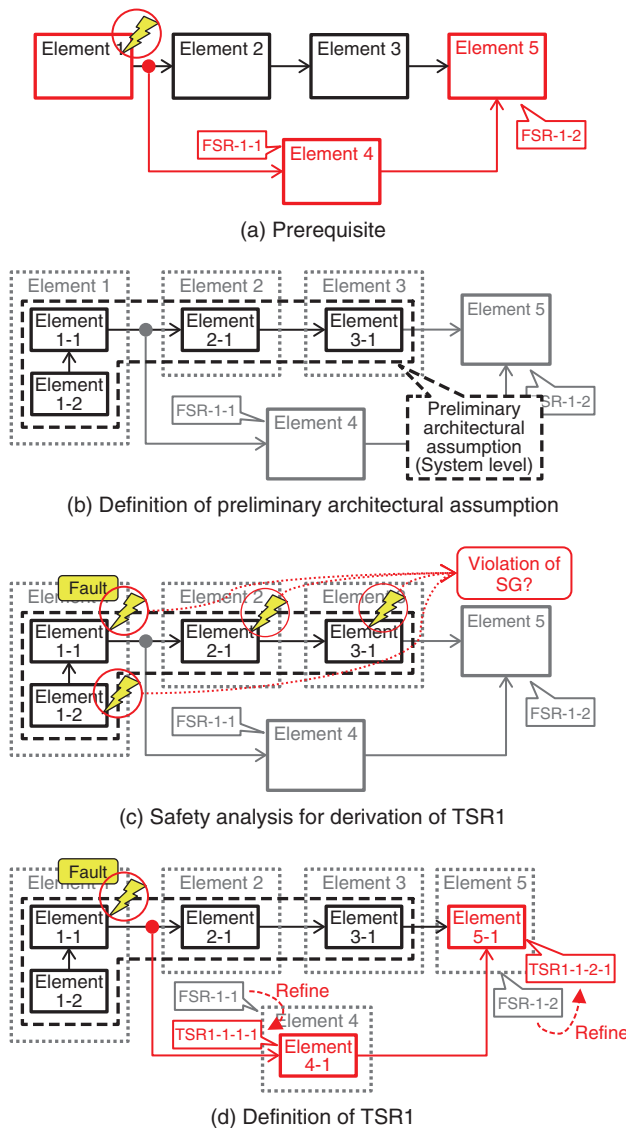


Fig. 7 Procedure for derivation of TSR1

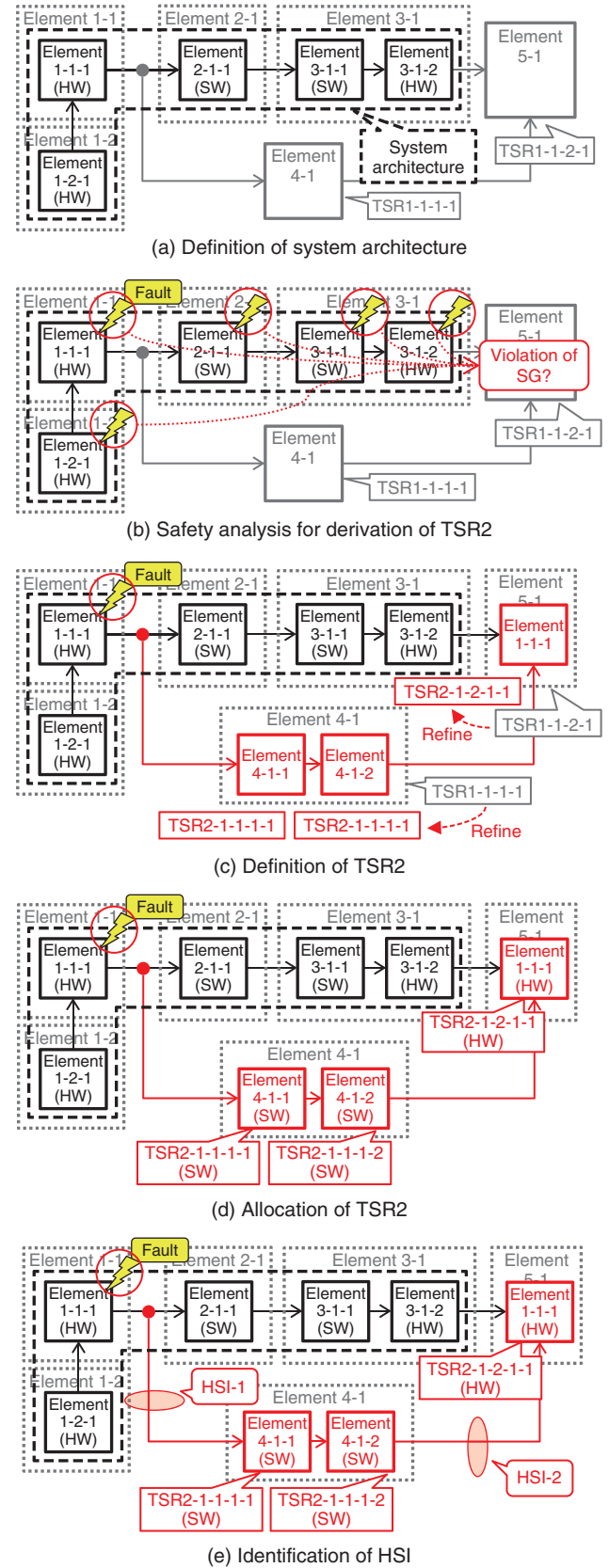


Fig. 8 Procedure for system design (Including derivation of TSR2)

architecture that might lead to violate safety goals, and the failure modes of these elements, are identified. However, where elements that will not lead to violate safety goals have been identified in the safety analysis conducted in Section 3.2.2., it is not necessary to conduct a safety analysis when these elements are updated later in the process [Fig. 8(b)].

3.3.3. Definition of TSR2

The TSR1 defined in Section 3.2.3 are further elaborated to the stage at which the roles of HW and SW can be specified in relation to the failure modes of the elements of system architecture identified in Section 3.3.2. The results of this process are defined as TSR2 [Fig. 8(c)].

3.3.4. Allocation of TSR2 and determination of roles of HW and SW

The TSR2 defined in Section 3.3.3 are allocated to the elements of the system architecture. If necessary in order to realize the TSR2, new elements are added to the system architecture at this time. The respective roles of HW and SW are also defined [Fig. 8(d)].

3.3.5. Definition of hardware-software interfaces

HW and SW elements related to the TSR2 are specified in the updated system architecture formulated in Section 3.3.4. Interface specifications in areas in which HW elements and SW elements are directly connected are defined as hardware-software interfaces (HSI) [Fig. 8(e)].

4. Creation of WPs

4.1. Overview of WPs

ISO 26262 stipulates the formulation of technical safety requirements as WPs for Part 4-Clause 6, and of technical safety concepts, system design specifications, and HSI specifications as WPs for Part 4-Clause 7. All of these are essential documents proving theoretical compliance with functional safety standard ISO 26262, and it is necessary to formulate them having implemented the process demanded by the standard.

The development of a process to help ensure conformity to ISO 26262 was discussed in Chapter 3. Given this, it would be sufficiently possible to prove theoretical compliance with the functional safety standard via the WPs if the information obtained in the implementation of this process was reflected in them.

This section will therefore discuss a procedure for the creation of WPs based on the process discussed in Chapter 3.

4.1.1. Specified technical safety requirements

The TSR1 and TSR2 respectively formulated in Sections 3.2.3. and 3.3.3. are organized to become WPs for technical safety requirements. It is possible, by reflecting the information obtained as a result of the hierarchical design process (including traceability information) in the WPs, to formulate documents able to prove compliance with the

Table 1 Example of work product of TSR

SG	FSR	TSR1	TSR2
SG-1	FSR-1-1	TSR1-1-1-1	TSR2-1-1-1-1
			TSR2-1-1-1-2
		TSR1-1-1-2	TSR2-1-1-2-1
	FSR-1-2		TSR2-1-1-2-2
		TSR1-1-2-1	TSR2-1-2-1-1
...	...	...	...

Table 2 Example of work product of technical safety concept

TSR2	Allocated system element	HW or SW
TSR2-1-1-1-1	Element A	HW
TSR2-1-1-1-2	Element B	SW
TSR2-1-1-2-1	Element C	HW
...	...	...

Table 3 Example of work products of HSI

Description	HW			SW			Interface type	Related TSR2
	Symbol	Range	Unit	Symbol	Range	Type		
XXX1	xxx1h	0 to 5	V	xxx1s	0 to 255	Byte	A/D	TSR2-1-1-1-1
...								

functional safety standard without any additional work. For example, if TSR1 and TSR2 are formulated using SysML requirement diagrams, it is possible to use the requirement diagrams themselves as WPs. As another example, the process from FSR to TSR2 can be organized and expressed as a table, as shown in Table 1.

4.1.2. Technical safety concept and system design specifications

The results of allocation of TSR2 to the elements of the system and of the selection of the roles of HW and SW are organized as WPs for the technical safety concept. It is sufficient to clearly express the subjects of allocation of TSR2 and the roles of HW and SW, as shown in Table 2.

4.1.3. HSI specifications

The interfaces between the HW and SW elements specified in Section 3.3.5 are organized as WPs for HSI specifications. Documents of the type shown in Table 3 can be used as HSI specifications documents.

5. Case Study of Application to Electric Power Steering Control System

Electric power steering (EPS) systems are systems designed to reduce the steering load for the driver. These systems determine the amount of assistance to output based on the driver's steering torque.

Using a representative example of EPS, this chapter will present a case study of the application of the process developed in Chapters 3 and 4 to an actual development.

5.1. SG and FSR

For this discussion of an example of system design in relation to functional safety in EPS systems, a representative example of an EPS system, with a concept definition including the SG and FSR necessary as preconditions, has been defined. SG is defined as prevention of output that would turn the vehicle against the driver's intentions. FSR is defined as isolation of output when a failure in the steering torque detection function is detected. The concept architecture based on the above was defined as shown in Fig. 9.

5.2. Formulation of TSR1

Figure 10 shows the preliminary architectural assumption for the EPS system at the system level. Steering torque is detected by a torque sensor, and the amount of

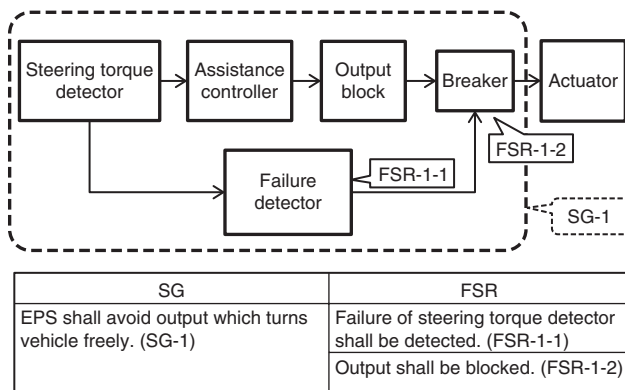


Fig. 9 Example of SG, FSR, and architecture at concept level

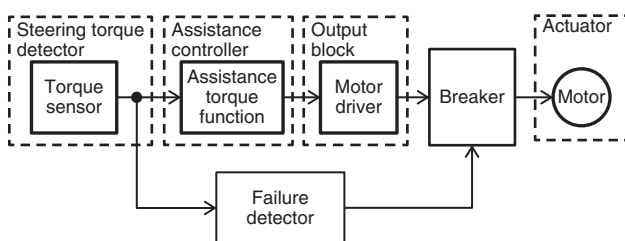


Fig. 10 Example of preliminary architectural assumption at system level

assist provided is determined based on the figure output by the sensor. Motor control is applied in order to output the amount of assist, and the actual amount of assist is output by the motor.

Based on this preliminary architectural assumption, the factors of failure which might lead to violate the SG set in Section 5.1. were analyzed. The results showed that if a failure in torque sensor output resulted in the output of a figure that deviated from the specified range, and an inappropriate amount of assist was calculated and output, there is a possibility that SG is violated and a hazardous event might occur. Based on these results, TSR1 was defined as the cutting off of motor drive by means of a relay function if torque sensor output deviated from the specified range for a specific period or longer (Fig. 11).

5.3. Formulation of TSR2

Figure 12 shows the system architecture of the EPS system. This is the result of further elaboration until the roles of HW and SW in relation to each element of the preliminary architectural assumption formulated in Section 5.2. can be discriminated. Here, another analysis

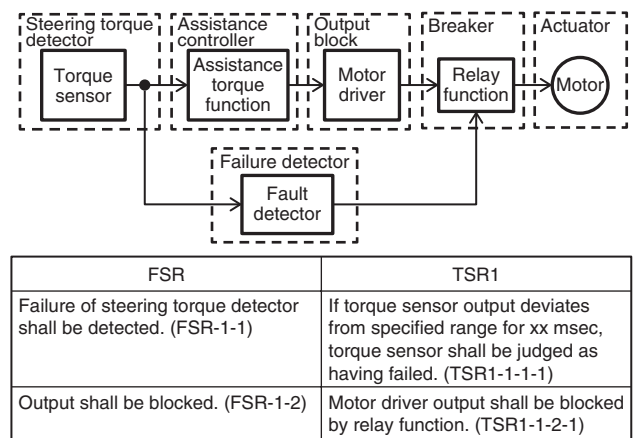


Fig. 11 Example of TSR1 and refined preliminary architectural assumption at system level

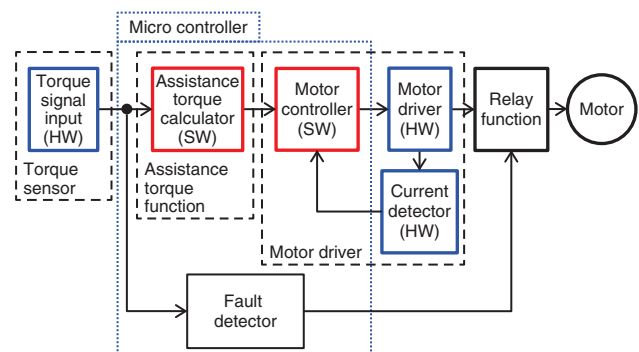


Fig. 12 Example of system architecture

of elements at the system architecture level was conducted. The results showed that if a failure occurred in the torque signal input, an HW element, the phenomenon identified in Section 5.2. would occur. Based on these results, TSR2 was defined as the cutting off of motor drive by means of a relay if the output of the torque signal input deviated from the specified range for a specific period or longer.

In addition, TSR2 was compartmentalized and allocated to elements of the system architecture. The TSR2 allocated to the torque sensor failure detector, an SW element, was defined as monitoring the deviation of the output of the torque signal input from the specified range for a specific period. The TSR2 allocated to the relay controller, an SW element, was defined as outputting instructions to switch the relay off. The TSR2 allocated to the relay, an HW element, was to cut off the output of the motor drive by switching the relay off. Based on these results, the system architecture was updated as shown in Fig. 13.

5.4. Formulation of HSI

In the updated system architecture formulated in Section 5.3., the interfaces between the torque signal input and the torque sensor failure detector, and between the relay controller and the relay, were related to TSR2, and were therefore identified as elements subject to definition as HSI (Fig. 14).

5.5. Effect of Application of Development Process

As a result of application of the newly formulated development process in the design of an EPS system, it

was possible to eliminate potential factors that could lead to violate safety goals and result in rework in downstream processes. As one example, the verification accuracy of the reviews, simulations, and other procedures conducted at the design stage to identify and eliminate elements has been increased, thanks to system structures and requirements being clearly and hierarchically defined. In addition, because the system architecture made clear the subjects of HW and SW development in downstream processes, it was possible to eliminate factors originating in oversights when communicating information.

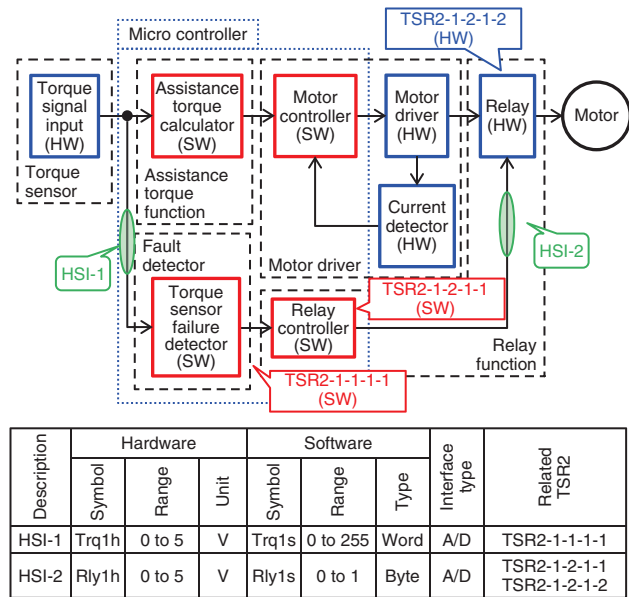


Fig. 14 Example of HSI

6. Conclusion

A new development process has been formulated with the following results:

- (1) It was possible to control increases in the person-hours associated with the creation of WPs by directly reflecting information obtained in the design process in the WPs.
- (2) It was possible to control increases in person-hours by hierarchically defining system structures and safety requirements in order to reduce the number of factors that might lead to violate safety goals and result in rework.

References

- (1) ISO26262: Road Vehicles – Functional Safety (2011)
- (2) Murakami, M., Nomura, K., Hisaki, T., Kasahara, Y.: System Modeling Technology for Powerplant Control

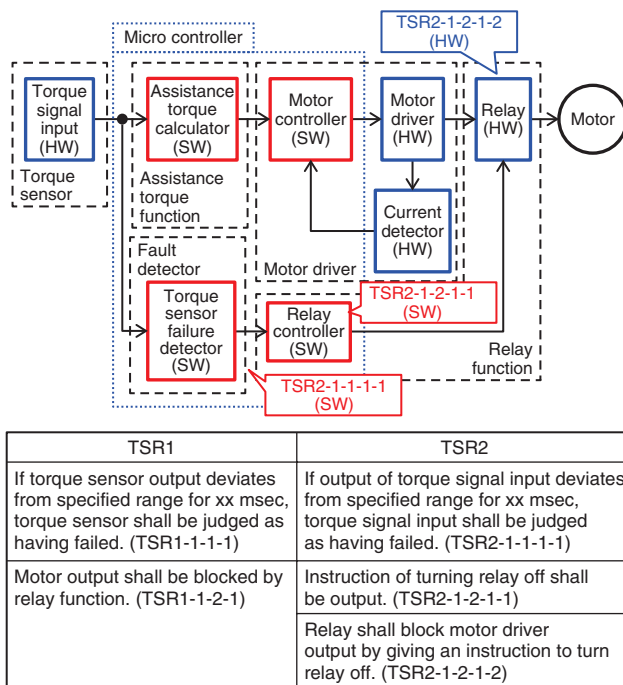


Fig. 13 Example of TSR2 and refined system architecture

Systems, Honda R&D Technical Review, Vol. 22, No. 2,
p. 101-108

- (3) <http://www.omgsysml.org/>
- (4) IEC61025: Fault tree analysis (FTA) (2006)
- (5) IEC60812: Analysis techniques for system reliability –
Procedure for failure mode and effects analysis (FMEA)
(2006)
- (6) IEC61882: Hazard and operability studies (HAZOP
studies) – Application guide (2001)

■ Author ■



Hiroki SAGAMI



Shinji HIRONAKA



Ryōji MORI



Takuyuki MUKAI